IEEE 802.11 WI-FI Security: Survey

Michael Schoenberg

CONTENTS

LIST OF FIGURES

***Abstract*—Wireless devices must broadcast transmissions in order to send and receive data on the internet. This, combined with the limited system resources available to wireless devices, has necessitated the development of security protocols that require fewer system resources. These protocols are tailored to meet the security needs of a plethora of devices and are constantly evolving alongside ever more advanced computer technology. Additionally, the focus of security protocols is shifting to include the protection of wireless networks as well as devices. The importance of securing wireless communications will become increasingly critical as wireless devices continue to grow more integral to daily life.**

I. INTRODUCTION

Since the introduction of Wi-Fi, wireless Internet devices have become increasingly ubiquitous in personal and professional life. They are used by individuals to do their shopping, banking, and social networking as well by businesses to allow their employees greater flexibility and mobility. This has resulted in growing amounts of sensitive data being transmitted over wireless frequencies and a need for methods of securing that data. Additionally, as technology is constantly evolving, security protocols must evolve with them in order to continue protecting sensitive data. Furthermore, the shape and form of wireless technology has become increasingly diverse and each type of device has its own unique features requiring equally diverse security protocols tailored to meet their individual needs. Finally, one of the cornerstones of wireless technology is wireless networks. Without these networks, wireless devices are useless and thus their security must also be addressed.

II. BACKGROUND

A. Challenges

Although security protocols predate wireless technology, wireless devices introduce additional security challenges that make using these protocols less than ideal. Wireless devices must achieve the same functionalities as wired devices while under several additional restrictions. The first is that wireless devices must broadcast messages to communicate with an access point. This allows anyone with the proper equipment to receive it and makes security a primary concern [8]. Additionally, wireless devices must operate off of a limited supply of battery power. More complex security protocols increase the workload of the processor which results in more power consumption and shorter battery life [8] [2]. Another restriction is the speed of processors available in wireless devices. These processors are not capable of doing the computations required for complex security protocols in a timely manner [8] Finally, wireless devices must contend with higher bit error rates in the process of transmitting data. The transmission medium is much less reliable and security protocols must make considerations for this [2].

B. Wired Equivalent Privacy

The first protocol designed to meet the security challenges presented by Wi-Fi was Wired Equivalent Privacy (WEP). WEP encrypts each packet individually by an exclusive or of the packet with a stream of bits generated by the RC4 algorithm. RC4 generates bits based on a 64 bit key comprised of a 40 bit WEP key and a 24 bit Initialization Vector(IV) choosen by the sender. It then computes and appends an Integrity Check Value(ICV) generated from a function using the packet as input. The receiver can then use the same function using the message as input and if the ICV they calculate matches the ICV from the sender, the message has arrived as sent and can be read by reversing the encryption process [2].

WEP was soon discovered to contain a variety of weaknesses and provide only minimal protection. The 40 bit WEP key and the 24 bit Initialization Vector proved to be susceptible to brute force attacks, attempting every possible key in order to decrypt a message. While a lack in turnover in each of these values left a potentially lengthy time between the success of a brute force attack and the switch to a different key. Additionally, the ICV and the authentication system made WEP vulnerable to man in the middle attacks. A third party could intercept packets and alter their contents in such a way that the ICV value remained unchanged. Alternatively, a third party could gain the ability to forge authentication messages by intercepting authentication messages between two other users. Thereby gaining access to the keys and IVs being used for encryption [2]. These vulnerabilities lead to WEP being quickly phased out in favor of more effective security protocols.

C. Wi-Fi Protected Access

The next security protocol, Wi-Fi Protected Access(WPA), was designed to address the weaknesses of WEP. WPA made use of the Temporal Key Integrity Protocol(TKIP), an improved form of WEP's encryption. TKIP uses a hash function to combine a 128 bit key with a 48 bit IV. It then used this key with the RC4 algorithm rather than the 40 bit key and 24 bit IV used in WEP. WPA also improved on the use of an ICV, it computes a 64 bit Message Integrity Code(MIC) from the data being sent and sets the ICV as the cyclical redundancy code of the data and the MIC [2]. The cyclical redundancy code is calculated by treating the message as a binary number and taking the remainder after dividing by some value [7]. WPA latter became WPA2 which replaced TKIP with a new encryption algorithm called CCM. In CCM, the sender and the receiver agree on a key. Messages are then separated into blocks of binary the same size as the key and multiplied by it to obtain the encrypted message. Both WPA and WPA2 remain in use today.

