MediTrust: Secure Client Systems for Healthcare IT to Protect Sensitive Data of Patients

Ammar Alkassar[1], Biljana Cubaleska[2], Hans Löhr[2], Ahmad-Reza Sadeghi[2], Christian Stüble[1], Marcel Winandy[2]

[1]Sirrix AG security technologies, Bochum, Germany
a.alkassar@sirrix.com, c.stueble@sirrix.com

[2] Ruhr-University Bochum, Germany
{biljana.cubaleska,hans.loehr,ahmad.sadeghi,marcel.winandy}@trust.rub.de

Abstract: **Healthcare professionals typically use their computer systems not only for accessing patient health records, but also to connect to medical accounting and billing services as well as other services on the Internet. This raises security and privacy concerns as client platforms may be infected by malware and could manipulate data or leak data to unauthorized parties. The project MediTrust aims to protect medical data of patients from being leaked to unauthorized parties. We propose a security infrastructure that builds privacy protection domains and enforces them up to the end-user platforms. Usability and effectiveness of the security mechanisms will be evaluated in user studies.**

I. INTRODUCTION

The use of information technology in healthcare enables new and efficient applications like immediate access to and automatic analysis of medical data. E-health systems like electronic health records (EHRs) are believed to decrease costs in healthcare. However, the increasing use of digital medical data and computing systems operating on these data pose new risks with respect to security and privacy. Health professionals, like doctors and nurses, are not trained security experts, but they use standard computing platforms for various tasks, including accessing privacy-sensitive medical data of patients. These platforms may be vulnerable to malicious software, e.g., Trojan horses. In this context, analyses of e-health infrastructures show that the end-user systems are the least secured part [1].

II. PROJECT GOALS AND APPLICATION SCENARIO

The objective of MediTrust is to develop a usable and secure end-user platform that is able to protect sensitive medical data from being accessed or manipulated by unauthorized parties. We define the following goals:

- protecting medical data that are processed on the same computing platform together with other tasks;

- establishing a security infrastructure that securely separates the data of different workflows;
- providing a usable and user-friendly end-user platform that does not impose an overhead in the normal workflow of health professionals.

We consider a scenario where a doctor's practice uses a computer system to process electronic health records of patients that are stored on a centrally managed server (EHR Server). The same computer system is used to send accounting and billing data to a Healthcare Accounting & Billing Server, and the computer is also used to connect to other services, e.g., web sites on the Internet. We propose to construct privacy domains for medical data as a technical measure to support the enforcement of privacy and data protection policies (see Figure 1). The client platforms, e.g., desktop or notebook computers, must be able to partition execution environments for applications into separate domains that are isolated from each other. Data is kept within a privacy domain, and the domain infrastructure ensures that only authorized entities can join this domain [2]. Moreover, data leakage from the domain is prevented by the security architecture and the domain infrastructure. The same system should be able to be used for different workflows that are strictly isolated. Therefore, the focus of MediTrust is on the development of secure client platforms that can be used not only for accessing sensitive health records and associated accounting data securely, but also support standard operating systems and applications which are strictly isolated from the sensitive data and the healthcare client software.

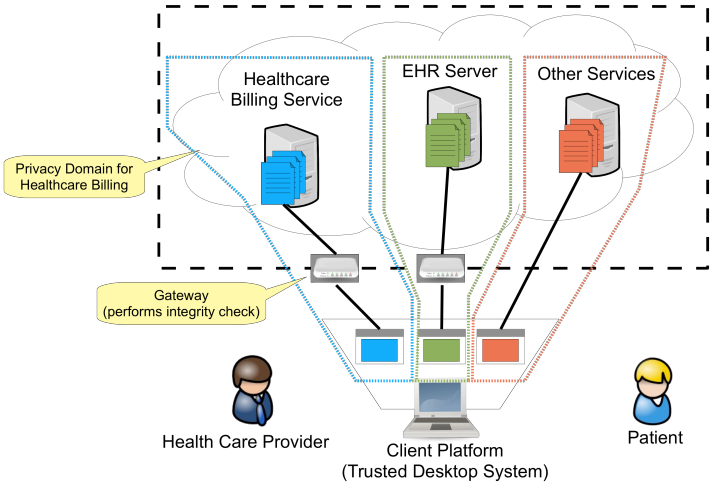

Figure 0: Conceptual view of privacy domains in MediTrust

III. TECHNOLOGY

The technical solution of MediTrust is based on the TURAYA security platform [3][4]. TURAYA implements a trusted desktop that is based on strong isolation of critical applications and the reliable enforcement of security policies. The underlying security architecture enables a comprehensive and auditable protection of all user data.

