Information systems security with PDAs as a part of information system of the company

Cestmir Halbich

Summary

This contribution focuses on the security with PDAs for enterprises and their information systems. Secure communication via tunnelling, strong encryption and integrated Firewalls are the integral parts of the solution, but there are some facts which leads to that events as a ILOVEYOU virus epidemic with human failure cause. We can built security models, and find ways to improve information systems security. There are basic rules in a corporations, which we can describe by common valid scheme. Into this model we can implicate "visible exposure", but "invisible exposure" can be often more important , see some types of misinformation. In the article is described security model of whole information system with PDAs as a part of this. There are discussed advantages of information systems security via our model in conclusions.

Key words: risk assessment, security model, personal digital assistant

1. Introduction

The relevance of the information security in practice is no longer underestimated nowadays. The value of information, which is used in the information system (further IS) of a company, is constantly increasing, which is why it pays to employ more sophisticated methods and means of data protection, even though the overall cost for new precautions may be higher than before. The cost of such precautions is mostly comparable to the cost of the data.

The use of personal digital assistants (further PDA) as a part of the information system of a company seems to be very forward-looking nowadays. This statement is supported by the tendencies of the market with T and the author‘s own experience. As the appropriate use of personal computers has increased people‘s working performance in the office, the PDAs can do the same in mobile surroundings, where computers of the desk-top kind will always be unusable. The great advantage of the PDA market in comparison with that of PCs, where more than 90 per cent desktops are IBM clons, is its greater diversity (with all the pros and cons implied). The possibility that one would choose a suitable computer is thus heavily reduced, while a suitable PDA can be chosen substantially more easily. The market-share of various solutions is nowadays standing as follows: Palm OS 60%, Microsoft Windows for Pocket PC 30% (PocketPC), EPOC

10% etc. The PDA user can choose according to application, price, size and also the time it can run on batteries, which ranges roughly from 3 or 4 weeks to 2 or 3 hours. If PDAs are to become an integral part of the IS of the company, we have to consider also the security element of the process of integrating them into the IS. It is a well-known fact that an IS is only that secure as the weakest element of the system. If the security rate of the PDAs were the lowest, we would have to search measures to increase their security rate.

2. Brief description of the individual PDAs from the point of view of their use in the IS of the company

It is generally suitable, owing to the use of pen and touch screen usually without any keyboard, to use the PDAs for applications where not many pieces of unique data are stored (which are not possible to be written down into tables and forms on a PC in advance). If the input of data is limited to the selection of values, prepared beforehand in a table, or ticking off a box in a form, the PDA is the very proper means. All types of PDAs are able to be synchronised with PCs, which has to be maximally used.

PDAs using the Palm OS – are used most often, are the most widespread, users prefer, according to the manufacturer, the easier way of work, with which they are marked off. It is advisable to use such IS which employ only a few applications. They are suitable for use with a dedicated (and secure) application, the advantage being that they can run on batteries for a long time (battery life is from 2 to 4 weeks depending on application in use). Considering the tried-and-true and compact operating system (further OS), either in ROM or Flash, the applications can be more secure and the IS of the company more attack resistant. The development of the actual secure application is easier than with the PocketPCs. In case of extremely high security requirements, it is possible to develop one‘s own secure OS following the principles of the OS theory (microcore, layers etc.). An OS is single-tasking and single-threaded, the security analysis is more conclusive than with other OS types.

The PocketPCs are more appropriate for the use of experienced PC users because the architecture of their OS resembles very much MS Windows on desk-top PCs. Some of their advantages include their proximity to MS Windows users, multimediality, their multitasking OS and colour display. These advantages won‘t, however, come in useful in the whole range of the IS applications of the company (they are, no doubt, the merits in the field of entertainment). A significant disadvantage can be their lower operational time on batteries, up to 8 hours depending on the application. It does not stand for such a serious restriction in the office but what about the fieldwork without energy?

Other OS are a minority which does not necessarily have to be a disadvatage with critical applications concerning the IS of the company, where their specific merits can come in useful. These types of OS include eg. EPOC, a rather robust OS with the battery life of some 12 hours and hardware possibilities between the Palm OS and Pocket PC.

3. Security characterictics of the PDAs and the possibilities to improve them

The PDA security consists of the actual security of the PDA (it is very easy to lose it) and the security of communication with other elements of the IS. It is possible to protect all PDAs with a password at the start of the OS, however, it does not present a basic problem for an experienced and financially and technically armed opponent. It is possible to increase the data protection by encryption the content of the PDA. There is a whole range of products for all types of operating systems and hardware platforms of PDAs, a whole lot of them, however, is not more closely particularised at all and all we can do about the power of the cipher is to speculate (but eg. for PocketPC there is a BlowFish encryption algorithm implementation, which enables us to at least estimate the power of the protection). When using PDAs with critical applications, it is possible to implement the encryption algorithm right for the application. It is advisable to implement a tried-and-true encryption algorithm, on the other hand, this can cause problems with the use of libraries for operations with large numbers etc.

