Increasing SmartChair Data Integrity through Cybersecurity Analysis

by

Joseph Daniel Biagini & Logan Iver Johnson

An Honors Capstone

submitted in partial fulfillment of the requirements

for the Honors Diploma

to

The Honors College

of

The University of Alabama in Huntsville

April 24, 2019

Honors Capstone Director: Dr. Rhonda Gaede

Associate Professor, Electrical & Computer Engineering Department

Joseph Biagini 4/24/19
Student 1 Date

Logan Johnson 4/24/19
Student 2 Date

Rhonda Kay Gaede 4/24/19
Director Date

4/24/19
Department Chair Date

4/24/19
Honors College Dean Date

HONORS COLLEGE
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Honors College
Frank Franz Hall
+1 (256) 824-6450 (voice)
+1 (256) 824-7339 (fax)
honors@uah.edu

Honors Thesis Copyright Permission

This form must be signed by the student and submitted as a bound part of the thesis.

In presenting this project summary in partial fulfillment of the requirements for Honors Diploma or Certificate from The University of Alabama in Huntsville, I agree that the Library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by my advisor or, in his/her absence, by the Chair of the Department, Director of the Program, or the Dean of the Honors College. It is also understood that due recognition shall be given to me and to The University of Alabama in Huntsville in any scholarly use which may be made of any material in this thesis.

Joseph Biagini

Student 1 Name (printed)

Joseph Biagini

Student 1 Signature

4/24/19

Date

Logan Johnson

Student 2 Name (printed)

Logan Johnson

Student 2 Signature

4/24/19

Date

Increasing SmartChair Data Integrity through Cybersecurity Analysis

by

Joseph Daniel Biagini & Logan Iver Johnson

An Honors Capstone

submitted in partial fulfillment of the requirements

for the Honors Diploma

to

The Honors College

of

The University of Alabama in Huntsville

April 24, 2019

Honors Capstone Director: Dr. Rhonda Gaede

Associate Professor, Electrical & Computer Engineering Department

Student 1	Date	Student 2	Date
Director	Date		
Department Chair	Date		
Honors College Dean	Date		

Honors College
Frank Franz Hall
+1 (256) 824-6450 (voice)
+1 (256) 824-7339 (fax)
honors@uah.edu

Honors Thesis Copyright Permission

This form must be signed by the student and submitted as a bound part of the thesis.

In presenting this project summary in partial fulfillment of the requirements for Honors Diploma or Certificate from The University of Alabama in Huntsville, I agree that the Library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by my advisor or, in his/her absence, by the Chair of the Department, Director of the Program, or the Dean of the Honors College. It is also understood that due recognition shall be given to me and to The University of Alabama in Huntsville in any scholarly use which may be made of any material in this thesis.

_____	_____
Student 1 Name (printed)	Student 2 Name (printed)
_____	_____
Student 1 Signature	Student 2 Signature
_____	_____
Date	Date

Table of Contents

Acknowledgements

We would like to thank Dr. Rhonda Gaede for advising us and providing us with helpful feedback during the course of the semester regarding this research. We would also like to thank Dr. Aleksandar Milenkovic for advising and funding the development of the SmartChair product. We would like to thank Alex Dillon for cooperating with us as we messed with his computer hosting the web server. Finally, we would like to thank Dr. Tathagata Mukherjee for providing not only direction, but also the necessary hardware for this project.

Abstract

The SmartChair is an embedded systems device used to monitor health data including heart rate, posture, movement, sitting time, and air quality. This data is measured by multiple sensors, and processed by a microcontroller which sends the data to a database on a remote server. The user can then view the data on a separate website. Due to the fact the SmartChair is connected to the Internet, security vulnerabilities exist. In order to secure the SmartChair product, we sought to find, exploit, and then suggest mitigations to cyber vulnerabilities of the SmartChair in order to improve the overall data integrity for the SmartChair product.

