Security in SPECIAL: the Quality of Security Service

Firoz Kaderali, Werner Poguntke, Andreas Rieke, Markus Schneider
FTK - Forschungsinstitut für Telekommunikation
Martin-Schmeisser-Weg 4
44227 Dortmund

Abstract

The paper first gives a short description of the ACTS project SPECIAL which is part of a larger overall project called InfoCity NRW covering the provision of interactive multimedia services in a specific region. After that, an overview of relevant security related principles and mechanisms is given. Finally, the concept of Quality of Security Service (QoSS) is introduced in this context, and some ideas of service related QoSS as well as network related QoSS are presented.

1. The SPECIAL project

SPECIAL is an ACTS project which started in January 1996. The acronym stands for „**S**ervice **P**rovisioning **E**nvironment for **C**onsumers **I**nteractive **A**pp**L**ications“. The goal of the project is to develop and validate an information model for customer care within a service provisioning environment for consumer-oriented interactive applications. It is part of a larger overall project called **InfoCity NRW** (North-Rhine Westfalia) covering the provision of consumer-oriented and professional applications in a specific region. InfoCity will be realised by Vebacom which is also the responsible partner of the SPECIAL consortium. The role of SPECIAL is to cover those aspects of the overall project which deal with customer care in the context of consumer-oriented service provisioning. InfoCity NRW will actively sponsor SPECIAL by contributing the demonstrator in which the concepts developed by SPECIAL will be validated. It is one of SPECIAL's tasks to evaluate the concepts in light of the practical experiences and adapt them accordingly.

The objectives of SPECIAL are:

- to specify an accounting concept which results from tariffing and billing
- to develop and validate a customer care concept
- to utilise the concept by assessing its impact on network planning
- to elaborate a conditional access concept
- to conceptualise a reverse channel approach
- and to validate all concepts within the InfoCity NRW trial.

The following Figure presents a high level view of the consumer part of the InfoCity project in the context of which the information model for customer care will be specified.

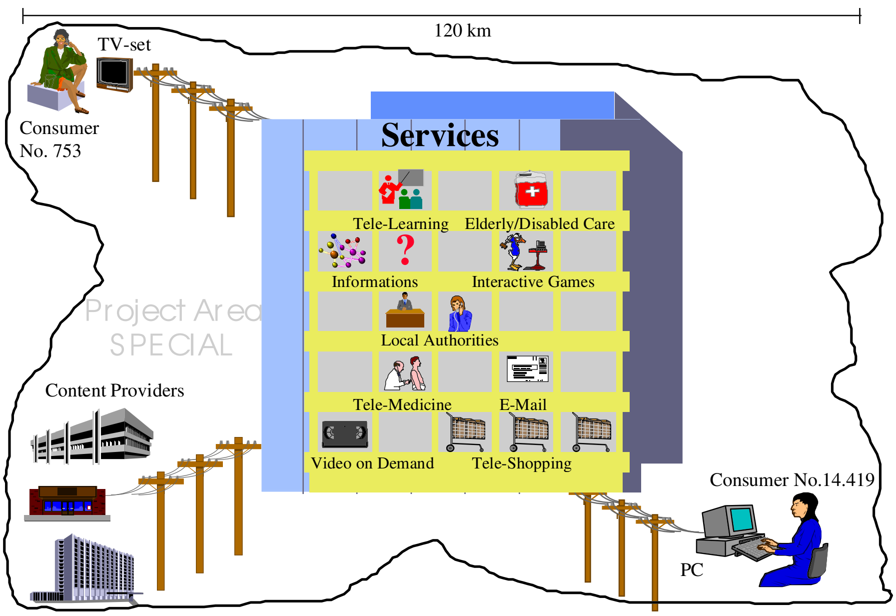

Fig. 1: The consumer service environment of the InfoCity project

The main effort of the project is dedicated to elaborating an information model for customer care as part of the service provisioning environment of a separate service demonstrator. This aspect covers both sides of the service provisioning environment’s interface, i.e. to end-users as customers and to service providers. The number of pilot test end-users will be continuously upgraded to 15 000 at the end of the InfoCity project. The end-users will get home-based as well as public access to services such as:

- Video on Demand (VoD)
- Near Video on Demand (NVoD)
- Teleshopping
- Helpdesk
- Banking applications
- Interactive games
- City information services
- Additional new narrowband/broadband services (Retrieval services, Interactive Services)
- Messaging service (point-to-point connections).

