Trusted IT-Infrastructures: Not only a Technical Approach

Author:	**Norbert Pohlmann**
	Utimaco Safeware AG
☎	+49 (0)241-963-1380
📠	+49 (0)241-963-1390
E-mail:	norbert.pohlmann@utimaco.de

Contents

1 Introduction

Traffic regulations, street dimensions, constraints on vehicles and police checks are only some examples of the various accords and agreements at national and international level which constitute the basis for a common transport infrastructure and have resulted in the transport system that we take for granted today.

Similarly, when it comes to establishing trusted communication over the Internet, secure and predictable business processes over the Internet can only be achieved if common security infrastructures can be created.

The exchange of e-mails in open IT systems such as the Internet is extremely important to electronic business processes. Compared with normal postal channels and fax transmissions, e-mails can be re-used, processed electronically, saved and forwarded without having to switch media. IT systems offer the means by which individual organizations can implement large-scale rationalization, achieve high cost savings and improve flexibility and speed.

As the information (development data, customer information, strategic plans etc.) that is exchanged by e-mail actually constitutes a valuable asset, appropriate IT security must be available so that companies' assets can be adequately protected.

Suitable e-mail protection operates using public key procedures that are based around a public key infrastructure. In order that this security infrastructure can be used organization-wide, open standards must be used and practical solutions must be developed.

Only together can infrastructures be created!

2 The Need for IT Security

In recent years the value of information and along with this the need for protection of that information has grown considerably.

The increasing value of information held on computer systems has become an important economic factor, if not the most important one. Examples are:

- Complete development and production documentation: many organizations possess hardware worth thousands of dollars on which information worth millions is stored.
- Financial and operating results, strategic plans: if such results or plans were to be disclosed, this could, for example, cause changes in stock valuations which in turn could precipitate significant financial loss.
- Logistics information: if computer systems or data were to cease to be available, no one would know any longer how much unsold inventory there was, what needed to be produced, which customers had ordered what, and when and to whom goods needed be delivered.
- Customer data is particularly valuable and in need of protection.

Modern computer systems enable people to work efficiently and tasks to be performed in a logical manner which in many areas can effectively no longer be performed by any other means. We have become so dependent on computer systems that our economic capability will be endangered if the functional capability of computer systems cannot be guaranteed in an appropriate fashion.

Global expansion and changing business processes

In the past, most business processes were processed on paper (e.g. the preparation of quotations, acceptance of orders, orders, receipt of deliveries) or else in person (e.g. visits to customers). These processes can be designed far more rationally if human and material resources are replaced by electronic procedures. All the business processes listed above can be created by computer system and electronically transferred so that there is no need to switch media any more.

This makes our computer systems, and especially access to our computer systems from outside, all the more attractive to potential attackers. At the same time no official body, bank or company can manage today without relocating business processes or networking computer systems.

On the one hand it is desirable to have a connection to the outside that is easy to use and always available. On the other hand company data and relationships with business partners have to be protected against theft and willful destruction.

In department stores security guards and detectives, video cameras and steel shutters are taken for granted. But it was not until quite recently that organizations began to appreciate that data should be protected against unauthorized access as well, because it represents considerable value and in fact often constitutes the bulk of an organization’s assets.

Information technology has created the wherewithal to conduct industrial espionage conveniently with computer systems. In this new form of espionage, which does not require any walls to be torn down or safes to be broken into, often the perpetrators happily perform their deeds from the living-room without any awareness that what they are doing is illegal. The tools for such activities are available on the software market or can even be downloaded free of charge from the Internet, and detailed information is available on all the tricks both in the literature and in the Web.

Experts estimate that the economic damage resulting from computer crime already comes to billions of dollars and is increasing all the time.

