Portable Computer Risk Analysis - End User Perspective

Jorma Kajava
University of Oulu, Department of Information Processing Science,
Linnanmaa, Fin-90570 Oulu, Finland
e-mail: kajava@rieska.oulu.fi

Vesa Mäntylä
Helsinki Telephone Company ltd
Kasarmikatu 36, Fin-00130 Helsinki, Finland
e-mail: vesa.mantyla@hpy.fi

Abstract

Portable computers play an increasingly important role in modern computing. The computing power and storage capacity of today's laptop computers is much bigger than that of computers at the beginning of the 1980's. Aspects related to the security of information in portable computers has, however, attracted less attention than the security of information in the office environment.

And yet, portable computers are more vulnerable than ordinary PCs in many ways: they are easy to steal, their use discloses information to outsiders and they are often used in uncontrollable areas. More importantly, their communication capabilities and remote connections to company networks may expose the entire computing system of the company in question.

Due to the abovementioned reasons, threats to information security must be approached differently in the portable environment than in the office environment. The main concern in the former environment is that information in a portable computer is often more valuable than the computer itself. The crucial question is then what kind of information should we carry around in our portables and what kind of countermeasures against potential threats should we implement?

In spite of the problems, we must not lose sight of the fact that portable computers also have a number characteristics which improve their security. One of these is that, owing to their nature as highly personalized individual tools, portable computers are Personal Computers in a very real sense of the word.

Keywords

Portable computers, Information Security

1. DATA IN PORTABLE COMPUTERS

Fairly simple methods can be used to analyze risks in the portable computing environment, because the laptop is an entity itself, and the limits of the system are clearly defined. Risk analysis should be used to refine a policy aiming at defining a corporate laptop protection plan [Eloff 93].

Risk analysis must begin with an analysis of the data carried in portable computers. Employees have always carried classified information with them, but this information has traditionally been in printed form and the volume has been limited. A portable computer with a 1 Gb hard disk, drastically increases the amount of sensible data that may end up in wrong hands and cause serious to the company and its business.

As a consequence, benefits should be weighed against risks before introducing laptops into everyday use. The company must have a clearly defined policy as to what kind of data its employees can have in their laptops and what measures they must take to protect themselves against existing risks.

Information is usually divided into two main categories: public and secret. Secret information is further classified as confidential, secret and top secret. The classification varies slightly from country to country and company to company, but the main classes are usually roughly the same. Table one is a simple matrix showing what kinds of information can be held in differently protected portable computers. It should be noted that this kind of matrix must include at least one type of information which is newer allowed in portable computers. After a company has introduced a system of classifying information, they can go on to produce a similar matrix to meet their particular needs.

Table 1. Allowed information in portable computers [modified Maier 95]

	NORMAL LAPTOP	PROTECTED	HIGHLY PROTECTED	NOT ALLOWABLE IN LAPTOP
PUBLIC	**YES**	**YES**		
CONFIDENTIAL	**NO**	**YES**	**YES**	
SECRET	**NO**	**NO**	**YES**	**x?**
TOP SECRET	**NO**	**NO**	**NO**	**YES**

YES = information is allowed in laptop
NO = information is not allowed in laptop
x? = depends on company policy

Sometimes the value of the information contained in a portable computer is higher that the value of the information available in the internal information system of a company. In these cases, even more attention must be paid to aspects related to the secrecy of information.

2. THREATS AGAINST PORTABLE COMPUTERS

Threats against information in portable computers can be divided into three main categories: disclosure of data, loss of data and modification of data.

2.1 Disclosure of Data

Harmful disclosure of data is much more obvious in the portable computer environment than in the office environment. This is because the environments where laptops are generally used, are full of observers who can be regarded as ehostilek. 'Looking over the shoulderk can pass unnoticed and be totally innocent in purpose, but there is, nevertheless, always a certain degree of risk associated with it. The data on the screen may contain such information as UID, password and dial-in phone numbers, which can later be used to break into the company's information system. Thus, such disclosure of information poses a threat not only to the information in the laptop, but also to the information assets of the entire company.

