Trust model, communication and configuration security for Personal Area Networks[1]

Christian Gehrmann, Thomas Kuhn, Kaisa Nyberg and Peter Windirsch

Ericsson, Siemens AG, Nokia and T-Systems Nova

ABSTRACT

This paper describes new security architecture for personal area networks. We give an overview of the PAN model and the PAN security problems that we have tackled. The problem area is illustrated with a business meeting example. We base our architecture on a new PAN reference model, which we describe. The trust model on which the security architecture is based is also described. Our novel idea of a PAN "personal CA" concept fits well into this new trust model. Internal PAN communication security as well as secure configuration and access control are discussed.

I. INTRODUCTION

Next generation of mobile communications is expected to be different from current systems. We foresee changes both for the type of *accesses* to the networks and the *terminals* used to access the networks. We expect future multi-function mobile terminals to consist of several different configurable components, which may be worn about the body and are connected through local wireless communication. The second work package of the IST SHAMAN project addresses security problems for *distributed dynamically configurable* terminals. A distributed terminal consists of several *components* within physical proximity to each other and the user or users. They are interconnected with local communication links like short-range wireless connections, for example Bluetooth. This type of personal local network used to be called a *Personal Area Network* (PAN). Our project addresses the security problems related to the configuration and communication in a PAN. This paper contains an overview of the most recent results of the second work package of SHAMAN.

A. PANs and PAN security

Within the SHAMAN work we focus on personal networks consisting of a limited number of components within the proximity of a person. Only components *owned* and controlled by one user or components directly communicating with a component in control of one user are considered. Using this limitation, we can define a PAN *reference* model of reasonable complexity that is applicable for the distributed terminal scenarios we would like to cover [1].

We have as a goal to provide security architecture applicable to our PAN reference model. Several security problems need to be tackled in order to provide a sound architecture. The basis for the architecture is a trust model that describes the basic security relations between different PAN components. We have decided to use a component centric trust model. We view the surrounding component in relation to a *PAN reference component.* Once the basic trust relations are defined, we can work with solutions of how to set up the *security associations* between the different components. A security association in combination with appropriate security protocols can be used to secure the local communication interface between components in the PAN. The level of security needed for a communication service offered by on component to other components is determined by security *policies.* Furthermore, the access to particular services should be restricted and part of the component security policy. In summary, our paper covers the following security topics:

- Trust model
- Internal PAN communication security
- Secure configuration and access control

In order to illustrate how these different areas fit together when providing secure configuration and communication for a typical PAN scenario; we next discuss a PAN business meeting example.

B. Business meeting example

We consider a business meeting scenario where two persons, an employee and a guest, meet in a room equipped with a video projector. The two persons in the room are both carrying one laptop each. The laptops contain presentation information that the both users would like to present to each other using the video projector. Furthermore, after the presentation, the guest would like to send over his presentation to the employee. We assume that the video projector and the laptops support common short-range wireless interfaces that they use for the communication. Hence, we have a PAN scenario with three different components:

1. A video projector
2. A guest laptop
3. An employee laptop

The situation is illustrated in Figure 1 below.

[1] The work presented in this paper has been partially funded by the IST-2000-25350 SHAMAN project.

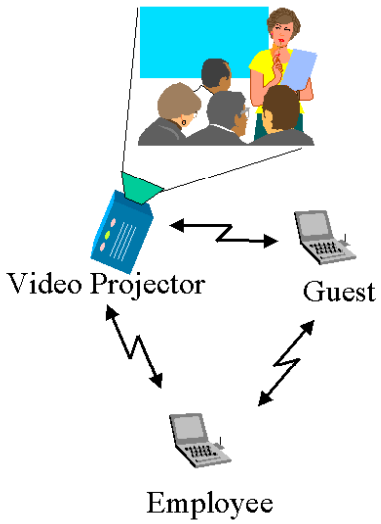

Figure 1: business meeting

In this example we have only three components and no complex trust relations can be expected. We can choose to consider the whole network from any of the three components point of views. If we consider the view of the video projector, it can be connected to either the employee laptop or the guest laptop. It is reasonable to assume that since the video projector and employee laptop both belong to the same organization, the video projector would trust the employee laptop more than the guest laptop. We will in section III introduce a *trust model* that reflects this type of differential trust using three trust levels.

