SECURITY AND RELIABILITY CONSIDERATIONS FOR DISTRIBUTED HEALHCARE SYSTEMS

Kamil Matoušek, Ph.D.
The Gerstner Lab, Department of Cybernetics
Czech Technical University in Prague
Technická 2, Prague 6, CZ-16627
Czech Republic
matousek@fel.cvut.cz

Abstract – The article summarizes and introduces into the basic security and reliability considerations for developing distributed software systems in healthcare. It describes security objectives and protection of system assets. Stress is given to the need of risk analysis. Possible system vulnerabilities and system threats are enumerated. Necessary security awareness of humans, typical security and reliability requirements, as well as typical security methods and corresponding infrastructure for application protection, data protection and network protection are reflected.

Index Terms – System Security, Distributed Healthcare Systems, Healthcare Information Systems.

I. INTRODUCTION

In order to implement distributed software applications in healthcare domain, there are many engineering considerations to be taken into account. Due to their nature, such systems often contain sensitive private and/or life-critical data, which has to be appropriately preserved and protected. Prevention of undesirable data loss is critical, as well as possible data modification or misuse. On the other hand the software solutions distributed in a computer network environment (especially in case of, but not limited to Internet) can be vulnerable to many kinds of attacks and communication problems. Moreover the operation properties of healthcare applications have to address the reliability requirements, which have to guarantee the seamless operation of the supported healthcare services respecting the necessary standards of care.

Mainly because of these reasons the distributed software applications in healthcare domain typically require different infrastructural components and services.

The rest of the article is organized as follows: The following section introduces into security objectives, while section III. discusses system assets and the need of their protection enumerating possible system threats and necessary security awareness of humans. Typical security and reliability requirements can be found in section IV. Finally, section V. contains typical security methods and corresponding infrastructure and services for application protection, data protection and network protection. Concluding remarks then offer further reading concerning security and reliability considerations.

II. SECURITY OBJECTIVES

The security objectives aim at protecting identified assets (see the next section). They should be formulated in terms of availability, confidentiality, integrity of those assets, and legitimate use of the system. Concerning availability, there can be e.g. required operation continuity in the whole 24 hours/7days of week. Confidentiality of all data assets shall ensure that only duly authorized users have access to the data content. Integrity of data contributes to prevention of continued use of the contaminated system or corrupted data, which could result in inaccuracy, fraud, or erroneous decisions.

III. ASSETS AND THEIR PROTECTION

Assets represent any resource within the healthcare system that must be protected from all types of risks possibly damaging the ordinary operations. In general, there are valuable data assets, software assets, physical assets and even reputational assets of the healthcare provider to be protected.

The assets should be analyzed in order to estimate the value of potential impact (e.g. loss of reputation, loss of performance or financial losses). Risk analysis should take place and envision potential that a given threat will exploit vulnerabilities and cause loss or damage to an asset.

Vulnerabilities are weaknesses associated with identified assets. Vulnerability can be represented as a condition or set of conditions that may allow a threat to affect an asset. Therefore, a vulnerability that cannot be exploited by a threat need not be considered harmful to the asset.

A. System Threats

Generally, threats are in potentially loss-causing events

resulting in harm to the healthcare institution and its assets. This can take many forms. Threats can be an act of nature (such as flood, fire and earthquake), intentional or accidental acts. In general, it could result in:

1. Destruction of an asset (facilities, data, equipment, communications, personnel);
2. Corruption or modification of an asset (data, applications);
3. Theft, removal or loss of an asset (equipment, data, applications);
4. Disclosure of an asset (data);
5. Interruption of services.

A threat would need to exploit the vulnerability of the asset in order to successfully cause harm. The threats can be intentional or accidental and in detail they are typically represented by illegitimate use of the system by insiders (regular users), illegitimate access by outsiders (hackers, criminals), denial of service (DoS) attacks, sniffing (where an attacker uses software to listen to all traffic passing across the network), unauthorized software changes, introduction of damaging or disruptive software (e.g. viruses), theft or damage of data and facilities, user errors, communication failures, software errors and other technical failures. Last but not least there are also environmental threats (like natural disasters), which may influence the system availability and functionality.

When designing the healthcare system, the risk of the aforementioned threats should be carefully evaluated so that the appropriate probability of occurrence and level of possible damage can be estimated.

B. Security Awareness

Administrators as well as ordinary users should be aware, that security failures may significantly harm systems and networks under their control, that potential harm to others can arise from interconnectivity and interdependency. They should be also aware of the configuration of the system, and of available updates for the system and available good practices to enhance security.

The responsibilities of individual actors should be clearly defined – e.g. user responsibilities might need to be accountable, developers, designers, and suppliers shall address system and network security and distribute appropriate information including updates in a timely manner.

IV. SECURITY AND RELIABILITY REQUIREMENTS

This section discusses the considerable security and reliability requirements to the distributed healthcare systems.

A. Security Requirements

Distributed software systems in healthcare should reflect existing security risks as well as legal and user requirements.

Based on this, the main sources of information security requirements can be enumerated as follows:

1. Unique security risks which could result in significant losses if they occur;
2. Legal, statutory and contractual requirements that the healthcare providers have to comply with;
3. Healthcare-wide principles, objectives and requirements to support ordinary workflow operations;
4. Any other relevant source of information as far as information security is concerned.

Each of them should be formulated in terms of the confidentiality, integrity and availability of the information.

B. Reliability Requirements

Typical reliability requirements for healthcare applications include system availability, information integrity, information reliability, sensitive data protection and misuse prevention. The developed reliable system has to respect ethical, privacy, as well as timeliness of information processing constraints and other additional constraints like the need for parallel information processing, synchronization, system deadlock prevention etc.

