Manchester Metropolitan
University

Secure Network Design

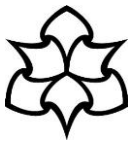
Student name: Karan Nihalani

Student id: 17023122

Unit: Information and Network Security (6G6Z1112)

Department of Computing and Mathematics

Manchester Metropolitan University



Abstract:

This proposal is meant to present a secure network design proposal for a multinational financial company. Further on, we will dive in deeper into the potential security problems and vulnerabilities the system might encounter, judging from the current proposed network design, provided by the IT department technician and what attacks these vulnerabilities can be led to. In addition to this, some proposed security solutions to these vulnerabilities and attacks will be explored, with an attempt to mitigate these in the future and employ these solutions in the network design itself. Furthermore, making use of these solutions, an enhanced and improved secure network design will be presented for the company to review, with the purpose of improving the company's security aspects.

Keywords:

Vulnerability, attack, security, solution, DNS, IPSec, DoS, mitigation

Table of Contents

1. Critical Analysis

- **Vulnerability 1:**
  DNS servers used is a vulnerability as users on the system would trust the host-address mapping provided by the DNS itself, leading to the disadvantage that requests can be intercepted. If the DNS servers are compromised or hijacked, the responses from the server can be malicious or erroneous.
- **Attack 1:**
  An attack performed could be DNS Cache Poisoning, where the goal of the attack is to "divert Internet traffic away from legitimate servers to fake ones" (C. Hoffman, 2017) and the attacker could have the capability of forcing the DNS server in re-directing users to an incorrect and malicious IP address, if they have control of the DNS' cache.
- **Vulnerability 2:**
  A second vulnerability within the system is the fact that FTP is used to share files through an FTP server, where FTP does not make use of encryption when transferring data.
- **Attack 2:**
  An attack that can exploit this issue is packet sniffing or packet capture via a man-in-the-middle attack and due to the idea that data being transferred is not being very well protected, the 'packets' being transferred from one place to another can be "susceptible to eavesdropping and even modification" (J. Watson, 2018). This type of attack can be shown represented below (**Fig. 1**).

