CPSC 457/557:

Sensitive Information in a Wired World

The National Strategy for Trusted Identities in Cyberspace

Aaron Segal

Outline

- What is the National Strategy for Trusted Identities in Cyberspace (NSTIC)?
- How is it supposed to work?
- What are the difficulties in implementing it?
    - Integrity/Security
    - Privacy
    - Economics and the role of the government

NSTIC – What is it

- National Strategy for Trusted Identities in Cyberspace
- Broad outline of what a new trusted identity system would look like
- To be implemented by private or public sectors
- No deadline, no plan, no dedicated funding

NSTIC’s Vision

- “Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.”
- “Identity Ecosystem” to manage identities, credentials, and trust
- “Fair Information Practice Principles” (FIPPs) to ensure privacy of users

Identity Ecosystem

- Privacy protections
  - No additional information given, no personal information need be stored
- Convenience
  - No passwords
- Efficiency
- Ease-of-use
- Security
- Confidence
  - “Trustmarks” would indicate Identity Ecosystem compliance
- Innovation
- Choice
  - The Identity Ecosystem should be optional and have multiple providers

How Credentials Would Work

- Credentials are physical or data objects that hold data about a person
- **Identity providers** issue credentials with ID information
- **Attribute providers** issue anonymous, single attribute credentials
- **Relying parties** check credentials without needing to contact providers

Identity Credential

- {Name : Aaron Segal}
- {Sex: Male}
- {Birthdate : 3/4/1988}
- {Address: New Haven, CT}

Attribute Credential

- This person is a student at Yale University

Example Uses

- I want to gain access to an anonymous message board for Yalies only
  - Get attribute credential from Yale
  - Website verifies the credential
    - I stay anonymous
    - Yale is not contacted
- I want to buy a book from a website and get the student discount
  - Get identity credential from anywhere
  - Vendor verifies the credential
    - No need to open an account
    - No need to enter personal data

Identity Credential

- {Name : Aaron Segal}
- {Sex: Male}
- {Birthdate : 3/4/1988}
- {Address: New Haven, CT}

Attribute Credential

- This person is a student at Yale University

Simplistic Implementation

- I go to Yale and request a credential that says I go to Yale
- Yale verifies my identity and gives me a smart card
- I use the smart card to authenticate myself to a Yale website
- If the website can verify the signature, it gives me access

Smart Card

- Data = “This person is a student at Yale University”
- SK_{Yale}
- PW_{User}
- getTime()
- sign(m)
- getCredential(PW):
  - If $PW==PW_{User}$
    - σ=$sign_{SK}$(Data, getTime())
    - return (Data, getTime(), σ)

Risks to Integrity

- When I request the credential, Yale must verify my identity and status
- Vulnerability:
  - Public information
  - Fake IDs
- Any choice of providers means I can choose a less thorough identity check
- Ecosystem only as reliable as weakest identity verifier

Risks to Security

- Real credentials might be stolen
  - Phishing
    - Hopefully defeated by physical card, but private keys can sometimes be extracted
  - Physical theft
    - Hopefully defeated by passphrase, but could be guessed or brute-forced
  - Other exploits?
- Possession of a fake/stolen credential means:
  - Access victim’s private information
  - Act as victim for financial transactions
  - Anonymity means it may be hard to detect misuse

Revocation

- How can identity/attribute providers revoke credentials that are reported fraudulent/stolen?
- Expiration dates not strong enough
- Revocation lists
  - Frequent updates
  - Potential loss of privacy from exposing data
- Online Certificate Status Protocol
  - Providers will know when credentials are used
  - Vulnerable to replay attacks
    - Oblivious transfer protocols, nonces

Revocation and Privacy

- In either case:
  - Providers must be always online
  - Impetus is on relying party to check for revocation
    - Computational overhead
  - Credentials must have unique identifiers
- Unique identifiers on credentials means at best pseudonymity
- Using the same credential on many sites could allow de-anonymization attacks on privacy
- It seems anonymity is incompatible with the need to revoke lost or stolen credentials

Relying Parties and Privacy

- Ease of use may mean relying parties choose which credential fields to request
- How many websites will choose to request less than all the user's information?
- How many users are going to un-check these boxes?
- How will users know what information is being accessed?

☑ Click here if we may use your information to provide a personalized online experience!!!

☑ Click here if you would like to receive special discount offers from our partners!!

Implementation: Interoperability

- Critical part of the strategy: All providers should be recognized and compatible with all relying parties
    - Industry must adopt standards
- Every provider's key needs to reach every verifier
    - Barriers to entry from national key database or certificate authority hierarchy
    - What if a provider's key is compromised?
    - What if a provider goes out of business?
- Weakest link

Supply & Demand

Demand

- Remember only one password
- Enhanced privacy, maybe
- Carry around a smart card (or several)
- More secure
  - Unless it’s not
- Paid online services are unpopular

Supply

- Costs to enter market:
  - Publicize keys
  - Develop software
- Verify identities before issuing credentials
  - Potential liability
- Maintain revocation lists, security
- Payment options
  - Pay once?
  - Pay per month?
  - Free perk?
  - Ad-driven credentials?

Role of the Government

- Trustmarks: Verify whether the site is compliant
  - Who is in charge of this?
  - Will users care if the site has no trustmark?
  - Tragedy of cryptography
- Incentives
  - The government won’t mandate the use of credentials, but…
    - Require credentials for online tax filings
    - Give out free credentials to federal employees
    - Grants, subsidies, tax breaks
    - Limit liability for loss of data
- If privacy is going to be compromised anyway…

Thank You!

Questions?