

Daisuke Mashima and Mustaque Ahamad, Georgia Institute of Technology, Atlanta, GA

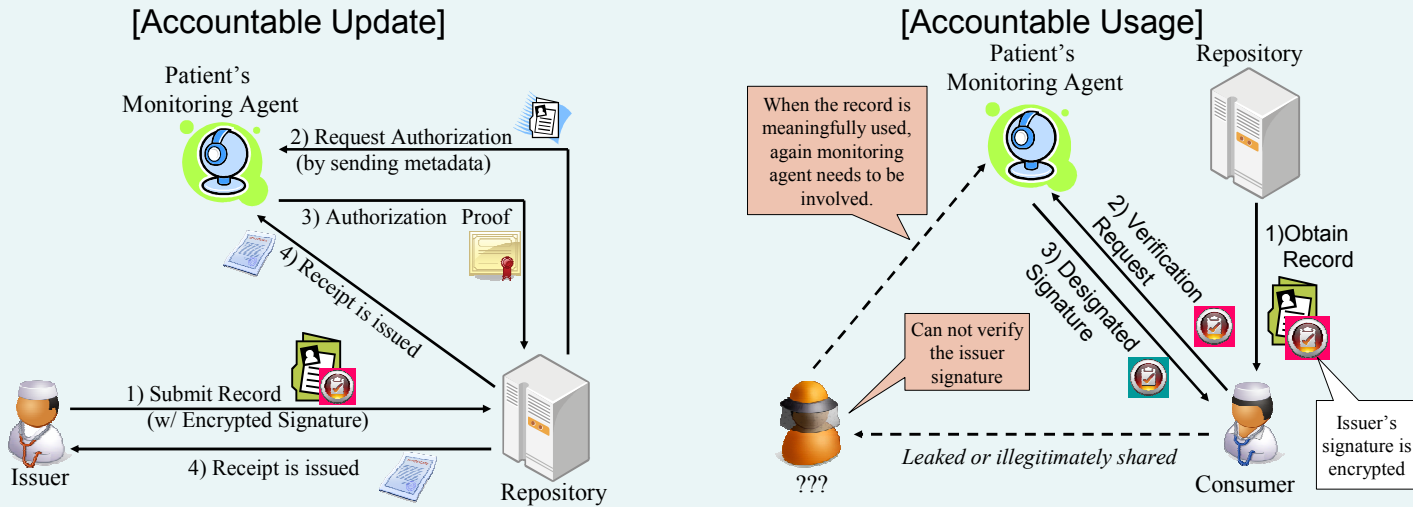
Background

- Paper-based records are moving to electronic health (medical) records
 - EHR / PHR systems
- “Meaningful Use” Promotion by Government
- Efforts to enable nation-wide health information sharing
 - National Health Information Network (NHIN)
- Major players have joined PHR and health record sharing using NHIN Direct standard
 - Microsoft HealthVault
- Benefits of Electronic Health Records
 - Complete and accurate information
 - Better access to healthcare data
 - Patient empowerment
- Security and Privacy Threats
 - Leakage of healthcare data
 - Deliberate breach by insiders
 - Medical identity theft

Goals / Scope / Assumptions

- Enabling patient awareness and control over usage and update of electronic health records
- Design and implementation of **“Patient-centric Monitoring Agent”**
 - Run on an online entity chosen/trusted/managed by patients themselves
 - Mediate usage and update of the patients’ healthcare records
- Allow patients to be aware of by whom and when records are meaningfully consumed
 - E.g., medical treatments, insurance services etc.
- Assumptions:
 - Criminals can profit from stolen data only by presenting it to legitimate consumers which are motivated to verify the authenticity of data
 - Patients are co-owners of data and have the right to be notified of creation / update and also authorize them

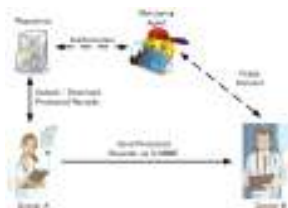
System & Protocol Overview



Protocol Summary

- Monitoring Agent can mediate updates of health records on repositories
 - Repository needs to obtain Authorization Proof.
- Monitoring Agent can log every entity that meaningfully consumes health records
 - The issuer signature can be verified by nobody but the designated consumer.
- Transaction proofs are implemented
 - Protect honest entities while misbehavior or omission of protocol execution can be punished

Implementation in NHIN Direct



- Client (Issuer/Consumer) device
 - Pentium M 750, 2GB RAM, Windows 7
 - Network connectivity: Cable TV and 3G network
- Server (Monitoring agent/Repository)
 - Intel Xeon 5150, 8GB RAM
 - 12 hops away from the client device

Client Type	File Size		
	100KB	100KB (3G)	2MB
Issuer (Dr. A)	0.82 sec	2.88 sec	5.06 sec
Consumer (Dr. B)	0.72 sec	1.20 sec	0.86 sec