Mobile phones as secure gateways for message-based ubiquitous communication

Walter Bamberger[1], Oliver Welter[1], and Stephan Spitz[2]

[1] Technische Universität München, Germany
[2] Giesecke & Devrient GmbH, Germany

Abstract. For ubiquitous communication self-organising adhoc networks become more and more important. We consider mobile phones as an appropriate trusted gateway for external machines with low communication needs. A message-based approach is best in such a scenario with moving mobile phones and machines. We propose a security model for access control to the communication infrastructure that is also message-based. To meet the requirements of ubiquitous communicating machines, all algorithms on the sender's side are based on symmetric cryptography resulting in low computation needs. A sophisticated symmetric key infrastructure for message authentication provides the necessary key management. The trustworthiness of the mobile phone is achieved by using the SIM as a secure storage and computing module. This makes it possible to use the mobile phone not only as a user terminal but also as a trusted infrastructure component of the mobile network.

Keywords. SIM, mobile network, machine-to-machine communication, symmetric key infrastructure, message-based communication.

1 Introduction

2G/3G mobile networks with packet transport capabilities are widely spread today. They are also used for machine-to-machine communication. This paper introduces a security architecture for a communication technology, in which the external (sending) machine is equipped with a personal area radio (PAN, like ZigBee of Bluetooth) instead of a wide area radio (WAN, like GRPS or UMTS). This keeps the module complexity on the sender's side as well as the resource allocation in the mobile network very low. Interesting applications include all sorts of vending machines, escalators or environmental sensors.

Figure 1 illustrates the communication architecture considered in this paper. An external machine (on the left hand side) wants to send a message to a host in the Internet (e.g. running a web service). For this it looks for a randomly passing mobile phone and uses it as a relay. We call such a mobile phone the *gateway* in the following. In the mobile network there is another intermediate component named *proxy*. It performs accounting and security actions. In this paper we only discuss the unidirectional case from the external machine to the Internet host, although a bidirectional extension can be imagined.

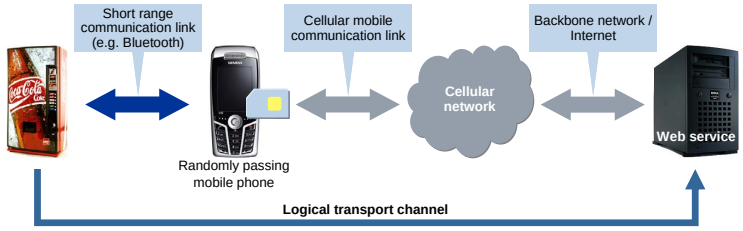

Fig. 1. The considered communication scenario: An external machine should be able to send messages supported by a trusted mobile phone.

This paper deals with the security concerns that come along with this new approach. As the communication is message-oriented with one or more hops, a message-based security concept (Sect. 4.3) must be chosen. We show how this paradigm can be integrated in the existing security architecture of the mobile network. Message authentication is done using *symmetric keys* backed by a lightweight key management system (Sect. 4.2 and 5). A public key infrastructure like X.509 is not feasible as external machines have very low computation capacities and miss some prerequisites like access to a reliable time source. The proposed system respects the necessity of an easy deployment and allows implementing a simple application on present cheap hardware. For example the software could directly be implemented on the integrated micro-controller of the Bluetooth transceiver (like the BlueCore 4 of CSR). Then the hardware costs will be very low compared to other solutions.

The subscriber identity module (SIM) as a key component of the mobile network security serves as a key component in this new concept too. Because the gateway should operate as an external security wall preventing unauthorised traffic in the mobile network, the functionality of the gateway is split into a trusted and an untrusted part (Sect. 4.3). The SIM provides the trusted environment for storing the secret keys and does the security relevant calculations. The untrusted component handles the hardware access and is executed in the main processing unit of the mobile phone.

2 Related work

There are interesting activities in the research community to enhance today's mobile networks with relaying techniques. The goals are mostly coverage extension and capacity improvements at moderate costs. Pabst et al. [1] provide a good starting point. We specialise our concept on machine-to-machine communication only.