In case of a critical application it pays to develop such an application which is able to “recognise” the situation, when a PDA user fills in a password under the constraint of the attacker. In such a case the IS should pretend a normal activity, but it should also signalise an attempt to violate the IS security and give to disposal counterfeit data and IS activities so that the life and health of the user were not endangered. In case of a loss, it is advisable to implement some kind of an auto-destructive program.

The second scope of security problems is the synchronisation of the PDA content with the IS. PDAs usually use information which are prepared on PC and then transferred to PDA, where can be used. Although only a minor amount of information is usually transferred in the opposite direction, those pieces of information may on the other hand be of the very underlying and irreplacable character, obtained by the application and the user right in the field (factory, wood, field, street etc.).

The safest but the least comfortable is to synchronise data with the help of a cable, which belongs usually to the PDA accessory. Of the same security level can roughly be the transfer of the encoded data via the IR ray. With this means we no longer have a hundred percent control over any possible unauthorised monitoring (we can use the freeware programs of the IR monitor type). Problems should not arise if we use an adequatelly strong cipher.

For completely uncritical applications it is possible to use the standard unciphered data transfer, supplied by the manufacturer, via IR rays, where even simple technical equipment enables practically everyone to monitor our entire communication in the range of our PDA. If it involves IS with openly accessible information, the unciphered transfer may not matter at all, but usually we have to protect our company from undesirable activities of the competitors.

PDAs can be used also for wireless access to the internet, WAP service etc. At present it is the most dangerous access to the IS in the Czech republic whatsever. The passwords are sent to the GSM nets unciphered (usually via the IR port of the mobile phone) and the one who knows the TCP/IP protocols, internet servers and other vital information can misuse our activities for his/her own sake. In such a case I would very much consider the password system in IS and PDAs, very much recommend the division of applications working with the IS or internet.

At present, it is possible to secure very well only the synchronisation between the PDA and the IS, not the interactive work between the PDA and internet. Although this interactive work is possible, it is not very safe. We can also imagine that the PDA is the authentisation item for the access to the IS. It is highly probably that this application will not be the only one run on the PDA. A PDA as an authentisation item in comparison with the usual authentisation items enables to use the IS independently on the location of the user on Earth.

4. The risk assessment when employing the PDA as parts of the IS

If we try to guess the risk, we proceed from the general layer model of the IS see Fig.1., where individual layers shade off the hardware from the software and the individual layers of the software mutually provide, by a defined way, communication and so security. In case of the deficient level of IS security, it is possible to insert another layer, which provides precisely the IS security (see eg. SSL protocol, which among the four layers of the TCP/IP protocol adds into an

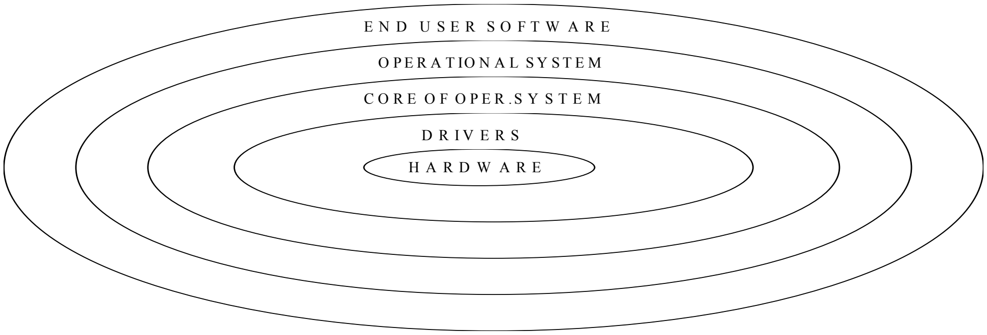

Fig. 1. Layer structure of IS

appropriate interface (between transport and application layer) its own layer and in this substantial way increases the security of the whole IS).

Reliability theory provides a way to examine a multiple component system calculating its overall reliability, the probability that the system will work. Many systems can be modelled using series structures, parallel structures or both. The same way we can use for the evaluation of the information system security. The system is working or it failures through security incident. The other possibility does not exist.

The following are examples of series structures:

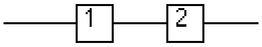

Fig.1.

