Assignment 3  
  
SENG2250

Sam Dolbel – 3130069

# Network Security

# When an employee is away from the business, they need to establish a secure connection to the company server. Depending on the key exchange protocol used for the client-server connection, the connection may be vulnerable to a **Man-In-The-Middle** attack. The main way to prevent a MITM attack is to prevent malicious users from entering access points in the first place. Strong protection/encryption on router access points can prevent attackers from working, as can Public Key authentication like RSA.

# Since the bank is dealing with sensitive financial information, customers and employees will be required to use secure passwords to protect themselves. Passwords are susceptible to a few attacks, the simplest being the **Brute Force** attack, where the attacker attempts to guess the password. Brute force attacks rely on being able to attempt millions of passwords in a short space of time. This is generally curtailed by imposing limits on how many wrong guesses the user can make. In this solution, the account is locked if more than a small number of wrong guesses are made, whether for 24 hours or indefinitely.

# The customer services themselves are vulnerable to a **DDoS (Distributed Denial of Service)** attack. This means that the bank’s servers can be overwhelmed with malicious traffic from bots, blocking customers and employees from using vital services. The current solution to this attack is to employ anti-DDoS protection services like Cloudflare. These services detect suspicious traffic and block bots, keeping the server connection clearer.

# To begin, this process should only be performed internally. Ideally, the process should be blocked to all users outside the network/IP. Without the added risk of establishing a secure external client-server connection, this curtails the danger of outside attackers Sniffing or performing a Man-In-The-Middle attack. This also means there should be no Back Door. Next, the employee should input their credentials; user name and password. A secure, difficult-or-impossible-to-guess password will prevent access via a Dictionary attack, and wrong answer limitations prevent a Brute Force attack. Only with this two-factor authentication will the user be granted access. Finally, the user will attempt to perform the action. Although the user has input the right credentials, they still need to be authorised – for example, a trainee or intern should have access restricted to some sensitive applications. The user sends their authorisation details to the server for analysis, using a service like OAuth or Kerberos. If the user is authorised, they can successfully update

# **SAML** would be the better option for internal system access and authorisation for an employee. OAuth is ideal for granting limited access to a large external base, making it ideal for social networks and the like. Kerberos is extremely restrictive, forbidding authentication forwarding and forcing encryption even offline. By contrast, SAML provides a single login for multiple applications – once the user is properly authenticated, they have access to all the internal applications. Once the user is authenticated, they can navigate the internal system with efficiency.

# **IPSec** has the advantage of flexibility compared to its compatriots. As a Transport Layer protocol, IPSec can carry many different varieties of data. Additionally, the ability to operate in Tunnel Mode allows IPSec to completely obscure its IP address.

# SSL Handshake Code

 

