

E_RUSSELL_P151512

by Edward Russell

FILE	2659_EDWARD_RUSSELL_E_RUSSELL_P151512_113613_1434247137.D OCX		
TIME SUBMITTED	21-MAY-2018 03:50PM (UTC+0100)	WORD COUNT	2839
SUBMISSION ID	89667834	CHARACTER COUNT	16035

Network Operating Systems and Security

Network security

Tim Bashford

Ted Russell
5-19-2018

Contents

Abstract	2
Introduction	2
Denial of Service	2
ARP Spoofing.....	3
Packet Sniffing	3
Password Cracking	4
Malware	5
Conclusion	5
Bibliography	6

Abstract

The aim of this report is to outline and explain several possible risks that can affect modern computer networks. It will cover the risks, what they do and how they do it, along with some methods of mitigating the damage or preventing the risks.

Introduction

As there is an ever-increasing flood of Internet of Things (IoT) devices to the market, there is also an increasing rate of security challenges across these devices [1]–[3]. These can vary in the potential damage that they can cause, from temporary loss of accessibility to private or confidential information being leaked. These can be extremely damaging in nature to either the network itself, the data on it, or the reputation of the company in some situations. As such they must be considered and protected against when a computer network is created.

Security attacks such as Denial of Service, Password cracking or ARP Spoofing are common and well documented. As such many of them have a variety of methods available to detect, mitigate and/or prevent them. Several of these security attacks, including those just mentioned, will be covered in the following sections, along with examples of solutions for each of them.

Denial of Service

Denial of Service, often known as DoS attacks, are designed to render the affected service inaccessible [4]. The affects that are seen depend entirely on your perspective. For example, it could appear that the site you are trying to view has stopped displaying content if you are a customer, however if you are a business it could mean that some or all of the systems you rely upon have stopped responding [4]. These attacks can occur through legitimate use in some cases such as during Black Friday sales, however it can also be malicious.

There are two types of DoS attack, Bandwidth Depletion and Resource Depletion. Bandwidth Depletion occurs by sending a considerable number of seemingly legitimate data packets to the target and by doing so uses up its network bandwidth. This leaves the network unavailable for legitimate traffic [2], [5]. This method can be split into Flood and Amplification attacks. Flood attacks send a great volume of IP traffic to the target machine restricting its available network resources. Amplification attacks instead exploit the *broadcast IP address feature* in routers. A packet is sent to the broadcast IP address of a network and this causes all hosts to send a reply to the target [1], [2], [5].

A Distributed Denial of Service attack is similar to a normal DoS attack. The key difference is with a DDoS attack, it occurs from multiple sources. If the attacker can organise a large quantity of systems to connect to the same website (often via a Trojan) simultaneously, it can push the server beyond its maximum capability, denying any further connection.

DDoS attacks can attack through different layers of the TCP/IP model. This means that they are classified as either Network Level or Application Level. In a Network level attack, the Network or Transport layer protocols are utilised to

deny the access to the target services. Application level attacks exhaust the target's resources using Application layer protocols [2].

Mitigating the damage from a Denial of Service attack can be done in several ways. One method is through the use of Honeypots. These effectively act as an 'intrusion deception device' and are designed to emulate a system connected to a network to lure in the malicious parties. This allows Honeypot systems to be attacked and as important data, applications and services are stored elsewhere there is a negligible impact [3].

ARP Spoofing

Address Resolution Protocol (ARP) is an unauthenticated and stateless layer 3 protocol which can be used as a tool for an attack into a local area network (LAN) [6]–[8]. It is used to resolve a MAC address of a host to the relevant IP address. This is achieved by sending a broadcasted ARP request packet. All hosts have a cache containing all of the address maps that have been learnt from the network or configured. ARP Spoofing is a process which forges ARP packets to impersonate a host on a network [7].

