2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)

Security Aspects of e-Health Systems Migration to the Cloud

Antonis Michalas
Security Lab
Swedish Institute of Computer Science
Stockholm, Sweden
antonis@sics.se

Nicolae Paladi
Security Lab
Swedish Institute of Computer Science
& Lund University, Sweden
nicolae@sics.se

Christian Gehrmann
Security Lab
Swedish Institute of Computer Science
Stockholm, Sweden
chrisg@sics.se

***Abstract*—As adoption of e-health solutions advances, new computing paradigms – such as cloud computing – bring the potential to improve efficiency in managing medical health records and help reduce costs. However, these opportunities introduce new security risks which can not be ignored. Based on our experience with deploying part of the Swedish electronic health records management system in an infrastructure cloud, we make an overview of major requirements that must be considered when migrating e-health systems to the cloud. Furthermore, we describe in-depth a new attack vector inherent to cloud deployments and present a novel data confidentiality and integrity protection mechanism for infrastructure clouds. This contribution aims to encourage exchange of best practices and lessons learned in migrating public e-health systems to the cloud.**

***Index Terms*—e-Health, Security; Cloud Computing; EHR Protection; Storage Protection**

I. Introduction

Visions of an electronic healthcare system are more than twenty years old. Researchers aimed for a paperless medical system where patients and doctors are able to book appointments via the Internet, create electronic prescriptions and store their medical history in a central database, easily accessible from anyone with appropriate access rights.

During these years, there has been a steady increase in research focus and funding aiming to modernize existing healthcare systems and provide reliable and cost effective e-health services. Both private organizations, such as Microsoft, Google and IBM, and public administration bodies have taken steps towards e-health. For example, president of the United States B. Obama, approved $38 billion to digitize the American health care and believes that at the end of 2014 the nation's health records will be fully computerized. In addition, the Australian government invested $20.3 million in "telehealth" projects, Tasmania committed $1.8 million in order to update the information systems responsible for four of its public hospitals, while Germany has introduced the electronic health card [1] – a challenging mission in which all insured Germans received a smart card with which they can securely communicate with various healthcare stakeholders (doctors, hospitals, pharmacies etc) by means of telematics.

Based on the advancements in e-health research and development, analysts believe that in the near future the modernization of existing healthcare systems will lead to a wide adoption of electronic health records (EHRs) [2]. More precisely, it is expected that scientists and doctors will collect more data about the human body and individual patients than they have done in all of history so far. There is no doubt that are many barriers to that: besides addressing usability issues, e-health system vendors need to attract user attention and convince them that e-health systems are reliable, secure and will have tangible positive impacts on the day-to-day healthcare experience.

Healthcare has been slow to adopt IT, especially when compared to other sectors like banking where customer information is also sacrosanct. Among the most important reasons for the slow adoption of e-health services is the fear of storing sensitive data online. Without proper security mechanisms to protect user data from unauthorized access, sensitive information may leak to interested, unauthorized third parties, such as insurance companies or potential employers. "It's not about being scared of technology; it's about the appropriate safeguards," says Marc Rotenberg, executive director of the Electronic Privacy Information Center [3].

Despite the relatively slow adoption of IT in the healthcare industry, the medical community gradually advances towards wider adoption of electronic healthcare. New computing technologies, such as cloud computing, fit squarely into this evolution. Cloud based e-health services could bring significant benefits [4]–[6]. Patients would be able to "carry" their whole medical history everywhere preventing duplicate tests. Doctors would have the option to share healthcare data across various settings and geographies, avoiding delays in treatment and unnecessary confusion. Cloud computing technologies allow healthcare organizations to improve services to their customers – the patients – to share information easier than ever before, and improve operational efficiency. Finally, cloud computing can reduce e-health expenses, such as hardware, software, networking, personnel and licensing fees [6]. However, along with the improvements in service availability, scalability as well as operational savings, migration of electronic records system to fully virtualized environments also introduces additional security risks.

A. Contribution

Our contribution in this paper is three-fold. First, we describe "Melior", an electronic patient records system developed by Siemens Healthcare and used by several Swedish regional administrations in order to manage patient data.

Second, we present a list of core security requirements that must be considered when migrating e-health systems to

978-1-4799-6644-8/14/$31.00 ©2014 IEEE

an IaaS cloud environment. These security requirements were derived based on our experience with migrating "Melior" to a private IaaS cloud. We discuss an important attack vector characteristic for IaaS clouds, namely the virtual machine (VM) image management process and propose techniques in order to provide tighter security when building cloud services.

Finally, we address the problem of weak security guarantees for data generated by e-health applications in IaaS clouds. We present a storage protection protocol which improves confidentiality and integrity protection of the medical records in IaaS clouds, without affecting the data access functionality.