After examining the SmartChair system, four possible avenues of attack were revealed: spear phishing, WiFi spoofing, a man-in-the-middle attack, and an exploitation of the software running on the physical machine hosting the database. Although the phishing and man-in-the-middle attacks were not attempted, an analysis shows how they could theoretically be performed. The WiFi spoofing attack and the web server exploitation were both attempted, but both attacks proved unsuccessful. (Also, a fifth avenue of attack was unexpectedly discovered when exploring the other vulnerabilities. This was an exploitation of the SmartChair source code which allowed packet information to be rerouted.) Ultimately, the SmartChair product proved to be a system with high data integrity that is secured against various attack avenues. For the situations where the SmartChair is not secure, actions were suggested to mitigate the vulnerabilities discovered.

Introduction

In the modern world, a large portion of the workforce spends the majority of their time sitting in a chair - whether for work, school, at home, or elsewhere. Therefore, it is useful to know how sitting in such chairs for long periods of time may affect the user's health. In order to satisfy this need, a prototype of a device named the "SmartChair" was designed as part of the UAH Computer Engineering senior design course by Joseph Biagini, Alex Dillon, Logan Johnson, Joseph Kerns, and Christopher Taylor under the guidance of Dr. Aleksandar Milenkovic. The ultimate purpose of the SmartChair is to provide the user with their health data in order to improve the user's quality of life.

The SmartChair obtains data by using multiple sensors, including pressure, heart rate, air quality, and motion sensors. These sensors are used to measure the user's heart rate, posture, movement, sitting time, and air quality (more specifically, carbon dioxide and volatile organic compound levels). The SmartChair works by utilizing a microcontroller connected via wiring to the sensors to process the data. The microcontroller sends the data by WiFi to a database on a remote server. To retrieve the data, the user must perform two installation steps. First, the chair must be registered to the server. This is done by connecting a device to the SmartChair's WiFi broadcast, visiting the registration webpage, and sending the authentication details of a local access point so the embedded platform can connect to the Internet. Second, the user must go to the main SmartChair website (which is separate from the registration webpage), create a user account, and pair the embedded system using a pairing code obtained from the registration webpage. Once the pairing has occurred, the user can view a dashboard on the SmartChair website which contains multiple graphs that show the data.

As noted, the SmartChair requires Internet connectivity in order for the data to be sent from the chair to the web server. Therefore, just as with any computer device that connects to the Internet, the chair likely contains security vulnerabilities. Malicious actors who are interested in compromising the integrity of a user's data may find and exploit these vulnerabilities in order to do so. Even though the data cannot do any harm, the attacker could still be interested in knowing a user's health information or tampering with it, perhaps as an attack against the reliability of the SmartChair product.

We determined that there were four possible attack methods available for exploit. One method is that the attacker sends a phishing link to a user which sends the user's password to the attacker. A second method is that the attacker performs what is known as an "evil twin" attack, in which the attacker uses a network spoofing device in order to disguise itself as a particular access point. Thus, the attacker effectively tricks the microcontroller into sending its data to a fake router and the attacker receives the data. A third method exists where the attacker performs what is known as a "man-in-the-middle" attack. A man-in-the-middle attack is a method of data interception achieved by breaking the wireless transmission protocol used between the SmartChair and its user-assigned access point. A fourth method is for the attacker to exploit vulnerabilities in the web server's operating system for the purpose of performing a privilege escalation attack on the system and gaining access to secured user data stored upon the same machine. While attempting the evil twin attack, an unexpected vulnerability was encountered which allowed the adversary to assign the access point of the SmartChair.

Avenues of Attack

Spear Phishing

A spear phishing attack refers to a situation in which an adversary targets a specific user via email that is disguised as if sent by a credible source. These attacks have the intention of tricking the user into revealing (willingly or unwillingly) secret user information to the disguised adversary because an embedded malicious link does not perform the action specified by the apparently credible source. For example, the attacker may send an email to an unsuspecting victim, in which the attacker claims to be from a bank and needs the victim's bank account username and password. If the victim enters their username and password in the link provided in the email, the attacker may be able to gain access to the victim's bank account and steal money.

A similar spear phishing attack could also target a SmartChair user. The attacker could send an email to a victim, in which the email seems to have originated from the SmartChair website. The email could ask the victim to send the attacker the username and password for the victim's account. If the victim responds with that information, the attacker will be able to log in to the victim's account and obtain the victim's health data from the SmartChair.