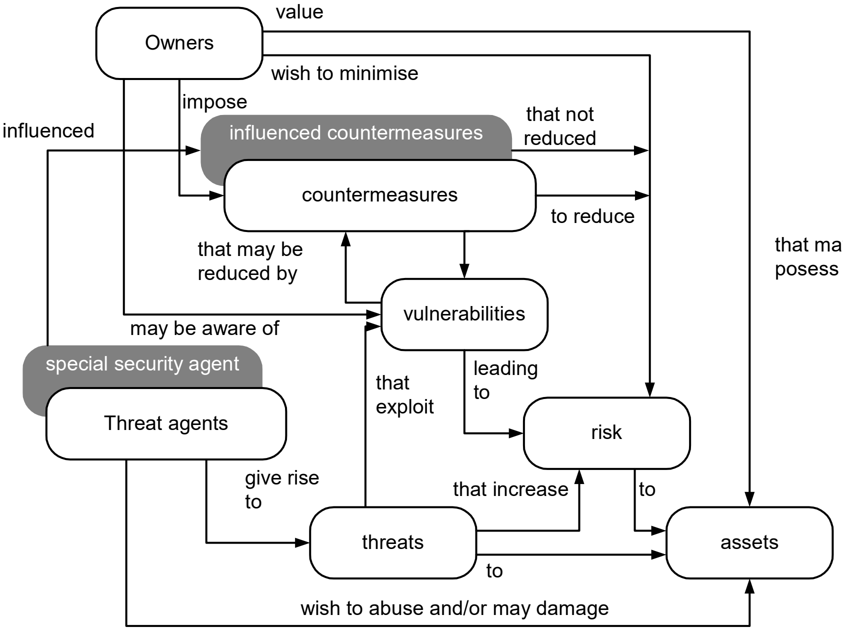
Industrial and economic espionage by the State

IT criminality is growing as methods of communication become more varied: industrial espionage is a major problem in the business world today and since the end of the Cold War has taken the place of military espionage. The main dangers here are no longer defined by geography and politics (the West versus eastern Europe) but are judged according to the competitive strength of the countries.

IT security in context

For most organizations it is either important or very important that their information (electronic assets) is protected against loss of confidentiality, integrity, availability, binding character and authenticity.

Security is generally concerned with the protection of assets against attack, where the objective of the attacker is to use these assets for his own purposes or to harm the owner of the assets.



The owner of an asset is responsible for protecting it. Attackers (or "threat agents") seek by attacking the assets to exploit their advantages and hence to work to the detriment of the owner of the assets. As far as the asset owner is concerned the attack reduces the value of his assets – if he notices it – which is not directly possible, for example, when an e-mail is intercepted.

Specialist attackers (e.g. intelligence services) are in a position to influence the manufacturers of countermeasures so that they build into their products the means of gaining access to such information assets even despite the countermeasures. For the asset owner this in turn means a reduction in the value of his assets, with the supposed reduction in the risk to which they are exposed being merely illusory.

Specialist attackers (e.g. intelligence services) are in a position to influence the manufacturers of countermeasures so that they build into their products loopholes enabling certain groups to continue to have access to the assets. For the asset owner this in turn means a reduction in the value of his assets with the reduction in the risk to which they are exposed being merely illusory.

Attacks on IT assets generally (but not necessarily) involve one or more of the following:

Loss of confidentiality

The attacker gains unauthorized possession of assets (information).

Loss of integrity

The attacker is able to manipulate assets (information) without authorization.

Loss of availability

The attacker prevents the owner from enjoying the access to his assets (information, resources and services) to which he is entitled.

Loss of binding character

The binding character of the transaction can be repudiated, i.e. a person is able to deny having sent or received assets or information.

Loss of authenticity

The communication partner is not who he purports to be, there is no certainty as to the origin of the information (data).

Opportunities and risks – two extremes of uncertainty

Companies and organizations should use the opportunities which information technology opens up to them - for example, by making full use of the Internet - but at the same time they must make the correct investment in suitable countermeasures (firewall systems, VPN, intrusion detection systems, anti-virus systems etc.) to reduce the risk of vulnerability.

Only if this is done does it become possible to conduct one's business in a responsible fashion and enhance one's capability, profit and market share, so that the business and the economy as a whole may thrive.

Positive action is necessary

When considering the security of companies, it is extremely important that overall responsibility for security matters is assumed by senior management. In practical terms this means providing resources, both financial and staffing.