When dial-in lines and cellular phones, not to mention the Internet, are used to access the information system of a company, the possibilities for data disclosure increase,

because cellular phone connections are easy to eavesdrop, and often no encryption is used during some such connection [Cullinane 96].

Unintentional disclosure of data occurs when a laptop is used by several persons. Generally, the various users are not interested in the contents of the hard drive, but they are, however, keen to store their own data on it. Thus, data accumulates on the drive until, finally, someone finds it in their interest to use it wrongly. We must remember that the delete command does not actually erase the data on the disk, it merely removes pointers to the data, enabling the original data to be restored with the undelete command.

2.2 Loss of data

Loss of data and destruction of data are threats that can cause a lot of harm and even render the laptop completely unuseful. It will be major a catastrophe if, for example, a laptop containing all the information needed for a business trip gets lost for some reason (if it is left behind or disappears with the luggage).

Data can also disappear due to theft. Although an ordinary thief is usually interested in the computer itself, not in the information it contains, the information too will be lost if there is no back-up copy. Illegal copying of data constitutes another form of information theft. This may happen, for example, in a hotel room or in conference facilities during breaks. Unfortunately, this kind of theft is often unnoticed, which is why no countermeasures are taken to prevent it from happening. A new threat has emerged in the shape of the PCMCIA hard drive, which can be quickly unplugged and stolen. When this kind of theft occurs, the thief is more likely to be interested in the information on the disk than in the disk itself, which, paradoxically enough, enables us to apply fast and accurate countermeasures.

2.3 Modification of data

Mistakes by users and access by unauthorized users and malicious software (viruses etc.) comprise threats to the integrity of data. Unauthorized users may modify data purposefully or accidentally but, on the whole, viruses are much more likely to alter or erase data than unauthorized users. However, by applying proper countermeasures against viruses, we will be more or less secure.

When portable computers are used at home, small children's fascination with new and interesting things should be taken into account. As for teenagers, they tend to bring home games acquired from school or friends, and these can be infested by viruses. Both forms of access are significant threats to the integrity of data in a portable computer.

3. PROTECTION METHODS

The security of information in portable computers must be based on the same basic principles as the security of information in other computers. Protection must be built in accordance with the nature of the information to be protected, but it should not be oversized so that the availability of the information will decrease essentially. The first step in all security measures involves arranging education concerning information security. Special emphasis must be placed on explaining potential threats against portable computers.

The following properties are the laptop's assets in terms of information security:

1. Real Personal Computer
2. Size
3. PCMCIA-cards
4. External floppy disk drive
5. Removable power source

The first item on the list is the most valuable asset, as it contains no disadvantages in terms of security. The other four can also be seen as disadvantages.

Real Personal Computer - when a laptop is considered as a real personal computer, the holder of the laptop has total responsibility for using and maintaining it. As a consequence, the machine is better taken care of and more attention is paid to possible threats.

Size - owing to it's small size, a laptop can be locked in a hotel safe or stored securely in some other place. Size, however, is also a vulnerability, as a small machine is easy to steal.

PCMCIA cards - instead of a non-removable hard disk, secret critical information can be stored on a flash-memory card or on a hard disk card, both of which are easily removed and can be put in a safe place. Of course, if not properly stored, these cards too can be a threat to information security.

No floppy or external floppy disk - unauthorized copying of information from a hard disk to a floppy disk is rendered considerably more difficult when a laptop has no internal floppy drive. Although this may decrease the usability of the laptop, it is definitely an advantage from the security perspective.

Removable power source - removable batteries and mains power sources make laptops unusable.

Figure 1 shows some common threats as well as safeguards against them.

