JOURNAL OF
INFORMATION SYSTEMS
APPLIED RESEARCH

Volume 14, Issue. 3
September 2021
ISSN: 1946-1836

In this issue:

iscap
Information Systems
& Computing
Academic Professionals

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer reviewed academic journal published by ISCAP, Information Systems and Computing Academic Professionals. Publishing frequency is three to four issues a year. The first date of publication was December 1, 2008.

JISAR is published online (https://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (https://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of ISCAP/EDSIG who perform the editorial and review processes for JISAR.

2021 ISCAP Board of Directors

Journal of
Information Systems Applied Research

Analysis of Security Features and Vulnerabilities in Public/Open Wi-Fi

Jason E James
jason.james@indstate.edu
School of Criminology and Security Studies
Indiana State
Terra Haute, IN 47809

Abstract

As a student at a university or college, have you ever, whilst using the local wireless hotspot sitting in the campus common area, library, coffee shop, food court, or in classroom buildings, had the feeling that someone is looking over your shoulder at what you are doing on your computer? Indeed, someone might be, but it's not what you think. Hackers are looming everywhere looking to steal your personal information and identity. The author used Kali Linux and Ubuntu OS to discover and analyze students who use open Wi-Fi (Wireless Fidelity) and the security risks they are exposed to and associated safeguards they can take. In this paper, the author analyzed the security features and vulnerabilities of the open Wi-Fi's like Starbucks, McDonald's, Panda Express, and college campus free attwifi, by using both active and passive attack methods. For active attack, the author performed MAC address spoofing, SSL Stripping, and DHCP Exhausting attacks. For passive attack, the author captured the pcap file and used Wireshark for analysis.

Keywords: Open Wi-Fi, security, vulnerabilities, colleges/universities, Kali Linux

1. INTRODUCTION

In the age of technology, Wi-Fi has significantly changed the way we work and play, enabling us to interact with the digital world from anywhere in the physical world. In fact, elementary, middle and high schools, and colleges and universities are offering Wi-Fi. Some provide the networks with a required login access and/or open, unencrypted and free for anyone to jump on (Siciliano, 2017). The explosion of free, public Wi-Fi has been an enormous godsend for college and university students. In fact, many colleges and universities have free access points all over campus, including those provided by retail and service giants like Starbucks, Barnes and Nobles bookstores, Comcast, and AT&T and students are rarely more than a short trip away from access to a campus network. Unfortunately, the freedom of connectivity 24/7 comes at a price, though, students are at risk from hackers that are looking to steal their identity. Students and many users of open Wi-Fi truly do not understand the risks associated with these connections (Kapersky Lab, 2017).

Hundreds of thousands of students use campus or open public Wi-Fi every day, but are they protecting themselves when they use it? With growing needs for wireless networks in colleges and universities, problems created by an attacker exploiting the networks is also growing. Attackers exploit open Wi-Fi security networks and listen to the traffic and retrieve sensitive information. In fact, students using open Wi-Fi networks, particularly in a university setting, can have their personal information compromised and become a victim of identity theft before they even graduate and can cause issues when trying to gain employment. Lack of protection over open Wi-Fi and ignorance with wireless security may cause very big damage to sensitive data of an individual. So, it is very important to understand the vulnerabilities and the solutions in order to protect your identity and make it more complicated for attackers.

2. BACKGROUND ON WIFI

Wi-Fi is a type of wireless local area network (WLAN) technology that enables an electronic device, such as a laptop, tablet, or smartphone, wireless access to applications, data, information and media, without the constraints of physical hardware connecting the devices to the Internet using radio waves. The core technology behind Wi-Fi is a device called an access point (AP), which acts like a bridge between the wired network and the Wi-Fi network. The access point, in turn, typically connects to the Internet via a network router (Kasten, Okhrimets & Kharchenko, 2015).

Wireless is about convenience not being restricted by physical infrastructure of one location. It allows wireless enabled devices to access a network or other devices when within range of one another. Wireless networks can be created relying on wireless network technology. College and universities have increased Wi-Fi hotspots significantly over the past several years and are now offering free open Wi-Fi through companies like AT&T and X-Finity, as well as the college or university network. Wi-Fi eliminates the constraints of physical hardware and can result in a significant cost saving (Rudman, 2008).

Many colleges and universities provide Internet connection via APs throughout campus. This type of connection requires a login name and password to access. Most people, let alone students, think when they "login," their session is encrypted and secure. However, logging in with a user name and password doesn't necessarily mean it's a secure network. The traffic on many campus networks requiring a login is unencrypted, which means anyone who connects to the network with the right "sniffing" tools can see everyone's information (Siciliano, 2017).

In order to prevent attackers from stealing data, Wi-Fi includes a set of protocols for user device authentication and data encryption. The protocols, which reside on both the access point and the connecting device, use a pre-defined passphrase or other form of unique identification to authorize the user and encrypt data so that it can only be accessed by a designated device. WPA/WPA2, the currently recommended security standard, uses a pre-shared key (PSK) in the form of a series of text letters to authenticate users and encrypt data (Kasten, Okhrimets & Kharchenko, 2015).

When connecting to a campus network that requires a login and password, the easiest way to know if it has encryption is to view the list of wireless networks from your wireless control panel by looking at the properties by right clicking or just hovering over each with your mouse. If the Wi-Fi states a *WPA* or *WP2* password is required then the network has encryption. However, if it's labeled *WEP*, it also has encryption, but at an unacceptable level that is easily hacked. If the Wi-Fi does not state anything and just requires a login and password then it is unsecure (Siciliano, 2017).

The other type of Wi-Fi on campuses is provided by a third party free of charge such as AT&T, Comcast, and even Starbucks and Barnes and Nobles. This type of Wi-Fi connection requires no username or login credential and allows guests to access the Internet via unsecured access. Many colleges and universities offer this type of access to guests.

3. RISKS ASSOCIATED WITH OPEN WI-FI

In many colleges and universities, open public access points, called "hotspots," allow students Internet access. As discussed previously, those APs may be provided by AT&T, Comcast, and even Starbucks and Barnes and Nobles. In other words, if a student is sitting in a in a common area on campus or in the Starbucks café, they can access the one of these channels to connect to the Internet. Unfortunately, these open hotspots also allow anyone within the area to potentially read data that is not meant for them (Kasten, Okhrimets & Kharchenko, 2015).

The same features that make these free Wi-Fi hotspots desirable for students make them desirable for hackers; namely, that it requires no authentication to establish a network connection. This creates an amazing opportunity for the hacker to get unfettered access to unsecured devices on the same network.

The biggest threat to free Wi-Fi security is the ability for the hacker to position himself between you and the connection point. So instead of talking directly with the hotspot, you're sending your information to the hacker, who then relays it on.

While working in this setup, the hacker has access to every piece of information you're sending out on the Internet: important emails, credit card information and even security credentials to your business network. Once the hacker has that information, he can — at his leisure — access your systems as if he were you (Kapersky Lab, 2017).

Some of the ways a student's privacy can be invaded while on these open Wi-Fi hotspots include Network Sniffing, Wi-Phishing, Third Party Data Gathering, and Accidental and Malicious Access Points that use Page Spoofing and Evil Twin attacks to invade a student's privacy (Kasten, Okhrimets & Kharchenko, 2015).

Network Sniffing

If a hacker wants to steal a student's personal, financial information or identity, all they need is a "sniffing" application, like Wireshark or Kali Linux Kismet, that intercepts and gathers all visible traffic on a channel. Since open Wi-Fi does not have any security using a pre-shared key (PSK) like WPA2 where each connection is encrypted between a Wi-Fi network and a user's client, a hacker's job is already done since all is plaintext and not encrypted and can just "sniff" the network and grab student's personal information (Kasten, Okhrimets & Kharchenko, 2015).

Wi-Phishing

In Wi-Phishing, a hacker sets up a "soft" access point (or unauthorized devices) to get wireless-enabled devices to connect to it as a prelude to an attack to steal a user's identity (i.e. Id-spoofing). This can also take the form of a man-in-the-middle or insertion attack, where a hacker sets up a "soft" access point that acts as a relay to the "real" access point. When information flows through the "soft" access point, the attacker copies the data (Rudman, 2008).

Third-Party Data Gathering

Third-party data gathering is when sensitive unencrypted data or data encrypted with poor cryptography is intercepted, disclosed to unauthorized parties and stolen, deleted or lost while being transmitted between two wireless devices (Rudman, 2008).

Even without the presence of active data hackers, your privacy is never guaranteed when you access an open public hotspot. Often the biggest breaches of privacy are performed by the very establishments offering free Wi-Fi. Sometimes Wi-Fi is used to identify potential customers who are in the vicinity of the access point, and sometimes it's used to track the websites that users visit. Below are some common techniques that hotspot providers use to obtain information about Wi-Fi users.

- Asking visitors to leave their phone number or email in exchange for the PIN to access the Internet.
- Asking visitors to share something via a social network or give a program access to their social identity (e.g., to display targeted advertisements)
- Leveraging multiple access points to triangulate the visitor's physical location based on Wi-Fi signal strength (for example, to track their route through a store or to identify which establishments are currently the most crowded/popular)
- Injecting cookies into their browser to track their history (e.g., to display targeted advertisements) (Kasten, Okhrimets & Kharchenko, 2015).

Accidental and Malicious Access Points

Accidental association is when in a populated area, multiple wireless areas may overlap. A user may turn on a wireless device, which in turn connects to a wireless access point from a different overlapping network (other than the intended access point). Data from the overlapping network as a result of this could be exploited.

Malicious association, also known as a rogue access point, is when a hacker sets up an access point illicitly and looks like a legitimate access point using a cloned ID. The user believes he/she has gained access to a legitimate device. This access point is used to intercept data and can be used to bypass security controls (Rudman, 2008). Since there are often multiple networks to choose from, you often guess which hotspot belongs to a specific venue. Some Wi-Fi users will even connect to a completely unknown network simply because it is unlocked. Obviously, this practice poses some serious risks, especially if the access point is malicious or being manipulated by an attacker (Kasten, Okhrimets & Kharchenko, 2015).

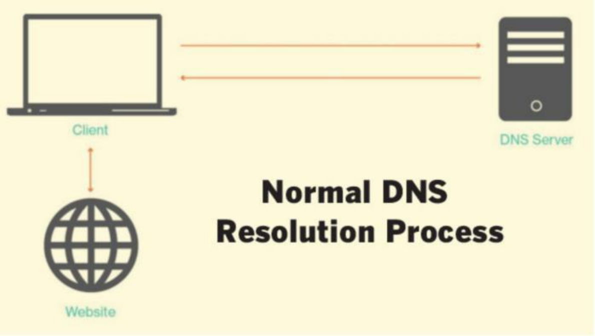


Fig. 1. Normal DNS Resolution Process (Kasten, Okhrimets & Kharchenko, 2015).

One of the biggest malicious association threats is "page spoofing," where a malicious access point controls a domain name resolution (i.e., how a domain name is translated into its numerical IP address). In the normal DNS resolution process, a user's client will communicate with a server to connect to the Internet (Kasten, Okhrimets & Kharchenko, 2015).

In a spoofing attack, a hacker creates a fake version of a website to steal credentials. For example, you may be asked to "like" something on Facebook before you can access the Internet and then be directed to a fake Facebook login page that looks like the real thing. As you log in, this fake page would record your credentials, show a login error, and then redirect you to the real Facebook page for a "second attempt" at logging in. Before you're even aware of what has happened, your social identity has been stolen (Kasten, Okhrimets & Kharchenko, 2015).

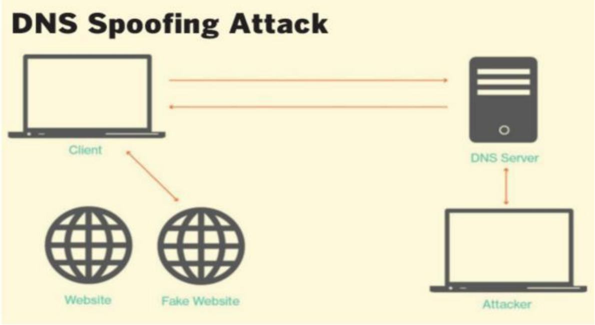


Fig. 2. DNS Spoofing Attack (Kasten, Okhrimets & Kharchenko, 2015).

Evil twin attack operates similarly. An attacker fools' wireless users into connecting to the attacker's network by placing an 'unauthorized' access point with a stronger signal in close proximity to the 'legitimate' wireless device. Users then log in to the attacker's network and unknowingly disclose data (Rudman, 2008).

This tactic is most often attempted in public parks or other large, unmonitored areas. Using a laptop with a wireless card, the attacker will access a legitimate access point to create an "evil twin" access point with a similar name. Imagine for a moment that you are at your local park, and your iPad detects a free Wi-Fi hotspot named "CityPark1." Many of us would probably connect to the network based on its name alone. However, by not confirming the legitimacy of an access point before connecting to it, you enable attackers to gather an even wider range of personal information (Kasten, Okhrimets & Kharchenko, 2015).

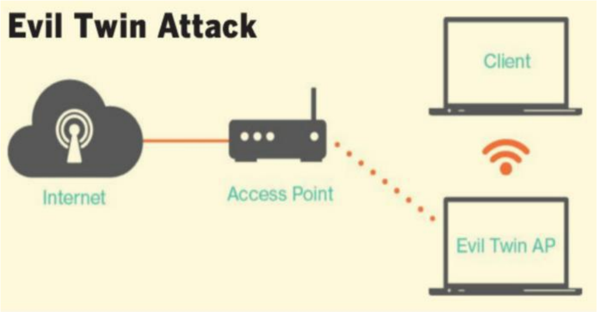


Fig. 3. Evil Twin Attack (Kasten, Okhrimets & Kharchenko, 2015).

These are the most common risks even though other risks such as denial-of-service attacks exist. Why do these risks exist? Three reasons exist for these types of attacks, each with different intentions. First are thrill seekers and drivers who are motivated by the thrill of electronic trespassing and in most cases, are harmless. Second are bandwidth thieves who use another's Wi-Fi to remain anonymous or to download software without paying for the software or bandwidth. The last reason, and the most common reason and the focus of this article are knowledgeable attackers or 'hacker who are out to steal data and information or steal someone's identity (Rudman, 2008).

4. PAST RESEARCH

The purpose of the literature review was to examine the existing literature for research on open Wi-Fi insecurity and if any research was conducted on college and university student access. Therefore, the review of the literature focused on literature related to Wi-Fi, security, and colleges/universities.

A second annual online survey was conducted by Norton by Symantec, although not specifically on college and university students, but rather a global study in order to better understand consumers' public Wi-Fi perceptions and practices and to unveil consumer misconceptions and worries about the safety of these connections. The survey explored consumers' knowledge about the safety of public Wi-Fi connections and while the use of public Wi-Fi is nearly universal, most consumers are unaware of the dangers when connecting to public Wi-Fi and continue to put their personal information at risk. The survey's findings provide consumers with much needed context to make better decisions about protecting their personal information while using public Wi-Fi.

In May 2017, Norton by Symantec (Norton by Semantec, 2017) surveyed 15,532 mobile device users who had connected to Wi-Fi to discover their attitudes to and behaviors using public Wi-Fi. The result was at least 1000 respondents from 15 global markets: Australia, Brazil, Canada, France, Germany, India, Italy, Japan, Hong Kong, Mexico, Netherlands, New Zealand, United Arab Emirates, the United Kingdom and USA. The research was conducted by Norton by Symantec and Reputation Leaders through international online panel company Research Now with data collected from May 18th to June 5th, 2017. The key findings included the following:

1. **Consumers are unable to resist a strong, free Wi-Fi signal.**
    a. More than half of consumers globally (55 percent) wouldn't think twice about exchanging, sharing or even doing something to get a strong Wi-Fi signal.
    b. 25 percent have accessed a Wi-Fi network without the Wi-Fi network owner's permission; 8 percent guessed or hacked the password
    c. 46 percent of consumers can't wait more than a few minutes before logging onto a Wi-Fi network or asking for the password after arriving at a friend's place, café, hotel or other location.
2. **Even when travelling, access to public Wi-Fi is a must.**
    a. Respondents say that access to a strong Wi-Fi signal is a deciding factor when choosing the following: A hotel/holiday/hostel rental (71 percent), a transport hub for traveling and/or commuting (46 percent), a place to eat or drink (café, bar, restaurant, etc.) (43 percent), an airline (43 percent)
    b. Nearly half (49 percent) of people say the most important reason for having access to strong public Wi-Fi is so they can use Maps, Google Maps or another GPS app to get around.
3. **Nevertheless, what some people choose to do over public Wi-Fi may surprise you.**
    a. One in six people admit to having used public Wi-Fi to watch adult content.
    b. Of those who admit to using public Wi-Fi to watch adult content, they've done so in the following locations: Hotel/Airbnb (40 percent), Café/Restaurant (30 percent), Work (29 percent), Airport (25 percent), On the street (24 percent), Train/bus station (18 percent), Public restroom/toilet (16 percent)
4. **Consumers' dependency on public Wi-Fi is putting their personal information at risk. What someone thinks are private on his or her personal device could easily be accessed by cybercriminals via compromised apps or Wi-Fi networks.**
    a. 60 percent feel their personal information is safe when using public Wi-Fi, yet 53 percent can't tell the difference between a secure or unsecure public W-Fi network.
    b. 75 percent of consumers don't use a Virtual Private Network (VPN) to secure their Wi-Fi connections, even though it's one of the best ways to protect your information.
    c. 87 percent of consumers have potentially put their information at risk while using public Wi-Fi.
5. **When consumers think about a hacker or malicious person stealing their personal information and posting it online, emotions run high.**
    a. 48 percent would feel horrified if the details of their bank accounts and financial information were posted online.
    b. 38 percent would feel angry if their photo library, including intimate, personal and family photos were posted online.
    c. 36 percent would be worried if their children's schedule, location or academic details were posted online.
    d. 21 percent would be embarrassed if the details of their private chats/texts conversation or closest secrets were posted online (Norton by Semantec, 2017).

Although no studies were found in the literature review search on open public Wi-Fi insecurity and college/university students, other studies were done on Wi-Fi and security.

In 2013, a study was done to propose a solution to monitor Wi-Fi networks that is under unauthorized access attack via rogue APs. The author provided the required user permissions to allow/block connect and access files on the secure ad-hoc client. The experiment results showed the effectiveness of the proposed solution (Sobh, 2013). Additionally, a study on the disadvantage of Wi-Fi networks (Chernukin, 2014) on offering low level of protection against unauthorized access and the problems related to such use of the Wi-Fi technology, poses a threat to information security. Also, describes the causes for appearance of threats, drawbacks of legal character, and to substantiate the offers concerning improvement of legal and organizational measures for preventing the use of brand-new technologies for destructive purposes.

Sagers et al examined the relationship between wireless access points collected via war driving and a series of US Census socioeconomic variables in two communities in the United States (Sagers, Hosack, Rowley, Twitchell & Nagaraj, 2015). They found significant correlations between Wi-Fi security race/ethnicity, which may also correlate to education levels and income. Their findings suggest that a greater awareness and/or manufacturer-driven default security for wireless access points may be necessary to ensure better security. Their presents a large-scale attempt to collect data from thousands of Wi-Fi networks to measure their security in two distinct geographic regions to determine what, if any, socio-economic factors affect the level of security and suggest a number of possible solutions to the gaps that exist in Wi-Fi security (Sagers et. Al., 2015).

Very few studies were found on open Wi-Fi insecurity and none were found as it relates to college/university students accessing open Wi-Fi on campus. This study utilizes Kali Linux to explore students accessing open public Wi-Fi one universities campus and the potential risk they are exposed to from attackers. The next few sections details the methodology used for this study, the results and solutions for security using open Wi-Fi on campus.

5. OPEN WI-FI SECURITY ANALYSIS

In this paper, the author considered analyzing the security features and vulnerabilities of the open Wi-Fi like Starbucks, McDonald's, Panda Express, and college campus free attwifi, by using both active and passive attack methods. The author was in no way hacking these devices in these places but rather emphasizing the issues of open Wi-Fi. For active attack, The author performed MAC address spoofing, SSL Stripping, and DHCP Exhausting attacks. For passive attack, the author captured the pcap file and used Wireshark for analysis.

MAC Address Spoofing

MAC address spoofing is technique for faking originally assigned Media Access Control (MAC) Address of a network device. MAC address spoofing is considered as a significant step for attacker to launch a variety of attacks on open Wi-Fi networks, such as man-in-the-middle, side jacking, and denial of service.