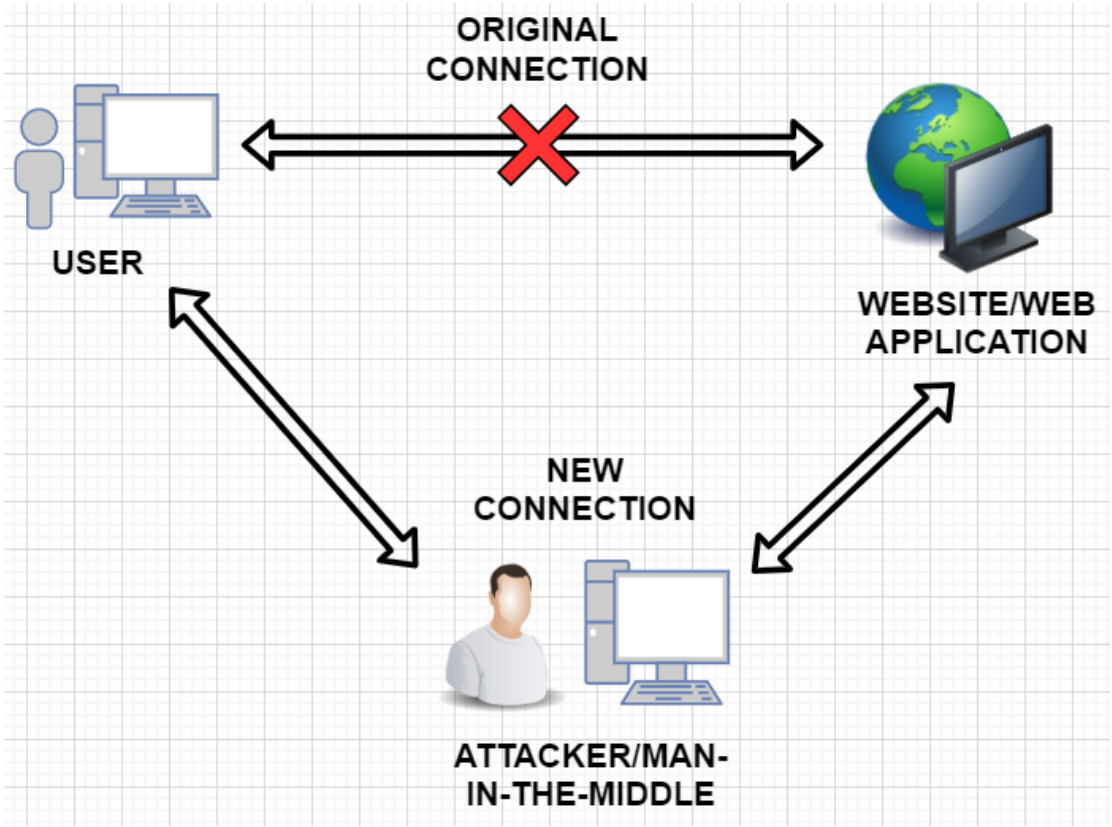


Fig. 1

- **Vulnerability 3:**
  A free AVG Antivirus is installed on all of the local machines, which turns out to be very vulnerable for all of the systems and because it is free, it misses out on other key features it would have if the antivirus would be paid for, e.g. no safe bank transactions or payments. Other vulnerabilities can lead to attacks, as well.
- **Attack 3:**
  One attack would be DLL injection or a "code injection vulnerability", where an attacker would be able to "bypass a self-protection mechanism" (CVE Details, 2017) and take control over the AVG process.
- **Vulnerability 4:**
  A vulnerability here would be the use of the Internet through a basic broadband router provided by their ISP, where "most LANs interconnected on the Internet today are highly insecure and do not follow any essential outline for security" (IEEE Xplore Digital Library, 2003), suggesting the eventual lack of protection of confidential data.
- **Attack 4:**
  A potential attack would be 'wiretapping'. Even though it isn't as common, it can still be a problem when dealing with ISPs, as telecommunications on the Internet can be intercepted secretly.
- **Vulnerability 5:**
  The use of packet-filtering firewalls. They are not safe for many types of attacks and can be vulnerable for other, e.g. TCP SYN floods and IP spoofing. These cannot prevent attacks from the application layer either.
- **Attack 5:**
  An attack employed would be a DoS attack. As this type of firewall isn't able to perform authentication information, it not being a layer 7 (Application) process, they can take place. In these attacks, hosts or users aren't able to access a device, information system or service due to an attacker typically "flooding a network server with traffic", directing a large amount of "requests to the target server, overloading it with traffic" (CISA, 2009). Below, you'll be able to observe a simple DoS attack diagram (**Fig. 2**).