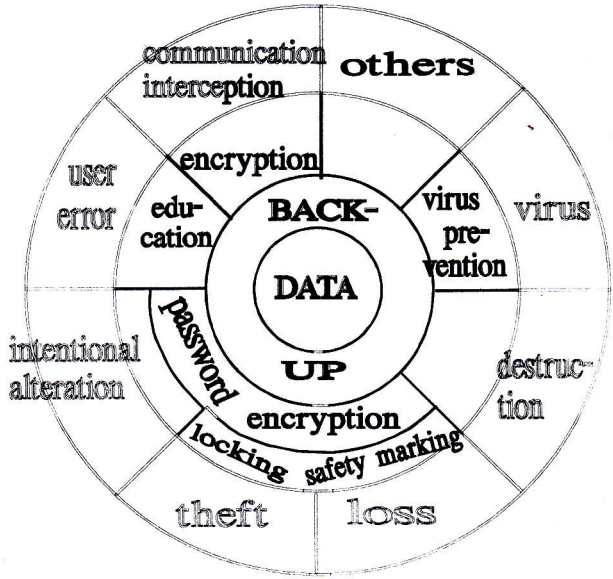

Figure 1. Threats and safeguards against portable computers.

3.1 User identification

Most laptops have a good BIOS-based password protection system. Some operating systems have their own, fairly reliable, user-ID/password protection mechanisms, but that is not quite enough when secret information is held in a laptop. In such cases, more secure methods must be employed to identify the user. These methods include passwords that are used just once, some form of challenge/response identification or the generation of time-based passwords. There are several commercial products on the market suitable for strong user authentication, and it is up to the companies to select the best one to achieve the required security level.

Communication with the internal network of the company must take place through a firewall. The firewall must utilize strong user authentication methods before allowing anyone access to the internal network.

3.2 Prevention of data disclosure

When protecting data against unauthorized access, disclosure or modification, the least one can do is to use proper UID/password protection methods. First of all, passwords must not be stored in plain text format on a hard disk. Secondly, booting the computer from a diskette without a password must be prevented. The next step involves encrypting the data. It should be noted in this context that we can ensure total secrecy only by encrypting all data on a hard disk. If we encrypt only those files that are classified as secret, and store swap files and temporary files in plain text format, we are exposing ourselves to security threats. Again, commercial products are available for data encryption. Products originating in the USA come only with 56-bit DES-keys, but there are products from other countries without such key escrow. These products also enable strong user authentication and diskette encryption. An easy method of making data unavailable to a possible intruder or a thief is by locking it in a safety box. Diskettes, PCMCIA-cards, detachable hard disks and, indeed, the entire laptop, can be kept in a safe place when not in use. Data can be protected by making the laptop inactive when not in use, simply by removing the battery or the power source. These methods are recommended only for meticulous users.

When the Internet is used as a communication channel, care must be taken not to transfer company secrets in plain text format. End-to-end encryption is the only reliable way of ensuring the secrecy of data. Furthermore, if a company has several portable computers, the management of encryption keys must be properly arranged. If the encryption method used by the company is weak, the keys must be changed frequently.

3.3 Virus protection

Virus protection in the laptop environment must be as rigorous as virus protection in the office environment. This type of threat is considerably diminished when the laptop does not have a diskette drive and if all diskettes are virus-checked before use.

4. SECURITY SOFTWARE AND PORTABLE COMPUTERS - SOME EXPERIENCES

Personal workstation protection is used because preventing all the others expect the workstation special user to get to research the files in workstation. The protection concerns only files stored on the workstation, not network contacts or applications used through a network.

Protection software should be easy to install and use. It should be also transparent to the end-users at the hardware level.

We have investigated and tested two programmes designed to protect workstations. Because this kind of software is meant to be run on end-user workstations, the programmes must fulfil a set a requirements. Firstly, the software must be easy to install and uncomplicated to use. Then, it must start with password prevention at all levels, it must come with effective password management and it must encrypt files using at least a DES level algorithm. Furthermore, the software must be transparent and fast enough not to slow the computer down significantly. Finally, the software must facilitate easy handling of diskettes in a protected environment.

In our tests we looked at two programmes: Safe Guard Easy (SGE) and AR DISKrete. As our test arrangements and results are described in an earlier paper [Mäntylä 96], the following is merely a short synopsis.