Phishing is particularly difficult to prevent, because it relies on betraying human trust! This avenue of attack is not one that can be patched from the end of the SmartChair. It can only be prevented by training people to recognize, avoid, and report phishing attempts. Training can occur in one of two ways. Often it is the responsibility of a corporate organization to train their employees on the reality and practicality of phishing schemes. However, if the SmartChair team wanted to achieve total coverage, perhaps their best practice to prevent phishing scandals would

be to distribute a security awareness leaflet with every copy of the SmartChair product which included information detailing phishing tactics and how to avoid them.

Evil Twin Attack

When any computer, no matter if it's a personal computer or a microcontroller, connects wirelessly to the Internet, it does so by sending WiFi signals to a nearby router which in turn relays the signals over wired networks to the destination. A computer can connect to any router of its choosing, usually specified by the user. The computer always has the ability to connect to a different access point; it is not locked to any particular one. An evil twin attack is one that takes advantage of this principle of wireless networking. The adversary sets up an access point (AP) identical in every way to the one the computer is connected to except that the AP is connected to some sort of device which can collect all packets being sent to the adversarial AP. An intentionally identical AP is termed a "spoofer." The spoofed AP works because it is in closer proximity to the computer than its original connection. The computer connects to the AP with the strongest broadcast. However, even if the adversary brings its AP right next to the computer, the computer will remain connected to the original AP. Thus the adversary's AP ought to have the capability to deauthenticate the computer from its original AP and then establish a connection with the computer. Once the attacker connects the victim's computer to the spoofer, they are able to analyze the network traffic from the victim's computer using a network packet analyzer program.

An attempt was made to simulate this attack in which the SmartChair microcontroller was the victim's computer. In order to simulate such an attack, the WiFi Pineapple NANO was

used as the spoofer device; the device was connected to a personal computer, which was near a SmartChair microcontroller. Wireshark was used as the network packet analyzer program.

The Pineapple NANO proved capable of achieving its purpose. First, the Pineapple device was configured such that the network was successfully spoofed. This means that the Pineapple was able to mimic the SSID of each accessible local network and then provide a point of connection to that SSID. Secondly, the Pineapple provided the capability to deauthenticate the SmartChair from its non-spoofed router. However, we were unable to get results for the third and final step of the evil twin attack. The idea was that the WiFi Pineapple NANO would, after deauthentication, broadcast the SSID of the network the SmartChair was trying to connect to, then as the SmartChair tried to reconnect, would be tricked into a connection with the Pineapple because the Pineapple broadcast a stronger signal with the same credentials. In the end, the Pineapple was not successful in establishing a connection to the SmartChair. This is likely due to the fact that the WiFi Pineapple NANO hosted its clients only on an open WiFi network. Since the non-spoofed router was using a secured WPA2 channel, the SmartChair expected to connect to a WPA2 secured channel, and the Pineapple was unable to comply.

These results are reassuring from the data integrity perspective. A common evil twin tool was unable to compromise the security of the SmartChair. Even if the Pineapple was able to spoof the access point properly, the data captured via Wireshark would be encrypted with the TLS protocol used between the SmartChair and web server. Theoretically, this encryption could be broken using a cryptographic approach, but that is beyond the scope and budget of this research.

Man-in-the-Middle Attack

A man-in-the-middle (MITM) attack refers to an attack in which an adversary is able to obtain or alter data sent between two computers. The sophistication of the attack depends upon the environment in which it is performed. A simple MITM attack, for example, is one in which a computer is plugged into a network hub. Since a network hub forwards data to all connected computers, it would be easy for an adversary to listen in on the data or even intercept the data with a bit of sophisticated network manipulation. The evil twin attack discussed previously is an example of a man-in-the-middle attack. It is believed that it could theoretically be possible for a MITM attack to be performed on the SmartChair microcontroller WiFi signal without using a spoofer. However, the attack would require a much more sophisticated approach than the one attempted with the WiFi Pineapple. Without the help of a network spoofer, the next alternative option to achieve an MITM attack is to break the TLS encryption using a cryptographic approach. While all network communication protocols have their flaws and weaknesses, breaking cryptography is beyond the scope of this project. Doing so would not only require an in-depth analysis of the protocol, but also the software means and computational power to reach the assumably achievable outcome.

