Acquisitions Editor: Kristin Klinger
Development Editor: Kristin Roth
Senior Managing Editor: Jennifer Neidig
Managing Editor: Sara Reed
Copy Editor: Ashlee Kunkel, Holly J. Powell
Typesetter: Jamie Snavely, Carole Coulson
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanonline.com

Copyright © 2008 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher.

Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Handbook of research on wireless security / Yan Zhang, Jun Zheng, and Miao Ma, editors.

p. cm.

Summary: “This book combines research from esteemed experts on security issues in various wireless communications, recent advances in wireless security, the wireless security model, and future directions in wireless security. As an innovative reference source for students, educators, faculty members, researchers, engineers in the field of wireless security, it will make an invaluable addition to any library collection”--Provided by publisher.

Includes bibliographical references and index.

ISBN 978-1-59904-899-4 (hardcover) -- ISBN 978-1-59904-900-7 (ebook)

1. Wireless communication systems--Security measures. I. Zhang, Yan, 1962- II. Zheng, Jun, Ph.D. III. Ma, Miao. IV. Title.

TK5102.85.H35 2008

005.8--dc22

2007036301

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book set is original material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

If a library purchased a print copy of this publication, please go to http://www.igi-global.com/reference/assets/IGR-eAccess-agreement.pdf for information on activating the library's complimentary electronic access to this publication.

Chapter XI
Key Distribution and Management for Mobile Applications

György Kálmán
University Graduate Center – UniK, Norway

Josef Noll
University Graduate Center – UniK, Norway

ABSTRACT

This chapter deals with challenges raised by securing transport, service access, user privacy, and accounting in wireless environments. Key generation, delivery, and revocation possibilities are discussed and recent solutions are shown. Special focus is on efficiency and adaptation to the mobile environment. Device domains in personal area networks and home networks are introduced to provide personal digital rights management (DRM) solutions. The value of smart cards and other security tokens are shown and a secure and convenient transmission method is recommended based on the mobile phone and near-field communication technology.

A PROBLEM OF MEDIA ACCESS

On the dawn of ubiquitous network access, data protection is becoming more and more important. While in the past network connectivity was mainly provided by wired connections, which is still considered the most secure access method, current and future users are moving towards wireless access and only the backbone stays connected by wires. In a wired environment, eavesdropping is existent, but not as spread and also not easy to implement. While methods exist to receive electromagnetic radiation from unshielded twisted pair (UTP) cables, a quite good protection can be achieved already by transport layer encryption or deploying shielded twisted pair (STP) or even fibre.

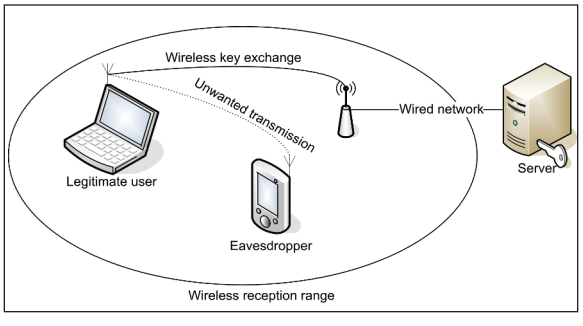
New technologies emerged in the wireless world, and especially the IEEE 802.11 family has drastically changed the way users connect to networks. The most basic requirements for new devices are the capability of supporting wireless service access. The mobile world introduced general packet radio service (GPRS) and third generation (3G) mobile systems provide permanent IP connectivity and provide together with Wi-Fi access points continuous wireless connectivity. Besides communications devices such as laptops, phones, also cars, machines, and home appliances nowadays come with wireless/mobile connectivity.

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

Protecting user data is of key importance for all communications, and especially for wireless communications, where eavesdropping, man-in-the-middle, and other attacks are much easier. With a simple wireless LAN (WLAN) card and corresponding software it is possible to catch, analyse, and potentially decrypt wireless traffic. The implementation of the first WLAN encryption standard wired equivalent privacy (WEP) had serious weaknesses. Encryption keys can be obtained through a laptop in promiscuous mode in less than a minute, and this can happen through a hidden attacker somewhere in the surrounding. Data protection is even worse in places with public access and on factory default WLAN access points without activated encryption. Standard Internet protocols as simple mail transport protocol (SMTP) messages are not encoded, thus all user data are transmitted in plaintext. Thus, sending an e-mail over an open access point has the same effect as broadcasting the content. With default firewall settings an intruder has access to local files, since the local subnet is usually placed inside the trusted zone. These examples emphasise that wireless links need some kind of traffic encryption.

When the first widespread digital cellular network was developed around 1985, standardisation of the global system for mobile communication (GSM) introduced the A5 cryptographic algorithms, which can nowadays be cracked in real-time (A5/2) or near real-time (A5/1). A further security threat is the lack of mutual authentication between the terminal and the network. Only the terminal is authenticated, the user has to trust the network unconditionally. In universal mobile telecommunications system (UMTS), strong encryption is applied on the radio part of the transmission and provides adequate security for current demands, but does not secure the transmission over the backbone. UTMS provides mutual authentication through an advanced mechanism for authentication and session key distribution, named authentication and key agreement (AKA).