Since the presentation material might be sensitive information, the employee and guest would like to have the local wireless communication protected from eavesdropping. This can be provided by a proper *security protocol* and a shared secret that is a part of a *security association* between the two components. It is reasonable to require that a security association between the video projector and employee laptop should be possible to create with no or almost no user interaction. On the other hand, it is reasonable to assume that a security association between the guest laptop and the video projector (or the one between the two laptops) might need some user interaction. Furthermore, some user actions might be required in order for the video projector to grant the guest laptop *access* to the projector services. These types of security aspects and requirements are included into the security architecture described in this paper.

II. A PAN REFERENCE MODEL

In order to provide a nice PAN security architecture we first need to define a PAN. We have defined a PAN reference model that we think is easy to understand and work with, and that is applicable to our practical use cases [1].

Inspired by the work of the IEEE 802.15 working group [2], we define a PAN as follows:

A PAN is a collection of fixed, portable, or moving components within or entering a Personal Area, which form a Network through local interfaces. A Personal Area is a sphere around a person (stationary or in motion) with a typical radius of about 10 meters.
The definition includes components that are carried, worn, or located near the body, e.g., personal digital assistants (PDAs)/handheld personal computers (HPCs), printers, microphones, speakers, headsets, bar code readers, sensors, displays, pagers, mobile phones, and smart cards.

Below a list of basic PAN reference model terms is given:

- **Component / Service / Application:** A PAN consists of components. Each *component* is an independent computing unit. That is, it must have processing capabilities as well as digital memory. A component must have at least one local interface that it can use to connect *directly* to at least one other component but need not to be connected to every PAN component. A component can be both stationary and mobile. A *service* is a communication or computing service offered by a component either locally (i.e. through a user interface of some sort), or remotely to other components. A service need not be security related. Each component keeps a list of services it offers as well as rules/policies for access and service discovery and/or advertisement. An *application* is a process running on a component. An application can be a service offered within a component or to other components. An application might try to connect to other components and utilise the services they offer.
- **User / Owner:** The *user* of a component is the person who physically controls and operates the component in accordance with the policies configured in the component. Each component has a single *owner*. By specifying an appropriate policy, the owner of a component might allow users to temporarily use his or her device.
- **Local interface / Global network interface:** Each component has at least *one local communication interface* suitable for direct connection to other PAN components. We consider both fixed and wireless PAN interfaces. Apart from one or several PAN interfaces a component may also have a *global network interface*.
- **Security policy:** Each component has different *security policies*. We distinguish between two different types of security policies: local and remote. The local security policy determine which resources on the component that a user is allowed to manage and if authorisation is demanded or not. It also describes how configuration and executables should be installed. The remote security policy determines the requirements on access to the component services and the communication between the service and the entity in the PAN that utilise the service. This includes authentication and encryption requirements as well as access rules.

III. NEW TRUST MODEL AND PERSONAL CA CONCEPT

The trust model we use describes the security relationships between the components in a PAN. On component level we use a model with one component as reference. We view all other components in relation to this single component. This allows us to describe any trust relation between any component and all other components in a PAN. We only distinguish between three different *basic* trust levels:

- Untrusted components
- Second party components
- First party components

A. Untrusted components

Untrusted components are by definition all PAN components that the reference component has no security relations with and that it has not been able to identify and/or verify the identity of. Typically any new component that a user buys is an untrusted component from the perspective of all the other components belonging to the same user.

B. Second party components

A second party component has an owner different from that of the reference component. Second party component identities can be verified, i.e., authenticated. A second party component might be trusted for some actions while still be untrusted for other actions. The fine grain level of trust given to a particular second party component is determined by the security policy of the reference component and is part of the service level trust model.

C. First party components

A first party component has the same *owner* as the reference component. Furthermore, all first party components are able to identify all other first party components and *distinguish* a first party component from a second party component or untrusted component.

In order to distinguish between a first party and non-first party component, a first party component must hold some unique protected information. Here we slightly extend the "resurrecting duckling" model used by Stajano and Anderson in [3]. At manufacture a component does not have an owner or users. Instead, the component is made first party by an *initialisation* or (referring to [3]) at an *imprinting* phase. At the imprinting phase the necessary keys are created or transferred to the component that can be used to identify the component to all other first party components of the same owner. It is the owner that is responsible for the primary imprinting of his/her devices. We suggests an imprinting procedure based on transfer of public keys and issuing of certificates (see personal CA concept below).

A first party component might be trusted for some actions while still be untrusted for other actions. The fine grain level of trust given to a particular first party component is determined by the security policy of the reference component and is part of the service level trust model.

