PRE-AUTHENTICATION USING INFRARED

Amir Spahić
aspahic@foi.hr
Faculty of Organization and Informatics Varaždin
University of Zagreb
Pavlinska 2, 42000 Varaždin, Croatia

Michael Kreutzer, Martin Kähmer, Sumith Chandratilleke
{kreutzer, kaehmer, sumith}@iig.uni-freiburg.de
Institute of Computer Science and Social Studies
Dept. of Telematics
University of Freiburg
Friedrichstraße 50, D-79098 Freiburg, Germany

ABSTRACT

Using complex authentication and verification methods is not always feasible in application fields with time and resource restrictions. However, fast and configuration-less authentication methods are required in infrastructure-less application fields like emergency aid. In this paper we present an authentication mechanism which uses context information for its first phase, the so called *pre-authentication phase*. During this phase a connection between two devices is established to generate a common secret as a prerequisite for the subsequent authentication. We present an implementation of a special device called "magic wand", using optical communication for the pre-authentication phase. With the help of this device it is also possible to quickly authenticate devices for subsequent use in service discovery.

1. SCENARIO

Personal health monitoring can be done with sensors that are connected wirelessly with a base station on the belt of the patient. These sensors measure values like body temperature, blood pressure and pulse etc. The doctor only has to connect his PDA to the patient's base station to simply read their values. In a disaster area this technology could accelerate the triage of patients [VeKr03]. However, as this communication is wireless, the doctor must be sure that he has taken values of the right patient.

In this scenario there is need for an authentication mechanism that will explicitly interconnect the right devices during a restricted time period and locality. Authentication mechanisms for infrastructure-less environments like the above mentioned example should be based on wirelessly retrieved data (optical, radio, sensors). At the same time it must disable intentional or unintentional involvement of a third party. Besides solving the security problem the mechanism should be fast, cheap, simple and easy to use.

2. ATTACKER MODEL

The endpoints of the communication, i.e. both devices in consideration, are assumed to be trustworthy. Using exclusively wireless technology, the focus of the attacker model lies in the air interface. According to the application fields in infrastructure-less environments and the dynamics of an ad-hoc basis of usage we assume as intentional attack eavesdropping (originated by a man in the middle also capable to effectuate a subsequent replay attack) and as unintentional attack the identification of the false device (misdirection). Denial of service attacks are not regarded in this paper.

3. RELATED WORK

Even if the wireless technology gets more and more important, two devices that are in the range of each other, should not in each case "talk" to each other: this imposes not only scalability problems but also security problems, especially related to authentication [StAn00]. However, an authentication mechanism is needed to explicitly "marry" two formerly mutually unknown devices [FeAW01], i.e. two devices which haven't any (even partial) knowledge about the existence of one other. Such an authentication mechanism has been proposed in [BSSW02] and has been called "ad-hoc authentication" in [ChKr03].

As the focus of [BSSW02] lies in asymmetric cryptography, its mechanisms even protect against active attacks like impersonation during authentication establishment. However, it is questionable whether this attacker model is realistic for the majority of the application scenarios. According to [VeKr03] being secure against passive attacks is often sufficient in infrastructure-less environments. Furthermore asymmetric cryptography is a heavyweight mechanism that can be only performed by computationally strong devices. Looking at small devices as they are widely used in pervasive computing, in many cases asymmetric cryptography is too slow and needs too much energy. For many of these devices this mechanism is unfeasible.

In this paper we present a concrete implementation and evaluation of the ideas and concepts presented in [ChKr03].

4. FOUR PHASES OF AD-HOC AUTHENTICATION

According to [ChKr03] the four phases of ad-hoc authentication are (in [BSSW02] these are almost the same, however it lacks the last phase):

I. Pre-authentication: Secure establishment of a shared secret or mutual knowledge of identifying data about the other device (for example a public key). This may be done not only by direct communication**,** but also with the help of, or even exclusively by using context (in [BSSW02] the latter is also called "demonstrative identification"). Context may not only be sensed but also can be explicitly created, cf. the acceleration events of smart-its friends [HMSA01].

II. Authentication: Verification of the identity using the shared secret.

III. Use of authentication: In most cases authentication is the basis for subsequent security mechanisms like access control, encryption, integrity, etc.

IV. Releasing the security association: This means "forgetting" the data collected in *I* and *II*, i.e. explicitly deleting any information relating to the (former) partner device. This is done to prevent replay attacks.

5. PRE-AUTHENTICATION MECHANISM

5.1. Design decisions

The following design decisions are derived from the needs of infrastructure-less environments.