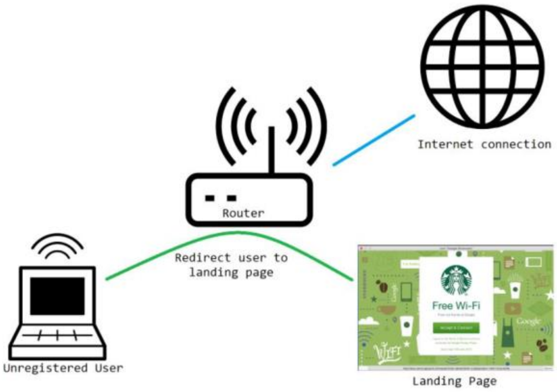


Fig. 4. Captive Portal Landing Page Structure [10]

The author tried to spoof the MAC address of the target machine to bypass the captive portal page of open Wi-Fi networks. Captive Portal works by intercepting, impersonating, and altering the connection between client and web server. Even though the author define the captive portal as a firewall for open Wi-Fi network, it is a man-in-the-middle attack. However, it has good intentions (for security reasons and safe environment) to filter the traffic. For example, to providing a safe and secure environment, adult contents are blocked in Google Starbucks Wi-Fi and McDonalds Wi-Fi (where they are combinedly more than 21,000 store locations in the U.S).

Even though the author, as an attacker, could duplicate the same MAC address of target who is already connected to an open Wi-Fi. The author was unable to bypass the captive portal using that MAC address spoofing. Additionally, the author experimented spoofing MAC address of Access point (AP) itself to bypass the captive portal. Even this time, results are negative. This could be because of 802.11 association process.

The 802.11 association process happens when a user tried to access Wi-Fi, i.e. the mobile station and AP will exchange a series of 802.11 management frames to get to an authenticated and associated state before connection is established. There are three 802.11 connection states: Not authenticated or associated, authenticated but not yet associated, and Authenticated and associated respectively. All these states conditions can be identified in the frame control fields.

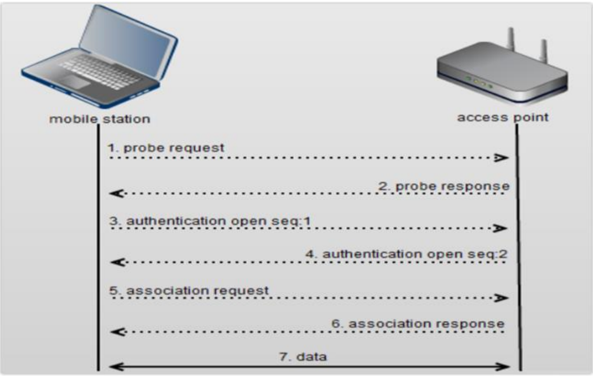
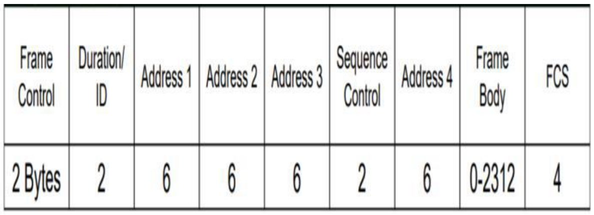


Fig. 5. 802.11 Association Process (Meraki, 2017)

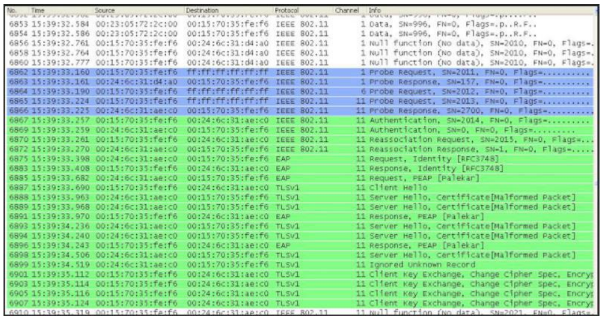
Each frame includes frame control, duration, BSSID, Source MAC, Destination MAC, Sequence control, frame body, and frame control field.



Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS
2 Bytes	2	6	6	6	2	6	0-2312	4

Fig. 6. Frame Control Field (Meraki, 2017)

So, by implementing devices with Sequence Number tracking, Operating System (OS) fingerprinting & tracking, and Received Signal Strength fingerprinting & tracking MAC address spoofing attack to bypass the captive portal can be prevented. Below Fig. 7. shows our Wireshark analysis of the 802.11 association process.



```
No.  Time         Source             Destination        Protocol      Channel Info
6853 15:39:32.584 00:23:05:72:2c:00  00:15:70:35:fe:f6  IEEE 802.11    1 Data, SN=996, FN=0, Flags=.p..R.F..
6854 15:39:32.586 00:23:05:72:2c:00  00:15:70:35:fe:f6  IEEE 802.11    1 Data, SN=996, FN=0, Flags=.p..R.F..
6856 15:39:32.761 00:15:70:35:fe:f6  00:24:6c:31:d4:a0  IEEE 802.11    1 Null function (No data), SN=2010, FN=0, Flags=.
6858 15:39:32.764 00:15:70:35:fe:f6  00:24:6c:31:d4:a0  IEEE 802.11    1 Null function (No data), SN=2010, FN=0, Flags=.
6860 15:39:32.777 00:15:70:35:fe:f6  00:24:6c:31:d4:a0  IEEE 802.11    1 Null function (No data), SN=2010, FN=0, Flags=.
6862 15:39:33.160 00:15:70:35:fe:f6  ff:ff:ff:ff:ff:ff  IEEE 802.11    1 Probe Request, SN=2011, FN=0, Flags=.........
6863 15:39:33.161 00:24:6c:31:d4:a0  00:15:70:35:fe:f6  IEEE 802.11    1 Probe Response, SN=157, FN=0, Flags=.........
6864 15:39:33.190 00:15:70:35:fe:f6  ff:ff:ff:ff:ff:ff  IEEE 802.11    6 Probe Request, SN=2012, FN=0, Flags=.........
6865 15:39:33.224 00:15:70:35:fe:f6  ff:ff:ff:ff:ff:ff  IEEE 802.11   11 Probe Request, SN=2013, FN=0, Flags=.........
6866 15:39:33.225 00:24:6c:31:ae:c0  00:15:70:35:fe:f6  IEEE 802.11   11 Probe Response, SN=2700, FN=0, Flags=.........
6867 15:39:33.257 00:15:70:35:fe:f6  00:24:6c:31:ae:c0  IEEE 802.11   11 Authentication, SN=2014, FN=0, Flags=........
6869 15:39:33.259 00:24:6c:31:ae:c0  00:15:70:35:fe:f6  IEEE 802.11   11 Authentication, SN=0, FN=0, Flags=........
6870 15:39:33.261 00:15:70:35:fe:f6  00:24:6c:31:ae:c0  IEEE 802.11   11 Reassociation Request, SN=2015, FN=0, Flags=...
6872 15:39:33.270 00:24:6c:31:ae:c0  00:15:70:35:fe:f6  IEEE 802.11   11 Reassociation Response, SN=1, FN=0, Flags=.....
6875 15:39:33.398 00:24:6c:31:ae:c0  00:15:70:35:fe:f6  EAP           11 Request, Identity [RFC3748]
6883 15:39:33.408 00:15:70:35:fe:f6  00:24:6c:31:ae:c0  EAP           11 Response, Identity [RFC3748]
6885 15:39:33.682 00:24:6c:31:ae:c0  00:15:70:35:fe:f6  EAP           11 Request, PEAP [Palekar]
6887 15:39:33.690 00:15:70:35:fe:f6  00:24:6c:31:ae:c0  TLSv1         11 Client Hello
6888 15:39:33.963 00:24:6c:31:ae:c0  00:15:70:35:fe:f6  TLSv1         11 Server Hello, Certificate[Malformed Packet]
6889 15:39:33.968 00:24:6c:31:ae:c0  00:15:70:35:fe:f6  TLSv1         11 Server Hello, Certificate[Malformed Packet]
6891 15:39:33.970 00:15:70:35:fe:f6  00:24:6c:31:ae:c0  EAP           11 Response, PEAP [Palekar]
6893 15:39:34.236 00:24:6c:31:ae:c0  00:15:70:35:fe:f6  TLSv1         11 Server Hello, Certificate[Malformed Packet]
6894 15:39:34.240 00:24:6c:31:ae:c0  00:15:70:35:fe:f6  TLSv1         11 Server Hello, Certificate[Malformed Packet]
6896 15:39:34.243 00:15:70:35:fe:f6  00:24:6c:31:ae:c0  EAP           11 Response, PEAP [Palekar]
6898 15:39:34.506 00:24:6c:31:ae:c0  00:15:70:35:fe:f6  TLSv1         11 Server Hello, Certificate[Malformed Packet]
6899 15:39:34.519 00:24:6c:31:ae:c0  00:15:70:35:fe:f6  TLSv1         11 Ignored Unknown Record
6901 15:39:35.112 00:15:70:35:fe:f6  00:24:6c:31:ae:c0  TLSv1         11 Client Key Exchange, Change Cipher Spec, Encry
6903 15:39:35.114 00:15:70:35:fe:f6  00:24:6c:31:ae:c0  TLSv1         11 Client Key Exchange, Change Cipher Spec, Encry
6905 15:39:35.116 00:15:70:35:fe:f6  00:24:6c:31:ae:c0  TLSv1         11 Client Key Exchange, Change Cipher Spec, Encry
6907 15:39:35.124 00:15:70:35:fe:f6  00:24:6c:31:ae:c0  TLSv1         11 Client Key Exchange, Change Cipher Spec, Encry
6910 15:39:35.319 00:15:70:35:fe:f6  00:24:6c:31:ae:c0  IEEE 802.11   11 Null function (No data), SN=2021, FN=0, Flags=.
```

Fig. 7. 802.11 Association Process captured in Wireshark

SSL Strip

SSL Strip is a type of attack that tricks a victim's browser into communicating with an attacker in plain-text over HTTP. As a matter of fact, the author can identify SSL strip as a form of man-in-the-middle attack. The goal of SSL Strip when performed by attackers on open Wi-Fi, is to route all the traffic from the victim’s machine via a proxy that is created by the attacker. To better understand the SSL Strip’s concept, the author has to understand HTTP and HTTPS, which are application-layer protocols in TCP/IP model. In fact, when communicating over open Wi-Fi, HTTPS utilizes a secure tunnel to ensure data is transmitted in a secured way; this secure tunnel is commonly called as SSL.

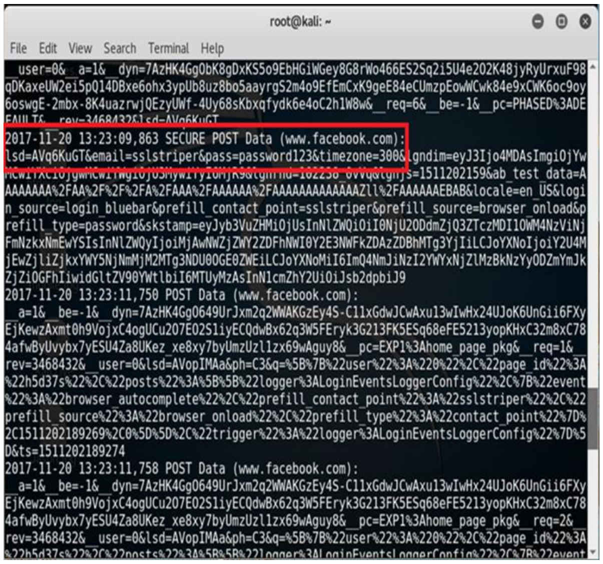
Though, there are many ways to perform SSL Strip the author used ARP spoofing as a method of evaluation in our research. Indeed, through ARP spoofing the author was able to downgrade the connection established by the victim’s browser from HTTPs to HTTP. In our scenario, a victim has connected to an open Wi-Fi and tried to connect to www.facebook.com using his credentials, while the attacker is running SSL Strip on another machine, which is a proxy server. The description of the attack’s scenario is as followed:

- Victim tries to initiate a secure communication with www.facebook.com.
- The victim’s browser that is connected to the attacker’s machine requests a response from the Facebook’s server (attacker acts as man-in-the-middle, by sending victim’s request to server and await from response). Here, the Kernel forwards everything along except for traffic destined to port 80, which it redirects to 8080
- Attacker received secured feedback from Facebook’s server and modified the response from the server from https to http and sends it to victim. At this point, the victim is provided with in insecure login http://www.facebook.com, and attacker can easily sniff all the data entered by the victim and see credentials (data is in plaintext format). Figure X below depicts the result of SSL Strip on a Facebook’s user, connected to an open Wi-Fi.

DHCP Exhausting – A DoS Attack

DHCP is a critical part of the Layer 2 and Layer 3 link, as

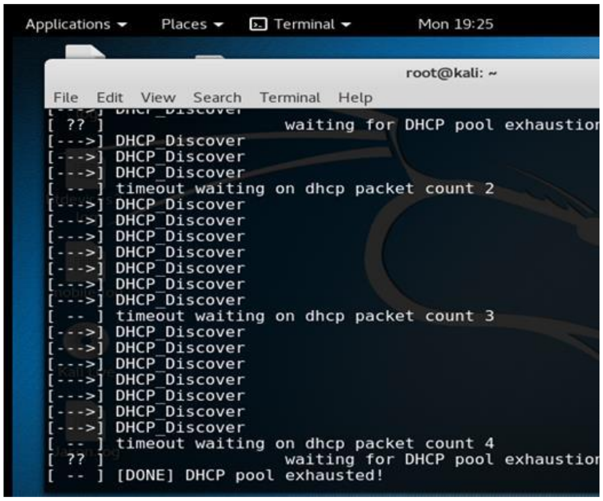
well. Nowadays intelligent switches assign temporary IP addresses to hosts in networks. Most switches provide further configuration information such as a subnetwork mask, default gateway, and DNS services etc. Moreover, DHCP is an inherently insecure protocol. Some well-known attacks at Layer 2 utilizing DHCP are rogue DHCP servers, DHCP starvation, and DoS attacks among others. This project takes advantage to exploit the weakness by DHCP starvation in captive portal to exhausting its IP addresses. By issuing this command, Pig.py wlan0.



```
__user=0&__a=1&__dyn=7AzHK4GgObK8gDxKS5o9EbHGiWGey8G8rWo466ES2Sq2i5U4e202K48jyRyUrxuF98
qDKaxeUW2ei5pQ14DBxe6ohx3ypUb8uz8bo5aayrgS2m4o9EfEmCxK9geE84eCUmzpEowWCwk84e9xCWK6oc9oy
6oswgE-2mbx-8K4uazrwjQEzyUWf-4Uy68sKbxqfydk6e4oC2h1W8w&__req=6&__be=-1&__pc=PHASED%3ADE
FAULT&__rev=3468432&lsd=AVq6KuGT
2017-11-20 13:23:09,863 SECURE POST Data (www.facebook.com):
lsd=AVq6KuGT&email=sslstriper&pass=password123&timezone=300&lgndim=eyJ3Ijo4MDAsImgiOjYw
MCwiYXciOjgwMCwiYWgiOjU3MywiYyI6MjR9&lgnrnd=102258_0VVq&lgnjs=1511202159&ab_test_data=A
AAAAAAA%2FAA%2F%2F%2FA%2FAAA%2FAAAAAA%2FAAAAAAAAAAAAAZll%2FAAAAAAEBAB&locale=en_US&logi
n_source=login_bluebar&prefill_contact_point=sslstriper&prefill_source=browser_onload&p
refill_type=password&skstamp=eyJyb3VuZHMiOjUsInNlZWQiOiI0NjU2ODdmZjQ3ZTczMDI1OWM4NzViNj
FmNzkxNmEwYSIsInNlZWQyIjoiMjAwNWZjZWY2ZDFhNWI0Y2E3NWFkZDAzZDBhMTg3YjIiLCJoYXNoIjoiY2U4M
jEwZjliZjkxYWY5NjNmMjM2MTg3NDU0OGE0ZWEiLCJoYXNoMiI6ImQ4NmJiNzI2YWYxNjZlMzBkNzYyODZmYmJk
ZjZiOGFhIiwidGltZV90YWtlbiI6MTUyMzAsInN1cmZhY2UiOiJsb2dpbiJ9
2017-11-20 13:23:11,750 POST Data (www.facebook.com):
__a=1&__be=-1&__dyn=7AzHK4Gg0649UrJxm2q2WWAKGzEy4S-C11xGdwJCwAxu13wIwHx24UJoK6UnGii6FXy
EjKewzAxmt0h9VojxC4ogUCu207E02S1iyECQdwBx62q3W5FEryk3G213FK5ESq68eFE5213yopKHxC32m8xC78
4afwByUvybx7yESU4Za8UKez_xe8xy7byUmzUzl1zx69wAguy8&__pc=EXP1%3Ahome_page_pkg&__req=1&__
rev=3468432&__user=0&lsd=AVopIMAa&ph=C3&q=%5B%7B%22user%22%3A%220%22%2C%22page_id%22%3A
%22h5d37s%22%2C%22posts%22%3A%5B%5B%22logger%3ALoginEventsLoggerConfig%22%2C%7B%22event
%22%3A%22browser_autocomplete%22%2C%22prefill_contact_point%22%3A%22sslstriper%22%2C%22
prefill_source%22%3A%22browser_onload%22%2C%22prefill_type%22%3A%22contact_point%22%7D%
2C1511202189269%2C0%5D%5D%2C%22trigger%22%3A%22logger%3ALoginEventsLoggerConfig%22%7D%5
D&ts=1511202189274
2017-11-20 13:23:11,758 POST Data (www.facebook.com):
__a=1&__be=-1&__dyn=7AzHK4Gg0649UrJxm2q2WWAKGzEy4S-C11xGdwJCwAxu13wIwHx24UJoK6UnGii6FXy
EjKewzAxmt0h9VojxC4ogUCu207E02S1iyECQdwBx62q3W5FEryk3G213FK5ESq68eFE5213yopKHxC32m8xC78
4afwByUvybx7yESU4Za8UKez_xe8xy7byUmzUzl1zx69wAguy8&__pc=EXP1%3Ahome_page_pkg&__req=2&__
rev=3468432&__user=0&lsd=AVopIMAa&ph=C3&q=%5B%7B%22user%22%3A%220%22%2C%22page_id%22%3A
%22h5d37s%22%2C%22posts%22%3A%5B%5B%22logger%3ALoginEventsLoggerConfig%22%2C%7B%22event
```

Fig. 8. SSL Strip Password capture

Below is a screen shot depicting a successful DHCP starvation on captive portal at McDonalds Café.



```
[ ... ] DHCP_Discover
[ ?? ]                      waiting for DHCP pool exhaustion
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[ -- ] timeout waiting on dhcp packet count 2
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[ -- ] timeout waiting on dhcp packet count 3
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[ -- ] timeout waiting on dhcp packet count 4
[ ?? ]                      waiting for DHCP pool exhaustion
[ -- ] [DONE] DHCP pool exhausted!
```

Fig. 9. DHCP Exhausting

The author was able to exhaust one subnet, but because the wireless access portal run on multi-subnets the effect of IP starvation was not achieved. Most captive portal mitigate such problems by putting in place measures such as:

- WLC (Wireless LAN Controllers) to terminate the user traffic and by examining DHCP requests to ensure that the client MAC address matches the chaddr. If the addresses do not match, the DHCP request is dropped.
- An H-REAP AP (Hybrid Remote Edge Access point) terminates the user traffic. The user VLAN is terminated locally, the DHCP request does not go through the controller, and an analysis of the chaddr cannot be performed.

DHCP Exhausting – A DoS Attack
The author did a ping response test in attwifi (Campus), Starbucks, McDonalds, and Panda Express open Wi-Fi. All of them provided us a same result "Destination host unreachable". The author did a quick research to understand the result. The wireless network has their firewall turned on to block ICMP packets from to help prevent DDoS Ping Flood attacks.

6. SOLUTIONS FOR SECURITY USING OPEN WI-FI

Even without an elaborate phishing scheme, it is impossible to completely secure a public hotspot. In fact, many times access points will only display an end-user agreement (EULA) or advertisement before allowing users to connect to the Internet.

Although there is no connection between the open public Wi-Fi network and a student's personal network (i.e., different SSIDs and IP addresses), there is still the concern that a hacker can connect to a network hosted on the user's device and exploit any potential vulnerabilities.

Students should never connect to open public Wi-Fi, since many risks exist as described earlier in this article, but since that is almost impossible, there are certain measures students can take to protect against attackers. Here are the most common precautions:

1. Always confirm the legitimacy of a Wi-Fi network before connecting to it; do not rely on the name alone. If there are multiple access points for the same venue, ask a staff member which one to use. Similarly, be sure to read that venue's Terms of Service carefully to ensure that your privacy will not be breached.
2. Ideally, you should only use public Wi-Fi to browse websites that do not require login credentials (e.g., news forums, etc.). However, if you do need to access sensitive data or enter login credentials (for, say, email), only go to websites that start with HTTPS (a more secure version of the standard HTTP web protocol). Just be aware

that even if a website uses HTTPS for the majority of its content, the images on that website might still be distributed via HTTP since links are not typically encrypted. However, most current web browsers will warn you if this linked content is unsecure or when the certificate from a secured HTTPS site is not valid or verifiable.

