Wireless Security in the Home and Office Environment

Michel Barbeau
School of Computer Science
Carleton University
1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6
Email: barbeau@scs.carleton.ca

May 28, 2010

Abstract

The ubiquity of wireless communications, in the home and office environment, introduces information security risks specific to WLANs and handheld devices. It is crucial to continuously monitor their evolution but every threat must be examined in terms of potential impact and likelihood. Only when both conditions are present, it does need to be mitigated. This paper shows how the problem can be addressed in a methodological manner. By conducting a proper risk assessment we can identify the threats, to the security of wireless communications, that are real and the ones that are inoffensive. Examples related to the protection of confidential information, in the wireless home and office environment, are used to illustrate the point.

1 Introduction

The term wireless, or its synonym radio, finds its root in the word radius, which conveys the nature of its inherent security problems. Waves, even from a very weak source, travel far in all directions, akin to light rays, fading very slowly. Waves can also traverse obstacles such as ceilings, floors and walls.

Wireless is by nature an open and wide coverage medium of communications that facilitates the perpetration of attacks.

Given the pervasiveness of wireless networks in our day-to-day activities and the blind trust invested in them, it is crucial to continuously monitor the evolution of the security threats to wireless networks. A threat must first be evaluated in terms of importance, and only then it does need to be mitigated. The wireless security scientific literature has neglected threat and risk evaluation. We are not the first and we won't be the last to raise the issue. The problematic is well illustrated in a recent article authored by Zanero [1]. The topic is wireless malware propagation. Zanero is critical about the lack of perspective of his own past work [2] and the work of other authors [3] on the topic. The theoretical merit of wireless malware propagation modeling is not the concern, but the likeliness of the attack in practice is severely questioned. The main reason being that the large diversity of wireless hardware offers a natural barrier to malware propagation.

Perspective can be achieved in a predictable, methodological manner by determining which threats are real, and thus metaphorical giants to be slain, and which are no more than harmless windmills. Yet distinguishing between the two can be just as arduous for the wireless research community as it was for Cervantes Don Quixote. Not all scientific papers consider this distinction. It is imperative to determine which threats are real and which threats are nothing more than inoffensive windmills.

This article is on the assessment of the threats and risks to the security of information associated to the use of wireless communications. The protection of confidential information in the wireless home and office environment is used as an example. Using risk assessment work published in the literature, we show how real threats to wireless network security can be methodically identified and prioritized. At the end, costly countermeasures commensurate to risk can be implemented.

The threat and risk assessment problem is examined in Section 2. Section 3 assesses risks that the use of wireless networks in the home and office environment present to the protection of confidential information. We conclude with Section 4.

2 Threat and risk assessment

A threat is an attack that, when successfully carried out against a system, has harmful conclusions, such as annoyance, communication loss, personal information leak, network breakdown or revenue loss. Attackers achieve their goal by exploiting design weaknesses and vulnerabilities of systems. Risk assessment is a way to deal with the uncertainty of threats and their potential for harmful conclusions. Threat and risk assessment produces level indicators that may be used to decide if a wireless system is worth using given a potential of harmful consequences. When confidentiality is needed, threat and risk assessment can be conducted to identify safeguards adapted to the criticality of the information that needs to be protected and vulnerabilities of the system in which the information is flowing.

Risk management refers to an activity where threat and risk assessment is a continuing process following the evolution of the technology, threats and safeguards. The bottom line is to identify, implement and maintain safeguards, that commensurate to the criticality of the information and risks to which it is exposed, and stay current with respect to newly uncovered vulnerabilities.

A threat and risk assessment is best conducted with the use of a methodology, which can be quantitative or qualitative. A quantitative methodology outputs a numerical level of risk representing the probability that a threat is successfully carried out. This approach works when historical data is available. The realty is that relevant historical data about constantly evolving wireless systems is seldom available. A qualitative methodology outputs a symbolic level of risk. Historical data is not required. It is best adapted to the wireless environment where new systems are regularly introduced and new vulnerabilities are frequently uncovered. A word of caution although, qualitative threat and risk analysis is largely subjective. Relevance and quality of a qualitative analysis heavily depend on point of views, knowledge and experience.

Most of the qualitative risk assessment methodologies produce a verdict as a function of the likelihood and potential impact of a threat. Such a methodology has been proposed by the European Telecommunications Standards Institute (ETSI) [4]. Their evaluation grid is shown in Figure 1. A risk is evaluated as Minor, Major or Critical, according to estimated values for the likelihood of occurrence and impact of the threat upon a user or a system. As a guideline, a threat that is ranked as Minor typically requires no

