Touchstone of Trust: Physical Contact in Ad-Hoc Wireless Network

Pin Nie
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
niepin@cc.hut.fi

Abstract

Due to the distinct application conditions and environment, ad-hoc wireless network presents particular requirements on security establishment. Traditional solutions and frameworks for trust building and authentication do not fit anymore, because of either lack of some key elements or the new constraints imposed. This paper examines the differences of ad-hoc wireless network, extracts the problems during the initial setup of a security association and provides a method called *Physical Contact* to guarantee the reliable first connect between two devices for subsequent secure communication. A collection of existing models and designs serve as the basis and are introduced to explain the concepts and ideas. A new proposal is extended at the end of the paper.

KEYWORDS: trust, authentication, security establishment, ad-hoc wireless network, out-of-band channels, visual channel

1 Introduction

One developing trend of embedded systems and devices is to enable network communications, especially in ad-hoc wireless pattern. In this way, the benefit of each node can be maximized and services can be enjoyed anywhere at anytime. Let's take a look at some typical situations. Several friends meet at a place and want to play games together on their portable terminals, e.g. PSP (PlayStation Portable) or mobile phones. Electronic devices in the home can "talk" to each other and fulfill a complicated mission, say using a terminal (e.g. laptop or PDA) to give orders to other devices or read values from them. In a scope-limited public place, e.g. airport or cafe, people want to use some services, like printing or surfing on the Internet. Information or files sharing among the PDAs (Personal Digital Assistant) during the group meeting. By virtue of the ad-hoc wireless network, all these applications can be easily carried out to satisfy people's needs. At that time, each device, as one node of the network, may take advantage of the services provided by its neighbor devices. Instead of duplicate the functional modules, the existing services spread to all members. The cost is low and the efficiency is high.

However, the security issues of this improvising wireless connectivity bring up many questions. How to identify other peers and authenticate their claims? How can I trust the strangers? How to build up the basic trust and exchange security parameters (e.g. keys) for subsequent secure communication in an open environment? In this paper, we investigate the conditions and rules behind these questions and make up the general assumption in Section 2. Based on the assumption, the proposed method: Physical Contact is analyzed how well it solves the problems in Section 3. In Section 4, pertinent approaches and solutions that have been proposed are discussed. An proposal concerning specific circumstances is extended in Section 6. Section 7 gives a summary of the topic.

2 Assumption Statements

Considering the connectivity, applications in ad-hoc wireless network can be divided into two modes. One is end-to-end direct services, such as peer-to-peer information exchange, master-slave model and client/server paradigm. The typical situations aforementioned belong to this type. The other is multipoint relay service, like ad-hoc routing. There are many differences between these two categories, though they have overlapping area. Herein, we discuss the issues under the first mode, which is the necessary condition of our method stated later.

For the end-to-end services in ad-hoc wireless network, there are five features regarding to the "first connect" of security establishment as below.

1. **Direct Talk**, there are only two parties involved for each session of communication. No intermediary node is required. Any middle node is treated as unwanted third party, which may be an attacker. Pairing is the most typical case.

2. **No trusted third party**, unlike the Public Key Infrastructure (PKI), there is no trusted third party or element, like Certificate Authority (CA), in ad-hoc wireless environment. Hence, there is no such *security token or trust assertion* that can be passed over the network. No way to collect information about the other peer.

3. **Demonstrative Identification** [1], is required for two reasons. Firstly, the initiator or the service requester should show his intention by intuitive act of touching the callee. Otherwise, the request may be a mistake or the caller may not actually know which callee he is trying to contact. Secondly, it is also a presence confirmation for both sides [7]. It can serve to limit the control range of the authority. This is a strong restriction for any attack, if the attack must be done without being detected, especially for the malicious outsiders. Further-

more, presence property can reduce the confusion and mistakes.

4. **Security Transient Association** [9], implies that the security bindings have to change frequently, due to the unstable relationship between any two peers in ad-hoc manner and ephemeral session of communication. For example, in the group meeting, a PDA may switch its role repeatedly between master and slave, depending on the source location. Paired devices have to be re-paired due to the change of their owners.

5. **No previous context**, means the trust and security has to be established without any history, such as blacklist or whitelist. No experience of the other peer.