Figure 1. A basic problem of broadcast environment



A LONG WAY TO SECURE COMMUNICATION

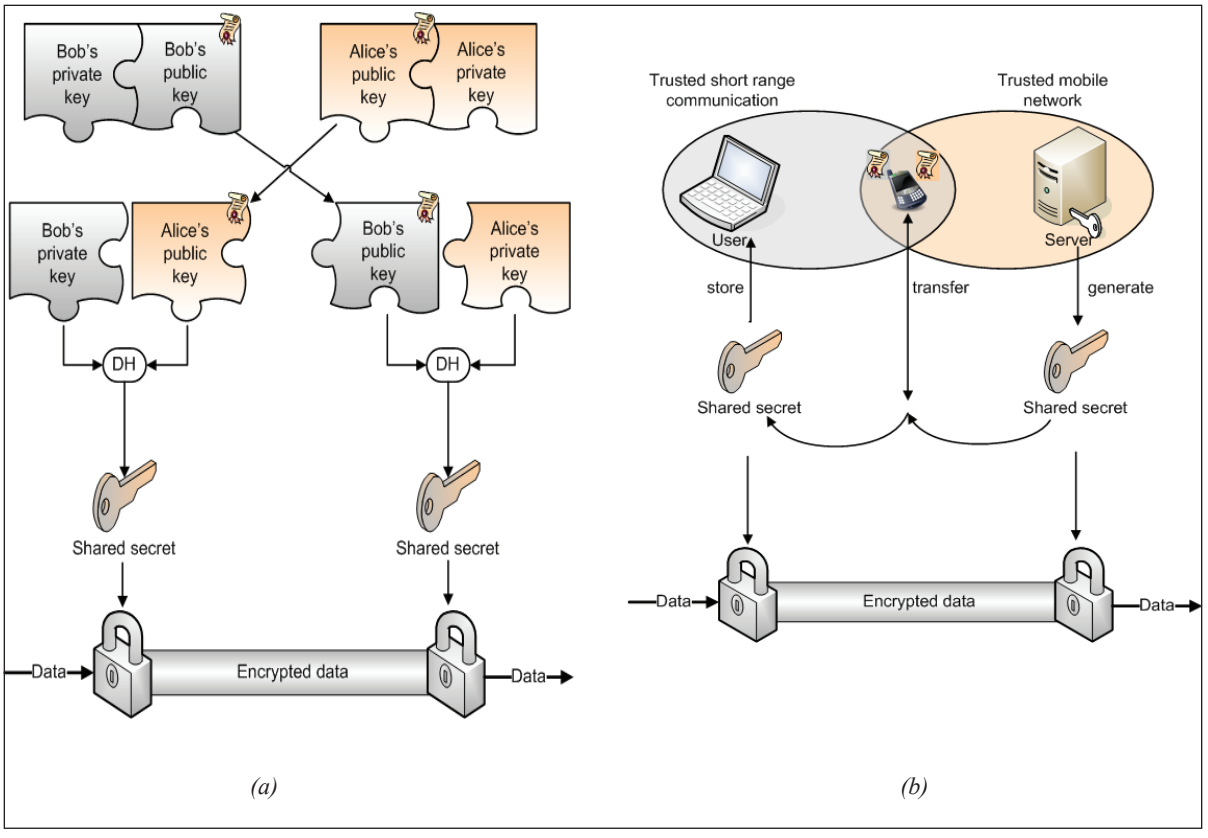
Applying some kind of cryptography does not imply a secured access. Communicating parties must negotiate the key used for encrypting the data. It should be obvious that the encryption key used for the communication session (session key) cannot be sent over the air in plaintext (see Figure 1).

In order to enable encryption even for the first message, several solutions exist. The simplest one, as used in cellular networks is a preshared key supplied to the mobile terminal on forehand. This key can be used later for initialising of the security infrastructure and can act as a master key in future authentications.

In more dynamic systems the use of preshared keys can be cumbersome. Most of WLAN encryption methods support this kind of key distribution. The key is taken to the new unit with some kind of out of band method, for example with an external unit, as indicated in Figure 2. Practically all private and many corporate WLANs use static keys, allowing an eavesdropper to catch huge amounts of traffic and thus enable easy decryption of the content. This implies that a system with just a secured access medium can be easily compromised. Non-aging keys can compromise even the strongest encryption, thus it is recommended to renew the keys from time to time.

Outside the telecom world it is harder to distribute keys on forehand, so key exchange protocols emerged, which offer protection from the first message and do not need any preshared secret. The most widespread protocol is the Diffie-Hell-

Figure 2. (a) Diffie-Hellmann key exchange and (b) out-of-band key delivery



man (DH) key exchange of Figure 2, which allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

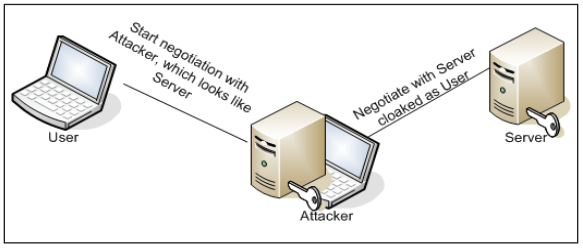
This protocol does not authenticate the nodes to each other, but enables the exchange data, which can be decoded only by the two parties. Malicious attackers may start a man-in-the-middle attack (see Figure 4). Since this problem is well-known, several modifications enable identity based DH, for example Boneh, Goh, and Boyen (2005) showed a hierarchical identity based encryption method, which is operating in fact as a public key system, where the public key is a used chosen string.

