ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 *2010. No. 9(105)*
ELEKTRONIKA IR ELEKTROTECHNIKA

MEDICINE TECHNOLOGY
T 115
MEDICINOS TECHNOLOGIJA

Risk and Protection of Medical Information Systems

Tz. D. Dimitrova
Technical University of Sofia, Bulgaria,
8, Kliment Ohridsky str. 1000 Sofia, Bulgaria, phone, +359 (2) 9652278, e-mail: tz.dimitrova@gmail.com

Introduction

Medical data confidentiality is an essential demand for each kind of data processing and information handling in medicine nowadays. The delivery of healthcare to patients increasingly relies on Medical Informationm Systems (MedIS). These systems rely on modern information technology (IT) to electronically collect, process, distribute, display, and store patient data. Telemedicine is one of the very important scientific area which developed a lot last decades with the new technologies. There are many health networks FTTH „fibre to the home“, which includes not only many hospitals, but many patients also (Fig. 1).

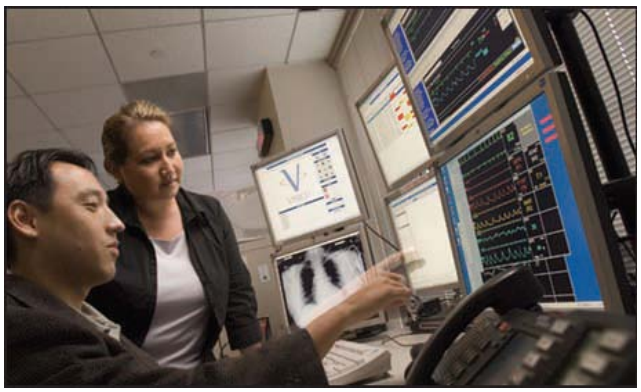

Fig. 1. Centre of a health network „fibre to the home“

These new information and communication technologies in medicine create new problems. MedIS, like other IT-systems, are vulnerable to malware attacks. Data protection, confidentiality and computer security are basic requirements for the appropriate introduction and use of information and communication technologies in health care. The basic technical challenge is the openness of modern data processing and communication systems. There is virtually no paper on medical data processing that doesn't mention the need of data protection. But with new technologies the situation becomes even worse, as they change the way medical data have to be protected.

The paper identifies some of the main problem domains.

Potential Vilnerabilities

Systems become vulnerable to malicious logic when they are placed in an environment that allows an attacker access. The most invulnerable MedIS would have proprietary software, running only one dedicated application, isolated from other systems, afforded perfect physical access control, developed in a malware-sterile factory, requiring no service. Every deviation from this impossible hypothetical system results in the risks and vulnerabilities outlined in this section. [1, 2].

Physical Access to Medical Information Systems. A knowledgeable attacker with physical access to a system including media access, e.g., floppy disk or CD-ROM drives, may be able to infect it with malware. Highly mobile systems increase the difficulty of controlling physical access to them. This increases the likelihood of unauthorized use and modification.

Connectivity

Vulnerabilities appear when MedIS come into contact with the outside world. This may happen via direct serial port connection, modem, or network connections.

Stand-Alone Systems. Stand-alone systems without media access (i.e., no floppy drives, CD-ROM drives, nor net-work) are at the least risk of attack. They remain vulnerable to:

- Infected service tools used on-site;
- Malicious or inappropriate actions by service technicians;
- Malicious or inappropriate actions by vendors or suppliers during manufacture;
- Malicious or inappropriate actions by users.

Media Access. In the past media was the predominant means of interconnecting IT systems with each other. Malware-infected media can cause infection of systems that access it. So infected media was a common vector for attacking systems with malicious logic [11]. Though still an issue, in-fected media is losing importance as MedIS is

increasingly becoming electronically interconnected [10].

Networked Systems. Networked devices are increasingly replacing standalone systems to improve workflow and reduce administrative costs [2]. They share the above risks (Fig. 2). In addition, they also are subject to wider ranges of malicious logic that can traverse the network from one machine to the next and therefore, are vulnerable to:

- Internal forms of malicious logic, which can also be propagated from one system to an-other, e.g., worms;
- External forms of malicious logic that operate from outside of the MedIS, e.g., malware-induced DoS.