In addition to the five security characteristics in ad-hoc wireless network, there are three constraints on the portable terminals [4] in the applications, which we must take into consideration for the sake of feasibility of solutions.

1. **User Interface**, input and output of the terminal may be very limited. Some low end may only have a few buttons and a single light-source, such as an LED, but high performance handsets may have camera and high resolution LCD display. Therefore, we need to consider different situations and take full advantage of any form of input and output as much as possible.

2. **Computing Power and Memory**, the computing power of the portable devices is often minuscule compared to PC. High demanding on computing and memory would cause the slow response of the device, which makes it impractical to be applied in an ad-hoc environment.

3. **Battery Consumption**, every portable device has a time limit to function before the next recharging. As the only power support, battery is used for all the functions and operations on the device. We must note that the security establishment usually is not the primary mission. It means the battery consumption should not take too much, which affects other functionalities. Thus, the energy exhaustion attacks are a real threat in this situation. In the paper [9], a new attack named *sleep deprivation torture* is addressed.

3 Principles of Physical Contact

With the assumptions given in the previous section, a few technical requirements on the solution can be deduced as follows:

1. **Bootstrap**, the method should be able to provide an intuitive imprinting on one party or both during the first connect to bootstrap the security establishment. This can compensate the lack of trusted third party.

2. **Proximity Detection**, in order to fulfill the demonstrative identification, proximity should be counted in as a main factor, which is also a hidden feature of ad-hoc communication.

3. **Presence Confirmation**, it is the best way to capture the intention and set location restriction to prevent most of attacks. Meanwhile, as a weak property, presence reduces the requirements (e.g. algorithm complexity) and improve usability [8].

4. **Pre-authentication** [1], because there is no context for the first connect, a pre-authentication phase is necessary to be done for subsequent authentication (e.g. key exchange) of the parties. This step could be carried on another channel other than the wireless link for content communication later. It refers to the out-of-band channels, which is talked in section 4.2.

5. **Flexibility**, due to the various constraints of the portable devices, each specific solution is attached with some conditions on the equipment, for example, camera or radio transmitter. The term *Physical Contact* is to define a general framework. Popular cases are detailed as examples.

3.1 Attack Models

For better understanding of the purpose of Physical Contact, a brief of attack models is also needed. By applying different criteria, attacks can be categorized into several types. Most general taxonomy is to separate attacks into *Active Attacks* and *Passive Attacks*. In the Active Attacks, the attacker is able to transmit data to one or both of the parties, or block the data stream in one or both direction. It is possible that the attacker is located between the communicating parties. It has three major forms as below [5]:

1. **Modifying data stream**, it includes both inserting into the data stream or deleting data from it. It breaks the integrity of the data.

2. **Playback of data**, it has two modes, playback of data from another connection (e.g. reflection attack) and playback of data that had previously been sent in the same and opposite direction on the same connection (e.g. replay attack).

3. **Man-in-the-middle**, abbreviated as MITM. In this attack, the intruder sits in the middle of the communication link, intercepting messages and substituting them with his own messages. Simply say, the attacker tries to fool the parties to believe they are talking to each other directly, while they actually are talking to the attacker.

The first two attacks are actually based on the third one, i.e. the MITM attack. They are separated out for the clarity of the actions behind. MITM is a bit too general to cover all active attacks, launched by the third party.

In the Passive Attack (a.k.a eavesdropping), the attacker cannot interact with any of the parties involved, but listen to the communication imperceptibly. He attempts to break the system solely based upon the observed knowledge. Often, this is the first step of a sophisticated attacking. The adversary collects the data and values for making use of them later in the active attacks or illegally get access to the sensitive information. Fig.1 illustrates these two attack models.