Public key infrastructure (PKI) can help defending corresponding parties against man-in-the-middle attacks. Public key cryptography is based on the non polynomial (NP) time problems, for example of factorisation or elliptic curves.

Two keys, a public and a private are generated. The public key can be sent in plaintext, because messages encrypted with the public key can only be decoded by the private key and vice versa. The two way nature of public keys makes it possible to authenticate users to each other, since signatures generated with the public key can be checked with the public key. Message authenticity can be guaranteed. Still, the identity of the node is not proven. The signature proves only that the message was encoded by the node, which has a public key of the entity we may want to communicate with.

Identity can be ensured by using certificates. Certificate authorities (CA) store public keys and after checking the owner's identity out of band, prove their identity by signing the public key and user information with their own keys. This method is required for financial transactions and business and government operations. Without a

Figure 3. Principle of a man-in-the-middle attack



CA, the public keys can be gathered into a PKI, which provides an exchange service. Here, most commonly, a method called web of trust is used. A number of nodes, who think that the key is authentic, submit their opinion by creating a signature. The solution enables community or personal key management, with a considerable level of authenticity protection.

While public keys can be sent, private keys must be kept secret. Although they are protected usually with an additional password, this is the weakest point in the system. If the user saves a key in a program in order to enter the key automatically, security provided by the system is equal to the security of the program's agent application. Private firewalls and operating system policies usually will not stop a good equipped intruder.

Another security issue for terminals is the lack of tamper resistant storage. Usage of smart cards is a solution to this issue, but introduces additional hardware requirements. The lack of secure storage is getting much attention in DRM schemes. Most DRM schemes use a software-based method, but also hardware-assisted ones have lately been introduced.

All these authentication methods, secure storage and rights management support secure data exchange, but they do not protect the privacy of user credentials, preferences, and profiles. Ad hoc networks, like personal area networks (PANs), which move around and are dynamically configured open for intrusion attacks on the privacy.

Thus, protection of user credentials in wireless environments is one of the focal points of current research. Before addressing privacy, we will first summarise issues in key management protocols.

FROM KEY EXCHANGE TO ACCESS CONTROL INFRASTRUCTURE

Mobility and wireless access introduced new problems in network and user management, as compared to fixed network installations with, for example, port-based access restrictions. The network operators want to protect the network against malicious intruders, charge the correct user for the use, and provide easy and open access to their valued services.

The first step to get access to an encrypted network is to negotiate the first session key. This has been solved in coordinated networks like mobile networks through pre-shared keys. Authentication and access control is provided by central entities to ensure operations.

In computer networks, which are not controlled in such way and usually not backed-up by a central authorisation, authentication, and accounting (AAA), different methods have been created for connection control. The basic method is still to negotiate encryption keys based on a preshared secret. Typical preshared keys are a password for hash calculation, one time password sent via cell phone or keys given on an USB stick.

There are several solutions to protect the data transmitted over a wireless link. In private networks, security based on preshared keys is a working solution. In corporate or public networks, a more robust solution is needed. The most promising way is to integrate session key negotiation into the AAA process. Since providers or companies have to identify the connected user, they rely on an AAA infrastructure and have an encryption of user credentials as compulsory policy. A certificate-based medium access control and AAA system is advised, where AAA messages can carry also the certificates needed to secure the message exchange.

As public key operations induce a lot of network traffic, the negotiated session keys have to be used in the most efficient way. Encryption protocols designed for wired environments, like transport layer security (TLS) do not consider problems associated with the broadcast transmissions and limitations of mobile devices. In a wired, or at

Figure 4. TLS key negotiation

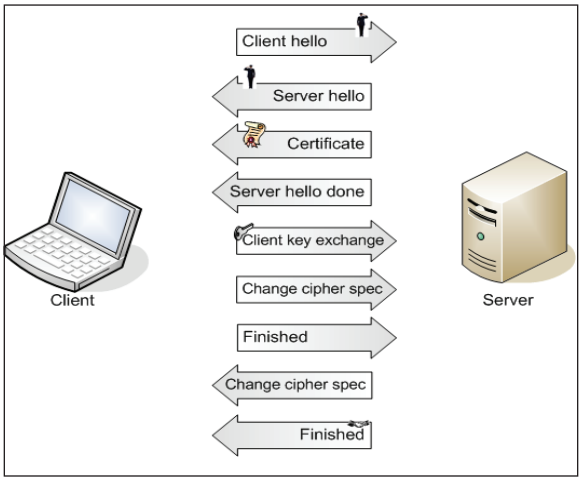
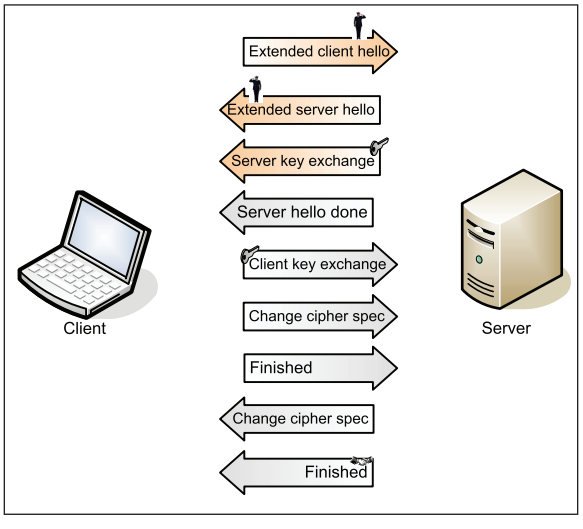


Figure 5. TLS-KEM key negotiation



least fixed environment, computational cost of key negotiations is usually neglected. For example TLS is using several public key operations to negotiate a session key. This can be a problem for mobile devices, since computational cost is much higher in asymmetric encryption. The standard TLS suite uses lots of cryptographic operations and generates a too large message load on wireless links (see Figure 5).