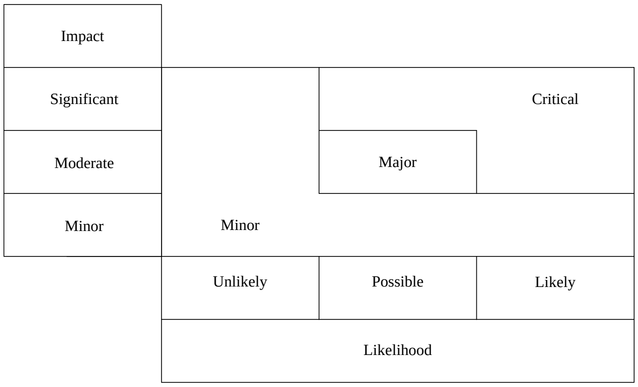


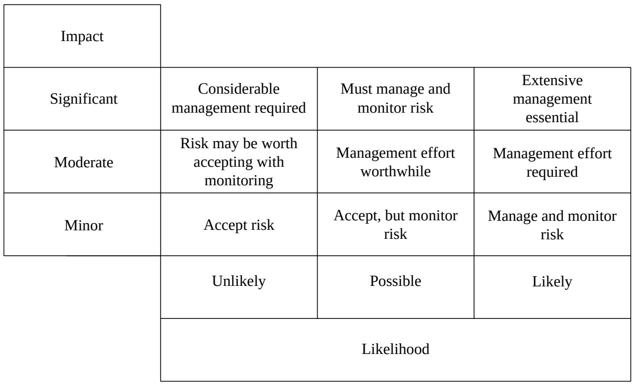
Figure 1: Risk as a function of likelihood and impact.

additional countermeasures, a Major one needs to be dealt with, and a Critical threat must be addressed with the highest priority. A threat is ranked as Critical under the following conditions: it is likely and has potentially significant impact or it is likely and has moderate impact or it is possible and has significant impact when perpetrated with success. A threat is only assessed as Major if it is possible and has potentially Moderate impact. In all other cases, the risk is considered to be Minor. We found, through experience with the ETSI methodology, that some threats tend to be over-classified as Critical when they are better ranked as Major [5, 6, 7, 8]. In some instances, we had to make adjustments to place more emphasis on the truly critical threats.

From a risk management perspective, the Integrated Risk Management Framework [9] suggests an alternative risk assessment grid, see Figure 2. The verdict emphasizes the proactive nature of risk management. Risk management includes deciding on a course of action in uncertain conditions. The course of action encompasses communicating the risk to the system users and selecting potential safeguards that are proportional in measure to the risk. In short, risk management involves understating, communicating and acting to exercise a control on risk issues.

2.1 Likelihood assessment

The Likelihood risk factor denotes the possibility that attacks associated with a given threat are actually carried out, see Figure 3. ETSI defines



Impact			
Significant	Considerable management required	Must manage and monitor risk	Extensive management essential
Moderate	Risk may be worth accepting with monitoring	Management effort worthwhile	Management effort required
Minor	Accept risk	Accept, but monitor risk	Manage and monitor risk
	Unlikely	Possible	Likely
	Likelihood		

Figure 2: Risk management actions as a function of impact and likelihood.

three discrete levels of likelihood: Unlikely, Possible, and Likely. In order to evaluate the likelihood of a threat, two additional risk factors are taken into account: the motivation for an attacker to carry out the attack and the technical difficulties that must be resolved by the attacker in order to do so. A threat is Unlikely if there is little motivation for perpetrating the specific attack or if significant technical difficulties must be overcome. A threat is Possible if the motivation for an attacker is sufficiently high and the technical difficulties are few or solvable because the required theoretical and practical knowledge for implementing the attack is available. A threat is Likely if a user or a system is almost assured of being victimized, given a high attacker motivation and lack of technical obstacles. Motivation and difficulty assessment is further discussed in the sequel.

2.2 Motivation assessment

Motivation assessment explores factors that drive an attacker. Rounds and Pendgraft [10] have identified general profiles of network attackers, see Table 1. The main points in their work are i) that a knowledge of the motivations of the potential attackers helps to better evaluate and react to a threat and ii) motivations are multiple and not solely of economic nature.

In an analysis of threats to WiMAX/802.16 security [7], we assessed the possibility of gain in terms of money and power to be somewhat more motivating than prestige. We associated a High motivation with an attacker reaping significant financial or power-based gains, a Moderate motivation

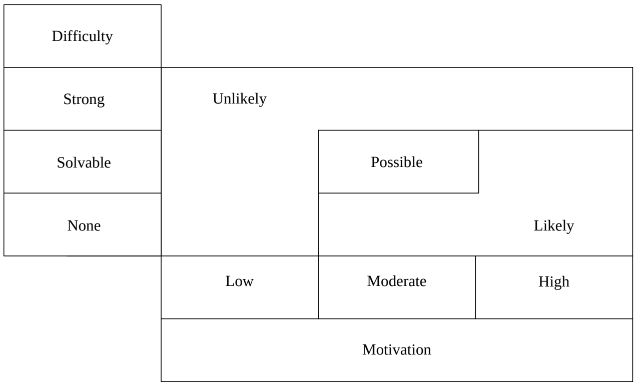


Figure 3: Likelihood as a function of attacker motivation and technical difficulty (derived using guidelines provided by ETSI).

Table 1: Rounds and Pendgraft profiles of network attackers.