For security related concepts a look at adhoc networks is also interesting. There are several proposals [2, 3] to meet the adhoc nature with asymmetric cryptography and secret sharing techniques. Yang et al. [4] introduce a very localised and self-organising approach. However they do not really meet the

characteristics of our communication system. Further more we want to evaluate the chances of symmetric cryptography.

Therefore a closer look at existing symmetric key infrastructures (SKI) can help for inspiration. The classical Needham-Schroeder protocol or Kerberos, but also newer proposals of Crispo et al. [5] target at user / machine authentication though. Some investigations show that this is rather different from a symmetric key infrastructure for message authentication with its keys which are shared by many devices.

Most closely related to our architecture, protocol and applications is the work of the Delay Tolerant Networking Research Group (DTNRG) in the Internet Research Task Force (IRTF). The main protocol is the Bundle Protocol [6], accompanied the Bundle Security Protocol [7]. Both are still drafts. The protocol is much more complex targeting more applications. However the security protocol still has a couple of open issues, especially the key management. With our simpler protocol we can provide a thorough and practical solution.

3 Technical Fundamentals

The mobile phone consists of three logical parts which are involved in the data exchange. The first hardware component is the insecure communication unit of the device responsible for the Bluetooth, NFC or IrDA communication with the external machine. The SIM module acts as a trusted storage and run-time environment for the security critical processes. The third component is the communication interface to the outside world, in our case the GSM network as a connection towards the Internet.

The SIM is the security critical gateway between both sides and is therefore responsible for all security related tasks. Data received from the insecure communication unit are verified, authorised and sent in a secure manner into the mobile network by the SIM. The communication to the SIM can be established via the classical APDU interface according to ISO 7816 or via a TCP/IP protocol stack on top of an USB connection to the SIM.

As we show in Sect. 5.1 the SIM must receive sensible key material from a server in the mobile network. Using the latest generation of Internet-enabled SIMs (like the Giesecke & Devrient GalaxSIM) a direct transport layer security (TLS) tunnel can be established between the server and the SIM. Then the mobile phone simply acts as a router between the SIM and the server. In case of an APDU based communication all data is routed through the insecure mobile phone operating system. Then additional security mechanisms have to be applied on the application level. We detail them in Sect. 5.1

The packet data protocol context (PDP context) [8] is another concept in 2G/3G networks that is important for this paper. A mobile phone, which wants to send packet switched data (e.g. via the general packet radio service (GPRS)), must request a packet data protocol context first. This context can be imagined as a virtual channel. A network protocol (e.g. IP), an interface address (e.g. an IP address) and other information is associated with this virtual channel. This

also includes specific routing and charging rules. In our system the mobile phone requests a certain PDP context to deliver messages to the proxy in the mobile network. Using this PDP context the routing to the proxy is possible and the data transport is not charged to the mobile phone owner's account.

Because the PDP context is requested from an early component in the core network (the serving GPRS support node (SGSN)), refusing the PDP context for a given device is an efficient way to keep unwanted traffic to the proxy (which is free of charge) out of the mobile network.

4 Securing the Transport

The main purpose of this new communication approach is the message transport. Therefore this chapter discusses security aspects of the message transmission process. Starting with the required security services, the necessary symmetric key infrastructure is outlined next. With this background the message transmission process can be explained. The final section details a few important topics further.

4.1 Security Services

Talking about necessary security services corresponds with compiling the security requirements of the system. Therefore we first discuss these security services and show the realisation afterwards. For example Zhou and Haas [2] give the fundamentals.

In this scenario the data should not be transmitted through an end-to-end connection. Instead a message should be forwarded using one or more relays to reach its final destination. Each relay must verify the message *integrity* and whether it is allowed to use the infrastructure (*authentication*). This makes some kind of message authentication necessary.