If a mobile device wants to execute mutual authentication with a service provider, with certificate exchanges, it can lead to big amounts of data transferred over the radio interface beside the high computing power needs.

In environments with limited resources, authentication and identity management based on preshared keys is still the most effective solution. Badra and Hajjeh (2006) propose an extension to TLS, which enables the use of preshared secrets instead the use of asymmetric encryption. This is in line with the efforts to keep resource needs at the required minimum level in mobile devices. A preshared key solution was also proposed by the 3rd Generation Partnership Projects (3GPP, 2004) and (3GPP2, 2007) as an authentication method for wireless LAN interworking. The problem with the proposed solution is preshared keys does not provide adequate secrecy nor identity protection in Internet connections. To deal with this problem, the TLS-key exchange method (TLS-KEM) provides identity protection, minimal resource need, and full compatibility with the original protocol suite as seen in Figure 6.

In direct comparison, the public key based TLS needs a lot more computing, data traffic, and deployment effort.

In UMTS networks, an array of authentication keys is sent to the mobile in authentication vectors. In the computer world a good solution would be using hash functions to calculate new session keys, as these consume low power and require little computing.

A moving terminal can experience a communication problem, as the overhead caused by key negotiation might extend the connection time to a network node. A preserved session key for use in the new network is a potential solution in a mobile environment, as it speeds up the node's authentication. Lee and Chung (2006) recommend a scheme, which enables to reuse of session keys. Based on the AAA infrastructure, it is possible to forward the key to the new corresponding AAA server on a protected network and use it for authentication without compromising system security. This can reduce the delay for connecting, and also reduces the possibility of authentication failure. Since the old session key can be used for authenticating the node towards the new AAA server, connection to the home AAA is not needed any more. The

messages are exchanged as follows (Lee & Chung, 2006): when sending the authorisation request to the new network, the node also includes the old network address it had. The foreign agent connects to the new local AAA server and sends an authentication request. The new AAA server connects to the old one sending a message to identify the user. The old AAA authenticates the message by checking the hash value included, and generates a nonce for the terminal and the foreign agent. The server composes an AAA-terminal answer, which is composed from a plain nonce, an encrypted nonce using the key shared between the old foreign agent and the terminal. Then the whole message is signed and encrypted with the key used between the two AAA servers. When the new AAA receives it, decrypts and sends the message to the new foreign agent. Based on the plain nonce, the agent generates the key and sends down the reply, which includes also the nonce encrypted by the old AAA. After the authentication of the user towards the network, the user can start using services.

Key distribution and efficiency in e-commerce applications is another important aspect. The network's AAA usually does not exchange information with third parties or can not use the authentication data of the network access because of privacy issues. Current security demands require mutual identification of communicating parties in an e-commerce application. This can easily lead to compromising the customer to companies (for example in a GSM network, the user has to trust the network unconditionally). If the user can also check the identity of the service provider, at least man-in-the-middle attacks are locked out.

When a user starts a new session with a service provider, this session should be based on a new key set. The session key has to be independent from the previous one in means of traceability and user identity should not be deductible from the session key, thus ensuring user privacy. For mutual identification, a key exchange method is proposed by Kwak, Oh, and Won (2006), which uses hash values to reduce resource need. The key calculation is based on random values generated by the parties, which ensures key freshness.

The use of hash functions is recommended in mobile environments, providing better performances for public key based mechanisms (Lim, Lim, & Chung, 2006). Mobile IPv4 uses symmetric keys and hashes by default. Since symmetric keys are hard to manage, a certificate-based key exchange was recommended, but this demands more resources. To lower the resource demand, a composite architecture was recommended (Sufatrio, 1999). The procedure uses certificates only in places where the terminal does not require processing of the public key algorithm and does not require storage of the certificate.

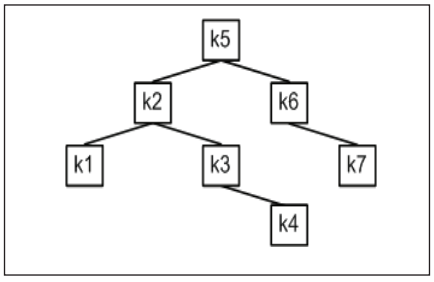
The result of the comparison shows that hash is by far the most efficient method in terms of key generation, but suffers from management difficulties. Lim et al. (2006) also demonstrates that a pure certificate-based authentication is unsuitable for mobile environments. Partial use of certificates and identity-based authentication with extensive use of hash functions can be a potential way ahead.

