Threat modeling of the security architectures of various wireless technologies

Naïm Qachri Olivier Markowitch Yves Roggeman

Université Libre de Bruxelles,
Département d'informatique
CP212, boulevard du Triomphe, 1050 Brussels, Belgium
nqachri@ulb.ac.be olivier.markowitch@ulb.ac.be yves.roggeman@ulb.ac.be

Abstract

In this paper, we introduce some tools to design wireless data transmission technologies and a generic model of security layers. This model would help the engineers to introduce good security practices with less efforts and based on a threat modeling methodology. We propose also the usage of generic documents as well as a methodology that bridges the gap between the generic model and a formal tool in cryptography that will allow to update a concrete model.

1 Introduction

Since the wireless data communication technologies became more affordable and widely adopted by private users, privacy and security became important issues. Many of the present technologies have encountered some failures (WEP in WiFi) or flaws (WPA for WiFi or E0 for Bluetooth). A methodology dedicated to security would help to eliminate many of these problems of the technology development. The aim of the paper is to initiate a reflexion on how wireless technology designers could think about security design.

We will look back on what has been done on RFID, WiFi, Bluetooth, WiMAX and Wimedia technologies in the past. We will point out the main security components of those wireless technologies designed for wireless data transmission: these components being either cryptographic primitives or protocols and their combinations can have an impact on the general security of the system. We will develop a draft to study the impact of these combinations on the technologies from a security and quality point of view.

We will use, through this paper, some of the documents of the threat modeling methodology [13], developed by Microsoft, to build a generic model of security architecture for wireless data transmissions. It exists other threat modeling methodologies (such as Trike or OCTAVE [1]), but we think that the threat modeling methodology developed by Microsoft is more generic than the others and that it could be used regardless of the kind of project. Using a threat modeling methodology involves the security from the design of a project (in this case a technology). Furthermore, we will try to develop some guidelines to allow the model to be updated and expanded in the future.

The main goal of this paper is to present the basis to design the security of wireless data transmission technologies. This basis is the first step of a larger work that, we hope, will help the engineers to consolidate the security of their technology. We also want, with this model, to allow the security specialists to bring their formal analysis tools to strengthen the generic security architecture. The ideas exposed are maybe yet partial but give a good start to develop a robust generic security architecture on the basis of the chosen methodology. For that reason, we conclude in the seventh section on the theoretical and practical paths that could be followed in the future. We hope that these paths will strengthen and make the model practical and efficient.

2 Recent technologies

In this section, we will present the actual wireless technologies and their security architecture. We will point out some common points between all these technologies. These presentations are short and focus on the main security features of the technologies. We consider here only point to point technologies or technologies based on an infrastructure mode of operation, and not dynamic modes such as the ad-hoc mode, because those technologies have routing and multi-party issues that are too complex to be solved here.

2.1 WiFi

In WiFi, the architecture of the security has known many changes. From the WEP (Wire Equivalent Protection), that has known critical flaws [10, 6], the evolution of the standards has allowed to develop two safer security layers, WPA and WPA2. The first security layer is mainly axed on little size LAN and home applications and use mainly pure symmetric cryptography. The second is more axed on enterprise applications and use servers of certificates and an heavier infrastructure. Some research [7] points out today some little flaws, but they are not today critical.

2.2 Bluetooth

In Bluetooth, the architecture of the security is composed of a number of protocols and cryptographic primitives that are used to achieve integrity and confidentiality. The main primitive is E0. E0 is a stream cipher algorithm that uses a non-linear feedback shift register. Many research and flaws in the non-linearity of the system has diminished the security of E0 and the bluetooth technology [14, 16]. To summarize the security architecture, the system makes an association step thanks to the challenge and response protocol based on a PIN (with a special procedure if the PIN is fixed, as in bluetooth headset devices for example). Afterwards, each time that the two devices want to communicate, they make a pairing through an another protocol and use E0 to communicate.

2.3 WiMAX

The WiMAX technology is more difficult to analyze, because this technology is declined in two standards [2, 3] and each of the standards has developed a security layer compatible, but not exactly similar. Moreover, the infrastructure of WIMAX is very difficult to manage. Nevertheless, the security layer of the technology has some interesting common mechanisms with the other technologies.

A secret is shared between the Connectivity Service Network (CSN) and a device. Authentication of the two parties is made through different versions of EAP [4], and they can then generate session keys. This key generation allows encrypted communication through DES-CBC or AES-CCM, for the first standard, and AES-CBC or AES with CCM, for the second standard.

The weak points of the standards are the usage of DES for the encryption (this algorithm became a bit older today) and possibility to use mode of encryption without authentication of the communication.