Because the transmission in the mobile network causes costs, the mobile network operator must ensure the *non-repudiation* of origin. Another key infrastructure is set up for non-repudiation purposes, as the requirements are very different from the ones for message authentication. Note that, using symmetric keys, the mobile network operator can only prove that the message has not been created by a third party as he is able to create verifiable messages himself. A trust relation between the machine operator and the mobile network operator is assumed, so this will not become a problem.

Finally the *anonymity* of the mobile phone outside the mobile network must be ensured. We also increase the *availability* through redundancy: An external machine may re-transmit a packet several times depending on the booked service level. It should give attention to use different gateways for each re-transmission for security reasons.

Our system provides *confidentiality* too, but as an optional feature. There are a few applications that do not need this service but want avoid the extra effort.

4.2 Key Infrastructure

As mentioned in the previous section two sets of symmetric keys are used. With the *access control key set* each relay and the proxy can verify that a message (i.e. the sender) is authorised to use this mobile network for message-based communication. The *non-repudiation key set* is necessary for accounting purposes. With these keys the mobile network operator can determine the creator of the message uniquely. They are also used for packet encryption.

The access control key set consists of 32 keys. Each key is valid for a chosen time period (e.g. 3 years), and is replaced by a successor afterwards. It is identified with an identification number and a version number. Section 5 describes the key management for the access control key set further. The proxy in the mobile network has access to all 32 keys.

The access control key set is divided into two subsets of 16 keys each. A gateway has the keys of one subset, resulting in two types of gateways depending on the actual subset. This ensures that the system still runs, even if all 16 keys of one mobile phone are compromised. The keys are deployed onto the subscriber identity module card (SIM card) and cannot leave it. This guarantees the secrecy of them, as the subscriber identity module is considered to be a rather secure key storage. Section 4.3 details further how this module is used as a security kernel in this architecture.

An external machine has six keys, three out of each subset. During connection establishment with the gateway a subset is negotiated. Actually those six keys are not specific for a machine but for all machines of a machine operator (one company). External machines and their operating companies are considered to be the major risk for the secrecy of the keys.

In contrast the keys of the non-repudiation key set are not shared between the machine operators and the gateways. Each machine operator has its own unique key. The proxy in the mobile network uses these keys to verify the sender for accounting purposes. The keys are versioned as well, but the update process is not automatic. Instead the keys are exchanged during other service tasks onsite (e.g. every 5 years), so a sufficient long overlap between two consecutive key versions is required. Using only one key per machine operator reduces the size of the key database compared to individual SIMs in GSM modules.

4.3 Message Transmission Process

With this key infrastructure we can describe the transmission process of a message in the following.

External machine to gateway: First the external machine needs an *access control message key* derived from a key out of the access control key set and a *non-repudiation message key* derived from the machine's non-repudiation key. These message keys are recomputed for each message and help in combination with a nonce to hinder attacks based on a large collection of data or on messages with the same payload but different keys. Because there is no end-to-end

connection the message key must be generated with a pseudo-random function and parameters only depending on header respectively packet information (see Sect. 4.4). The secret keys the message keys are derived from are called *master keys* in the following. Another parameter is the nonce which is generated by the mobile phone to prevent replay attacks. Therefore the message keys must be computed after the external machine has connected to the gateway.

With the non-repudiation message key the external machine encrypts the payload first. The encryption is indicated through a certain value in the content type header, as it is optional – meeting the needs of a few applications. Then two message authentication codes (MACs) must be computed, the *access control MAC* for the relaying and the *non-repudiation MAC* for accounting (see Fig. 2). To avoid the necessity to perform the hashing over the payload twice, a modification of the HMAC algorithm [9] is introduced in Sect. 4.4. With this the non-repudiation MAC is based on both message keys while the access control MAC is a common HMAC over the whole message, including the non-repudiation MAC. This makes it possible that every gateway can test the integrity of the message and verify that the message is authorised for this service. In addition the proxy can prove that the sender address indicates the right customer.

