Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

EXAMINING THREAT FACTORS TO THE COMMON HOME NETWORK FOR CONSTRUCTING MITIGATION STRATEGIES

Author: Timothy Ferfers (1903054)
Supervisor: Dr Kapilan Radhakrishnan
Emil: tim.ferfers@gmail.com

School of
Applied Computing

1. Introduction

This project endeavours to understand the common risks to home networks and the appropriate mitigating actions one may utilise, the habits and choices of home network users in regard to how their network security is managed, and subsequently produce advisory network configurations to benefit the users in such an environment.

2. Aims & Objectives

The **aim** of this project is to examine threats common to home networks from research and through subsequent experimentation, use any findings to provide clear, concise guidelines on the optimal methods to securing a home network.

In order to achieve the aim of this project, these **objectives** must be met accordingly:

- Develop further understanding on home networks possible threats and mitigation.
- Establish understanding of applicable configurations, protocols, and methods to home network environment.
- Provide a literature review of relevant materials.
- Create a simulation for practical testing and examination of findings.
- Assess the effectiveness of certain measures safeguarding networks.
- Consider conventional and alternative security methods.
- Create guidelines advising on optimal home network security.
- Provide a finalised version of the project's guidelines.

3. Research Sources

Various sources including research papers, published journals and books regarding home network security configurations are used to gather information regarding threats of consideration for home networking. Other focuses include average user awareness and optimal home networking configurations [1-5].

4. Design & Implementation

The typical home network consists of multiple devices directly connected to the home router. These connections can be wired but are often established through Wi-Fi. These factors influence the nature of experiments conducted, putting focus the ways in which a home device could be compromised through end devices security failings, wireless risks, and standard encryption flaws.

5. Experiments

There were 3 experiments conducted for this project to ascertain network devices vulnerabilities to certain threats. These include a Man-in-the-Middle attack, testing end devices for the KRACK WPA2 vulnerability and testing home routers WPS feature through brute force attacks. These experiments incorporated various tools, including VirtualBox to host a virtual machine of Kali Linux to carry out the tests and the use of a wireless adapter supporting monitor-mode.

6. Ramifications of Man-in-the-Middle attacks

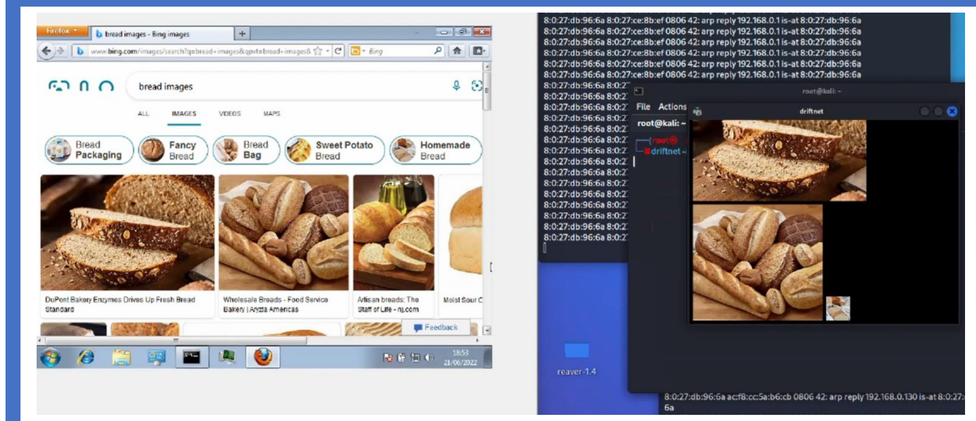

Figure 2: MitM attack where Kali client (right) sniffs images sent to Windows user (left).

Figure 2 shows the successful result of using Driftnet tool in MitM connection (established through ARP spoofing) to eavesdrop images sent to the Windows host, intercepted the Kali client. Using static ARP tables on devices would prevent this form of attack.

7. Exploiting WPS vulnerabilities to crack 8-PIN authentication

```
[+] Trying pin "55555678"
[+] Sending authentication request
[+] Sending association request
[+] Associated with AC:F8:CC:5A:B6:C9 (ESSID: VM8320226)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M1 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[!] WPS transaction failed (code: 0×03), re-trying last pin
[+] 0.06% complete @ 2022-06-19 14:39:37 (0 seconds/pin)
```

Figure 3: Reaver tool attempting new WPS pin at 0.06% completion.

Figure 3 shows the tool Reaver in the process of authenticating with the router but failing WPS negotiations. It was discovered this was due to inbuilt protection on the Virgin Media Hub 3.0 being tested, which used AP rate limiting to prevent the attack upon detection of repeated cracking efforts. This protection signifies the existence of such countermeasures in some home routers.

8. Testing End Devices for Key-Reinstallation Vulnerability

Table 1 shows the outcome of testing 4 devices for different instantiations of KRACK [4]. These results indicate the presence of protection against the Key Reinstallation attack in newer devices, however some older devices were vulnerable.

Device	Vulnerability				
	CVE-2017-13077	CVE-2017-13078	CVE-2017-13080	CVE-2017-13077 (*AM)	CVE-2017-13078 (*AM)
OnePlus Nord	Resilient	Resilient	Resilient	Resilient	Resilient
Samsung Galaxy S5	Vulnerable	Resilient	Vulnerable	Vulnerable	Resilient
SM-T700	Vulnerable	Resilient	Resilient	Vulnerable	Resilient
Amazon Echo Dot 2	Resilient	Resilient	Resilient	Resilient	Resilient

Table 1: Comparison of Result for Testing End Device for KRACK vulnerability.
*AM: Alternative Method for CVE-2017-13077 / CVE-2017-13078.

These devices were tested for:

- CVE-2017-13077: Pairwise encryption key reinstallation in 4-way handshake.
- CVE-2017-13078: Group key reinstallation in 4-way handshake.
- CVE-2017-13080: Reinstallation of the group key (GTK) in the group key handshake

9. Conclusion

This project has successfully outlined optimal methods to securing home networks through consolidation of research findings. These findings are culminated to produce the Advisory Guidelines created for the project report. This document covers various networking considerations for home networks, including:

- Risks of default configurations
- Alternatives to standard WPA2 encryption
- How to limit home network access
- Wireless threats and how to mitigate them
- Further advice for situational measures

Figure 4 shows a sample view of the document's introduction section.

A Guide to Securing your Home Network

Welcome to this comprehensive guide on securing your home network. The rapid growth of home networking and the technologies we use over recent years can make it difficult to keep up to date with modern standards, especially security.

Figure 4: Advisory Guidelines introduction sample

10. References

[1] Justin T. Ho, David Dearman, Khai N. Truong. 2010. "Improving users' security choices on home wireless networks". In Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10). Association for Computing Machinery, NY, USA, Article 12, 1–12.
[2] E. Kritzinger and S. von Solms, "Home user security- from thick security-oriented home users to thin security- oriented home users," 2013 Science and Information Conference, 2013, pp. 340-345.
[3] Rick C, "Secure home working on personal IT" National Cyber Security Centre. UK Gov. May 18, 2020.
[4] Mathy Vanhoef, Frank Piessens. "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2". In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Association for Computing Machinery, New York, NY, USA. 2017.
[5] Mathy Vanhoef. A Security Analysis of the WPA-TKIP and TLS Security Protocols. Ph.D. Dissertation. KU Leuv. 2016.