If context is used for pre-authentication, a location-limited channel should be taken [BSSW02]. When using communication technologies, they should have physical limitations in their transmissions, for example the necessity of line of sight and limited range, like "the PDAs are directed to each other and have a distance less than 20 cm". The reasons for the need for a location-limited channel are twofold:

1. This kind of channel guarantees authenticity. This means that it is impossible or difficult for an attacker to transmit in the location-limited channel. This property is sufficient to ensure that information exchanged over the location-limited channel will allow the parties involved to securely authenticate each other (even in the presence of potential attacker).

2. This kind of channel prevents unintentional false identification of the partner device (misdirection).

All radio technologies are inappropriate for *phase I* as radio propagation is undirected, they do not guarantee the necessary location limited channel.

We chose IrDA (standard according to the Infrared Data Association based on optical communication via infrared) for the pre-authentication phase. The connection is limited to a one-meter distance and the beam widening is only 30º. Infrared beams have defined orientation and we can use them to transfer data (the so called "point and shoot" principle).

There are also some other possible solutions concerning *phase I* like physical contact (for instance key distribution device interface, also called "fill gun"), common acoustical experience, shaking two devices (common acceleration experience, cf. [HMSA01]), etc. We suppose usability to be scenario-dependent. The question of usability and fitness for different application fields must be evaluated by making a usability study with existing implementations of all these approaches.

As we don't want to use asymmetric cryptography, we establish a Diffie-Hellman secret in the pre-authentication phase. An eavesdropper cannot calculate the resulting common key of both parties even if the attacker is able to intercept all messages.

Phases II, III, IV can be done based on a radio link (we are planning to use bluetooth).

We are using PDAs for our sample implementation and evaluation, as they are most appropriate to the above-mentioned example of triage in disaster areas.

5.2. Pre-authentication as a three-step mechanism

Now we can define pre-authentication as a three-step mechanism:

1. Establish an infrared connection,
2. Use the Diffie-Hellman algorithm to create a key,
3. Terminate the infrared and establish the radio (bluetooth) connection.

These three steps are the basis for the subsequent phases.

6. IMPLEMENTATION

The used PDAs have some limitations like small processor power and restricted energy resources.

In the following we will call our implementation of pre-authentication phase IrEx. According to the example of triage we have implemented a client-server model. Both partners must have a self-standing application running called the irexserver. The client part is also a self-standing application, called the irexclient. The device which starts the irexclient is the client which initiates the exchange.

First we developed IrEx primarily for the Pocket PC platform but now we have a solution for Palm devices too – this means we can use *Pocket PC – Pocket PC*, *Palm – Palm* and *Pocket PC – Palm* connections.

6.1. Basic idea

To create a Diffie-Hellman key we need the following parameters:

1) P and Q – large prime numbers, where (P < Q) and ((Q-1) / 2) is also a prime number
2) Xa and Xb – secret random numbers (each side has its own X)
3) Ya and Yb – public numbers

P and Q are common for both sides so we give the right to the initiator to choose them. In our case these numbers are determined by the irexclient application.

The random number generators on both sides create their appropriate X numbers. Those numbers are kept secret and they are not exchanged.