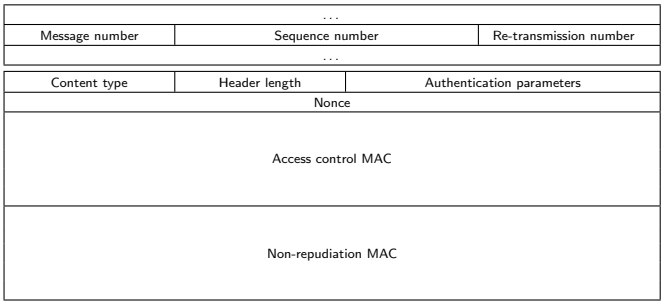

Fig. 2. Header of each packet

All in all when the external machine has found a gateway, it receives the number of the access control key set and a nonce, chooses an appropriate master key out of that key set, optionally encrypts the payload, computes both MACs and finally delivers the message to the mobile phone.

Processing within the gateway: In this concept the new extension to the security of the 3G network is the understanding of a mobile phone as a trusted gateway for message-based access. The trust originates from two measures: First we use the subscriber identity module as a secure key store and trusted processing platform, second each packet can be associated by the mobile network operator with a mobile phone and thus with a real world person.

Figure 3 shows that a server module in the main processing area of the mobile phone accepts the incoming messages from external machines. The symmetric

keys for the access control MAC verification must be stored in a trusted environment. Therefore the server module forwards the message to the SIM card next. The method for the data exchange depends on the actual SIM card type. A small software module in the SIM verifies the access control MAC and sends it back to the main processor if the HMAC is valid. Otherwise it simply drops the message. This ensures that faked messages do not pass the mobile phone. The only chance for an attacker to send messages through the gateway consists in revealing a valid access control key. Compromise of the key will be detected at the proxy, because of a wrong non-repudiation key MAC. The key management system (see Sect. 5) provides methods for key revocation, so once the compromise is noticed, the abuse of the network is intercepted. All sensitive data is handled inside the trusted environment of the SIM and no secrets are visible from the untrusted domain at any time. This concept makes it obsolete to use an expensive trusted platform.

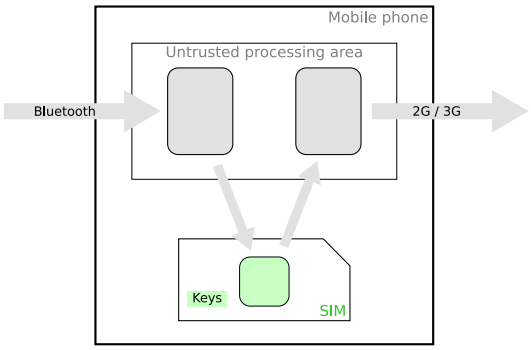

Fig. 3. Software architecture in the gateway

When the message passes the HMAC test in the SIM successfully, it is given back to another software module in the untrusted processing area of the gateway.

Gateway to proxy: To send the packet to the proxy in the mobile network, a software component in the untrusted area of the mobile phone first requests a specific packet data protocol context (PDP context) from the serving GPRS support node (SGSN). With this PDP context the mobile phone can access the proxy. It delivers the packet via an unsecured hypertext transfer protocol (HTTP) connection. Because a packet is usually much smaller than 100 kByte, the use of an authentication protocol like the transport layer protocol (TLS, [10]) would lead to a high overhead. It is more efficient to accept every packet, limit the packet size and verify both MACs. Therefore it is better in this situation to react effectively on attacks, instead of preventing them – although this channel into the mobile network is very vulnerable, because it is not charged to the mobile phone owner's account.

If one of the MACs or the combination of the non-repudiation key and the access control key is not valid (one non-repudiation key and exactly six access control keys are assigned to each machine operator), the proxy can detect an attack. The nonce and the various numbers in the header (see Fig. 2) make it possible to detect replay attacks. In addition optional destination filters at the proxy can protect companies if their non-repudiation key has been compromised. There are several measures available to react on those attacks:

- Traffic from manipulated mobile phones can be suppressed refusing the packet data protocol context for them. The mobile phone cannot send any data without charging anymore.
- Further criminal acts can lead to legal consequences, because the mobile phone owner is known.
- Attacks from devices behind the mobile phone are detected by the gateway. Only newly compromised keys could pass the gateway.
- Key management mechanisms as described in Sect. 5 make it possible to react precociously on compromised keys.

