LIBERTY ALLIANCE PROJECT

Identity Theft Technical Overview

Washington D.C.

April 26, 2006

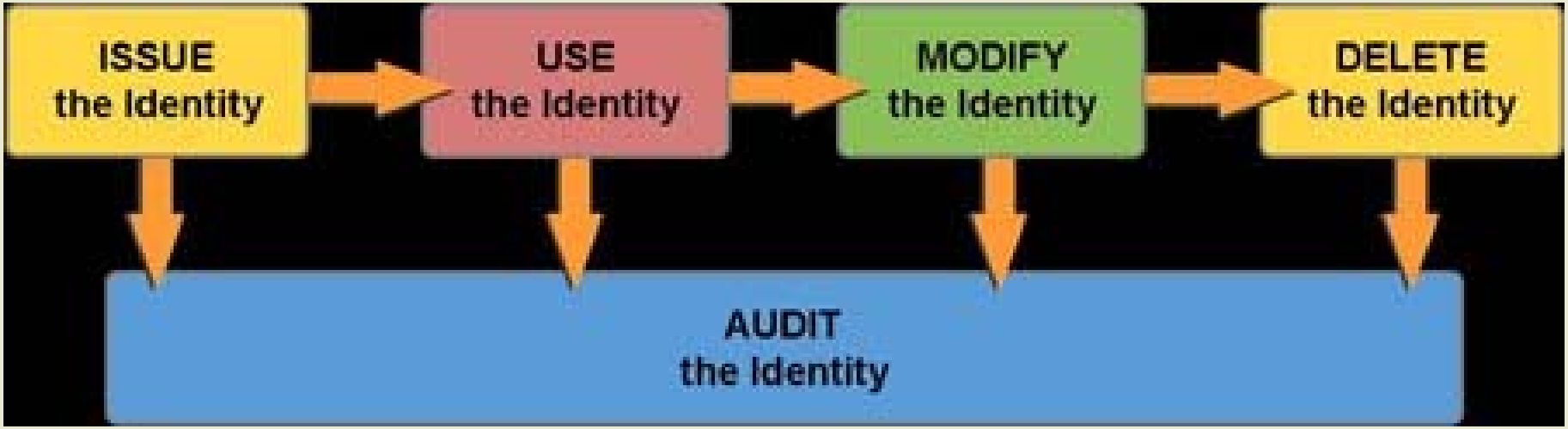
Identity Theft

The United States Federal Trade Commission (FTC) defines identity theft as 'a fraud that is committed or attempted, using a person’s identifying information without authority'.