3 TeleTrusT Stands for Trusted Technology

TeleTrusT is a non-profit making initiative whose members include manufacturers, users, research institutes, government bodies, consumer associations, consultancy firms, network operators and service providers. The aim of the organization is to increase confidence in electronic business processes. To examine the huge range of issues extensively and in an interdisciplinary manner and achieve a broad consensus, member companies and organizations are grouped together into subject-oriented study groups. Here a lively and above all continuous exchange takes place, increasingly at a European level, so that TeleTrusT is paving the way for successful and trusted applications.

- *Bridges between research and practice.* The exchange at this level enables research and development to be user-oriented so that security mechanisms that match real world requirements can be offered. Conversely, inputs from the world of research and development are of great interest to industry.
- *Bridges between developers and users*. If security is to be a reality, it is essential that this is combined with ease of use. The instruments of security must be uncomplicated and simple to use. Security must be directly integrated into the application or into the business processes. Only then will users be prepared to integrate implementation of their companies' security policies into their daily work routine.
- *Plugging the gap between theoretical security and market-oriented security solutions*. Not everything that is theoretically possible is also wanted by the market. The first 80% of security is quick to implement. Even 90% security is affordable. But anyone who is aiming, at impossible expense, for 100%, may actually be impeding security. A basic measure of security must, first and foremost, be practicable.

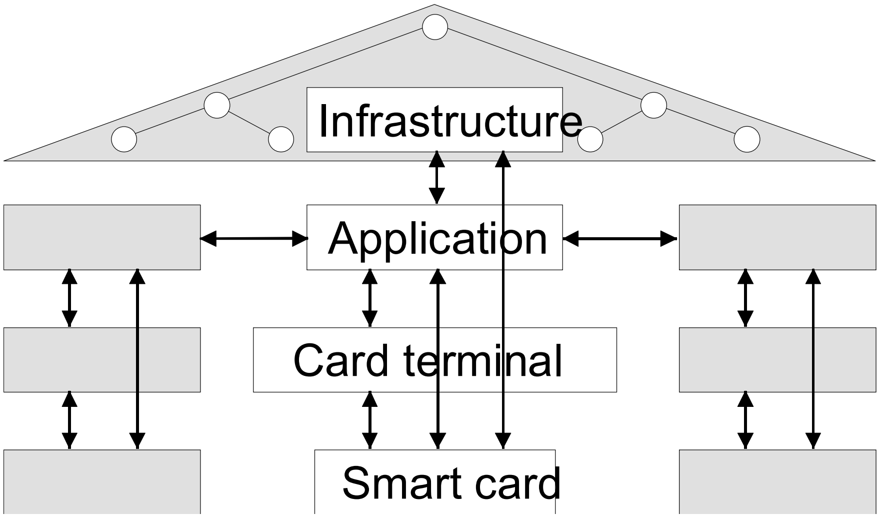
Measures aimed at achieving IT security operate with calculable residual risks – no different in fact from safety measures adopted in connection with road traffic. Different classes of automobile offer different safety equipment. But no automobile offers complete security against accidents. Market-oriented security solutions often consist of overlapping and supplementary security solutions – which to all intents and purposes constitute security.

For this reason TeleTrusT is particularly committed to e-mail security at two levels:

1. MailTrusT – interoperable security solutions for e-mail
2. Bridge-CA – the bridge which inspires confidence

4 MailTrusT – Interoperable Security Solution for e-mail

In a security system that is used across an entire corporation, the infrastructure is especially important. The diagram below shows that many different interfaces have to be considered during implementation. With virtual worlds such as the Internet, the common security infrastructure stretches beyond all geographical and political boundaries, laws and cultures and thus constitutes a new and unfamiliar challenge



In order to be able to implement a trusted application, a security technology – a security product – which provides the necessary security functions such as confidentiality through encryption and digital signatures must be integrated. Typically the user needs a security token, which can be a smart card or a special diskette. If a smart card is chosen, a smart card reader must be connected to the application.

