

Information and Network Security

6G6Z1012

Joshua Michael Ephraim Bridge
joshua.m.bridge@stu.mmu.ac.uk
14032908

March 14, 2018

Abstract

Keywords— LAN - Local Area Network, DNS - Domain Name System

1 System Analysis (Vulnerabilities & Attacks)

1.1 Insecure IP packets

At the moment, the branches communicate to the headquarters over the internet in an insecure way. As the packets being sent over the internet are not protected, anyone could read the contents of these messages and potentially use them to attack the system. Any router or system that lies in the network path between each branch and the headquarters could intercept any message sent between them and possibly modify, remove or replay that message.

Replay Attack The current network is very susceptible to a replay attack with its user/password system. As there is no underlying security protocol to protect messages over the internet, a packet sniffer could be used to listen for a valid sign-in message and then that message could be re-sent by an attacker to gain access to the system.

1.2 Unprotected Web Server

The current web server is serving public clients with unprotected HTTP traffic, which is easily exploitable and a very critical vulnerability when the company is dealing with financial information. Attackers can easily trick clients in a multitude of ways into sending personal information to attacker-controlled servers.

Man-in-the-middle Attack While on an unencrypted public wifi hotspot, a user may try to access the website while an attacker intercepts this unprotected traffic. The attacker could then replace the response with their own malicious server page where the user might enter personal information.

1.3 Internal Access Control

A major issue with the current network layout is that all devices in each location are grouped together within the same LAN, so any computer/server can access every other computer/server. There is no access control which could prevent resources being accessed by users who should not be able to.

Internal Malicious Access Either an employee with internal network access or an outside attacker who has gained access to the network is able to access all of the resources within any location. This allows the possibility of a whole host of attacks such as offline dictionary attacks & DNS cache poisoning.

1.4 User/Password Authentication

A user/password system is unsuitable for secure authentication when connecting over the internet. Usernames and passwords for users are often very simple for the sake of being able to remember them, therefore this makes them much more susceptible to being guessed by an attacker.

Dictionary Attack If an attacker manages to get hold of the endpoint used for login, then they can start using dictionary attacks to try and guess username/password combinations. This is possible due to the lack of authentication for which devices can log in to the company system.

1.5 Unprotected DNS

The DNS server at the headquarters is currently located within the same LAN as the public facing servers and the office workstations. Therefore if any of these devices were to be compromised then the DNS server is very susceptible to being attacked.

DNS cache poisoning Due to the current network design, once an attacker has gained entry to an employee computer via either a Replay or Dictionary attack it is possible to then reach the DNS server via the LAN and poison its cache. It would therefore be possible to redirect any authentication traffic to an attacker-controlled server and collect the passwords of every user that tried to log in while the cache is poisoned.

2 Design Proposal

References