3. Never install software while using public Wi-Fi, as it could introduce viruses into your computer. For example, a common attack is to inform the user that his browser is using outdated Flash and then redirect the user to a fake Adobe website that will install a virus instead of the real software.
4. A good way to ensure security while accessing public Wi-Fi is to use a Virtual Private Network (VPN). A VPN essentially creates a tunnel between your device and a third-party server. All data that passes through this tunnel is encrypted and therefore hidden from both the Wi-Fi provider and anyone trying to sniff the network. If you cannot access a VPN through the school, consider installing a trusted third-party VPN like Cyber ghost.

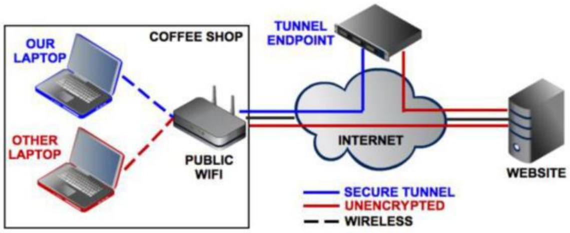


Fig. 10. Tunneled Traffic

5. If all else fails, students should use a personal mobile hotspot, either on their phone or with a separate device. In fact, many companies like AT&T offer unlimited plans so there is no limit on how much you can surf the Internet.

It is easy to take free Wi-Fi access for granted. Unfortunately, as public hotspots become more prevalent, so will hackers. Your best protection against data theft is a solid understanding of Wi-Fi and its vulnerabilities and taking a few commonsense precautions (Kasten, Okhrimets & Kharchenko, 2015).

7. CONCLUSION

Users of wireless hotspots are ultimately responsible for their own security. Although some tools give them enhanced security functionality when using a hotspot, the situation remains unpredictable and insecure for the majority of users. Operating system vendors and third-party software developers do not provide enough information and direction to users regarding the threats on wireless networks. The attacks against Wi-Fi are not terribly complicated, but without tools for triggering alerts and defensive measures aimed at hotspot users, there's little these users are able to do to protect themselves.

For all their utility and ease of use, hotspots are dangerous places. While every coffeehouse and lounge may not include an attacker lying in wait for victim hosts, the fact is attackers are likely to be successful. Users in enterprise environments have the luxury of a single point of control and administration that creates "security of scale" for wireless users. In open public hotspots, users are on their own. Despite the availability of tools and point solutions, most users represent easy prey for sophisticated attackers.

The state of the art with respect to wireless defense is behind the state of the art with respect to wireless attack. As technologies evolve, users will become better armed to deal with the threat posed in hotspots. In the meantime, it may be better to shut the laptop, enjoy the coffee, and keep an eye on the people nearby (Potter, 2006).

8. REFERENCES

Baul, P., Venkatachary, S., Balachandran, A. (2001). "Secure wireless Internet access in public places," ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No.01CH37240), Helsinki, 2001, pp. 3271-3275 vol.10.doi: 10.1109/ICC.2001.937274

Chernukin, I. (2014). NEW CHALLENGES TO INFORMATION SECURITY CAUSED BY THE INTRODUCTION OF WI-FI TECHNOLOGIES. *Information & Security, 31*(1), 79-86. doi:http://dx.doi.org.proxy.ulib.uits.iu.edu/10.11610/isij.3105

Cypriani, M., Lassabe, F., Canalda, P., Spies, F., (2009). "Open Wireless Positioning System: A Wi-Fi-Based Indoor Positioning System," 2009 IEEE 70th Vehicular Technology Conference Fall, Anchorage, AK, 2009, pp. 1-5. doi: 10.1109/VETECF.2009.5378966

Eslami, M., Karimi, O., Khodadadi, T. (2014). "A survey on wireless mesh networks: Architecture, specifications and challenges," 2014 IEEE 5th Control and System Graduate Research Colloquium, Shah Alam, 2014, pp.

219-222. doi: 10.1109/ICSGRC.2014.6908725

Hills, A. (1999). "Wireless Andrew [mobile computing for university campus]," in IEEE Spectrum, vol. 36, no. 6, pp. 49-53, Jun 1999. doi: 10.1109/6.769269

Jones, K., and Liu, L. (2007). "What Where Wi: An Analysis of Millions of Wi-Fi Access Points," 2007 IEEE International Conference on Portable Information Devices, Orlando, FL, 2007, pp. 1-4.doi: 10.1109/PORTABLE.2007.45

Jyrki, T., and Penttinen, J. (2015a). "Future of Wireless Solutions and Security," in Wireless Communications Security:Solutions for the Internet of Things , 1, Wiley Telecom, 2015, pp.336-doi: 10.1002/9781119084402.ch10

Jyrki, T., and Penttinen, J. (2015b). "Security Risks in the Wireless Environment," in Wireless Communications Security:Solutions for the Internet of Things , 1, Wiley Telecom, 2015, pp.336-doi: 10.1002/9781119084402.ch8

Kapersky Lab. (2017). How to Avoid Public WiFi Security Risks. [Online]. Available: https://usa.3.com/resource-center/preemptive-safety/public-wifi-risks

Kasten, T. Okhrimets, A., and Kharchenko, A., (2015). Is it safe to use public Wi-Fi networks? [Online]. Available: https://www.networkworld.com/article/2904439/wi-fi/is-it-safe-to-use-public-wi-fi-networks.html

Kavianpour, A., and Anderson, M., C., Anderson (2017). "An Overview of Wireless Network Security," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, 2017, pp. 306-309.doi:10.1109/CSCloud.2017.45

Meraki, C., (2017). 802.11 Association Process

Explained.[Online].Available:https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/802.11_Association_process_explained

Muppavarapu, R. (2015). Open Wi-Fi hotspots-Threats and Mitigations. [Online]. Available: https://dl.packetstormsecurity.net/papers/wireless/openwifimitigations.pdf

Norton by Symantec (2017). Norton Wi-Fi Risk Report: Report of online survey results in 15 global markets. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/2017-norton-wifi-risk-report-global-results-summary-en.p

Potter, B. (2006). Wireless hotspots*. Association for Computing Machinery. Communications of the ACM, 49*(6), 50-56. doi:http://dx.doi.org.proxy.ulib.uits.iu.edu/10.1145/1132469.1132501

Ray, S., et al. (2017). "An efficient association of a mobile client in wireless mesh network," 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2017, pp. 497-500.doi: 10.1109/IEMCON.2017.8117225

Rudman, R. (2008). Wi-fi TECHNOLOGY: Is someone watching you? [Online]. Available: https://search-proquest-com.proxy.ulib.uits.iu.edu/docview/215225473?accountid=7398

Sagers, G., Hosack, R., Rowley, J., Twitchell, D., and Nagaraj, R. (2015). "Where's the Security in WiFi? An Argument for Industry Awareness," 2015 48th Hawaii International Conference on System Sciences, Kauai, HI, 2015, pp. 5453-5461

Siciliano, R. (2017). School WiFi Often Open and Insecure. [Online]. Available: http://www.huffingtonpost.com/robert-siciliano/school-wifi-often-open-an_b_4276082.html

Sobh, T. (2013). Wi-Fi Networks Security and Accessing Control. International Journal of Computer Network and Information Security. 5. 9-20. 10.5815/ijcnis.2013.07.02

Sosa, P. (2017). BREAK FREE! - BYPASSING CAPTIVE PORTALS. [Online]. Available: http://konukoii.com/blog/2017/03/07/break-free-bypassing-captive-portals

Editor's Note:

This paper was selected for inclusion in the journal as an CONISAR 2020 Meritorious Paper. The acceptance rate is typically 15% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2020.

Enhancing Analytics in Higher Education: The Rise of Institutional Research

LeeAnn Perkins
perkinsl3@xavier.edu

Thilini Ariyachandra
ariyachandrat@xavier.edu

Business Analytics and Information Systems Department
Xavier University
Cincinnati, Oh 45207, USA

Abstract

The need for analytics and data-driven decision making in higher education has been on the rise as college and university leaders deal with student success, affordability, and competition in the management and growth of their institutions. Within higher education, Institutional Research (IR) offices on campus have traditionally acted as the data keepers and official reporters for institutional information. In response to the need for analytics and data-driven decision making, IR offices have started to shift from being reporters to analysts. This paper will provide an overview and history of business intelligence (BI) in higher education and the shift towards BI in IR offices. In addition, the paper will also analyze The Association for Institutional Research (AIR), the national professional organization for IR, annual forums to provide trends and insights on analytics and BI in higher education.

Keywords: Analytics, Higher education, Learning Analytics, Institutional Resources, BI infrastructure, Student learning outcomes.

1. INTRODUCTION

Massive growth in data created throughout the world has become a common everyday occurrence today. The annually released infographic "Data never sleeps," aggregates the amount of data created by billions of people globally in a single minute by different categories (Hutchinson 2020). The infographic indicates that there is 1.7 megabytes of data created each second for each person on earth in 2020. As the mass of available data, as well as devices that capture data are skyrocketing, IDC predicts that data will grow at a compound annual growth rate of 42% through 2025 (Reinsel, Rydning and Gantz 2020). This has impacted decision making in every industry. Though late to the game, it has also impacted higher education (Krawitz, Law and Litman 2017). Postsecondary institutions are large organizations that have various community and governmental ties as they enroll, house, and credential students. Some institutions are long standing and have vast amounts of data that can be tapped for knowledge. As schools compete for students, face declines in state and federal funding, and are asked to address affordability and accountability in their operations, the need for analytics and business intelligence (BI) is only growing (Miyares & Catalano, 2016). The pandemic has added a new set of challenges for higher education institutions from retaining students to addressing issues related to the institution's survival (Catalano 2020). Few innovative higher education institutions are trying to implement BI and data analytics as a solution to maintain student engagement and provide an enriched learning experience during the pandemic (Foresman 2020).

For the past decade, data and analytics has continued to stay on the top ten IT issues list facing higher education according to EDUCAUSE's annual survey (Grajek 2020). The most recent survey revealed that data and advanced analytics driven decision making to simplify and innovate was predominantly featured in higher education IT issues themes (Grajek 2020). Part of the challenge, Grajek (2016) notes, is that fewer than 15% of analytics programs are described as strong or excellent in the industry. While higher education does lag other industries in terms of technology adoption, it seems the adoption and maturity of analytics in higher education is long overdue. This paper describes the history and current landscape of BI and analytics in higher education, the challenges faced as well as best practices for the implementations of BI and analytics in higher education. Next it sheds light on the role of institutional research (IR) entities in the implementation of BI on higher education campuses.

2. BUSINESS INTELLIGENCE IN HIGHER EDUCATION

Applying Analytics and BI on Campus

Yanosky and Arroway (2015) define analytics as, "the use of data, statistical analysis, and explanatory and predictive models to gain insight and act on complex issues". Higher education institutions are seen as the perfect fit for analytics and BI as a lot of schools have been in operation for over a hundred years and have big data. Laney (2001) defines big data collection in 3 v's: the increase in volume, the increase in the velocity, and the differing varieties of data. When looking at the application of analytics in higher education, there has been a greater emphasis on institutional vs. learning analytics (Yanosky & Arroway, 2015). Institutional analytics look at business practices and services provided by the institution while learning analytics focus on factors impacting student success (Yanosky & Arroway, 2015). Areas where analytics were most adopted on campuses were in enrollment management, undergraduate student progress, finance, and budgeting (Yanosky & Arroway, 2015). In Yanosky and Arroway's research of the landscape of analytics in higher education (2015), most institutions did not have a chief data officer or executive level leader who led the analytics work for the institution and only 9% had dedicated analytics centers.

Successful Implementations and Advice

While the adoption of BI has not been widespread in the industry, there have been pockets of successful implementations. The University of Maryland undertook a 5 year implementation project to transform analytics on their campus. The university hired a private sector analytics expert to lead the charge and found four lessons learned: prioritize data collection, focus on building data models, communicate, and connect (Miyares & Catalano, 2016). In prioritizing data collection, the institution centralized its analytics and data collection into a central location; the institution also hired an executive at the institution for analytics leadership. To focus on building data models, the institution increased spending in analytics within the areas of high performance cloud computing, data integration, and a data visualization platform. Communicating and connecting with people across campus was pivotal to the success of the university's program. The university invested resources into hiring people who could build data science and storytelling for the office of analytics; in addition to people, the office of analytics also made demonstrations on the potential of cross-departmental data analysis. Miyares and Catalano (2016) noted that by combining data sets from different departments, the university was able to start answering complex questions like the effect of student financial aid on bad debt.

St Cloud University also had success in implementing an IT infrastructure on their campus to support BI efforts. The strategies the university used were using a data warehouse, changing the culture to view information as the most valuable asset for the institution, and having a data governance structure with clear ownership of data and processes (Guster & Brown, 2012). To implement the IT infrastructure successfully, St Cloud relied on business logic as well as a clear implementation methodology. The strengths of the implementation methodology for St Cloud included designing service level agreements (SLA), building data governance and data definitions, developing security and access protocols, and accessing data quality (Guster & Brown, 2012).

The development and effective use of the predictive analytics platform at University of South Florida is another great example of analytics leading organizational change in higher education (Dosal 2019). Many of the early steps taken by the University of Maryland were taken at USF as executive sponsorship led by the Provost, President and CIO set the tone for the centralization of analytics efforts from disparate data silos. The focus on communication, training and building relevant analytics tools that includes artificial intelligence for student success resulted from collaboration between the main reporting entity on campus, Institutional Research, and IT at USF (Miller and Irwin 2019). The main results of the analytics platform adopted led to the six-year graduation rate of students at USF to increase from 48% to 73% between 2008 and 2018 (Miller and Irwin 2019). The best practices at University of South Florida included the creation of a culture of 'student in the center' across the organization along with making data driven decision making an organization wide imperative.

Advice for Implementing BI

For institutions considering analytics and BI, industry experts and leaders have advice on getting started. Grajek (2016) states that BI and analytics is one of the top 10 IT issues facing higher education. In order to respond, institutions should divest, reinvest, and differentiate in their IT operations. Institutions should divest from processes and technologies that are inefficient and reinvest into resources like the IT workforce and IT funding to achieve competitive differentiation in BI and analytics (Grajek, 2016). Leaders are seen as the biggest advocates for adopting BI on campus and should work to build a data-driven culture that invests resources into analytics. Durso (2009) also echoes the sentiment of having an advocate in the administration of the University for BI implementation projects. When choosing tools, Institutions should spend time researching tools and their current systems to ensure they choose the right tools for their school; legacy systems can prove to be challenging to adopt to BI tools. Similar to St Cloud's implementation, Durso (2009) notes the importance of establishing a data governance structure and to focus not only on the IT side of the BI implementation but also the business model and processes. Research into higher education practices in analytics adoption by McKinsey Consulting suggests changing operations and mindsets are the key best practices in implementing BI and analytics in higher education (Krawitz et al 2018). Table 1 summarizes the overall best practices for implementing BI in higher education.

Challenges of BI in Higher Education

From a general business standpoint, 90% of corporate strategies will explicitly mention information as a critical asset and analytics as a critical competency by 2022 according to Petty (2019). While BI is a promising practice that is well suited to provide knowledge to decision makers, the implementation and adoption has been slow in higher education (Krawitz, Law and Litman 2018). EDUCAUSE, a non-profit that promotes the use of information technology in higher education developed an analytics maturity index to measure analytics adoption in higher education. The index has six dimensions: decision making culture, policies, data efficacy, investment/resources, technical infrastructure, and IR involvement (Dahlstrom, 2016). A score of 1-5 (5 being the highest) is given for each dimension and then the mean is computed to give the index. In 2012, the analytics maturity index for higher education was 3.2; the index increased to 3.4 in 2014 and remained flat at 3.4 in 2015 (Dahlstrom, 2016). When looking at the reasons for the slow to non-existent growth, the literature points to higher education's business model, infrastructure, and gap in talent as challenges.

Best Practices for Higher Ed BI Success
1. Upper management champion and sponsorship. 2. Data governance that considers IT strategy and university business strategy (e.g., Analytics Centers of Excellence). 3. Create a culture of data-driven decision making. 4. Talent acquisition and development. 5. Divest, reinvest, and differentiate in their IT operations.

Table 1 Best Practices for Higher Ed BI Success

Higher education's business model generally focuses on long term goals in 5-7 year strategic plans. Many leaders focus on long term goals such as employability, critical thinking skills, and developing civic leaders that are not easily collected or analyzed in the short term using BI (Dede, Ho, & Mitros, 2016). Traditionally, the adoption of BI and analytics has been used in admissions and enrollment management where there is more emphasis on institutional analytics (Yanosky & Arroway, 2015). Guster & Brown (2012) also note that politics, differing management styles, and expectations of BI hinder the use of BI; BI is often seen as cost-prohibitive by university executives that don't understand the advantages. Infrastructure issues also exist as higher education lacks IT infrastructure, data collection and cleaning processes (Dede, Ho, & Mitros, 2016). Guster and Brown (2012) noted that data integration at universities is non-existent and there is a garbage in garbage out trend that hinders the effectiveness of BI models. Higher education also deals with privacy (FERPA), security, and safety challenges with using data that adds to its existing list of challenges which makes the data accessibility by various analysts across the organization or/and the distribution analytics results more challenging (Dede, Ho, & Mitros, 2016).

People are considered to be higher education's most valued and important resource. Grajek (2016) echoes this line of thinking with saying, "institutions won't progress without the right people", and in higher education, there's a lack of people with talent in analytics. In a 2015 survey conducted by EDUCAUSE, institutions noted they needed additional personnel to provide analytics services; this need ranged in size from a 59% increase from schools with more than 15,000 students to a 100% increase from schools with less than 2,000 students (Yanosky & Arroway, 2015). When asked for the type of skills needed, the top were predictive modeling (92%), analytics tool training (89%), data visualization (88%), user experience development (87%), and data analysis (87%) (Yanosky & Arroway, 2015).
Historically, personnel in Institutional Research entities have acted as the data keepers and reporters in higher education institutions. Often understaffed, the IR offices have been the natural choice to be charged with the adoption of analytics and BI on campus. The historical perspective and discussion of IR's current mission provides insights on how it can be transformed to serve the BI and analytics needs of higher education.

3. INSTITUTIONAL RESEARCH OFFICES

History, Staffing and Functions

More than fifty years ago, institutional research became an established entity of importance within postsecondary institutions. They were established as vehicles to more systematically inform and provide data reports to key decision makers across the postsecondary institutions. While the demand for data has continued to grow across various industries and transformed them, higher education has lagged behind and continues to be in early stages of analytics maturity in its offerings to users in higher education (Grajek 2020). At present, IR provides services to a highly ranked set of users from the president, provost (chief academic officer) to other major administrative positions on campus (e.g., Chief Business Officer) including those that report to government agencies and accreditation bodies.

According to the last national survey of institutional research offices, the major contribution of the IR office to top decision makers across institutions involving development of routine and ad hoc reports, analyses, alerts, and forecasts (Swing, Jones and Ross 2016). The primary responsibilities breakdown from the survey reveals that the executive levels of higher education depend on IR for a broad range of decision support, monitoring, and mandatory reporting (See Figure 1).

IR PRIMARY RESPONSIBILITY
83% data reporting – federal mandatory
81% data reporting – guide books/rankings
81% institutional fact books
80% data reporting – state mandatory
74% enrollment reporting and analyses
64% data sharing with consortia
53% key performance indicators

Figure 1 Primary responsibilities of IR adopted from Swing, Jones and Ross (2016, pp 6).

While IR caters to lower level data needs of departments and colleges as well, they are often understaffed and hard pressed to meet data and reporting needs related to the success of educational programs and student cohort success. Still, it is considered the largest center for analytics within the majority of higher education institutions though its functionality is limited to responding to basic reporting needs (Volkwein 2008).

Aspirational Statement for IR

As IR has evolved over the past 50 years, the Association for Institutional Research (AIR) published an aspirational statement for IR in the future. The aspirational statement was developed and vetted by IR offices in the United States in conjunction with the AIR staff. In the statement, four overarching roles are stated for IR offices. The first is for IR to become a change agent on campus broadening the decision makers on campus (Swing and Ewing-Ross, 2016). Instead of the executive leadership being the main decision maker, IR offices are aspiring to include staff, faculty, and students as decision makers and provide data to the various groups. Secondly, IR is aspiring not to be the only source of truth with the data but work to be data coaches for decision makers (Swing and Ewing-Ross, 2016). Instead of focusing on traditional enrollment counts and graduation metrics, IR offices are now aspiring to focus more on the student experience (Swing et al, 2016). Lastly, the future role of IR offices should focus on the oversight of analytical tools as resources for all, not just top-level leaders (Swing and Ewing-Ross, 2016). With this new vision in place, IR offices are setting themselves up to expand their analytical capabilities and foster a culture that is conducive for BI.

