Secure Wireless Networks, Secure Future

Harinder Singh Mashiana
Applied Science Department, Guru Nanak Dev Engineering College, Ludhiana
email:hsmashiana@gmail.com

Abstract: Breaking away with the myths regarding false sense of security and exposing vulnerabilities in currently implemented wireless networking protocols. The standards are not keeping up with the pace of hackers. They are finding new loopholes everyday and compromising our security. The current standards let hackers monitor data and in some cases even modify it. This paper deals with exposing some of the biggest flaws in our currents standards of encryption and data transfer protocols such as WEP,WPA,TKIP,AES,WPS. IPFIX protocol and its features, abilities and measurement requirements are also provided. The new standards provided by the IETF for IPFIX serve the future of network security.

Keywords: WEP,WPA,AES,TKIP,IPFIX,IETF.

Introduction

With continual advances in technology, coupled with increasing price/performance advantages, wireless accessibility is being deployed increasingly in office and public environments. With this are also increasing the threats to the safety of those networks. The hackers are finding new ways to crack our security systems and get into our secure networks and the standards that are made to stop them are not evolving fast enough with time and some of the most advance and secure systems are failing to be deployed worldwide .If an unauthorized person is able to get access to this network, he can not only spy on us but he can easily mess up our lives. This paper provides the recap of the cryptographic methods and protocols that were earlier considered secure and now are obsolete or so to say because of their still widespread use, also insights into newer better protocols and standards for these protocols and what they have to offer to the future security.

Wired Equivalent Privacy Protocol

Wired Equivalent Privacy (**WEP**) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in 1997.WEP protocol is considered insecure and unreliable after a major flaw was exposed in the protocol but still many enterprises,localbusinesses,home routers use WEP protocol. This ignorance leads to major data leaks. Ten years have passed since this flaw was released. The problem is that WEP uses a user-defined key along with an "initialization vector" (IV) to generate the RC4 traffic key used to encrypt your data. If enough of these IV's can be gathered, then your key can be figured out and your network is now compromised. Therefore WEP should not be used unless a better option is unavailable.

Although major flaws have been exposed in WEP still it is extensively used by enterprises,local business and home routers.So here I have decided to outline few of the many attacks that have come forward exploiting the flaws in WEP.

Summary of WEP attacks:

Key recovery attacks

Table 1.Key recovery attacks

Name	Type	Year	Packets	Ratio
FMS	Statistical	2001	6,000,000(64-bit WEP)	86
KoreK	Statistical	2004	200,000(64-bit WEP)	3
PTW	Statistical	2007	70,000(64-bit WEP)	1

Packet building attacks

Table 2.Packet Attacks

Name	Type	Year	Packets
Chopchop	Fake ARP	2004	1 at the begin(later:injection capture)
Fragmentation	fragmentation	2005	1 at the begin(later:injection capture)
Google replay	replay	2005	1 at the begin(later:injection capture)
Coolface	Man-inthemiddle	2010	0 at the begin(later:injection capture)

WI-FI Protected Access And WI-FI Protected Access 2

WPA and WPA2 are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP.WPA (sometimes referred to as the *draft IEEE 802.11i* standard) became available in 2003.WPA2 became available in 2004 and is a common shorthand for the full IEEE 802.11i standard.

WPA provides users with a higher level of assurance that their data will remain protected by using Temporal Key Integrity Protocol (TKIP) for data encryption. 802.1x authentication has been introduced in this protocol to improve user authentication. WPA2 has features supporting stronger cryptography (e.g. Advanced Encryption Standard or AES), stronger authentication control (e.g. Extensible Authentication Protocol or EAP), key management, replay attack protection and data integrity.

TKIP Exploits

There are two attacks known against TKIP:

- Beck-Tews attack
- Ohigashi-Morii attack (which is an improvement on the Beck-Tews attack)

Both of these attacks only could decrypt small portions of data, compromising confidentiality. What they can’t give you is access to the network. To give you an idea of how much data can be recovered, a single ARP frame would take around 14-17 minutes to get the plain text. Getting useful information with this type of attack is very improbable (but not impossible) considering the rate of recovery.