Profile	Motivation
Script kiddy	Fun and adventure
Malware developer	Recognition in their virtual community
Hacktivist	Propagation of a Message
Vigilante	Investigation of potentially criminal activity
State sponsored agent	Victim's identity
Thief	Steal money
Defensive hacker	Active response against attackers, retaliation
Innocent hacker	None, compromised/used by other attackers
Enforcement	Law enforcement, pinpoint attackers

with limited gains or with creating mischief for the purpose of garnering prestige, and a Low motivation with little gain for the attacker.

2.3 Difficulty assessment

Technical difficulty assessment reviews the technological barriers encountered by an attacker in his attempts to implement a threat. It should be noted that such difficulties are dynamic in nature. What seems like an insurmountable obstacle today may not be so in a few years' time. For example, WiFi implementations based on the IEEE 802.11 standard employ Wired Equivalent Privacy (WEP) in an attempt to provide confidentiality. Originally, the standard's working group believed that WEP encryption posed Strong technical difficulties to attackers. In 1999, the technical difficulty for attacks directed at WEP was Strong, and thus attacks were Unlikely to occur. However, it quickly became obvious that WEP had weaknesses. WEP's shortcomings were discovered by cryptography experts Fluhrer, Mantin, and Shamir and made public in 2001 [11]. The technical difficulty became Solvable and the likelihood of attacks rose to the level of Possible. In 2002, security researchers Stubblefield, Ioannidis, and Rubin carried out the attack on WEP and were able to recover its secret key, thus opening the door to deciphering encrypted messages [12]. Since that time, the attack has been well documented, and the associated software has been available, reducing the technical difficulty to none and upgrading the likelihood of the attack to Likely. WiFi Protected Access (WPA), WEP's successor, is currently believed to pose Strong technical difficulties to attackers. It remains to be seen whether this assumption stands the test of time. More on this topic in Section 3. We may assign a Strong technical difficulty to threats to security mechanisms that currently may not be defeated because some theoretical elements needed for perpetrating an attack upon them are missing. A Solvable technical difficulty is associated with a security mechanism that may be countered or has been defeated in a related technology. A technical difficulty of None is assigned when a precedent for the attack already exists. Above all, adequate evaluation of technical difficulty requires technical knowledge.

2.4 Impact assessment

Impact assessment looks at the consequences on the victim(s) of an attack. The Impact criterion evaluates the consequences for a user or a system if a given threat is carried out with success. From the single user's point of view, the impact of a threat is rated as Minor if an attack results in only annoyance and the consequences, if there are any, are reversible and can be repaired. From the point of view of a system serving several users, a threat is ranked with Minor impact if the possible outages are very limited in scope, for example with few users impaired for a short duration. For the user, the impact is Moderate if a loss of service occurs for a short amount of time. For a system, the consequences of a Moderate impact threat consist of outages that are limited in both scope and possible financial losses. A threat carries a Significant impact for a user if an attack causes a loss of service for a considerable period of time. If targeted at a system, an attack associated with a Significant impact threat results in outages over a long period of time with a large number of users impaired, possibly accompanied by law violations or substantial financial losses.

Here are three concrete examples. February 2009, the Royal Canadian Mounted Police (RCMP) seizes 66 jammers of cellular phone, 911 and emergency service frequencies [13]. The police found the equipment while intercepting its owner on the road after a minor traffic law violation. While trying to verify the papers with the base, the police officer couldn't communicate, became suspicious and after verification found a jammer in operation in the car. Ownership of jammers is forbidden in Canada. One of the largest (a 50 watt device) had several hundred meter range. The owner had a compact size device (for a car cigarette lighter) in his car. Generally, the impact of jamming is minor. It generates mainly temporary disruption of service with limited scope and annoyance. It is a well understood problem and sources of jamming are easy to pinpoint.

October 2006, a woman is arrested at her arrival at the Cairo International Airport with 48 cellular phones likely destined for the cloning market [14]. The cell phone pregnant woman was trying to speed up her passage through the customs complaining about pains. The pregnant lady had numerous stamps in her passport, which what a frequent traveler would have, but not a woman in her condition. Suspicious customs officers uncovered the phones after a search. The total value of the phones was estimated to be around $20,000, which may be considered of moderate impact.

Poland, Lodz January 2008, a schoolboy hacks into city's tram system [15]. He adapted a television remote control so it could change track points. The teenager told that he had changed the points for a prank. He trespassed at tram depots to gather information and the equipment needed to build his device. He wrote the technical details of his attack in a school exercise book. Twelve people were injured in one derailment. The boy was suspected of having been involved in several other similar incidents. The impact was significant in that case.

From a confidentiality perspective, correct evaluation of the motivation or impact of a threat depends on the attacker or victim and the importance that he/she gives to the information flowing on the network. For example, the level of sensitivity of the information can be used to rank the motivation or impact of a threat. Governmental organizations explicitly require protection of their information, which is considered to be one of their asset [16]. For instance, the Canada's government has established a ranking for sensitive, but non classified, information [17]. This category of information is termed *protected*. There are three subcategories corresponding to three levels of sensitivity, namely, A, B and C. Protected A indicates low-sensitive information which disclosure may cause embarrassment or certain damage, for instance, the disclosure of salary, employee number, or banking information.