A basic requirement for cross-organizational security is a common infrastructure which ensures that all persons have unique names, that all persons involved in the security system have electronic identification, or “certificates”, in which the public key of a public key system is certified. In addition the application must be able to access directory services which provide information at all times as to whether certain users with whom it is planned to communicate still have valid certificates or whether they have been entered in a list of barred users. All these interfaces must be specified in a system concept. It is here that MailTrusT comes in.

MailTrusT is a system concept for the trustworthy exchange of e-mails and other electronic objects and also for the necessary security infrastructure in open systems. The achievement of MailTrusT is to have defined a subset of the possibilities of the individual industry standards and, in combination with various standards, to have created a useful and practicable whole.

Objectives of the MailTrusT system concept

The MailTrusT system concept consists of a series of partial specifications and covers the objectives presented below that are necessary for a successful application:

- **Interoperability**

The MailTrusT system concept ensures that products of different manufacturers which satisfy this system concept are directly interoperable without any modifications or further coordination.

- **Minimality**

The MailTrusT system concept is minimal in order to allow product manufacturers the maximum design freedom. It essentially limits itself to what is necessary to the interoperability of different components for a range of functions that will generally be sufficient (as much as necessary, as little as possible). This ensures that vendors retain some latitude so that they can accommodate market requirements.

- **Continuity**

Continuity will, moreover, ensure the maximum degree of investment security both for manufacturers and also for customers of MailTrusT-compliant components. This approach will continue to be pursued in the future as well.

- **Universality**

The MailTrusT system concept does not presuppose any particular model of a public key infrastructure, but supports central, decentralized and combined models. The MailTrusT system concept is also not limited to particular applications. Rather, it has been designed for a broad range of applications.

- **Modularity**

The MailTrusT system concept consists of several harmonized modules which are parts of a comprehensive system concept. Under the MailTrusT system concept it is not necessary for every vendor to implement all the modules in order to be able to offer a MailTrusT-compliant product. As the modules are harmonized with each other, modules produced by different manufacturers can be combined with each other. The token interface means, for example, that components of one manufacturer can use smart cards from another manufacturer.

- **Conformity with standards**

The MailTrusT system concept is based as far as possible on established and widespread standards. As well as S/MIME, X.509 and PKCS#11 (“Cryptoki”), the specification of the PKIX working groups of the IETF and the signature interoperability specifications for the Digital Signature Act, in particular, are taken into account. On the basis of these standards profiles which make the standards interoperable and are consistent with the objectives of MailTrusT will be defined.

- **Independence**

The MailTrusT system concept was developed on the basis of the practical experience of different users, providers, research establishments, consumer associations and manufacturers. The MailTrusT system concept expressly avoided using any proprietary solutions of individual product manufacturers as a yardstick.

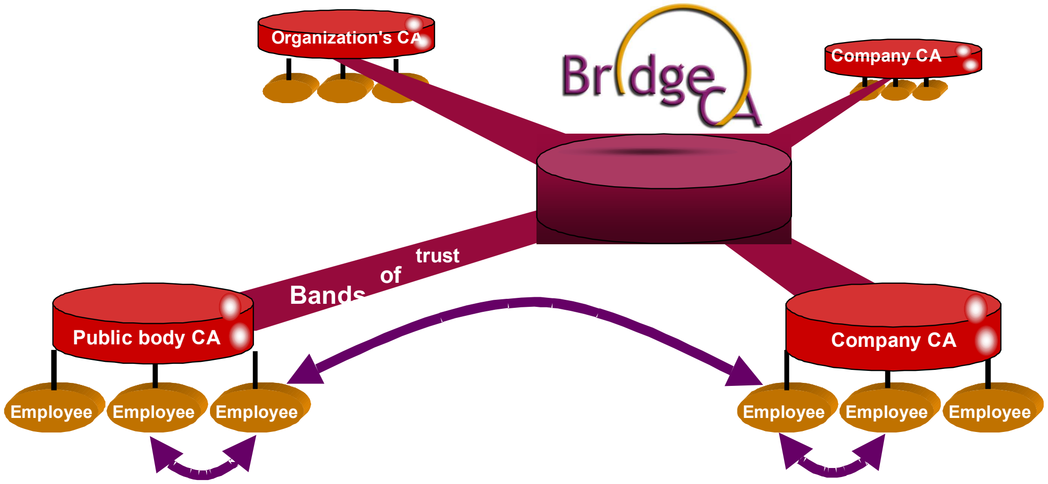
5 Bridge-CA – the Bridge Which Inspires Confidence