Currently there is a lack of charging and accounting systems for ATM networks. This topic forms a central part of the SPECIAL project which is a platform to discover and evaluate the related conceptual and technical problems and to provide input to European standardisation activities.

Within the consortium, **FTK**-Forschungsinstitut für Telekommunikation is responsible for the work package „Safety, security, privacy and legal issues". Security and related aspects are of central importance to most aspects of SPECIAL. In particular, these topics are closely related to the accounting and conditional access concepts.
The general objectives of the security work package are:

- To develop an overall security model for SPECIAL
- To develop an efficient and reliable model for European access management including conditional access
- To define protocols and role-dependent requirements for access management, conditional access
- To investigate legal issues in an European context.

2. Security related principles and mechanisms

With the introduction of electronic information processing and transmission systems, there is a growing requirement in information security. In former times, information security was guaranteed by physical or administrative means. Within an organisation, important information printed on paper had to be protected in a safe and the authenticity of a received document was proved by a hand signature. In a modern computer based processing or interchange of information these old security related principles are no longer suitable. There is a growing need to provide modern security mechanisms to offer information security. In this context one also has to look at network security because it will be the resource for the transmission of data and the access of systems.
The necessary security mechanisms to be provided have to prevent or detect passive and active attacks of an opponent. Passive attacks give information of the message contents or enable traffic analysis. Active attacks involve the modification, masquerading, replaying of a data stream and the denial of service. Considering the flow of information in a network from a source to a destination, we can conceive several possible attacks:

- interception: gives access to sensitive information, passive attack on confidentiality

- modification: changes the content of a message coming from the source, active attack on integrity
- fabrication: creates a message and masquerades as another user, active attack on authenticity
- interruption: disables a communication, active attack on availability.

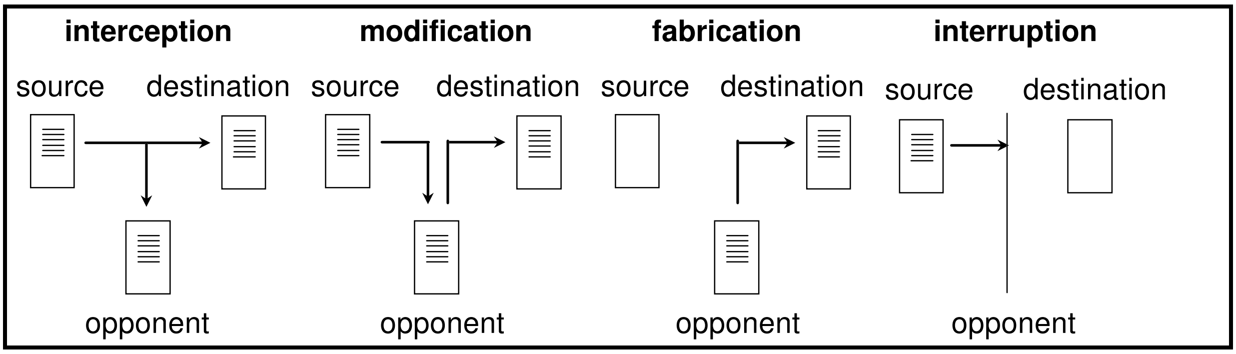

Fig. 2: interception, modification, fabrication and interruption

The attacks mentioned require a differentiation of the security related principles that have to be considered for the implementation of security functions in the network or services. We have to consider these security related principles in networks or information services as the electronic counterpart of the functions that are normally associated with real physical documents. These documents have normally the date and a signature to prove the authenticity of the source; furthermore they are protected against disclosure, tampering or destruction. All these functions have now to be performed on documents/messages/data/information that exist in electronic form. The variety of possible attacks to a system leads to the following subdivision of the security principles:

Confidentiality

Confidentiality requires the protection of data from disclosure to keep the associated content secret. To manage this, the involved parties can use an enciphering system. Such an enciphering system consists of two elements: an algorithm and a key or two keys. We distinguish symmetric and asymmetric enciphering methods. Symmetric methods require one secret key between two partners or within a group. Asymmetric methods provide two keys for each party, a public one and a secret one.
Another differentiation for the classification of enciphering systems is given by blockciphering and streamciphering. Blockcipher systems map plaintext codewords to ciphertext codewords of the same length depending on a key. Streamcipher systems encipher the plaintext bit by bit with the help of a binary pseudorandom sequence. Streamcipher systems are advantageous for the enciphering of bitstreams with high transmission rates because the actual enciphering process consists of simple modulo-2-additions.

