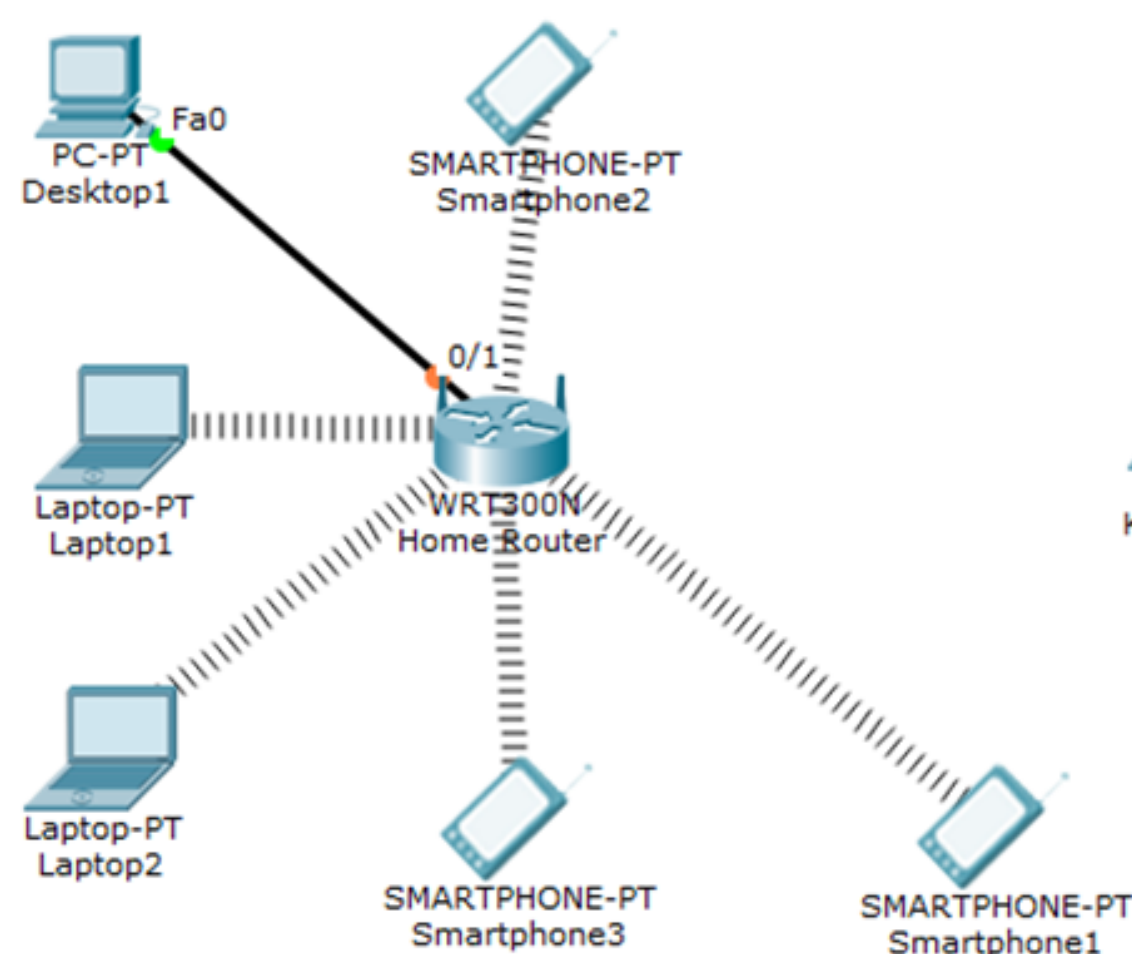


Analysing and Attacking a Typical Home Network

University of Wales Trinity Saint David Swansea
Ryan Joseph - P143413

Introduction

Home networks are so common these days that security is extremely vital [1]. This project looks at the security of a typical home network and how different attacks can be utilized to gain access to the network and steal information from the users on the network. Three attacks were used against the network, including a WPA2 password cracking, a man in the middle attack to steal credentials and a denial of service attack to stop users connecting and communicating within the network. A list of security features are further written up to suggest how a home network user can help prevent and protect themselves from these attacks.



Types of Attacks

WPA2 Brute Force - Uses Fern WiFi Cracker to deauthenticate devices on the network and capture the handshake packet between them. It then brute force attacks the packet and cracks the WPA2 password found inside.

Man in the Middle - Uses ARP spoofing, Site Cloning, DNS spoofing and credential harvesting to capture login credentials from a victim computer. In this case it was stealing login credentials from a user using Facebook.

