

# Applications of Trusted Computing for Medical Privacy

Rachel Greenstadt

Jean-Francois Raymond

{greenie,jraymond}@eecs.harvard.edu

Portia Workshop on Sensitive Data

July 8, 2004

# Electronic Health Records

Buzz about EHRs for 40 years:

- Ease sharing of patient records among practitioners
- Improve patient safety, reduce medical errors
- Support patient billing procedures
- Reduce healthcare costs
- Current status: Paper records mailed between providers, faxed in emergencies.

So, what's the problem?

# Privacy and Liability Issues

- Majority of Individuals Concerned about Medical Privacy
  - ◆ Discrimination—stigma of certain illnesses, medications
  - ◆ Disclosure might discourage treatment
  - ◆ Increased insurance premiums
  - ◆ Incidents of misuse increase concerns
- Regulation (HIPAA)
- Other Obstacles to EHR: cost of transition, finding good products, making business case

# Traditional Won't Work

# Security

# Methods

- Normally solved with access control and cryptography
- Rules may not be followed after decryption
- Heterogeneous Domains—Need human intervention for transfers between administrative domains
- Compromised machines still a problem
- But, these technologies are well established

# Medical Privacy and DRM

- Goals
  - ◆ Data-centric security across administrative domains
  - ◆ Prevent unauthorized use of sensitive data as well as unauthorized access
- Same goal as Trusted Computing (TC) and Digital Rights Management (DRM)

# Contrasts with “Traditional DRM Applications”

- Similar tech: prevent rule circumvention
- Need increased flexibility
  - ◆ Data may need to flow—lives at stake
- Incentive structures are different:
  - ◆ Keeping honest people honest
  - ◆ Benefit to the consumer (bureaucracy, liability)
  - ◆ Power balances?
  - ◆ Better chance to succeed?

# What is Trusted Computing (TC)?

- Industry consortium to “Improve security and confidence in computer systems”
- Many pages of specifications and chip (in IBM thinkpads now)
- Widely distrusted
  - ◆ Unpopular DRM uses
  - ◆ Can leverage monopoly power to create lock-in
- Can it be useful in the medical privacy space

# What Does TC Buy?

- Secure ID of remote computer  $R$
- Answers: Is  $R$  running software I trust? If yes,  $R$  will follow rules with regard to data I send

# How does TC Work?

- Consists of TPM chip and software specs
- Provides a secure means for
  - ◆ Verifying software integrity—hashes of software stored on chip in platform configuration registers (PCRs)
  - ◆ Sharing measurements—Chip stores a key inaccessible to the machine administrator
- Example: Allow decrypting a “blob” contingent on software measurements

# Design Properties

- Secure data transfer between administrative domains
- Emergency overrides and secure audit
- Hardware key management and encryption primitives for increased data security
- Simple and transparent

# File Transfer Example

- Patient Alice is admitted to a hospital in N.Y., needs records transferred from D.C.
- D.C. physician learns that N.Y. hospital has a machine with a TPM chip and a particular key
- D.C. physician sends the records conditionally encrypted with the recipient's key—the records can only be opened if the PCR values of the machine are correct

# Reading Files

- When record is received
  - ◆ Decrypted by TPM chip
  - ◆ PCR checks are executed
  - ◆ The signature is verified
- If checks succeed
  - ◆ Decrypted file is passed to the Secure Data Manager (SDM)
  - ◆ SDM looks up the Rule Set for the data
  - ◆ Polices access and usage for the administrative domain

# Logging and Secure Overrides

What if the hospital isn't running a correct software configuration?

- Some administrative domains should send data anyway
- System can provide secure documentation of how the data left
- Logging software can be protected with a PCR check

# Limitations of TC

- Physical Attacks
- Small data items
- Reading memory?
- Underspecified

# Microsoft NGSCB

- New MS operating system, in development
- Uses TPM-like hardware
- Often associated / confused with TC
- May solve the memory problems
- Can cause widespread adoption of TC

# Fitting in with HIPAA Regulations

- HIPAA privacy rule specifies industry should use best practices
- TC could improve these practices
  - ◆ File transfer—improved security and efficiency
  - ◆ Secure Logging
  - ◆ Data security

# Conclusions

- DRM technology seems like the right answer
- Can mediate trust between administrative domains
- Not ready for prime time yet
  - ◆ Hardware chips in some computers (IBM laptops)
  - ◆ Most of software unimplemented
  - ◆ No one knows how it will play out

# Architecture