TURAYA.TrustedDesktop consists of a security kernel that provides isolated execution environments (which we call compartments) for applications. The security kernel virtualizes the legacy operating system on the client and enables multiple operating systems running concurrently and isolated in different compartments. Communication between compartments is controlled and enforced according to an information flow policy. Therefore, each compartment is associated to a Trusted Virtual Domain (TVD) [3], which spans a closed virtual processing area across multiple platforms. Data leaving a compartment is automatically encrypted and can only be accessed in a compartment that belongs to the same TVD, whether the compartment is on the same machine or on a different physical platform.

The system also ensures that protected information is only processed by trusted components. This is made possible by security kernel technology along with the employment of Trusted Computing technology. The client platform contains a trusted hardware component, the Trusted Platform Module (TPM), which can be used for the verification of the integrity of the software running on the machine.

TURAYA.TrustedDesktop provides the following main security features, which are used to protect medical data from other workflows:

- **Full hard-disk encryption**, sealed to the TPM security chip. The encryption key is never revealed to the operating system of a compartment and, thus, a malicious compartment (e.g., infected by a virus) cannot leak or change sensitive key material.
- **Secure networking**. The TURAYA security kernel enables secure links between compartments according to the TVD policy, and automatically manages dedicated virtual private network (VPN) encryption.
- **Transparent file encryption**. Instead of banning portable storage devices like USB sticks and external hard-disks, TURAYA transparently encrypts data leaving a compartment and restricts the access to other compartments of the same TVD. Thus, it provides offline transport capabilities for exchanged data, e.g., when electronic health records are stored on USB sticks.

- **Secure graphical user interface**. The user interface system supports the different TVDs graphically so that users always know which domain they are currently interacting with. Each compartment has its own virtual screen, which ensures isolation and prevents unintended information flow from one compartment to another without being allowed by the TVD policy. The virtual screens of the compartments are graphically marked with a color and short textual name. Each TVD is assigned a distinct color and name to allow the user to distinguish the different domains. The graphical security information is always under the control of the TURAYA security kernel and shown at the top bar of the screen, which cannot be overwritten by compartments.

IV. Outlook

We will conduct an intensive field study in real life settings with about 20 users (doctors). We aim to analyze whether the concept of TVDs and corresponding graphical security indicators are properly understood by ordinary users. Moreover, we want to find out whether the system is used correctly (i.e., users do not enter sensitive data into the wrong domain), can be used efficiently (i.e., it does not introduce additional delay in the workflow of the users), and if the screen design approach is sufficient or other security indicators are needed. Potential users of such a system would be over 325,000 physicians in Germany [5], and could be useful in other countries and scenarios as well, e.g., government and enterprises.

V. Acknowledgment

This work was partially funded by the German federal state North Rhine-Westphalia and supported by the European Regional Development Fund under the project RUBTrust/MediTrust [6].

References

[1] A. Sunyaev, A. Kaletsch, C. Mauro, and H. Krcmar. Security analysis of the german electronic health card's peripheral parts. In *ICEIS 2009 - Proceedings of the 11th International Conference on Enterprise Information Systems*, pp. 19–26, 2009.

[2] H. Löhr, A.-R. Sadeghi, M. Winandy. Securing the E-Health Cloud. *Proceedings of the 1st ACM International Health Informatics Symposium (IHI 2010),* ACM, 2010.

[3] L. Catuogno, H. Löhr, M. Manulis, A.-R. Sadeghi, C. Stüble, M. Winandy. Trusted Virtual Domains: Color Your Network. *Datenschutz und Datensicherheit (DuD)* 5/2010, pp. 289-298.

[4] Sirrix AG security technologies. TURAYA Trusted Infrastructure. Online at http://www.sirrix.com/content/pages/50580.htm

[5] Bundesärztekammer. Die ärztliche Versorgung in der Bundesrepublik Deutschland. http://www.bundesaerztekammer.de/page.asp?his=0.3.8175.8176, December 2009.

[6] RUBTrust/MediTrust project website. http://www.rubtrust-meditrust.de