The only attack known, besides flaws in firmware of some routers, is bruteforcing the WPA key. Generally the key is generated as follows:

Key = PBKDF2(HMAC−SHA1,passphrase, ssid, 4096, 256)

The algorithm takes the type of HMAC to be used, the passphrase, the ssid as salt, the amount of iterations the password will be hashed and the final length of the generated hash. Considering this algorithm is meant to prevent hashed passwords from being broken it can take a huge amount of time. The only reasonable attack would be to use a dictionary attack (hence it is important to use long passwords containing characters, numbers and letters).

Also note that you need to change your SSID to something very random. Rainbow-Tables have been generated for the top 1000 used SSIDs. Which can reduce attack time significantly.

WPA also supports AES (which can be used instead of RC4). While AES is more secure than RC4 the biggest problem of WPA is still present, namely the integrity check is still done using TKIP-MIC.

WPA2 exploits

The few attacks against WPA2:

- Hole196:Hole196 is a vulnerability in the WPA2 protocol that abuses the shared Group Temporal Key (GTK). It can be used to conduct man-in-the-middle and denial-of-service attacks. However, it assumes that the attacker is already authenticated against Access Point and thus in possession of the GTK.
- Predictable Group Temporal Key (GTK):In 2016 it was shown that the WPA and WPA2 standards contain an insecure expository Random Number Generator (RNG).Researchers showed that, if vendors implement the proposed RNG, an attacker is able to predict the group key (GTK) that is randomly generated by the Access Point (AP). Additionally, they showed that possession of the GTK enables the attacker to inject any traffic into the network, and allowed the attacker to decrypt all internet traffic transmitted over the wireless network. They demonstrated their attack against an Asus router that uses a MediaTek wireless chip, and showed the GTK can be recovered within approximately 4 minutes. Vendors can defend against this attack by using a more secure RNG.

TKIP was designed to use with WPA while the stronger algorithm AES was designed to use with WPA2. Some devices may allow WPA to work with AES while some others may allow WPA2 to work with TKIP. But since November 2008, vulnerability 3 in TKIP was uncovered where attacker may be able to decrypt small packets and inject arbitrary data into wireless network. Thus, TKIP encryption is no longer considered as a secure implementation. New deployments should consider using the stronger combination of WPA2 with AES encryption.

Wi-Fi Protected Setup

WPS is a network security standard to create a secure wireless home network.

Created by the Wi-Fi Alliance and introduced in 2006, the goal of the protocol is to allow home users who know little of wireless security and may be intimidated by the available security options to set up Wi-Fi Protected Access, as well as making it easy to add new devices to an existing network without entering long passphrases. Prior to the standard, several competing solutions were developed by different vendors to address the same need.

SecurityIssue

In December 2011 a freelance information security researcher **Stefan Viehböck**reported a design and implementation flaw in WPS that makes it vulnerable to a very basic hacking technique: brute-force attacks, feasible to perform against WPS-enabled Wireless networks. The vulnerability revolves around the acknowledgement messages transmitted between the registrar and enrollee during the validation process of a PIN. The PIN, which is printed on the side label of each WPS-enabled Wi-Fi router,

is and 8 digit number. As the last digit is a checksum of the previous digits,there are seven unknown digits in each PIN, yielding a total of 10^7 = 10,000,000 possible combinations. The first and second halves of the PIN are separately validated and reported by the registrar when an enrollee tries to gain access through the PIN. Now the maximum number of guesses required for PIN recovery is 11,000 (10^4=10,000 from the first half + 10^3=1,000 from the second half). This is a drastic reduction of the orders of degree from the number of PINs that would have to be tested in the absence of the design flaw (i.e. 10^7=100,000,000). The result of this flaw is the presence of a practical attack which can be finished within hours. The difficulty of exploiting this flaw is that it is dependent on the implementation of WPS by the vendor, as Wi-Fi router manufacturers could guard against this attacks by slowing down or disabling the WPS feature after some failed PIN validation efforts.

