Securing the Health Information Grid: Facilitating Meaningful Sharing with User Awareness and Control

Mustaque Ahamad
Georgia Tech Information Security Center
Georgia Institute of Technology

Joint work with Doug Blough, Musheer Ahmed and Daisuke Mashima.
Health IT: Improving Care Quality and Reducing Cost

• Emerging health information sharing infrastructure
  ‣ Electronic and personal health records
  ‣ Health Information Exchange (HIE), National Health Information Network (NHIN)
  ‣ Mobile health

• Meaningful use [National Coordinator for HIT]
  ‣ Complete and accurate information
  ‣ Better access to information
  ‣ Patient empowerment
Need for Securing Health Information

• Privacy and security is key requirement [HITECH Act of 2009]

• Sophisticated cyber criminals are certain target health information systems
  ‣ Medical identity theft: a criminal gang defrauded Medicare more than $100 million
  ‣ Medical identity theft is worse than identity theft – your health information integrity is lost as well

• Securing health information at community and small physician offices will be a challenge

• Patient awareness and consent is a key mechanism to meet compliance requirements
• Accountable access to health information: enhancing patient awareness and control
• Securing health information on mobile devices
• Other Georgia Tech research in health information security
Secure access monitoring for accountability

• Complete mediation in a distributed environment
  • When / by whom / how records are updated?
  • When / by whom / how records are consumed?
• General distributed information flow is very hard to address in systems that are currently deployed
• Use of cryptographic primitives to solve a reasonable instance of the problem
  • Monitor all accesses when health information is presented to authorized entities
  • Public disclosure cannot be addressed
System Model

- Patient (owner) exercises control via an agent (monitoring agent)
  - May read or update health information and also provides explicit or implicit consent
- Health information repository
  - Provides long term storage for health information
- Issuers and consumers
  - Issuers generate health data and send it to repository (e.g., physician office)
  - Consumers access health information (insurance company, specialist office etc.)
Assumptions

• Secure communication across various entities

• Trusted Monitoring Agent
  ‣ Networked entity run on a third party trusted by a patient
  ‣ Monitors health record update/usage

• Authenticity and Integrity Verification
  ‣ Health record repository accepts records authorized by patients (*Patient’s signature*)
  ‣ “Meaningful usage” of health records is always accompanied by authenticity and integrity verification of the record (*Record issuer’s signature*)
Cryptographic Preliminaries

• Certificates for various parties
• Encrypted storage of health data
  ‣ Encryption alone does not solve the problem because one authorized party can share with others
• Digital signatures for integrity and authenticity
  ‣ Threshold signatures
  ‣ Designated verifier signatures
  ‣ Universal designated verifier signatures
Accountable Updates

- Use “partial” patient authorization
  - Can be verified by contacting Monitoring Agent
  - Forces repository to communicate with Monitoring Agent to obtain “full” patient authorization
  - Implemented with **Threshold Signature**

- Countering malicious repository behavior
  - Use transaction proof
    - Record receipt issued by repository
    - Patient authorization proof
Usage Monitoring

• Every record consumer verifies issuer signature by communicating with Monitoring Agent
  ‣ Providers do not give publicly verifiable signature to consumers
  ‣ Designated Verifier Signature (DVS) can make issuer signature non-transitive
  ‣ Issuer can not know who will be consumers

• Proposed solution
  ‣ Encrypt issuer signature s.t. only Monitoring Agent can decrypt
  ‣ By using *Universal Designated Verifier Signature* scheme, Monitoring Agent designates the issuer signature online
Establish shared secret (sec)
Assign a private key share (ks)

K = Encsec{Hash}
Encsec{Signissuer}
TSignks{Authzn}

Hash
Sign

Doctor

K

Now can verify patient signature

Authorization Proof

SignRepo{Receipt} TSignks{Authzn}

Signpatient {Authzn}

Data Receipt

Repository

Georgia Institute of Technology - Converging Infrastructure Security (CISEC) Laboratory
[Usage Monitoring]  
Monitoring Agent  

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

K' = Encsec{Hash}

Encsec{Signissuer}

Hash

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

K' = Encsec{Hash}

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.

Encsec{Signissuer}

Hash

Leaked or shared...

UDVS can not convince non-designated entity. Then, to use record meaningfully, he is also required to contact Monitoring Agent.
Integration to NHIN DIRECT

Typical flow of NHIN DIRECT
Flow enforced by our scheme
Securing Health Information on Mobile Devices

- Mobile devices are the most convenient place for accessing data
  - Pervasive connectivity
  - Rich applications
  - Aggregation of information captured by health sensing devices
  - Security concerns have limited use of mobile devices.

Joint work with Jon Giffin and Patrick Traynor.
Mobile Attacks

• Attacks from the desktop world moving into the mobile environment
  ‣ 2010: Google remotely nukes two apps that violated TOS
  ‣ 2010: 20% of Android apps leak private user data
  ‣ 2010: Android media player trojan spreads via text message
  ‣ Recent DreamDroid malware
Current Mobile Device Security

- Ignore
- Direct interaction with service provider
- Periodically check revocation server
- Migrating desktop solutions

Georgia Institute of Technology - Converging Infrastructure Security (CISEC) Laboratory
Mobile Malware

- Mobile application marketplace can be used to propagate infected or malicious applications

- How are applications being evaluated?
  - Sophistication of malware in the desktop space (GT Mtrace system)
  - Analysis must focus on what they do rather than what they are
  - Utilizing available resources (IP reputation, DNS domain reputation, blacklists etc.)
  - Drive-by-downloads
Security Goals

- Prevent infected third-party healthcare applications from leaking sensitive medical information.
- Implement HITECH/HIPAA inspired policy on mobile device.
Approach

- Applications that interact with sensitive healthcare data are termed constrained applications.
- Our policy only applies to constrained apps.
- Mediate data exit points from the constrained app.
- Non-sensitive data should be unaffected.
Sources of Healthcare Information

- External repositories
  - Google Health etc.
- Medical devices connected via Bluetooth/USB
  - Glucometers, BP monitors etc.
- Memory card
- User input
Security Policy

- Sources of healthcare information are classified as sensitive locations.
- Data downloaded from sensitive locations into a constrained app is tainted.
- Healthcare data leaving the constrained app on the network, IPC and external storage is mediated.
- Healthcare data can leave the constrained app to sensitive locations.
- Healthcare data leaving the constrained app to non-sensitive or unknown locations can be blocked or generate a user prompt.
- Non-sensitive data can move freely outside the constrained app.
- Unknown locations are classified by the user.
Other Healthcare Security/Privacy Research

- Access control policies for Health Information Exchanges (Doug Blough)
- Security architectures for clinical research (Atlanta Clinical and Translational Science Institute – joint work with Emory University)
- Privacy driven access control (joint work with Ling Liu, Calton Pu and Lilly Immergluck – Morehouse School of Medicine)
Conclusions

- Achieving trustworthy health information sharing will require us to overcome many challenges.
- We must build security-in as we deploy HIE and NHIN infrastructure.
- Mobile devices will play a key role as access and capture points for health information.
- Do patients really want or need the awareness and control?
- People are the weak link and the healthcare environment is more people rich than any other domain.
- We need to better understand the threats and risks posed by compromised health information.