Protected B denotes particularly sensitive information which disclosure may lead to serious damage, for example, loss of reputation or loss of competitive advantage. Information such as medical records and annual performance appraisals may fall in this subcategory.

Protected C designates extremely sensitive information. It is the highest level and disclosure of such information may cause grave damage (e.g. bankruptcy) or loss of life. Information such as identities of informants in criminal investigations may fall in this category.

Access to Protected B or C designated information will certainly highly motivate an attacker and when he/she succeeds will have significant impact. On the other hand, Protected A information will moderately motivate an attacker and will have minor or moderate impact.

3 Example Risk Assessment of Threats to Wireless Confidentiality

In this section, we illustrate risk assessment of threats to the confidentiality of information transiting over wireless networks. Confidentiality is a requirement that stipulates that the understanding of the content of messages is limited to their source and destination(s). We assess in particular, under different scenarios, the eavesdropping attack and the malware/spyware attack in a wireless home and office environment. For the purpose of the evaluation, we assume Protected B or C information. To eavesdrop such information, the motivation and potential impact are High. Remain to clarify the degree of difficulty to determine the level of risk, according to the scenario. The final result of the evaluation is presented in Table 2. For the sake of simplicity, the short ETSI verdict is used. A corresponding risk management type of verdict can also be obtained using the table in Figure 2. The eavesdropping attack involves interception of wireless traffic and decryption of traffic, discussed hereafter.

3.1 Interception of traffic

At least three avenues can be used to intercept wireless traffic. Firstly, one can use an application software with monitoring capability, for example Wireshack [18], or a scanning software, for example, Aircrack-ng [19], iStumbler [20], MacStumbler [21], KISMAC [22], and Kismet [23]. Secondly, one can write his/her own software to capture frames using an application programming interface such as Linux Packet Socket (see Chapter 4 in Ref. [24] for an introduction to this API). Thirdly, information can be intercepted at the signal level using a technology called Software Defined Radio (SDR). Halperin et al. describe a SDR-based attack on a wireless reprogrammable implantable cardioverter defibrillator [25]. Other SDR-based eavesdropping work has been reported for GSM A5 traffic [26], WiFi/802.11 and Bluetooth [27, 28]. In summary, there is no technical difficulty associated with the interception of wireless traffic. Hardware and software are readily available for facilitating the work of any potential interceptor. There is nowhere one can hide from them in the radio spectrum!

Now, intercepted traffic may be encrypted or unencrypted. Wireless security surveys conducted in 2008 in the cities of London, Paris and New York indicate that the number of non secured WiFi/802.11 networks varies from 3% to up to 14% [29].

Nemat and Osborne have completed a wireless network site survey for the downtown area and a residential area of Ottawa [30]. They used the Kismet Linux survey tool and a Bluetooth GPS. The survey was done at pedestrian speed. Firstly, was is striking is the number of sites that were surveyed. For the downtown area, 1383 networks were found, see Figure 4 for a Google map of downtown Ottawa showing positions of found wireless network sites. Statistics were generated, see Figure 5. It is interesting to note that in the downtown area, 46% of the networks use no encryption or WEP. In the residential area, 51% of the networks use no encryption or WEP. A

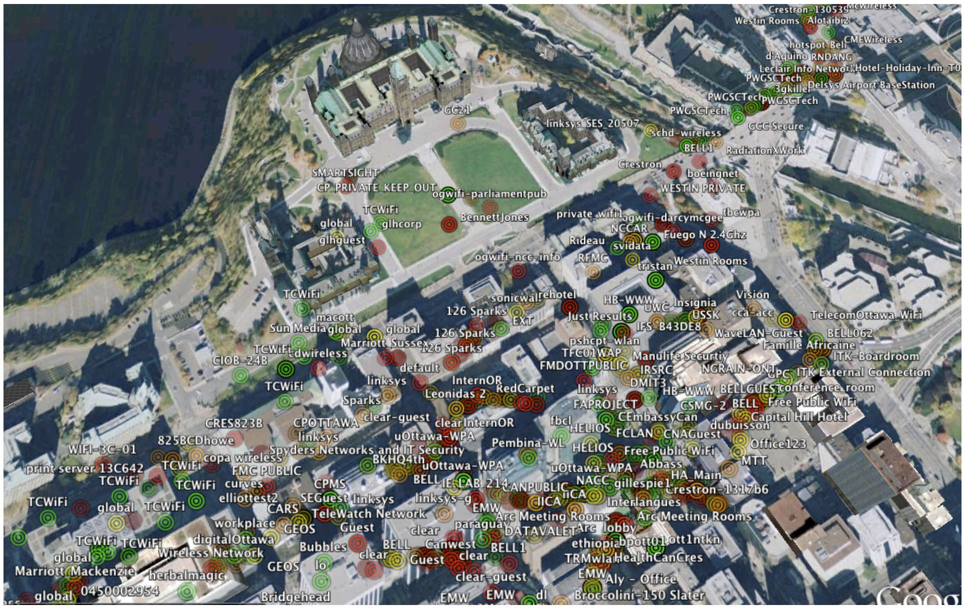


Figure 4: Wireless network site survey map for downtown Ottawa.

