TECHNICAL SECURITY: THE STARTING POINT

Jan Van Auseloos

S.W.I.F.T., Avenue E. Solvay 81
B–1310 La Hulpe, Belgium

Abstract. Cryptographic security measures for encryption, authentication, non repudiation are important ... but not sufficient. My intention is to make the reader aware of non-technical security issues.

I. S.W.I.F.T.

I.1 What is S.W.I.F.T. ?

The Society for Worldwide Interbank Financial Telecommunication (S.W.I.F.T.) is a non-profit co-operative society of some 1600 member banks in more than 60 countries, dedicated to provide EFT (transmission, storage, arbitration) in a standardized manner. Between the 3000 connection points, we handle 1.000.000 messages every day: customer transfers, bank transfers, foreign exchange confirmations, credit/debit confirmations, ...

Banks are connected locally to a regional processor, which acts as concentrating point in a country. Every RGP is connected to one of the two Operation centers. An OPC validates, acknowledges, stores and controls the delivery of every input message. SWIFT II, the new generation of systems will provide for more flexibility, functionality and capacity. The EFT (SWIFT I today) will be one of the applications of SWIFT II.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 243-248, 1990.

I.2 What is security in S.W.I.F.T. ?

Security is a service (like any other service) which relates to the following objectives:

- Integrity of the network and messages: detect and prevent unauthorized manipulation of system and messages.
- Confidentiality of the network data and messages: restrict all unauthorized access to sensitive operational data and messages (while stored, processed and transmitted).
- Availability of the network and messages: no authorized user will be denied the normal service.
- Accountability: when integrity, confidentiality and availability are compromised the ability to measure the damage and to reconcile.

Since the world (science and reality) is changing all the time, the word security should be seen as an objective, rather than a state.

II. Practical Security in a service company

II.1 Practical Security (top down)

When a user accepts the services presented by a service company, like S.W.I.F.T., a contract appears between the service provider and the service user. This agreement is written down because moral, religion, common sense, loyalty, fair play, ... will change from individual to individual, from company to company.

After signing this contractual agreement, both parties know what they can expect and what they have to provide. It binds every user with S.W.I.F.T. and with all the other users, since a network service depends heavily on the cooperation of all users. As a consequence, R&L (Responsibility & Liability) boundaries are defined and an arbitrator is assigned. Three types of parties are now defined by the R&L boundaries: the service users, the service provider and the arbitrator. Each of them will try to work according to the R&L rules set forward in

the contract and will have to spend money on preventive measures or insurance coverage to guarantee its obligations. E.g. to guarantee the above security definitions, S.W.I.F.T. has to implement preventive and corrective controls, they can be technical, procedural, organizational of contractual. Examples of controls are: encryption, authentication, access control, segregation of duties, dual authorization, audit trails, insurance coverage, separate security administration department, ...

When new services are added or when a service changes, the contract has to be changed, the R&L boundaries shift and the costs to guarantee security are re-distributed.

In S.W.I.F.T. this contract is called the User Handbook. In the policy volume you can find:

- description of the services provided,
- where each one's responsibility starts and stops,
- what each one's reaction should be in case of problems,
- what security measures are to be performed by each party,
- ...

The Chief Inspector acts as an arbitrator and handles all claims between users and between users and S.W.I.F.T.

II.2 Practical Security (bottom up)

Risks and threats are a fact of life. In every operational environment, they are predictable or unpredictable. When we have defined the risks and threats, applicable to our operational environment, we can start organizing it to be able to prevent or recover from them. In the bottom up approach we have to select a security related threat, analyse it and find solutions. Let's take the example of message tampering/viewing on the local S.W.I.F.T. connection: every EFT network carries information generated by the senders and should deliver this information to the receiver. The users give their messages to a 'non owned' environment (network of another bank, PTT lines or radiowave or even satellite). This EFT information is ideal for passive/active attacks:

Passive attack: traffic analysis. This involves recording traffic without interfering. From this data, specific figures or names are noted or statistical analysis is done. This is than interpreted. (e.g. traffic analysis, text analysis)

Active attack: traffic manipulation. Now somebody or something intervenes actively in the flow of messages with the intention to:

a. disrupt normal operations or to harm sender, receiver or network.

b. benefit personally (money, knowledge, prestige, ...).