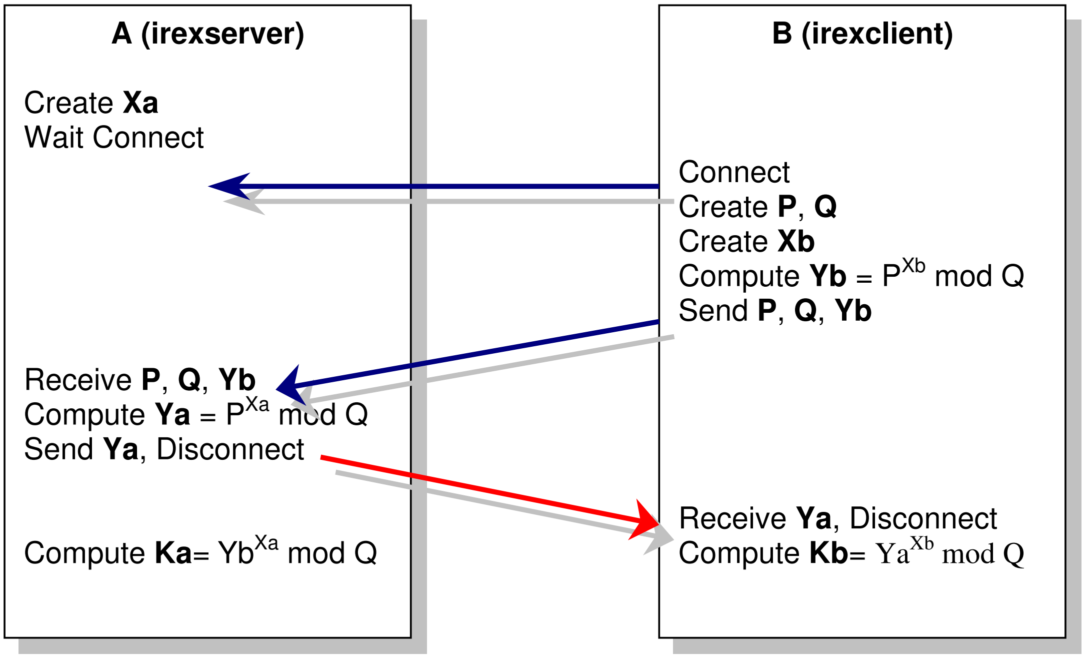

Figure 1: Protocol of the pre-authentication phase

As it can be seen in *figure 1*, the server waits for an incoming request. When the client is started it tries to connect itself to the server. If the client finds the server, first it sends and then receives the necessary parameters for the creation of the common secret key K. After exchange of three messages on both sides, both of them can compute K and terminate the infrared connection.

6.2 Implementation details

To test the IrEx application, HP iPaq 2210 Pocket PCs were used. It is recommended to specify buttons in order to start the applications irexserver and irexclient. The irexserver starts with the right button and the irexclient with the left button. Pressing the right button starts the server program. It listens for incoming requests or shuts down if the client program is called.

When the irexserver is started on both sides, nothing will happen until one side initiates an exchange and thus takes the client role. When the right button is pressed the irexclient (and with it the secret key creation) is started.

When an incoming request is noted, the server closes all other server ports until the exchange procedure is done. Pressing the left button (on the second device) starts the client program and the exchange procedure is started. This procedure consists of the following steps:

- The server opens a socket and waits for the client
- The client opens the socket and sends the request (sending the generated prime numbers and the public key in the same message)
- The server gets the prime numbers (P, Q), computes its public key and sends it to the client; at the same time it sends a message to close the socket_client.

If the client doesn't receive an instruction within 5 seconds it knows that something went wrong and it gives a double beep alert. In the other case, it gives a single beep and an LED signal. The server has no timeout.

The procedure will not start automatically; it demands explicit user action which increases the security.

7. CONCLUSION AND FUTURE WORK

We have made a conceptual design of the pre-authentication phase of ad-hoc authentication. Furthermore, we implemented it using the infrared technology. The performance results of the first tests are promising; however, to gain reliable results we need further systematic testing.

Our application does not have the full functionality of ad-hoc authentication. When using bluetooth for phase II and possibly III we will take the key from the IrEx application as a basis to ensure the desired security property between the partners. The bluetooth part will probably implement the OBEX protocol too. At this stage of the project we will make performance measurements and user tests.

Our prototype inspired us to a new user interface: the initiating PDA can be used as a "magic wand" to select one device from a group of devices. This is useful to support device discovery: in many cases it is more natural to select a device in the vicinity by pointing to it instead of selecting it from a list of service alternatives on a small screen. It is even thinkable to implement such a "magic wand" on a smaller device, to enhance it with an RFID reader, thus building new security bridges between the real world and the virtual world.

8. ACKNOWLEDGEMENTS

We thank Kerry McGawley for her helpful comments on readability and Prof. Dr. Günter Müller and Prof. Dr. Blaženka Divjak for encouraging support. This research has been supported by the Kolleg "Living in a smart environment" of the Gottlieb Daimler- and Karl Benz-Stiftung and by the TEMPUS project of the European Commission.

9. REFERENCES

[ChKr03] S. Chandratilleke, M. Kreutzer: "Credential-basierte Ad-hoc-Authentifikation" (engl.: Credential-based Ad-hoc-Authentication), netzwoche Netzguide E-Security Netzmedien AG, Basel, March 2003.

[BSSW02] D. Balfanz, D. Smetters, P. Stewart, H. Wong: "Talking to strangers: Authentication in adhoc wireless networks", In Symposium on Network and Distributed Systems Security (NDSS '02), San Diego, California, february, 2002

[FeAW01] L. M. Feeney, B. Ahlgren, A. Westerlund: "Spontaneous networking: an application-oriented approach to ad hoc networking". IEEE Communications Magazine, June 2001.

[HMSA01] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, H. W. Gellersen: "Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts". Proc. of UBICOMP 2001, Atlanta, GA, USA, Sept. 2001

[VeKr03] G. Venghaus and M. Kreutzer: "Cooperation agreement of the German Red Cross with the department of telematics of the university Freiburg and requirements specification for the use of pervasive computing in mobile hospitals". Emergency Response Unit of the German Red Cross, Berlin, 2003.

[StAn00] F. Stajano, R. J. Anderson: "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks". Lecture Notes in Computer Science, Vol. 1796, Springer, 2000 pp. 172-194.