D. Service level trust model

Access to a specific service might require service lookup, authentication, encryption etc. All service lookup, authentication and encryption are performed on *component* level. That means that a specific service on a component cannot be authenticated, but only the component providing this service. The access rules as well as communication security requirements are determined by the security policy. In section V we describe how we handle security policies in our architecture. Which components and users of components that are allowed to access specific services are completely determined by the policy rules. The policy rules might distinguish between different second party components as well as different first party components and users.

E. Personal CA concept

First party components have a specific status in our security architecture. The reason for introducing this category is that for many PAN applications it is enough with a straightforward security policy for connections to first party components. A simple policy would demand authentication to identify a first party component. Once authenticated, we would like to set up a secure communication channel towards the first party component and it will be given automatic access to most services (compare for example the video projector to employee connection in the business meeting example in section I). Hence, we need user friendly and convenient methods for identify/authenticate first party components and to create security associations with first party components.

A nice solution for authentication and key exchange with first party components is to use public keys and certificates. Authentication and key exchange using a certificate demand the certificate being signed by a common trusted third party. In a personal environment this can be achieved by letting the owner issue certificates to all his/her component using a particular "CA device". We call such a device a "personal CA device". A personal CA device might be a mobile phone, PDA or laptop device that fulfil security requirements for certificate issuing and signing. The general principles for using a personal CA device in our security architecture are the following:

- At least one component, the personal CA device, among the set of component belonging to one owner possesses the private signing key of the owner (can be a person or an organization).
- Each component in the PAN possesses a private-public key pair.
- When the person (or organization) receives a new PAN component, the component is imprinted (see subsection C above) by securely transferring the

public key of the personal CA. Furthermore, the personal CA issues a new certificate certifying the public key of the new component by signing it together with other information using the private key of the personal CA. The imprinting can be carried out in several different ways. The personal CA concept requires a "personal PKI" that must satisfy several security requirements. Detailed descriptions and different options are given in [4].

- Two components belonging to the same owner that would like to authenticate each other and exchange secret keys can do this by using standard protocols based on public key exchange and certificates. This can be done automatically without any user involvement. This is an improvement compared with key exchange methods based on user PIN inputs that is used in for example Bluetooth [5].

IV. INTERNAL PAN COMMUNICATION SECURITY

The PAN security architecture defines a higher layer method for establishing security associations between first party components through imprinting as explained in Section III.*C*. This initial security association is used as a key management facility for securing internal PAN communication.

It may be foreseen that in the future personal devices are capable of running general-purpose transport layer protocol for transporting communication between the devices. Then the natural approach would be to perform authentication of the devices above or at the transport layer, and secure the communication data also at the transport layer. However, this is still not always the case, and may not be in the future, either. The new applications such as ubiquitous computing make use of PAN networks consisting of simple devices that may have only link layer capabilities. Therefore the PAN security architecture supports security services at the link layer in order to make full benefit of the existing link layer security systems.

In internal PAN communication the protocols performed at different layers end within a single device thus making it easy to transform security associations of a PAN component between different layers.

The decision about the usage of available security services is made by the PAN component as defined by its security policy.

In what follows, it is assumed that the first party components have been imprinted by a personal CA, share the public key of the CA, and own certificates of their credentials, including a public key, signed by the CA.

A. Authentication and key establishment

After being imprinted two first party components can exchange any information authenticated and confidentially based on their certificates and the public key of the CA. It is possible to run a higher layer authentication protocol based directly on their public keys, and derive mutually known authenticated secret keys for confidentiality and integrity protection of the communication.

Another possibility, is to perform only the authenticated key exchange at the higher layer. The mutual authentication of the components is performed at link layer, where also the keys for integrity and confidentiality protection of the data are derived. This approach is favorable for devices running a wireless link technology with good authentication and key agreement functions.

Two second party components need to perform an initialisation step before they can start the mutual authentication step. The purpose of the initialisation is to exchange an integrity-protected copy of the public key of each other's CA. After this has been done the components can verify each other's certificates, obtain each other's public keys, and continue in the same way as explained above for the first party devices.

The initialisation of two party components can be performed directly assisted by the users. If the corresponding two second party CA components have already been initialised, then the components can get the public key of each other's CAs through their own CA.

B. Integrity and confidentiality protection

Integrity and confidentiality protection of data can take place at link layer or at a higher layer. Existing link layer mechanisms can be used if allowed by the security policy of the component. It is also possible to protect the integrity of the communication at the link layer and the encryption at a higher layer, or vice versa. It is essential that the keys for both purposes have been established through authenticated key exchange mechanisms.

