INFORMATION SECURITY IN POWER ENGINEERING

BĂLĂŞOIU LEONARD

University of Bacău

Abstract: Safety and quality of the supplied energy are not only depending on the traditional power engineering background, but are strongly determined by the security conditions of informatics, too. The formation and the operation of the energy market (like any other electronic commerce application) have to be based on secure communication between the partners. The secret and authentic communication can be ensured using e.g. public key infrastructure. Important goal of the authors was to present the connection, the joint role of several, originally separated fields, namely power engineering, telecommunication and information security. Some of the new results of the research work carried out at S.C.Electrica S.A. are also presented in the paper. Electromagnetic compatibility between mobile telecommunication systems and other civil control and communication systems (e.g. banks, hospitals, air and municipal traffic, industrial digital control systems, fire alarm systems) has been investigated.

Keywords:, information security, security policy.

1. SECURITY POLICY

1.1 What is a security policy and why have one?

The security-related decisions you make, or fail to make, as administrator largely determines how secure or insecure your network is, how much functionality your network offers, and how easy your network is to use. However, you cannot make good decisions about security without first determining what your security goals are. Until you determine what your security goals are, you cannot make effective use of any collection of security tools because you simply will not know what to check for and what restrictions to impose. For example, your goals will probably be very different from the goals of a product vendor. Vendors are trying to make configuration and operation of their products as simple as possible, which implies that the default configurations will often be as open (i.e., insecure) as possible.
While this does make it easier to install new products, it also leaves access to those systems, and other systems through them, open to any user who wanders by.
Your goals will be largely determined by the following key tradeoffs:
1. services offered versus security provided - Each service offered to users carries its own security risks.For some services the risk outweighs the benefit of the service and the administrator may choose to eliminate the service rather than try to secure it.
2. ease of use versus security - The easiest system to use would allow access to any user and require no passwords; that is, there would be no security.Requiring passwords makes the system a little less convenient, but more secure. Requiring device-generated one-time passwords makes the system even more difficult to use, but much more secure.
3. cost of security versus risk of loss - There are many different costs to security: monetary (i.e., the cost of purchasing security hardware and software like firewalls and one-time password generators), performance (i.e., encryption and decryption take time), and ease of use (as mentioned above). There are also many levels of risk:

loss of privacy (i.e., the reading of information by unauthorized individuals), loss of data (i.e., the corruption or erasure of information), and the loss of service (e.g., the filling of data storage space, usage of computational resources, and denial of network access). Each type of cost must be weighed against each type of loss. Your goals should be communicated to all users, operations staff, and managers through a set of security rules, called a "security policy." We are using this term, rather than the narrower "computer security policy" since the scope includes all types of information technology and the information stored and manipulated by the technology.

1.2. Definitions of a security policy

A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.

1.3. Purposes of a security policy

The main purpose of a security policy is to inform users, staff and managers of their obligatory requirements for protecting technology and information assets. The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. Therefore, an attempt to use a set of security tools in the absence of at least an implied security policy is meaningless.
Another major use of an AUP is to spell out, exactly, the corporate position on privacy issues and intellectual property issues. In some countries, if the company does not explicitly state that e-mail is not secure, it is considered to be so and any breach could cause privacy and confidentiality liabilities. It is very important to spell out what is and is not acceptable in intellectual transfers and storage and what the corporate privacy policies are to prevent litigation about same.
An Appropriate Use Policy (AUP) may also be part of a security policy. It should spell out what users shall and shall not do on the various components of the system, including the type of traffic allowed on the networks. The AUP should be as explicit as possible to avoid ambiguity or misunderstanding. For example, an AUP might list any prohibited USENET newsgroups. (Note: Appropriate Use Policy is referred to as Acceptable Use Policy by some sites.)

1.4. Who should be involved when forming policy?

In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. It is especially important that corporate management fully support the security policy process otherwise there is little chance that they will have the intended impact. The following is a list of individuals who should be involved in the creation and review of security policy documents:

- site security administrator
- information technology technical staff (e.g., staff from computing center)
- administrators of large user groups within the organization (e.g., business divisions, computer science department within a university, etc.)
- security incident response team
- representatives of the user groups affected by the security policy
- responsible management
- legal counsel (if appropriate)

The list above is representative of many organizations, but is not necessarily comprehensive. The idea is to bring in representation from key stakeholders, management who have budget and policy authority, technical staff who know what can and cannot be supported, and legal counsel who know the legal ramifications of various policy choices. In some organizations, it may be appropriate to include EDP audit personnel. Involving this group is important if resulting policy statements are to reach the broadest possible acceptance. It is also relevant to mention that the role of legal counsel will also vary from country to country.