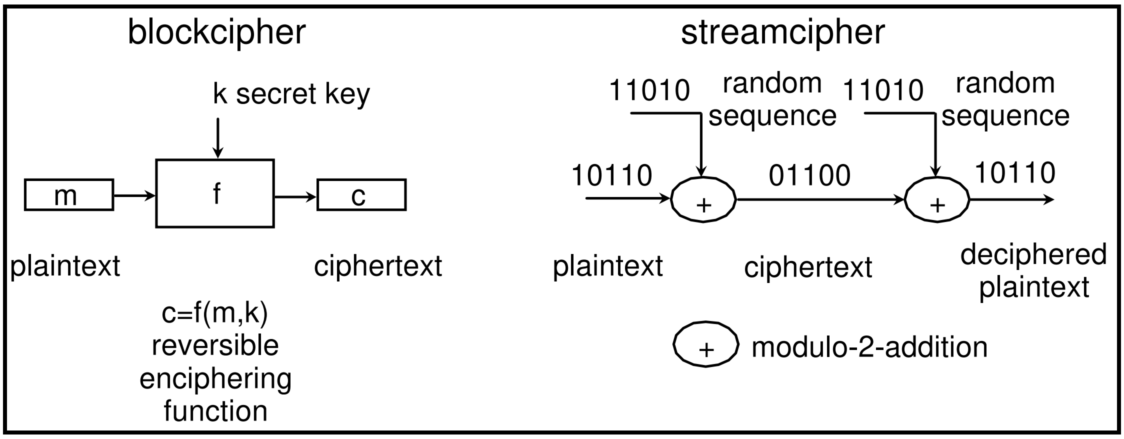

Fig. 3: blockcipher and streamcipher

Authentication

Authentication concerns the aspect that communication is authentic. It assures the recipient that the message comes from the source that it claims to come from. Therefore, every user has a tool to let all the other parties taking part in the communication process to verify his identity uniquely. To do this, he appends a signature to the message. This signature depends on the message and the party to be authenticated. The verifier can verify the authentication code but is not able to produce this code by himself. To create this code, one has to know a special secret - a key - which is only known to one person and - probably - a trusted party. A possible signature scheme is the asymmetric RSA algorithm. Using an asymmetric method, the parties need not negotiate for a common secret. Also, symmetric methods are possible for the creation of signatures. In this case, all the parties involved in the communication process have to choose a common secret key prior to the communication, which is disadvantageous. This solution requires a secret channel.