All in all we have seen that the use of the subscriber identity module as a trusted kernel combined with other existing security mechanisms of the mobile network makes it possible to keep unwanted traffic out of the mobile network. This architecture extends the 3G network efficiently for message-based external access.

4.4 Implementation Details

Message key computation: A limited number of 32 keys is used across many devices and many messages respectively packets. This makes it necessary to use a message key (k^m) for the MAC computation instead of one of those 32 master keys (k_i, $i = 1, \ldots, 32$) directly. The algorithm is the same for both, the access control message key and the non-repudiation message key. The only difference is the chosen master key.

The message key must be derived with a pseudo-random function (PRF) from a master key. In addition a nonce is necessary to randomise the message key. It is the nonce generated by the gateway and shown in Fig. 2. The function must be able to provide a bit stream with variable length depending on the actual hash function in the HMAC computation.

The pseudo-random function as defined in the draft of the Transport Layer Security protocol (TLS) v1.2 [10] is chosen here. The only difference is the absence of the label (see appendix A for convenience). The nonce concatenated with the source address, the destination address and the message number builds up the *seed*; the master key is used as the *secret*. A nonce may not be used twice, but it may be counted sequentially; the (pseudo-) randomness is provided by the PRF. All input values of the PRF are part of the header (see Fig. 2). Therefore all hops equipped with the master key can and should verify the access control MAC before forwarding the message.

Message authentication code computation: As Sect. 4.1 explains, two MACs are necessary for two different purposes: one to control the access to the relaying mechanism and another one to prove the origin of the message for accounting purposes. Using the conventional HMAC algorithm, this would result in two hash computations over the complete message. Since this system targets at external machines with low computation power, a modified combined method is proposed in the following. As a result the access control MAC can be verified with the usual HMAC verification algorithm, whereas the non-repudiation MAC needs both keys – the access control message key and the non-repudiation message key.

For the MAC generation an HMAC operation over the message m (without the not yet computed MACs) is performed with the access control message key k_{ac}^m first.

$$h_i = \text{HMAC}(k_{ac}^m, m) \tag{1}$$

The non-repudiation MAC h_{nr} can be derived from this intermediate result with the non-repudiation message key k_{nr}^m:

$$h_{nr} = \text{HMAC}(k_{nr}^m, h_i + nonce)$$

To verify this MAC both keys (k_{ac}^m and k_{nr}^m) must be known. This is true for the external machine and the proxy.

To complete the access control MAC, h_{nr} must be appended to the HMAC operation of (1). The state of that first HMAC computation must be preserved until this last HMAC computation. Then it is possible to verify the MAC with the usual HMAC algorithm over the complete message including the non-repudiation MAC, but in a slightly different order.

Both MACs can be inserted in the message as shown in Fig. 2.

5 Key Management

5.1 Access Control Keys

The system architecture as proposed in Sect. 4 relies on the secrecy of a set of keys for access control that is shared among all participants. In the following the proxy under control of the mobile network provider is considered equal with the central key management server.

Even if the main system uses symmetric cryptography, each subscriber identity module (SIM) contains an asymmetric key pair used for mutual authentication during key roll-out and key revocation.

Key roll-out: The SIM cards are delivered to the customers with an initial version of the secure application, an individual key pair and certificates necessary to authenticate themselves against the central server. On first start-up the subscriber identity module connects to the management system via a secure HTTP

connection with mutual authentication. The asymmetric key pair is used for this. Through this secure tunnel it receives a current version of the software and the current key set.

The initial set of keys in the external machine comes with the hardware roll-out; thus the keys leave the protected environment of the network operator. This deployment is a very critical task but not in the scope of this work. Section 5.2 details further thoughts on this topic.