Questions to ask…

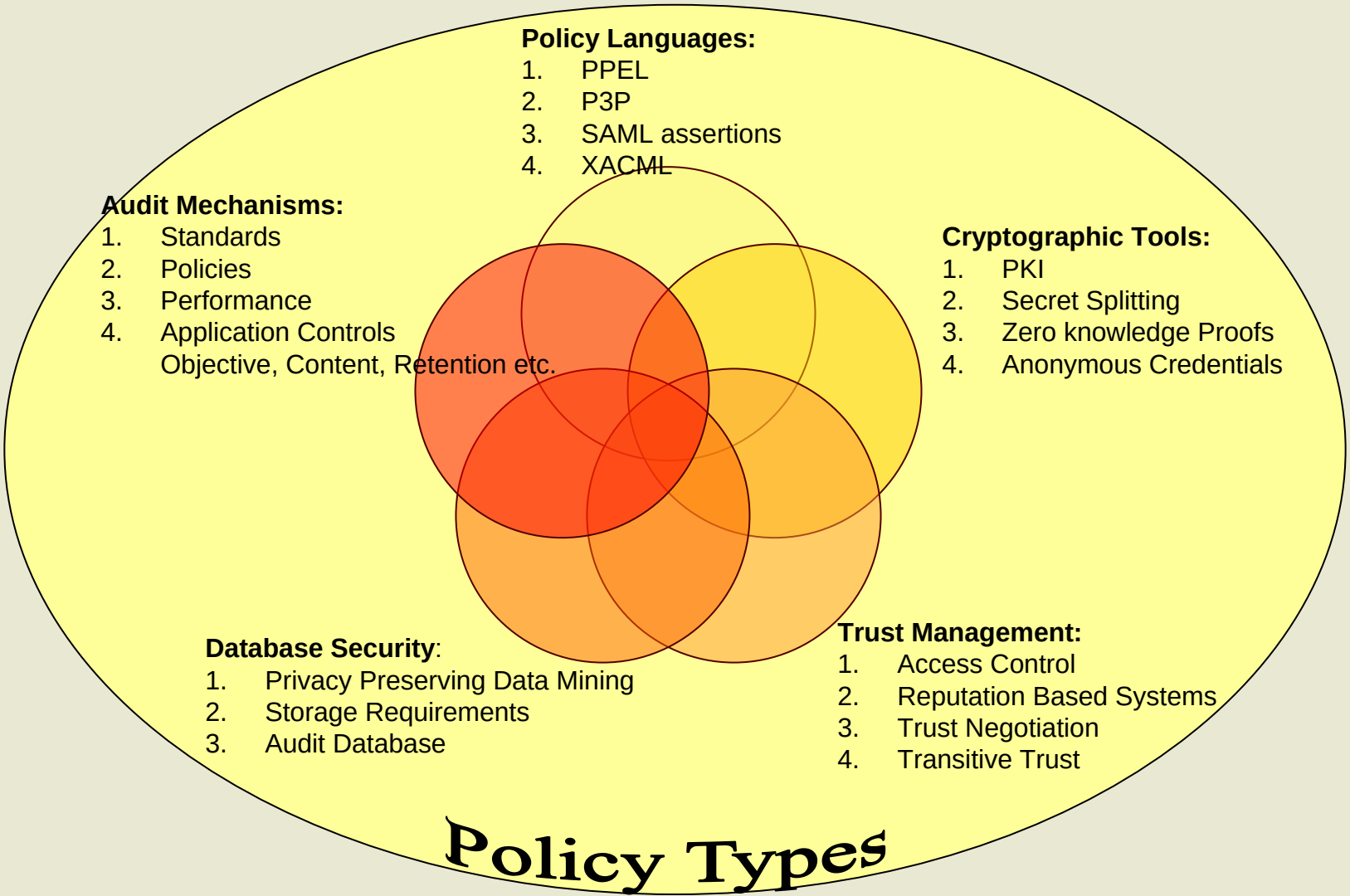
1. How does identity theft occur?
   - Obtain PII
   - Use or Sell for fraud
2. Why are we vulnerable?
   - Several isolated data warehouses
   - Little control of users over their PII
   - Lack of awareness or training
3. What are the threats?.
   1. Internet
   2. Insider threat
   3. Social Engineering
   4. Physical

Identity Lifecycle



1. Registration procedure
2. Storage Mechanisms
3. Access Control on usage (Authentication and Authorization)
4. Usability
5. Auditing and Accountability

Types of Technology Solutions



Policy Languages

- **Privacy Policies** [PPEL/ P3P]: Typically privacy policies state who the *recipients* will be for the user *data*, the *purpose* for which this data will be used, and how long the data will be *retained*.
- **Assertion Language** [SAML 2.0]:
  The Security Assertion Markup Language (SAML) is an XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain.
- **Authorization Policy**[XACML]:
  - General-purpose authorization policy model and XML-based specification language
  - XACML is independent of SAML specification
  - Triple-based policy syntax: <Object, Subject, Action>
  - Negative authorization is supported

Cryptographic Tools

- Public Key Infrastructure
  - To establish and maintain a trustworthy networking environment
- Secret Sharing
  - method for distributing a *secret* amongst a group of participants, each of which is allocated a *share* of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.
- Zero Knowledge Proofs:
  - Interactive method for one party to prove to another that a (usually mathematical) statement is true, without revealing anything other than the veracity of the statement.
- Anonymous Credentials/ E- cash

Trust Management

- TM asks the question *"Is someone trusted to take some action on some object?"* and *"why" trust is granted rather than immediately focusing on "how" cryptography can enforce it.*
  - "Each citizen has the right to establish trust in his or her own way"
  - "Computers can alter the equation only by substituting the explicit power of cryptography for the implicit power of psychology."
- Reputation System
- Automated Negotiation Systems (flexible policies)

LIBERTY ALLIANCE PROJECT

Database Security

- **Database Security** can be broken down into the following key points of interest.
  - Server Security
  - Database Connections
  - Table Access Control
  - Restricting Database Access
- **Datamining:**
  - Also known as Knowledge-Discovery in Databases (KDD)
  - Process of automatically searching large volumes of data for patterns.
  - Applies computational techniques from statistics, machine learning and pattern recognition.
  - Privacy Threat versus tool?