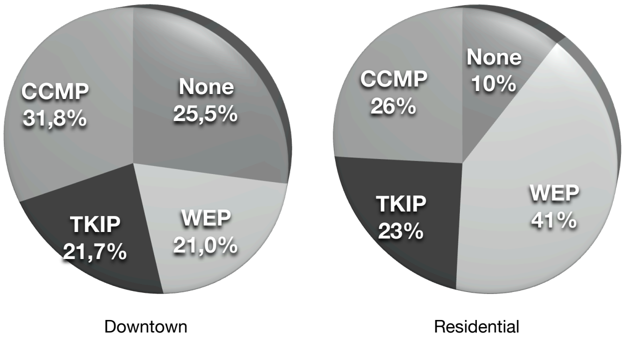


Figure 5: Wireless network site survey statistics.

possible explanation is that several sites use ADSL gateways with default settings determined by the provider.

The risk of eavesdropping for unencrypted traffic is high. For encrypted traffic, we examine two cases: stream-cypher based encrypted traffic and block-cypher based encrypted traffic.

3.2 Stream-cypher encryption

A good example of the use of a stream cypher for traffic encryption is Wired Equivalent Privacy (WEP) of WiFi/802.11. WEP uses the RC4 stream cypher. A great advantage of the WEP/RC4 solution is the ease of implementation. It doesn't require complex operations. WEP can be implemented in the wireless interface hardware. The RC4 algorithm is used to generate a pseudo random sequence of bits that are xored with the bits of a frame before sending it. The seed of RC4 consists of a symmetric key and an Initialization Vector (IV). The symmetric key can be either a default key, i.e. a 40- or 104-bit secret shared between an AP and several stations, or a key-mapping, i.e. a 40- or 104-bit secret shared between an AP and a single station. The IV is a 24-bit random value chosen by the sender independently for each frame. All frames, sent and received among those sharing a secret, are encrypted with the same key and the intent of the IV is to associate a unique pseudo random sequence for each frame. This turned out to be not very true, in practice, because of the size of the IV relative to the frame transmission rate. Much has been said and written on the weaknesses of WEP [31, 32, 33, 34]. The final nail in WEP's coffin was a courtesy of Bittau et al. [35]. WEP cracking tools and software are available online to anyone. It is well established that WEP is unsecure and that wireless WEP networks expose their traffic to a high risk of eavesdropping. The risk is High with WEP and it is not an option for Protected B or C traffic.

The Temporal Key Integrity Protocol (TKIP) is an encryption scheme aiming to replace and strengthen WEP. TKIP is part of the Wi-Fi Protected Access (WPA) certification program. TKIP uses the RC4 stream cypher, like WEP, but with per-packet RC4 encryption with longer keys. Firstly, there is a new IV format. 32 more bits are added to the 24 bits already allocated by WEP, yielding a 56-bit IV. Effectively, only the first six IV bytes are used. One byte is ignored for weak key avoidance. When a weak key is used, TKIP has undesirable properties and is easier to attack. A function mixes the encryption key, IV and MAC address of the sender to create the RC4 seed. The use of the MAC address as an input avoids the generation of identical seeds across stations. In principle, every station has its own pool of RC4 seeds.

A brute force attack can be ran on TKIP. The attacker must first get the nonces entering in the generation of the encryption key. The attacker must capture frames exchanged during the four-way handshake for key establishment. This is done when a station associates and authenticates with an access point. The attacker can also force the re-execution of this procedure using a deauthentication attack. A program, such as one of the aforementioned, can be used to capture the four messages of the four-way handshake process. The brute force attack tries all possibilities to find the encryption key. A brute force search has been implemented in a software called coWPAtty [36]. For each attempt, there are 4096 hash computations involved. The procedure can be speed up with the use of a rainbow table, i.e. pre-computed hash values. Rainbow tables are, however, generated as a function of the service set identifier (SSID) of the network being attacked. If no rainbow table is available for a SSID (likely to happen if the network doesn't operate with default values), than hash values need to be generated. Theoretically, the time complexity of a brute force attack on TKIP is $\mathcal{O}(2^{128})$. It can be very slow and take years!

A brute force attack can be greatly accelerated if combined with a dictionary attack. Entries in the dictionary are tried first as potential keys. This works if the network is configured with a predictable key. The pre-shared key of TKIP is generated with a passphrase of up to 63 character long, which can be alphanumeric and punctuation characters. If all characters are used and selected randomly, then a dictionary attack is very unlikely to succeed.