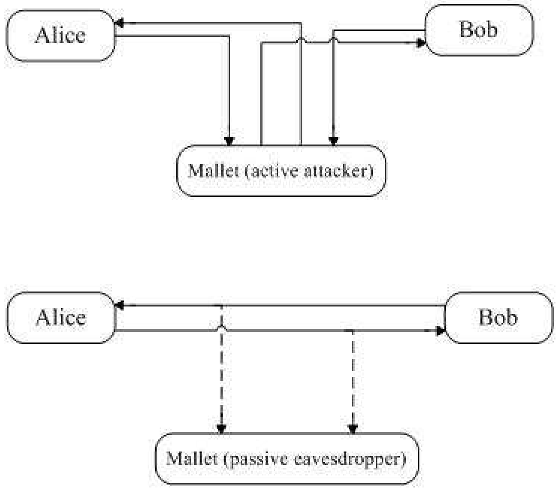

Figure 1: Attack Models: active attack and passive attack

In our method Physical Contact, we target at MITM and passive attacks. It means the first feature in the ad-hoc wireless communication, i.e. "Direct Talk" must be guaranteed, and the method should prevent any unwanted parties from obtaining any information as well. Note that we just need to make sure the design is valid before key agreement or other cryptography establishment, then it is secure enough. Because for the rest of the threats, the key protocols will take care of them.

To give a clear definition of Physical Contact on the basis of the ideas and purposes stated above, we say Physical Contact is a procedure to setup the basic trust and exchange security factors (e.g. keys if authentication is provided) during the first connect between two directly associated parties, within a scope-limited environment, where one can *sense* (e.g. seeing or touching) the other, or mutually for both. Meanwhile, one or both also have the basic perceivability of the surroundings. This imposes the real difficulty for the attacker to launch the attacks, without being detected.

4 Technologies and solutions

Using Out-of-Band (OOB) channel in the first connect phase is the primary idea in Physical Contact. OOB denotes a separate communicating band (i.e. auxiliary channel) other than the one used for the subsequent communications, for exchanging security parameters (e.g. transmitting authentication data) or control information. Based on human roles and underlying technologies' features, we categorize the available solutions into four types, i.e. Authenticated String, Radio, Infrared and Ultrasound, Visual Channel and Biometric Channel. Examples are given below and principles are inspected.

4.1 Authenticated String

The main idea in authenticated string is to use *Commitment Schemes* to exchange a commitment, which contains a "hidden value" combined with the keys for some cryptography protocols. It gets human involved as the auxiliary channel during the establishment. There are two ways to authenticate the value. One is String/Numeric Comparison, and the other is called Passkey-based scheme [10]. In the first model, the user (or two users) acknowledges the check values on both devices by either accepting or rejecting the result. It requires both devices should have a display and a simple input to reveal user's confirmation. For the second model, the user inputs the value (a shared secret) generated by one device, to the other devices. In this case, only the previous device needs a display, or both only have keypads. Authenticated string model is applied in Diffie-Hellman protocol to securely transfer the keys encrypted by the value. In the article [3], a technique named DH-SC (String Comparison) is proposed upon the model, which utilizes random verification strings and manual comparison. In order to make it easier to use, they encode results into human readable words and use human readable identifier in the calculation. This is important to be user-friendly, which is a key factor of security establishment. Another paper [11] introduced a solution to achieve message authentication by using extractable or equivocable commitment schemes, with Short Authenticated Strings (SAS). But it does not address how to exchange SAS securely. One obvious advantage of string-based designs is the narrowband channel could be used.

4.2 Radio, Infrared and Ultrasound

By employing the transmitting range of radio, infrared and ultrasound, Location Limited Channel (LLC) is devised with distance binding. It is based on an assumption that there are no other parties that are closer to dedicated parties thank they are to each other [3]. Simply say, the nearest node is the one the user wants to communicate. Otherwise, it fails. Thus, the proximity check between the two devices has to be performed. However, these techniques ask for special transmitter and receiver to carry the channel. Further, the high precise timing measurement (nanosecond) imposes another difficulty on the devices. It increases the cost of the devices and limit the scope of its usage. The article [3] also proposed another Diffie-Hellman extension called DH-DB (Distance Bounding) to prevents MITM and eavesdropping by doing the proximity verification. It assumes there should not be any other users in the integrity region of two dedicated communicating parties. Otherwise, they would be detected. Both ultrasound and radio can be employed as the carrier.

One more design with radio is the DH-IC (Integrity Codes) [3], which makes use of the un-reversibility of the signal transmitting in the communication media (channel). It implies the emitted signals cannot be blocked and the communicated sequence cannot be modified without being detected. The precondition is the receiver is turned on and is listening on the (correct) channel during the sender's transmission. However, the turn-on action has to be coordinated by the users. It ensures the integrity, but the passive attack is left untouched.