D. Robust Security Networks

One alternative to WPA2 is called a Robust Security Network(RSN). RSNs uses dynamic negotiation to select encryption and authentication algorithms. This allows RSNs to be easily altered to utilize new algorithms without changing the protocol. Making it ideal for use with more advanced devices. The drawback is that this precludes RSNs being used on older machines that cannot handle the more complex algorithms [2].

III. Technical Analysis

Although security protocols vary tremendously in their implementation, they all follow a similar framework for protecting data. They utilize encryption to keep data confidential, integrity checks to assure the data's validity, and authentication to verify the identities of senders and receivers. Although some protocols are forced to sacrifice elements of this structure in order to reduce processing costs, this structure represents the ideal security protocol framework.

A. Encryption

The goal of encryption is to transform data sent in such a way that it is incomprehensible except for those in possession of the key. Figure **??** shows the basic encryption process. The message, plain-text, is transformed using a combination of a binary key value and an encryption algorithm rendering the plain-text into cypher-text. The cypher-text is then transmitted to the receiver who uses the same key and the inverse of the encryption algorithm to convert the cypher-text back into plain-text [7].

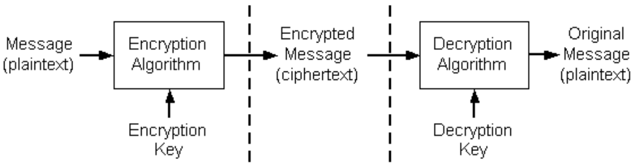

Fig. 1. A Basic representation of encryption

1) Keys: The most important aspect of a key is the size, the number of binary bits used to represent it. Larger key size results in more possible key values which makes the encryption algorithm more secure against brute force attacks. Wired Equivalent Privacy makes use of a 64 bit key which results in 2^{64} possible keys. This made WEP very vulnerable to brute force attacks as the processing capacity of computers improved and was one of the primary reasons for WEP's replacement by Wi-Fi Protected Access which uses a 128 bit key resulting in 2^{128} possible keys, making it more secure against brute force attacks [2]. WPA remains quite secure against brute force attacks however, it pales in comparison to the 128-512 bit keys commonly employed by encryption algorithms used by IPSecurity to protect wired devices [3] [7]. These devices do not have the same constraints in terms of processing power and are capable of executing the increased computational costs of the larger keys without sacrificing performance in other areas. No key size provides complete protection against this type of attack however the average length of time required for a brute force attack increases by an equivalent factor to the increase in key size.

2) Encryption Algorithms: Just as important as the key is the encryption algorithm itself. As any method of encryption is susceptible to brute force and cryptographic attacks. With sufficient time, a brute force attack will eventually find the key. Similarly, given enough data and computing resources, a cryptographic attack will be able to identify a pattern in the encrypted data and utilize that pattern to discern the content of encrypted messages. For this reason, the goal of encryption algorithms has been to make the execution of such attacks intractable. There are many ways to go about this and each algorithm utilizes its own method. WEP for example, uses its key to generate a string of bits the same length as the message and then does an exclusive or between that string of bits and the message. WPA uses this same method with a larger key size, while WPA2 multiplies blocks of the message by a large, binary number [2]. IPSecurity algorithms utilize similar techniques in combination with Cipher Block Chaining(CBC) which encodes a message into blocks of data which are each encoded using an individual key [7] [3]. The encryption algorithms used in IPSecurity are not a great deal more complex than those available to wireless devices. However, wired devices are able to leverage their more plentiful processing resources to take advantage of algorithms such as CBC which reduce the amount of data protected by any given key and there by provide superior security.