AUTHENTICATION OF DEVICE GROUPS

In a ubiquitous environment, moving networks appear. PANs and ad hoc connections based on various preferences emerge and fall apart. These devices communicate with each other and have usually very limited capabilities in terms of computing power and energy reserves. In order to provide secure communication between any part of the network, hierarchical key management methods emerged (Kim, Ahn, & Oh, 2006). Here a single trusted server is used to manage the group key. These entities are usually storing the keys in a binary tree, where nodes are the leaves.

Public key operations are usually required when a terminal wants to connect to a group for the first time. A group management system needs frequent key generation rounds, because it has to ensure forward and backward secrecy. Strict key management policies ensure that no new node is capable of decoding former traffic and none of the old nodes have the possibility to decrypt current traffic. To adjust resource usage to mobile environment, a management scheme which uses mainly simple operations like XOR and hash is advisable (Kim et al., 2006). As the key in the root of the

Figure 6. Keys in a binary tree



binary tree is used to authenticate the whole group, keys need to be regenerated when a node leaves the network. This procedure is starting from the parent of the former node and goes up to the root. Then the management unit sends out the new keys in one message. Building a tree from keys ensures fast searches and a simple, clean structure. In addition, all keys in the internal nodes are group keys for the leaves under them. So a subset of devices can be easily addressed.

The root unit has to compute these keys in acceptable time, requiring a more complex architecture. In PANs this is usually not a problem, but when a member of a larger subnet is leaving, calculations could be more demanding. A standard group key handling method is the Tree-based Group Diffie-Hellman (TGDH), where management steps assume that all nodes have the same processing capabilities. To ensure maximal efficiency, the highest performance unit shall be the one in the root of the tree (Hong & Lopez-Benitez, 2006). When node computing capabilities are showing big differences, the overhead caused by tree transformations does not represent a drawback.

Another significant group of devices that need encryption can be found in home networks, where the focus is on management of content and personal data.

SECURE HOME NETWORK AND RIGHTS MANAGEMENT

Deployment of wired or wireless home networks happens in roughly 80% of all households with broadband access (Noll, Ribeiro, & Thorsteinsson, 2005). Network-capable multimedia devices, media players, game consoles, and digital set-top boxes are widespread and part of the digital entertainment era. Content is stored within this network, and provided through the Internet to other users. Since the birth of peer-to-peer (P2P) networks, such technologies are in the crosshair of content providers. Recently, some software developers and a few musicians started using the torrent network for cost effective delivery of their content. A digital rights management method designed for such network is still missing.

Current right protection solutions are not compatible with each other and the user friendliness is also varying. The basic problem is, that just a very few devices are equipped with tamper resistant storage and integrated cryptographic capabilities. Beside software solutions, which are meant as weak solutions, hardware-based encryption can severely limit the lawful use of digital content. Recent lawsuits related to Sony's rootkit protection mechanism also reveals that customer rights of usage is considered to be more important than the legitimate wish of content providers to protect the content.

Trusted platform modules (TPM) are the most likely candidate for content protection in hardware-based solutions. While providing encryption capabilities, it is very likely that these components will be used to dispose the users' right to decide over the user's own resources.

The current discussions on DRM for audio content are regarded as minor when compared to high definition (HD) content protection. Even the connection to the screen has to use strong encryption, which has to exceed GSM/UMTS encryption in order to be acceptable for content providers. Enforcing a digital, end-to-end encrypted stream means that a HD-TV purchased at the end of 2006 may not work with the new encryption standards for HD. There is no current solution for computers to legally play full resolution HD. By the end of 2006 it was announced, that a workaround is arising to deal with the advanced content protection system of HD.

A more discrete, but not intrusive business model discussion for digital content management

is presented in order to visualise the requirements of this market. Apple's FairPlay enables making backup copies of audio tracks, which is permitted by law in several European countries, and copy of content between the user's iPod players. This solution is considered being to open for some content providers, and the distribution is limited to a server-client infrastructure. For HD content with high bandwidth needs such a server-client infrastructure is not advisable, both from a server and network point of view. The ever growing size of P2P networks form a perfect infrastructure to deliver content with high bandwidth need practically without substantial transmission costs. P2P networks are usually run without any DRM support. An additional infrastructure supporting DRM in a P2P network used to transmit content will enable high volume distribution of digital content (Pfeifer, Savage, Brazil, & Downes, 2006). If seamless license delivery and user privacy could be guaranteed, such a network could be the foundation of a low cost content delivery scheme.

While the usage of P2P networks is an excellent idea, the recommended solution proposed by Nützel and Beyer (2006) is similar to the Sony's rootkit solution: It bypasses the user control and is thus not acceptable. While the primary goal is to secure content, the software used in such solutions acts like hidden Trojans and opens backdoors not only for the content providers, but also other hackers.

Content usage across platforms is not supported yet, as a common standard does not exist. Pfeifer et al. (2006) suggests a common management platform for DRM keys with an XML-based, standard MPEG-REL framework. Users will also produce content with digital protection, in order to ensure that personal pictures cannot be distributed electronically. Social networks and groups of interest, as well as distribution of content in PANs is a challenge for DRM development. Zou, Thukral, and Ramamurthy (2006) and Popescu, Crispo, Tanenbaum, and Kamperman (2004) propose a key delivery architecture for device groups, which could be extended by a local license manager. The central key management unit could distribute licenses seamlessly to the device, which wants to get access, without invading user experience.