There is another possible method to perform a MITM attack without actually breaking the encryption. If two parties want to send encrypted data but they are unable to meet in person, then there must be a public key that is exchanged as part of the message transmission. However, a third party could intercept this key transmission and send a different public key instead. Considering that the recipient now has a different public key, the attacker will know how to change the messages sent by the sender with the false key. In addition, since the attacker has the

real public key, he can now change the messages that are being sent. However, this situation does not apply to the SmartChair, since TLS uses private keys to encrypt and decrypt messages.

These are reassuring conclusions for the security of the SmartChair. Essentially, due to the complication of the task, the man-in-the-middle attack is not a feasible option to compromising the security of the SmartChair until the TLS encryption protocol is effectively broken. Even when network protocols are theoretically broken, there is still a large gap between theoretically broken and practically broken. Therefore, when the TLS encryption scheme has been broken in a way that is practically useful to intercept data, then the security of the SmartChair needs to be re-implemented using the most reliable network communication encryption protocol of the day, but until then, it is reasonable to conclude that data integrity will be preserved by using the TLS encryption.

Privilege Escalation

Modern software programs boast millions of lines of code. Due to the complexity of such programs, it stands to reason that countless vulnerabilities remain overlooked by software developers. Because there are so many lines of code, it is infeasible to test every case and condition presented by those millions of lines of code. Attackers spend countless hours trying to find vulnerabilities in software by presenting those software programs with a wide variety of obscure test cases looking for bugs that the original developers did not catch. These people then hope to create zero-day exploits. Zero-day exploits are exploits which are generated before the discovered vulnerability has a chance to get patched. Once patched, the software developers push a new version of the software so that their program is reliable. In this project, a possible attack

vector was the use of a zero-day exploit. The plan was as follows: perform a port scan on the machine hosting the database, enumerate the open ports on the machine, and then identify the version of each service running on them. Finally, a web search was performed to find exploits (preferably zero-day exploits) to the known vulnerabilities of the services running on the machine, gaining access to the machine wherein we could perform a privilege escalation event and gain access to the database.

Although this does not always have to be the case, the web server and database were hosted on the same machine for the senior design project. Because a web server typically requires more communication with the outside world than a database does, this allowed for the opportunity of more open ports than if simply a database were stored on the machine. The SmartChair web server was hosted from a Microsoft Windows 2016 Server virtual machine (VM). A second VM was set up on the same internal network running a Kali Linux image. This configuration allowed for port scans from Kali to the SmartChair VM. Nmap was chosen as the method to scan the SmartChair web server. Nmap is a powerful Linux command-line utility used to enumerate hosts on a network and open ports on a host. The results of the port scan using nmap version 7.70 are shown below.

Open Port Number	Service Running	Version
80	http	Microsoft IIS httpd 10.0
443	ssl	Microsoft IIS httpd 10.0
3389	ms-wbt-server	Microsoft Terminal Services

Services and Versions Running on Open Ports of Machine Hosting SmartChair Database

The results of this scan show that the system admin of the SmartChair web server had updated all services to their latest versions. Updates are released in order to minimize vulnerabilities. At the time of writing this paper, very few vulnerabilities have been discovered for the versions of these services. The versions were checked against cve.mitre.org, a database of Common Vulnerabilities and Exposures (CVE). This website compiles all publicly-known vulnerabilities and assigns a unique identifier to each. It is officially recognized and used by organizations like Microsoft. According to the CVE database, few vulnerabilities for the services hosted by the SmartChair web server have yet been discovered - none of which have known exploits. Since the SmartChair web server was up to date, and unused ports remained closed, the system admin of the SmartChair network successfully thwarted the attempt to penetrate the computer's defenses and perform a privilege escalation attack.

Exploiting the SmartChair Source Code

Throughout all the tests mentioned in previous sections, one vulnerability was encountered quite unexpectedly. This could quite possibly evolve into a fifth avenue of attack: an exploit against the vulnerable SmartChair source code.