ARP spoofing allows attackers to further attack the system by launching DoS or Man in the Middle (MiTM) attacks. A MiTM attack is when the attacker poisons the ARP cache of two linked devices with the MAC address of the network interface card. This results in both caches sending their data packets to the attacker when attempting to communicate with the other device [9]. This allows the attacker to go through any data that is being exchanged and it can generally be achieved without the hosts being aware [6]. During this attack however, it is possible for the MiTM host to modify the content of any traffic, this could be in the form of filtering, injecting commands or malicious code [10].

This can be countered in a variety of ways, one such way being replacing the ARP protocol with Secure ARP Protocol [7]. S-ARP extends the original ARP by integrating an integrity/authentication scheme for replies, this can prevent poisoning attacks. It is built upon ARP so the specification (cache, timeout etc) still utilises the original ARP [10]. It is still compatible with the insecure ARP as an additional header is added at the end of the standard protocol method to carry the authentication data. However, to maximise the security it should not be used with the insecure ARP, even though it is possible [10].

Another viable method for protecting against ARP Spoofing is utilising Static MAC entries. By assigning static MAC addresses to every host will prevent spoofing. The downside to this is that it is extremely unscalable as the quantity of entries to manage can be great [7]. It is also less desirable in a workplace where mobile hosts, e.g. Laptops, are introduced to the network on occasion.

Packet Sniffing

A packet sniffer is hardware or software that is used to monitor network traffic. They are also known as a packet analyser, protocol analyser or network analyser. They examine data packets that are sent between computers on a

network or over the wider internet [11]. They are also able to store packet details for later examining.

There are two main types of packet sniffers. Promiscuous mode and monitor mode. In promiscuous mode all of the data packets, regardless of destination, can be captured silently by the Network Interface Controller. In Monitor mode, the packets are checked without connecting to an access point [12]. They can be used for a variety of reasons, not all negative. These can include logging network traffic, analysing network performance or retrieving user-names and passwords [13]. Once in place, any data received can be sent to a command and control server for analysis. From there it is possible for attackers to undergo a MITM attack or attempt packet injection [11].

There are a number of ways of detecting a packet sniffer on the network, it is even possible to stop them working. To detect a packet sniffer a packet can be generated containing an invalid address. If any computer on the network accepts the packet then that computer is carrying a sniffer [13]. Another method for detecting packet sniffers is using the Simple Network Management Protocol (SNMP). This allows network managers to locate problems on the TCP/IP internet, it is also possible to log connection and disconnections to ports and gather statistics such as packets received. This can be analysed and can determine whether there is a packet sniffer on the device [13].

To protect against packet sniffers, you can configure a packet switched network. With this set up, each device is connected to a central hub. Packets are then transferred from one line card to another preventing sniffers running on a single machine from intercepting the data packets. Another solution is the encryption of data before it is transmitted. This will prevent the data packet from being read but will not prevent the sniffer from functioning [13].

Password Cracking

Passwords are universally used as the most common form of user authentication with modern computing. There are multiple ways of password cracking, two such methods are brute force and dictionary attack. Typically password cracking runs a cracking software such as JtR-J or Hashcat against a file, trying to find all of the matches for the hashes that constitute the password [14], [15].

Brute force password cracking relies on trial and error to decode passwords and other encrypted data. It requires large amounts of computational power to undertake this task [16]. This is generally only suitable for shorter passwords and works by hashing all available messages. The time taken depends entirely on the length of the messages and the character set making it up [17].

Dictionary attacks however, use large dictionary files containing millions of combinations of common words and passwords [18]. The hash value of each word in the dictionary file is compared to the hash value of any unknown password, if a match is found then the plain text is revealed showing the password.

Protecting against password cracking, whether it be brute forcing or dictionary attacks, is achievable in a variety of ways. Firstly hashing passwords, this

involves putting passwords through a hashing algorithm, the result of which is stored in a file [14]. There are a variety of hashing algorithms out there, some examples are MD5, Sha-1 or NTLM. These algorithms turn the password into a fixed-length string of characters, a "fingerprint", this is a one way process [14].