The methods for encryption are ever evolving at a consistent pace along side processing speeds. The driving force behind this is brute force attacks. For example, while WEP was replaced for a variety of reasons, one of the central reasons was that computers had become fast enough that WEP's encryption algorithm provided inadequate protection against brute force attacks. The same was true for WPA's encryption algorithm, Temporal Key Protocol [2]. They were phased out not primarily because of flaws in their encryption but because newer algorithms provided better defenses against brute force attacks. So long as brute force remains a viable method of attack, security algorithms will need to account for it in their design.

B. Message Integrity

The second function of security protocols is maintaining message integrity. When transmitting messages over an unsecured medium such as the Internet, insuring that messages have not been altered in transit is of paramount importance. Message integrity is also addressed by Internet Protocol as a means of dealing with bit errors in messages that occur during the course of transmission as a result of problems in the course of transmission. However it holds a different significance for security, specifically, "Man in the Middle" attacks. This type of attack takes place when a third party intercepts a message and alters it before sending it on to the intended receiver [7].

The first method of insuring message integrity is simply to encrypt messages. Encrypting a message prevents an attacker from being able to decipher the message and renders any changes they might make meaningless. Without access to the unencrypted text, any alteration would simply be treated as a message that had accrued errors in transmission and be discarded or retransmitted. This is also the most effective method as detecting changes becomes considerably more difficult if the attacker has access to the unencrypted text. This is because methods of checking message integrity rely on the content of the message. The most common tool for proving message integrity is a Cyclical Redundancy Code(CRC).

The CRC is calculated by first adding bits to the end of the message based on its length. It is then divided by an agreed upon value and the remainder, the CRC value, is attached to the end of the message. The flaw is that if the attacker alters the message in such a way that it maintains the same CRC the alteration will go undetected. Although there are other methods of checking message integrity, they encounter this same problem. Control of the text confers the ability to manipulate the integrity check value. More complex algorithms that generate more unique outputs make this attack more complex to execute however detecting changes remains difficult and a greater emphasis has been placed on user authentication as a result [7]. For this reason, there is not a great deal of difference in the effectiveness of integrity checks between wired and wireless security protocols. Access to the unencrypted text allows WEP's message integrity check to be easily circumvented and while WPA's integrity check is more complex, it does not erase this vulnerability. The same could be said of IPSecurity, there are some hash algorithms available for this purpose however they do not eliminate this vulnerability [7] [3]. While the hash algorithms accessible to wired devices are superior to those available to wireless devices, they are all inferior to the assurance of message integrity provided by unbroken encryption.

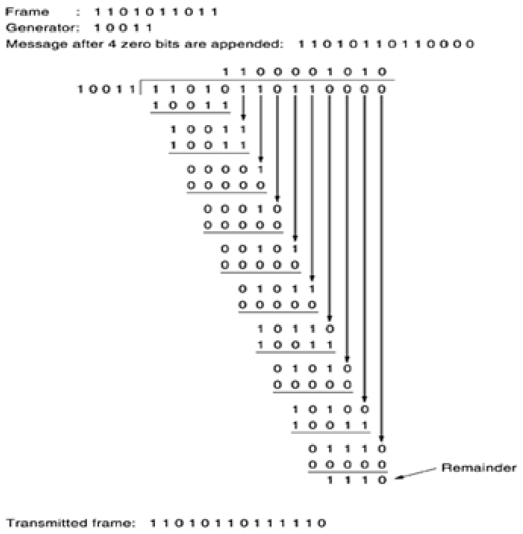

Fig. 2. Cyclical Redundancy Code used in WPA2

C. Authentication

1) Public Key Authentication: The third goal of security protocols is to provide user authentication. To ascertain the source of a message and that the sender are who they claim to be. As with encryption, there are several methods of accomplishing this. The most common of which is public and private keys as shown in figure 3. This method of authentication is predicated on each user being in sole possession of their private key and their public key being the inverse of that algorithm. For example if Alice encrypts something with her private key and Bob's public key, Bob can tell that the message is from Alice by decrypting it first with his private key and then her public key. Since Alice is the only one with her private key, she is the only one who could have encrypted and sent the message [7]. This system provides reliable authentication however it is several orders of magnitude slower than symmetric key algorithms and is typically used only for authentication and to establish a session key that will be used in conjunction with a symmetric key algorithm for the duration of the communication. The second issue is the task of compiling and maintaining a list of entities as well as their public and private keys. This function is carried out by trusted third parties called Certificate Authorities.(see figure **??** below).