B. Organization

In Section II, we present an electronic patient records system that is used in a few major Swedish County Councils in order to manage medical data of patients. In Section III, we analyse the core set of requirements for a successful migration of an e-health application to the cloud, while in Section IV we discuss in depth one of the common security risks related to migration to the cloud. In Section V, we describe a protocol that ensures the protection of EHRs in the cloud and in Section VI we conclude the paper.

II. System Description

Region Skåne is a regional public body in Sweden, providing and managing public services – including healthcare services – for a population of approximatively 1.25 million inhabitants. Healthcare services in the region rely on a large set of information systems with varying levels of interoperability and intricate interdependencies. For this case study, we have chosen an electronic patient records system from Siemens Healthcare called "Melior", mainly due to its relatively low number of dependencies, manageable size and support availability [7]. "Melior" is one of the most widely used medical journalling systems in Sweden. Its development started in 1990 and it is now used at 46,6% of the hospitals, with a total of about 80,000 users[1]. Below, we briefly describe its functionality and the important characteristics of the system's environment.

A. Functionality

"Melior" provides functionality necessary for process administration in public healthcare. In particular, "Melior" supports patient administration, clinical documentation management and medical prescriptions management. The output of "Melior" includes issuing nutrition cards and medical investigation referrals as well as relevant letters and certificates.

B. Preliminaries

Currently "Melior" is deployed on hardware servers in one of the data centres located in the region, along with other healthcare information systems used by the Region Skåne. Besides the necessary functionality provided by "Melior", the essential non-functional requirements are: *(i)* high availability, *(ii)* high reliability, *(iii)* guaranteed data preservation.

"Melior" operates with medical records that carry important information with direct effect on the health of the patients in the region. As a result, the system must be available at all times and operates under strict requirements specified the service level agreement (SLA)[2] by the administration of Region Skåne. For example, the SLA with the outsourcing service operations partner of "Melior" assumes a 99,82% uptime throughout a year.

C. User patterns

Live "Melior" deployment in Region Skåne has currently up to 6,000 concurrent users. During daytime the average is around 5,000 concurrent users and 1,500 users during non-business hours (i.e 5*pm* to 7*am*). It is expected that in 5 years the deployment will host approximately 8,000 concurrent users during peak hours (i.e 9*am*, 2*pm* and 5*pm*).

D. Components overview

On a higher level, the current "Melior" deployment in Region Skåne can be described as a set of services deployed on separate load-balanced clusters. Figure 1 depicts the client and server side of the deployment, as well as interactions between them. The server-side consists of the application layer with a set of essential "Melior" services accepting client connections and a data layer containing data storage.

These components will be addressed below.

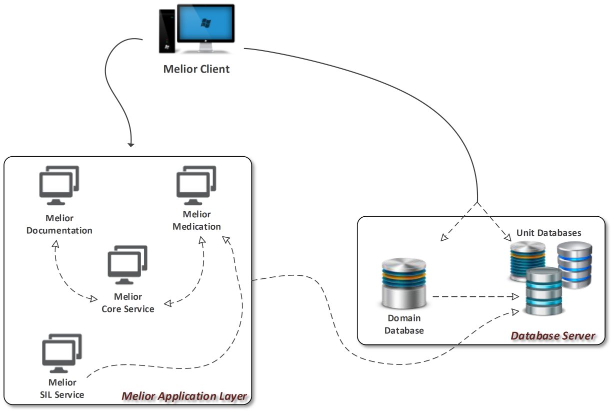

Fig. 1. Components of "Melior".

1) "Melior" client: Users interact with "Melior" by means of a Microsoft Windows-based application that runs on personal workstations and communicates with the "Melior" core (described below) through protected network channels. Security of the communication channels between the "Melior" client and the rest of the system is provided by the deployment environment.

2) "Melior" core: Processing and storage of medical records is performed in the "Melior" core. In a simple deployment scenario, it represents the interplay of three services: the *front-end service*, the *back-end service* and the *data store*.

[1] Webpage of Siemens Melior: http://www.nwe.siemens.com/sweden/internet/se/healthcare/it-losningar/melior/pages/melior.aspx

[2] SLA is an agreement between two or more parties, the customer and the service provider(s). SLA can be seen as a contract between a customer and a service provider in which the latter provides some level of assurance regarding the provided service (*e.g* availability, liability, security etc.). For more information about SLAs we refer the reader to [8].

3) External dependencies: In order to support its full functionality, “Melior” is integrated with a range of external services, both on the client and on the server side. Integration with external services on the server side is aggregated in the integration layer, by application layer or data layer. Integrations serve to both push and retrieve data relevant for the “Melior” users and ensures interoperability of the systems used in daily medical care.