Another method for protecting against password cracking is simply having a stronger password. A password that utilises letters, both lower and upper case, numbers and symbols is considered to be a strong password, stronger still if it avoids dictionary words. A strong password combined with hashing as mentioned above will be more effective than a weak password combined with hashing [18].

Another common measure against password cracking is a salt. This appends a randomised string to the end of the password and is then hashed along with the password [14]. This means that the hash generated for two users with the same password will be different.

Malware

Malware is a common threat to any computing system, whether it is an individual system or a network. There are several types of malware, the most common are viruses, worms and trojans.

A virus replicate themselves into a program and transfer themselves from one computer to another spreading the infection [19], [20]. They are generally connected to an executable file, meaning they won't activate until the relevant .exe file is accessed. They have a variety of affects, some can be minor annoyances whereas some can damage data or results in a denial of service.

Computer worms are similar to viruses as they replicate themselves and have a similar impact, however, unlike viruses they do not require another program to run as they are standalone [19]. They spread by exploiting a system vulnerability or by tricking the users to run them.

Trojans are harmful software than appears legitimate, because of this apparent legitimacy they are able to trick users into loading and running them. Once loaded it can do a variety of attacks from pop up windows to deleting or encrypting files. One example of a trojan is the Cryptowall trojan [19].

Any of these forms of malware can enter a system though varied means such as a mistake in the firewall or an infected link clicked by an unaware employee. In a network that is fully connected, one machine getting infected with a form of malware opens up the entire system to the hidden threats [21].

With the commonality of malware such as viruses, worms and trojans however, comes a reprieve. There is a plethora of anti-malware software available that is compatible with almost every device [22]. These can allow a system to be regularly checked for all types of malware, many of which can be removed by the software if they are detected.

Conclusion

There are a variety of risks that can affect a computer network from Denial of Service attacks to packet sniffers to password cracking. Denial of service

attacks prevent legitimate users from accessing websites or aspects of a system whilst ARP spoofing can result in either a DoS or a MiTM where an external system is able to inspect any data packets sent between two systems on a network. ARP and packet sniffing are similar in this aspect as both can result in a loss of privacy if the data packets are not encrypted before transfer. Password cracking can result in large security breaches if an important password is cracked through brute force or a dictionary attack. Malware is a common issue that could cause some extremely damaging and costly issues for a network however it is easily solved through some anti-virus software and extra precautions. All of these issues can cause major concerns and issues for computer networks, however all of them have solutions that can be easily implemented to either prevent, mitigate or prepare for any impact they might have.

Bibliography

- [1] V. Adat, A. Dahiya, and B. B. Gupta, "Economic incentive based solution against distributed denial of service attacks for IoT customers," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 2018, pp. 1–5.
- [2] M. De Donno, A. Giaretta, N. Dragoni, and A. Spognardi, "A taxonomy of distributed denial of service attacks," in *2017 International Conference on Information Society (i-Society)*, 2017, pp. 100–107.
- [3] D. C. Grant, "Distributed detection and response for the mitigation of distributed denial of service attacks," in *2018 International Conference on Information Networking (ICOIN)*, 2018, pp. 495–497.
- [4] National Cyber Security Centre, "Understanding denial of service (DoS) attacks," *National Cyber Security Centre website*, 2018. [Online]. Available: <https://www.ncsc.gov.uk/guidance/understanding-denial-service-dos-attacks>.
- [5] W. Navid and M. N. M. Bhutta, "Detection and mitigation of Denial of Service (DoS) attacks using performance aware Software Defined Networking (SDN)," in *2017 International Conference on Information and Communication Technologies (ICICT)*, 2017, pp. 47–57.
- [6] R. R. Saini and H. Gupta, "A security framework against ARP spoofing," in *2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions)*, 2015, pp. 1–6.
- [7] V. Ramachandran and S. Nandi, "Detecting ARP Spoofing: An Active Technique," Springer, Berlin, Heidelberg, 2005, pp. 239–250.
- [8] B. Scott *et al.*, "An interactive visualization tool for teaching ARP spoofing attack," in *2017 IEEE Frontiers in Education Conference (FIE)*, 2017, pp. 1–5.
- [9] CISCO, "ARP Poisoning Attack and Mitigation Techniques - Cisco," *CISCO Website*, 2016. [Online]. Available: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500->

series-switches/white_paper_c11_603839.html. [Accessed: 20-May-2018].