The role of a certificate authority is to provide users with a reliable means of establishing identity. The Certificate Authority collects the identity of the entity being certified, its public key, the identity of the signer, their digital signature, and the digital signature algorithm identifier. This informations uniquely identifies each entity and can users can draw on a Certificate Authority to obtain reliable identity information for use in authentication. Additionally, they can do this on a scale large enough to be useful in a system with a multitude of users. Certificate Authorities also maintain a certificate revocation list. This list contains a list of all,once valid, certificates that have been revoked for containing outdated or fraudulent information. There is an alternative to this system called Pretty Good Privacy(PGP) in which this process is carried out by each user individually. However, PGP is limited in that it cannot collect and manage identity information on the same scale as a Certificate Authority [7].

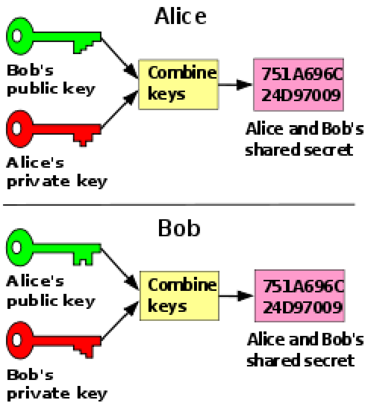

Fig. 3. Public/Private Key Authentication

An additional feature that is often included in public key authentication is a timestamp. Timestamps are included to protect against variations of a replay attack. One in which an attacker intercepts a valid message and resends it at a different time. The message has not been altered and thus still appears as a valid communication. In this manner, an attacker could intercept authentication messages and use them to impersonate a given user, thereby obtaining confidential information. The inclusion of a timestamp prevents this by establishing a shared clock by which the timeliness of messages can be used to verify their authenticity. A visual representation of this process can be seen in Figure 6 below.

Alice begins the communication with a message containing a timestamp encrypted with her private key. Bob responds with the timestamp from Alice and his timestamp, encrypted with his private key. Alice then sends Bob a message containing a timestamp based on what Bob sent her and a session key encrypted with Bob's public key. Bob can then decrypt the message with his private key and determine if the message is authentic based on the timestamp from Alice. This combats a

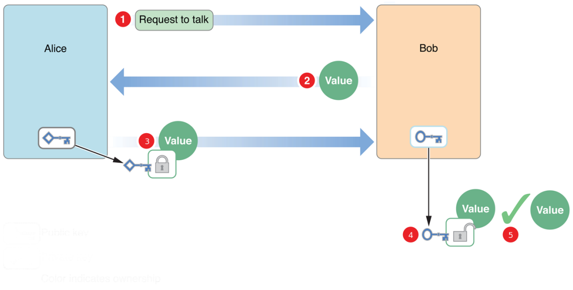

Fig. 4. An example exchange implementing public key authentication

replay style attack by providing a means to assess how long messages have been in transit. As messages are only valid for a predetermined length of time, those intercepted by a third party would presumably exceed this length of time and become invalid [7].

The lack of authentication was one of the primary reasons for the replacement of WEP by WPA. The authentication protocol utilized in WPA/WPA2, Extensible Authentication Protocol(EAP), is based on this public key method of authentication. IPSecurity also makes use of this type of authentication as well as additional information that is passed in the message header as part of the routing protocol. In this area, the capabilities of wired and wireless protocols are equivalent. Public key authentication is one of the most common, effective authentication algorithms available. Additionally, unlike encryption, it does not place a proportionately larger processing burden on wireless devices making it nearly universally accessible and ubiquitous. Research is ongoing however, Certificate authorities are not inviolate and establishing identity over the Internet is an ongoing topic of research and debate.

D. Wireless Sensor Nodes

An alternative means of user authentication makes use of the fact that wireless devices must broadcast a signal to the access point. This is accomplished using modified access points referred to as snoopers. An example of such a system is shown in Figure 5 [9].

