Applications of Trusted Computing for Medical Privacy

Rachel Greenstadt and Jean-Francois Raymond

June 15, 2004

1 Motivation and Overview

The problem of protecting privacy of electronic medical information cannot be solved using traditional security methods such as access control and cryptography. Medical records must be transferred between various heterogeneous application domains that may or may not be trusted. Currently, this problem is solved at the political layer; contracts are drawn up between the parties that legally bind them to use the data appropriately. This process is both cumbersome and insecure. Ultimately, this problem is similar to digital rights management of entertainment content: the patient and/or physician would like to control the *use* of their data after it has passed out of their control. Among the most promising (or feared, depending on perspective) of digital rights management technologies is the Trusted Computing Initiative (TC). We describe a design for a system that uses TC for securing medical data and analyze its security and financial and technical viability.

2 Trusted Computing Background

Trusted Computing is the result of an industry consortium whose stated goal is to improve security and confidence in computer systems. TC is widely distrusted because of its potential to be used for digital rights management or to leverage monopoly power and create lock-in. The question we are trying to answer is, can it also be used for medical privacy and, if so, how?

The basic idea behind TC is that computers will contain a chip, the Trusted Platform Manager (TPM) that can protect keys and do cryptographic processing. The controversial (and useful) bit is that this chip protects these keys from the administrator of the machine, allowing trust to be built between administrative domains. On top of the TPM is the Trusted Software Stack(TSS) that interfaces with the chip. It is somewhat difficult to understand how the TSS works. It was designed by committee and it shows. There are thousands of pages of incomplete, buggy and badly written specifications as well as high level white papers. None of these specifications are implemented (publicly). However, it is possible to gain some understanding of the primitives that this combination (TPM and TSS) is supposed to provide.

Attestation is the ability to prove to a remote third party that a machine is running some specific software configuration. In TC, this is done by hashing the appropriate pieces of software and storing them in Platform Configuration Registers(PCRs). The TPM can then check that what is running on the machine matches what is stored in these registers. TC can also improve the security of key managment by having keys generated on the TPM, preventing keys from being exported off the TPM, and requiring authorization data before the keys can be used. TC can provide sealed storage by encrypting and decrypting data upon presentation of authentication data. This decryption can be contingent on certain PCR values. Certain events and commands can be logged and tick counters are provided by the chip.

3 Approach

Let's say a patient gets admitted to a hospital in New York and needs to have her medical records transferred from her primary care physician in D.C. for treatment. The D.C. physician would learn, perhaps

through an electronic registry, that the New York hospital had a machine with a TPM chip with a particular cryptographic key. The D.C. physician would then send the records encrypted to the recipient's key. However, the decryption of these records would be conditional on certain PCR values. These PCR values could demonstrate that the hospital's machine was running an appropriate software configuration, including a secure application for reading sensitive medical data. If these checks succeeded, the NY hospital would be able to open the files within the secure medical application. This application could then access a rule set for the hospital that would, for example, allow the hospital to read the record but not copy the information outside of the application.

Of course, this presumes that the hospital in New York has a TC chip and an approved software configuration. The system both suffers and benefits from the network effect. Realistically, not all health care systems will be compliant, and realistically, because lives may be at stake, the information should probably flow anyway. One thing TC can provide in this case is secure documentation of how the information left the TC network. A secure log is one of the things implementable with the TSS 1.2 specification. The software that does the logging can be protected with a PCR check. The log can be stored on the normal hard disk, encrypted and integrity protected with keys managed through the TPM. The log can be protected from replay or roll back attacks by secure timestamps created using the TPM's secure tick counter.

4 Caveats and Issues

There are some fundamental limitations to this approach. These chips are cheap: a determined physical attack is going to succeed at circumventing them. With the current Trusted Computing design, information might be readable (and copyable) in unprotected memory. Later versions of the Trusted Software Stack, or other initiatives like Microsoft's Next Generation Secure Computing Base, might provide these properties. In addition, Trusted Computing can't protect information that is seen or read, like the fact that an athlete's shoulder is irreparably damaged, from being emailed to the media. On the other hand, it might protect the xray that led to that analysis.

It is interesting to study how a TC system would fit in with HIPAA, the primary legislation regulating health care privacy in the United States. HIPAA has few hard and fast requirements but it does specify certain areas in which firms should follow best practices. TC could improve the best practices for (1) Data security—the secure key management makes data less vulnerable to outside software attack (viruses, etc), (2) Logging—HIPAA requires documentation and audit trails; the log is secure and nonrepudiable and can also happen transparently to the user for convenience, and (3) Secure data transfer between administrative domains could be enabled without layers of human bureaucracy.

It is important to consider the financial impact of this type of solution. If these chips turn out to be incorporated into everything by default, this may not be much of an issue, but what about doctors who want to view records on phones or PDAs? How much will the software (TSS and secure medical applications) cost? Research remains to understand the cost-benefit analysis of this scheme. In this, the network effect will need to be considered. It is clear that there is some benefit to using TC software independent of the rest of the industry (for key management and logging), but is it enough? Could a few large players (or a few lawsuits) force the industry to adopt this technology?

Ultimately, the technology is quite promising for providing privacy, but it is too vague to make strong claims about. The chips are already shipped in IBM laptops, but how far will they penetrate? Microsoft's NGSCB operating system which requires hardware similar to the TPM will have an important impact, but it is unclear what that impact will be. Still, if we make some assumptions about the primitives provided it is possible to do some system design and start a debate about how best to use this technology to protect privacy, so that when it is available it can protect something more than just music and DVDs.