

Networks assignment 2 - Toby

by Thorbjorn Ravnaas Kristiansen

FILE	2652_THORBJORN_RAVNAAS_KRISTIANSEN_NETWORKS_ASSIGNMENT_2_-_TOBY_113613_2088126905.DOCX		
TIME SUBMITTED	23-MAY-2018 03:52PM (UTC+0100)	WORD COUNT	2944
SUBMISSION ID	89799177	CHARACTER COUNT	18029

University of Wales, Trinity St. David

Cyber Security: Threats and Defenses

BEng Computer Systems and Electronics

Thorbjørn Kristiansen (P151226)
Lecturer: Dr Tim Bashford, UWTSD
May 2018

Contents

Introduction	2
Computer Network Risks	3
Attacks without Physical Access.....	3
Distributed Denial of Service (DDoS)	3
Password Cracking	3
Packet Sniffing	3
WPA2 Handshake Vulnerability (KRACK).....	4
Rogue DHCP Server.....	4
ARP Spoofing	4
Attacks with Physical Access and IoT	4
Theft and Sabotage	4
IoT	5
Security Measures and Preparation	5
DDoS.....	5
Password Cracking.....	6
Packet Sniffing.....	7
Conclusions.....	7
Further reading	8
References.....	9

Introduction

Cyber security has been an increasingly debated topic over the last decade. It has become the collective description of previously separate entities like computer security, IT security, etc as shown by Schatz et. al.[1]. It can be assumed that this is due to an ever-increasing number of computers in the world, which raises both knowledge and attentiveness of consumers as a large part of their life may be dependent on the Internet. Since different network types provide access to virtually all the computers and devices in the world, they (networks) need to be secure.

The scope of a cyber-attack can be argued to encompass all existing electronics systems (i.e. all systems are vulnerable). Some parts of governmental infrastructure are vulnerable to attack. Power grids that are digitally monitored and controlled are an example, where a hacker with malicious intent may access the control systems in several ways and may affect it adversely[2], [3]. Other critical systems like medical systems also need to be very secure. Although the damage outcome for a security-critical system is perceived as higher, personal computing also needs to be secure when communicating over a network.

This essay will focus on some of the different ways to affect computer systems negatively (mainly networks), as well as the different methods to circumvent or block them. Cyber security awareness will hopefully be raised through this essay.

Computer Network Risks

As gaining access to a system is what renders the system compromised, the most common risks should be analysed and prepared for. Gaining access is not always the objective, as discussed later in the text.

Attacks without Physical Access

It can be argued that software-based attacks are the most threatening because of the detectability. Security cameras, locks and motion sensors are rendered useless when a remote attack is successfully executed.

Distributed Denial of Service (DDoS)

A DDoS attack's main purpose is not to manipulate or steal data, but rather make it inaccessible. The data in question are usually websites, and the goal is to make them inaccessible to the public by overloading the host with unnecessary traffic[4]. This can be accomplished in several ways, for example loading the host with computationally expensive tasks or pinging the server constantly[5].

Password Cracking

Password cracking is the action of either guessing the password by attempting every possible combination on the keyboard until a match is found (brute forcing) or simply guessing the password based on some assumptions the program will iterate upon (dictionary attack). These assumptions range from the seemingly obvious (number of letters in the alphabet, attempting variations of the username, common passwords, etc) to the more sophisticated variants utilising word lists (dictionaries) of commonly used passwords[6]. Some password cracking techniques reverse engineer this by obtaining a list of usernames. The perpetrator now has the ability to test the most common password on all of these usernames one at a time, which usually results in a match. This is due to people favouring convenience over absolute security[7].

Packet Sniffing

Passwords can be made infinitely stronger but are worthless if anyone but the intended person has access to it. Intercepting transmitted data (packet sniffing) is a type of attack which focuses on stealing data[8], and is thus able to intercept or "sniff" the data packets from the transmission channels. Passwords

are not the only category of sensitive information being transmitted, so a perpetrator could conceivably have access to PIN numbers, social security numbers, etc. This can be done remotely, or in some cases, by utilising sniffing hardware for listening to Wi-Fi-signals on multiple channels[9].

WPA2 Handshake Vulnerability (KRACK)

The WPA2 handshake vulnerability (KRACK, Key Reinstallation AttaCK) is a way for unintended clients to exploit the Wi-Fi protocol to gain access to packets which subsequently could be decrypted to reveal passwords or other vital information. It works by exploiting the 4-way handshake authentication method in the Wi-Fi protocol by making the host resend the 3rd handshake multiple times. This allows for decryption. This exploit is especially severe, since it exists on every device who utilises the Wi-Fi standard[10]. Patches for this vulnerability are rolling out, so keeping device drivers updated is paramount.