4. IR's ROLE IN BI

In looking at the responsibilities for analytics on campus, Yanosky and Arroway (2015) found that 43% of analytics were a shared responsibility between IR/IT departments, while 27% were a sole responsibility for IR departments, and 17% were a sole responsibility for IT departments. One of the biggest challenges facing IR as it tries to take on a more active role in higher education analytics is that it often has restricted or no access to critical institutional data needed by decision makers (Swing et al 2016). On average almost 40 to 50 percent of data that is often required to give a holistic view of student success and retention (see Table 2) is not accessible by IR and it limits its ability to offer the best analytics metrics, forecasting and KPI dashboards needed for effective student interventions.

No Access	Restricted Access	Data Type
57%	15%	Class Attendance
49%	22%	Student early warning alerts
43%	22%	High school transcripts
43%	25%	Academic advising data
23%	36%	Financial aid data

Table 2 IR's Institutional Data Access adopted from Swing, Jones and Ross (2016, pp 7).

It is essential that IR gain better access to data distributed across the organization. Clune-Kneuer (2016) notes the importance for IR/IT offices to collaborate on analytics as competing resources and time constraints can result in tensions between the two entities. By working together, IR and IT can help translate technical systems and processes to the campus that can be understood more easily (Clune-Kneuer, 2016). As a field, IR appears to be evolving in the roles, perspective and functionality it offers to an academic institution. The professional organization for IR has always been a beacon in introducing and directing this latest evolution of institutional research on campus. To understand how the field has evolved, the influence of its professional organization is assessed next.

BI Trends in IR Community: Examining IR's Professional Organization

The Association for Institutional Research (AIR) holds an annual conference for professionals working in institutional research offices in higher education. According to AIR, the annual conference, also known as the Forum, is the world's largest gathering for higher education professionals working in institutional research, assessment, and planning (Association for Institutional Research, 2019). To examine the rise in BI and analytics in IR, the Forums conference books from 2012 to 2018 were analyzed to look for trends in keywords used and sessions offered.

Keyword Search

A keyword search was conducted for BI and analytics keywords in each year's AIR conference book (Association for Institutional Research, 2012/2018). The keywords searched for included: data science, business intelligence, analytics, dashboard and visualization. Figure 2 located in the Appendix details the results of the search for the 2012 to 2018 timeframe. The results indicate the biggest increase in referencing visualization and analytics. In 2012, visualization was mentioned 14 times and jumped to 86 in 2016. Analytics jumped from being mentioned 42 times to 84 in 2018. Business intelligence remained flat and data science was not mentioned in the conference book until 2014 and was only mentioned 6 times in 2018. In 2019, an entire session on data science was offered: "Data Science Communicator: The Sexier Job of the 21st Century." This session presents the first time that an entire session was presented on this topic that provides further evidence of the growing importance of this topic.

Sessions Offered

The AIR Forum conference provides participants with the opportunity to learn more about the latest trends in higher education institutional research. Most of the sessions are geared towards education on the latest methodologies/approaches, best practice case studies and collaboration opportunities for participants to discuss common issues. Participants can submit session proposals for the Forum in one of six categories: (1) assessment, accountability, and accreditation, (2) data analysis and research, (3) operations, (4) campus decision support, (5) technologies, and (6) reporting and transparency. BI and analytics sessions would traditionally fall under one of three categories: data analysis and research, technologies, and campus decision support. To look at the trends in sessions offered, each session was tallied with the category submitted and a percentage of the total sessions were calculated for each category (Association for Institutional Research, 2013/2017). The results from 2013 to 2017 presented in Figure 3 in the Appendix show an increase in technology sessions and a decrease in assessment sessions over the years (Note that 2012 could not be added to this analysis as in Figure 1 as the session categories were different in 2012. Furthermore, the 6 categories were changed and a completely different format was adopted starting in 2018; as such, the results in Figure 3 only go up to 2017). Technology presentations rose 7% to 17% of the total sessions while assessment decreased 8% to 17% of the total sessions in 2017. Data Analysis and Decision Support sessions also show an upward trends indicating the growing importance of BI and analytics in the field.

5. CONCLUSIONS

The need for more comprehensive Business Intelligence and advanced analytics in higher education keeps growing as higher education becomes more complex. While some institutions have adopted BI in their business models, most institutions are still in the planning or consideration phase (Yanosky & Arroway, 2016). The University of Maryland, St Cloud University and University of South Florida provide case studies of implementations and pockets of success within the industry. From the literature, institutions face challenges in leadership, culture, skills gap in human capital, and a lack of IT infrastructure in building a robust BI operations (Dahlstrom, 2016). When looking at the field of Institutional Research within higher education, similar trends exist. There is an uptick in technology presentations at the annual conferences and an increase in the use of keywords such as visualization and analytics, the terms and number of sessions on BI are small but are on the top of the lists of areas that are trending according to Figure 2 and 3. As institutions move forward, the need for BI is critical. Data and analytics provided through institutional research entities within higher education has the potential to help higher education students and institutions succeed. Institution leaders who have been on the forefront of these changes such as St Cloud have seen these benefits.

University leaders should invest resources into their institution’s IT infrastructure and view data as a strategic asset to transform their information into knowledge for decision making to ensure a positive future for their schools. According to the Association for Institutional Research (AIR), EDUCAUSE, and the National Association of College and University Business Officers (NACUBO) data analytics can transform higher education and save it from the current perils it faces. In a joint statement they stated that “the meaningful use of analytics that take advantage of the power of data to make decisions and take actions just may save higher education” giving hope to many higher education institutions that are struggling with the uncertainty posed by market conditions today (Neelakantan 2019).

6. REFERENCES

Association for Institutional Research. (2012). 52nd annual AIR forum program book and schedule. Retrieved July 10, 2020 from http://forum.airweb.org/2012/Documents/WebResources/AIR2012ProgramBook.pdf

Association for Institutional Research. (2013). 53rd annual AIR forum program book and schedule. Retrieved July 10, 2020 from https://www.airweb.org/EducationAndEvents

Association for Institutional Research. (2014). 54th annual AIR forum program book and schedule. Retrieved July 10, 2020 from http://forum.airweb.org/2014/Documents/2014ForumProgramBookFinal.pdf

Association for Institutional Research. (2015). 55th annual AIR forum program book and schedule. Retrieved July 10, 2020 from https://www.airweb.org/EducationAndEvents/AnnualConference/Documents/2015%20Forum%20Program%20Book%20Web.pdf

Association for Institutional Research. (2016). 56th annual AIR forum program book and schedule. Retrieved July 10, 2020 from https://www.airweb.org/EducationAndEvents/AnnualConference/Documents/2016_AIR-Forum_Program-Book.pdf

Association for Institutional Research. (2019). 59th annual AIR forum program book and schedule. Retrieved July 10, 2020 from https://www.airweb.org/EducationAndEvents/AnnualConference/Documents/2019_AIR-Forum_Program-Book.pdf

Catalano, D. (2020, August 6). What Data Can and Can't Yet Tell Us. Www.Insidehighered.Com. https://www.insidehighered.com/views/2020/08/06/due-covid-demand-analytics-has-risen-significantly-information-doesnt-mean-action

Clune-Kneuer, K. J. (2016). Growing an IR and IT garden. *EDUCAUSE Review, 51*(3), 48-19.

Dahlstrom, E. (2016). Moving the red queen forward: Maturing analytics capabilities in higher education. *EDUCAUSE Review, 51*(5), 36-54.

Dede, C., Ho, A., and Mitros, P. (2016). Big Data Analysis in Higher Education: Promises and Pitfalls. *EDUCAUSE Review* 51, no. 5.

Dosal, P. (2019). Culture, Care, and Predictive Analytics at the University of South Florida, EDUCAUSE Review, December 9.

Durso, T. (2009). From data to information: Business intelligence and its role in higher education today. *University Business*, 24-27.

Foresman, B. (2020, October 19). U. Wisconsin taps analytics to ensure students learn during pandemic. Www.Edscoop.Com. https://edscoop.com/university-wisconsin-madison-data-analytics-pandemic-student-learning/

Grajek, S. (2016). The top 10 IT issues 2016: Divest, reinvest, and differentiate*.* *EDUCAUSE Review, 51*(1), 10-63.

Grajek, S. (2020). The top 10 IT issues 2020: The drive to digital transformation begins*.* *EDUCAUSE View Special Report,* 1-34.

Guster, D. and Brown, C. G. (2012). The application of business intelligence in higher education: Technical and managerial perspectives. *Journal of Information Technology Management*, *23*(2), 42-62.

Hutchinson, A. (2020, August 11). What Happens on the Internet Every Minute (2020 Version) [Infographic]. Social Media Today.

Krawitz, M., Law J., and Litman, S. (2018, August 8). How higher-education institutions can transform themselves using advanced analytics. Retrieved https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-higher-education-institutions-can-transform-themselves-using-advanced-analytics.

Laney, D. (2001). 3D data management: Controlling data volume, velocity, and variety. *META Group*, 3.

Miller, T., and Irwin, M. (2019). "Culture, Care, and Predictive Analytics at the University of South Florida," EDUCAUSE Review, December 9.

Miyares, J. and Catalano, D. (2016). Institutional analytics is hard word: A five year journey. *EDUCAUSE Review, 51*(5), 8-9.

Neelakantan, S. (2019, November 26). 'Data Analytics Can Save Higher Education', Say Top College Bodies. *EdTech*, https://edtechmagazine.com/higher/article/2019/11/data-analytics-can-save-higher-education-say-top-college-bodies

Petty, C. (2019). Why Data and Analytics are Key to Digital Transformation. Gartner. Retrieved July 10, 2020 from. https://www.gartner.com/smarterwithgartner/why-data-and-analytics-are-key-to-digital-transformation/.

Reinsel, D., Rydning, J., and Gantz, J. (2020, April). Worldwide Global DataSphere Forecast, 2020-2024 (Rep No. US44797920). Retrieved https://www.idc.com/getdoc.jsp?containderID= US44797920.

Swing, R. L. and Ewing-Ross, L. (2016). A new vision for institutional research. *Change*, 6-13.

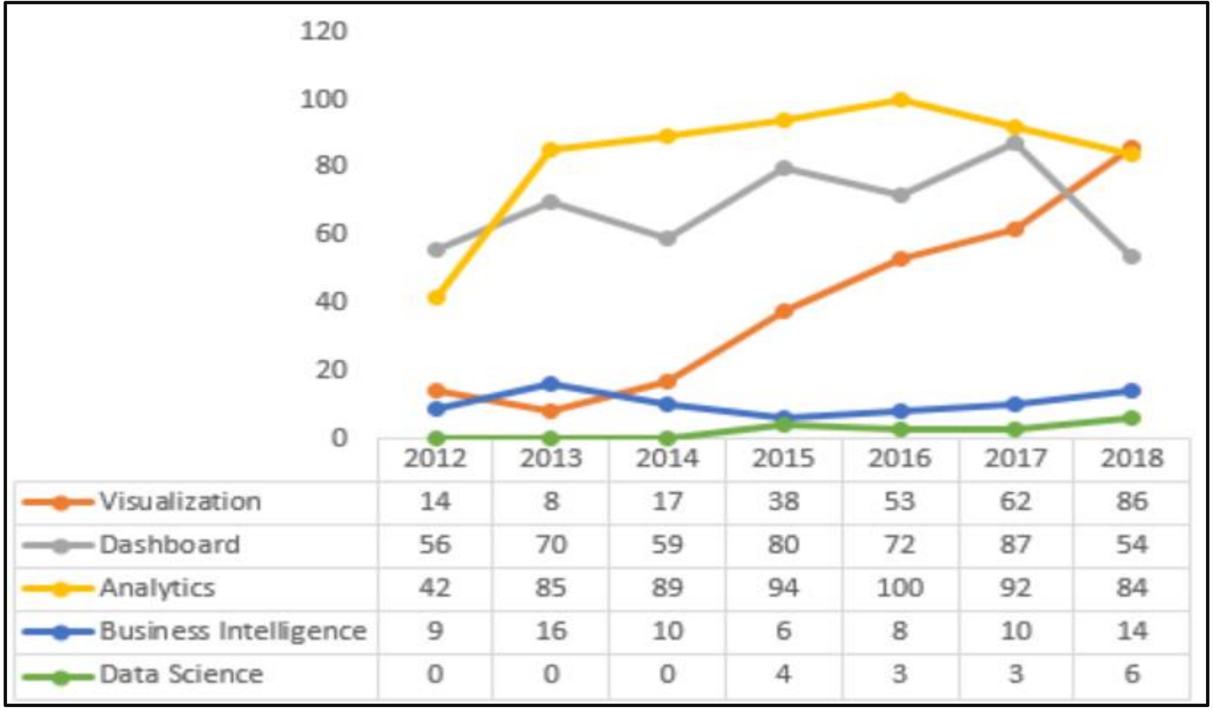
Swing, R. L., Jones, D., and Ross, L. E. (2016). *The AIR National Survey of Institutional Research Offices*. Association for Institutional Research, Tallahassee, Florida. Retrieved July 10, 2020 from http://www.airweb.org/nationalsurvey

Yanosky, R. & Arroway, P. (2015). The analytics landscape in higher education. *Education Center for Analysis and Research*, 1-34.

Volkwein, J. F. (2008). The Foundations and Evolution of Institutional Research. New Directions for Higher Education, 141, 5-20.

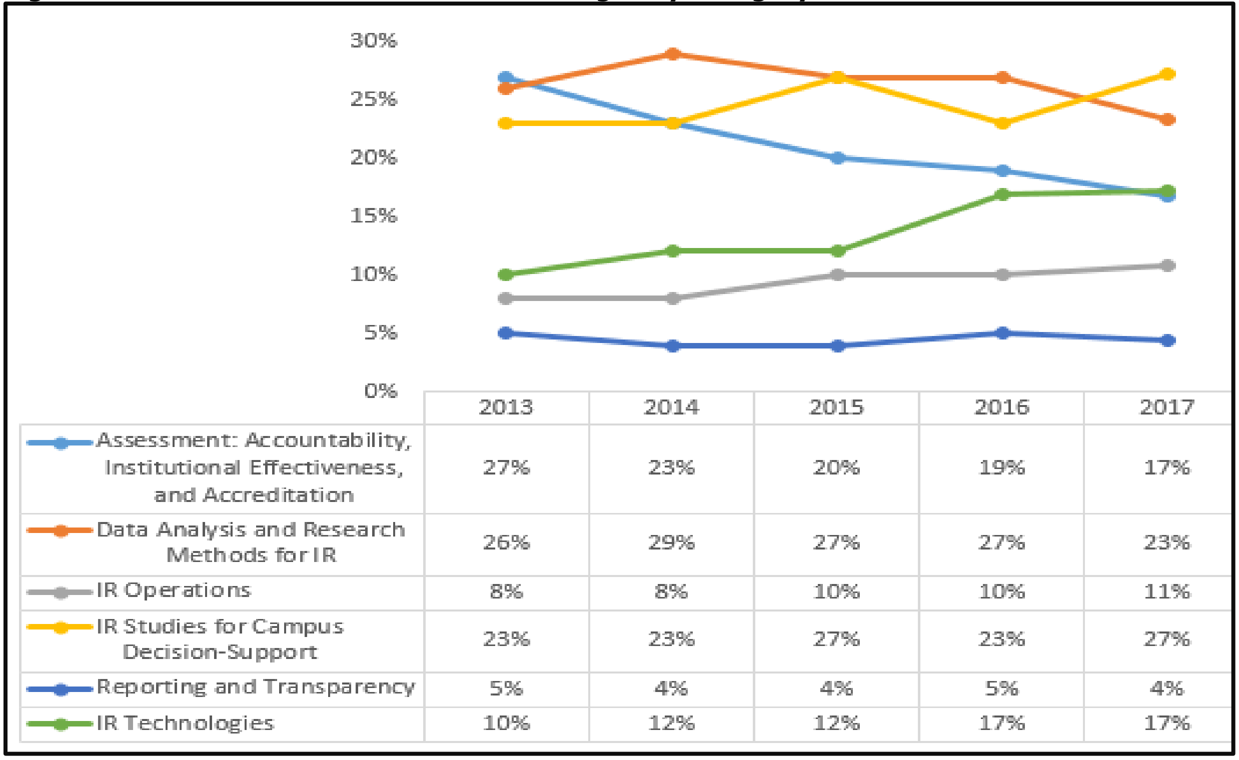
Appendices

Figure 2. AIR Conference Book Keyword Search



	2012	2013	2014	2015	2016	2017	2018
Visualization	14	8	17	38	53	62	86
Dashboard	56	70	59	80	72	87	54
Analytics	42	85	89	94	100	92	84
Business Intelligence	9	16	10	6	8	10	14
Data Science	0	0	0	4	3	3	6

Figure 3. AIR Conference Sessions Percentages by Category



	2013	2014	2015	2016	2017
Assessment: Accountability, Institutional Effectiveness, and Accreditation	27%	23%	20%	19%	17%
Data Analysis and Research Methods for IR	26%	29%	27%	27%	23%
IR Operations	8%	8%	10%	10%	11%
IR Studies for Campus Decision-Support	23%	23%	27%	23%	27%
Reporting and Transparency	5%	4%	4%	5%	4%
IR Technologies	10%	12%	12%	17%	17%

Case Study of Blockchain Applications in Supply Chain Management-Opportunities and Challenges

Blaise Smith
smithba7@appstate.edu

Jason Xiong
xiongjj@appstate.edu

Dawn Medlin
medlinbd@appstate.edu

Department of Computer Information Systems
Walker College of Business
Appalachian State University
Boone, NC 28608, USA

Abstract

Blockchain and its related technologies start to present business values recently. This research analyzes blockchain adoption within the field of supply chain management by looking at companies that have already put blockchain technology into practice. Fascination and doubt have grown exponentially will Blockchain technology and with cryptocurrencies in general. Since blockchain technology is relatively new, there is much to be looked at with thinking about its impacts, good or bad, on the field of supply chain management. This research investigates the challenges that companies will face and potential opportunities when adopting blockchain applications. Overall, the research question is What are the opportunities and challenges of blockchain adoption in Supply Chain Management? This research conducts a case study of blockchain adoption within real companies. Different effects of blockchain on various aspects of supply chain management are discussed and analyzed.

Keywords: Case Study, Blockchain, Technology Adoption, Supply Chain Management.

1. INTRODUCTION

Blockchain was first introduced to the public in 2008 after Satoshi Nakamoto, whose real identity remains secret, released the whitepaper "Bitcoin: A Peer to Peer Electronic Cash System" (Marr, 2018). Nakamoto's whitepaper describes bitcoin as a "purely peer-to-peer version of electronic cash." The original purpose of bitcoin was to address double-spending, which is often a problem faced by digital artifacts. Digital tokens are known to be easily copied and spent multiple times, which is fraudulent. Copying digital tokens and spending them multiple times can cause inflation by creating massive amounts of money that were not previously there.

Since blockchain is the technology supporting bitcoin, it caused significant interest in blockchain technology to gain traction worldwide. Fascination since the whitepaper has grown exponentially for both blockchain technology and cryptocurrencies in general. Today, companies worldwide are exploring ways to incorporate technology into pre-existing business activities to meet new performance goals. Blockchain is a shared digital ledger that cannot be altered and facilitates business transactions and tracking assets in a business network. These assets can be tangible or intangible.

To fully understand blockchain, it is crucial first to understand distributed systems. At its core, Blockchains a distributed system, which is defined as a "computing paradigm whereby two or more nodes work with each other in a coordinated fashion to achieve a common outcome" (Bashir, 2017). It is modeled in a way that allows end-users to see it as a single logical platform. A distributed system is essentially a group of computers working together to appear as a single computer to the end-user (Kozlovski, 2018). The machines within a distributed system have a shared state but can fail independently without causing a huge problem, making them incredibly secure.

Unlike a typical financial ledger, Blockchainllows for parties to transact without using a central authority to validate the transactions (Jaikaran, 2018). Typically, the central authority is a third party, such as a bank or another financial institution. Transactions within the blockchain are not limited to financial ones. It may also include tracking items, identity logging, verifying complete actions, or any other activities not mentioned. In blockchain technologies, there is no need for a third party. The transactions are added, the identities of the parties conducting the transactions are verified, and the transactions are verified before putting them into the ledger as a block. Since each transaction block depends on the previous block, any change made will alert all users of change to the history of transactions, making it incredibly secure for all parties. Also, relationships between identities, transactions, and the ledger allow for parties to have a higher degree of confidence in the state of transactions (Jaikaran, 2018).

Overall, the research question is **What are the opportunities and challenges of blockchain adoption in Supply Chain Management?** This research conducts a case study of blockchain adoption within real companies. Different effects of blockchain on various aspects of supply chain management, such as quality, efficiency, and traceability, are discussed and analyzed.

2. BLOCKCHAIN TECHNOLOGY MARKET

Blockchain technology is one of the most promising upcoming and technological trends in the information technology domain (Grand View Research, 2019). The global blockchain technology market was valued at USD 1,590.9 million in 2018. It is expected to grow at a compounded annual growth rate of 69.4% from 2019 to 2025, according to a new study conducted by Grand View Research, Inc.

