Bellevue University

IPSec

Timothy Jelinek

CIS313-T301 Cryptography

10/29/2023

IPSec is known for being a secure network protocol suite that allows private communication. The way this is accomplished is through using a Security Association between the VPN peers. This is accomplished by using a key-based method of encrypting and decrypting data, which is then flowed across the VPN tunnel after the association. If there are flaws with an underlying protocol, then the IPSec is affected, too.

An attack that is known to be used against IPSec is called man-in-the-middle. A man-in-the-middle attack is when an attacker may be able to obtain a weak Pre-Shared key. This attack targets IKE's handshake, which is used for IPSec-based VPN connections. This will lead to a leakage in VPN session data.

Another attack is password cracking. This is used based on how a VPN user sends a password, which is encrypted and then compared with stored values before giving the user access. Using weak passwords in a VPN creates a vulnerability where someone can attack using an offline dictionary or through brute force. To help prevent password cracking, a good idea is to use complex passwords.

A third attack used is a buffer overflow. Attackers are creative and send UDP packets to a system experiencing buffering, allowing them to execute arbitrary code and obtain complete control.

Hackers can take advantage of vulnerabilities within IPSec to decrypt information. An investigative team successfully used an attack called the "Bleichenbacher's Attack" in 2008. This attack is done by purposefully filling an encoded message with errors and then repeatedly sending that content to a server. With the

error-filled messages being sent, a hacker can study the responses the server sends. Through studying the responses, the hacker can gain more and more accurate knowledge about the contents of the encrypted information. When the person gets enough information, they can pretend to be one of the communicating parties and steal data.

There was another research assignment where the investigative group found password-related problems. This study went more in-depth on the ability to find simple passwords easier than complex passwords. When a password is used, it is hashed and compared with stored hashes. Through this study, the researchers found that to prevent users from getting their passwords compromised, it is a good idea to choose extremely complex passwords.

There are some things to keep in mind when creating a more complex password. It is best to use upper and lower letters. You can also include numbers and special characters. It is best to avoid information that is relevant to you, such as birthdates, pets' names, or information easily found on your social media.

Through reading these two articles, I have learned how important it is to have a complex password and how people perform attacks to obtain passwords and other encrypted information stored in IPSec. Watching what I post on social media is also a brilliant idea in order to not give away too much personal information that may be used in one of my passwords. It is best to be careful with the login information you create so that your information does not get compromised.

Sources:

"IPSec Vulnerabilities and Fixes" George, https://bobcares.com/blog/ipsec-vulnerabilities/#:~:text=As%20we%20already%20saw%2C%20IPSec,keys%2C%20it%20can%20decrypt%20connections. Accessed 29 October 2023.

"Security Gaps Found in IPSec" Matthews, https://hackernoon.com/security-gaps-found-in-ipsec-5a075b44609e. Accessed 29 October 2023.