Talal Jawaid

Amrit Singh

Roberto Ochoa

Rafael Garcia

Minquan Li

Brogrammers 154 Project - Wireless Access Point Intrusions

In February of 2016 a famous bank in Bangladesh was experiencing printer difficulties. This was an obvious nuisance; the automated printer was supposed to print the banks transaction reports in real time. This technical glitch was thereafter realized as a factor in one of the biggest bank heists of all time. When the printer started running again the employees flagged 35 suspicious payment orders totaling almost a billion dollars. Because of the printer glitch it was too late to cancel the orders and it seemed that Bangladesh had just lost an absurd amount of the nations reserve. Cyber security analysts as well as investigators concluded that this heist began nine months in advance.

In May of 2015 four men walked into a RCBC bank in the Philippines. They created bank accounts with 500 dollars each and seemingly abandoned their accounts as there was no activity until the time of the heist. After some time had passed, An employee clicked on a malicious email in January of 2016 which installed a program in the central banks computer systems. This malware allowed individuals to enter the system and gain access to the inner workings of the bank. The culprits then spent some time studying the banks operational procedures from the inside. Swift sends trusted payment orders to banks, which they then act on. Swift is protected by military grade security, and is a standard software used in banks across the world. The hackers were able to retrieve swift credentials using the malware they had planted in the bank. Using these credentials, the culprits were able to process 35 money transfer requests totaling 951 million dollars to the federal reserve bank in New York, where it would then go to different banks across Asia eventually leading back to the RCBC bank in the Philippines.

Due to a fortunate coincidence 30 out of 35 of the requests were flagged since the names on the orders matched that of a shipping company “Jupiter” that had been blacklisted for evading U.S. sanctions against Iran. This “Lucky Break” saved Bangladesh $871,000,000 dollars. Because these orders were flagged for manual review, they were not able to be processed right away. The Federal Reserve was able to get in contact with the Bangladesh and retract the orders so that this money was saved. Unfortunately, the remaining five transactions went through totaling $101,000,000. Other factors such as the size of the remaining transactions as well as trivial mistakes like the spelling of the word “foundation” raised suspicions and caused more of the money to be retracted, leaving the hackers with only $51,000,000.

It was later concluded that North Korea was behind this among other cyberattacks. CNN reported, “FBI cyber investigators have identified the North Korean hackers behind a 2016 cyberattack on Bangladesh's central bank. The North Koreans infiltrated Bangladesh Bank's systems with hopes of stealing as much as $1 billion from accounts held at the New York Federal Reserve, FBI investigators found. The hackers got away with $81 million before the bank transfers were stopped “(CNN).

Another assault involving local network security came in the form of the Shamoon malware attack in August 2012. This attack, conducted by a group named the "Cutting Sword of

Justice", consisted of getting access to the network of Saudi Aramco, Saudi Arabia's national oil firm. The group created and shared a Pastebin describing their reasoning behind the attack, stating that they were “fed up of crimes and atrocities taking place in various countries around the world. (Justice, Untitled, 2012)” The attack targeted the Al-Saud regime for their support of the oppressive matters the group wished to end. Saudi Aramco happened to be the “largest financial source for the Al-Saud regime. (Justice, Untitled, 2012)” The remainder of the Pastebin issues a warning to tyrants of other countries and invites other hacker groups to join them in a movement against tyranny.

The attack exploited a vulnerability with Saudi Aramco internet connection to gain access via an outside source. Once inside the network, the hackers spread malware across the local network connection and infected at least thirty thousand of the firm's workstations. (Justice, Untitled, 2012) The payload of the malware was set to be executed on August 15, 2012. Tofino Security explains the three separate portions of the malware that were later discovered. They are named the Dropper, Wiper, and Reporter. The Dropper was “the main component and source of the original infection. (Mackenzie, 2012)” It placed copies of the other two onto the infected computer, then sent copies of itself throughout the network. In addition, it also executed itself to create a service that starts when Windows is booted. The Wiper contained the destructive code, with the purpose of deleting files and gathering file information to be sent back to the attacker’s computer. The deleted files also had their data replaced with corrupted jpeg images, “obstructing any potential file recovery by the victim. (Mackenzie, 2012)” The Reporter finally sent the information of the files gathered and destroyed by the Wiper back to the attacker's computer.