Key renewal: To allow key versioning each key index is extended by an additional version number. A new version number is the increment-by-one of its direct predecessor value. This enables the devices to decide if a presented key is newer or older than the one it currently uses without having access to the whole key history. In addition each key is associated with an expiration date. This time information is not security critical but is one way to trigger a key renewal procedure in the gateway.

The key renewal is done in two steps: In step I the new keys are made available on the central management node, from where the gateways can fetch them. A mobile phone starts the update procedure, when the expiration date has been exceeded or when a delivered message is rejected by the proxy because of an outdated key.

First the gateway sends a list of the key versions in its local key store to the server via an HTTP connection. The server compares the list with the key version in the repository and returns updates for all keys which posses a version difference of one. In this key renewal response the new key is encrypted with its predecessor, so no further authentication or transport encryption needs to be done (for details about the key renewal response see Sect. 5.3). The device must store the new key and the key renewal response for later use. If the distance between the key versions is larger than one or if the outdated key is comprised, the mobile phone must fetch the latest key and its key renewal response using the schema described for key revocation below.

In step II the new keys are distributed to the external machines. When a machine sends a message to the gateway, the key version of the message is examined and – if the version number in the local store is higher – the communication is instantly rejected. To distinguish such a rejection from other communication problems, a special (OBEX) error code is sent. The machine then requests a key update and receives a key renewal response as described in Sect. 5.3.

Again only a difference of one in the version number can be bridged by this mechanism. A larger gap would need an on-site service (compare Sect. 5.2). In the meanwhile the machine could use one of the remaining five keys. If the key version presented by the machine is newer than the one in the mobile device, the communication request is accepted but the message is kept in a quarantined state. As soon as a connection to the management system is available, a key update is performed and the message is evaluated using the new key.

Because the adhoc connection between the external machine and the gateway is very short-lived, some further considerations are necessary about the software

architecture in the mobile phone. The access to the subscriber identity module is too slow. Section 5.3 details this further.

Key revocation: If one of the keys becomes compromised, any communication that is secured with that key must be rejected by the gateway. To signal the key invalidation to the participants in the network the version number is incremented by two to distinguish normal and revoking updates. The procedure for a revocation and a key renewal in case of a version difference larger than one is the same. The double increment forces the gateways to fetch the key update via an authenticated connection and breaks the update path for external machines.

In case of a revoked key, the subscriber identity module in the gateway establishes a secure HTTP connection with mutual authentication similar to the key roll-out procedure. Through this tunnel the SIM directly receives the new key and a key revocation note (see below). The latter one is forwarded to the untrusted area in the mobile phone to notify external machines about the key revocation.

There are a couple of ways to notify the gateways about compromised keys. The most promising methods are push messages like short message system (SMS) messages and notifications during message delivery. In the latter case the proxy informs the mobile phones about newly compromised keys every time they deliver a message (with this or another key). This can be done during the first three months for example. It seems to be a good heuristic as very active gateways are informed very fast this way without a traffic overhead.

There is no secure way to update compromised keys inside the external machine. The knowledge of the other keys is not sufficient to receive the new version of the key. Even if a key exchange is not possible, it is wise to push a key revocation note to the machine, so it no longer sends messages with an invalid key. This key revocation note is presented to machines using the compromised key, and it is secured by an HMAC with the compromised key. It is safe to use the compromised key to authenticate the key revocation note as an attacker may also send this note with all its keys he has got.

5.2 Non-repudiation Keys

The non-repudiation keys are known only to two parties – the machine operator and the network operator. Therefore a complex key infrastructure as introduced above is not necessary here. Instead these keys are considered to be more long-lived. If we assume that a service technician comes on-site at least once in two years, the key renewal process does not lead to an additional effort.

The key deployment demands a secure process within the company of the machine operator. It depends strongly on the organisational structure there and is therefore out of the scope of this work. Some thoughts on it include, that all keys (the non-repudiation and the access control keys) reside in an encrypted form on a cheap exchangeable flash memory (something like SD cards). All machines have a super key in their fixed flash to access their keys. This way it the keys do not leave a certain area in the company unencryptedly.