Kálmán and Noll (2006) recommend a phone-based solution. This represents a good trade-off between user experience and content protection. The phone is practically always online, most of them have Bluetooth or other short range radio transmitters, so licenses can be transmitted on demand. Since the phone has a screen and a keyboard, it is possible to request authorisation from the user before every significant message exchange, so the user can control the way licenses are distributes.

If we look aside the issues related to business aspects, computational issues still remain. Highly secure DRM entities will use asymmetric encryption and certificates. Sur and Rhee (2006) recommend a device authentication architecture, which eliminates traditional public key operations except the ones on the coordinator device. This is achieved by using hash chains including the permission, for example, a device can get keys to play a designated audio track ten times or permission to use five daily permits on demand. Such schemes allow end devices to be simpler and lower network communication overhead.

If a central device is not appreciated, a composite key management scheme may be used. The parties in the PAN will form a web of trust like in a confidentiality scheme, for example, pretty good privacy (PGP). In this web, the main key is split between nodes and cooperation is needed for significant operations. This means that if the scheme is operating on a (k, n) basis, k-1 nodes can be lost before the system needs to be generate a new key. Fu, He, and Li (2006) mention the problem of the PAN's ad hoc nature as the biggest problem. Since this scheme selects n nodes randomly, the ones that are moving between networks fast can cause instability in the system. Also, the resource need of this proposal is quite high on all nodes present.

When a scheme is enabling off-line use of license keys, attention should be given to problems arising from leaving or compromised nodes. Identity-based schemes become popular recently because of their efficiency in key distribution. The main drawback is that these proposals do not provide a solution for revocation and key renewal. Hoeper and Gong (2006) propose a solution based on a heuristic (z, m) method. The solution is similar

to the threshold scheme shown before, but enables key revocation. If *z* nodes are accusing one node to be compromised, based on their own opinion, the node is forced to negotiate a new key. If a node reaches a threshold in number of regenerations in a time period, it could be locked out, since most likely an intruder is trying to get into the system or the internal security of the node is not good enough. The assumptions about the system are strongly limiting the effectiveness of the solution. The most stringent assumption is that they require to nodes to be in promiscuous mode. This can lead to serious energy problems. Another requirement is that there has to be a unit for out-of-band key distribution. This unit could be the cellular phone.

SMART CARDS AND CELLULAR OPERATORS

The use of smart cards has its roots in the basic problem of security infrastructures: even the most well designed system is vulnerable to weak passwords. A card, which represents a physical entity, can be much easier protected compared to a theoretical possession of a password. Smart cards integrate tamper resistant storage and cryptographic functions. They are usually initialised with a preshared key and creating a hash chain, where values can be used as authentication tokens.

The remote authentication server is using the same function to calculate the next member. The encryption key is the selection of a collision resistant hash function. While the tokens they provide are quite secure, a problem with smart cards is that they represent a new unit that has to be present in order to enable secure communication, and user terminals must be equipped with suitable readers. The additional hardware does not only cause interoperability problems, but is usually slow, as a measurement conducted shows (Badra & Hajjeh, 2006). This becomes eminent when high traffic is associated with asymmetric encryption; sending a "hello" message with standard TLS to the smart card needed 10 seconds. In contrast, the modified TLS-KEM needed 1.5 s.

A user-friendly, seamless key delivery system can be created with the help of cellular operators and SIM cards with enhanced encryption capabilities. The SIM and USIM modules used in GSM/UMTS are quite capable smart cards. They offer protected storage with the possibility of over the air key management, good user interface, and standard architecture. Danzeisen, Braun, Rodellar, and Winiker (2006) shows the possible use of the mobile operator as trusted third party for exchanging encryption keys out of band for other networks.

Delivery of the mobile phone key to a different device can be problematic, since most devices do not have a SIM reader, or it is inconvenient to move the SIM card from the mobile phone to another device. New developments in near field communication may overcome this and enable short range secure key transfer.

BREAKING THE LAST CENTIMETRE BOUNDARY

Frequency of authentication request is a key factor in user acceptance. If a system asks permanently for new passwords or new values from the smart card hash chain, it will not be accepted by the user. On the other hand, if a device gets stolen and it asks for a password only when it is switched on, then a malicious person can impersonate the user for a long time. A potential solution is to create a wearable token with some kind of wireless transmission technology and define the device behaviour such that if the token is not accessible, it should disable itself in the very moment of notification.

Since the main challenge is not securing data transfer between the terminal and the network, but to authenticate the current user of the terminal, a personal token has to be presented. As proposed by Kálmán and Noll (2007), the mobile phone can be a perfect personal authentication token if it is extended by a wireless protocol for key distribution.

With the capabilities of user interaction, network control of the mobile phone, it can be ensured that critical operations will need user presence by requiring PINs or passwords. Possible candidates for key exchange are Bluetooth

(BT), radio frequency identification (RFID), and Near Field Communications (NFC). NFC is a successor of RFID technology in very short range transmissions. BT is close to the usability limit, since its transmit range reaches several meters. But the two later ones are promising candidates. Depending on the frequency, general RFID has a range of several meters while NFC operates in the 0-10 cm range. NFC is recommended, as the range alone limits the possibilities of eavesdroppers and intruders who want to impersonate the token while it is absent. The use of repeaters in the case of NFC, a so-called wormhole attack as described by Nicholson, Corner, and Noble (2006), looks not feasible because of the tight net of repeaters required. Also, the capability of user interaction provides an additional level of security.