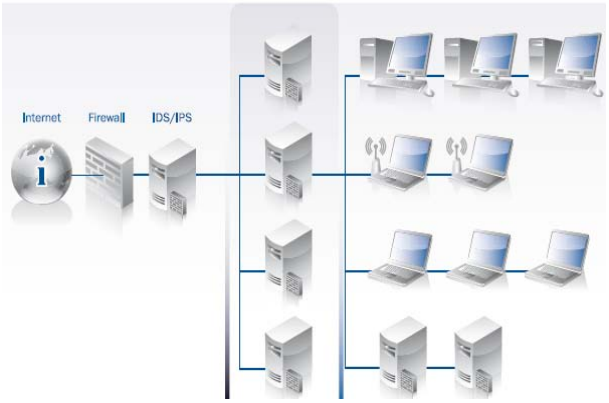

Fig. 2. Network accessible for vulnerabilities

Malware propagates between interconnected MedIS using the same technical mechanisms intended for normal communication. Networked systems may require specific services, e.g., http, ftp, SSL, and others, and correlated preassigned ports, depending on the intended use.

Attackers typically desire to affect the greatest number of systems they can, so most frame their service-related attacks on the most common implementations of a service. The more of these services are on a system, the more likely that system will be affected by a successful attack. Likewise, the greater the interconnectivity of devices, the more opportunity an at-tacker may have to gain access.

The more potential attackers, the greater the risk. Devices connected directly to the Internet have the greatest risk. It is not the kinds of vulnerabilities that change, but the potential num-ber of attackers that increases.

Software Related Vulnerabilities

MedIS Using Common Software Platforms. Malware attacks often attack commonly used platforms because they are easy to find, weak-nesses are known, and they have the highest impact. General purpose systems, which are based on common standards and protocols, are therefore more vulnerable than specialized systems. Despite the increased risk, the healthcare enterprise has benefited greatly from using common software platforms.

Device-Specific Application Software . The software intended to accomplish the dedicated task of a specific type or model of medical equipment can be termed device-specific. It likely will be written to take advantage of common protocols and to operate with a standard operating system such as Unix or Windows, but is specific and functional only with particular MedIS. Such device-specific software is not general-purpose and, as compared to other application software – like office applications for word processing or spreadsheets – is distributed in narrow communities under strict licensing and version controls.

Shared Use Systems. MedIS installed onto a shared use general purpose IT system remains vulnerable to all of the relevant media and network access threats of a dedicated system. In addition, it becomes vulnerable to all the preexisting or subsequent malware infections of the host system. The MedIS vulnerability further increases when the host system also includes E-mail, en-ables Internet access, or offers services such as FTP, NFS, and RPC. The shared use system cannot make as many changes because the sys-tem must support the needs of all the different uses. [3, 4, 6]

The first and most important use of a computer in a clinic or a physicians practice is the management of the patient data. The electronic patient record (or computer-based patient record–CPR) serves several purposes: billing the patient, legal documentation, quality control, scientific research. The doctor has to archive the data for several years and has to transmit some of the data to a health insurance company for billing. Technical means should ensure that the patient record is disclosed only to authorized persons or institutions, according to the 'need to know' principle, and that the integrity of the data is protected.Defence .

Against Malicious Logic for MedIS

The definition of administrative and technical measures should be started with an intended use risk and threat analysis, so that resources are utilized where most beneficial. It should consider the following points.

System Integrity Assurance. Integrity assurance can prevent or at least detect modification of the software installed in the system. Unintended or unexpected software changes might be due to the introduction of malware anywhere in the design, manufacturing, installation, and service process. We will discuss some technical approaches to assuring integrity of the system in the following sections. [1, 7, 8, 9]

Hardware Protection. Hardware can be used to raise the level of assurance that software has not been changed in an unauthorized way, for example, Read Only Memory (ROM) and key-locked cabinets.

Checksum Calculation. Checksums can be computed and compared to assure that a file is not modified. A check-sum is a value calculated from the content of a file that gives the system ability to check its integrity before use. Possible implementations range from a simple parity bit check, as typically used when transmitting data over a serial line, to a 128-bit hash created when using the MD-5 algorithm. In principle, all methods share the common properties of ease in computing and low probability that correct matches between computed and expected values occur with changed data. However, the ease in computing, in terms of CPU load, varies widely with techniques, as

does the probability of detecting problems.

Digital Signatures. Digital signatures are an extension of checksums. When a checksum is digitally signed, the probability that the original file has been changed by an unauthorized user or process can be further minimized.

System Profiles. System profiles are sophisticated check summing systems that go beyond a simple list of checksums. They verify complete directory structures, e.g., including verification of file attrib-utes, presence or absence of files, and many other characteristics of the entire combination of files present. System profiles often employ digitally signed databases and may incorporate file system checks that bypass normal operating system facilities in order to detect the more sophisticated checksum aware malicious logic.