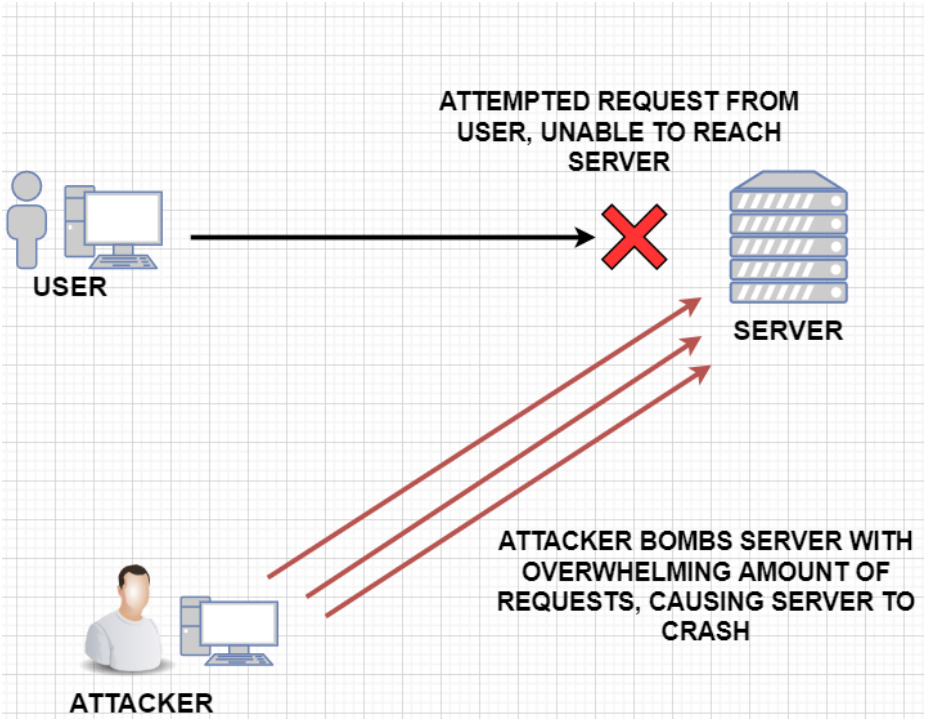


Fig. 2

2. Secure Network Design Proposal

2.1 Proposed Security Solutions

- **Solution 1:**

  DNS cache poisoning was the first attack mentioned above and the solution would be to upgrade the DNS with security to DNSSEC, which is a security extension to the DNS protocol. This allows for strong authentication, using "digital signatures based on public key cryptography" (ICANN, 2019). The reason why this was chosen over other remedies is due to the fact that it is DNS metadata that is signed by the person who owns the data. The solution is deployed at the root level, as that is where IP addresses and the domain names are stored and is located in both the headquarters and branch offices.

- **Solution 2:**
  Packet sniffing is the second attack and the solution to this would be to make use of cryptography, which would make packet sniffing irrelevant, therefore suggesting that it becomes the most adequate solution for this attack. Cryptographic protocols for network security include SSL and SSH protocols, where both "offer data-in-motion encryption, server authentication, client authentication, and data integrity mechanisms" (JScape, 2016). These protocols are said to be operating on the TCP port 22 by default, found at the Transport Layer of the OSI Model and would be used at both the headquarters and the branch offices.
- **Solution 3:**
  The third attack mentioned was DLL injection through malware, which would bypass the self-protection mechanism and take control of the AVG process. A solution to this would be to make use of "whitelisting tools" or Software Restriction Policies, to block and prevent access to malicious software that could contain these DLL injections. This solution would be installed on the Application layer, as it is normally found within the User's files and configuration. To add to this, it would be installed on all of the computers, both headquarters and branch offices.
- **Solution 4:**
  The fourth attack that was presented is 'wiretapping.' The proposed solution for this is to preinstall a software security solution that would allow for secure communications which make use of the ISP. An example on the market would be *Secusmart*, allowing "end-to-end encryption of voice calls and text messages" (Secusmart, 2020). It would be installed in the transport layer and physically, in the branch offices. This is because the servers would be set up and users/employees would be able to receive a key to activate the software.
- **Solution 5:**
  The final attack mentioned was a DoS attack. The solution to this would be to employ IPSec (Internet Protocol Security), which is designed to provide security "through authentication and encryption of IP network packets" (TechTarget, 2020). The subprotocol used or protocol used is IP itself, except it is made secure through forms of authentication and the solution is deployed at the Network layer itself, as it works in "tunnel" mode (with VPNs) and in "transport" mode (for end-to-end). This would be used at headquarters and branch offices alike.

2.2 Additional Requirements

- **Authentication:**
  This requirement is already discussed above, as it is covered by solutions 1 and 5, dealing with DNSSec and IPSec.
- **Access Control:**
  Access Control is able to determine what operations a certain "subject" has for a specific set of "objects." There are various models used as a solution for different attacks and vulnerabilities. DAC (Discretionary Access Control) and MAC (Mandatory Access Control) are common, where in DAC, the user is able to define the access policy and in MAC, the system does this

instead. These would be found within the Network Interface layer and would preferably be used in both the headquarters and branch offices.