First of all, both programmes were fairly uncomplicated from the users' point of view and easy to run on workstations. AR DISKrete can be said to be easily adaptable to the portable environment, as it provides hard disk encryption and a stable environment for handling diskettes. Unfortunately, there were some practical difficulties with our portable test computer owing to/resulting in the fact that some results were not as reliable as could be hoped. As for Safe Guard Easy, our tests indicated that it was easier to adapt it to hard disk share encryption in portable computers and office PC than AR DISKrete.

5. USER EDUCATION

An informed and responsible user is the most important resource in secure portable computing. This can be achieved by user education and coaching. Clear directions as to handling different situations when using portable computers and an awareness of the special threats in the portable environment go a long way toward achieving the goal. Special methods and procedures, which often complicate the use of laptops, must be explained in such a way that the users understand the rationale behind their introduction.

The following short checklist can be given to all laptop users [Maier 95]:

- have a virus prevention program active at all times
- use only diskettes intended for internal use
- protect the laptop physically whenever it is outside the perimeters of your office

- when working in the presence of other people, make sure that no one is "looking over your shoulder"
- encrypt your hard disk when possible
- report all observations relating to company information (disappearance of data, unexplained changes, etc.)
- when using a communication connection to the internal network of the company:
  - use strong authentication methods
  - encrypt the whole session
  - notify network administration when a connection is no longer needed.

6. CONCLUSIONS

Portable computers represent an increased risk to the security of information in a company. If, however, adequate attention is paid to these risks and the users are properly educated, the risks can be greatly reduced. The countermeasures should not be oversized so that they unnecessarily complicate the use of portable computers, lest people avoid these methods. When education and protective measures are in step, people are comfortable with their laptops. And when users realize that it is their responsibility to protect the data and the computer, an adequate level of protection has been reached. This is decidedly easier with laptops than with PCs. PCs in the office environment are usually connected to LANs, and most applications are network dependent. This explains why office PCs are not quite as personal tools as laptops, and why the sense of responsibility among their users is not as high as that of laptop users.

Portable computers can reach the status of the most secure computer, if their users' sense of responsibility is high, and we think that this feeling is achieved easier with laptops than with office PCs.

ACKNOWLEDGMENT

We are greatful to Mr. Matti Paadar for bringing our attention to some new ideas regarding how portable computers can achieve more higher level of security. We would also like to thank Mr. Rauno Varonen for checking our English.

REFERENCES

Some of the following books and bublications have given ideas how the portable computers security should be handled and some have been used as direct references during this work:

Cullinane 96 Cullinane Dave: Protection of Mobile Computing Assets. Information Systems Security, Auerbach Publications, Vol. 5 no 1, Spring 1996.

Davies 89 Davies D. W., Price W. L.: Security for Computer Networks (Chapter 7. Identity Verification). John Wiley & Sons LTD, Great Britain 1989.

Eloff 93 Eloff J.H.P. , Labuschagne L. and Badenhorst K.P. : A comparative framework for risk analysis methods. Computers & Security 12/1993, Elsevier Science Publishers Ltd.

Feuerlicht 88 Feuerlicht J., Grattan P.: The Role of Classification of Information in Controlling Data Proliferation in End-User PC Environment. Caelli W. J. (Editor): Computer Security in The Age of Information . IFIP Sec'88.

Jackson 92 Jackson K. M., Hruska J. (Editors): Computer Security Reference Book. Part 4: Personal Computer Security. Butterworth- Heineman Ltd, UK 1992.

Kajava 95 Kajava J., Leiwo, J. : Information Security for Workstations: Implications for End-Users. In R. von Solms (ed.): Notes on Information Security Management 1995. International Federation of Information Processing, Port Elizabeth, South Africa, 1996.

Maier 95 Maier Phillip Q.: Protecting the Portable Computing Environment. Information Systems Security, Auerbach Publications, Vol 4 No 2, Fall 1995.

Mäntylä 96 Mäntylä V., Kajava J. : Information Security in Portable Computers. University of Oulu, Department of Information Processing Science, Working Papers Series B 44, Oulu, 1996 (in Finnish).