Manufacturing Scan. Using virus detection software, with up-to-date virus signature files, at appropriate stages of the manufacturing process is another way to assure system integrity. A scan by an off-the-shelf virus detection tool could assure the delivery of malware free products and updates.[5] This does not prevent a subsequent infection.

Defensive System Design. Many attack paths utilize flaws that result from common software development errors that do not introduce problems during normal operation. The most common such mistake is called the "buffer overflow" error already exploited by many malicious attacks. It permits a malicious code to overflow the allocated buffer and take control of the system. The design methodology used by the engineering staff should help to avoid, detect, and eliminate these flaws. Specific tools and techniques should be used by engineering staff, several of which are discussed within this section.

Developmental Tools. There are development tools and methodologies that can analyze systems to detect and help eliminate flaws. Some of them are formal evaluation methods, such as those found in the Common Criteria (ISO/IEC 15408) ,as well as code analysis, requirements analysis, and design analysis tools.

Programming Language. Some programming languages, such as Java and C#, incorporate security features that provide protection against some forms of malware attack. There are also support library and compiler features for some languages, such as C and C++, which can be used to reduce vulnerability to some forms of attack.

OS and Hardware Services. Some operating systems and hardware provide security features such as execute protection bits, privilege rings, etc. Applications should run with the lowest privilege practical.

Network Service Restrictions. Many MedIS systems are based upon common computer platforms that incorporate many network features such as logical ports and a suite of available network services. Remove or close all unnecessary features, ports, and services to eliminate potential malware attack points. For example, e-mail or web access facilities should be deliberately removed from MedIS that have no need for these services. Their absence may be noticeable to the users who are accustomed to generic computer platforms but it should be understood as normal and desirable to increase IT security.

Security-focused Engineering Services. Software audits and inspections by independent personnel, including peer reviews and soft-ware walkthrough sessions, can further reduce inadvertent errors. These techniques are commonly used for detection of functional flaws. Their scope should be expanded to include vulnerability reduction.

Host Virus Checkers. Virus checkers or virus scanning software is well known as a class of application software that searches hard drives, disks, etc.Unfortunately this software i only for viruses which arre known by that software. Virus checkers typically consist of an executable application (scan engine) and a data file of virus patterns containing the information required by the scan engine to detect known viruses. After detecting a virus the virus checker performs a preconfigured action e.g., making an entry in a log-file, spawning a pop-up window with a warning text, performing an automated at-tempt to repair the infected file. Virus scanners have significant drawbacks when used with MedIS. Some common impacts when using virus scanners with MedIS include the following:

- Medical images, e.g., x-rays, can be damaged because the virus scanner consumes too much system resources;
- Medical image files can be damaged because the virus scanner attempts to fix what it falsely identified as a virus;
- Virus scanning software set to detect system behavior abnormalities can falsely identify medical software as having malicious behavior and shut down the medical software;
- Pop-up windows from virus scanners can obscure medical images and medically nec-essary alerts.

Specifics and Restrictions for Medical Information Systems

Healthcare-specific regulatory and technological requirements further influence the choice of countermeasures used in MedIS as compared to those that might be used with standard of-fice IT:

– MedIS must operate safely and effectively. Protection mechanisms must not interfere with the intended medical use of the equipment.

– When there is a failure, MedIS usually "fails open," leaving the system usable. Non-medical IT equipment usually shuts down upon failure, e.g., Automatic Teller Machines go out-of-service in the event of a problem.

Defenses Against Malicious Logic for MedIS Users

Behavioral/Administrative Defenses. In addition to the protective measures described above, organizations should consider the following additional processes and technologies:

- Risk analysis and mitigation planning.
- Restrict physical access to MedIS whenever possible by physically hiding MedIS, closing doors, locking keyboards etc.
- Review all connections of MedIS to other equipment and networks for necessity and reduce

such connections to the absolute minimum. Properly configured routers by trained IT staff can deliver a high level of security.

- Wireless communications must receive special attention. For example improperly con-figured devices could inadvertently connect to an adjacent but unknown network.

Defense in Depth. The Defense In Depth concept realizes that protecting the security of an enterprise is best achieved by duplicating controls at multiple locations. A healthcare facility should establish a multi-layered defense against the risks and consequences of malware and other MedIS threats. It is helpful to provide defenses at different layers. In this way, if an attacker gets through one network security measure, there are additional security measures to help thwart the attack.