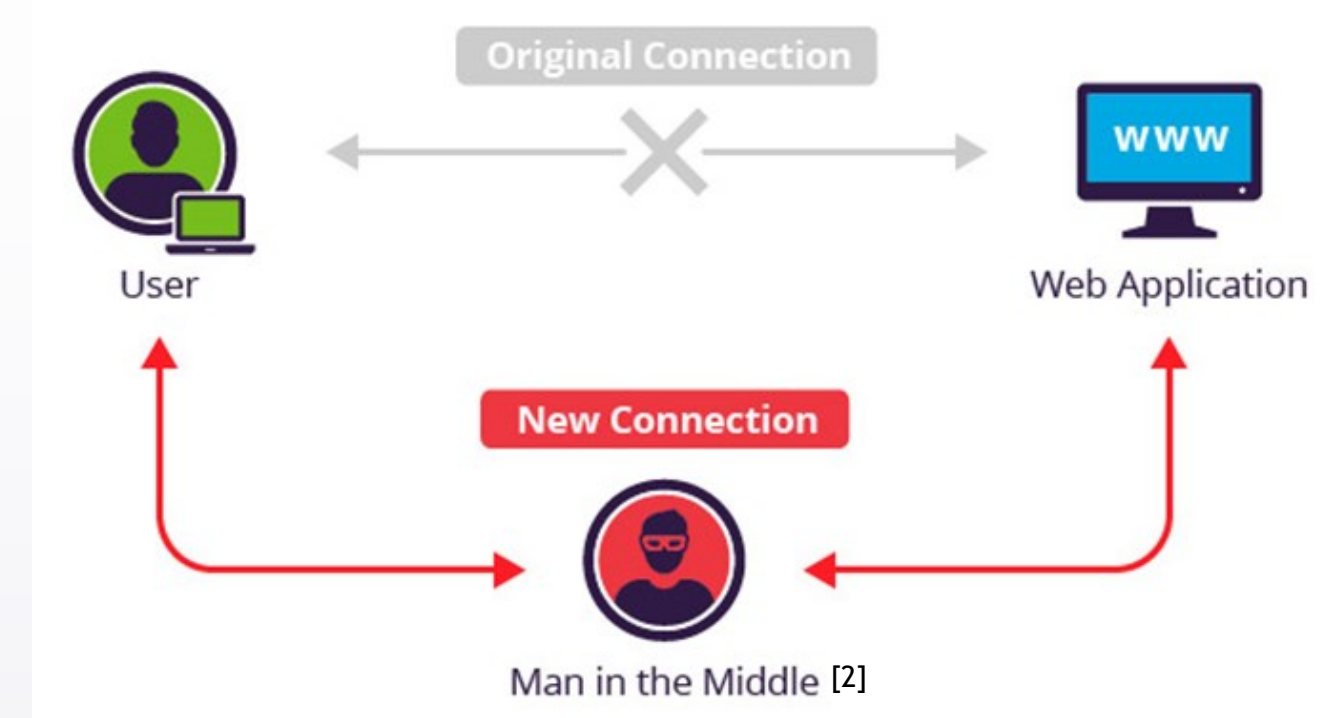
Denial of Service - Uses mdk3 to flood the network with deauthentication packets. This disconnects all users on the network and prevents communication between them or communication to the internet.

Aim

The main aim of this project is to analyse current issues with home network security and analyse how a home network can be breached. Different attacks will be demonstrated to test how efficient they are and how easy they to conduct.

Objectives

- Research into the common security flaws in home networks, the most common attacks to take place to a home network and other common threats to a home network.
- Analyse and compare previous literature and experiments that are similar in nature to this project. From there they can be used to influence this project and the results can be compared back to them.
- Identify the research methods used for this project and analyse how and why they were chosen and used.
- Utilize software to simulate some of the typical hacks that happen on home networks and show how they are carried out.



Conclusion

To conclude, this project as a whole was a success. The original aim and objectives have been addressed fully and all have been completed and achieved. All 3 attacks were carried out and performed successfully. Five passwords tried to be cracked and 3 were successful where 2 were not. This was expected though and was to prove a point showing that complex passwords are harder to crack. Facebook login credentials were successfully stolen and the denial of service attack ensured that all the devices had connectivity issues. From these attacks a security recommendations were drawn up for the reader and they show how a home network user can keep their network secure and safe. The entire point of this project was to show a average home user how easy a home network is to break and access and then suggest ways in which the user can protect their network from attacks. Both these tasks have been accomplished .

References

- [1] Us-cert, "Securing Your Home Network." [Online]. Available: <https://www.us-cert.gov/ncas/tips/ST15-002>.
[2] <https://www.incapsula.com/images/illustrations/web-app-security-mini-site/man-in-the-middle-mitm.jpg>