E. Deployment overview

Next, we provide some details about the current deployment of the components of “Melior” described above.

1) Application services: “Melior” is flexible enough to operate with core services deployed on one or multiple servers, depending on the SLA requirements. In the current deployment scenario, multiple instances of the “Melior” core services run in parallel on different physical servers, in order to satisfy the availability requirements of the SLA. Similarly, the services are *load-balanced* in order to ensure optimal performance under peak load times.

2) Data storage: “Melior” consist of at least two databases, one Domain database and one or more unit databases. The Domain database stores information regarding authorization, clinics, departments, process and terminology. Unit databases maintain medical records stored in tables and accessed for both mutating and non-mutating operations. The data layer is divided into 4 separate domains with a total of 26 databases holding approximatively 4 TB of data, typically images and text files. Three core operation principles are relevant in this deployment:

- All data should be equally available at all times
- No data shall be obsoleted
- No data shall be deleted

Typical operations on the data are: `INSERT`, `UPDATE` and `DELETE`. However, in the case of the `DELETE` operation, data is not actually discarded but rather “hidden” from the user. No data is permanently stored on the client side; versioning history is not kept for data maintained in the data store.

III. Requirements

There is a number of steps for a successful transition from traditional architecture to a cloud architecture. In this section, we highlight some essential steps for moving an e-health system to the cloud. We use this analysis to guide us in the development of our cloud environment and we hope that it will provide essential knowledge to organizations that wish to migrate their EHR systems to the cloud and minimize project and security risks by avoiding common pitfalls.

Security: When building cloud services, one of the biggest areas to focus on is security. The externalized aspect of outsourcing can make it harder to maintain data integrity and privacy [9] and organizations should include mechanisms to mitigate security risks introduced by virtualization. Especially when they deal with sensitive data, such as EHRs, protection of stored information comes as a top priority. Therefore, data security can be seen as the foundation upon which the whole e-health initiative should be based on. Multiple risks must be addressed in order for an organization to guarantee the safety of personal health records. One of the most important aspects is security of sensitive information. To this end, the deployment must ensure that all patient data is stored in encrypted form. Complementary to this, proper key management must ensure encryption keys are not revealed to malicious users.

Following the migration of e-health systems to the cloud, users have the option to store, organize, share, and access sensitive medical information from almost anywhere and any device, including public computers. Thus, strong authentication protocols must to be deployed in order to prevent impersonation of authorized users. In addition, patients are able to make their medical history partly of fully available to doctors when needed. Even though the shared information should be provided in an efficient and timely manner, it is essential to ensure its privacy. Additionally, users must have full control of the information they share, control the access rights and see viewing history.

Integrity is another aspect of data security relevant in this context. Considering that information in the EHRs has an important impact on the individual healthcare process, it is essential that EHRs are not altered or deleted without proper authorization.

Availability: One of the key arguments when migrating an e-health system to a cloud platform is availability. Organizations must thoroughly analyse and understand the impacts on performance and availability and must take actions in order to be able to provide resources for the highest possible load. The risk of systems unavailability in e-health industry is a major issue since there are many cases where healthcare providers are unable to operate if their applications and/or patient's data are not accessible. Even though cloud services could experience failures due to software and hardware faults, network faults or even natural disasters [10] cloud providers must ensure that services will be available to end users. To do this, organizations must plan on disaster scenarios in order to improve the redundancy and reliability of their systems. Thus, it is necessary to apply known safety best-practices and enable replication between multiple geographical locations to prevent data loss in case of disasters.

Scalability: Cloud based e-health systems needs to be designed in such a way that will take advantage of the rapid scalability and deployment capabilities that cloud computing offers. In such environments scalability can be defined as “the ability of a computing system to grow relatively easily in response to increased demand” [11]. In other words, relying on IaaS clouds, e-health services are able to augment on demand existing resources in order to accommodate sudden increases in requests, or scale down when the load is low – without incurring additional capital expenses.

Regulatory Compliance: By storing data in the cloud, users hand it over to a provider that may have data centres in different geographical locations, countries or even continents. However, organizations that work with sensitive data, such as health records, require complete control over the physical storage location and data access. As a result, storing sensitive data in the cloud complicates adherence to regulatory compliance laws, since such data may fall under different regulations depending on where it is physically stored. If for example data is moved to a different country, a set of different regulatory requirements may apply. Thus, prior to storing and processing data through the cloud, organizations must take into consideration the legal issues in order to ensure that users are in legal compliance [12].