1.5. What makes a goog security policy?

The characteristics of a good security policy are:

1. It must be implementable through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods.
2. It must be enforceable with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible.
3. It must clearly define the areas of responsibility for the users, administrators, and management.
The components of a good security policy include:
1. Computer Technology Purchasing Guidelines which specify required, or preferred, security features. These should supplement existing purchasing policies and guidelines.
2. A Privacy Policy which defines reasonable expectations of privacy regarding such issues as monitoring of electronic mail, logging of keystrokes, and access to users' files.
3. An Access Policy which defines access rights and privileges to protect assets from loss or disclosure by specifying acceptable use guidelines for users, operations staff, and management. It should provide guidelines for external connections, data communications, connecting devices to a network, and adding new software to systems. It should also specify any required notification messages (e.g., connect messages should provide warnings about authorized usage and line monitoring, and not simply say "Welcome").
4. An Accountability Policy which defines the responsibilities of users, operations staff, and management. It should specify an audit capability, and provide incident handling guidelines (i.e., what to do and who to contact if a possible intrusion is detected).
5. An Authentication Policy which establishes trust through an effective password policy, and by setting guidelines for remote location authentication and the use of authentication devices (e.g., one-time passwords and the devices that generate them).
6. An Availability statement which sets users' expectations for the availability of resources. It should address redundancy and recovery issues, as well as specify operating hours and maintenance downtime periods. It should also include contact information for reporting system and network failures.
7. An Information Technology System & Network Maintenance Policy which describes how both internal and external maintenance people are allowed to handle and access technology. One important topic to be addressed here is whether remote maintenance is allowed and how such access is controlled. Another area for consideration here is outsourcing and how it is managed.
8. A Violations Reporting Policy that indicates which types of violations (e.g., privacy and security, internal and external) must be reported and to whom the reports are made. A nonthreatening atmosphere and the possibility of anonymous reporting will result in a greater probability that a violation will be reported if it is detected.
9. Supporting Information which provides users, staff, and management with contact information for each type of policy violation; guidelines on how to handle outside queries about a security incident, or information which may be considered confidential or proprietary; and cross-references to security procedures and related information, such as company policies and governmental laws and regulations.
There may be regulatory requirements that affect some aspects of your security policy (e.g., line monitoring). The creators of the security policy should consider seeking legal assistance in the creation of the policy. At a minimum, the policy should be reviewed by legal counsel.
Once your security policy has been established it should be clearly communicated to users, staff, and management. Having all personnel sign a statement indicating that they have read, understood, and agreed to abide by the policy is an important part of the process. Finally, your policy should be reviewed on a regular basis to see if it is successfully supporting your security needs.

1.6. Keeping the policy flexible

In order for a security policy to be viable for the long term, it requires a lot of flexibility based upon an architectural security concept. A security policy should be (largely) independent from specific hardware and software situations (as specific systems tend to be replaced or moved overnight). The mechanisms for updating the policy should be clearly spelled out. This includes the process, the people involved, and the people who must sign-off on the changes. It is also important to recognize that there are exceptions to every rule. Whenever possible, the policy should spell out what exceptions to the general policy exist. For example, under what conditions is a system administrator allowed to go through a user's files. Also, there may be some cases when multiple users will have access to the same userid. For example, on systems with a "root" user, multiple system administrators may know the password and use the root account.

1.7. Threats

A threat can be any person, object, or event that, if realized, could potentially cause damage to the LAN. Threats can be malicious, such as the intentional modification of sensitive information, or can be accidental, such as an error in a calculation, or the accidental deletion of a file. Threats can also be acts of nature, i.e. flooding, wind, lightning, etc. ***The immediate damage caused by a threat is referred to as an impact.***

Vulnerabilities are weaknesses in a LAN that can be exploited by a threat. For example, unauthorized access (the threat) to the LAN could occur by an outsider guessing an obvious password. The vulnerability exploited is the poor password choice made by a user. Reducing or eliminating the vulnerabilities of the LAN can reduce or eliminate the risk of threats to the LAN. For example, a tool that can help users choose robust passwords may reduce the chance that users will utilize poor passwords, and thus reduce the threat of unauthorized LAN access.

A security service is the collection of security mechanisms, supporting data files, and procedures that help protect the LAN from specific threats. For example, the identification and authentication service helps protect the LAN from unauthorized LAN access by requiring that a user identify himself, as well as verifying that identity. The security service is only as robust as the mechanisms, procedures, etc. that make up the service.

