Summary for the thesis: "Wireless Network Privacy"

2 Summary

In wireless networking, data is transmitted over the air via radio waves, which means anyone with the right equipment can eavesdrop on this data. One of the main research questions that is investigated in the thesis "Wireless Network Privacy" is to what extent this form of communication impacts the privacy of its users. Here, the term "users" may refer to both the companies that deploy wireless networks as well as the clients that connect to it. Given the number of authentication protocols that exist in context of enterprise wireless networks (WPA2-Enterprise), the thesis focuses on these networks in favor of consumer networks, which typically implement WPA2-Personal.

The first part of the thesis describes a case study, which was conducted in order to estimate the current applicability of some known, existing attacks. Particularly, the applicability was determined by non-intrusively perfoming the attacks on various networks. Results from this case study may be useful information to incorporate in the security risk analysis of companies in the ICT domain. For example, the thesis shows that today's success rate of the "Evil Twin" attack is 16%, and that 28% of the EAP users is vulnerable to the "EAP dumb-down" attack.

These figures indicate that the aforementioned attacks are still a threat today, despite their age. It is therefore vital that companies and consumers understand the causes and mitigation strategies for these attacks, so that exploitation by malicious individuals can be prevented. Several mitigation strategies and causes are detailed in the thesis, which can be applied in practice. Finally, a ranking was proposed of all examined WPA2-Enterprise authentication methods based on their security risks. This ranking may be considered by network administrators when choosing an authentication protocol.

The second part of the thesis comprises a feasibility study, which focuses on finding new attacks that could compromise the privacy of wireless network users. Such a new attack was indeed found for WPA2-Enterprise networks that use the PEAP or EAP-TTLS authentication protocol. All Apple devices supporting EAP authentication were vulnerable to this attack at the time.

3 Personal contributions

- A novel vulnerability was discovered in all Apple devices supporting EAP authentication, which allows an attacker to gain immediate unauthorized access to WPA2-Enterprise networks by impersonating an existing user (CVE-2014-4364). The vulnerability was responsibly disclosed to Apple, and fixed in iOS 8 and OS X Yosemite. A paper describing the attack technique was accepted and presented at the ACM WiSec 2014 conference (acceptance rate 26%, overall acceptance rate 26%). The attack left many networks vulnerable, since Apple devices and PEAP / EAP-TTLS authentication are a prevalent combination in enterprise context. Even today, the attack can be exploited on devices that use older versions of iOS or OS X.
- The properties of several EAP methods such as PEAP, EAP-TLS, EAP-TTLS, EAP-GTC, etc. were examined and compared in order to rank them in terms of security.

- Experiments were conducted on several networks in the field in order to determine the success rate of the newly discovered Apple attack, the Evil Twin attack, EAP dumb-down attack, and sslstrip attacks. For this purpose a number of tools were developed: peapwn (proof-of-concept implementation of the Apple attack)[1], hostapd_spoof (hostapd fork to perform Karma attack with many other features), freeradius_spoof (freeradius fork to perform dumb-down attack) and snoopy (Python + Scapy implementation to extract sensitive data such as passwords and EAP credentials).
- Implementation of an optimized brute-force tool for MSCHAPv2 and LEAP challenge responses based on the "asleap" tool.
- Audit of a few high profile websites regarding vulnerability to SSL stripping attacks.
- Implementation of a fake AP / fuzzer using Scapy and Python (prototype.py in the thesis, now scapy-fakeap), which can be used by wireless interfaces in monitor mode[2].
- Determined per OS (Linux, Mac OS X, iOS, Android, Windows 8.1 and Windows Phone 8) which alternative EAP methods are allowed. Such alternative methods could pose a security risk.

4 Contributions to IT security

- The thesis describes the impact of existing attacks. Several mitigation strategies that must be implemented in order to protect against these attacks were proposed. This information can be used by network administrators in order to improve the security of their wireless networks or by security researchers who wish to develop better mitigation strategies.
- The new attack on Apple devices was possible because of several vulnerabilities, some of which could be present / could be introduced in other devices as well. The discovered vulnerabilities provide new insights into the dangers of reusing credentials over different EAP methods and relay attacks. Finally, it is demonstrated how MSCHAPv1 credentials can be used partly in the MSCHAPv2 authentication handshake and why this is insecure.
- Protocol, handshake, and authentication procedure descriptions are freely available via MSDN and RFC documents. However, this information is often fragmented over multiple pages (e.g. the PEAP protocol) and vague. The thesis provides a summary for this information, which could aid researchers who wish to learn about the subject.
- The "scapy-fakeap" tool provides researchers with a flexible fake AP implementation in Python, suitable for fuzzing / discovering new vulnerabilities.

[1] This tool is available on Github: `https://github.com/rpp0/peapwn`
[2] This tool is available on Github: `https://github.com/rpp0/scapy-fakeap`