Cost: A core benefit of cloud migration is the potential for cost savings. By migrating an e-health platform to the cloud, organizations can get powerful functionality in the most cost effective manner. Cloud migration can help organizations reduce the need for IT teams to operate and maintain expensive internal infrastructure, reduce maintenance costs, shed at least some of their expensive IT infrastructure and shift computing costs to more manageable operational expenses. Nonetheless, if the transition is not planned carefully, it can lead to disappointing results. While a plethora of solutions is available, many of them are not able to meet the specific needs of an e-health system. Thus, a cloud solution that will not attain the above mentioned criteria can have catastrophic results for the migration of an e-health system to IaaS clouds.

IV. Cloud-specific security aspects for e-health systems: the case of VM image management

While migrating systems to a cloud infrastructure, certain security risks characteristic to cloud computing become especially acute in the case of e-health systems. The reason is the inherently sensitive information collected, stored and processed by such systems. In our experience with migration of “Melior” to an IaaS cloud deployment, improper management of VM images with installed components and databases can not only lead to data losses and version compatibility issues, but is also a potential attack vector. Below we discuss the security risks introduced by the VM image management process and propose a set of procedures to mitigate such risks.

A. VM images as an attack vector

VM image management is a relatively new aspect of information security management, present in IaaS clouds. Long-term operation of an IaaS cloud leads to an eventual build-up of ancillary data produced by the cloud platform, such as logs, data backups, configuration backups and snapshots of virtual machine images. While all of the above mentioned data streams may contain sensitive information and thus require structured and systematic management, VM images may be *instantiated* at an arbitrary point in the future and become part of the IaaS cloud. From a security point of view, the use of diverse sources of VM instantiation bloats the security perimeter of the deployment, potentially allowing creation of VM images with old, unpatched operating system and application-level software. On the other hand, the composition of different versions of operating systems and applications may in itself create new vulnerabilities not present in individual components. This is valid in general for IaaS clouds and is aggravated by the complex architecture of e-health applications. As described in Section III, such applications usually have much more stringent requirements with respect to identity management and data protection than typical cloud-based applications. Consider the example of “Melior”: deployment of *most* of the system components requires that an additional set of ports (beyond the so-called “well-known ports”) is opened on the virtual servers hosting some of the servers. In case when each component (such as front-end, back-end and database server) is deployed on a separate virtual server, a tendency is to first configure a “master” VM image with opened additional ports and *next* deploy the components on clones of the VM image. However, this process leads to a situation when even the components that do not require additional ports (e.g. the database server) will be deployed in a VM instance with unneeded open ports, unnecessarily increasing the attack surface.

Early research efforts to address this issue focused on image management [13] in cloud environments that allow image sharing and designed mechanisms to create image sources and verify images prior to instantiation. Later, research in [14] demonstrated a range of serious vulnerabilities found in public VM images available in the Amazon Web Service cloud platform. The suggestions provided by the authors are organizational measures, automated tools to manage the image publishing process, regular scanning of the images and improvement of the image store. This important building block for a secure VM image management process must also be applied in the case of e-health systems and would prevent the problem described above in the context of “Melior” deployment in an IaaS cloud.

B. The way forward

Based on the security requirements outlined in collaboration with Region Skåne as well as current best practices and our experience with the transfer of “Melior” to a fully virtualized IaaS cloud, we present the following VM image management process for cloud-based e-health systems (Fig. 3). We will map the below process to the steps that were taken in the migration of “Melior” to an IaaS deployment.

1) Image creation: For e-health system deployments and other security-critical applications, security of virtual machine images is one of the cornerstones to ensuring data confidentiality. We propose the following principles for the creation of tailored VM images for e-health applications:

- *Trusted source of the operating system (OS).* As an initial bootstrap step, the OS images are obtained from a valid source through a protected, authenticated channel. The integrity of the obtained images is verified by comparing their hashes with the respective hashes provided by the OS vendor.
- *Thorough hardening of the OS according to organization policies and best practices.* The default configuration of the OS is modified to e.g. reduce application attack surface, install the target e-health application, enable mandatory access policies, exclude redundant remote access channels, etc.
- *Traceability of the VM image creation process.* The VM image creation process is automated and made traceable and consistent with the applicable security policies. Deviation from the established VM image creation process is regarded as a security vulnerability and leads to discarding the created VM image.

