Persistent Security, Privacy, and Governance for Healthcare Information

Knox Carey, Jarl Nilsson, and Steve Mitchell
Intertrust Technologies Corporation

USENIX HealthSec Workshop
9 August 2011
The Fundamental Problem

- Medical information needs to be widely distributed
  - To the point of care, regardless of origin
  - To specialists consulting on a particular case
  - To researchers and public health authorities
  - To family caregivers
  - &c.

- Technology can make this happen

- This is not happening
Nature of the Problem

- Every interface between systems poses risk
  - Systems may not interoperate at all
  - Policies differ between systems
    - Laws and regulations
    - Corporate policies
    - Patient preferences
  - No assurance that policies will be respected

- Resulting behaviors
  - Data hoarding
  - Asking patients to sign away rights
Elements of the Solution: Persistent Governance

- Protect healthcare information at its source
- Persistently associate rules that govern access
  - Access granted to certain principals or roles
  - Rules under the control of the patient, ideally
  - Access can be audited
- Ensure uniform enforcement of those rules
Elements of the Solution: Consistent Trust Management

- Systems must be able to interoperate
- No prior interaction should be assumed
- Senders must be able to rely upon computations performed by a recipient
- Role for government?
Elements of the Solution: Derived Resources

- Meeting the conditions in a rule unlocks a resource
- Should the resource look the same to all?
  - You
  - Your doctor
  - The nurse
  - Your physical therapist
  - Your therapist therapist
  - Your children
  - An epidemiologist
Derived Resources

- A derived resource combines:
  - A resource
  - A set of rules
  - A set of computations to be performed upon the resource
In Conclusion

• Our goal is to get information moving

• Trusted distributed computing, policy management are essential ingredients

• New applications require new approaches
Questions