Audit Mechanisms

- Define audit objective
- Standard for information system auditing
- Performance of audit work
- Reporting
- Security and Privacy concerns
  - Content
  - Retention
  - Access control (Authentication and Authorization)
- Application transaction lifecycle

Auditing

- Use of several security enhancing techniques cannot completely eliminate fraud and identity theft attempts. Therefore there is a fundamental need of strong audit mechanisms that can detect attacks, misuse and maintain a certain level of assurance in the system.
- 3 cases: 1) Individual 2) Data Custodian 3) Third Party

LIBERTY ALLIANCE PROJECT

Technology/Id-Lifecycle Matrix

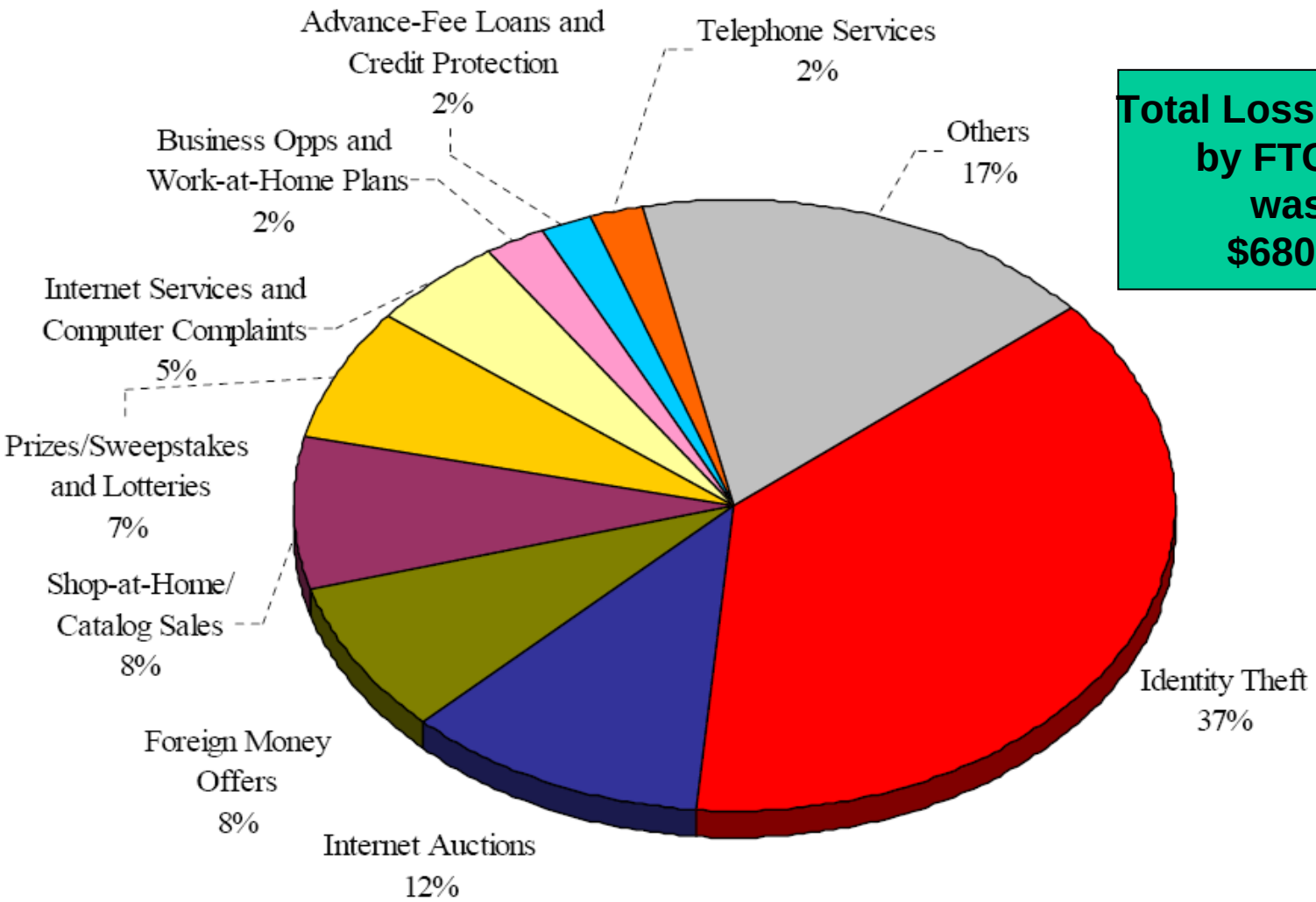
	Technical Tools			
Identity Lifecycle	**Policy Types**	**Cryptographic Tools**	**Trust Management**	**Database Security**
Registration/ Enrollment	Validation Policy	Challenge-Response Protocols, PKI	Automated Trust Negotiation	Encrypted Databases
Propagation	Authentication Policy, Privacy Policy, Attribute Release Policy, Attribute Acceptance policy	Encrypted Channels, Anonymous Credentials, Zero Knowledge Proofs, PKI	Automated Trust Negotiation, Trusted Validation	Secure Access to Identity Databases
Maintenance/ Management	Privacy Policy, Attribute Release Policy	Revocation and update mechanism of the crypto tokens	Revocation, Credential Discovery Protocols	Consistent Databases, Recovery, Integrity of Databases
Termination	Privacy Policy	Revocation Mechanism	Revocation Mechanism	Consistent deletion