When migrating “Melior” to an IaaS cloud, this meant obtaining the operating system directly from the vendor’s authenticated web-site using SSL. In addition, the integrity of the VM image was corroborated with the one presented by the

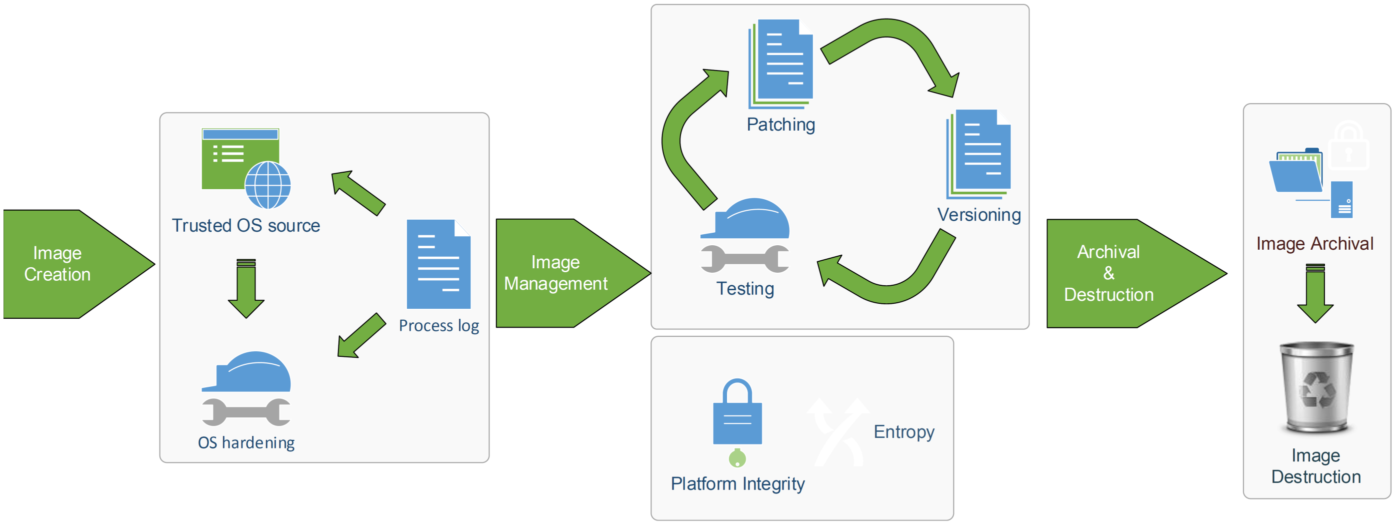

Fig. 2. VM image management process

vendor. Next, the images were hardened by removing unnecessary components and only leaving open the ports required by the components of "Melior". One master image was tailored for each type of components of "Melior": front-end, back-end and database server. The types, licence keys and descriptions of VM images were documented in order to provide traceability.

2) Image and snapshot management: Most of the ancillary information produced by the cloud platform is created during the active use of the VM images. In this context, "active use" starts from the moment when an image was created and made available for instantiation, to its archival combined with destruction of all instances created from it. The following principles are relevant for this stage.

Centralized, traceable and reproducible VM image patch service and image version control and compatibility testing. Both security patching and the resulting versioning of VM images is managed in a centralized manner to prevent version inconsistencies. Considering the combined complexity of the operating system and e-health system software stacks and the rapid changes in the combinations of VM image and e-health application versions, automated security tests are necessary when patches are applied to any component in the deployment.

Security services for VM instances. During regular operation, VM instances may benefit from additional security services. One example is launch on verified platforms [15], to ensure that the VM instance runs on a host which has not been compromised. Another such example is providing instances with high quality pool of entropy, which is needed for cryptographic operations performed on the VM image to confidentiality and integrity protect the e-health data processed by the instance. Entropy starvation could lead to both decreased security [16] and poor performance of the VM instance.

During the prototype migration of "Melior" to an IaaS cloud, we relied on versioning the VM images in order to clearly trace the changes to functionality and configuration that have been made to VM images between any two snapshots.

3) Image archival and destruction: The life cycle of a VM image ends with its (optional) archival and eventual destruction, depending on the relevant organizational policies. If VM image archival is applicable, the archived images used in the e-health deployment are encrypted and assigned the highest information sensitivity classification available in the context of the e-health application. The reason for this is that such images are likely to contain *aggregated* traces of medical record information which could be misused by adversaries.

Destruction of VM images is the final step of the proposed VM image management process. In a survey of secure data deletion techniques, the authors provide a taxonomy of secure data deletion techniques analysed by the target adversary, integration level, granularity, scope and efficiency [17]. Deletion of VM image files takes into consideration the above aspects when choosing the deletion approach. In the context of IaaS clouds however, e-health system users ensure that the cloud provider has followed the suitable deletion approach.

Similarly, in the case of "Melior", special attention must be paid to protection and when needed guaranteed deletion of the database VM image. VM images with other components – the front-end and back-end components – also require careful deletion when discarded, as they may contain session keys and cached data that have the potential to affect confidentiality and integrity of the EHRs.