2.4 RFID

The different existing technologies for RFID tags have led to the development of many protocols (some of them are presented in [15]) to allows secure authentication to manage some accesses. Today, many applications use RFID tags to obtain short information about a product, someone ...etc. In this context, it does not exist one security architecture but many, each depending on the kind and the manufacturer of the RFID tags used for the application. We can say that RFID is a kind of wireless data transmission medium where the hardware limitation is a strong constraint, because informations are exchanged between a tag and the reader for authentication or any other application like in any point to point technology.

2.5 Wimedia

Even the Wimedia technology is neglected now by the developers of wireless technologies, a security layer has been developed to guarantee the integrity, the authentication and the confidentiality of the data transmissions between two devices. Some of the first analyses [12] indicate that the security layers have some flaws and do not completely respect de state of art in term of security (for instance using one key for authentication and encryption instead of two). The association model has not been developed extensively in the medium access control layer of the standard, but more in the Wireless USB standard.

2.6 Summary

Many technologies with different purposes have been developed. Each time, a complete security layer has been designed and implemented, with more or less success, but all of them have common processes that are detailed in the next section. It means, for each technologies developed, that a complete security layer has been built with the same purposes than sometimes an other security layer already existing, and sometimes without reusing the experience gained on the older one. From that processes, a generic development could build strong and efficient security layers for any point to point technologies or technologies based on infrastructure mode of operation.

3 Common points

In this section, we will highlight some useful patterns to isolate the processes that play a role in the security of the technology. First, all of those technologies needs to share a secret key to authenticate and communicate with devices. This key is sometimes called the *master key*. The two devices must be associated to each other to exchange and generate that key (sometimes called the association step). From that shared secret or key, the device can use a key agreement protocol at each session of communication to generate a session key or temporary key (sometimes composed with an initialization vector). In many cases, an authentication of the devices is done during the key agreement protocol.

After the key agreement, the communication can be initiated (only if needed for RFID technologies). The majority of the presented technologies uses now an authenticated encryption scheme to communicate (the most common is the CCM mode [9], which is a combination of counter encryption mode with the cipher block chaining message authentication code algorithm and criticized in [5]).

From those technologies a generic scheme appears where the lifecycle of two devices is composed of three main steps.

1. The association step made before the first session (generally this step appears once in the lifecycle between two devices);
2. The pairing or key agreement step;

3. The authenticated secure communication step (optional step for some RFID applications).

The step 2 and 3 are used iteratively until the master (or secret) shared key is renewed. In fact, it is very rare for those architecture to renew the master key without reinitiate the association step. Sometimes, it is not possible to change it at all. Furthermore, in WPA for instance, the master key exchanged between a wireless access point and a device is the same for every device connected to the wireless access point.

Another thing that is common to those technologies, the proposed security layers generally use one single temporary key for the encryption and the authentication algorithm during a communication. In fact, two keys should be generated for each algorithm, because using the same key to authenticate and encrypt a communication could reveal informations about the key. These informations could be found thanks to some correlations between the authentication code and the encrypted message.

Sometimes some procedures are also available to manage or recover efficiently the keys in case of desynchronization, for instance, but they are in some cases dependent of the underlying technology or the application that use the technology.

4 The general threat model

The threat modeling has been developed to encompass the main threats of a technology or an IT project from the design. For that reason, we have decided to use the threat modeling methodology presented by Microsoft [13]. Since its publication, the threat modeling methodology has been integrated in the SDL (Secure Development Lifecycle) methodology. The threat modeling methodology is used to integrate the security as a part of the design of a project and not as an issue that must found an answer during the development. Using the maximum potential of the methodology can consolidate the development of a security layer for an application or a technology.

The methodology requires to implement some interesting documents. What we need in a generic technology development context are the following documents collection:

1. Internal security notes capture the important design and implementation choices for the security of the application or technology;
2. External security notes collect what the customer should be aware when he uses his device;
3. Entry points document collects information about the different way to gain access to the application or technology;
4. The project assets collects the different assets that are involved within the security layer that must be protected
5. The data flow diagram represents graphically the process of the system developed and its interactions;

These documents are really interesting, but developing them entirely in this paper would be too long, nevertheless most of these documents can be developed to capture the good practices in the world of security in wireless data transmission technology.

For instance, the external security notes should describe how customers could interact with the device and what the customer should be aware to guarantee the maximum of security when he uses a device implementing the model. If the association step requires that the user registers the master secret key from a wireless access point to the device, then he must be aware that the master key should remain secret and strong enough to not be guessed by an adversary.

Another example, the entry point must collect the possible user interfaces that a user could interacts with for a wireless data transmission. The main entries are the physical device, the wireless access to the device and, if the device is included in an computer for example, the configuration software.

The assets are not numerous in the generic model: the master key, the temporary keys, the user information (in case of RFID technology for instance), and the availability of the system are the main assets to protect. These assets can be largely described without making the generic model too specific.