V. SECURE CONFIGURATION AND ACCESS CONTROL

Besides of securing the communication between different components within a PAN it is mandatory to manage the security features and policies for shared use of PAN components to protect the data and resources. Due to the limitations of the PAN components on computation power, memory space, and communication bandwidth, the security methods have to take these restrictions into account. It is also important to rely only on the features provided by the two communicating PAN components since it could be possible that no external or centralized infrastructure (e.g. CA and PKI services) is available, e.g. due to the absence of wireless network coverage.

A. Policy handling and authorisation

The PAN device security policies are used to define the authorisation to

- access private or public data on the PAN component. This may include user data (files, directories) as well as device configuration and status information.
- access services and applications provided by the PAN component by a user or by other components in the PAN.
- access resources on the reference component, such as available memory space and CPU performance, consumables (e.g. paper on a printer component) or other cost incurring services (e.g. a remote network access service) available for the requesting component.
- use the secure execution environment on the PAN component for remote program code to be downloaded and executed.
- set up the communication between the PAN components in a secured (encrypted) or unsecured way.

As mentioned in Section II, the security policies can be differentiated according to PAN component local or remote scope. The identity of a service requesting remote PAN component can be derived from the authentication procedure (see Section IV) and might be required for checking the access control information carrying PAN certificates or PAN tickets described below.

To reduce the user interaction requirements for policy configuration to a minimum, default policies for at least the three basic categories of PAN component trust levels (as introduced in Section III) shall be available. These default policies may be used as a starting point to further refine the authorisation and access policies depending on the party requesting a certain service.

B. Access control mechanisms

For the access control mechanisms, we can make the distinction of those methods using local storage for the access control information on the reference component which provides a certain service and the remote storage. We can assume each manageable object on the PAN component (e.g. file, service, application, …) has attached access attributes for the three basic trust classes (first party – second party – untrusted). In the case that more refined access control is required (e.g. depending on the requestor's identity, …), the additional attributes could be stored on the serving PAN component by means of an access control list (ACL). Such an access control list therefore belongs to the local storage category and sufficient memory space needs to be allocated for the attribute records of all possible users and / or PAN component trust levels. To limit the effect of continuous growth of memory space for the attribute records, aging mechanisms to limit the lifetime of the permissions shall be implemented.

In the second storage category, the access attribute records are generated by the serving PAN component when a new requestor is registering for a service. The attribute record is secured against modification and delivered to the requestor for storage and presentation when accessing the serving PAN component. Different approaches for securing the attribute records can be chosen:

- PAN certificate: it is based on the personal CA concept and contains the attributes which are signed by the private key of the issuer. When presented to the serving PAN component, the signature is validated and the access permissions are granted to the specified level.
- PAN ticket: due to the higher computational requirements of public key algorithms compared to secret key methods, an alternative approach would cryptographically hash the attributes with a secret key only known to the serving PAN component. It is the only one who could then also check for the validity of the access permission record.
- Encrypted PAN ticket: this extension of the previous approach keeps the attribute information secret to the requestor.

If required, the PAN certificates could be generated by a different first party component e.g. in the case that the serving component has no appropriate user interface to manage the access policies.

Both the PAN certificate and PAN ticket approach have the advantage of lower memory requirements for the serving component compared to the ACL approach. However, the latter approach has the advantage of simple modification of permissions, even if the device to which these permissions were granted is (temporarily) not connectable by the serving component. ACLs may still be needed for managing the local user's permissions even if the access control information for remote components is stored remotely. In all cases, local management of already consumed resources (CPU time, memory, consumables, external network access time, …) relevant for accounting is needed to check for compliance with the resource attribute values stored remotely in the PAN certificate or ticket.

REFERENCES

[1] IST-2000-25350, "SHAMAN DO3 - Interim Report (Security Architecture for Future Mobile Terminals and Applications)", June 2001.

[2] IEEE 802.15 Working Group for WPANs™, at http://grouper.ieee.org/groups/802/15/

[3] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security for Ad-hoc Wireless Networks". B. Christianson, B. Crispo, and M. Roe (Eds.*), Security Protocols, 7th International Workshop Proceedings*, LNCS, vol. 1796, Springer1999.

[4] IST-2000-25350, "SHAMAN D07- Intermediate specification of PKI for heterogeneous roaming and distributed terminals", *Draft*, February 2002.

[5] Bluetooth SIG, *Specification of the Bluetooth system, Core, Part B "*Baseband specification*",* Version 1.1, 22 February 2001, at http://www.bluetooth.com/