Bridge-CA is an all-embracing, independent bridge between the public key infrastructure of all the participating parties who wish to communicate with each other in a trusted fashion over the Internet.

The objectives of a common public key infrastructure are obvious:

- Open communication must be implementable internationally, quickly and pragmatically
- It is essential that business and administration can be confident that any investment will pay off. Hence underlying conditions that are calculable must be created.
- The first application should be the secure exchange of e-mail as this is the most widely used Internet application.

The MailTrusT specification, based on the S/MIME standard, provides a good basis for later migration to a higher security level: the legal force of the electronic signature is assured and it complies with the EU Directive on electronic signatures. One can start by using software certificates, with optional smart card support. The bridge CA is a non-profit-oriented service CA, independent of any manufacturer, controlled by an independent board and run by TeleTrusT.



The bridge CA, as root, certifies the other CAs, as a result of which it has a security level similar to baseline protection. The user CAs integrate themselves into the infrastructure. There is no control function and no checking. The certificates issued can be revoked. Personal registration takes place at the beginning.

The easy-to-use PKI solution, SafeGuard Sign&Crypt, allows addresses to be imported from Lotus Notes.

6 Cost-benefit trade-off

This section considers certain aspects of the costs and benefits of IT security.

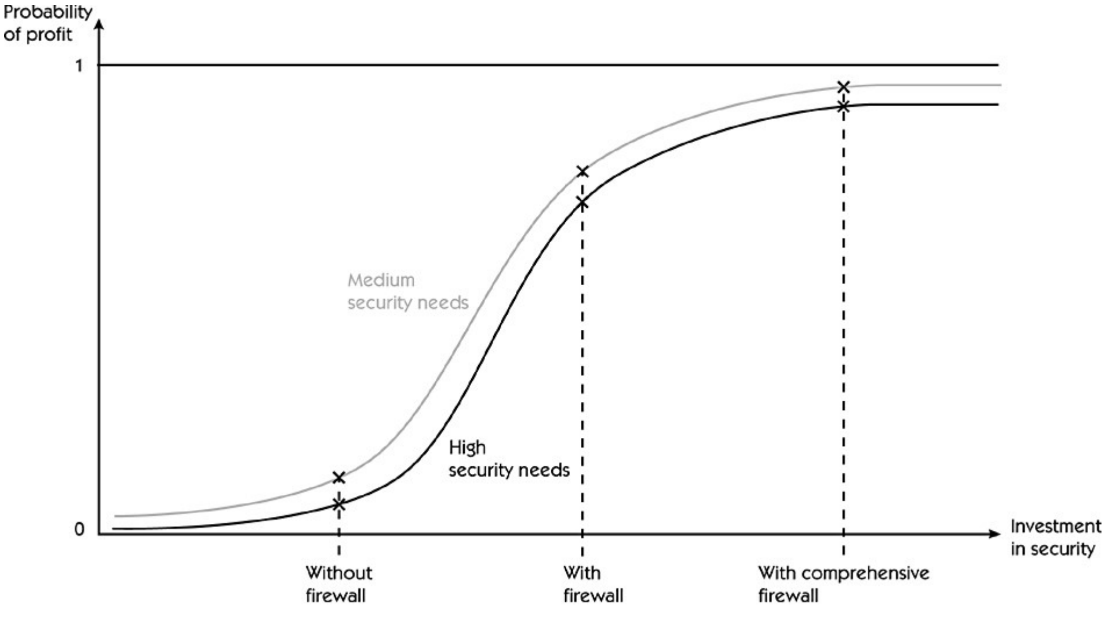
Cost-benefit considerations relating to the non-implementation of business process re-engineering

If due to his concerns about security a user declines to use the Internet as a business communications medium, then he cannot take advantage of the often considerable rationalization potential offered by the Internet. In the longer term there is the danger of losing out on business opportunities and hence of losing market share.