- **Secure Connection & Remote Access:**
  To prevent risks with remote access and issues with secure connections, IDS (Intrusion Detection Systems) can be employed. It can be a device or software which "assumes that a system will not be secure, but violations of security policy (intrusions) can be detected by monitoring and analyzing system behaviour" (Association for Computing Machinery, 1998). The IDS would normally be located, along with a firewall at the Transport Layer, inspecting the network's activity. The IDS would be used on the employee's computers in the branch offices and the headquarters.
- **Adequate Attacks Detection & Mitigation:**
  To be able to detect adequate attacks, we would be to manage patches by regularly updating software and to employ secure configuration at all layers. This is to "restrict the functionality of every device, operating system and application to the minimum needed for business to function" (National Cyber Security Centre, 2018). This should be applied to every single system in the headquarters, as well as, the office branches.
- **Efficient Solution for DDoS:**
  IPSec was proposed as an efficient solution for both DoS and DDoS attacks, as mentioned in solution 5.

2.3 Cost-effectiveness Justification

The proposed design as seen below is deemed as cost-effective, as some of the solutions above can be achieved for free. Examples include, frequently updating the systems to manage patches and deploying Software Restriction Policies. Another reason the design is cost-effective is due to the security policies implemented within, which allows the network to be an upgraded version of the design proposed by the IT department technician. As you can see in the figure below, the layout of the network remains as a hierarchical one, yet it implements all the security measures proposed above. One of the completely new additions is the use of the *SecuSmart* software for monitoring purposes.

The diagram is found on the next page (**Fig. 3**).