V. Storage Protection

One of the key benefits that cloud based solutions can provide to the e-health systems is the ability to share information, such as EHRs, between different organizations and information systems that may be located in different countries. Nevertheless, storing confidential health data in the cloud rises many security challenges. With personal medical information in hand, corrupted users are able to commit medical identity theft by impersonating other users in order to receive goods or services, potentially wreaking havoc on the victim's records and creating liabilities for service providers and increasing costs for everyone. Thus, healthcare organizations must provide strong security mechanisms that will prevent unauthorized users from accessing sensitive data.

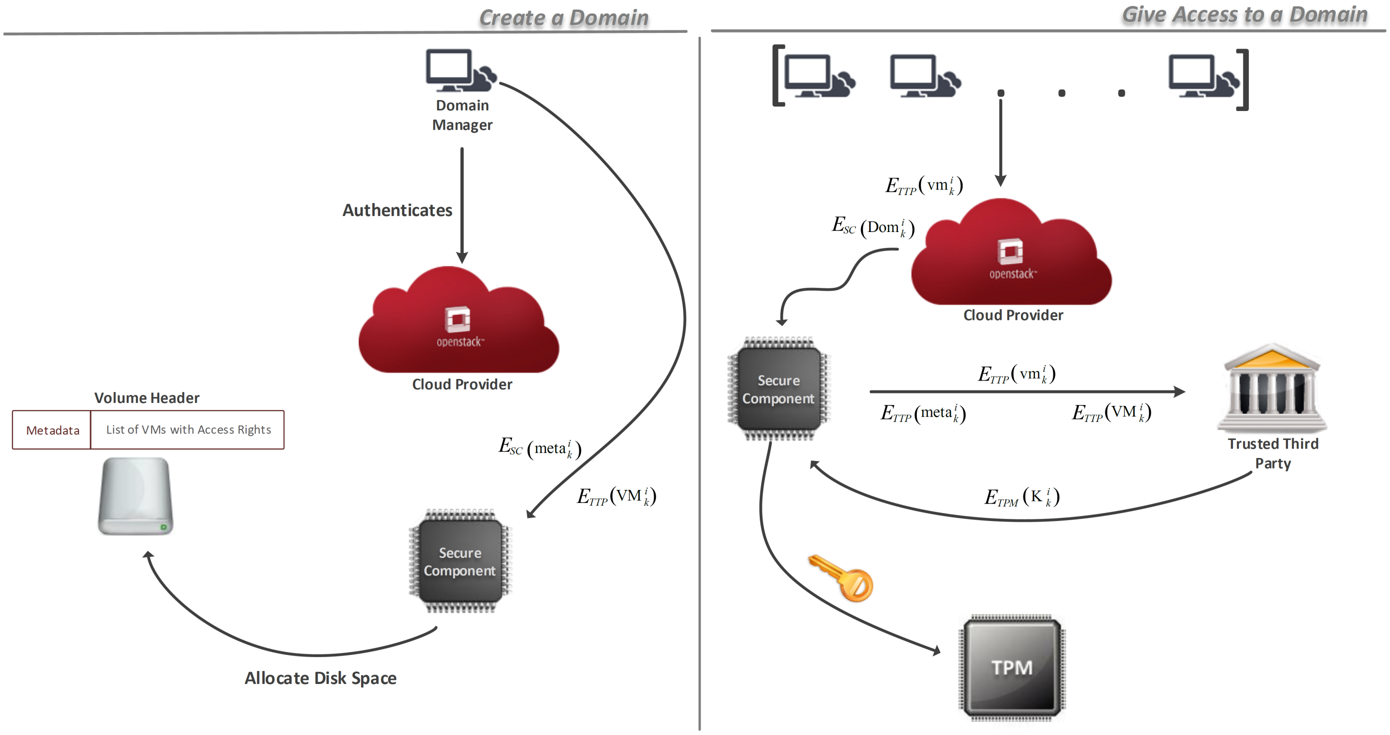

Fig. 3. Secure Storage – Protocol Overview

In the rest of this section we provide a high level description of a protocol that was implemented for the needs of "Melior" and provides mechanisms for securely storing and sharing medical data in an e-health cloud platform.

Our protocol consists of a cloud platform (CP), virtual machines (VM), a trusted third party (TTP), a secure component (SC) and domain managers (d). Furthermore, we assume that basic functionality normally provided by a CP, such as registration and authentication of a user, is available. Similar to [18], domain managers can launch new VM instances, which can in turn create data and securely share it with other VM instances *both within the same and other IaaS clouds*. The proposed protocol also relies on the principles of trusted computing and capabilities of the Trusted Platform Module (TPM) [19].