Mobile phones with integrated NFC functionality are already available and serve as user authentication devices. To use these devices as tokens for other terminals, they have to be placed very close to each other. This prevents accidental use in most cases. To check presence of the token, heartbeat messages might be introduced. By design, this solution is very capable of distributing preshared keys for other devices out of band. Meaning, the phone can get the keys from the cellular network from an identity provider and send it down to the appropriate device by asking the user to put the devices close to each other for a second or two.

Transmission of the key must be done only when needed, so the programmable chip on the phones has to be in a secured state by default and only activated by the user's interaction. Protection of RFID tags is shown by Rieback, Gaydadjiev, Crispo, Hofman, and Tanenbaum (2006), where a proprietary hardware solution is presented. In case of a phone-based NFC key transmission, additional active devices might be unnecessary to use, but for general privacy protection, IDs with RFID extensions must be treated with care.

Transmission of certificates would not need additional encryption over the NFC interface, while other keys may require a preshared key between the phone and the terminals, which can be done via a wired method or by the phone provider. Most providers have at least one secret key stored on phones and a public key connected to that one. Based on this, DH key exchange would be possible between terminals and the phone using the cellular network as a gateway. An NFC-enabled phone could be the central element of a home DRM service, as it is online, capable of over the air downloads, and still able to ensure user control.

ON THE DAWN ON PERSONAL CONTENT MANAGEMENT

From the viewpoint of secure data transmission and user authentication, access and distribution of digital content can be ensured. Open issues remain for moving PANs and devices with limited capability. Focus nowadays is on protecting the user's privacy. As usage of digital devices with personal information was limited, user privacy was not of primary concern for a long time. Since PANs and home networks hold a large amount of critical personal data, this has to change (Jeong, Chung, & Choo, 2006; Ren, Lou, Kim, & Deng, 2006).

In a ubiquitous environment users want to access their content wherever they are. This has to be enabled in a secure manner. With upcoming social services, also fine grained access control methods have to be deployed inside the personal infrastructure. The focus of DRM research has to shift towards the end user, who will also require the right to protect himself/herself and his/her content with the same strength as companies do.

Extending the phone's functions may be problematic because of energy consumption and limited computing power. This could be easily solved by the technology itself, since a new generation of mobile terminals is arriving every half year. The capacity and functionalities of the SIM cards will be extended, the newest 3GPP proposals are predicting high capacity and extended cryptographic possibilities.

Regarding legal aspects, extending the SIM possibilities may cause some concern, since the SIM cards are currently owned by the network operators.

CONCLUSION

Transport encryption and authentication of devices has been the subject of research for a long time and resulted in sufficient secure solutions with current technologies. The focus in recent proposals is on the limited possibilities of mobile terminals and adoption of encryption technologies for mobile and wireless links.

Distributing keys between nodes is solved, except for the first step, which usually requires out-of-band transmissions. A solution for this initial key distribution might be the mobile phone with its integrated smart card and already existing communication possibility. As phones come with NFC, they may act as contact-less cards to distribute keys between devices.

While device authentication is handled sufficiently, user identity is hard to prove. A knowledge-based password or PIN request is not a user-friendly solution. Current proposals tend to be insecure when performing the trade-off between user experience and security.

Focus on research should be paid towards personal area and home networks. These networks hold most of the user's personal private data and content, either purchased or created by the user. Currently no standard solution exists for managing content rights or for access control of own content.

REFERENCES

3rd Generation Partnership Projects (3GPP). (2004, July). *Technical standardization groups-system and architecture (TSG-SA) working group 3 (Security) meeting, 3GPP2 security—Report to 3GPP, S3-040588*. Retrieved December 20, 2006, from www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_34_Acapulco/Docs/PDF/S3-040588.pdf

3rd Generation Partnership Projects (3GPP)2. (2007). *TSG-X/TIA TR-45.6, 3GPP2 system to wireless local area network interworking to be published as 3GPP2 X.S0028*. Retrieved December 22, 2006

Badra, M., & Hajjeh, I. (2006). Key-exchange authentication using shared secrets. *IEEE Computer Magazine, 39*(3), 58-66.

Boneh, D., Goh, E.-J., & Boyen, X. (2005). Hierarchical identity based encryption with constant size ciphertext. In *Proceedings of Eurocrypt '05.*

Danzeisen, M., Braun, T., Rodellar, D., & Winiker, S. (2006). Heterogeneous communications enabled by cellular operators. *IEEE Vehicular Technology Magazine, 1*(1), 23-30.

Fathi, H., Shin, S., Kobara, K., Chakraborty, S. S., Imai, H., & Prasad, R. (2006). LR-AKE-based AAA for network mobility (NEMO) over wireless links. *IEEE Selected Areas in Communications, 24*(9), 1725-1737.

Fu, Y., He, J., & Li, G. (2006). A composite key management scheme for mobile ad hoc networks. In *On the move to meaningful Internet systems, OTM 2006 Workshops* (LNCS 4277).

Hoeper, K., & Gong, G. (2006). Key revocation for identity-based schemes in mobile ad hoc networks, ad-hoc, mobile, and wireless networks (LNCS 4104).