Almost all major router/AP vendors have WPS-certified devices and WPS–PIN (External Registrar) is mandatory for certification, which makes a lot of devices vulnerable to such an attack. Having a sufficiently long lock-down period (vendor mitigation method) is most likely not a requirement for WPS certification for the device. However it should be a requirement in the new specifications.

Future Security Standards

IPFIX and PSAMP

IPFIX defines a format and a protocol for the export of flow information from routers or measurement probes. IPIFX uses a push-based data export, from IPFIX exporters to IPFIX collectors, and can run over TCP, UDP and SCTP. In the IPFIX protocol, { type, length, value } tuples are expressed in Templates containing { type, length } pairs,specifying which { value } fields are present in Data Records conforming to the Template, giving great flexibility as to what data is transmitted.Since Templates are sent very infrequently compared with Data Records, this results in significant bandwidth savings. Different Data Records may be transmitted simply by sending new Templates specifying the { type, length } pairs for the new data format.

IPFIX isn't just another name for NetFlow v10, it's an open standard that allows vendors to liberate themselves from the constraints of NetFlow. It is the catalyst in networking for the freedom of exportation. In other words, IPFIX is an enabler technology that allows vendors to export any performance detail they can dream up.The IPFIX protocol provides network administrators with access to IP Flow information.Traffic on a data network can be seen as consisting of flows passing through network elements. For administrative or other purposes, it is often interesting, useful, or even necessary to have access to information about these flows that pass through the network elements.

Figure below shows the process of measurement and export of IPFIX and PSAMP data. Core functions are always part of the measurement process.

Optional functions can be placed in the processing sequence for different operations like post processing or data selection.

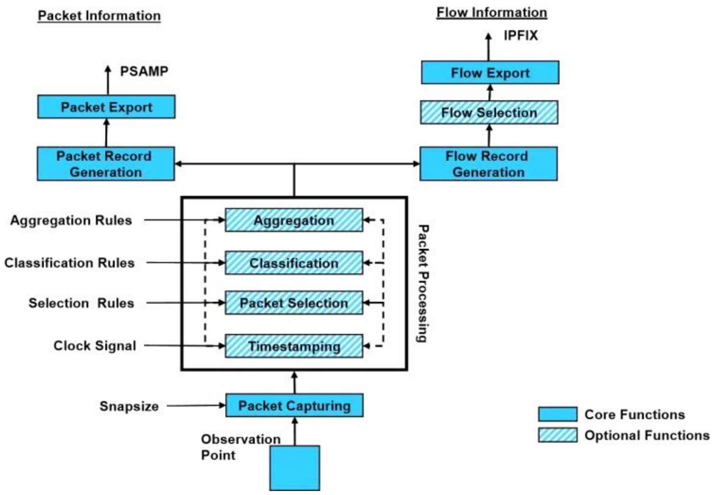

Figure 1.Information flow in IPFIX Architecture

Why IPFIX?

- IPFIX provides an extremely flexible flow definition; a flow is defined as a set of packets with common properties. Each property is defined as a result of applying a function to one or more packet header fields (e.g. destination IP address), to further packet properties (e.g. number of MPLS labels) or to values derived from packet treatment (e.g. output IF).
- IPFIX is a push-based protocol. Currently the sending of flow records is triggered by flow termination criteria (e.g. flow idle time, TCP FIN, etc.) or resource limitations (cache full). If attack detection metrics are calculated directly on the router thresholds on these metrics could be used to trigger flow export. This would allow to reduce flow export to only those cases were suspicious behavior was observed

An interoperation of measurement functions with AAA functions provides further features for network security. AAA Functions may be able to map the traffic to specific users (e.g. by using the src address) and can stop network access for suspicious systems or users. Furthermore AAA provides secure channels to neighbor AAA servers and can inform neighbors about incidents or suspicious observations. Although most providers are still reluctant to information sharing, the ability to share information with neighbor domains is a useful feature. IPFIX provides the means to do that: TCP or SCTP can be used as transport protocol to ensure congestion-awareness and IPsec and TLS can be used to provide security features.