V. SECURITY INFRASTRUCTURE

When securing a software system, the most important infrastructural service often deals with unambiguous identification of all principals (persons, organizations, devices, machines, systems, applications, components, etc.) directly and indirectly involved in patient care. In that context, the identification of patients, healthcare professionals, but also non-human actors like healthcare institutions, individual computer servers and other devices must be managed. Corresponding application security services, such as credentialing, privilege management, user management, role management, authorization, role-based access control, and audit are basic requirements. For achieving the main security objectives, advanced security services represent the most important challenge. These services include other communication security and application security services guaranteeing security, privacy, safety, and quality of data, processes and results beyond the aforementioned identification and authentication of any principal. The risk analysis results should be used in design and implementation of the security infrastructure components in systems, computer networks, as well as in the security management tools and rules.

Different means to efficient system security range from organizational working rules and instructions for physical protection of computing accessories and data storage, through organizational (e.g. hospital) computer network protection from outer Internet attackers causing denials of service or remote misuse of known software bugs. These threats are lowered by firewall systems or network address translation. Related technologies are *secure sockets layer* (SSL) or *virtual private networks* (VPN), encrypting information content, and thus eliminating its “wiretapping“. Next security level should secure computers themselves against viruses, malware and spyware using regular operation system and antivirus updates. E-mail spam filters and attachment blocking techniques also hamper tries to reach sensitive data using

social engineering (phishing, pharming).

A. Application Protection

The protection of biomedical applications and systems should apply authorization management system to assign access rights to users and user groups or profiles (e.g. physicians, nurses, etc., as well as software components or different devices). When assigning rights, the national healthcare data protection legislation has to be respected – e.g. when passing data among healthcare providers. The selected user authentication method influences the quality of system security. Username and password systems or integrated authentication (e.g. based on Kerberos/Active Directory) are not satisfactory for all cases. Stronger level can be reached using biometric systems like fingerprint or retina exploration, as well as smart card identification, or their combinations. The way of authentication of connections to remote computer systems is another worthwhile consideration.

Audit logs recording exceptions and other security-relevant events can be produced and kept for a period to assist in future investigations and access control monitoring. Even the secured system should log access attempts to different system functionality in order to document the possibly problematic situations in future. Logs of user activities can be maintained and regularly, independently checked. Faults should be reported as soon as possible and corrective actions taken.

All the applications and systems should be reviewed and tested after implementation and again later, when any software changes occur.

In design, implementation or investing in a software system, care must be taken, when software components from third parties are used. In the absence of support or source code of such components, the potentially existing vulnerabilities and errors might be hard or almost impossible to eliminate and maintainability of such a system, hence also future reliability, might be strongly influenced, as well. Moreover such components should be tested against undesirable channels and Trojan code.

B. Data Protection

Data should be validated on input to software applications to ensure that it is correct and appropriate. Additional validation checks can be incorporated into applications to detect any corruption of the data processed.

Physical separation of stored administrative data like name and address from medical data such as diagnoses helps to protect data from undesired access to the combination and it may be required as a legal requirement in electronic healthcare record (EHR) systems.

Back-up copies of essential healthcare information and software have to be taken and tested regularly. The management of removable computer media, (tapes, flash disks, cassettes etc.) may be controlled and sensitive media should be disposed of securely. Procedures for information handling and storage should be established in order to protect the information from unauthorized use. Moreover, system documentation may need to be protected from unauthorized access.

C. Network Protection

Network encryption should be applied to protect the confidentiality of sensitive or critical information during their transport over vulnerable networks. In addition, digital signatures can be applied to protect the authenticity and integrity of electronic information.

In larger systems like complex hospital systems and their networks, groups of information services, users and information systems can be intentionally segregated in separate networks in order to minimize the security risk. That network segregation can be guaranteed by the mean of isolation devices, such as firewalls.

VI. CONCLUSIONS

This work has shown an overview of the elementary security and reliability requirements and methods in distributed healthcare systems.

Other methods and approaches can be found in a variety of papers and books on security in software systems in general, as well as in the healthcare domain. The suggested further reading is [1] on data and system security, as well as security and confidentiality requirements in management of information in integrated delivery networks, [2] on security and confidentiality in use of electronic medical records, [3] on secure web-based healthcare applications and secure internet access to medical data, and [4] describing the security component of a clinical information system.

VII. ACKNOWLEDGEMENT

The acknowledgement goes to the management of the K4Care project [5], which enabled to compile this article in close connection with the electronic healthcare record-related research.

VIII. REFERENCES

[1] E.H. Shortliffe and L. Perreault (eds), G. Wiederhold and L. M. Fagan (assoc. eds.), *Medical Informatics: Computer Applications in Health Care and Biomedicine, Second Edition*, New York, NY: Springer-Verlag, 2001.

[2] J. H. Carter (ed.), *Electronic Medical Records: A Guide for Clinicians and Administrators*, Philadelphia, PA: American College of Physicians, 2001.

[3] R. Grutter (ed.), *Knowledge Media in Healthcare: Opportunities and Challenges*. Hershey, PA: Idea Group Publishing, 2002.

[4] R. Van de Velde and P. Degoulet, *Clinical Information Systems: A Component-Based Approach*, New York, NY: Springer-Verlag, 2003.

[5] D. Riaño et al., *K4CARE: Knowledge-Based HomeCare eServices for an Ageing Europe*, available online: http://www.k4care.net/fileadmin/k4care/public_website/downloads/k4c_Factsheet.pdf, accessed in 2008.