Currently, the annual value of fraud and cyber-attacks within the Banking, Financial Services, and Insurance (BFSI) sector is estimated to be thousands of millions of dollars. This has become a challenge for companies globally. To overcome this problem, companies like Microsoft Azure and Deloitte are focusing on offering blockchain-as-a-service. Improved penetration in deploying "Proof of Concept" solutions by leading providers of blockchain technology and the rising need for faster and transparent transactions across various industries is expected to propel the market's expansion during 2018-2025.

As technology applications in business processes are growing, the need for solutions such as blockchain technology is expected to disrupt current activities. One of the main drivers of blockchain adoption is the growing adoption of distributed ledgers among banking and financial institutions (MartketWatch, 2019). This is one of the significant portions of blockchain technology. Another driver within the market today is the rising capitalization of cryptocurrencies. As mentioned before, Bitcoin and Ethereum are prime examples of cryptocurrencies. The growing need for technological solutions is also a driver within the market for blockchain technology, especially in more prominent companies with many resources to focus on. Another driver for adopting blockchain technology is the increasing venture capital investment in Blockchain and Initial Coin Offering (ICO). ICO is the funding of cryptocurrencies.

Researchers have found that more and more companies believe that blockchain technology will be critical within the next 24 months (Deloitte Insights, 2019). In a study by Deloitte, 53% of respondents believe that technology will be vital within the top 5 strategic priorities. More respondents now than in 2018 believe that blockchain technology is broadly scalable and can be utilized in many different industries. Blockchains maturation is expected to continue as an overall investment in the technology increases. This supports the notion that in the long term, blockchain technology has much potential. Taking a closer look at companies putting into place blockchain technologies, we can see the positive impact on supply chains.

3. CASE STUDY

Walmart

Walmart is one of many industry leaders that is putting into place blockchain technology initiatives. For example, Walmart Canada has launched the "world's largest full production blockchain solution for any industrial application" (Retail Info Systems, 2019). This initiative is a partnership between Walmart and DLT Labs; a company solely focused on developing blockchain solutions for enterprises. The new system uses distributed ledger technology to track deliveries, verify payments, and automate payments. It also follows reconciliation between Walmart Canada and its carriers. The company's carriers deliver products to over 400 retail stores across Canada annually. Walmart Canada went live with the operations in February of this year after completing two pilot programs with IBM: one for pork and one for mangoes.

Walmart worked with IBM to design and implement food pilots using blockchain technology. According to McDermott, "Blockchain solves business problems where trust is part of the solution" by providing what traditional databases cannot, which is data immutability as well as speed and security and dissemination (Kamath, 2018). IBM's solution was based on Hyperledger Fabric, which supports modular architecture as well as plug-and-play components. Records within the system include audits, agricultural treatments, identification numbers, manufacturers, known security issues, granted permissions, and safety protocols. This data is logged in real-time and is permanently store for future use. The technology is thought to provide trust, enabling higher efficiency and complete sharing of data, which is highly useful in supply chain environments and business in general.

Walmart uses this technology in China to ease consumers' worries regarding food safety in growing food automation (Kamath, 2018). In October of 2016, Walmart launched the Food Safety Collaboration Center, where the center studies foodborne contaminants and develops risk assessment models to use other companies. Walmart has also invested in technologies to detect foodborne pathogens and to monitor package food contaminations. The cooperation with government agencies was crucial to the success of Walmart's pilot programs.

Blockchain technology enables food traceability down to the item level, rather than batch level or even facility. Walmart's initiative helped to identify which information is essential to track. This allows for data categories to be documented as mandatory or optional, as what data can be cut out of the tracking process. This document provides for the amount of data to be manageable and keeps the process efficient. The pilot program also ensures the reliability of data collected and works out all potential problems that the company would otherwise face.

Coca-Cola

In November of 2019, Coke One North America (CONA) announced that they would be deploying blockchain technology (Williams, 2019). Coke One North America is the technology firm that manages IT operations for Coca-Cola's bottlers. The company is currently utilizing SAP's blockchain technology to shed light on its many transactions each year.

The blockchain technology allows bottlers to see into the inventory of other suppliers, allowing them to purchase the items needed to fulfill demand if not already on hand. The technology helps CONA by processing those transactions at a faster pace, making the company more efficient. Torsten Zube, who is head of the SAP Innovation Center Network, believes that the blockchain technology is creating a document flow across the supply chain for CONA (Williams, 2019). The SAP Innovation Center Network is tasked with finding use cases for the new emerging technology. Using the tool, CONA hopes to spur greater productivity, increase cost savings, and speed up cash flow between the different franchises.

The pilot program originally started between just two bottlers, Coca-Cola United and C.C. Clarke. This program has been scaled across all bottlers after seeing improved results. With the technology put into place, franchises can see if an order can be fulfilled and leads to necessary adjustments to happen faster. Blockchain technology also allows CONA to dispute transactions quicker and more effectively since it can now see all the online ledger transactions. The technology makes the transactions clearer and more transparent.

UPS Case

Early 2019, UPS announced its partnership with Inxeption, creating the platform Inxeption Zippy. It aims to set up shipments and send shipments easier going from business to business within the marketplace. The platform helps businesses market and distribute their products on multiple online channels, making it more secure (Conwell, 2019). The platform allows merchants to quickly set up an account that enables manufacturers, distributors, and wholesalers to be more connected and conduct e-commerce transactions. Since technology is blockchain-backed, sensitive information is ensured to be safe. The information collected is only available between the buyer and seller. The partnership between UPS and Inxeption allows for a more seamless end-to-end experience. Since the partnership involves UPS, merchants can view their entire supply chain every step of the process.

UPS has also partnered up with HerdX, which provides end-to-end insights into food supply chains. The partnership between UPS and HerdX has already completed a test trial to use blockchain for beef traceability from a farm in the United States to Japan. HerdX's blockchain solution uses connected tags, readers, and verified data, much like Walmart (Ledger Insights, 2019). HerdX monitors both animal movement and health to ensure the best quality beef for consumers. UPS's partnership with HerdX allows for live updates of the product from farm-to-table essentially.

HerdX's blockchain collects data such as the animal's birth, where the herd was raised and enabled farmers to keep a watch on each animal. Since UPS is a transportation company, HerdX and UPS's partnership allows for the business to track shipments using blockchain throughout the entire supply chain process. UPS Logistics and Freight provides services for over 200 countries worldwide, which gives HerdX the massive scalability power to provide for cattle producers worldwide, changing the entire industry as more and more companies utilize the technology.

In the trial, a shipment of beef left from Kansas in one of UPS's temperature monitoring packaging (Ledger Insights, 2019). The packaging had sensors monitored and recorded data throughout the shipment's journey. Once the package arrived at its destination, the data was recorded in HerdX's blockchain platform. Customers who want to look up where exactly a product came from can scan the QR code to view the verified health and data of the meat they are buying. This creates trust between both the customer and the farm. This case can also be applied to other products, not just food.

4. ANALYSIS

Efficiency

There are many potential applications and benefits of utilizing blockchain technology within supply chain networks. One of the main advantages of deploying blockchain technology is to improve efficiency for everyday business activities such as communicating with business partners, completing transactions, tracking documents, as well as much more. For example, the use of smart contracts is typically part of blockchain technologies. A smart contract is a self-executing contract where the terms of the agreement are directly written into node (Frankenfield, 2019). After being written into the lines of code, it now exists in a blockchain network.

Within the supply chain field, smart contracts can be used to automate the transfer of title to goods and money, which removes the need for third-party facilities. An example of this is Letters of Credit. The use of smart contracts helps to streamline the whole process. Also, since there is no need for third parties, the overall cost will be reduced, thus saving companies money in the long term. Smart contracts cause faster cycle times by reducing the amount of time it takes by creating a more efficient process.

Maersk's partnership with IBM is just one example of blockchain technology being implemented to improve efficiency. Through the use of blockchain technology, Maersk can more efficiently and effectively work with the company's partners. For example, the average end-to-end container shipment involves more than 30 organizations, more than a hundred people, and more than two hundred information exchanges. Through the use of technology, the process of sharing and collaborating with documents is streamlined. Blockchain allows for the transfer of data and information to be transferred at a much faster pace.

Transparency/Traceability

As globalization and growing complexities in the marketplace grow, supply chain transparency becomes exponentially more critical. Today, companies face many problems in the everchanging market due to a lack of transparency in supply chain networks. An example of this is Coca-Cola's partnership with SAP to develop a blockchain solution to track and validate transactions between0 different franchises (Battrick, 2019). Coke One North America (CONA), as mentioned previously, is the technology firm that manages IT operations for Coca-Cola bottlers. Currently, CONA oversees 12 suppliers with hundreds of thousands in orders.

Since Coca-Cola is so large, the technology's ultimate goal is to increase efficiency, reduce cost, and accelerate cash flow in the company's supply chain. Coca-Cola's supply chain is currently worth $21 billion in yearly revenue, which is a massive amount. With SAP's blockchain solution, CONA can reduce the duration of order reconciliation from 50 days to just a few days (Huillet, 2019). This drastically improves its efficiency as well as provides the company with more insights. The technology also offers real-time insights into shipment information and the transactions made by all the different bottlers on the Network. As an example, let's say a bottle maker is short of stock for an order. The Network will quickly provide options for filling the shortfall. This allows for fewer shipping errors, less missed deadlines, and lowers operational costs as a result.

If more companies were to implement technology, transportation costs across many industries would be significantly reduced. This is because they would get shipments faster and have less cost associated with the holding of shipped items. This would also allow for increased transparency, giving companies better insights into how its efficiency is and would provide companies the opportunity to invest more into components of its business practices rather than efficiencies.

Walmart is also utilizing blockchain technology to improve transparency within its supply chain. There is no widely adopted industry standard for how the food industry tracks and records data for traceability purposes. Companies within the industry will often record data on paper, while other companies use digital methods to track. While some companies are using these digital methods, there is no way for companies to communicate effectively and efficiently. The current system for food tracking is highly limiting transparency for all organizations within the industry. Since the system is lacking, Walmart is leading the industry in creating a solution to this problem (Yiannas, 2018).

UPS has also started to use blockchain technology for its operations. Last year, the company applied for a United States patent to use blockchain technology to track packages through multiple carriers globally. This technology allows the company to track international air freight shipments and verify shipments. Also, in 2017, the company joined the Blockchain in Transportation Alliance. This is a group of corporations that set a standard of utilizing blockchain technology in transporting products. Having a set standard is beneficial because the more companies that operate blockchain, the better off they are using the technology. Having other businesses within the same industry utilize similar technology allows for the technology to grow, and each company can learn from each other.

Quality

Blockchain technology also can provide many insights for companies looking to improve the visibility of its entire supply chain and increase efficiency and improve product quality. One way to enable higher quality products is by providing essential information such as environmental aspects when transporting goods throughout the entire process. By providing critical information, manufacturers can pinpoint exactly where problems may occur.

By looking at the food industry, this can be seen very easily. For example, if a truck is transporting milk, strict temperature guidelines must be followed to keep the product healthy for customer consumption. Blockchain technology can track what temperature the truck is transporting the goods and information regarding if the product is spoiled or not. If a truck thermostat topped working, the company would be able to see that the temperature is wrong and pinpoint precisely when it malfunctioned. This would allow the company to identify precisely which group of products is affected by the malfunction, enabling the company to save time and money by knowing which products need to be thrown away.

This type of example can be transferable to all other products. Another example of this is cars being manufactured. Recalls are widespread within the car industry and cost manufacturers a lot of time and resources each year to fix. Often when a part is recalled, the company does not know which exact cars have the defective part. If car manufacturers were to put into place blockchain technology, it would save the company a lot of time and resources by enabling the company to see where exactly the defect happened and which cars were affected instead of the company guessing a large batch of vehicles. This would allow for fewer resources to be wasted, saving the company a lot of money each year.

Vulnerabilities

Since the technology is so new, there are many potential problems that companies should be aware of before deciding to implement blockchain technology. One problem with blockchain technology is double-spending. Although blockchain technology was created to combat the problem of double-spending, it can still happen. Double spending is a fundamental problem that businesses could face after implementing blockchain technology. Double spending occurs when a user makes multiple payments using one funding form. This can appear because transactions are validated by solving a mathematical problem. When unprocessed amounts are broadcasted across the Network, broadcasting disruptions can happen, causing double-spending (Hasanova et al., 2018). For example, an attacker could trick a retailer into accepting a transaction that the retailer cannot reverse by doing the following.

In this scenario, the attacker could start a transaction just like the original except change the recipient's address. If both transactions are initiated simultaneously to peers on the chain, the chain will not accept multiple transactions that share common inputs. Instead, they will only accept the version of the transaction that reaches them first. Although, the transaction could go out to other peers, making it successful in causing double-spending. There is no way for companies to get around double-spending; it will always be a potential threat.

Another potential challenge faced by companies implementing blockchain technology is a 51% attack. Both a 51% attack and double spending can happen at any time, meaning companies must know this possibility. A 51% attack refers to miners controlling more than fifty percent of the network hash rate, which is the computing power. During this attack, an attacker could be able to obstruct the confirmation of new transactions. An attacker can also reverse transactions, but only if they hold the majority power over the Network. This could cause double-spending. Although a 51% attack could happen, it would be tough for an attacker to take over the blockchain. This is because transactions are locked before the start of an attack if the attempt has to do with historical blocks.

In August of 2016, both Ethereum Krypton and Shift experienced 51% attacks. While they experienced the attacks at low levels, a 67% attack would cause severe problems to a company (Hasanova et al., 2018). At the 67% level, the attacker can essentially block and reject any transaction they want to. They can also form any transaction themselves. To combat this, precautions must be set into place to make sure that something like this does not happen. Also, companies should take necessary measures to protect themselves and to protect customers within the system.

Another challenge of blockchain technology is that it takes up a large amount of energy and can be costly. Currently, developers are looking into ways to make blockchain technology more energy-efficient and develop the technology to be faster than it already is. One way developers are looking to make the technology more efficient is by enabling parallel processing. This allows for simultaneous transactions to be processed. Some recently developed technologies can process thousands of transactions per second, making the technology highly scalable.

Also, while there is a lot of growth within the industry in developing blockchain technologies and implementing it, there is still not a standard for the technology. Since there is no standard, companies must figure out how to either develop their own technology or implement an already developed technology version. This can cause massive amounts of money to be invested and to be improperly used. This would essentially be creating a technology that will not be used and would burden the company. Although this is an issue, as more companies utilize the technology, standards will be developed, thus benefiting all companies utilizing similar technology.

5. CONCLUSION, LIMITATIONS, AND FUTURE RESEARCH DIRECTION

Blockchain technology can prove highly valuable for companies willing to learn new technology and be willing to take some risks. While blockchain technology is fairly new and evolving, many potential benefits make investing in technology worthwhile. Some of the benefits seen are improved efficiency, transparency, and traceability and the ability to enable higher quality products to be sold to consumers. Blockchain does this by providing distributed ledgers that are immutable and provide real-time data regarding shipments and provide access to documents needed throughout the supply chain process.

While improving efficiency, transparency, and traceability, the technology allows a company to save money by producing products more effectively. Blockchain technology enables companies to spend less time completing tedious tasks without the use of blockchain. Activities such as shipping details, tracking details, ad much more can all be stored in one place and accessed by various company groups. This data can also be shared with people outside of the company, making collaboration easier to accomplish, enabling greater productivity and higher cash flow.

While there are many benefits to deploying blockchain technology, there are also potential issues that need to be thought about before scaling the technology company-wide. This is why companies such as Walmart, Coca-Cola, and UPS do pilots before fully committing the technology to their entire organization business practices. Some of the risks include double-spending, cyber-attacks, high energy costs, and high set-up costs. While the technology was created to combat the problem of double-spending, it can still happen. Keeping this in mind, companies can take protective measures to help ensure their information is secure.

Since technology is online, there is always a potential of cyber-attacks. This can take form in many different ways, one of those being a 51% attack. Companies such as Ethereum Krypton and Shift have both reported this kind of attack happening to them. As the problem of double-spending, companies should take countermeasures to ensure that their information is as secure as they can make it and be careful about which data is stored. This can prevent anything wrong from happening to the company's data.

High energy cost and high set-up cost can also be avoided. Companies will often provide the software as a service, enabling organizations to focus more on its practical usage rather than deal with the high costs associated with maintaining it and developing it. In many cases, there is at least a framework developed which will save costs. Also, blockchain technology's adoption will save companies more money in the long run, making the investment worth the high set-up costs. Overall, companies should weigh both the potential benefits and challenges that are associated with blockchain technology.

Limitations

This study's main limitation is that there is little to no quantitative data to measure the direct impact of blockchain technology on supply chain networks. This study's research is mostly based on theory and not necessarily have data to back it up. As more companies introduce technology, the association between technology and its impacts will be more measurable. Since the technology is so new much of the data regarding its direct impacts is kept secret within the company itself. It is not out there for public access. Also, as more companies use the technology, the data will become more accessible, and a conclusion regarding its impacts on a supply chain will be directly seen.

Future Research Direction

This research looks at qualitative data drawn from real company case studies and draws conclusions based on that. In future research of the topic, quantitative research should be addressed to add to assumptions already made. As the data becomes available, it will allow for a more holistic view of the direct impacts of blockchain technology on supply chain networks. The direct costs associated with the implementation of blockchain will be addressed as well as the amount of cost savings for each company. This will allow for both researchers and companies looking to implement the technology to plan ahead better, as well as provide them with the knowledge to make business decisions regarding the technology. As more companies implement the technology, it impacts on other areas besides efficiency, transparency, traceability, and quality can be addressed. Research in these areas can also be added to, providing more research overall.

6. REFERENCES

Archana Prashanth Joshi, M. H. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing*, 121.

Asma Khatoon, P. V. (2019). Blockchain in Energy Efficiency: Potential Applications and Benefits. *Energies, 12*(17), 3317-3317.

Bashir, I. (2017). *Matering Blockchain.* Birmingham, UK: Packt Publishing.

Battrick, R. (2019, November 19). *Coca-Cola Blockchain Solution to Address Complex Supply Chain*. Retrieved from Business Blockchain HQ:

https://businessblockchainhq.com/supply-chain-blockchain-news/coca-cola-blockchain-complex-supply-chain/

Conwell, V. (2019, 03 21). UPS And Inxeption Collaborate To Make B2B E-Commerce Easier For Merchants.

Deloitte Insights. (2019). Deloitte's 2019 Global Blockchain Survey : Blockchain gets down to business.

Frankenfield, J. (2019, October 8). *Smart Contracts*. Retrieved from Investopedia: https://www.investopedia.com/terms/s/smart-contracts.asp

Huillet, M. (2019, November 5). Coca Cola Using Blockchain for $21-Billion-Per-Year Network.

Jaikaran, C. (2018). *Blockchain: Background and Policy Issues.* Congressional Research Service .

Jayachandran, P. (2017, May 31). *The difference between public and private blockchain*. Retrieved from IBM: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Kamath, R. (2018). Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM. *The Journal of The British Blockchain Association*, 47-53.

Kozlovski, S. (2018, April 27). *A Thorough Introduction to Distributed Systems*. Retrieved from Free Code Camp: https://www.freecodecamp.org/news/a-thorough-introduction-to-distributed-systems-3b91562c9b3c/

Ledger Insights. (2019, November). UPS partners with HerdX for blockchain beef traceability.

MartketWatch. (2019, October 31). Global Blockchain Technology Market 2024 Industry Growth, Trend, Key Players Analysis.

Peter Verhoeven, F. S. (2018). Examples from Blockchain Implementations in Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology.

Retail Info Systems. (2019, 12 02). Walmart Canada Launches "World's Largest" Blockchain-Based Freight Network.

Williams, J. (2019, November 4). Coca-Cola bottlers and SAP are scaling a major blockchain project poised to remake a $21 billion-a-year supply-chain operation. It's one example of the still nascent tech's promise.

Yiannas, F. (2018). A New Era of Food Transparency Powered By Blockchain. *Innovations: Technology, Governance, Globalization*, 46-56.

Interpreting Organizational Security Governance Objectives for Strategic Security Planning

Sushma Mishra
mishra@rmu.edu
Computer Information Systems Department
Robert Morris University
Moon Township, PA 15108, USA

Abstract

The goal of this research is to conduct a case study examining the contextual use and purpose of organization security governance (OSG) objectives in strategic planning and preparedness for security initiatives. This study also explores for underlying dimensions of OSG practices. Mishra (2015) proposed 17 means OSG objectives that are theoretically driven and empirically grounded. An in-depth case study is conducted to examine and interpret the meanings of the above objectives in a real organizational setting and identify the dimension of OSG practices. There were 13 interviews conducted at various levels in the organization, and other secondary sources of data, such as policies, mission documents, and audit documents were reviewed. The findings suggest all 17 means objectives are useful in preparing the organization strategically for better security practices. The results also suggest four underlying dimensions of OSG into play in overall improving security practices. These dimensions are Structural, User, Facilitation, and Processual. This study empirically validates all means objectives for OSG from prior research. The OSG dimensions identified to provide a useful basis for strategic planning of comprehensive security. The practical implications lie in providing real organizational security governance dimensions that allow practitioners to use these as a tool to assess and implement security governance practices at all levels. The originality of the paper lies in its unique contribution to security governance literature in terms of empirically examining OSG objectives for strategic security planning purposes. It also proposes OSG dimensions that allow for in-depth preparedness for security initiatives at multiple levels.