From the analysis of the recent technologies and with the help of the data flow diagram, that we will describe in the next section, we can now develop the process involved in a point to point wireless security layer.

5 Common processes

From the previous sections, we have established that the link between two devices can be visualized like a generic system divided in mainly three phases. The Figure 1 shows the succession of the three phases.

We must now represent graphically the different processes involved in those three steps. This graphical representation is called a Data Flow Diagram (DFD) where the arrows indicate how the data are exchanged between the processes. In the Figure 1, an arrow shows the relation *send information to.*

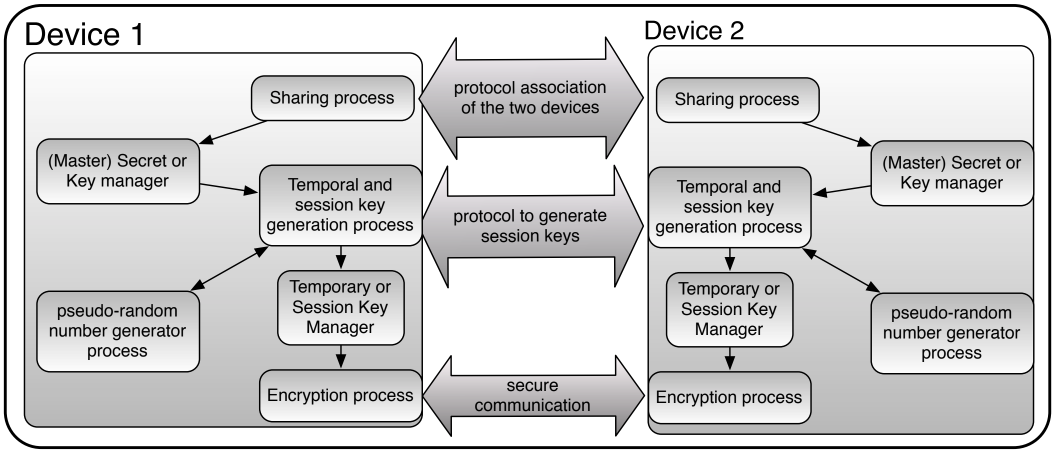
Device 1
Device 2
Sharing process
(Master) Secret or Key manager
Temporal and session key generation process
pseudo-random number generator process
Temporary or Session Key Manager
Encryption process
protocol association of the two devices
protocol to generate session keys
secure communication
Sharing process
(Master) Secret or Key manager
Temporal and session key generation process
Temporary or Session Key Manager
pseudo-random number generator process
Encryption process

Figure 1: The data flow diagram of the generic model of security for wireless data transmission

Thanks to this graphical representation, we have a clear and generic vision of a security architecture for wireless data transmission. We have then described the main informations of a generic threat model. From this model, each process are related to different topics where it exists already some secure protocols or cryptographic primitives that could be used to achieve the purpose of the security process.

From a development overview, the data flow diagram can help to build a way to compare the computational efficiency of security architectures, because each process has a cost in term of computations linked to the protocols and cryptographic primitives involved in each process.

From that generic model, it is possible to choose generic protocols and compose a complete generic architecture that uses generic cryptographic primitives. From that generic security layer, it is possible to assess the efficiency of the model from the number of call to the cryptographic primitives for a session. This measure is a good first assessment of the computational efficiency of the model. This is a useful efficiency tool for the technology designer before any implementation.

We have developed the processes and the computational efficiency assessment tool, nevertheless a formalization of that generic model will open the door to many tools that will help the cryptographic community to assess efficiently the security of a generic security architecture. A first step in the formalization of the security assessment would be to document what are the security goals for each process.

6 Data Flow Diagram, universal composability and formalization

The formalization will be possible thanks to a framework that comes from the cryptographic world called the universal composability [8]. If we develop a security layer, it will be important to determine the security goals that must achieve the technology.

This security goals have a formal equivalence named ideal functionality. An ideal functionality determine which functionality should ideally achieve a protocol to be secure. This notion comes from the universal composability framework where a protocol must emulates the ideal functionality to which it has been designed. If a protocol is said *universally composable*, using that protocol to compose a more complex protocol will not diminished the security of the protocol.

If the processes goals are described in term of ideal functionalities, then we can choose or consolidate the choice of security protocol to emulates a process of our model thanks the ideal functionalities reached. The iterative methodology is simple:

1. First, we choose the generic processes that we want design. From that processes, we choose the equivalent ideal functionalities that must reach the protocol. We develop (or adapt already existing) robust protocols that meet the needs of the ideal functionalities to compose the processes.
2. Once a protocol is chosen, it remains to choose the most secure cryptographic primitives available depending on the hardware context. The choices must be clever and coherent, because using two different hashing functions, for instance, in a security layer dedicated for RFID tags is not efficient from the implementation point of view.
3. After the development, it would be possible to simulate and test the performance of the security layer developed.