First, the snoopers must "learn" the layout of the environment in which they are placed. It is possible to utilize snoopers in an environment for which they have not learned the layout but it greatly reduces the accuracy with which the system can locate devices. Each snooper is provided with a list of possible device locations and signal strengths from those locations. The snoopers can then measure the strength of the signal they are receiving from a device and compute the device's probable location from the signal strength within a margin of 2 meters. This accuracy is possible because wireless devices broadcast messages that can be picked up by any access point in range of the device. Multiple access points can be used to reduce the number of possible points of origin and improve accuracy [9].

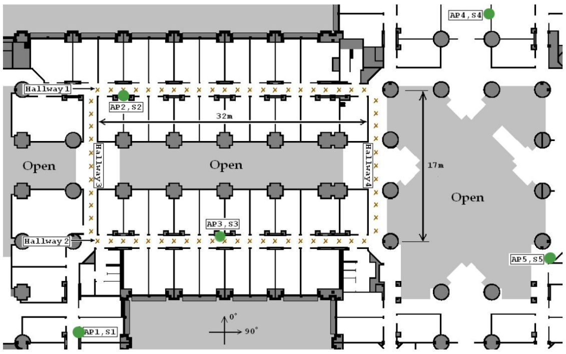

Fig. 5. An example of a test system employing wireless node sensors. The green dots represent the location of snoopers and the x's represent possible device locations

This method of authentication assigns a device that is tied to its physical location rather than an identity based on the public/private key system. The location data could be used in a system like that used for public key authentication, however that is not currently the case. Wireless devices are designed to be mobile and this makes physical location a less useful identifier than a single public/private key pair. It is however, very useful in a localized system for managing users and access. For example, access to a wireless device might be restricted to devices within a certain area or blocking a certain device from being able to access the network. These possibilities, currently, make wireless sensor networks a very useful tool in securing wireless networks rather than individual devices or communications [9]. This does however have the potential to change the way authentication is done in the future. It offers the ability to tie attach a physical identity to a device in a way that public key authentication cannot. Ongoing research continues to improve the accuracy of these devices and may open up more uses for this technology. An important issue however, is privacy. Privacy has been a cornerstone of the Internet and this is an important consideration in the advancement of authentication methods.

E. Ad-Hoc Network Security

Although there are security protocols designed for the limited computing resources available to wireless devices there are some devices for which this is not efficient enough. Protocols such as WEP and WPA were designed at a time when laptops were the primary wireless devices and this is reflected in their design. Recent years have seen an influx of devices that seek to provide wireless internet capabilities but lack the processing power to run security protocols such as WPA. These devices require security protocols that can be run on very limited resources while also offering some level of security. Figure 6 presents an example of how such a system works [6].

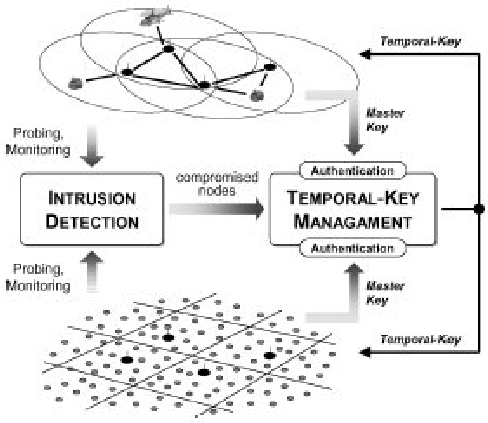

Fig. 6. Light Weight Security Protocol for Wireless Sensor Networks

In this model, groups of sensors share the same Temporal-key. Devices join the network freely but are forced to leave the network should they become compromised. Temporal-keys are broad casted using a master key that all of the devices share and can be changed either periodically or reactively. Changing keys reactively entails changing the temporal-key in reaction to an event, such as device joining or leaving the network. This option does not scale well with an increase in the size of a network due to the overhead associated with changing to a different key. More devices correlates to more opportunities for an event that initiates a key change and increases overhead costs. Changing the key periodically entails setting an interval at which the key will be changed and allows the network to minimize the overhead associated with changing keys [6].