- [10] D. Bruschi, A. Ornaghi, and E. Rosti, "S-ARP: a secure address resolution protocol," in *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, pp. 66–74.
- [11] Kaspersky Lab, "What is a Packet Sniffer? | Kaspersky Lab US," *Kaspersky lab Website*. [Online]. Available: <https://usa.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer>. [Accessed: 20-May-2018].
- [12] P. Goyal and A. Goyal, "Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark," in *2017 9th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2017, pp. 77–81.
- [13] S. Ansari, S. G. Rajeev, and H. S. Chandrashekar, "Packet sniffing: a brief introduction," *IEEE Potentials*, vol. 21, no. 5, pp. 17–19, Dec. 2002.
- [14] J. A. Chester, "Analysis of Password Cracking Methods & Applications."
- [15] S. Ji, S. Yang, X. Hu, W. Han, Z. Li, and R. Beyah, "Zero-Sum Password Cracking Game: A Large-Scale Empirical Study on the Crackability, Correlation, and Security of Passwords," *IEEE Trans. Dependable Secur. Comput.*, vol. 14, no. 5, pp. 550–564, Sep. 2017.
- [16] I. L. S. Hendarto and Y. Kurniawan, "Performance factors of a CUDA GPU parallel program: A case study on a PDF password cracking brute-force algorithm," in *2017 International Conference on Computer, Control, Informatics and its Applications (IC3INA)*, 2017, pp. 35–40.
- [17] A.-D. Vu, J.-I. Han, H.-A. Nguyen, Y.-M. Kim, and E.-J. Im, "A homogeneous parallel brute force cracking algorithm on the GPU," in *ICTC 2011*, 2011, pp. 561–564.
- [18] J. Jose, T. T. Tomy, V. Karunakaran, Anjali Krishna V, A. Varkey, and Nisha C.A., "Securing passwords from dictionary attack with character-tree," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2016, pp. 2301–2307.
- [19] CISCO, "What Is the Difference: Viruses, Worms, Trojans, and Bots? - Cisco," *CISCO Website*. [Online]. Available: <https://www.cisco.com/c/en/us/about/security-center/virus-differences.html>. [Accessed: 20-May-2018].
- [20] M. Rafiq, M. S. Arif, A. Raza, and M. O. Ahmad, "Numerical modeling of virus outbreak in a computer network with limited anti-virus ability," in *2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 2018, pp. 415–421.
- [21] E. Jennings, "Securing Data Centers, Handheld Computers, and Networked Sensors against Viruses and Rootkits," in *2017 IEEE International Conference on Rebooting Computing (ICRC)*, 2017, pp. 1–8.
- [22] Kaspersky, "Computer Viruses vs. Network Worms | Kaspersky Lab US," *Kaspersky lab Website*. [Online]. Available: <https://usa.kaspersky.com/resource-center/threats/computer-viruses-vs->

worms. [Accessed: 20-May-2018].

FINAL GRADE

GENERAL COMMENTS

Instructor

70/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

GRADING FORM: SMU GENERIC_GJ

EDWARD RUSSELL

70

RESEARCH-INFORMED LITERATURE



A good number of generally high-quality sources used. Some are incomplete - e.g. #14. You're a bit too close to the source material in a few places, especially in the ARP spoofing section.

18

KNOWLEDGE AND UNDERSTANDING



Good evidence of knowledge and understanding. You obviously have some previous knowledge in this area.

22

ANALYSIS



Some reasonable analysis - evidence of synthesis and a modest conclusion included.

19

PRACTICAL APPLICATION AND DEP.



N/A - no marks assigned.

SKILLS FOR PROFESSIONAL PRAC.



A well-written report. You might consider including a few relevant images or tables to illustrate your points and break up the walls of text.

11