5.3 Implementation Details

Key renewal response: For each outdated key the server sends a new key encrypted to the gateway. The encryption is the bit-wise difference between the old and the new key: $u = k_i^n \oplus k_i^{n-1}$. To proof the authenticity of the update message, an HMAC using the old key is appended $r = u + \text{HMAC}(k_i^{n-1}, u)$. If the HMAC is valid, the update message is considered authentic and the gateway can recover the new key k_i^n with another XOR operation.

The above response is saved to be used for the key renewal between the gateway and the external machine as well.

Software architecture in the gateway for the key renewal: The key renewal between a gateway and an external machine imposes some problems based on the nature of adhoc networks. The time slot available for communication between the subscriber identity module and the machine can be very short and dispatching a message from the Bluetooth stack to the trusted execution environment on the SIM card has a high latency. To provide a fast response on key version errors and for key renewal responses, the version list and the encrypted key material is stored (in copy) in the untrusted area of the mobile device. Then the gateway can immediately respond on messages with outdated keys and on key renewal requests. Because no unsecured confidential data is involved in this process, the update process can be executed over any untrusted media to any kind of gateway or external machine.

6 Discussion of selected attacks

This section focuses on the vulnerabilities the above system imposes. Attacks on Bluetooth ([11–13] are good points of entry) or the mobile network are out of the scope because these technologies are present with or without our system and those attacks are mostly implementation dependent.

A major thread on today's communication systems are denial-of-service (DoS) attacks as they tend to be easy to execute. Looking at the external machine such an attack could be executed by simulating a legal gateway and capturing all packets a machine wants to send. Two methods could be combined to prevent this. First, it is part of the communication concept, that an external machine may send a message several times according to a booked service level. For re-transmission different gateways should be used to complicate a successful attack. Second, machine operators who need a very high service level could configure their machines to authenticate the phone (with the access control keys). Because this costs much time, this decision should be well considered.

Next someone could try to attack the MACs of a captured message. To hinder this, message keys have been introduced. But basically it depends on the hash function, whether such an attack is possible. The HMAC specification [9] details the requirements for an appropriate hash function.

The next component is the gateway. All kinds of faked messages (including replayed messages) can be detected by the mobile phone, if it chooses the nonce

appropriately. Only wrong non-repudiation MACs cannot be found. However the attacker must know access control keys in this case.

The application on the subscriber identity module must be written with security in mind, as a successful attack on it might reveal a whole subset of access control keys and possibly one authentication key pair. In general we consider a successful attack on the card hard but possible. However the keys on the SIM are not sufficient to successfully send a message into the Internet. A non-repudiation key is necessary too. Therefore the economic benefit in attacking a SIM is limited.

Finally the MACs, the combination of the keys, the nonce and the various numbers in the header of each message help to detect all kinds of attacks on the proxy in the mobile network. Revoking compromised keys and refusing the PDP context for the affected gateways are effective measures in this situation (compare with the end of Sect. 4.3).

Spreading a shared secret over many entities increases the probability of a compromisation. Alternatives like asymmetric cryptography or a significantly increased number of keys have many other downsides. Therefore we designed a dynamic system (with key renewal and revocation) which keeps nearly unaffected if either a SIM or an external machine is compromised.

7 Conclusion

This article proposed a security concept to extend the present 2G/3G network for message-based communication. It enables three interesting communication features: The asynchronous transfer provides a communication service even in areas without direct network coverage (the handset can carry the message into mobile coverage). The trust relationship between the external machine and the mobile phone is of a kind, that every user can become a potential node in this relay network. And finally the accounting and key infrastructure is company-based, leading to a minimal resource allocation in the mobile network.

To realise this we introduced a symmetric key infrastructure appropriate for message authentication in a relay network. It is supported by asymmetric keys which are only used for the initial enrolment and to renew compromised keys. All algorithms used in the external machines have been chosen to work with very low computation power.