For this reason the investment in IT security components can produce cost savings in that it costs less than the value creation which it makes possible. This means an increase in efficiency, which at the end of the day can also improve the company's growth prospects.

Investment in IT security as a strategy for securing profits

The investment in security mechanisms depends on a company's own protection requirements and the probability of being able to achieve a certain profit, and is effectively an investment in profit protection.



The above diagram shows that in areas where the protection requirement is high (e.g. in financial institutions) higher investment in security measures is necessary in order to preserve the same prospects of making a particular profit.

As money is invested in security mechanisms, the probability of achieving a particular profit also increases. In other words, the procurement of security systems such as e-mail security systems or firewall systems (as shown in the picture) is an investment in the protection of profits. The more money is invested in security mechanisms, the greater the probability of achieving a particular profit. However, these measures alone cannot provide 100% certainty of making a profit, as there is always a residual risk.

The probability of achieving a given profit depends also on the protection requirement and, along with this, on the probability of an attack. The greater the probability, the greater the need for protection against an attack.

If the protection requirement is very high, the probability of achieving a given profit is lower than when the protection requirement is only low.

If the use of security mechanisms is abandoned, this difference is much bigger than where extensive use is made of security mechanisms, as the probability of an attack is lower where the protection requirement is only low. In the final analysis, Management of the company is responsible for the security in the enterprise and must make a decision on the correct cost-benefit ratio.

Management would be well advised to spend a certain percentage of the profit on IT security by way of profit insurance. This percentage will be higher in companies whose success is based on their image as a trustworthy company (e.g. banks and insurance companies) than in companies such as hauliers and breweries in respect of which IT security has only a minor effect on image.

Firewall Systems from the Point of View of the Economy as a Whole

In the former industrial society, production plant safety was a major issue. In today’s information society the security of IT systems is extremely important. Information (information products, digital products etc.) is for the first time of paramount importance for production and consumption. The method of production leaves its mark on society. It is therefore appropriate to speak of the transformation of an information economy into an information society.

When one considers the economy as a whole it is possible to speak of static and dynamic aspects of defects in IT security.

Static aspects of defective IT security result in the loss of effectiveness and efficiency in both the private and public sectors and thus have an adverse effect on the performance of the economy as a whole. Sporadically, i.e. in certain companies or certain sectors, the consequences can be particularly serious.

Dynamic aspects of defective IT security reduce and hinder exploitation of the rapidly changing advantages of digital technologies and markets (the “New Economy”), for example due to higher costs and lower acceptance, and lead indirectly to foregoing of the strategic advantages arising from market dominance.

It is necessary that those responsible in the business sector and in official bodies themselves take the measures necessary to achieve the required security, and do not wait to see if regulations are issued, backed by legislation, in order that sufficient security can be attained for our information society.

The problem with statutory provisions is that these have to be international if they are to apply globally to Internet usage. It was only last year that the G8 finally commenced efforts aimed at producing international legislation, and this is bound to take five to ten years to achieve.

However, given the global nature of the economy in which more and more companies are becoming internationally active and are pursuing activities well beyond the range of the statutory framework of the countries or regions in which they are based, we need to find practical solutions which can provide us with a reasonable level of security.

For this reason, initiatives such as the bridge-CA are a practical approach which can help to implement security quickly, comprehensively and globally.

7 Summary

Security systems aimed, for example, at protecting e-mail, which have to function organization-wide, require a common security infrastructure. In an international, rapidly growing market such as the Internet, implementation of these security systems needs to be interoperable, pragmatic, flexible and neutral.

For this reason, standards such as MailTrusT and initiatives such as bridge-CA, are helping to establish e-mail security, which in turn will help to safeguard our future.