Keywords: organizational security governance**,** case study, Facilitation, structural, processual, user, strategic, controls, IT audit

1. INTRODUCTION

Organizational Security Governance (OSG) objectives are critical in providing overall strategic leadership to the security preparedness of an organization (Mishra, 2015). OSG is a set of responsibilities and practices used by management to provide vision and direction to an organization and, in the process managing risks appropriately while optimally using resources available (ISACA Manual, 2012). Having the right security strategy requires the right OSG objectives for guidance. There are situations where security strategies created are not reflective of the values and strengths of the organization. OSG objectives provide clarity on "what is it that needs to be managed (Brotby, 2009)" and allow for meaningful management metrics.

Mishra (2015) proposed six fundamental and seventeen means objectives for OSG. In this study, the value-focused approach was used to develop theoretically driven and empirically grounded objectives. The study defines fundamental objectives as an objective that is essential and important in its own right for the decision context, in this case, security governance. An objective that leads to another objective being considered in decision-making is a means objective. The role of an objective (means or fundamental) is determined by its direct or indirect impact on the decision making context. The proposed objectives in Mishra (2015), however, have not been studied in an organizational setting to understand its implications on security preparedness.

This study examines the significance of the proposed seventeen means objectives in a real organization using a case study method. Fundamental objective, by definition, is established as critical for OSG practices; hence, the scope of this study is all the proposed means objectives. The main goal of this study is to assess and inform how the proposed means OSG objectives shape the strategic security planning and preparedness. This research also examines what are, if any, underlying dimensions of OSG objectives? The research question posed is: how do seventeen means (OSG) objectives influence security strategic planning and preparedness in an organization? The results suggest four underlying dimensions of OSG, namely, Structural, Processual, User, and Facilitation.

The section following the introduction presents the methodology section of the paper and describes the organizational context, data collection, and data analysis process. The subsequent section presents the results in the form of four underlying dimensions of OSG. Following the four dimensions of OSG, a discussion is generated that draws on research literature to explain the importance of the proposed dimensions. The implications and contributions are presented, and future research directions are suggested.

2. CASE STUDY

This study adopts an in-depth interpretive case study approach to understand the nature and significance of the developed governance objectives in an organizational context. Interpretive research does not predefine dependent and independent variables, but focuses on the complexity of human sense-making as the situation emerges (Kaplan and Maxwell 1994); it attempts to understand phenomena through the meanings that people assign to them (Orlikowski 1991). Case study help in getting a rich picture of the phenomenon under study without disturbing the natural state of entities.

Organizational Context

The case study site was the information technology (IT) department of a major City Council (hereafter referred to as CCIT) in the southeast of the United States of America. The (CCIT) is a state agency responsible for the administration of the City. The organizational goal is to work with customers to align business and technology objectives. A set of guiding values have been explicitly stated in the mission statement of the organization. Managing information security governance is identified as a strategic area of improvement by the agency. Security architecture at CCIT is focused on five areas: applications, authentication, networking & infrastructure, physical, and process. The management emphasizes that improving security controls will drive efficiency and effectiveness across the City.

CCIT helps its citizens to receive more from the state government in terms of the state of the art facilities enhanced by a strong information technology network. It also supports publicly accessible computers for free use by the citizens. The state uses an innovative technology planning process, which is driven by the business needs of the state and aligned with the City’s business initiatives. The strategic plan of the organization is to establish a standard framework and processes that deliver IT services for each agency and sets an enterprise view. Such planning intends to develop more enterprise-level targets and evolves from an agency focused goals. The benefits of such an approach are manifold. An enterprise approach by the agency reduces the costs of maintenance and helps manage enterprise-level risks. Building standard services leverages the resources and establishes effective partnerships between CCIT and other agencies.

The organizational structure includes the CIO as the head of the agency. Five managers directly report to the CIO.

The technology planning process is integrated among agencies and requires investment of resources from all. The organization must keep its procedures auditable so that public scrutiny is plausible. The organization, having the ownership of IT services, acts as a service provider to all the other agencies supported by the state. To provide excellent infrastructure, the organization approaches every agency individually and assesses the agency’s information needs and the current state of technology utilization. The organization targets improvements based on the specific needs of different agencies. These improvements are based on joint maps created with the IT organization and the agency.

Data Collection

Several sources of data were used for the case study. The primary source of data was the semi-structured interviews. Secondary sources include the policy and procedure manual, the audit manual at CCIT, the policy guidelines provided by the state agency, which is responsible for the security policies of the state agencies. Key stakeholders were identified at the case study site with the help of our point of contact at the organization. The participants were able to provide adequate insight into the organization's internal control structure in the context of information systems security. The target organization has four main divisions: IT development, IT infrastructure, Security, and Project management. Each division head and the manager from the particular department were interviewed. The CIO of the organization and the chief audit officer were interviewed as well. The overall representation of the respondents (top management, middle management, and operational level) provided useful insights into the applicability of the developed objectives in the particular organizational context.

Data analysis

Huberman and Miles (1994) suggest three ways of data analysis for qualitative interview data: data reduction, data display, and conclusion drawing. In the data reduction process, the researchers identify portions of the data, which is relevant for the theoretical construct under study. With useful data, the researchers categorize and structure the data in a way the meaningful interpretations can be drawn. The categorization is done through writing summaries, synopses, or making networked diagrams that permit conclusion drawing. Finally, conclusion drawing is the interpretive process through which the researcher compares themes, patterns, and then compares and contrasts to triangulate the data. Walsham (2006) suggests that even though the researcher is the agent of the interpretation, but a theoretical framework should be used to guide and bound the researcher. Each of the above three steps was performed several times, iteratively before actual results emerged. The initial 17 objectives were converted into groups based on the data from the case study. These clusters were revisited multiple times to finally come up with four clusters of objectives based on underlying themes. Identifying an informant and the key stakeholders in the case study setting helped in applying the triangulation technique. Each dimension of OSG is discussed in the results section.

3. RESULTS & DISCUSSION

Mishra (2015) proposed seventeen means OSG objectives (table 1). In the data analysis stage, data triangulation from interviews, manuals, policies, and audit guidelines, these objectives were clustered together based on the emergent themes and underlying meaning represented. Four organizational security governance dimensions were identified, and a discussion about each is presented below.
Insert table 1 here

Structural Dimension

The first underlying dimension identified in the thematic analysis is the Structural dimension. In this dimension, the scope of the objective is top management in the organization, and the target is the entire organization. The objectives that are grouped under this dimension are: *Establish formal control assessment functionality, Encourage management commitment, Resource allocation, Ensure visible executive leadership, and Data criticality.* All objectives in this group are meant for strategic long term changes in the organization, providing a directional path to the future. Such decisions are under the purview of top management and measure instituted; as a result, are for an entire organization to follow.

Formal controls assessment functionality allows establishing security governance as a functional requirement. Security has always been considered a nonfunctional requirement. Also, a distinctive feature of security requirements is that they are asset-driven – their goal is to protect the set of identified assets (Savola, 2013). Having a centralized entity for controls assessment would allow separate budget allocation for security governance functions and help in establishing a business case for security governance. A controls department would integrate controls into the business processes.

Management needs to actively participate in security governance initiatives by rewarding conformity with controls and encouraging values such as dedication, determination, open-mindedness, and truth. If management communicates effective governance as "top priority," the controls instituted are considered seriously by the employees. Management at CCIT participates actively in ensuring that precise controls are developed and implemented in the organization. The input from upper management is crucial for the success of the controls. The CIO of CCIT gets involved in the development process of the controls and the policies at every stage and demands a weekly progress report.

Resources are the lifeline of the security governance program. Before developing the precise controls and implementation plan, organizations need to take initiatives to build the right environment for controls. Some of the proactive control initiatives that this research suggests are getting adequate resources for developing physical controls, encouraging coordination between departments, and discouraging an environment of fear and politics in the organization.

An effective information security governance program requires visible leadership to provide the direction to controls management in the organization. This objective entails a leadership style and philosophy that gives momentum to the controls program (Mishra, 2020). The perception about security governance is created by the leaders who should be able to "walk the talk." This objective suggests that the leadership in that organization should present exemplary behavior and be able to nurture relationships with cohorts.

Data criticality entails assessment and classification of data according to sensitivity level and identification of data owners. Maintaining the confidentiality, integrity, and availability of the data is not only required for securing business processes but also needed for regulatory compliance purposes. Since CCIT forms and supports the backbone of the IT infrastructure for the City, it is imperative that the organization ensures the protection of critical data and make it available to all.

The management at CCIT feels that developing controls for proper access to data requires adequate segregation of duties. To summarize, all objectives in this dimension are essential, and the measures used have long term strategic implications for the organization and its OSG program.

Insert table 2 here

User Dimension

The User dimension emerged as the second dimension of OSG. The scope of this dimension is the individual user of controls, and the target is all controls instituted to implement the security plan. Objectives grouped under this dimension are: Achieving group cohesiveness, Alignment of individual and organizational values, Ethical and moral values established, Maximize trust building mechanisms. All objectives in this group are aimed at individuals who ultimately use the controls and ensure their success.

Enhancing group cohesiveness helps in regulating the group behavior about security controls. Peer pressure and groups' behavior influences and shapes the action of the individuals (Mishra, 2015). It is essential to encourage the ability to share the work and credit for the accolade, discourage favoritism and self-interest in groups and respect personal integrity in the group. Developing teams (Eloff and Eloff, 2005) is a vital, OSG objective. People derive part of their identity from workgroups (Hogg and Terry, 2000). The groups influence whether particular rules and controls would be followed or not. Thus encouraging cohesive groups with favorable security governance perceptions can help the organization's security program.

The management encourages groups to achieve goals. The groups' achievements could trickle down to the individuals. It was also evident from informal meetings and observations that the organization has an influential 'group' culture. Enhancing group cohesiveness would undoubtedly have an impact on the controls knowledge and behavior in this organization.

Security controls should be in alignment with the individual's beliefs and values such that the probability of success of the governance program increases. This alignment could be achieved in so many ways. Leach (2003) argues that in situations of conflict between individual and organization value systems, most people are unable to survive the tension for long. Even in the light of various legislations the agency had to follow, there were incidents of non-conformity with rules and regulations. An ethical organization would encourage the right work ethics and institute appropriate moral values in the employees to shape a favorable perception about security controls. Management should encourage people to take pride in their jobs and that the correct display of morality is rewarded and valued in the organization. Strong leadership helps in actually establishing the importance of ethics and morality in the organization (Mishra, 2020). At CCIT, the administration respects the personal integrity of people and rewards examples of ethical and moral behavior through a "star of the month" program. In this program, employees who have, in some way, set standards of proper ethical conduct, which can influence people, are acknowledged publicly by the management monthly, and the description of the action along with the winner's name is displayed in the meeting areas.

Building trust is critical to ensure that individuals can work according to the expectations of the management without close supervision. Trust is the enabling of confidence that something will or will not occur in a predictable or promised manner. The enabling of faith is supported by identification, authentication, accountability, authorization, and availability (Mishra and Dhillon, 2006). Employee beliefs about strong security governance in the organization are a good predictor of security success in the organization (Stanton and Stam, 2005). Outsider stakeholders should be able to trust the security measures in the organization to work with it and develop a positive perception about the reliability of the firm in the market. In summary, all actions taken by CCIT under these dimensions is to align individual users of controls with the organization's values about OSG objectives. Table 3 below presents the summary.

Insert table 3 here

Processual Dimension

The third dimension that emerged, Processual, represents processes orientation of organizational security governance. The scope of this dimension is every process that comes under control implementation purview, and all people linked to these processes are the target of the dimension. The objectives that are grouped in this dimension are Efficacy of Audit Processes, Clear controls development process, Monitor and Feedback, Standardization of controls, and clarity in business processes. All objectives in here have the focus and intent of developing, improving, and sustaining the process of security governance to better security practices.

Auditing acts as a catalyst for the management to accelerate its efforts for information systems security governance. This objective is useful, especially in the context of change management, to ensure the segregation of duties in the organization. Audit efficacy is required to assess management's adequacy with dealing with vulnerabilities. The role of auditing in improving the effectiveness of security controls is well understood and communicated at CCIT. The perceived purpose of auditing at CCIT is to assure the quality of controls that are in place and active. The management believes that auditing "gives them meaning for doing things." Even though the medium of business transactions have changed from paper format to electronic data, the traditional wisdom accrued from auditing and accounting standards is still valid.

The transparent control development process creates a positive perception of the controls and ensures transparency in control activities. This objective emphasizes the importance of systemization in the control development process and defines achievable goals. This objective encourages developing simple, flexible, timely, and easy to use controls. The transparent control development process helps in protecting critical business processes through multiple layers of controls as the requirements of such complicated controls are established for everyone.

The clarity in control development processes is emphasized at CCIT. The management encourages employees to clarify any doubts about the policies and welcomes questions about them. The administration has created a channel through which such requests are formally processed. The human resources department in this organization is responsible for enabling all the employees to get access to any resource that the employees might need to understand the policies better.

Monitoring controls require effective and established channels to incorporate feedback for further enhancements. Periodic review from external auditors strengthens the structure of the control and helps in analyzing the alignment between control objectives and overall business objectives. Monitoring controls and incorporating the feedback from employees is emphasized by all the prevalent governance models (ISACA, 2012). CCIT believes in robust monitoring and feedback channels for the success of information security governance. It has a monitoring program, for the most part, for all its processes and controls.

Standardization of the controls helps in benchmarking the governance activities, such as design and implementation of controls and investment in security governance activities, against other players in the industry Standardization provides opportunities for learning from others and avenues for growth. It also helps an organization gain acceptance internationally in the eyes of regulatory authorities or third party vendors.

The controls developed at CCIT need to be specific to the organization. The standardization process also helps in meeting the compliance criteria and is seen positively by the external auditors.

Establishing clarity in business processes is essential to maintain business integrity. This objective emphasizes the role of an adequate understanding of the workflow. Unless the interrelationships of the business activities and the flow of information are established, it is challenging to integrate appropriate security controls seamlessly and protect the business. Many businesses suffer vulnerability because of the lack of a deep understanding of the business processes resulting in inappropriate controls being implemented.

At CCIT, the management believes that controls should be integrated into the business processes. For governance purposes, it is crucial to understand the dynamics of business processes within the system for good security (Savola, 2007). It is essential to recognize the linkages of information security with business processes and have abilities to create and distribute new knowledge horizontally and vertically in the organization by using regular business interactions (Savola, 2007).

INSERT table 4 here

Facilitation dimension

The final dimension proposed in the study is Facilitation. The scope of this dimension is all the other three dimensions, and the target is all employees, management, and processes. The central role of these dimensions is to facilitate the interaction of three dimensions with one another. The OSG objectives grouped under this dimension are: *Communication about Controls, Training, and education about controls and Ensure punitive structures.* All measures taken under these objectives are to ensure that management, user, and processes interact as intended and aligned with the overall aim of securing informational assets.

Communication about controls is vital to articulate the vision of the management about security and establish a constructive debate about the usefulness of such activities. The management at CCIT is serious about communication with the employees regarding controls. The CIO has an informal meeting every second Friday with the employees where the pertinent issues about security and controls are discussed, employee feedback is taken, and agreement on the future course of development is reached. The emphasis on developing communication channels help employees to identify with the organization and the work that they do in groups.

Education about the need for controls creates awareness in the organization about risks, responsibilities, and social engineering issues. Training employees about usage and scope of controls help the end-users in understanding the impact of controls on day-to-day work and also reminds people to apply their knowledge in practice. Training should be enforced, and the effect of such measures should be assessed periodically. Regular training programs should be designed early on in the security governance strategy.

Training and education are much emphasized in CCIT, in theory, and practice. The upper management in the organization schedules regular training of the employees on various issues, including security awareness and controls.
Training the employees on the use of various applications for business processes and other related technologies ensures a better understanding of the expectations of the employees.

The training and education emphasis at CCIT has helped create awareness about security controls and governance. There is evidence in the research literature to support CCIT's efforts on training and education. The management utilizes resources for the knowledge of its employees about security control issues, which in turn prevents the unintentional breaches of security. Training could communicate higher-level concepts such as security action cycles but also detailed information about specific vulnerabilities (Yaokumah, 2014).

Punitive structures require the management to establish clear consequences for non-compliance with policies and ensure disciplinary action against unacceptable behavior. The impact of deterrence activities, according to our data, is significant for impeding non-compliance with controls and procedures. Developing countermeasures helps in conformity with rules and regulations. Information systems security research has established the importance of deterrence criteria for better security (Dhillon and Torkzadeh, 2006; Straub, 1998).

A punitive structure continually reminds the employees about the consequences of their actions. A combined proactive and preventive approach to security prevents users from IS misuse (Darcy and Hovav, 2007). Repeated efforts are required to instill the results of non-conformity with polices into the minds of the employees. The top management also feels that one of the biggest drivers for establishing deterrence in not adhering to the controls in the organization is frequent auditing. The management believes that the process of auditing implies that "you are being watched" and "you will get caught" if you are deviating from the accepted behavior.

Insert table 5 here

4. DISCUSSIONS AND CONCLUSIONS

This study presents four dimensions of OSG objectives based on the scope and targets these objectives in an organization. These dimensions are well supported by research literature (table 6) and overall provide end-to-end coverage of security initiatives in an organization. The first three dimensions present a holistic picture of an organization and every possible security activity that could be performed to negate threats. The last dimension, Facilitation, enhances the interaction of these dimensions with each other. For example, training and education enable end-users to understand and comply with policies in a better way. The clear punitive structure ensures that users follow procedures at all times. The proposed dimensions of OSG are essential in undertaking holistic, comprehensive, and strategic security planning for controls.

Insert table 6 here

This research makes a unique contribution to the security governance field. This study empirically validates the OSG objectives that are developed are grounded in the values of the organizational stakeholders (Mishra, 2015). OSG objectives, such as *ensure clarity in controls development processes, ensure corporate control strategy, ensure punitive structures, ensure formal control assessment functionality, and maximize group cohesiveness*, are relatively unused in the research literature in this area. This case study examines and supports the importance of such objectives and calls for better use of these constructs in real settings. This study contributes to practice significantly by establishing that these objectives are ready to be used and can improve an organization's comprehensive security plan and elevate their security posture. The dimensions of OSG proposed in this study allows management to focus on specific areas relevant to their environment. This study should fuel further inquiry in this area. Further studies in this area could look at correlations of these objectives and their statistical significance.

Organizational security governance objectives provide the basis for strategic planning of security initiatives in an organization. The security controls, derived from OSG objectives, ensure that the corporate vision is reflected in and aligned with the security activities designed for day-to-day business operations. The means objectives developed by Mishra (2015) were reviewed to validate the objectives empirically. The results show that the objectives proposed in a prior study provided new insights into OSG practices in a real organization. The organization is using all OSG objectives, and the management acknowledged the usefulness of such objectives for comprehensive security in the organizations.

5. REFERENCES

Abu-Musa, A, (2010) "Information security governance in Saudi organizations: an empirical study," Information Management & Computer Security, Vol. 18 Issue: 4, pp.226-276, https://doi.org/10.1108/09685221011079180

Alotaibi, M., Furnell, S. and Clarke, N. (2019) "A framework for reporting and dealing with end-user security policy compliance," Information & Computer Security, Vol. 27 Issue: 1, pp.2-25, https://doi.org/10.1108/ICS-12-2017-0097

Brotby, W. (2009).Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement, Taylor & Francis Group, FL

D'Arcy, J. Hovav, A. and Galletta, D. (2009) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research, Vol. 20, No. 1, March 2009, pp. 79–98

Dhillon, G., and Torkzadeh, G. "Value-focused Assessment of information systems security in organizations," Information Systems Journal (16:3) 2006, pp 293-314.

Eloff, J., and Eloff, M. "Integrated Information Security Architecture " Computer Fraud and Security (11) 2005, pp 10-16

Hogg, M. and Terry, D. (2000), Social Identity and Self-Categorization Processes in Organizational Contexts, The Academy of Management Review, Vol. 25, No. 1 (Jan. 2000), pp. 121-140

Huberman, A., and Miles, M. (1994). Data Management and Analysis Methods, in Handbook of Qualitative Research, N. Denzin, and Y. Lincoln (eds.), Sage, Thousand Oaks, CA, 1994, pp. 429-444.

ISACA. (2012). "CISA Review Manual," Information Systems Audit and Control Association, Rolling Meadows, IL, 2012

ISACA 2012. COBIT 5: Enabling Processes.