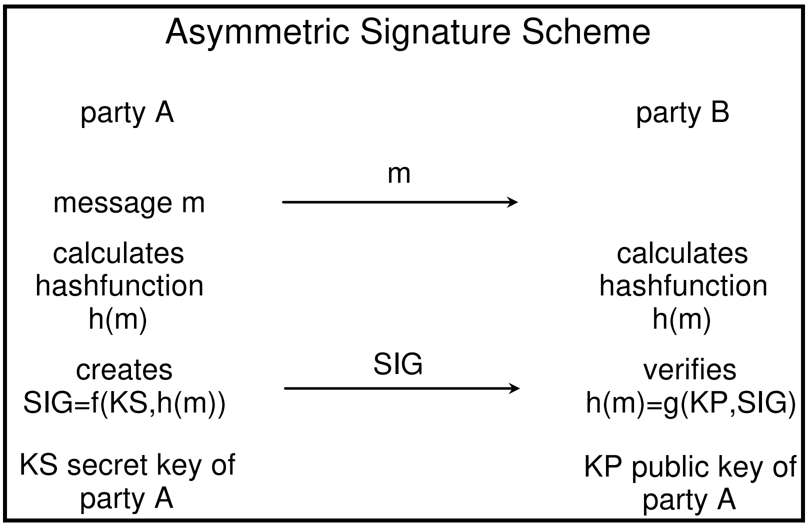

Fig. 4: Asymmetric Signature Scheme

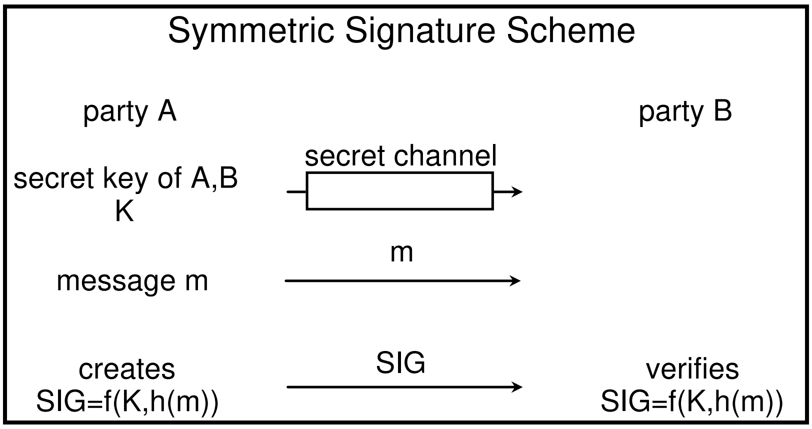

Fig. 5: Symmetric Signature Scheme

Integrity

Integrity deals with the detection or the avoidance of the modification of the contents of a message. This security principle needs a mechanism which assures the receiver that the message has not been changed. The problem can be solved by the introduction of cryptographic checksums or message authentication codes (MACs), which are appended to the message. This is similar to the creation of digital signatures to solve the authentication problem. In fact, the same cryptographical functions and methods can be used.

Access Control

Access control is the mechanism to limit the access via communication links to systems or resources only to authorised parties. A very well known method to provide access control is the password mechanism. In modern networks with high level security requirements the password mechanism should not be applied. Normally this password is transmitted in the communication network over insecure channels to an instance that grants access to the party to be identified. Considering the possibility of a wiretapping opponent, this simple exchange of highly sensitive information like passwords is too dangerous.
For access control, other methods have been developed which are more suitable to be used in communication networks. One possible alternative is the employment of challenge-and-response-procedures. They have the property that the secret which is necessary for the identification has never to be exchanged over the communication network. Both parties, the prover and the verifier know the same secret. The verifier sends a random number chosen by himself to the prover. He calculates a response using the secret and the random number and sends it back to the verifier. The verifier compares the response with the result calculated by himself. If the response and the own result correspond, the verifier grants access to the prover.

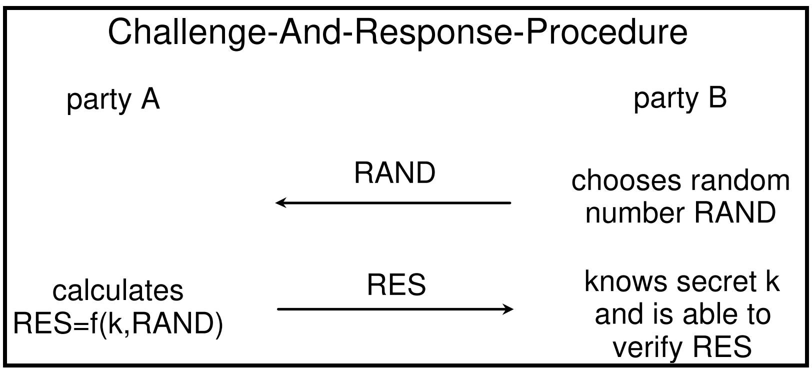

Fig. 6: Challenge-And-Response-Procedure

Another alternative to implement a mechanism for access control is the use of Zero-knowledge-protocols. In difference to the Challenge-And-Response-Procedure presented above, the parties have no common secret. One well known protocol was developed by Fiat and Shamir in 1986 [FiSha 87].