Changing keys is important to this type of network as a result of their use of a stream based encryption method, similar to those used in WEP and WPA. It is known that using this method makes these devices more vulnerable to attack and the solution in these protocols is to change keys relatively frequently and to isolate devices whose security has been compromised. The less secure encryption is compensated for by limiting the use of any particular key and leaving attackers with a smaller window of opportunity in which to carry out their attack. Additionally, isolating the compromised nodes mitigates the potential for damage when an attack succeeds [6].

Protocols designed for this purpose, such as Light Weight Security protocol (LiSP), fall somewhere between WEP and WPA2 in terms of security. Although WEP and LiSP use the same type of encryption algorithm, LiSP is more secure because of its key management. The frequent key changes compensates for the less secure encryption. However, resource restrictions prevent LiSP from providing message integrity or authentication making it less secure than WPA. WPA draws on greater computational resources and is able to provide more security oriented functionalities [6]. This will likely improve as more research is done in this area. Wireless devices are becoming an increasingly ubiquitous part of daily life and securing them is becoming a priority. Particularly because of the existence of brute force attacks. These types of devices don't have the computational resources to combat brute forces attacks by the traditional means of using more complex encryption algorithms. This necessitates the development of a different approach that makes brute force attacks less effective without increasing the computational load.

IV. Future Trends

Over the past twenty years there have been three primary security protocols, each shoring up the weaknesses of its predecessor. Whether they are designed to protect phones, laptops,or light switches, security protocols must constantly evolve alongside the devices they protect. Improving technology provides more processing power allowing devices to utilize more complex security protocols in addition to more effective brute force and cryptographic attacks which necessitate their use.

A. Security Protocols

Current security protocols seek to provide their users with an assurance of confidentiality, message integrity, and user authentication using encryption, message integrity checks, and public key authentication respectively. This model is highly modular and unlikely to be put aside in the near future. Of the three primary portions of security protocols, encryption is the most subject to change. Message integrity is unlikely to change in the near future as the methods for implementing this functionality can be rendered useless should a third party gain access to the unencrypted message. Currently, the most effective method of ensuring message integrity is restricting access via encryption. Authentication is similarly unlikely to change in the near future. Barring the discovery of a significant flaw, the public key authentication method will likely remain the predominant method of identity authentication [7].

1) Further Development of Encryption algorithms: The most likely changes in the near future will be in the algorithms used for encryption. The constant increase in processing capacity makes it possible for wireless devices to utilize increasingly complex algorithms. This becomes necessary as the same advancements are available to the malicious entities these algorithms are designed to combat. In addition, recent events have revealed suspect activities on the part of the National Security Administration that suggest they may have discovered a means of circumventing popular means of encryption making the development new encryption algorithms a priority [4]. The focus for new encryption algorithms will be making them more resistant to brute force attacks that attempt to decrypt a message using every possible key. The alternative, Cryptographic attacks, have not been a significant factor in the development of Wifi security protocols. They require the attacker to discover and exploit a flaw in the encryption algorithm. Brute force attacks are less complex to execute and become more effective the more processing resources they have access to. The exponential growth in the speed of processors since the introduction of Wifi has made this type of attack far more prevalent than a cryptographic attack. Consequently, brute forces are a driving force in the development of new encryption algorithms.

Wired equivalent privacy(WEP), for example, was phased out as it became apparent that its 64 bit key no longer provided sufficient protection against brute force attacks. This occurred again when Wifi Protected Access(WPA) became WPA2, the encryption algorithm, temporal key integrity protocol(TKIP), to advanced encryption standard(AES) which allowed for the use of a larger key size and a more complex encryption process. While there were some cryptographic weaknesses in WEP it was primarily replaced because of how susceptible it was to brute force attacks. TKIP however, was upgraded to AES because AES is a more complex, more secure algorithm rather than because weaknesses had been discovered in TKIP [2].

This has been the traditional mode of development for security protocols. From the exclusive or used by WEP and TKIP, to the multiplication used in AES, to modulus based equations used in public key encryption algorithms. None of these algorithms suffer from pronounced cryptographic weaknesses however each is more complex and requires more mathematical computations than the last. This leads them to require more resources to utilize and exponentially more resources to attack via brute force. This trend will likely continue for the foreseeable future. While AES may be vulnerable to large organizations, such as the NSA, it is secure against those who do not have access to this level of resources and will likely remain in use for several years until it's put aside for a more complex algorithm.