Rogue DHCP Server

A rogue DHCP server is a device or program which sends address information to the wrong location. This can be both intentional and unintentional (an individual unknowingly connecting routing equipment inappropriately[11]). The addressing system of a network is extremely important to ensure correct data flow. By altering the address system using a rogue DHCP server, data could be sent to other locations for malicious intent, or simply get dropped by the system. This effectively creates a localised paralysation of the affected network, or a small-scale Denial of Service (DoS) attack if configured this way.[12].

ARP Spoofing

ARP spoofing can have much the same effects as a rogue DHCP server, although it targets the Address Resolution Protocol of the network. By injecting false ARP-data into the system, the perpetrator could potentially reroute traffic back to one's self. It can also be used as a DoS attack by altering parameters such as the gateways, rendering the client unable to communicate further[13].

Attacks with Physical Access and IoT

Theft and Sabotage

The crudest form of attack to a computer system is theft of devices containing valuable data. Ironically, a server administrator could invest large amounts of money and time protecting his network from a cyber-attack, but this will be

forfeit the moment someone runs away with his or her hard drive. Investing in secure server locations and surveillance is the only obvious and effective prevention for this scenario. Additionally, this will most likely deter sabotage-based attacks as well. A faulty cable can cause substantial problems, so server redundancy (multiple hardware units designed to decrease downtime) is an imperative feature for a networked system.

IoT

The IoT (Internet of Things) is a relatively new connotation for all the different smart devices with Internet-connectivity. These pose a potential risk due to their widespread use and unregulated production. Botnets could be formed by either exploiting poor security protocols in existing IoT devices, or by selling devices designed to act as bots[14]. These devices are then remote controlled by the perpetrator and can be utilised to take part in multitudes of nefarious activities like DoS attacks or data interception techniques[15]. Other challenges with the IoT phenomenon is the electrical safety and network stability of these devices. It is not impossible to imagine a network crash due to an inexpensive malfunctioning Wi-Fi juice press, or a house fire caused by a baby-call system with minimal emphasis on fire safety.

Security Measures and Preparation

Although the techniques mentioned previously all span a large array of categories and attack angles, it is fully possible to defend against these attacks, or in some cases survive a successful attack with minimum data being compromised. Some solutions require complex implementations of expensive hardware or software, while others simply rely on an attentive attitude among users (increasing awareness and knowledge about cyber security). An increased awareness level will influence how users utilise network features and may perhaps provide a positive shift in network security statistics.

DDoS

Defending against a DDoS attack is no simple feat. The main problems lie in the way a DDoS attack functions and behaves. It is designed to behave erratically by distributing the attacks from multiple sources, which makes the attack near-impossible to block. The different sources applying stress to the network may not be doing it voluntarily, as botnets could be built and distributed utilising

malicious code[16]. The network is overwhelmed by the sheer amount of traffic from all the requests from the different sources and grinds to a halt[4].

Some hardware defence solutions exist. In a recent paper, Software Defined Networking (SDN) switches were tasked with redirecting data flow by analysing the pattern of a DDoS attack. This eliminated the need for understanding the context of the individual packets, as it detects data flow patterns instead[17]. Other types of switches have also been dedicated for DDoS defence with similar functionality[18]. The obvious problem with this is cost. Switches and other networking hardware are expensive on a large corporate level, where purchases and budgets are considerably larger than the average person's.

Some researchers found that expensive hardware and long deployment times are not necessary if the defence mechanism is implemented as software. One technique is sharing the network load over several domains, with centralised resource sharing as a load balancing mechanism[19], [20]. This also showed promising results. *It is "allowing" the attack to happen, while distributing the load over multiple branches to combat server overload* is a rough functionality description.

Password Cracking

Passwords rely on a human aspect and is therefore flawed from the beginning. Cracking them can be a trivial task if the password does not fulfil some base requirements, and the burden of protection often lies with the user[7]. A study has been made on the effect of human involvement and what motivates a stronger sense of security and deters from criminal action[21]. The user favours the simple life with uncomplex passwords, while the hacker takes advantage of this, as quoted from Nouredine et. al:

"Compared to human users and administrators, cyber attackers can be assumed to be rational decision makers aiming to maximize their profit while minimizing their relative cost. Users on the other hand, deviate from pure rational behavior and thus require, as we have discussed, more challenging models."[21]

Since password-cracking technologies evolve with the complexity of the passwords themselves, another solution is needed. Two-factor authentication gives the user a chance to verify a login attempt, as well as decline it since the

system usually relies on smartphones which most people carry on their person[22]. One-time code solutions are also viable countermeasures. These work by verifying time synchronisation between client device and host server, giving out a different code every set time interval[23]. These codes are mathematically linked to points in time, using a strong encryption method to make reverse engineering virtually impossible. The set time intervals also contribute to make it extremely difficult to reverse engineer a code before it expires[24].