After connecting a device to the SmartChair WiFi broadcast, it is necessary to go to the network registration page. When at the network configuration page, it is necessary to enter the SSID of the network you wish to use for connection. This is a great way to interface the SmartChair from the end user's point of view, however, it is insecure. As long as the router is configured using WPA2, any router's SSID and password can be entered. Although it is the end-user who is responsible for the initial setup of the device, anyone within range of that WiFi

signal can connect to the network configuration page and change its settings without noticeably affecting the performance of the SmartChair.

This exploit could be used by an adversary sitting on the other side of a nearby wall with a sophisticated network access point which can intercept all traffic coming from the SmartChair. All they need to do is to get in range of the SmartChair access point, connect to the network configuration page, change the target SSID and password, and then set up an access point to receive the intercepted data.

There are three suggested fixes to this vulnerability. The first option is to secure the networking configuration page using a variant of two-factor authentication. The board has Bluetooth capabilities. Perhaps the board could display a limited-time access code to a terminal via Bluetooth in order to confirm a change to the network settings. This would validate that only the network with the SmartChair embedded platform is registered. But still, Bluetooth can be intercepted. A serial cable could be connected between the SmartChair platform and the computer to guarantee that only one computer was able to see the transmitted access code. This would be very clunky. As the SmartChair was designed with usability in mind, the serial cable solution is not preferred.

Another possible solution which leads to this same conclusion is this: make the SmartChair WiFi signal a WPA2 access point rather than its current configuration of open. The issue with this fix is the same problem as previously mentioned - presenting data to the user, and the user alone. The first two solutions present the option of broadcasting the two-factor code or connecting via serial cable, both of which are less than ideal. In order to find a more ideal situation, the third solution must be considered.

The third proposed solution to this vulnerability is to disable the broadcast after the network settings are changed. Although this seems like the correct choice at first, it could be easily circumvented using a device such as the WiFi Pineapple. Such a device could deauthenticate the SmartChair from its network connection, then the user could connect to the SmartChair while it stumbles around looking to reestablish its broken network connection. Because of this, we believe the methods utilizing the serial cable seem to be the most reliable solution to the source code vulnerability.

Conclusion

In summary, five methods of attack were discussed as possible ways for attackers to obtain or alter SmartChair data. The first method discussed was a spear phishing technique, which could very easily be performed by exploiting the trust of a SmartChair client. The second method discussed was an evil twin attack. Although unsuccessful in this research project, this attack avenue is theoretically possible and merits further research as the resources provided (WiFi Pineapple NANO) were unsuccessful in achieving the end purpose. The third method discussed was a man-in-the-middle attack, though breaking the TLS encryption would make this attack quite sophisticated. The fourth method discussed was exploiting vulnerable software on the database machine. While no exploitable vulnerabilities were found in the research concerning the database software, an unexpected fifth exploit was found where a user could connect the SmartChair embedded platform to a malicious access point - the threat of which could be mitigated using a form of two-factor authentication.

Overall, exploiting the vulnerabilities was a very challenging task. We were not quite as successful as we were hoping in terms of successfully finding an exploit; we believe that every system has its vulnerabilities. However, the SmartChair system was held into the light and thoroughly analyzed through several different means. Since the database service versions were so new, few vulnerabilities had been suggested - and no documented exploits. In addition, it was unknown how to make the Pineapple NANO's spoofed SSID and the microcontroller's desired SSID compatible with each other. However, on a more positive note, we did feel that we were able to gain much experience with tools such as Nmap, Wireshark, and the Pineapple, which in turn allowed us to greatly increase our knowledge in cybersecurity.

Through this increase in cybersecurity knowledge and experience, we can ultimately conclude that the SmartChair system is actually quite robust as it is. Some of the methods discussed in this paper have a greater probability of yielding the desired results than others, yet employ techniques which require much more time and sophistication (and likely money) - resources we do not have. Yet, as for the methods tested in this report, the SmartChair was able to stand tall with simple cybersecurity practices of encrypted network transmission and keeping software up to date. In the end we may not have been able to walk away with groundbreaking results, but can declare with greater experience that the SmartChair has been designed with integrity of the user's data in mind.