To the best of our knowledge TKIP has not been cracked, but weaknesses has been reported. Moen et al. have shown that it is theoretically possible to resolve the 128-bit temporal key from TKIP RC4 encrypted frames [37]. The time complexity of their attack is lower than the brute force attack, but still on the high side, i.e. $\mathcal{O}(2^{105})$ and may not be significantly more practical than the latter. Beck and Tews [34] have developed a Chopchop kind of attack to TKIP encrypted Address Resolution Protocol (ARP) packets. The attack doesn't recover the temporal key, but decrypts the content of an ARP packet. The attack requires repeatedly resending to the access point the same packet that needs to be decrypted. The content of the packet is guessed byte by byte starting from the last. The reaction of the access point tells the attacker if he/she guessed right. Access points do implement mitigation mechanisms that slow down, but still make possible, the attack. WEP is vulnerable as well to the Chopchop attack. The attack has been described in detail in a video by Christen and Ng [38]. At this time, it is hard to claim that the level of difficulty of attacks on TKIP remains strong. Progress has been made. Motivation is high among researchers to break TKIP because of potential recognition of peers. It is likely that an eavesdropping attack on TKIP will eventually succeed. TKIP is a case where the risk is Critical and risk management effort is required, i.e. one needs to monitor the TKIP cracking progress.

It is worth mentioning the ongoing efforts to crack the stream cypher of Global System for Mobile Communications (GSM), namely, A5/1. There are two approaches. One assumes knowledge of some plaintext, i.e. the known-plaintext attack [39], the other not, i.e. the ciphertext-only attack [40, 41]. The real threat for GSM cell phone users is the ciphertext-only attack. At this time, it seems that A5/1 is theoretically broken. To make the attacks practical, however, there are still space complexity and time complexity issues to resolve. It is another case were risk management effort and cracking progress monitoring are required.

3.3 Block-cypher encryption

The Wi-Fi Protected Access 2 (WPA2) certification program prescribes the use of block-cypher encryption, that is the Advanced Encryption Standard (AES). Keys are 128 bits long. A mode of AES was created specifically for WiFi/802.11: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). The CCMP mode is based on cypher block chaining. It has similarities with a stream cypher. Indeed, the plain text of a frame is xored fragment by fragment, of 128 bits, with a 128-bit keystream. Successive 128-bit keystreams are obtained, for all fragments, by encrypting the combination of the key, IV and counter. A 104-bit nonce is used as a counter (of fragments of a frame) together with a 8-bit flag value and a 16-bit sequence number, for a total of 128 bits.

The brute force attack and dictionary attack described for TKIP apply as well to CCMP. To the best of our knowledge, this is as far we can go now. Assuming good passphrase management, to prevent dictionary attacks, the level of difficulty of an eavesdropping attack on CCMP traffic is strong and unlikely to happen at this time. The risk is minor, but good key management is required.

Note that the use of block-cypher encryption is not sufficient to guarantee security. A threat to the confidentiality of peer-to-peer (also termed PIN-to-PIN) email on BlackBerry devices has been documented by CSEC [42]. BlackBerry peer-to-peer emails are forwarded solely by the wireless service provider and bypass e-mail servers and security filters (firewalls, BlackBerry Enterprise Servers). Such traffic is encrypted with Triple-DES, but using a network key (shared by all BlackBerry devices of the world). Peer-to-peer BlackBerry traffic can be eavesdropped and decoded by insiders. The risk of eavesdropping is Critical.

3.4 Wireless Malware Propagation and Confidentiality

A malware is a piece of software designed to corrupt the normal execution of a computer. For example a spyware, a type of malware, can be installed on wireless devices (e.g. handsets, access points) to collect transiting personnal information. BlackBerry peer-to-peer emails are vulnerable to malware because the traffic bypasses e-mail servers and security filters [42]. Assessment of the problem of malware for smart-phones in general, and Google Android in particular, has been investigated in an article by Shabtai et al. [43]. Hereafter, we concentrate on malware attacks targeting the wireless link level. A malware running on a router can be used to intercept information. Hu et al. [3] proposed a malware epidemiology model for WiFi/802.11 routers. According to Zanero, however, a malware outbreak in the wireless world is only theoretical and unlikely to occur in practice [1]. The point made by Zanero is the difficulty to write a malware for a wide diversity of platforms. Indeed, malware propagation in the world of wireless is more challenging than in the fixed computing world because of the wide diversity of hardware. In particular for routers, at best a small fraction of the routers can be infected. Moreover, networks of routers being infected by malware would be substantially disrupted. The attack would be quickly noticed by network clients, provoke disconnection of the routers and stop malware propagation. Adopting Zanero's analysis of real malware propagation, we conclude that it is in effect unlikely to occur. Zanero's statement applies as well to mobile phones. The challenge faced by propagation is the difficulty to write malware that runs across a diversity of mobile phone hardware. This statement is although qualified by Shabtai et al. [43] for smart-phones. We conclude that, at the wireless level at this time, the risk of a malware outbreak is minor.

4 Conclusion

Threat analysis methodologies provide the means to differentiate between actual risks and perceived ones. The windmills of perceived risks must be dispelled and the giants unmasked so that future research efforts on wireless

Table 2: Risk assessment (assuming good passphrase management and Protected B or C information, motivation is High and potential impact is High).