4.3 Visual Channel

As the display and camera are becoming easier available and the quality keeps improving, visual channel is getting more popular and important in security establishment. The idea to use camera and LCD display on mobile phones, PDAs in a security setup communication is possible.

The paper [7] explored a solution, using camera phones for human-verifiable authentication. The system utilizes 2D barcodes and camera phones to implement visual channel for authentication and demonstrative identification of devices. It resembles the barcode scanning at the front of cash desk in the supermarket. But here the 2D barcode can be generated automatically and displayed on the screen of the device. It could be a sticker as usual, if the device that needs to be authenticated has no display and relevant logic module. In this case, it suffers the static drawbacks, which expose under the attack, like faking a sticker. Note that the device discovery must be performed beforehand in any case. Other out-of-band technologies could be applied for this purpose, like infrared and bluetooth. However, this design puts high assumption on the equipments, especially when doing mutual authentication for both sides.

To reduce the requirement posed on the devices, the paper [8] provides a better design of visual channel in constrained devices. It replaces the high quality LCD display with single light source (or LED), plus short authenticated integrity checksums. By transforming the identification information from barcodes into the blinking sequences of LEDs, the visual channel is implemented in another way with lower requirements on authenticated party. It fits many application cases, when the services are in master-slave or client/server model. For example, the public printer, copy machine and access point do not need such an expensive upgrade with high quality of LCD display anymore. Furthermore, it could be dynamically configured and repeatedly done with *security transient association* in ad-hoc environment. There is a variant solution (Loud-and-Clear) applying the same principle with audio technique [10].

4.4 Biometrics Channel

Rather than taking unique values from man-made generator or sticker, biometrics channel captures the unicity of human characteristics, like grip pattern, fingerprint, voice spectrum and so on. With certain encoding algorithm, the unique value can be extracted from these properties. The paper [2] explored grip pattern and proposed a new model to do so. From easy-to-use point of view, this channel is the best without any logic load on the users. However, the accurate recognition technique is a heavy burden on its applications. Such a recognisor module is expensive for wide use. Moreover, the accuracy of recognition still needs much improvements [6].

5 Evaluation

To evaluate all solution stated above, we should setup some criterions beforehand. The first criteria is the benefit, which means how many security requirements it can fulfill, for example, five items and attacking threats issued in section 3. The second criteria is the ranking sequence of security factors. According to the analysis [9], three predominate factors ranks in following order: Availability, Integrity (authenticity) and Confidentiality. For availability, usability and flexibility are two correlative elements, having great influence on popularity and applying scope. Usability is often related with another two conditions, i.e. device constraints assumption and employed algorithm complexity. The more extra assumptions made on devices, the less usability it has. The more complex of the algorithm, the less to usability. Concerning flexibility, we focus on the fundamental principles of the solutions for two questions. Is it good for mutual authentication or just unidirectional? Unidirectional methods have to be executed twice to do mutual authentication, which raise the overhead of communications. Could it be carried out in different forms with the help of various presentations of inputs and outputs? For example, visual channel has a fixed requirements, i.e. at least one camera. While for authenticated string policy, both the input and the output can vary a lot, depending on the specific situations. The third criteria is the user friendly. How much logic and operation loads imposed on the users?

With the evaluation standards above, human knowledge or biometric based solutions are simple with few easy operations. But the latter one requires more sophisticated devices (i.e. recognition modules). Visual channel is also easy to use with the same security level. But the algorithms are complex, leading to the intensive computing, which is a critical factor on portable devices' application. Radio, infrared and ultrasound designs is almost fool prove model. Nevertheless, the special modules and high measurement demands set a big barrier to distribute.

Considering two situations in ad-hoc wireless applications, we can give a fitting map for all solutions. The first case is one-way authentication for ad-hoc services in public places, where the requirements on SP's equipments should be as low as possible. This explains the two technical evolutions, i.e. from String Comparison to Passkey, and from SiB [7] to VIC [8]. The other case is mutual authentication for peer-to-peer communications, which we should make full use of popular equipments for functions on portable devices, e.g. camera and LCD on mobile terminals. Thus, String Comparison and SiB are more suitable here. To sum up, the balancing game happens all the time. The tradeoff between usability and complexity and the tradeoff between security and efficiency, execution overhead (e.g. integrity verification) need to be weighed according to the practical situations.