The techniques used are redirect, reorder, delay, insert, remove, change, obstruct, replace parts of traffic. Countermeasures are sequence checking, session reports, standards, authentication, access control, encryption, ...

The quality of the countermeasures against these known risks/threats is sometimes called 'level of security'. Secure means high quality measures and complete coverage of all known risks/threats, today; insecure means: no implemented measures or very poor quality of them.

Even when we imagine that our environment is static and that we documented all threats/risks, technical security methods cannot make complete secure systems for two reasons:

- countermeasures or combinations of them are never 100% effective: they sometimes introduce new risks/threats or endanger other measures (e.g. standardization to avoid disputes can be exploited by a cryptanalyst, reliance on key management, ...).
- for some known risks or threats countermeasures still have to be invented (e.g. virus, terminal identification, ...). Therefore, to achieve a certain level of security, a combination of 3 basic types has to be implemented: prevention, detection with correction and contracts with claims and arbitration.

Prevent: this type of measures is always resident in the system, they are automatically invoked, because they are part of the normal processing and they stop incorrect actions at the moment they occur.

Detect and correct: when prevention is not practical or can/did not work, detective measures detect an occurred risk/threat and try to reconstruct a correct situation (backups, insurance, ...).

Contract, claim and arbitration: when preventive and detective measures are not feasible or to costly, every party will try to shift responsibility to the other party. R&L boundaries will be created. Sometimes one of the parties claims being damaged by another party and asks arbitration.

III. Security administration, audit and development in a service company

Both approaches (bottom up and top down) lead to the same conclusion. They both lead to formulating R&L boundaries and therefore an independent arbitrator. This arbitrator can neither be part of the service company, nor can he be a user. When investigating claims he/she may not be biased when interpreting the contract.

Because of his independent and privileged position, he can do more:

III.1 Security administration

This is best explained with an example. Since he is not a user and since he is not part of the service company structure, he is in an ideal position to generate access codes which only the user will know and a security module in the network. This job cannot be given to a user, knowing the other one's passwords he could be tempted to make fraudulent use of it. Also this job cannot be given to the service company, since then we can expect internal fraud. He is the ideal trusted party in every key-scheme.

III.2 Security development

New services are created within the existing framework, new security inventions are made or new threats/risks pop up. This all requires development work, which should be monitored or initiated by this department.

I would like to make following comment here. Again the discussion has started to use either standardized or non standardized (own) security algorithms. On a standard algorithm, multiple, independent audits have been done, but people will keep on trying to break it. If suddenly broken, this will get worldwide press coverage, forcing the user to change overnight. Even worse, sometimes people claim to have broken it, the press blows this up and the service provider is embarrassed. A private, not widely published algorithm is not a prime candidate for breaking. The cryptanalyst does not have all the information about the algorithm itself, the design principles and the mathematical assumptions and cannot feed himself with research reports from other parties. The chance that a private algorithm is suddenly broken is therefore less. However developing a proprietary algorithm costs money. Why not take the way in between ?

III.3 Security audits

Reviewing security and reporting on the efficiency of it is a typical activity of a security audit department. In this department this role can be larger in scope: the arbitrator can also report to the user community on the security of the service provider or on the security of some service users.

IV. Conclusion

Let me now make a closing remark and perhaps a challenge to all cryptographers.

Let's focus on authentication for example. To get to an acceptable level of security it is necessary that the user community exchanges authenticator keys without communicating them to the service provider. It has always been suggested that a key change must only be known by the sender and receiver and, as a consequence, not auditable by the arbitrator. Key changes are therefore not auditable and completely up to the discretion of all kinds of users (security conscious or not). Would a Boolean function $f[\text{aut}(\text{key1}, \text{txt1}), \text{aut}(\text{key2}, \text{txt2})] = \text{def} = (\text{key1} = \text{key2})$ not increase security indirectly ?