The whole key management system was designed to work as a stand-alone solution, so a third party can provide this service using well defined interfaces to the mobile network operator. Nonetheless a good integration into the mobile network has been achieved, especially by using the SIM card as a secure storage pre-configured by the mobile network operator. The security level is similar to that of existing mobile networks.

If this service should be delivered by the mobile network operator only, the existing key infrastructure of the mobile network can take over some parts of the presented infrastructure. This will be subject of future work.

A Pseudo-random Function for Message Key Generation

This paper uses the pseudo-random function (PRF) of the draft of the transport layer security (TLS) standard v1.2. It only omits the label. Then the function reads as follows:

$$\begin{aligned}\mathrm{PRF}(\mathit{secret}, \mathit{seed}) = &\,\mathrm{HMAC\_hash}(\mathit{secret},\ \mathrm{A}(1) + \mathit{seed}) + \\ &\,\mathrm{HMAC\_hash}(\mathit{secret},\ \mathrm{A}(2) + \mathit{seed}) + \\ &\,\mathrm{HMAC\_hash}(\mathit{secret},\ \mathrm{A}(3) + \mathit{seed}) + \ldots\end{aligned}$$

where hash must be substituted by a specific hash algorithm as defined in the chosen cipher suite (see authentication parameters field) and "+" is the concatenation operator. The function A is defined as

$$\begin{aligned}\mathrm{A}(0) &= \mathit{seed} \\ \mathrm{A}(i) &= \mathrm{HMAC\_hash}(\mathit{secret},\ \mathrm{A}(i-1))\end{aligned}$$

References

1. Pabst, R., Walke, B., Schultz, D., Herhold, P., Yanikomeroglu, H., Mukherjee, S., Viswanathan, H., Lott, M., Zirwas, W., Dohler, M., Aghvami, H., Falconer, D., Fettweis, G.: Relay-based deployment concepts for wireless and mobile broadband radio. Communications Magazine, IEEE **42**(9) (September 2004) 80–89
2. Zhou, L., Haas, Z.: Securing ad hoc networks. Network, IEEE **13**(6) (Nov/Dec 1999) 24–30
3. Kong, J., Zerfos, P., Luo, H., Lu, S., Zhang, L.: Providing robust and ubiquitous security support for mobile ad-hoc networks. In: Ninth International Conference on Network Protocols, IEEE Computer Society (November 2001) 251–260
4. Yang, H., Meng, X., Lu, S.: Self-organized network-layer security in mobile ad hoc networks. In: WiSE '02: Proceedings of the 3rd ACM workshop on Wireless security, New York, NY, USA, ACM Press (2002) 11–20
5. Crispo, B., Popescu, B., Tanenbaum, A.: Symmetric key authentication services revisited. In: Information Security and Privacy. Volume 3108/2004 of Lecture Notes in Computer Science., Springer Berlin / Heidelberg (2004) 248–261
6. Scott, K., Burleigh, S.: Bundle Protocol Specification (Internet draft). IRTF. (December 2006)
7. Symington, S., Farrell, S., Weiss, H.: Bundle Security Protocol Specification (Internet draft). IRTF. (October 2006)
8. 3rd Generation Partnership Project: 3GPP TS 23.060 V7.3.0: General Packet Radio Service (GPRS); Service description; Stage 2. (December 2006)
9. Krawczyk, H., Bellare, M., Canetti, R.: HMAC: Keyed-Hashing for Message Authentication. RFC 2104. Internet Engineering Task Force. (February 1997)
10. Dierks, T., Rescorla, E.: The TLS protocol. Version 1.2. Internet Engineering Task Force. (October 2006) draft.
11. Bluetooth SIG: Security. Web page (2007) http://www.bluetooth.com/Bluetooth/Learn/Security
12. Bialoglowy, M.: Bluetooth security review, part 1. Web page (April 2005) http://www.securityfocus.com/infocus/1830
13. Bialoglowy, M.: Bluetooth security review, part 2. Web page (May 2005) http://www.securityfocus.com/infocus/1836