Kaplan, B. & Maxwell, J.A., 1994, Qualitative research methods for evaluating computer information systems, in Evaluating Health Care Information Systems: Methods and Applications, J.G. Anderson, C.E. Aydin, and S.J.Jay (eds), CA: Sage, p.45-68

Leach, J. "Improving User Security Behavior," Computers & Security (22:8) 2003, pp 685-692.

Mishra, S. (2015) "Organizational objectives for information security governance: a value focused assessment," Information & Computer Security, Vol. 23 Issue: 2, pp.122-144, https://doi.org/10.1108/ICS-02-2014-0016

Mishra, S. and Dhillon G (2006), “Information Systems Security Governance Research: A Behavioral Perspective,” 9th Annual NYS Cyber Security Conference and Annual Symposium on Information Assurance, June 14-15 Albany, NY

Mishra, S**.** (2020). Examining Organizational Security Governance (OSG) Objectives: How strategic planning for Security is undertaken at ABC Corporation? Journal of Information Systems Applied Research, Volume 13, Issue 2, July 2020

Nicho, M. (2018) "A process model for implementing information systems security governance," Information & Computer Security, Vol. 26 Issue: 1, pp.10-38, https://doi.org/10.1108/ICS-07-2016-0061

Orlikowski, W. "Integrated Information Environment or Matrix of Control? The Contradictory Implications of Information Technology," Accounting, Management and Information Technologies (1:1) 1991, pp 9-42.

Savola, R. M. (2007). Towards a Taxonomy for Information Security Metrics, International Conference on Software Engineering Advances (ICSEA 2007), Cap Esterel, France

Savola, R. M. (2013). Quality of security metrics and measurements. Computers & Security, 37:78–90.

Stanton, J., and Stam, K. (2005). "Analysis of end user security behaviors," Computers & Security (24) 2005, pp 124-133.

Straub, D. (1998). "Coping with systems risk: security planning models for management decision making.," MIS Quarterly (22:8) 1998, pp 441-465.

Tan, T., Maynard, S., Ahmad, A. and Ruighaver, T. (2017) "Information Security Governance: A Case Study of the Strategic Context of Information Security" (2017). PACIS 2017 Proceedings. 43. http://aisel.aisnet.org/pacis2017/43

Tickle, I. (2006). "Data integrity assurance in a layered security strategy" Computer Fraud & Security), pp 9-13.

Walsham, G. (2006) "Doing Interpretive Research," European Journal of Information Systems (15:3) 2006, pp 320-3.30.

Yaokumah, W. (2014) "Information security governance implementation within Ghanaian industry sectors: An empirical study," Information Management & Computer Security, Vol. 22 Issue: 3, pp.235-250, https://doi.org/10.1108/IMCS-06-2013-0044

Appendices and Annexures

	Objectives	Key Lessons
M1	Ensure the Efficacy of Audit Processes	Have frequent internal and external audits Treat auditors as consultants to assess management's adequacy
M2	Maximize Clarity in Business Processes	Efficiently designed mature business processes are better protected Provide an end-to-end view of the business process and manage changes
M3	Ensure Communication about Controls	Have frequent debates about controls Develop communications policy for constructive communication within and outside functional groups
M4	Ensure Alignment of Individual and Organizational Values	Promote values such as respect for others, privacy, integrity, self-pride in job and honesty Involve users in the development process to understand an individual's attitudes and beliefs about security
M5	Ensure Data Criticality	Assess and classify data according to sensitivity Identify data owners to assign responsibilities according to information criticality Link data with authorizations for secure and reliable IT infrastructure
M6	Ensure Punitive Structures	Establish clear consequences and disciplinary actions against non-compliance with policies Explain the meanings of criminal acts and respond effectively in cases on non-compliance
M7	Ensure Clarity in Control Development Process	Develop a favorable perception and transparency of the controls Develop simple, flexible, timely and easy to use controls
M8	Ensure Formal Control Assessment Functionality	Develop formal entity for control assessment Differentiate between lines of business and industries before applying popular OSG frameworks Stakeholder's viewpoints need to be reflected in the governance process Perform periodic cost-benefit analysis and IT architecture review for the correctness of design for the security controls
M9	Maximize Monitoring and Feedback Channels	Helps in achieving the performance standards set for the IT processes Assures "what is being claimed" is accomplished Incorporate the feedback into the controls
M10	Ensure Visible Executive Leadership	Fundamentally helps in improving the perception of security governance Lead by example and nurture the relationships with employees executive
M11	Maximize Group Cohesiveness	Group behavior influences and shapes individual' perception of security controls Discourage favoritism and self-interest in groups and manage peer pressure
M12	Maximize Management Commitment	The reward for conformity with controls and encourage values such as dedication, determination, open-mindedness, and truthfulness Establish adequate controls as a "top priority."
M13	Maximize Resource Allocation for controls	Groundwork before developing controls requires coordination of multidisciplinary functions Allocate appropriate resources in a politics-free environment
M14	Encourage Standardization of Controls	Create systemization in the control development process and assess against mechanisms employed by others Benchmark security investments and governance practices to learn from others
M15	Maximize Training and Education	Awareness about social engineering issues can be provided with work-related examples

		Apply the knowledge in daily practice with focused training and education
M16	Ensure ethical and moral values	Propagate right ethical environment Leadership establishes the right tone of ethics in organizations
M17	Maximize trust building mechanisms	Develop a conducive environment for controls deployment Enhance trust with partners within and outside the organization

Table 1: Means Objectives for Organizational Security Governance (OSG) in organizations as proposed by Mishra (2015).

OSG Objectives	Evidence from CCIT	Measures at CCIT
Formal control assessment functionality	"The biggest problem is that controls have limited resources. We want to do so many things but can't do it. Like it [controls] needs to be constantly modified and monitored, but that [modification and monitoring] needs investment. Do we have separate money for this as a department? We are always in a cash crunch."	Cost-benefit analysis for controls Ensure resources Developing a formal entity for centralized controls management
Encourage Management commitment	"Taking inputs from people is important, managers and directors. Decide how they want a particular environment, the money, and resources to be used, and the controls. Employees want more flexibility but don't know what they want. Employees are always asking- why do we need to do this when you incorporate their inputs. A better approach would be to stick to the top and find out what the management wants and work with your given constraints. Find out what it is that you can do with these resources."	Management seeks inputs from people Management ensures that a refined version of the policies and control is presented to the higher management as City level CIO is supportive and gets an updated every week
Resource Allocation	"We have tools you can buy and put them in place to protect that [data]. We don't currently have those; it's a great job to get those tools, to get the funding for that, to get the people for that."	Management ensures resources for the new development of policies and controls Enhance trust measures to encourage "demand for resources" being considered Seek more resources to get the controls working
Visible Executive Leadership	"With the City, it's not hard to get the support of the CIO. He is supportive of our actions. The hard part is getting to his colleagues, the other directors, who need to approve it but have no clue about it."	CIO is supportive of the new security policies and controls Management into confidence the leadership at the city level
Data criticality	"We do have data that is so crucial. We may have health data; we may have social security numbers and the names and dates and all of those things. Also, employee details that we need to keep private as well. We interact with other state agencies, and there is other information. We have access to DMV, which means details of basically anybody owns a car, so a lot of data. We must ensure that data doesn't go anywhere where it shouldn't be, so from that point, this is what we are going for. All of the IT security controls are all about the data."	Ensures confidentiality, integrity, and availability of data to all Provides a technically superior state of the art service center with 24/7 hotline and helpdesk services. Segregation of duties Stringent access control policies & authorization mechanisms Strict password policies

Table 2: Structural dimension of OSG

OSG Objectives	Evidence from CCIT	Measures at CCIT
Efficacy of Audit Processes	"I think that if I took over if I became the CIO, I would be looking at every one of my team members, and I would tell them to prepare for an audit. I would bring an auditor here, and each one of my team will get audited. That would give me a baseline as a new boss to work on; I can only improve. If it got any worse, my job should be gone, that's what I would do. Management should be responsible for what's going on. Economy improves if the government works."	Management believes in frequent audits Use audit as a deterrence tool Used to provide quality assurance "Audit on-demand" encouraged
The clear controls development process	"Creating the policy and the procedure needs to be clear because if nobody knows about the controls and procedures or understands it, they are not going to follow it."	Encourages employees to clarify doubts Make all resources about controls accessible Simple and easy to use controls
Monitor and Feedback	"The system in which I am right now, I am in a place where I can find out what they have done whatever needs to be done, seeing the audit trail. If they haven't done their work, we find that pretty quickly."	Monitoring tools are used Sessions for obtaining feedbacks Feasibility analysis of the controls through monitoring
Standardization of controls	"I guess one of the other very important things and a lot of people don't do this, establish acceptance criteria. That means that you are going to determine what the controls will do and how everyone has to act, for it to work, and then to ensure that it does act. It has to be consistent."	Consistent controls Refer to the industry frameworks Required for the third party vendors
The clarity in business processes	"I think they [controls] should be designed to help to ensure that your data and processes are sound, that your money is accounted for, and your resources are applied correctly. Also, your performances and expectations are met as an agency. It should improve the business process."	Control the software purchasing system Controls build along the business process Controls are essential for business success

Table 3: Processual dimension of OSG

OSG Objectives	Evidence from CCIT	Measures at CCIT
Achieving group cohesiveness	"What can you say at the end of the day that you have contributed? Ideally, you want the employees to plan at the beginning of the day, what they can accomplish that day, what is the next thing that they can do to accomplish their goals, and then achieve something at the end of the day. Here is what I started to do, and here's what I did in the day, goals, and accomplish on a daily, weekly, and monthly basis in the way it's measurable. So control would be to motivate them as a group."	Set group targets Encourage group activities Track the people based on their groups Educate groups about controls
Alignment of individual and organizational values	"I mean, in reality, our values, our values should define that we are going to do the best we can, do the right thing at any point in time. If my values allow, then only I will follow the rules."	Use psychological measures to understand employees Have frequent lunches to "draw in" the employees Portray controls as something to protect the employees against harm. It's about them not the bosses
Ethical and moral values instituted	"so we can make a rule, we can make a law that you have, to be honest. I mean, in reality, our values, our values should define that we are going to do the best we can, do the right thing at any point in time. If my values allow, then only I will follow the rules. My personal belief is that you can't legislate that; you can't provide enough legislation to do that."	"star of the month" program Leadership is encouraged to "walk the talk." Management provides the right environment
Maximize Trust building mechanisms	"I am talking about the whole City. They [other agencies under the City] have to trust IT to develop these policies and controls. We have the best interest in doing so. It is good for compliance as well with any federal state and local law".	Equipment lying openly in the office as there is mutual trust about not stealing City's property Managers maintain consistency in "saying and doing."

Table 4: User dimension of OSG

OSG Objective	Evidence from CCIT	Measures at CCIT
Communication about Controls	"Typically, in our case, we would draft a policy, edit it, and go to the City. Managers and other directors from other agencies need to work on this, but there is no communication among them. So there is no feedback. If there is the thing that you don't agree with, tell us, we need to get there input. They need to be treated. Differently, they are different departments".	The manager meets with employees every second Friday Communicate with people even when they communicate back Prevention is better than creating vulnerability hence express to protect the people
Training and education about controls	"Human nature it is that they [employees] may read the policy and go "ok I do know that" but they wouldn't read in the details. There is an education factor also, to get the word out to people. When you sign these forms, this is what it meant, and you are held responsible. Part of the procedure and guideline will keep, make it standard this is what happens when you don't do this, first warning, second warning, third warning. I believe that our HR is working on some of that now."	Extensive training about applications and business processes Explain with work-related examples Encourage the use of knowledge in practice Provides incentives for education (gift cards)
Ensure punitive structures	"I also think what you have to do is to have a clear punitive structure because big things are at stake. A punitive structure is a must. So you must have some type of thing that says even if the employee violates this, what is going to happen to him."	Explain consequences and send reminders Clear punitive structure Punish in case of security breach or non-conformity with controls

Table 5: Facilitation dimension of OSG

Dimension	Scope and Target	OSG Objectives	Literature support
Structural (5)	Top management/ Corporate-wide	Formal control assessment functionality Encourage Management commitment Resource Allocation Visible Executive Leadership Data criticality	Tickle, 2006; Myler and Broadbent, 2006; Savola, 2007; Yaokumah, 2014; Alotaibi, M., Furnell, S. and Clarke, N., 2019
User (4)	employee/ Individual-level	Achieving group cohesiveness Alignment of individual and organizational values Ethical and moral values instituted trust-building mechanisms	Mishra, 2015, Mishra and Dhillon, 2006; Nicho, 2018
Processual (5)	Security processes/ Anyone part of that process	Efficacy of Audit Processes The clear controls development process Monitor and Feedback Standardization of controls The clarity in business processes	Goel et al., 2006; Mishra, 2015; Tan et al., 2017; Mishra, 2015
Facilitator (3)	Management/individual/ Processual/ Multiple levels	Communication about Controls Training and education about controls Ensure punitive structures	Darcy et al., 2009; Dhillon and Torkzadeh, 2006; Fuller et al., 2007; Abu- Musa, 2010

Table 6: The four dimensions of OSG

Defense and Analysis of Hijacking User Login Credentials via Remote Code Execution and Raspberry PI

Patel Nishitkumar
Np05573@georgiasouthern.edu

Hayden Wimmer
Hayden.wimmer@gmail.com

Georgia Southern University
Statesboro, GA

Loreen Powell
lpowell@bloomu.edu
Bloomsburg University
Bloomsburg, PA

Abstract

Cyber-security is a rapidly growing concern for all organizations. Ransomware and Botnets are becoming pervasive across the internet. Management needs to understand how systems are compromised by attackers who implant payloads as ransomware and botnets. One such concern is physical access to machines by bad actors in the organization or mobile workstations working at offsite locations. Gaining physical access a bad actor can implant malware in the form of ransomware or a botnet which becomes an initial point of entry for assuming control over an organizations network. In this example, we illustrate the dangers of physical access and use a USB device to implant a payload via remote code execution. The remote code installs an application developed to mimic a Windows 10 login screen and populates the login screen with the username of the currently logged in user. Once the user logs in to this fake screen, the application logs the user’s credentials, namely the username and plain text password, via an HTTP post to a remote command and control server. Following our demonstration, we discuss implications and countermeasures to aid management in improving security of the organization.

Keywords: Cyber-security, Raspberry Pi, Payloads

1. INTRODUCTION

As technology continues to advance, malicious information technology (IT) attacks also become more complex focusing on rich data (Christensen & Dannberg, 2019). Kavitha and Kavitha (2016), report that there were 360 million malware variants were released into the wild in 2016. The Universal Serial Bus (USB) is commonly recognized as a vector for malicious attacks. Thus, when a USB is maliciously used, it can deliver malware, steal critical data, and cause other malicious attacks which pose significant threats to computers and network systems (Muller, Zimmer & de Nittis, 2019). Today, USB attacks that target IT infrastructures are gaining popularity (Neugschwandtner et al., 2016).

One of typical security threat attributed to computer and network infrastructure includes the hijacking of user login credentials in Raspberry Pi systems (Chandreshekar et al., 2017). A recent literature work by Martin, Kargaard, and Sutherland (2019) analyzed this issue and offer some significant perspectives regarding the development of Internet of Things (IoT) and its contributions in the hacking of login credential of such devices as Raspberry Pi systems. However, nobody has examined and documented the step-by-step process involved in such hackings. Emani, Glantz, Gamrat, and Hills (2019) explain that universities are beginning to explore and incorporate Raspberry Pi security learning projects into their IT courses and curriculum. They note that there is value to providing students with this type of hands-on experience.

The goal of this research is to document a novel process of how a successful remote code execution is carried out using Raspberry Pi Zero and a USB executable file. This study expands upon the implications of perspectives addressed in the literature by providing a better understanding about the vulnerabilities in preventing the hackings occurring with the Raspberry Pi. This work has practical implications for IT professional interested in gaining a comprehensive understanding of the attributes and process. As a result, this research will help IT professionals strengthen their systems and prevent malicious attacks attributed to computer systems and networks. Additionally, this work may serve as an applied resource for IT programs and faculty wishing to explore ongoing research to detect threats in Raspberry Pi devices. This research could be replicated at other institutions. The remainder of this paper is structured as follows: background/ literature review, methodology, results, and conclusion.

2. LITERATURE REVIEW

The mechanics used to hack Raspberry Pi remotely for the login credential payload require knowledge about innovations, security processes, protocols, and equipment that aid hackers to gain access into the systems. The main themes to consider in this regard include IoT, vulnerabilities of Raspberry Pi, and defense perspectives on how to prevent such hackings.

A. Internet of Things (IoT)

IoT is a major standpoint attributed to the growth of hijacking Raspberry Pi logins remotely. Martin, Kargaard and Sutherland (2018) implicated IoT as an essential factor towards the growth of login hijacking intrusions. Based on their perspectives, the manufacture and use of IoT over the past years has grown significantly vast. This development as a result, has led to an increase in the number of innovations in the field, both positive and negative. Ray (2018), analyzed similar perspectives, but with regard to the integrative innovations encompassing IoT. A common perspective shared by these literatures is the necessity of IoT devices in modern settings, which as a result, pose great security challenges. Accordingly, he argued that IoT implicate such attributes as economic benefits and efficiency, which renders their use across organization settings inevitable. Similarly, Martin et al. (2019) predicted that the value of the IoT would reach 7.1 trillion by the year 2020. Thus, it is evident that intrusion problem are likely to increase in the future.

With the number of IoT devices increasing and playing a more integrated role in our everyday lives, it is believed to have a played a significant role in the healthcare industry. Kaur and Jasuja (2017) proposed a system that would monitor pulse rate, body temperature of the person with sensors alongside with raspberry pi and IoT.

B. Vulnerabilities of the Raspberry Pi

A recent study by Al Saaidi et al. (2018) analyzed the functionality of the OpenSHH and security protocols that users can employ in securing the service of their Raspberry Pi. Specifically, they analyzed the functionality of the Debian v7.1 p2 systems, which they claimed is subject to vulnerabilities when installed in a Raspberry Pi 2. Their research established that SSH protocol exchange keys are points of weaknesses, especially when they allow multiple CRLF injections in the device. Because of this aspect of vulnerability, remote authenticated users can bypass the shell commands to extract significant payloads on command.

Neugschwandtner, Beitler and Kurmus (2018) analyzed the vulnerability in Raspberry Pi elaborating on the system's weaknesses from USB attack vectors. Particularly, they noted that USB attacks passively eavesdrop on communications by intercepting host devices without necessarily having a physical connection between the host and victim device. This intrusion aspect is crucial, as it constitutes the precise process of bypassing the Raspberry Pi protocols to access the login credentials of the victim device. They expressed concern that such intrusions are becoming more complex with the advancement of USB sticks.

Nissim, Yahalom and Elovici (2018) also explored USB-based intrusions. They noted that USB peripherals are vulnerable because they carry embedded malicious payloads deemed essential by hackers to launch attacks on victim devices. Because of such vulnerabilities, the setup of the P4wnP1 utilizes the USB functionalities to execute the necessary protocols in hijacking the login credentials of a Raspberry Pi.

Equally relevant perspectives regard vulnerabilities of Raspberry Pi login hackings concerns ineffective security protocols. In particular, some device users use similar passwords and usernames in multiple accounts, which undermines the security of information stored within the devices. Recently, Ahmed et al. (2019) analyzed this security issue with regard to threats attributed to physical security. In their analysis, they suggested the relevance of incorporating multiple security level in ensuring data security. More so, they advocated that device users should utilize five levels of security that include among other, entering passwords on interactive GUI, facial recognitions, and speech pattern recognitions. Sharing similar perspective Radzi et al. (2020) suggested the essentiality of using safe password systems as facial recognitions in Raspberry Pi systems. In their evaluation, the authors warned that users who disregard effective password security protocols stand the chance of consistent network intrusion that might compromise the entire system the Raspberry is attached. Based on these perspectives, users should ensure that they use the most effective and reliable password protocols to safeguard their systems from intrusions and login hackings.

C. Defenses Against Raspberry Pi Vulnerability Points

Across most IT research analyzing the process of Raspberry Pi hackings, authors provide perspectives regarding how the device users may address intrusions. According to Martin et al. (2018), one of the best solutions is to use Internet honeypots. Accordingly, the mechanisms are necessary because of their capacity to identify IoT-related malware. Furthermore, they recommend using honeypot mechanism that uses a Cowrie framework or a fully interactive secure shell. They argue that this process has been successful in curbing the Mirai attack that targeted IoT devices and routers as slaves. Echoing these sentiments, Tripathi and Kumar (2018) analyzed how honeypot mechanisms can be incorporated in Raspberry Pi among other devices as essential defense mechanisms. In their argument, however, they noted the relevance of maintaining data integrity and incorruptibility within the system.