From that point, if we define a set that contains suitable ideal functionalities for each process involved in point to point wireless data transmission, the cryptographic community could develop or improve actual protocols to meet efficiently the security needs. This definition of a set of ideal functionalities would involve an iterative process that would maintain the generic model updated.

Another aspect, that can be studied, is the interactions between the cryptographic primitives used in a generic security architecture. For instance, an article [11] has studied the loss of security through the interactions of cryptographic primitives (for example using a hash function as pseudorandom number generator).

7 Future Works and conclusion

We assume that the work done is a premise of a more larger and stronger tool that would help the development of the security of the future wireless data transmission technologies and improve the actual technologies. The involvement of the cryptography community and the wireless data transmission technology developer community would strengthen the privacy of our communication in an efficient way. Nonetheless, we have focused the development on the security of some critical processes and the three main steps to create a secure way to communicate. In a future work, we will integrate the notion of concurrent interactions within the process model, and study the weakening of cryptographic primitives through their multiple interactions.

In conclusion, we have showed in this paper that it is possible to find some generic patterns in all those security architectures. We have given a first version of an evaluative and formal tool to analyze the security layer in wireless data transmission. This threat model is generic and easily manipulable to be adapted, upgraded, and maintained without starting again from the beginning. We do not say that performance and quality testing should disappear, but the two approaches must be considered together during the development to ensure a security architecture against flaws. Many work must be done yet, but we are convinced that allowing bijective interactions between the technology and security developers will improve the general quality of the designs of security layers.

References

[1] http://www.cert.org/octave/.

[2] *"Ieee standard for local and metropolitan area networks part 16: Air interface for fixed broadband wireless access systems"*, 2004.

[3] *"Ieee standard for local and metropolitan area networks part 16: Air interface for fixed broadband wireless access systems: amendement for physical and medium access control layers for combined fixed and mobile operation in licensed bands"*, 2005.

[4] B. Aboba, L. Blunk, J. Vollbrecht, and J. Carlson. *"Extensible authentication protocol* (EAP)*"*. RFC 3748, June 2004.

[5] Mihir Bellare, Phillip Rogaway, and David Wagner. *"The EAX mode of operation"*. In Bimal Roy and Willi Meier, editors, *Fast Software Encryption*, volume 3017 of *Lecture Notes in Computer Science*, pages 389–407. Springer Berlin / Heidelberg, 2004.

[6] Andrea Bittau, Mark Handley, and Joshua Lackey. *"The final nail in WEP's coffin"*. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, pages 386–400, Washington, DC, USA, 2006. IEEE Computer Society.

[7] Cédric Blancher and Simon Marechal. *"Packin' the pmk of the robustness of wpa/wpa2 authentication"*.

[8] Ran Canetti. *"Universally composable security: A new paradigm for cryptographic protocols"*. Cryptology ePrint Archive, Report 2000/067, 2000.

[9] Morris Dworkin. *"Recommendation for block cipher modes of operation : The ccm mode for au- thentication and confidentiality"*. Special publication 800-38c, NIST, May 2004.

[10] Scott Fluhrer, Itsik Mantin, and Adi Shamir. *"weaknesses in the key scheduling algorithm of rc4"*. In Springer Berlin / Heidelberg, editor, *Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography*, pages 1–24, 2001.

[11] Chi-Jen Lu. *"On the security loss in cryptographic reductions"*. In Antoine Joux, editor, *Advances in Cryptology - EUROCRYPT 2009*, volume 5479 of *Lecture Notes in Computer Science*, pages 72–87. Springer Berlin / Heidelberg, 2009.

[12] Naïm Qachri and Yves Roggeman. *"the flaws and critics about the security layer for the wimedia mac standard"*. In *30-th symposium on Information Theory in the Benelux*, pages 89–96, may 2009.

[13] Frank Swiderski and Window Snyde. *"Threat Modeling"*. Microsoft professional. Microsoft Press, 2004.

[14] Serge Vaudenay and Lu Yi. *"Cryptanalysis of bluetooth keystream generator two-level E0"*. In Springer, editor, *The 10th International Conference on the Theory and Application of Cryptology and Information Security, Advances in Cryptology, ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, pages 483–499, 2005.

[15] Jiang Wu. *"Cryptographic protocols, Sensor network key mlanagement, RFID authentication"*. PhD thesis, University of Waterloo, Ontario, Canada, 2009.

[16] Yaniv Shaked and Avishai Wool. *"Cryptanalysis of the bluetooth E0 cipher using obdd's"*. In Springer Berlin / Heidelberg, editor, *9th international conference, ISC 2006*, volume 4176 of *Lecture Notes in Computer Science*, pages 187–202, 2006.