Threat	Likelihood	Risk
Eavesdropping WEP traffic	Likely	Critical
Eavesdropping TKIP traffic	Likely	Critical*
Eavesdropping CCMP traffic	Unlikely	Minor
BlackBerry peer-to-peer emails	Likely	Critical
Malware outbreak	Unlikely	Minor

*Need to monitor cracking progress.

security can be effectively focused on the irrefutable menaces lurking in the shadows.

If you find the exercise worthwhile and would like to read more about it, then we suggest looking at some of our work. Ref. [7] examines threats to the security of the WiMAX/802.16 broadband wireless access technology. Ref. [5] confirms with a risk analysis that impersonation attacks in wireless and mobile networks offer strong incentives to malicious criminal groups and should therefore be given highest priority in research studies. In Ref. [6], we identify the security threats inherent in the emerging Dedicated Short Range Communications (DSRC) Wireless Access in Vehicular Environments architecture. DSRC enabled road vehicles are on the brink of actualizing an important application of mobile ad hoc networks. It is crucial that the messages exchanged between the vehicles and between the vehicles and specialized infrastructure be reliable, accurate and confidential. Finally, Ref. [8] is a study of the problem in the context of Electronic Product Code networks.

Acknowledgment

I would like to thank collaborators Joaquin Garcia-Alfaro, Jeyanthi Hall, Evangelos Kranakis and Christine Laurendeau for several fruitful discussions on the topic of this paper. I also thank my students James R. Relyea, Michael Nemat, Matthew Ng, Nicholas Osborne, Chris Whiten for running wireless

LAN attack experiments [30, 44, 38]. Financial support from the Natural Sciences and Engineering Research Council of Canada (NSERC) is graciously acknowledged.

References

[1] S. Zanero, "Wireless malware propagation: A reality check," *IEEE Security and Privacy*, vol. 7, no. 5, pp. 70–74, September-October 2009.

[2] ——, "Studying Bluetooth malware propagation: The BlueBag project," *IEEE Security and Privacy*, vol. 5, no. 2, pp. 17–25, Arch-April 2007.

[3] H. Hu, S. Myers, V. Colizza, and A. Vespignani, "WiFi networks and malware epidemiology," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 106, no. 5, pp. 1318–1332, February 2009.

[4] ETSI, "Telecommunications and internet protocol harmonization over networks (TIPHON) release 4; protocol framework definition; methods and protocols for security; part 1: Threat analysis," European Telecommunications Standards Institute (ETSI), Tech. Rep. Technical Specification ETSI TS 102 165-1 V4.1.1, 2003.

[5] M. Barbeau, J. Hall, and E. Kranakis, "Detecting impersonation attacks in future wireless and mobile networks," in *Mobile Ad-hoc Networks and Sensors workshop (MADNES), Lecture Notes in Computer Science*, vol. 4074, Springer Berlin / Heidelberg, 2006, pp. 80–95.

[6] C. Laurendeau and M. Barbeau, "Threats to security in DSRC/WAVE," in *5th International Conference on Ad-hoc Networks, Lecture Notes in Computer Science*, vol. 4104, Springer Berlin / Heidelberg, 2006, pp. 266–279.

[7] M. Barbeau and C. Laurendeau, "Analysis of threats to WiMAX/802.16 security," in *Mobile WiMAX: Toward Broadband Wireless Metropolitan Area Networks*, ser. Wireless Networks and Mobile Communications Series, Y. Zhang and H.-H. Chen, Eds. New York: Taylor and Francis Group, 2007, pp. 347–362.

[8] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis, “Analysis of threats to the security of EPC networks,” may 2008, pp. 67 –74.

[9] Treasury Board of Canada Secretariat. (2001) Integrated risk management framework (IRMF). [Online]. Available: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=12254

[10] M. Rounds and N. Pendgraft, “Diversity in network attacker motivation: A literature review,” *IEEE International Conference on Computational Science and Engineering*, vol. 3, pp. 319–323, 2009.

[11] I. M. S. Fluhrer and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4,” in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science, vol. 2259. Berlin / Heidelberg: Springer, 2001, pp. 1–24.

[12] A. Stubblefield, I. Ioannidis, and A. Rubin, “Using the Fluhrer, Mantin and Shamir attack to break WEP,” in *Network System Security Symposium*, 2002, pp. 17–22.