For this system to work, both components 1 and 2 must work.

There may be many components in a series.

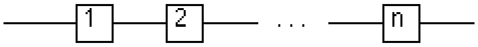

Fig. 2.

In a parallel system, the system will work as long as at least one component works.

The following are examples of parallel structures:

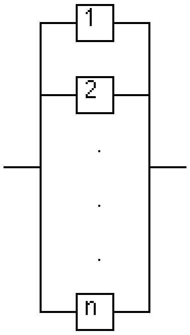

Fig. 3.

A system may also combine both parallel and series structures:

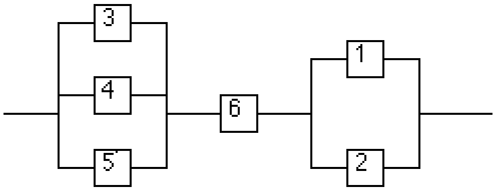

Fig. 4.

Practical complicated information systems are described usually with both parallel and series structures. But simple risk assessment can be implemented in a series or parallel structure of secure components. The improving of the information system security can be reach by added advisable parallel or series secure component. For example for series system which consists from three parts with reliability R=R=R=0.9 the reliability of whole system is $R_w = 0.999$. It means, that rather non reliable (non secure) components can create rather reliable structure (secure system).

The main term from the theory of the reliability is Mean Time To Failure(MTTF). It means Expected time that a system will operate before the first failure occurs (first secure incident). In the case of the exponential failure law the unreliability F(t) is

$$F(t)=1 - e^{-\lambda t}$$

and reliability R(t)

$$R(t) = e^{-\lambda t}.$$

This formulas lead to the term for MTTF

$$MTTF = 1/\lambda$$

For λt<< 0,1 we have a good approximations:

$$R = 1 - \lambda t \text{ and } F = 1 - \lambda t$$

Risk assessment of the system which consists from n elements with risk of failure λ_1, $\lambda_{2, \ldots}$ λ_n
Is computed from the formula

$$R_c = R_1\ .\ R_2\ .\ Rn = e^{-\lambda_1 t} . e^{-\lambda_2 t} \ldots.. e^{-\lambda_n t} = e^{-\lambda_c t}$$

The finite risk failure value is the sum of risk failure values of the individual components in the case of the reliability of series systems, assuming λ_i are independent

$$R_1(t) = R_2(t) = R_3(t) = 0.9$$

$$R_{series}(t) = 0.9\ .\ 0.9\ .\ 0.9 = 0.729$$

Reliability of Parallel Systems

Only one of n identical components is required for the system to function (for example the protection of the unauthorised access), it seems , that parallel system structure is better to understood the risk assessment in the area of information systems security.

When a system contains both series and parallel structure, we can reduce the reliability block diagram by replacing parallel portions with an equivalent single element.

This precaution (the insertion of the security module into the IS) can be easily incorporated into the security module and that can be done in two almost similar ways. We can either proceed from the idea that a chain tears when its weakest link is torn (serial progression of the articles of the system). In such a case the precaution is the parallel strengthening of the weakest link by a product, protocol, service, hardware etc., or we can use a parallel concept. If we have a system which includes a amount of parallel holes (here opens the analogy with the electric conductivity of a branches of a system), the largest hole (with the biggest conductivity), fill it with another precaution which will cause the lower conductivity of the hole in question (we will fill the hole by a precaution characterised by a higher resistance to breakthroughs). From the point of view of the mechanical analogy we either strengthen the weakest link of the chain or make the largest hole smaller, which is then more difficult to penetrate. From the point of view of the effective use of money and resources it is always correct to eliminate the greatest system weakness.

5.Conclusion

When we include PDAs in the IS, we get hold of the advantage a more mobile and flexible work with the IS. That brings the whole range of advantages to the economic profit of the corporation. The disadvantage on the other hand is the increase of security risks. These risks can

be reduced. On the basis of the analysis of the contemporary state and future trends we can generalise the following facts:
- the more user-friendly product, the less secure the product is (with comparable investments into the hardware, software and services),
- PDAs provide greater diversification of performance, OS potential and applications than PCs.

Each company can choose the optimal solution. It is possible to use methods of the risk assessment if we adequatelly use PDAs with the IS.

References:

HALBICH, C.: Information systems security as a competition advantage, In Proceedings of The eight annual international conference ”Business and economic development in central and eastern Europe: Implications for economic integration into wider Europe, pp. 262 – 269, Brno 2000, Czech republic

Author's address :
Cestmir Halbich, Department of information technologies, Faculty of economics and management, Czech university of agriculture, Prague, e-mail halbich@pef.czu.cz