NIST's Privacy Enhancing Cryptography Workshop

Rene Peralta
Computer Security Division

March. 2012

Privacy work.

- Information Technology Laboratory.
    - Computer Security Division.
        - Cryptographic Technology Group.

Privacy work.

- Information Technology Laboratory.
    - Computer Security Division.
        - Cryptographic Technology Group.

- Identify potential applications of cryptography in the area of privacy/identity.

Privacy work.

- Information Technology Laboratory.
    - Computer Security Division.
        - Cryptographic Technology Group.

- Identify potential applications of cryptography in the area of privacy/identity.
- We need guidance from policy people, advocates, industry for deciding which problems we should be looking at.

Privacy work.

- Information Technology Laboratory.
    - Computer Security Division.
        - Cryptographic Technology Group.

- Identify potential applications of cryptography in the area of privacy/identity.
- We need guidance from policy people, advocates, industry for deciding which problems we should be looking at.
- Cryptography can do surprising things. We need to do a better job of explaining these capabilities to people who can tell us how to leverage them in the privacy/identity arena.

Meeting on Privacy-Enhancing Cryptography

- Held in December of 2011 **(link)**

- Goal: Get the different communities talking to each other.

- Technical focus:

  Working with encrypted data without decrypting.

Techniques

- Secure multiparty computation.
- Auctions.
- Private information retrieval.
- Oblivious RAMs.
- Group signatures.
- Schemes for encrypting personal health records.
- Smart metering.
- Direct anonymous attestation.
- Conditional and revocable anonymity.

Techniques

- Secure multiparty computation.
- Auctions.
- Private information retrieval.
- Oblivious RAMs.
- Group signatures.
- Schemes for encrypting personal health records.
- Smart metering.
- Direct anonymous attestation.
- Conditional and revocable anonymity.
- Identity-based encryption.
- Attribute-based encryption.
- Format preserving encryption.

Reports, Panels, Motivation

- Marc Rotenberg, EPIC : “Why we should care about privacy in the identification domain”.

Reports, Panels, Motivation

- Marc Rotenberg, EPIC : “Why we should care about privacy in the identification domain”.
- SPAR/NICECAP pilots.
- Panel on medical (and other sensitive) databases.
- Panel on smart metering.
- Panel on privacy in the identification domain.

Technologies

- U-Prove.
- Idemix.
- EPID.

What have we learned so far?

What have we learned so far?

This stuff is really hard!

What have we learned so far?

This stuff is really hard!

- but we don’t need to understand the full picture in order to be useful...

Selective disclosure for NSTIC

- Model identity (persona?, something else?) as a set of attributes.

Selective disclosure for NSTIC

- Model identity (persona?, something else?) as a set of attributes.
- Signed attributes are stored in some device.

Selective disclosure for NSTIC

- Model identity (persona?, something else?) as a set of attributes.
- Signed attributes are stored in some device.
- A digital transaction involves a proof that my attributes satisfy a given criterion.

Selective disclosure for NSTIC

- Model identity (persona?, something else?) as a set of attributes.
- Signed attributes are stored in some device.
- A digital transaction involves a proof that my attributes satisfy a given criterion.
- Privacy is protected by restricting criteria to only what is necessary to complete the transaction.

Selective disclosure for NSTIC

- Model identity (persona?, something else?) as a set of attributes.
- Signed attributes are stored in some device.
- A digital transaction involves a proof that my attributes satisfy a given criterion.
- Privacy is protected by restricting criteria to only what is necessary to complete the transaction.
    - “born before March 15, 1991”

Selective disclosure for NSTIC

- Model identity (persona?, something else?) as a set of attributes.
- Signed attributes are stored in some device.
- A digital transaction involves a proof that my attributes satisfy a given criterion.
- Privacy is protected by restricting criteria to only what is necessary to complete the transaction.
    - “born before March 15, 1991”
    - “has valid prescription for Vicodin”

Selective disclosure for NSTIC

- Model identity (persona?, something else?) as a set of attributes.
- Signed attributes are stored in some device.
- A digital transaction involves a proof that my attributes satisfy a given criterion.
- Privacy is protected by restricting criteria to only what is necessary to complete the transaction.
  - “born before March 15, 1991”
  - “has valid prescription for Vicodin”

  This is not easy: the pharmacist does not find out who the prescribing doctor is.

What have we learned so far?

This stuff is really hard!

- but we don’t need to understand the full picture in order to be useful...
- multidisciplinary efforts are essential.

What have we learned so far?

This stuff is really hard!

- but we don’t need to understand the full picture in order to be useful...
- multidisciplinary efforts are essential.
- transactions in the online world are fundamentally different

What have we learned so far?

This stuff is really hard!

- but we don’t need to understand the full picture in order to be useful...
- multidisciplinary efforts are essential.
- transactions in the online world are fundamentally different
- ... and they occur in an evolving environment.

What have we learned so far?

This stuff is really hard!

- but we don’t need to understand the full picture in order to be useful...
- multidisciplinary efforts are essential.
- transactions in the online world are fundamentally different
- ... and they occur in an evolving environment.
- we can enhance the environment to make privacy preserving transactions easier.

What have we learned so far?

This stuff is really hard!

- but we don’t need to understand the full picture in order to be useful...
- multidisciplinary efforts are essential.
- transactions in the online world are fundamentally different
- ... and they occur in an evolving environment.
- we can enhance the environment to make privacy preserving transactions easier.

NIST randomness beacon

Report

We are writing a report.

A non-technical description of what crypto can do (rather than how it does it).

Report

We are writing a report.

A non-technical description of what crypto can do (rather than how it does it).

Mail to

peralta@nist.gov