For the needs of our protocol, we assume that the reader is familiar with the concept of public cryptography and that each party has generated a public/private key pair (pk/sk). The private key is kept secret while the public key is shared with the rest of the community. We assume that during the initialization phase, each entity obtains a certificate via the certification authority provided by the CP. These keys and certificates will be used to protect internal message exchanges and hence the communication between the parties assumed to be secure. Finally, our protocol relies on pseudorandom functions [20] to create symmetric keys, a major tool for the design of shared key cryptography protocols.

Domain managers can create different categories of data. Each category is referred to as a domain that contains encrypted data. Additionally, domain managers are able to share this data by giving access to the corresponding domains to certain VMs in the cloud, as well as to other domain managers within the same or other IaaS clouds.

Consider the following scenario. A domain manager d_i that manages a set of n VM instances ($VM_i = \{vm_1^i, \ldots, vm_n^i\}$) wishes to create a new domain Dom_k^i and share it with a set VM_i^k of VMs such that $VM_i^k \subseteq VM_i$. To this end, d_i first authenticates to the CP and requests the generation of the domain Dom_k^i. With the request for the generation of Dom_k^i, d_i also provides a list of VM instances belonging to the set VM_i that should have access to the specified domain, as well as the respective access rights. Furthermore, d_i provides a description of the data that Dom_k^i will store; we call this description as the metadata ($meta_k^i$) of Dom_k^i. Then, CP is responsible for creating Dom_k^i. This is done by allocating the corresponding disk space and by adding domain information in the header of the volume – CP adds $meta_k^i$ and an XML file that contains the list of the VMs that can access Dom_k^i along with their privileges.

Once Dom_k^i has been generated, any VM from VM_i^k can access the domain. Assume $vm_k^i \in VM_i^k$ wishes to access Dom_k^i. To do so, SC must retrieve from TTP the symmetric key (K_k^i) that will be used to confidentiality protect data in Dom_k^i. The domain manager operating vm_k^i sends a request to CP in order to mount Dom_k^i to the virtual machine instance; the call is forwarded to and processed by SC.

In the request, d_i sends a credential that proves that vm_k^i has access to Dom_k^i. SC extracts from the header of the domain Dom_k^i the metadata and the list VM_i^k and sends it to the TTP along with the unique identifier of vm_k^i. More precisely, the message is encrypted with the public key of TTP and is of the form $\langle E_{TTP}\left(meta_k^i\right), E_{TTP}\left(VM_i^k\right), E_{TTP}\left(vm_k^i\right)\rangle$. Upon reception, TTP finds the *id* of the VM that requests access by decrypting $E_{TTP}\left(vm_k^i\right)$. Then, decrypts the list with the VMs that can access Dom_k^i and checks if vm_k^i exists. If so, TTP needs to generate a symmetric key[3] that will be used to encrypt data in Dom_k^i. To create the encryption key K_k^i, generates a random nonce r_k and uses a pseudorandom function (PRF) [20] to calculate the following:

$$K_k^i = PRF\left(meta_k^i \| r_k, K_{TTP}\right),$$

where $meta_k^i \| r_k$ is respectively the concatenation of metadata and the random generated nonce, and K_{TTP} is a master key that is only known to the TTP. After generating the symmetric key for Dom_k^i, TTP encrypts it with the public key of TPM and sends it to the SC. Upon reception, SC, is responsible for forwarding it to the TPM. TPM, first checks if the state of the vm_k^i remains trusted. If so, it reveals K_k^i and SC uses it as input to the disk encryption subsystem on the compute host where vm_k^i is running. The disk encryption subsystem seamlessly decrypts the mounted volume hosting Dom_k^i. Next, the volume containing Dom_k^i is mounted as a disk device on vm_k^i, with read-write or read-only rights, depending on the permissions granted by the d_i.

Due to space limitations, we only described the case where a domain manager shares data with virtual machines in the same cloud. However, the protocol allows data sharing organizations that run in different cloud providers. Such functionality can be important in cases where a patient visits a hospital in a different country and medical staff needs to access her medical data to decide on the care plan for the patient. A prototype of the described protocol was implemented as an extension of Openstack, a popular cloud platform. For a detailed description of the protocol, a security analysis as well as a description of access rights management, we refer the reader to [18].

VI. Conclusion

In this paper, we have described aspects of prototyping the migration of a proprietary EHR system called "Melior", used by the Region Skåne in Sweden, to a fully virtualized IaaS cloud. We have presented a list of security requirements relevant for the deployment of "Melior" in an IaaS cloud. Next, we described a novel attack vector characteristic for IaaS clouds, namely vulnerabilities in the VM image management process and proposed a VM image management process that addresses VM image creation, management and decommissioning. Finally, we have presented the application of a storage protection protocol to the cloud deployment of "Melior". This storage protection protocol improves the confidentiality and integrity protection of the medical records without affecting data access functionality from a user perspective.