[13] J.-F. Nérond. (2009, February) La GRC saisit 66 brouilleurs d’ondes. [Online]. Available: cyberpresse.ca

[14] Cyberpresse. (2006, October) Une égyptienne ”accouche” à l’aéroport de 48 téléphones. [Online]. Available: cyberpresse.ca

[15] G. Baker. (2008, January) Schoolboy hacks into city’s tram system. [Online]. Available: Telegraph.co.uk

[16] Treasury Board of Canada Secretariat. (2004) Operational security standard: Management of information technology security (MITS). [Online]. Available: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text

[17] ——. (1996) Security policy-manager’s handbook. [Online]. Available: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tb_j2/spmh1-eng.asp

[18] (2010) Wireshark. [Online]. Available: http://www.wireshark.org/

[19] (2010) Aircrack-ng. [Online]. Available: http://www.aircrack-ng.org/doku.php

[20] (2010) iStumbler. [Online]. Available: http://istumbler.net/

[21] (2010) MacStumbler. [Online]. Available: http://www.macstumbler.com/

[22] (2010) KisMAC. [Online]. Available: http://mac.free.comprolive.com/2007/10/kismac-stumblerscanner.html

[23] Kismet. [Online]. Available: http://www.kismetwireless.net/

[24] M. Barbeau and E. Kranakis, *Principles of Ad Hoc Networking.* Chichester, West Sussex, England: John Wiley and Sons, Ltd., 2007.

[25] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *IEEE Symposium on Security and Privacy*, May 2008, pp. 129–142.

[26] J. Lackey and D. Hulton. (2007) The A5 cracking project - practical attacks on GSM using GNU radio and FPGAs - chaos communication camp 2007. [Online]. Available: http://213.73.91.78/camp/2007/Fahrplan/events/2015.en.html

[27] D. Spill and A. Bittau, "BlueSniff: Eve meets Alice and Bluetooth," in *WOOT '07: Proceedings of the first USENIX workshop on Offensive Technologies.* Berkeley, CA, USA: USENIX Association, 2007, pp. 1–10.

[28] K. Lakshminarayanan, S. Sapra, S. Seshan, and P. Steenkiste, "RFDump: an architecture for monitoring the wireless ether," in *CoNEXT '09: Proceedings of the 5th international conference on Emerging networking experiments and technologies.* New York, NY, USA: ACM, 2009, pp. 253–264.

[29] RSA, The Security Division of EMC, "The wireless security survey of London," Tech. Rep. DEC-TR-506, October 2008.

[30] N. Osborne and M. Nemat, "Real-World WiFi Security Inadequacies, Report done for the course COMP4203, Wireless Networks and Security," Carleton University, Tech. Rep., April 2010. [Online]. Available: http://people.scs.carleton.ca/˜barbeau/Honours/Osborne_Nemat.pdf

[31] N. Cam-Winget, R. Housley, D. Wagner, and J. Walker, "Security flaws in 802.11 data link protocols," *Commun. ACM*, vol. 46, no. 5, pp. 35–39, 2003.

[32] R. Housley and W. Arbaugh, "Security problems in 802.11-based networks," *Commun. ACM*, vol. 46, no. 5, pp. 31–34, 2003.

[33] K. Hole, E. Dyrnes, and P. Thorsheim, "Securing Wi-Fi networks," *Computer*, vol. 38, no. 7, pp. 28 – 34, july 2005.

[34] E. Tews and M. Beck, "Practical attacks against WEP and WPA," in *WiSec '09: Proceedings of the second ACM conference on Wireless network security.* New York, NY, USA: ACM, 2009, pp. 79–86.

[35] A. Bittau, M. Handley, and J. Lackey, "The final nail in WEP's coffin," in *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, May 2006, pp. 386–400.

[36] coWPAtty. coWPAtty MAIN. [Online]. Available: http://wirelessdefence.org/Contents/coWPAttyMain.htm

[37] V. Moen, H. Raddum, and K. J. Hole, "Weaknesses in the temporal key hash of WPA," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 8, no. 2, pp. 76–83, 2004.

[38] C. Whiten and M. Ng. (2010, April) Introduction to the Korek ChopChop Attack, Video done for the course COMP4203, Wireless Networks and Security. [Online]. Available: http://people.scs.carleton.ca/b̃arbeau/Honours/Whiten_Ng.m4v

[39] E. Barkan and E. Biham, "Conditional estimators: An effective attack on A5/1," in *Selected Areas in Cryptography, Lecture Notes in Computer Science*, vol. 3897, 2006, pp. 1–19.

[40] E. Barkan, E. Biham, and N. Keller, "Instant ciphertext-only cryptanalysis of GSM encrypted communication," *Journal of Cryptology*, vol. 21, no. 3, pp. 392–429, July 2008.

[41] T. Guneysu, T. Kasper, M. Novotny, C. Paar, and A. Rupp, "Cryptanalysis with COPACOBANA," *Computers, IEEE Transactions on*, vol. 57, no. 11, pp. 1498 –1513, nov. 2008.

[42] Communications Security Establishment Canada (CSEC). (2008, October) Security of BlackBerry pin-to-pin messaging. [Online]. Available: http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb57-eng.html

[43] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer, "Google Android: A comprehensive security assessment," *Security Privacy, IEEE*, vol. 8, no. 2, pp. 35 –44, march-april 2010.

[44] J.R. Relyea, "Security in residential wireless local area networks," Carleton University, Tech. Rep., December 2008. [Online]. Available: http://people.scs.carleton.ca/~barbeau/Honours/James_R_Relyea.pdf