Table 3. Summary of the measurement requirements and shows how IPFIX, PSAMP support specific features

Measurement Requirement	**IPFIX support**	**PSAMP support**
Network-wide passive measurements	Passive flow measurements integrated in routers	Packet capturing integrated in routers
Different aggregation levels	Flexible flow definition	Packet selection methods
Variety of metrics	IEs for flow statistics, extensible info model	IEs for packet capturing, extensible info model
Analysis of connections	TCP flags bitmap	Header and payload information
Correlation from multiple observation points	Header fields for packet ID generation	Header and payload info for packet ID generation
Storage of past data	-	-
Export of derived metrics	-	-
(Re-)configurability	-	Configuration of packet selection methods
Cost efficiency	Aggregation, packet selection	Packet selection methods
Link to AAA functions	-	-
Inter-domain data exchange	Standard format, congestionaware (TCP, SCTP), secure (IPsec, TLS)	Standard format, congestionaware(TCP, SCTP), secure (IPsec, TLS)

Conclusion

We are ushering into new era of technology. We need to push more resources into deployment of better security standards to every corner of the world and focus our attention to continuous evolution of these standards. TKIP still with its flaws is widely used although we have better methods now. The WEP is old news and although WPA and WPA2 are not completely secure, I would recommend upgrading to higher standards like IPFIX standards provided by IETF for networks used in big enterprises and controlling technology dealing directly with human life. IPFIX is the upcoming standard for IP flow information export. The protocol is well suited for anomaly detection, QoS measurement ,accounting and intrusion detection. The joint use of IPFIX and AAA functions can add further benefits and be useful to track and stop attackers. The networks are going to become more and more heterogeneous environment and traffic management tools need to be more advance to cope with it and IPFIX/PSAMP implementation is only going to increase to that extent.

References

[1] "Understanding WEP Weaknesses". Wiley Publishing

[2] Wi-Fi Security:The Rise and Fall of WPS-InfoSec Resources , http://resources.infosecinstitute.com/wifi-security-wps/

[3] Halvorsen, Finn M.; Haugen, Olav; Eian, Martin; Mjølsnes, Stig F. "An Improved Attack on TKIP" (September 30, 2009).

[4] B. Claise (Editor), "IPFIX Protocol Specification", Internet Draft, work in progress, June 2006

[5] FOKUS IPFIX Implementation, http://ants.fokus.fraunhofer.de/ipfix/

[6] Allar, Jared Vulnerability Note VU#723755 - WiFi Protected Setup PIN brute force vulnerability". Vulnerability Notes Database. US CERT (2011-12-27)"

[7] Y. Zhang, Z. Xiong, X. Wang, "Distributed Intrusion Detection Based on Clustering", International Conference on Machine Learning and Cybernetics, 2005

[8] (IPFIX) Implementation Guidelines https://tools.ietf.org/html/rfc5153

[9] WiFi security: history of insecurities in WEP, WPA and WPA2 , http://security.blogoverflow.com/2013/0 8/wifi-security-history-of-insecurities-i

[10] IPFIX/PSAMP: What Future Standards can Offer to Network Security , http://www.cert.org/flocon/2006/presentations/ipfix_psmap2006.pdf

[11] Wi-Fi Protected Access – Wikipedia https://en.wikipedia.org/wiki/WiFi_Protected_Access

[12] Wi-Fi Security:The Rise and Fall of WPS-InfoSec Resources , http://resources.infosecinstitute.com/wifi-security-wps/

[13] Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information, https://tools.ietf.org/html/rfc7011