Alsaadi et al. (2018), in their solution segment, also offered relevant perspectives concerning the defenses against Raspberry-based intrusions. More so, among the various solutions proposed was addressing the Raspberry Pi remote access. According to the authors, the employment of PuTTY, which is a free license Windows SSH client server, can offer the best security solution. Similarly, O'Leary (2019) analyzed the employment of PuTTY noted that this tool allow for the creation of secure remote sessions when users intend to access the Raspberry Pi hardware over a network. Furthermore, he argued, with the mechanic's cryptography, the system benefits from an added protection layer against eavesdropping or hijacking attacks.

Another study by Yevdokymenko, Mohamed and Onwuakba (2017) examined the relevance of ethical hacking as a way of preventing system breaches through uncovered network areas. Specifically, they argued that through a successful penetration testing and information gathering, system users could put in place the correct patches as a way to reinforce their network defense.

Finally, Balooch (2017) shared similar perspectives purporting that ethical hacking is critical because it assumes hackers' point of view in determining the security protocols to put in place when preventing such breaches as the hijacking of login credentials.

3. METHODOLOGY

The goal of this study is to document the step-by-step process of how a successful remote code execution is carried out using Raspberry Pi Zero and a USB executable file. This study expands upon the implications of perspectives addressed in the literature by providing a documented understanding about the vulnerabilities in preventing the hackings occurring with the Raspberry Pi. Raspberry Pi is a low-cost, credit card-sized computer that connects to a computer monitor or TV using HDMI, and uses a standard keyboard and mouse. It can run a host of operating systems, such as Raspbian (Debian Linux), Android, Windows 10, IoT Core, etc.

In this section, we briefly explain how to set up a Raspberry Pi, installing P4wnP1 and remote connection to device. We demonstrated step-by-step how a successful remote code execution is being carried out using Raspberry Pi Zero and USB executable file. Raspberry Pi is a low-cost basic computer that plugs into a computer and runs on Linux. We developed our own version of P4wnP1 and use it to demonstrate how we can hijack user login credentials using remote code execution. An outline of the network is referred to in Fig. 1. For the setup, we used a Samsung Laptop (Attacker), Lenovo PC (Victim PC), 8GB USB, and raspberry pi zero.

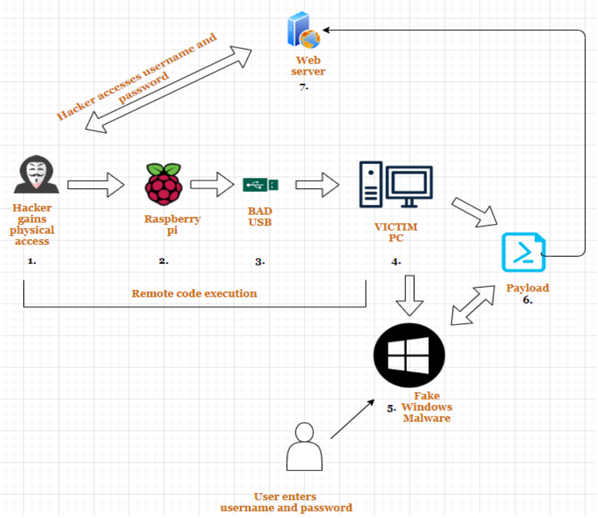


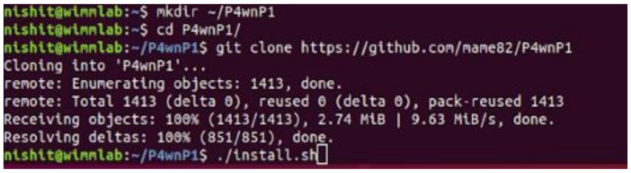
Figure 1: Configuration of the Network

A. Setting up Raspberry Pi

In order to get our raspberry pi setup as a USB device we needed: A long USB cable with power adaptor, Micro SD card, Power cable and Internet. We downloaded the latest version of Raspbian Stretch Lite to write the image onto a Micro SD card. We used angry IP scanner to find the IP address of the pi (172.24.0.1). Once we logged into the pi, we installed git and downloaded a clone of P4wnP1. P4wnP1 is a toolset that turns our pi into a WI-FI hotspot.

B. Installation and Testing the Connection

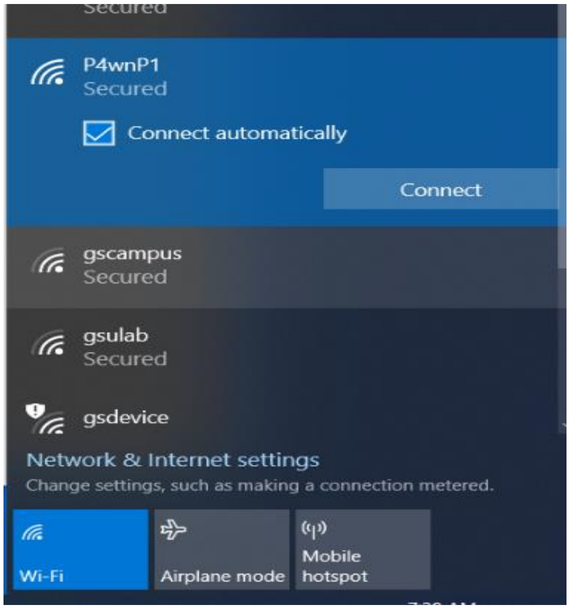
Figure 2 shows the code that we used to clone P4wnP1 from GitHub. After the install was completed, we then plugged the Raspberry Pi into the attacker machine and we were able to detect the Wi-Fi hotspot on the victim PC shown as “P4wnP1”



```
nishit@wimmlab:~$ mkdir ~/P4wnP1
nishit@wimmlab:~$ cd P4wnP1/
nishit@wimmlab:~/P4wnP1$ git clone https://github.com/mame82/P4wnP1
Cloning into 'P4wnP1'...
remote: Enumerating objects: 1413, done.
remote: Total 1413 (delta 0), reused 0 (delta 0), pack-reused 1413
Receiving objects: 100% (1413/1413), 2.74 MiB | 9.63 MiB/s, done.
Resolving deltas: 100% (851/851), done.
nishit@wimmlab:~/P4wnP1$ ./install.sh
```

Figure 2. Installation of P4wnP1

Figure 3 shows successful connection to PwnP1 Wi-Fi Hotspot. We connected to the Wi-Fi hotspot using the attacker machine. This allowed us to have connectivity to the raspberry pi so we could remotely login using PUTTY and execute commands.



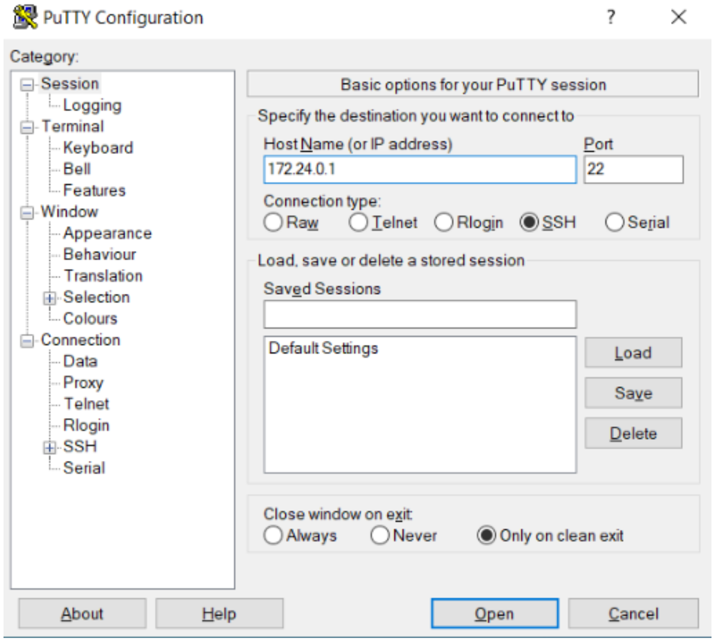
Change settings, such as making a connection metered.

☑ Connect automatically

Figure 3. Successful installation of P4wnP1

C. Raspberry Pi Remote Access

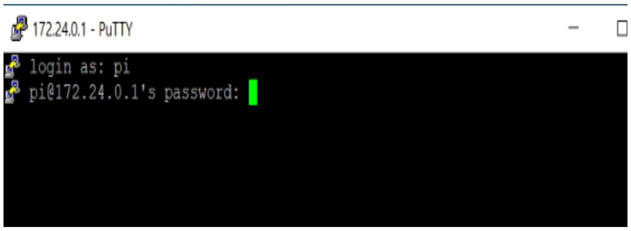
We used PuTTY, a free open-source terminal licensed Windows SSH client server. It allows users to create a secure remote session access to Raspberry pi hardware over a network connection.



Host Name (or IP address): 172.24.0.1
Port: 22
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 4. SSH connection to raspberry pi

SSH is a protocol for encrypted communications between computers that add protection against eavesdropping or hijacking attacks. We were successful in connecting the victim pc to the P4wnP1 network, we then SSH into the raspberry pi as shown in figure 4.



```
login as: pi
pi@172.24.0.1's password:
```

Figure 5. Successful Connection to the Pi

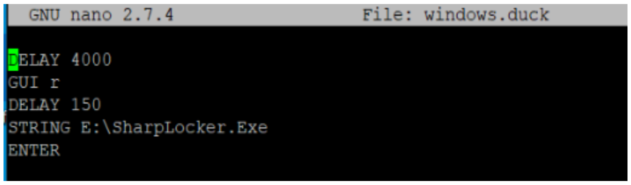
Figure 5 shows successful connection to the raspberry pi from the attacker pc. We were able to gain full access to the device. This will allow us to execute payload to the victim pc.

D. USB Loaded with exe File

We created a .NET application (fake windows lock screen) written in C#, all output is dumped into a HTTP request web server. We executed the application to create an .exe file, which was uploaded to a USB. The USB was plugged into victim pc to create a backdoor and hijack user login credentials.

E. Remote Code Execution

In order to do a remote code execution we wrote a USB Rubber Ducky Script. Figure 6 shows a simple scripting language that allows penetration testers to deploy payloads that mimic human keyboard input. The script will point to the USB drive E:\filename (SharpLocker).exe file.



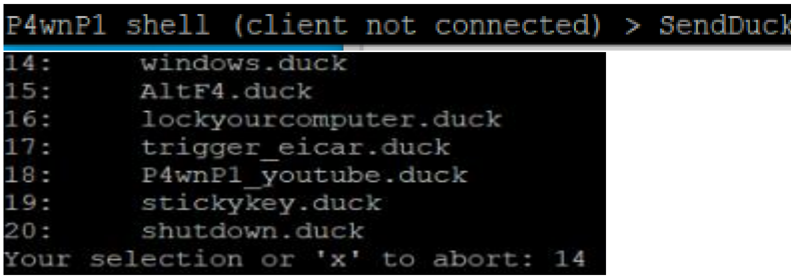
```
  GNU nano 2.7.4                    File: windows.duck

DELAY 4000
GUI r
DELAY 150
STRING E:\SharpLocker.Exe
ENTER
```

Figure 6. DuckyScript code

From the attacker pc, we executed SendDuckyScript injection to the victim pc, we chose option 14 (windows) as shown in Figure 7, this will execute a fake windows malware in victim pc and as soon as the victim enters the credentials we will hijack user login credentials on our web server.

Figure 8 shows a fake windows login screen pop up on the victim pc after the payload was executed. When the victim inputs the password, the password would be dumped into an external HTTP web server.



```
P4wnP1 shell (client not connected) > SendDuck
14:      windows.duck
15:      AltF4.duck
16:      lockyourcomputer.duck
17:      trigger_eicar.duck
18:      P4wnP1_youtube.duck
19:      stickykey.duck
20:      shutdown.duck
Your selection or 'x' to abort: 14
```

Figure 7. Choose option 14 to send to victim pc

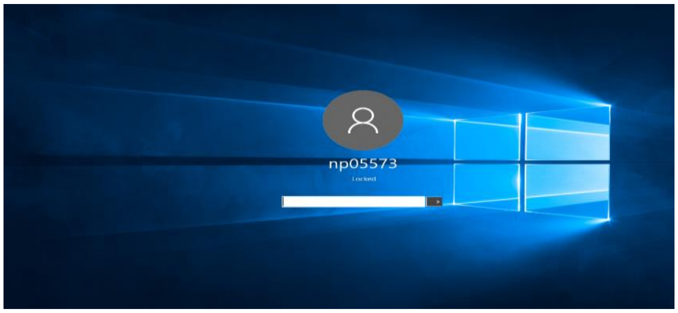
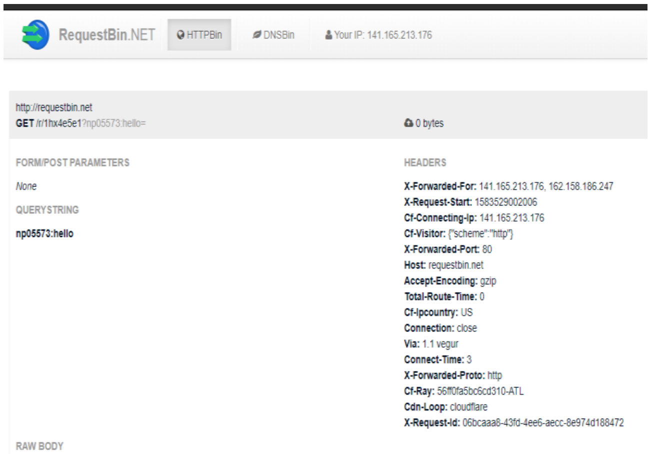


Figure 8. Fake Windows login screen on victim pc

4. RESULTS

The results as shown in Fig 9, we were able to successfully hijack user login credentials on our web server once the user entered the password. By incorporating the functionalities P4wnP1 network, it was possible to connect the protocols to victim system and to launch the execution controls. Nonetheless, the most essential attribute of this setup was its capacity to provide relevant information from the malicious attack targeting the system.



```
http://requestbin.net
GET /r/1hx4e5e1?np05573:hello=                    0 bytes

FORM/POST PARAMETERS                              HEADERS
None                                              X-Forwarded-For: 141.165.213.176, 162.158.186.247
QUERYSTRING                                       X-Request-Start: 1583529002006
np05573:hello                                     Cf-Connecting-Ip: 141.165.213.176
                                                  Cf-Visitor: {"scheme":"http"}
                                                  X-Forwarded-Port: 80
                                                  Host: requestbin.net
                                                  Accept-Encoding: gzip
                                                  Total-Route-Time: 0
                                                  Cf-Ipcountry: US
                                                  Connection: close
                                                  Via: 1.1 vegur
                                                  Connect-Time: 3
                                                  X-Forwarded-Proto: http
                                                  Cf-Ray: 56ff0fa5bc6cd310-ATL
                                                  Cdn-Loop: cloudflare
                                                  X-Request-Id: 06bcaaa8-43fd-4ee6-aecc-8e974d188472
RAW BODY
```

Fig 9. User login credentials hijacked

This attack opened a backdoor through which we were able to manipulate the whole system. Consequently, it was possible to create a fake windows lock screen through which the SendDuckScript was executed to eavesdrop on the credential input, which are consequently transferred as payloads to the USB infrastructure.

The countermeasures for mitigating Raspberry Pi hacking are in consideration with the strategies suggested in the Literature Review section. In brief, users can employ the honeypot mechanics that detect and prevent such intrusions. Second, the users can use such tools as PuTTY, which are client servers that offer security solutions. Last but not least, it is crucial to conduct ethical hacking, such as penetration testing, occasionally, which enable users to assume hackers' perspectives in order to secure their systems. Nonetheless, it is crucial to take precautionary measure that can prevent hackers from getting access and controlling network systems with sensitive information.

5. CONCLUSION

In summary, the remote hijacking of login credentials through Raspberry Pi are attributable to certain vulnerabilities within network systems. Through the input of such frameworks as P4wnP1 network, hackers can exploit network weaknesses by executing attacks through USB mechanics. Based on the step-by-step procedure, it is evident that such attacks, leading to compromised login credentials can be problematic. Nonetheless, by employing such measures as employment of PuTTY and honeypot mechanics, network users can secure their systems. More so, ethical hackings can be potent solutions against network hackings.

6. REFERENCES

Ahmed, S. U., Sabir, A., Ashraf, T., Ashraf, U., Sabir, S., & Qureshi, U. (2019, December). Security Lock with Effective Verification Traits. In *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)* (pp. 164-169). IEEE. DOI.101109/ICCIKE47802.2019.9004341

Alsaadi, H. H., Aldwairi, M., Al Taei, M., AlBuainain, M., & AlKubaisi, M. (2018, February). Penetration and security of OpenSSH remote secure shell service on Raspberry Pi 2. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-5). IEEE. DOI: 10.1109/NTMS.2018.8328710

Apple Inc., Hewlett-Packard Inc., Intel Corporation, Microsoft Corporation, Renesas Corporation, STMicroelectronics, & Texas Instruments (2019).Universal Serial Bus 4 (USB4™) Specification.https://www.usb.org/document-library/usb4tm-specification

Baloch, R. (2017). Ethical hacking and penetration testing guide. (2nd ed.) New York, NY: CRC Press.

Chandreshekar, K., Clearly, G., Cox, O., Lau, H., Nahorney, B., Gorman, B., Wueest, C. (2017, April). Internet threat security Report . *Symantec*, *22*.

Christensen, L., & Dannberg, D. (2019). Ethical hacking of IoT devices: OBD-II dongles. http://www.diva-portal.org/smash/get/diva2:1333813/FULLTEXT01.pdf

Denney,K., Erdin, E., Babun,L., Uluagac. A. S.(2019). POSTER: Dynamically Detecting USB Attacks in Hardware (Extended Abstract). InWiSec '19: ACM Conference on Security and Privacy in Wireless and MobileNetworks, May 15–17, 2019, Miami, FL, USA.ACM, New York, NY, USA,2 pages. https://doi.org/10.1145/3317549.3326315

Emani, R., Glantz,E. J., Gamrat, C. & Hills, M. K. (2019). Using the Raspberry Pi in IT Education. In *Proceedings of the 20th SIGITE conference on Information technology education (SIGITE'19)*. Tacoma, WA, USA, 1 page. https://doi.org/10.1145/3344254

Kavitha, G., & Kavitha, R. (2016). An analysis to improve throughput of high-power hubs in mobile ad hoc network.

Martin, E. D., Kargaard, J., & Sutherland, I. (2019, June). Raspberry pi malware: An analysis of cyberattacks towards IoT devices. In *2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 161-166). IEEE. DOI: 10.1109/DESSERT.2019.8770027

McDonald, G., Murchu, L. O., Doherty, S. & Chien, E. (2013).Stuxnet 0.5: The Missing

Link. https://docs.broadcom.com/doc/stuxnet-missing-link-13-en

Mueller, T., Zimmer, E., & de Nittis. L. (2019). Using Context and Provenance to defend against USB-borne attacks. In 2019 Proceedingsof the 14th International Conference on Availability, Reliability and Security (ARES 2019) (ARES '19), Canterbury, United Kingdom. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3339252.3339268

Neugschwandtner, M., Beitler, A., & Kurmus, A. (2016, April). A transparent defense against USB eavesdropping attacks. In *Proceedings of the 9th European Workshop on System Security* (pp. 1-6). DOI: 10.1145/2905760.2905765

Nissim, N., Yahalom, R., & Elovici, Y. (2017). USB-based attacks. *Computers & Security*, *70*, 675-688. DOI:10.1016/j.cose.2017.08.002

Nohl, K. & Lehl, J. (2014, August). BadUSB – On Accessories That TurnEvil. In Blackhat USA

O'Leary, M. (2019). Network Services. In Cyber Operations (pp. 649-720). Apress, Berkeley, CA. DOI:10.1007/978-1-4842-4294-0_13

Radzi, S. A., Alif, M. M. F., Athirah, Y. N., Jaafar, A. S., Norihan, A. H., & Saleha, M. S. (2020). IoT based facial recognition door access control home security system using raspberry pi. *International Journal of Power Electronics and Drive Systems*, *11*(1), 417. DOI:10.11591/ijpeds.v11.i1.pp417-424

Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University-Computer and Information Sciences,* 30(3), 291-319. DOI:10.1016/j.jksuci.2016.10.003

Tian, Bates & Buttler (2015). Defending Against Malicious USB Firmware with GoodUSB. *ACM ACSAC '15 Conference*, December 07-11, 2015, Los Angeles, CA, USA https://adambates.org/documents/Bates_Acsac15.pdf

Tripathi, S., & Kumar, R. (2018, December). Raspberry Pi as an intrusion detection system, a honeypot and a packet analyzer. In *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)* (pp. 80-85). IEEE. DOI: 10.1109/CTEMS.2018.8769135

Yevdokymenko, M., Mohamed, E., & Onwuakpa, P. (2017, October). Ethical hacking and penetration testing using raspberry PI. In *2017 4th International Scientific-Practical Conference Problems of Info communications. Science and Technology (PIC S&T)* (pp. 179-181). IEEE. DOI: 10.1109/INFOCOMMST.2017.8246375