6 Extensions

For the most normal scenarios, the policy and solutions stated above are good enough. Nevertheless, in some high risky environment, stricter design is required. For example, the first connect happens under a noisy and confusing circumstance. Many requests come to one end at the same time. In this case, they can be processed either in sequence way or in parallel. Whereas, the sequence order is suggested in complicated situation for three reasons. Firstly, to keep every "first connect" to be atomic makes the process safer. Otherwise, it suffers the "state failures", which means the procedure may break down during the states transit. This is critical sometimes when the system cannot clean or recover the procedure properly. Then some security hole would emerge. Secondly, parallel processing could easily lead to the resources exhaustion, especially when doing with the constrained devices in our assumption. The third reason is the complexity it introduces. For example, the interleaving management policy is often complicated in a parallel system.

However, since the physical contact gets human operation involved, the sequence processing may cause heavy delay problem, depending on the every person's response. To handle it, a fixed time count down is set as the default timeout scheme. Extensively, the idea of *exclusive serving* could be carried out during the whole security establishment, including key exchange protocol (e.g. only one connection is allowed and one request is processed at any time). A lock mechanism could be developed to build a "closed cycle" with only two dedicated parties in the open ad-hoc environment. The biggest benefit is all active attacks can be prevented within the validation period. For the rest of communication, the job is relayed to the encryption protocols. Upon this framework, more effort can be extended in the implementation on details.

7 Conclusions

In this paper, we examined the security issues that arise in the ad-hoc wireless network. According to the features of this network and its applications, a careful assumption is made. With the help of existing designs and solution, we try to give a more general framework to gather essential ideas behind. Examples are provided to demonstrate the principles and implementations with careful evaluation follows. Finally, an extension is proposed to deal with a specific situation, i.e. high risky environment. Due to the diversity of the applications in ad-hoc wireless network, no comparison is provided with precise measurement. Details of introduced solutions can be found in the reference.

8 Acknowledgements

I would like to thank Prof. K. Nyberg, Prof. N. Asokan, Jukka Valkonen and Vesa Vaskelainen for their valuable comments and suggestions on my paper.

References

[1] D. Balfanz, D. Smetters, P. Stewart, and H. Wong. Talking to strangers: Authentication in adhoc wireless networks. In *Symposium on Network and Distributed Systems Security (NDSS '02)*, San Diego, California, Feb. 2002. NDSS.

[2] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis. Feeling is believing: a location limited channel based on grip pattern biometrics and cryptanalysis. At `http://eprints.eemcs.utwente.nl/5694/01/00000174.pdf`, 2006.

[3] M. Cagalj, S. Capkun, and J.-P. Hubaux. Key agreement in peer-to-peer wireless networks. In *Proceedings of the IEEE on Cryptography and Security*, volume 94, pages 467–478. IEEE computer society, Feb. 2006.

[4] J.-E. Ekberg. Key establishment in constrained devices. At `http://www.tcs.hut.fi/Studies/T-79.7001/2006AUT/seminar-papers/Ekberg-paper-final.pdf`, 2006.

[5] A. Eng. Secure telnet. At `http://www.pvv.ntnu.no/~asgaut/crypto/thesis/thesis.html`, 1996.

[6] A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*.

[7] J. M. McCune, A. Perrig, and M. K. Reiter. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *IEEE Symposium on Security and Privacy*, pages 110–124. IEEE computer society, May 2005.

[8] N.Saxena, J-E.Ekberg, K. Kostiainen, and N. Asokan. Secure device pairing based on a visual channel. In *2006 IEEE Symposium on Security and Privacy*. IEEE computer society, May 2006.

[9] F. Stajano and R. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Proceedings of the 7th International Workshop on Security Protocols, ACM*, pages 172–194, London, UK, 2000. Springer-Verlag.

[10] J. Valkonen. Ad-Hoc Security Associations for Wireless Devices. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2006.

[11] S. Vaudenay. Secure communications over insecure channels based on short authenticated strings. In *CRYPTO*, pages 309–326, 2005.