Nonrepudiation

Nonrepudiation prevents either sender or receiver from denying having sent or received a transmitted message. This mechanism is necessary if commercial applications like transactions are offered within the communication network. This mechanism is necessary for the acceptance of the service. A nonfraudulent party will only subscribe to such a service if there is a high level security standard integrated concerning the nonrepudiation facility.

Availability

Some attacks can result in loss or reduction of availability. These attacks against availability are directed towards physical components within the communication network. To reduce the possibility of destroying or manipulation, all sensitive components of the network infrastructure should be installed at secure places.

In the principles described above, we can use methods in which the communicating parties can select their secrets - or keys - on their own. These secrets change from one communication process to the next. Other methods work with personal secrets that stay valid for a longer period. Probably, there is an instance, trusted by all parties, that generates these secrets and delivers them to the communicating parties. Such an instance is called *trust centre* and can be impersonated by a network carrier, a service provider or another neutral trustworthy party. The property of neutrality depends on the parties with their specific interests that are involved in the communication process. For example, a service provider is not considered a neutral party as far as the billing of subscribers is concerned. So, the trust centres have to be chosen carefully.

Another important aspect concerning the provision of security functions is their placement. If encryption is used to counter attacks on confidentiality, one has to decide where the encryption function is to be placed. There are two major solutions to encryption placement: link and end-to-end. The decision where the encryption function should be located poses restrictions on what information has to be encrypted. With link encryption, each vulnerable communication link is equipped on both sides with an encryption device. Thus, all information over the link is protected. Every time a message packet enters a switching centre it has to be decrypted, because the switch has to extract the signalling information (destination address, service related parameters), and must be encrypted when it leaves the switch. Inside the switch, the message is vulnerable. The user has no control over the security of the nodes.

With end-to-end encryption, the encryption process is carried out at the two end systems. The information is encrypted at the source and transmitted unaltered by the network. In this solution, the information is secure in the network links and switches. But there is also a weakness combined with end-to-end encryption: since the nodes have to read the signalling information, it can not be end-to-end encrypted. The end-to-end solution allows only the encryption of user data. To achieve the highest level of security, both link and end-to-end encryption are needed.

An interesting and perhaps a necessary application in a network which provides services as commercial transactions is an electronical payment system. In a prepaid payment system the user must buy so-called electronic money and load it into his electronic wallet before he can make payments. One can distinguish online and offline payment systems. Offline means that no contact to a central database is needed during the payment process for an additional verification of the data. The alternative, online payments, is far too costly for low-value payments. Withdrawal of electronic money is of course an online action. The electronic payment system has some advantages compared to the conventional physical money. In case of loss, possible by breakdown of the system, the user can be given the money back. The user can store different currencies in his electronic wallet or he can exchange it during a payment.
A digital payment system must have a very high security standard. It can be designed as a system with one-sided security in which all participants have to rely on the trustworthiness of a single party, usually the electronic money issuer. Considering the effects of a fraudulent employee of the money issuer it is preferable to rely on a multi-party security in an electronical payment system. In these systems all security requirements of a party are guaranteed without forcing this party to trust other parties.
Compared to the credit card payment system, an electronic money payment system can be developed in such a way that the payment service provider gets no information about the buy-profile of the user. Original money is untraceable. The coins do not identify the user. This property can also be realised in an electronical payment system.

The various possibilities and specifications in the design of the security functions are leading to different security standards. These have to be identified and considered side by side. The different security levels can be offered as a choice in the QoSS combined with a major service. Of course, with regard to some very sensitive applications, the possibility of choice by the user should be restricted.

3. Quality of Security Service

In modern communication systems like ATM, the Quality of Service (QoS) is defined for each virtual connection. During connection set-up, all partners agree on parameters like bandwidth, delay and delay variation. The connection is released immediately if one of the partners does not agree to the parameters.
The same concept can be used for the QoSS: In order to set-up a connection, each partner has to specify security parameters. If the partners agree on common security parameters, the connection will be established; otherwise, it will be rejected.
In contrast to the normal QoS, there is one major drawback in the QoSS: security is not exactly measurable. For this reason, parameter agreement can be performed in three steps: The first step defines the security functions which will be applied (encryption, authentication, ...). In the second step, security algorithms are defined (DES, RSA, ...), whereas, in the third step, a key length is specified.
The concept allows a flexible, simple, robust and individual negotiation on security parameters. In the following, the concept is applied to services and networks.