2) Mobile Ad-Hoc Networks: An alternative track of development is represented by the security protocols developed for mobile ad-hoc networks. The devices that make up these networks do not have the processing capacity necessary to run complex encryption algorithms like AES. They utilize their own security protocols that sacrifice message integrity and authentication functionalities in order to run on their limited system resources. LiSP for example, uses TKIP to encrypt messages and groups within the network of devices use the same key. To bolster the security of the protocol, these devices change keys periodically and exclude any device that may have been compromised from the network [1]. While this protocol does not provide the same level of security as WPA, it requires far less processing resources to run.

More and more of the electronic devices that people utilize in their daily lives are being connected to the internet. Additionally, many of these devices (lights, appliances, televisions, etc.) are a part of mobile ad-hoc networks. Access to the internet gives them new functionalities and the necessary wifi communications must be secured. At the same time, giving them the processing capacity necessary to run WPA would increase the price of these items considerably. This is the motivation for the development of protocols such as LiSP. They offer a cost effective solution to a growing problem. Although computers are getting smaller and cheaper, larger scale devices will maintain the advantage in terms of processing power and protocols of this nature will be necessary. In the next few years I foresee this type of security protocol becoming much more common and advanced

B. Miniaturized Computers and Wireless Sensor Networks

As well as advancements in encryption algorithms, in the next few years, I also see wifi security protocols widening their focus from individual devices to include security on the network level. The rapid spread of wireless devices has prompted an equally rapid spread of public and private wifi networks. The broadcast nature of wifi communication presents new security challenges in controlling access and establishing identity.

One such challenge is miniaturized computers. Miniaturized computers have the potential to allow an entity access to a wireless network without being in the physical location. The device could be hidden within range of a wifi network and used to perform denial of service attacks, intercept messages, or gather information about the network [5]. They can carry out all of the same attacks as a larger computer without a person being physically present. This presents a potentially significant problem for the future of wifi security. However, I believe that they will be counteracted by the development of wireless sensor networks.

Wireless sensor networks allow a network to determine the physical location of devices communicating to the wireless network. They utilize modified wireless access points determine a device's physical location based on the strength of that signal as measured by various sniffers they can calculate a device's probable location [9]. This could be used to directly counter the threat of miniaturized computers. For example, snoopers could be set up to deny access to any device attempting to communicate from a location where a person would not fit or normally be. While the devices are currently only accurate within two meters, this accuracy will likely improve with research and development. It also does not account for devices hidden under furniture where someone might reasonably sit. However, it could be used to preclude the less obvious possibilities.

Wireless sensor networks could also be used to provide user authentication. The device's the device's physical location would serve as its identity. Allowing the network to provide users certain levels of access based on physical location. There are some limitations in that the portable nature of wireless devices makes their physical location exceedingly mutable and the technology needing further development to become practical. However, in the next couple years I believe that these devices will become an important part of wireless network security.

C. Conclusion

As time goes on and processing speeds increase, brute force and cryptographic attacks become more effective. In order to keep data secure, it is necessary for security protocols to constantly evolve. In the late 1990s, it became clear that WEP provided insufficient protection against brute force attacks and, in response, WPA introduced a larger key size, key management, improved integrity checks, and public key authentication. WPA2 then improved on WPA by replacing TKIP encryption with AES. Each successive protocol preserved the strengths of its predecessor while addressing the weaknesses. This constant evolution allows security protocols to protect users' data in the face of ever changing threats.

Security protocols must also be tailored to the needs of the devices they protect. Protocols such as WEP, WPA, and WPA2 work well on laptops however, they require too much processing power to be used on even smaller devices. Similarly, protocols such as LiSP are able to run on very limited processing power by sacrificing authentication and message integrity checks while also using a less complex encryption algorithm. Different devices have different security needs and processing capabilities. Securing these devices requires the use of security protocols that provide an appropriate balance of encryption, message integrity checks, and authentication to meet their security needs and processing limitations.