Packet Sniffing

Defending against packet analysis attacks is a complex task in that the intrusion can happen anywhere on the transmission line, be it wireless or wired. Some intrusion detection systems attempt to identify attacks by searching for specific signatures unique to each attack[25]. The best solution for preventing packet sniff attacks is to be careful with non-encrypted Wi-Fi connections and using Secure Socket Layer connections where possible, allowing for end-to-end encryption of all transmitted data. Although WPA2 Wi-Fi encryption is generally deemed as safe, it has been compromised by the KRACK method. This serves as a reminder that no encryption standard is 100% secure forever.

Conclusions

From an attacker's point of view, a good attack is designed to be difficult to detect and defend against. To keep up with this arms-race, security and networking companies are in a constant battle. Updates and patches are the recurring theme since attackers would experience little to no resistance if these solutions did not exist. The general mindset of the user is also a substantial security risk. As mentioned, humans are prone to error and are therefore the weakest link in any security system. Key cards, tokens, passwords and countless other systems for logging in and network identification are worthless if the human aspect fails to conform with security standards. Although a meagre list of defences was listed in this essay, solutions do exist for most problems.

The simplest and arguably the most effective attack is the DDoS. This method is readily available for the public to use for various purposes. Tools like Low Orbit Ion Cannon provides the user with a simplified GUI, which makes taking part in the attack a trivial task[26] [27]. It can be argued that these tools are

important, since they can be used for activism purposes, while a competing argument could relate to the negative effects of vigilantism.

Network attacks will happen regardless of installed security solutions. Features like redundancy, backups and physical barriers between perpetrators and equipment will not necessarily stop an attack, but rather minimise the possible damage potential.

[Further reading](#)

Since technology is an ever-expanding subject, it is difficult to keep track with the latest changes. Therefore, it may be beneficial to follow the market leaders in each field, as they have the resources to research new threats and how to confront them. Large security companies like Norton and Kaspersky regularly publishes info on security risks and how to handle them. Large networking corporations like Cisco also have a comprehensive learning database on most matters regarding networking, safety included[28].

References

- [1] D. Schatz, R. Bashroush, and J. Wall, "Towards a More Representative Definition of Cyber Security," *J. Digit. Forensics J. Digit. Forensics, Secur. Law*, vol. 12, no. 2.
- [2] R. Liu and A. Srivastava, "Integrated simulation to analyze the impact of cyber-attacks on the power grid," *2015 Work. Model. Simul. Cyber-Physical Energy Syst. MSCPES 2015 - Held as Part CPS Week, Proc.*, pp. 1–6, 2015.
- [3] P. Kaster and P. K. Sen, "Power Grid cyber security: Challenges and impacts," in *2014 North American Power Symposium (NAPS)*, 2014, pp. 1–6.
- [4] A. B. Whinston, "Defeating Distributed Denial of Service Attacks," no. August, 2000.
- [5] R. K. C. Chang, "Defending against flooding-based distributed denial-of-service attacks: A tutorial," *IEEE Commun. Mag.*, vol. 40, no. 10, pp. 42–51, 2002.
- [6] T. Bradley and H. A. Carvey, *Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security: Everyone's Guide to Email, Internet, and Wireless Security*. Syngress Media Incorporated, 2006.
- [7] K. Schaffer, "Are password requirements too difficult?," *Computer (Long. Beach. Calif.)*, vol. 44, no. 12, pp. 90–92, 2011.
- [8] S. Ansari, S. G. Rajeev, and H. S. Chandrashekar, "Packet sniffing: A brief introduction," *IEEE Potentials*, vol. 21, no. 5, pp. 17–19, 2002.
- [9] P. Reddy B., H. Sharma, and D. Paulraj, "Multi channel wi-fi sniffer," *2008 Int. Conf. Wirel. Commun. Netw. Mob. Comput. WiCOM 2008*, pp. 1–6, 2008.
- [10] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks," *Proc. 2017 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS '17*, pp. 1313–1328, 2017.