Service related Quality of Security Service

In the InfoCity project, services like home banking and teleshopping will be available. Several security functions will be necessary and mainly depend on the service which is used and on the specific interests of the communication partners.

Thus, at connection set-up time, all partners (e. g. service provider and user) agree on security functions, security algorithms, and minimum key sizes.
In case of homebanking, the bank will specify user authentication and digital signatures for transfer of money, whereas the user may specify encryption of data. If both are able to agree on the security functions, they have to agree on security algorithms next. If both are able to agree on algorithms for each function and on minimum key sizes for each algorithm, the connection will be established.
The choice of security algorithms also prevents bad surprises: for example, there is only one encryption function (one time pad) that is proven to be absolutely secure [Sha 49], but this is very impractical to use. All the other encryption functions are normally very hard to break, but their security is not proven. Therefore, it is possible that a security algorithm may be broken in the near future; but it is not probable that all security algorithms will be broken within a short time, as far as they are not based on the same problem.
A predefined parameter setting must be defined for end users who have no special knowledge about security functions. It will be sufficient to define three levels of security: low, medium and high.
The QoSS need not be constant for the whole connection time, it can be changed: in the example above, the user may have forgotten to ask for a proof that he has transferred a certain amount of money. In this case, he can try to change the QoSS and ask for non-repudiation of the message, too.

The most important security functions are
- encryption
- user authentication and
- message authentication (digital signature).

The above list of security functions is not complete; further functions (anonymity, electronic voting) can be added. The necessity of additional security functions is a question not only of technical, but also of political, legal and financial interest.
Some of these security functions require the existence of (a) trust centre(s). The trust centre(s) are responsible for the storage and certification of public keys. Thus, the knowledge of the public key of a trust centre is sufficient for a user to receive a partners' public key in authentic form. In case of lost or stolen password, PIN (Personal identification number) and/or chipcard, the trust centre(s) are also responsible for a certificate revocation list, so nobody can make use of a stolen or found chipcard.
Another important application is electronic money. Electronic money enables the direct and anonymous payment of network services; but to realise this, a number of security functions are needed.

Network related Quality of Security Service

The network related QoSS refers to the access to the network and the protection of the network itself. In contrast to the service related QoSS, it is a static quantity.
The access to the network needs to be limited to authorised users. It has to be sure that access is given only to those users who will receive the bill later. Strong user authentication can be applied to perform billing on a high level of security.
The second aspect deals with the protection of the network itself; in this case, not only the security of the user data, but also signalling-, management-, administration- and system data is in question. In many cases, the concept of service related QoSS can be applied in connection with management-, administration- and system data.

There are a number of functions to protect: important ones are encryption of insecure links (GSM), strong user authentication in management-, administration- and system areas.

References:

[BeSchWo 95] Beutelspacher, Schwenk, Wolfenstetter: *'Moderne Verfahren der Kryptographie'*, Vieweg, 1995

[BoBoCra 94] Boly, Bosselaers, Cramer, Michelsen, Mjolsnes, Muller, Pedersen, Pfitzmann, de Rooij, Schoenmakers, Schunter, Vallée, Waidner: *'The ESPRIT Project CAFE - High Security Digital Payment Systems',* ESORICS 94 (Third European Symposium on Research in Computer Security), LNCS 875, Springer-Verlag, 1994

[FiSha 87] Fiat, A.; Shamir, A.: *'How To Prove Yourself: Practical Solutions to Identification and Signature Problems'*, Advances in Cryptology- Crypto 86, Springer LNCS 263 (1987), pp. 186-194

[Schn 94] Schneier, B.: *'Applied Cryptography'*, Wiley New York 1994

[Sha49] Shannon, C. E.: '*Communication theory of secrecy systems',* Bell Systems Technical Journal, vol. 28, pp. 656-715 (1949).

[Stall 95] Stallings, W.: *'Network and Internetwork Security: Principles and Practice',* Prentice Hall, 1995