The security risks and solution relevant to an EHR system deployment in a IaaS cloud presented in this paper cover only a fraction of the challenges facing a large-scale migration of public e-health systems to IaaS clouds. We hope this contribution will encourage an exchange of best practices and lessons learned in migrating public e-health systems to fully virtualized IaaS cloud environments.

Acknowledgements

The authors would like to express their gratitude to Martin Svensson and Olof Mårtensson of Region Skåne for sharing their advice, intricate domain expertise and insightful discussions throughout the project.

References

[1] "Gematik - gesellschaft fur telematikanwendungen der gesundheitskarte." http://www.gematik.de, 2011.

[2] R. J. Rodrigues, "Opportunities and challenges in the deployment of global e-health," *International Journal of Healthcare Technology and Management*, vol. 5, pp. 335–358, 01 2003.

[3] B. Saporito, "The e-health revolution," *TIME*, 2005.

[4] C. Chatman, "How cloud computing is changing the face of health care information technology," *J Health Care Compliance*, vol. 12, pp. 37–70, 2010.

[5] J. T. Dudley, Y. Pouliot, R. Chen, A. A. Morgan, and A. J. Butte, "Translational bioinformatics in the cloud: an affordable alternative," *Genome Med*, vol. 2, p. 51, 2010.

[6] J. Kabachinski, "What's the forecast for cloud computing in healthcare?," *Biomed Instrum Technol*, vol. 45, pp. 146–50, 2011.

[7] A. Nilsson, M. Grisot, and M. Aanestad, "Electronic patient records–an information infrastructure for healthcare," in *Proceedings of the 25th Conference in Information System Research in Scandinavian (IRIS), Bautahøj, Denmark*, 2002.

[8] B. R. Kandukuri, R. P. V., and A. Rakshit, "Cloud security issues," in *Proceedings of the 2009 IEEE International Conference on Services Computing*, SCC '09, (Washington, DC, USA), pp. 517–520, IEEE Computer Society, 2009.

[9] IBM, "Security and high availability in cloud computing environments," Tech. Rep. MSW03010-USEN-00, IBM SmartCloud Enterprise, East Lansing, Michigan, June 2011.

[10] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "e-health cloud: Opportunities and challenges.," *Future Internet*, vol. 4, no. 3, pp. 621–645, 2012.

[11] E. Frander, C. Schwarting, A. Hawkins, and S. Richter, "Getting your head in the clouds: The use of cloud technology to enhance student success," in *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2013* (J. Herrington, A. Couros, and V. Irvine, eds.), (Victoria, Canada), pp. 1415–1417, AACE, June 2013.

[12] J. Domzal, "Securing the cloud: Cloud computer security techniques and tactics (winkler, v.; 2011) [book reviews]," *Communications Magazine, IEEE*, vol. 49, pp. 20–20, September 2011.

[13] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, "Managing security of virtual machine images in a cloud environment," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 91–96, ACM, 2009.

[14] S. Bugiel, S. Nürnberger, T. Pöppelmann, A.-R. Sadeghi, and T. Schneider, "Amazonia: When elasticity snaps back," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, (New York, NY, USA), pp. 389–400, ACM, 2011.

[15] N. Paladi, C. Gehrmann, M. Aslam, and F. Morenius, "Trusted launch of virtual machine instances in public iaas environments," in *Information Security and Cryptology–ICISC 2012*, pp. 309–323, Springer, 2013.

[16] T. Ristenpart and S. Yilek, "When good randomness goes bad: Virtual machine reset vulnerabilities and hedging deployed cryptography.," in *NDSS*, 2010.

[17] J. Reardon, D. Basin, and S. Capkun, "Sok: Secure data deletion," in *Security and Privacy (SP), 2013 IEEE Symposium on*, pp. 301–315, IEEE, 2013.

[18] N. Paladi, A. Michalas, and C. Gehrmann, "Domain based storage protection with secure access control for the cloud," in *Proceedings of the 2014 International Workshop on Security in Cloud Computing*, ASIACCS '14, (New York, NY, USA), ACM, 2014.

[19] Trusted Computing Group, "TCG Specification, Architecture Overview, revision 1.4," tech. rep., Trusted Computing Group, 2007.

[20] O. Goldreich, S. Goldwasser, and S. Micali, "How to Construct Random Functions," *J. ACM*, vol. 33, pp. 792–807, Aug. 1986.

[3] All data in a single domain is protected with the same storage protection master key, the domain key. This key is generated by the TTP and cannot ever leave TTP's logical perimeter.