Conclusions

A single standardized solution to the issues raised by malicious logic cannot be offered in this paper. Instead, in Sections 2 and 3, a basic set of reasonable technical measures for users has been described. Depending on the local situation each measure by itself may help healthcare providers using MedIS to increase the level of protection against the threats imposed by malicious logic. Some of these measures require in-depth analysis of the impact to safe intended use of the MedIS and thus should be the joint responsibilities of the MedIS users. Most defenses are well-established common IT tools and may be properly configured by the healthcare provider. The best approach is defense in depth. Users must take special care when defining and configuring their local security concept to avoid implementing measures that weaken the inherent security level of their MedIS.

References

1. **Jordanova L., Dimitrova Tz.** Investigation on Noise Characteristic of Cable Channel for Telemedicine // Electronics and Electrical Engineering. – Kaunas: Technologija, 2009. – No. 4(92). – P. 103–106.
2. **Dimitrova Tz.** Medical Data risk exposure // 4th International Conference, CEMA'09. - Sofia, October, 2009. - P. 32-35.
3. **Cranor L., Guduru P., Arjula M.** User interfaces for privacy agents // ACM Transactions on Computer Human Interaction, 2006. – No. 12(2). – P. 135–178, 2006.
4. **de Paula R., et. al.** Two experiences designing for effective security // In SOUPS'05: Proceedings of the second symposium on Usable privacy and security. - New York, USA, 2005.
5. **Dhamija R., Tygar J., Hearst M.** Why phishing works // In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2006.
6. **Downs J. S., Holbrook M. B., Cranor L. F.** Decision strategies and susceptibility to phishing // In SOUPS'06: Proceedings of the second symposium on Usable privacy and
7. Security. - New York, USA, 2006.
8. **Dimitrov D. Tz., Ralev N. D.** Signals and Systems for Electrosleep // Electronics and Electrical Engineering. – Kaunas: Technologija, 2009. – No. 5(93). – P. 95–98.
9. **Working paper:** Project No.:8353Z, Contract No.:DAAB07-94-C-H601, Taxonomy of Threats and Security Services for Information Systems, Gulachenski and Cost, (MITRE, 1994)
10. **Dimitrov D. Tz.** Improving the Performance of Program Package for 3D Simulation of Low Frequency Magnetic Field in Medical Therapy // Electronics and Electrical Engineering. – Kaunas: Technologija, 2007. – No. 1(72). – P. 69–72.
11. **Dimitrov D.** An Investigation on Influence of Electromagnetic Field of GSM Apparatuses on the Human Body // The Mediterranean Journal of Electronics and Communication, 2006. - Vol. 2. - No. 4. - P. 141-147.
12. **Dimitrov D. Tz.** Visualization of a Low Frequency Magnetic Field, generated by Girdle Coil in Magnetotherapy // Electronics and Electrical Engineering. – Kaunas: Technologija, 2007. – No. 6(78). – P. 57–60.

Received 2010 02 14

Tz. D. Dimitrova. Risk and Protection of Medical Information Systems // Electronics and Electrical Engineering. – Kaunas: Technologija, 2010. – No. 9(105). – P. 109–112.

The delivery of healthcare to patients („fibre to the home") increasingly relies on Medical Information System (MedIS). MedIS, like other IT-systems, are vulnerable to malware attacks. MedIS owners and operators have a special responsibility to shield their systems from mali-cious attacks. These efforts involve technology and procedures that need to be considered during the whole product life cycle. MedIS presents additional challenges not usually present in the office IT environment. Medical data must be better protected because it is needed to protect the health of patients. Ill. 2, bibl. 12 (in English; abstracts in English and Lithuanian).

Tz. D. Dimitrova. Medicininės informacinės sistemos rizika ir apsauga // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2010. – Nr. 9(105). – P. 109–112.

Šviesolaidžio diegimas namų ūkyje leidžia didinti sveikatos priežiūros teikiamų paslaugų spektrą ir vis labiau priklauso nuo medicininės informacinės sistemos (MedIS). Kenkėjiškomis programomis pažeidžiamos tokios sistemos gali būti. Joms keliami ypač dideli apsaugos nuo kenkėjiškų programų reikalavimai. MedIS turi pranašumų, kurie paprastai nėra taikomi standartinėje informacinių sistemų aplinkoje. Pacientų sveikatai įtakos turintys medicininiai duomenys turi būti labai gerai apsaugoti. Il. 2, bibl. 12 (anglų kalba; santraukos anglų ir lietuvių k.).