The destruction caused by the malware was massive. The HuffPost reported that “More than thirty thousand computer that it infected at Aramco were rendered useless and had to be replaced. (Stewart, 2012)” Operations at Aramco shut down, as the company was forced to “disconnect all systems and data centers to stop the malware from travelling through the network. (Rashid, 2015)” This shutdown lasted for ten days, as on August 25th, Aramco declared they were continuing operations (Leyden, 2012). However, the attackers still had information to share, as on August 27th, the group released another Pastebin. This Pastebin contained sensitive information, including info on the routers at Aramco, the CEO’s email information, and the security appliances the firm had in place. (Justice, Saudi Aramco hug, another one, 2012) Eventually, Aramco was able to recover from the “most destructive virus to hit a business” (Stewart, 2012), but the impact was felt.

In both of these incidents, a local network was breached and access was gained to all computers on the network. Gaining access to a secure network can be nearly as harmful as gaining physical access to a machine since most security precautions and protections are aimed at preventing outside intrusions into the network. However, if those protections can be bypassed by simply breaking into the network itself, then those security safeguards are made useless. As such, our chosen topic is wireless network security.

In the Bangladesh bank heist, hackers were able to remotely break into the network by use of a trojan horse sent through email. In the second incident, attackers were able to break into a Saudi ARAMCO owned network and spread malware throughout the system.

While it is likely that both of these attacks were performed outside of the country, it is still much more difficult to break into a network from the internet due to internet facing security protections such as firewalls and intrusion detection software. However, there exists a much more dangerous opportunity for malicious hackers to infiltrate a network. It requires a hacker to break into the physical wireless network that the victim's systems are linked to. While a victim may have their computer hardwired into the network, the local network they are on may be exposed as a wireless access point. Hackers can and have successfully exploited the vulnerabilities in these wireless access points to gain access to secure networks. Once hackers are able to break into the network, they are able to spread malware and access local network files as easily as if they were hardwired into the network.

In the past, the most used form of wireless access point security was WEP encryption. This, however, was easy to exploit and insecure in nature. Software suites such as Aircrack would allow potential hackers to break into networks with relative ease. It would take no more than 10 minutes for most wireless networks to be cracked and their network to be exposed.

WEP was eventually phased out due to its insecure nature and replaced with the WPA and WPA2 encryption methods which were much more secure. Today, there exists a method using the same aircrack suite combined with a tool called Hashcat which allows users to crack WPA2 keys.

The first widespread WEP hack caused the wireless industry to immediately move towards a more secure protocol as soon as possible. The industry at the time understood the ramifications of easily accessible exploits that the general public can take advantage of. The implications of widespread usage of a WPA2 hack are enormous and most businesses do not realize how much sensitive data is exposed to other machines on the network. With use of the Aircrack suite along with Hashcat to crack WPA2 passwords, we will begin to see security leaks happening on a much more frequent scale. The attacks in Bangladesh and Saudi Arabia were relatively difficult due to the nature of the attack which hinged on breaking into the network from the outside. However, one can imagine how much easier an attack would be if all an attacker has to do is simply sit outside a victim's business with a powerful enough wifi adapter. Our project will focus on wireless access point intrusions. We will demonstrate the capability of the average person to break into a wireless network. We plan on using the Aircrack suite and the Hashcat tool to crack both WEP and WPA networks to show how insecure wireless security today really is.

References

Justice, C. S. (2012, August 27). Saudi Aramco hug, another one.

Justice, C. S. (2012, August 15). Untitled.

Leyden, J. (2012, August 29). *Hack on Saudi Aramco hits 30,000 workstations, oil firm admits*. Retrieved from The Register: https://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/

Mackenzie, H. (2012, October 25). *Shamoon Malware and SCADA Security – What are the Impacts?* Retrieved from Tofino Security:

https://www.tofinosecurity.com/blog/shamoon-malware-and-scada-security-%E2%80%93-what-are-impacts

Rashid, F. Y. (2015, August 8). *Inside The Aftermath of the Saudi Aramco Breach*. Retrieved from DARK Reading: https://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676

Stewart, P. (2012, December 11). *'Shamoon' Virus Most Destructive Ever To Hit A Business, Leon Panetta Warns*. Retrieved from HuffPost: https://www.huffpost.com/entry/shamoon-virus-leon-panetta_n_1960113?utm_hp_ref=technology