Security mechanisms are the controls implemented to provide the security services needed to protect the LAN. For example, a token based authentication system (which requires that the user be in possession of a required token) may be the mechanism implemented to provide the identification and authentication service. Other mechanisms that help maintain the confidentiality of the authentication information can also be considered as part of the identification and authentication service.

1.8. Threats and vulnerabilities

Identifying threats requires one to look at the impact and consequence of the threat if it is realized. The impact of the threat, which usually points to the immediate nearterm problems, results in disclosure, modification, destruction, or denial of service.

The more significant long-term consequences of the threat being realized are the result of lost business, violation of privacy, civil law suits, fines, loss of human life or other long term effects. The approach taken here is to categorize the types of impacts that can occur on a LAN so that specific technical threats can be grouped by the impacts and examined in a meaningful manner. For example, the technical threats that can lead to the impact 'LAN traffic compromise' in general can be distinguished from those threats that can lead to the impact 'disruption of LAN functionalities'. It should be recognized that many threats may result in more than one impact; however, for this discussion a particular threat will be discussed only in conjunction with one impact. The impacts that will be used to categorize and discuss the threats to a LAN environment are:

- **Unauthorized LAN access** - results from an unauthorized individual gaining access to the LAN.
- **Inappropriate access to LAN resources** - results from an individual, authorized or unauthorized, gaining access to LAN resources in an unauthorized manner.
- **Disclosure of data** - results from an individual accessing or reading information and possibly revealing the information in an accidental or unauthorized intentional manner.
- **Unauthorized Modification to data and software** - results from an individual modifying, deleting or destroying LAN data and software in an unauthorized or accidental manner.
- **Disclosure of LAN traffic** - results from an individual accessing or reading information and possibly revealing the information in an accidental or unauthorized intentional manner as it moves through the LAN.
- **Spoofing of LAN traffic** - results when a message appears to have been sent from a legitimate, named sender, when actually the message had not been.

Disruption of LAN functions - results from threats that block LAN resources from being available in a timely manner.

2. POWER ENGINEERING AND INFORMATION SECURITY

Unprecedented progress has been started in the generation,transportation and consumption of the electrical energy in the latest decades. On one hand, this revolution happened in the electrical devices, equipment and systems, but on the other hand power engineering has completely changed because of the wide spread of information technology. Today, the safety and quality of the supplied energy not only depend on traditional power engineering, but strongly depend on the safety and security of informatics and telecommunication too. The formation and the operation of the energy market (like any other electronic commerce application) have to be based on secure communication between the partners. The aim of information security is the protection of information. There are three main attributes of information that strongly determine its value:

• **Availability** means that the authorized users of an information system are able to access, deliver or process the required data. The availability of information is breached when the authorized users can not access the data needed for their work.

• **Confidentiality** means that only authorized users are able to access certain classified information. Confidentiality is violated if unauthorized people read or copy such classified information.

• **Integrity** means that information is unmodified, authentic or complete and can be relied upon. Information can loose its integrity if it is modified by accident or by a malicious attack.

While availability means reliable operation of the system, confidentiality and integrity are rather limitations on the operation for providing attacks (either natural disasters or deliberate attacks of a malicious adversary).The aim of all safety and security systems is to protect the value of certain assets. The question is: how much to afford for protecting our values? The cost of the protection has to be compared with the expected value of the loss. This latter can be evaluated based upon the value of a single damage, the frequency of the damages, and the expected life time of the device, equipment or system.

This value has to be compared with the certain cost of the protection (the sure investment cost and the estimated cost of maintenance for the life time). The different appearance of these costs in time has to be considered, too (discounting). If we are facing deliberate attacks, we may estimate how much the attacker can gain with a successful attack. In this case, a system can be considered to be safe, if the cost of the attack is much higher than the possible profit of the attacker. Perfect security can never be reached in practice, the solution can only be to reach a situation, when our risk is small enough.

The designers of most security systems follow the above principles, regardless the system belongs to electrical safety, burglar-alarm, prevention of accidents, lightning or overvoltage protection, protection against electric, magnetic or electromagnetic disturbances, but can cover even encryption or data security too. Protection always means considering risks, and developing various tools and countermeasures to diminish them. Naturally, these tools depend on the appropriate technological field. In this paper we consider the connection between the two, originally separated fields, namely power engineering and information security.

If we consider the problem of secure (encrypted and/or authenticated) communication over an insecure network then public key infrastructure (PKI) seems to be one of the most promising solutions. Such an infrastructure allows users who work at different companies (and possibly in different countries) to send secure messages to each other without having to meet and exchange secret information.

Such an infrastructure allows users of a huge and distributed insecure network (like the Internet) to make business without having to completely trust each other.