- [11] B. Patton, "How do you prevent a rogue DHCP server from taking control of your network? - Forum post," *Spiceworks*, 2010. [Online]. Available: <https://community.spiceworks.com/topic/114271-how-do-you-prevent-a-rogue-dhcp-server-from-taking-control-of-your-network>. [Accessed: 22-May-2018].
- [12] D. D. Dinu and M. Togan, "DHCP server authentication using digital certificates," *IEEE Int. Conf. Commun.*, 2014.
- [13] S. Puangpronpitag and N. Masusai, "An efficient and feasible solution to ARP Spoof problem," *2009 6th Int. Conf. Electr. Eng. Comput. Telecommun. Inf. Technol.*, vol. 02, pp. 910–913, 2009.
- [14] E. Bertino and N. Islam, "Botnets and Internet of Things Security," *Computer (Long. Beach. Calif.)*, vol. 50, no. 2, pp. 76–79, 2017.
- [15] K. Angrishi, "Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets," pp. 1–17, 2017.
- [16] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges. IEEE Communications Surveys and Tutorials, 17(4), 2242–2270. <http://doi.org/10.1109/COMST.2015.2457491>otnet in DDoS Attacks: Trends and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2242–2270, 2015.
- [17] J. Zheng, Q. Li, G. Gu, J. Cao, D. K. Y. Yau, and J. Wu, "Realtime DDoS Defense Using COTS SDN Switches via Adaptive Correlation Analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 7, pp. 1838–1853, 2018.
- [18] A. N. Viet, L. P. Van, H. A. N. Minh, H. D. Xuan, N. P. Ngoc, and T. N. Huu, "Mitigating HTTP GET flooding attacks in SDN using NetFPGA-based OpenFlow switch," *ECTI-CON 2017 - 2017 14th Int. Conf. Electr. Eng. Comput. Telecommun. Inf. Technol.*, pp. 660–663, 2017.
- [19] C. Fung and C. Fung, "CoFence : A Collaborative DDoS Defence Using Network Function Virtualization CoFence : A Collaborative DDoS Defence Using Network Function Virtualization," vol. 12, no. August, pp. 160–166, 2016.
- [20] Q. Wang, Z. Zhao, and H. Zhang, "DDoS defense mechanism based on

- software defined network," *2017 IEEE 9th Int. Conf. Commun. Softw. Networks*, no. 2, pp. 1122–1127, 2017.
- [21] M. A. Nouredine, A. Marturano, K. Keefe, M. Bashiry, and W. H. Sanders, "Accounting for the human user in predictive security models," *Proc. IEEE Pacific Rim Int. Symp. Dependable Comput. PRDC*, pp. 329–338, 2017.
 - [22] B. S. Archana, "Survey on Usable and Secure Two-Factor Authentication," 2017.
 - [23] K. C. Liao, W. H. Lee, M. H. Sung, and T. C. Lin, "A one-time password scheme with QR-code based on mobile phone," *NCM 2009 - 5th Int. Jt. Conf. INC, IMS, IDC*, pp. 2069–2071, 2009.
 - [24] TechQuickie - Linus Sebastian, "How Do Two-Factor Code Generators Work? [1:23-2:56] - YouTube," 2018. [Online]. Available: <https://www.youtube.com/watch?v=D6fRdCF9jyQ>. [Accessed: 23-May-2018].
 - [25] S. Srivatsa, "Detecting and preventing attacks using network intrusion detection systems," *Int. J. Comput. Sci. Secur.*, vol. 2, no. 1, p. 49, 2008.
 - [26] T. Nardi, "Low Orbit Ion Cannon: Exposed," *The Powerbase*, 2012. [Online]. Available: <https://web.archive.org/web/20120306042907/http://www.thepowerbase.com/2012/03/low-orbit-ion-cannon-exposed/>. [Accessed: 22-May-2018].
 - [27] Incapsula Imperva, "What is LOIC - Low Orbit Ion Cannon | DDoS Tools | Incapsula." [Online]. Available: <https://www.incapsula.com/ddos/attack-glossary/low-orbit-ion-cannon.html>. [Accessed: 23-May-2018].
 - [28] Cisco, "Cisco Networking Academy." [Online]. Available: <https://www.netacad.com/>. [Accessed: 23-May-2018].

Networks assignment 2 - Toby

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

76/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

GRADING FORM: SMU GENERIC_GJ

THORBJORN RAVNAAS KRISTIANSEN

76

RESEARCH-INFORMED LITERATURE

 An excellent number of very high quality sources used (bar Linus) - you obviously took on board my feedback from the previous assignment. Very good work here.

24

KNOWLEDGE AND UNDERSTANDING

 Good evidence of knowledge and understanding. A detailed, well-researched report.

20

ANALYSIS

 Good synthesis of material - again, taking on board the feedback from the first assignment. Good conclusions drawn, I especially like the advice in the "further reading" section, which is spot on.

22

PRACTICAL APPLICATION AND DEP.

 N/A - no marks assigned.

SKILLS FOR PROFESSIONAL PRAC.

 A well-written report with only a few minor style/grammar errors. Nicely presented, though presenting some of your data as tables or images'll help cement a few points and break up the walls of text a tad.

10