Hong, S., & Lopez-Benitez, N. (2006). Enhanced group key generation algorithm. In *Network 10th IEEE/IFIP Operations and Management Symposium, NOMS 2006* (pp 1-4).

Jeong, J., Chung, M. Y., Choo, H. (2006). Secure user authentication mechanism in digital home network environments. In *Embedded and Ubiquitous Computing* (LNCS 4096).

Kálmán, Gy., & Noll, J. (2006). *SIM as a key of user identification: Enabling seamless user identity management in communication networks.* Paper presented at the WWRF meeting #17.

Kálmán, Gy., & Noll, J. (2007). SIM as secure key storage in communication networks. In *The International Conference on Wireless and Mobile Communications ICWMC'07.*

Kim, S., Ahn, T., & Oh, H. (2006). An efficient hierarchical group key management protocol for

a ubiquitous computing environment. In *Computational Science and Its Applications—ICCSA 2006* (LNCS 3983).

Kwak, J., Oh, S., & Won, D. (2006). Efficient key distribution protocol for electronic commerce in mobile communications. In *Applied Parallel Computing* (LNCS 3732).

Lee, J.-H., & Chung, T.-M. (2006). Session key forwarding scheme based on AAA architecture in wireless networks. In *Parallel and Distributed Processing and Applications* (LNCS 4330).

Lim, J.-M., Lim, H.-J., & Chung, T.-M. (2006). Performance evaluation of public key based mechanisms for mobile IPv4 authentication in AAA environments. In *Information Networking. Advances in Data Communications and Wireless Networks* (LNCS 3961).

Nicholson, A. J., Corner, M. D., & Noble, B. D. (2006). Mobile device security using transient authentication. *IEEE Transactions on Mobile Computing, 5*(11), 1489-1502.

Noll, J., Ribeiro, V., & Thorsteinsson, S. E. (2005). Telecom perspective on scenarios and business in home services. In *Proceedings of the Eurescom Summit 2005* (pp 249-257).

Nützel, J., & Beyer, A. (2006). How to increase the security of digital rights management systems without affecting consumer's security, In *Emerging Trends in Information and Communication Security* (LNCS 3995).

Pfeifer, T., Savage, P., Brazil, J., & Downes, B. (2006). VidShare: A management platform for peer-to-peer multimedia asset distribution across heterogeneous access networks with intellectual property management. In *Autonomic Management of Mobile Multimedia Services* (LNCS 4267).

Phillips, T., Karygiannis, T., & Kuhn, R. (2005). Security standards for the RFID market. *IEEE Security & Privacy Magazine, 3*(6), 85-89.

Popescu, B. C., Crispo, B., Tanenbaum, A. S., & Kamperman, F. L. A. J. (2004). A DRM security architecture for home networks. In *Proceedings of the 4th ACM workshop on Digital rights management,* Washington, DC.

Ren, K., Lou, W., Kim, K., & Deng, R. (2006). A novel privacy preserving authentication and access control scheme for pervasive computing environments. *IEEE Transactions on Vehicular Technology, 55*(4), 1373-1384.

Rieback, M. R., Gaydadjiev, G. N., Crispo, B., Hofman, R. F. H., & Tanenbaum, A. S. (2006, December 3-8). *A platform for RFID security and privacy administration*. Paper presented at the 20th USENIX/SAGE Large Installation System Administration Conference—LISA 2006, Washington, DC.

Sufatrio, K. Y. L. (1999, June 23-25). *Registration protocol: A security attack and new secure mini-mal public-key based authentication.* Paper presented at the International Symposium on Parallel Architectures, Algorithms and Networks, ISPAN'99. Fremantle, Australia.

Sur, C., & Rhee, K. H. (2006). An efficient authentication and simplified certificate status management for personal area networks. In *Management of Convergence Networks and Services* (LNCS 4238).

Zou, X., Thukral, A., & Ramamurthy, B. (2006). An authenticated key agreement protocol for mobile ad hoc networks. In *Mobile Ad-hoc and Sensor Networks* (LNCS 4325).

KEY TERMS

Diffie-Hellman Key Exchange: Diffie-Hellman key exchange is a procedure, which allows negotiating a secure session key between parties, who do not have any former information about each other. The negotiation messages are in band, but because of the non-polynomial (NP) problem used in the procedure, adversaries are not able to compromise it.

Mutual Authentication: Mutual authentication occurs when the communicating parties can mutually check each others identity, thus reducing

the possibility of a man-in-the-middle attack or other integrity attacks.

Out of Band Key Delivery: Out of band key delivery occurs when an encryption key is delivered with a mean, which is inaccessible from inside the network it will be used in. An example is to carry a key on an USB stick between parties, where the key will never be transmitted over the network.

Rootkit: Rootkit is a kind of software to hide other programs. Mainly used by Trojans, they enable hidden applications to access local resources without user knowledge.

Seamless Authentication: Seamless authentication is a method where the user is authenticated towards an entity without the burden of credential requests. For high security requirements, transparent methods are not applicable, but can provide additional security in traditional username/password or PIN-based sessions.

Session Key: Session key is a short life, randomly generated encryption key to protect one or a group of messages. The main purpose is to use expensive encryption operations only when starting a session and use a simpler to manage cipher in the later part.