In a public key infrastructure, the identity of every user is based on two pieces of information (cryptographic keys).

One of them – called private key – is secret and is known by the user only. The one who controls a user's private key can digitally sign messages on his or her behalf, and can decipher all the messages that were sent to him or her. The other piece of information is called public key.

This one should be published, because the user's public key is needed to send encrypted messages to him or her or to check his or her digital signatures.

The two main key issues of public key infrastructure are the following:

• Each user has to keep his or her private key secret (confidential) while using it frequently (keep it available)

• Each user has to publish his or her public key authentically, in a way, that attackers cannot modify (its integrity) it unnoticed.

This second goal is fulfilled by so called certificate authorities. They issue digital certificates that encapsulate the users' private keys. Every time a public key is used, the corresponding certificate needs to be checked. A good description on this system can be found in [15].

One of the most promising solutions for the first goals seems to be the use of cryptographic tokens (e.g. smart cards). These devices are in fact small computers, which are tamper-resistant. They may even destroy the data they store if they detect that an attacker would receive it.
However, if an authorized user identifies him- or herself by a PIN code or by biometric means, they allow certain operations on the stored data (e.g. digital signature with the stored private key). Smart cards are not only used in PKI systems, but as ID cards, telephone cards or in loyalty applications.
The main drawback of smart cards is that they do not possess a user interface of their own. Thus, they need a terminal to communicate with the user. If this terminal is malicious (e.g. because it is infected by a virus), various attacks are possible. For example, the terminal may show one message to the user, and send another one to the user's smart card for signing. Thus, a malicious terminal can make a user sign something he or she would not sign.
This critical issue is subject to research all over the world.
Important new results have been presented in the Laboratory of Cryptography and System Security, at Budapest University of Technology and Economics. For example, new protocols have been developed, that rely on biometric messages. The user sends the message to be signed in a so called biometric format (e.g. video message), that is significantly harder to counterfeit the plaintext ones. The smart card places secure timestamps on the message to ensure, that the attacker had very little time to attack.

REFERENCES

1. Computer, Internet and Network Systems Security- S.K.PARMAR, Cst, N.Cowichan Duncan RCMP Det 6060 Canada Ave., Duncan, BC
2. Balog E., Berta I., *Fuzzy Logic in Electrostatics*, Hazard Assessment, Electrostatics, 1999. 10th Int. Conf. Cambridge, Inst. Phys.Conf.Ser.163. pp. 215-221.
3. Balog E., Berta I., *Fuzzy Solutions in Electrostatics*, Journal of Electrostatics 51 & 52 (2001), pp 409-415.
4. Berta I., *Static Control, Modelling and Application*, Journal of Electrostatics, 30 (1993) pp 365-380, invited lecture on the 7th International Conference on Electrostatics, Lahnstein, 1993.
5. Berta I.Zs., Mann Z. Á., *Evaluating Elliptic Curve Cryptography on PC and Smart Card*, Periodica Polytechnica 2001.
6. Berta I.Zs , Vajda, I., *Documents from malicious terminals*, SPIE Microtechnologies for the New Millenium 2003, Bioengineered and Bioinspired Systems, Maspalomas, 2003.
7. Electromagnetic compatibility, EN 61000
8. *Handbook of Electrostatics* (Chang J.S., Crowley J.M., Kelly A.J.) Berta I. Chapter 31. Static Electricity Hazards: Solid Surfaces and Gases, Marcel Dekker, Inc., New York, 1995. pp. 703-722.
9. *Guidelines for limiting exposure to time-varying electric, magnetic and electromagnetic fields* (up to 300 GHz), 1998 Health and Physics Society
10. Horváth T., Berta I., *Static Elimination*, Research Studies Press a Division of John Wiley and Sons Ltd. Chichester, 1982. p. 118.
11. Horváth T., *Computation of Lightning Protection*, Research Studies Press a Division of John Wiley and Sons Ltd. Towntown, 1993
12. Horváth T., Berta I., *Level and expected frequency of LEMP caused by near and far lightning strokes*, 26th International Conference on Lightning Protection, Proc. of ICLP 2002, pp. 574-578
13. Horváth T., *Protection of Antennas of Mobile Phone Relay Stations against Direct Strokes*, ICLP 2004.
14. *Safety of machinery, Guidance and recommendations for the avoidance of hazards due to static electricity*, CENELEC Report R044-001, 1999.
15. Schneier, B, *Applied Cryptography*, John Wiley & Sons, 1996.
16. www.icnirp.de
17. www.iegmp.org.uk
18. www.who.int/emf