Finally, one of the primary reasons that wired networks are more secure than their wireless counterparts is that access is controlled by the necessity of a physical connection to the network. Technologies such as wireless sensor nodes offer a means of offering a similar functionality to administrators of wireless networks. They utilize signals received from wireless devices to determine their physical location. This allows network access to be restricted to a physical location. It also networks the ability to assign devices an identity based on their physical location. The result of these features is greater control of the network for the administrator and a more secure network for users.

References

[1] Remi Badonnel, Radu State, and Olivier Festor. Management of mobile ad hoc networks: information model and probe-based architecture. *Int. J. Netw. Manag.*, 15(5):335–347, 2005. 1110965.

[2] Halil Ibrahim Bulbul, Ihsan Batmaz, and Mesut Ozel. Wireless network security: comparison of wep (wired equivalent privacy) mechanism, wpa (wi-fi protected access) and rsn (robust security network) security protocols, 2008. 1363229 1-6.

[3] S. Kent and K. Seo. Security architectue for the internet protocol, 12 2005. RFC 4301.

[4] Joeseph Menn. Nsa infiltrated rsa security more deeply than thought, 2014.

[5] Casey Mortensen, Ryan Winkelmaier, and Jun Zheng. Exploring attack vectors facilitated by miniaturized computers, 2013. 2527002 203-209.

[6] Taejoon Park and Kang G. Shin. Lisp: A lightweight security protocol for wireless sensor networks. *ACM Trans. Embed. Comput. Syst.*, 3(3):634–660, 2004. 1015056.

[7] Larry L. Peterson and Bruce S. Davie. Computer networks: a systems approach, 2012.

[8] Ravi Srivaths, Raghunathan Anand, and Potlapally Nachiketh. Securing wireless data: system architecure challenges, 2002. 581243 195-200.

[9] Ping Tao, Algis Rudys, Andrew M. Ladd, and Dan S. Wallach. Wireless lan location-sensing for security applications, 2003. 941314 11-20.

Appendix

A. Reflection

The courses I took that were the most relevant to this project were computer organization, algorithms, and networks. Networks was particularly helpful because the same textbook that I had used for that class had a lot of information that was instrumental to putting together the technical analysis portion of this project. Particularly the information regarding how data is transmitted over wired and wireless networks as well as the section of the book dedicated to encryption. A lot of what I learned came from doing the comparison of wired and wireless protocols. As I was trying to figure out what made wired protocols more secure I started thinking a lot about exactly how the two mediums function. I didn't necessarily go out and find a lot of information about the topic however, in thinking about it so much. I was able to make much more sense of the information that I already had and to understand it better. It was also very useful because the way that computers talk to each other over the internet an two entities trying to establish secure communications are very similar processes. In both cases, each side is trying to establish the credentials of the other and has protocols in place to make sure that messages are genuine. I really wasn't expecting to find this connection but I got a lot out of it.

Algorithms came into this project as I was trying to figure out exactly what it was that made one encryption algorithm better than another. To do this, I combined elements of what I learned in both courses. One of my primary realizations about encryption algorithms is that they seek to make the problem of getting a message from encrypted text without the key intractable rather than impossible. We spent a lot of time working with these kinds of problems in that class recognizing when problems were np complete or intractable. Trying every possible key will eventually work however if there are enough keys and calculations in the algorithm. Then it'll take long enough to decrypt that the information is useless before it is compromised. The challenge was figuring out how exactly one algorithm was better than another.

This is also how my experience in computer organization was helpful. One of the things we studied in computer organization was exactly how a computer did operations at a binary level. This helped me realize that AES was better than TKIP because it takes many more binary computations to do multiplication than it does to do an exclusive or. The result of this is that it takes longer to do AES encryption and exponentially longer to do a brute force attack on it. Eventually, everything on a computer ends up in binary and the realities of how it performs operations is critical to high level concepts like algorithms. This is one of the major things I got from this project. I acquired a better understanding of just how connected these seemingly disparate subjects are. Wireless devices are becoming more and more ubiquitous in daily life. This puts them in possession of more and more sensitive data and makes it critical that wireless security measures are developed to continue protecting that data.