Policy Types

- The implementation of the technical solutions depend on the policy and the laws in place.
- Policy can be of different types depending on the purpose of the policy. Example:
  - Validation policy (Enrollment)
  - Authentication policy
  - Integrity policy
  - Privacy policy
- Helps in Risk Analysis

Sentinel Top Complaint Categories[1]

January 1 – December 31, 2005

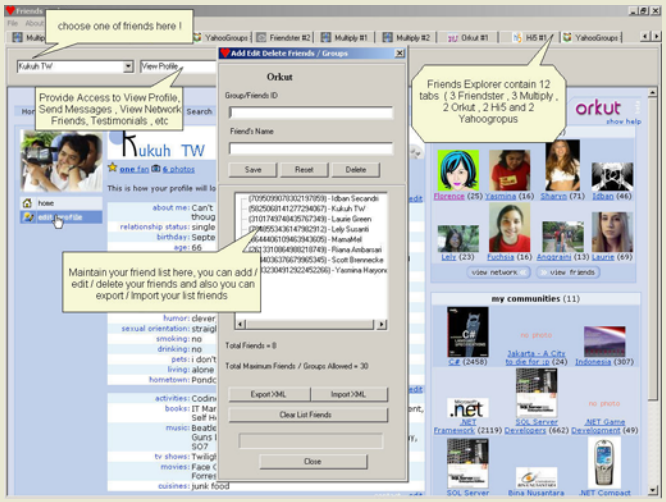


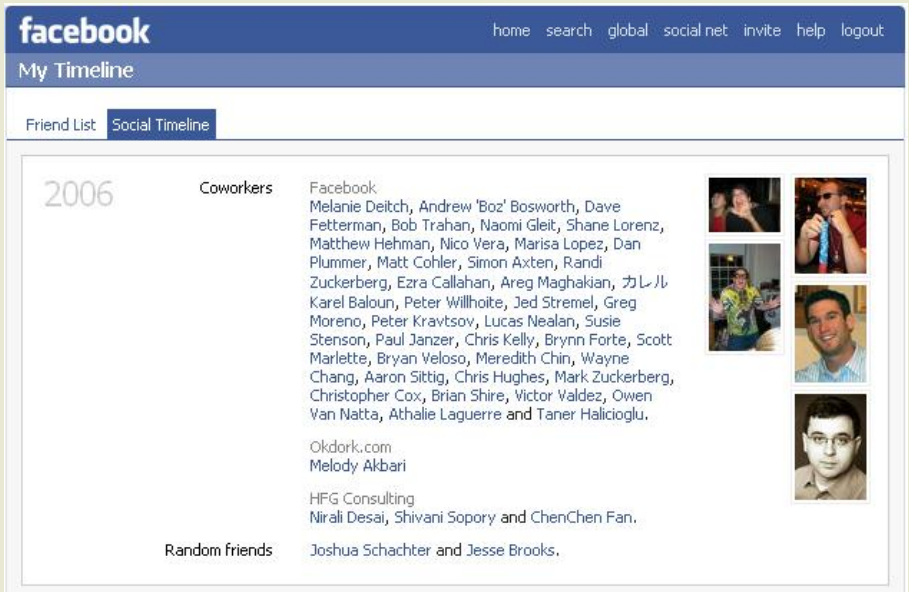
Total Losses estimated by FTC in 2005 was over $680 million

[1]Percentages are based on the total number of Sentinel complaints **(686,683)**

Problems (Why the explosion of ID-Theft)

- Gathering and trafficking of PII is increasing
- More exploits are bound to come with new applications-services being delivered.





Brainstorming session

- 1:15 to 3:45