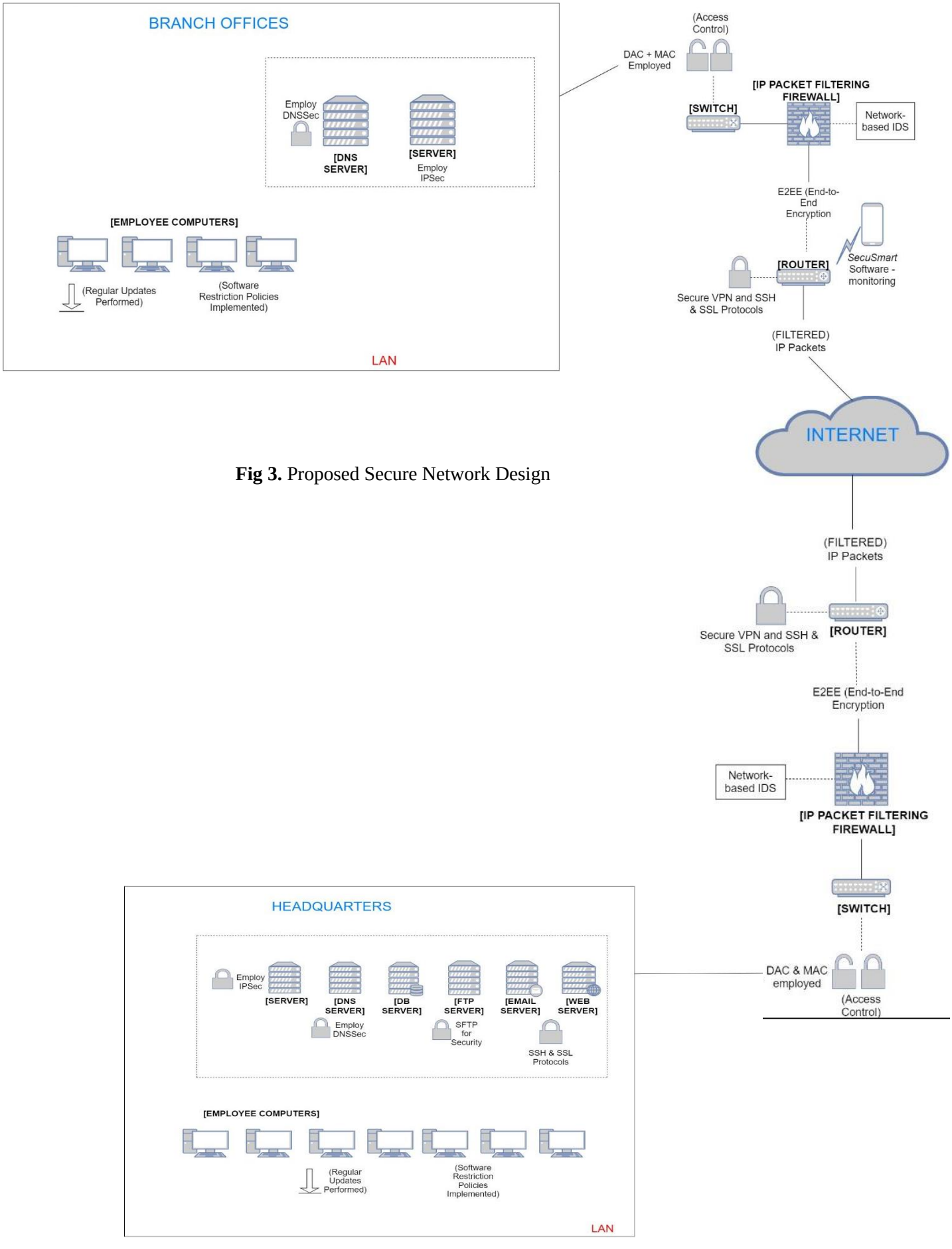


Fig 3. Proposed Secure Network Design

3. Conclusion

In conclusion, it is made clear of the potential risks an unprotected network design can propose, from DoS attacks and DLL injections to packet sniffing attacks, causing a leak in data. Therefore, the purpose of the new secure network design that is proposed is to essentially provide more layers of security protocols and protection to the network, as a whole, from the branch offices to the headquarters. The benefits of providing such as secure design are that the company would have to worry much less about potential threats and improving their network now would mitigate future attacks. Furthermore, personal and confidential data is protected, enhancing the trust of employees within the company and clients outside the company, which can surely lead to increased productivity and profits for the entire company, itself.

4. References

[1] Chris Hoffman, 2017 "What is DNS Cache Poisoning?" [Online] [Accessed on 18th February 2020]
https://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/

[2] Jon Watson, 2018 "What is packet sniffing and how can you avoid it?" [Online] [Accessed on 29th February 2020]
https://www.comparitech.com/blog/information-security/what-is-packet-sniffing/

[3] CVE Details, 2017 "Vulnerability Details : CVE-2017-5566" [Online] [Accessed on 29th February 2020]
https://www.cvedetails.com/cve/CVE-2017-5566/

[4] IEEE Xplore Digital Library, 2003 "Vulnerabilities of ISPs" [Online] [Accessed on 29th February 2020]
https://ieeexplore.ieee.org/document/1238687

[5] CISA (Cybersecurity and Infrastructure Security Agency), 2009 "Understanding Denial-of-Service Attacks" [Online] [Accessed on 29th February 2020]
https://www.us-cert.gov/ncas/tips/ST04-015

[6] ICANN, 2019 "DNSSEC – What Is It and Why Is It Important?" [Online] [Accessed on 11th March 2020].
https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

[7] JScape, 2016 "SSL vs. SSH – A Not-So-Technical Comparison" [Online] [Accessed on 11th March 2020].
https://www.jscape.com/blog/ssl-vs-ssh-simplified

[8] Secusmart, 2020 "SecuSUITE for Government" [Online] [Accessed on 20th March 2020]
https://www.secusmart.com/en/home/produkte/secusuite-government

[9] TechTarget, 2020 "IPSec (Internet Protocol Security)" [Online] [Accessed on 20th March 2020]
https://searchsecurity.techtarget.com/definition/IPsec-Internet-Protocol-Security

[10] Association for Computing Machinery, 1998 "Intrusion detection using sequences of system calls" [Online] [Accessed on 20th March 2020]
https://dl.acm.org/doi/10.5555/1298081.1298084

[11] National Cyber Security Centre, 2018. "Common cyber attacks - reducing the impact" [Online] [Accessed on 20th March 2020]
https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/introduction-to-cyber-security/common-cyber-attacks-reducing-the-impact