Various Underlying Technologies

- Passwords (static vs. one-time)
- Challenge-response mechanisms
- PKI
- Biometrics
- . . .

Static Passwords

- Apparently simple to implement
- *Seem* to require little training
- No special equipment needed

But…

- Susceptible to guessing and interception
- Easily shared, between users and between verifiers
- Require costly infrastructure for issuance, revocation, resetting
- Often used inappropriately

Not simple, not cheap, training needed

Therefore:

- Education is needed with respect to weaknesses of password-based approaches
- Tradeoffs must be taken into account
- Great care should be taken in the design of systems that rely on static passwords

PKI

- Implementation and deployment details are key
- Centralized (public) CA can pose problems
  - Hard to do right
  - Trusted vs. authoritative CAs
  - User's certificates are linkable
- User education and interfaces critical
- Limited context PKIs pose fewer privacy concerns

Limited Context PKI

- Each verifier (or related group of verifiers) has its own CA
- Avoids many of the harder issues of user identification; revocation
- Harder to cross-link across applications

Therefore:

- Many problems that appear intrinsic to PKI derive from the scope of the specific PKI
- Limits in scope will simplify deployment and limit adverse privacy effects
- Public CAs and trusted third parties represent significant privacy concerns

Biometrics

- Effectiveness depends on context+
- Revocation is not possible
  - Better if kept very local
- Remote authentication with biometrics may be problematic
  - Remote verifier simply sees a string of bits

CSTB · Computer Science and Telecommunications Board

Biometrics Guidelines

- Avoid remote enrollment or re-enrollment
- Biometrics linked to name or other identifying info can reveal your identity
- Biometrics cannot be reissued if stolen or sold
- Exception-handling mechanisms are needed
- User control of templates is most privacy-sensitive
- Currently, biometrics not useful for tracking people

CSTB • Computer Science and Telecommunications Board

Therefore:

- Biometrics hold promise with regard to user convenience
- Can pose privacy and security risks if implemented poorly
  - If servers are used to compare against stored templates
- Local contexts are best
- Biometrics should not be used to authenticate via templates on remote servers

CSTB • Computer Science and Telecommunications Board

Design Stage -- Multiple Points at which Privacy is Affected

1. Authentication, generally
2. Choice of Attribute – if attribute required
3. Selection of Identifier – if identifier required
4. Selection of Identity – if identity required
5. The Act of Authentication

- These are just in the design stage, *before* transactional data collection, linkage, secondary use issues, etc.

Chapter 7's toolkit describes each of these in detail

Example: Attribute Choice Affects Privacy

- Informational privacy
  - Distinctive vs. more general
  - Minimize disclosure
  - Ensure data quality
  - Avoid widely-used attributes
- Decisional – If sensitive, may impinge on willingness
- Bodily integrity – If requires physical collection, may be invasive
- Communications – If attribute reveals address, phone, network

Additional Issues

- When is authentication really necessary?
- Secondary use of identifiers
  - Without original system limits in mind, usage can become highly inappropriate
  - This can lead to privacy and security problems, compromise original mission, and generate additional costs
- Explicit recognition of the appropriateness of multiple identities for individuals
- Usability
  - Design systems with human limits in mind!
  - Employ user-centered design methods
- Identity theft as a side effect of authentication system design choices

CSTB · Computer Science and Telecommunications Board

Major Findings/Recommendations

- Context, scope, implementation matter greatly
- Local contexts/uses usually more privacy-sensitive
- Secondary uses are particularly problematic
- Toolkit for thinking through design is provided
- Checklist for evaluating/designing authentication systems is presented

Government's Unique Role

- Regulator, Issuer of identity documents, Relying Party
- Unique Relationship with Citizens
  - Many transactions are mandatory
  - Agencies cannot choose their markets
  - Relationships can be cradle-to-grave
  - Individuals may have higher expectations for government
- Provider of Services
  - A common identifier may be in tension with principles of Privacy Act

Foundational Documents Pose Risks

- Many of these documents are very poor from a security perspective
  - Diverse issuers
  - No ongoing interest on part of issuer to ensure validity/reliability
- Birth certificates are particularly poor
  - Should not be sole base identity document

CSTB • Computer Science and Telecommunications Board

Ideally…

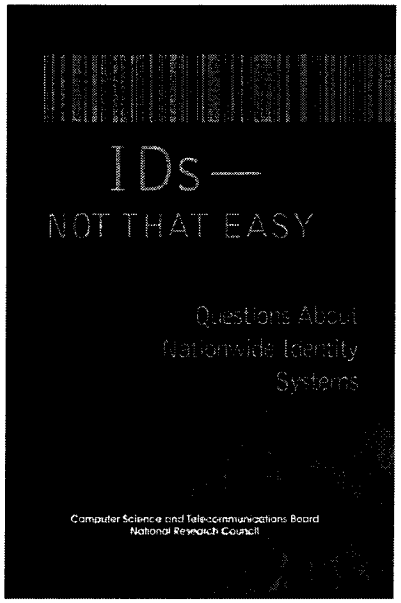
- Authentication systems should not infringe on autonomy and expression
- Systems that facilitate multiple identities are better
  - Anonymous interactions should be preserved whenever possible
- Designers and implementers should respect informational, bodily integrity, communications, and decisional privacy
- Linkage and secondary uses should be minimized
- Studied attention needed to avoid erosion of privacy

CSTB · Computer Science and Telecommunications Board

When Designing a Privacy-Sensitive Authentication System:

- Authenticate only for necessary, well-defined purposes
- Minimize the scope of data collected
- Minimize the retention interval of data collected
- Articulate what entities will have access to the collected data
- Articulate what kinds of access to and use of the data will be allowed
- Minimize the intrusiveness of the process
- Overtly involve the individual to be authenticated in the process
- Minimize the intimacy of the data collected
- Ensure that the use of the system is audited and that the audit record is protected against modification and destruction
- Provide for individuals to check on and correct information held and used for authentication

CSTB · Computer Science and Telecommunications Board



As for Nationwide Identity Systems…

- Driver's licenses are a nationwide identity system
- The challenges are enormous
  - Inappropriate linkages and secondary use likely without restrictions
- Biometrics databases and samples would need strong protection
- Any new proposals should be subject to analysis here and in *IDs—Not That Easy*

Overall Assessment

- Care must be taken to assess the privacy implications of authentication systems
  - Privacy, like security, far from optimal in most systems
  - Need appropriate incentives
- Design and implementation choices weigh heavily on the privacy impact of authentication systems
- No easy answers or panaceas – very context- and system-dependent

CSTB · Computer Science and Telecommunications Board

Follow-Up

- **http://cstb.org/**
  - description of the project: http://cstb.org/project_authentication
  - the report
- Obtaining a hardcopy version of the report
  - http://www.nap.edu
  - or contact lmillett@nas.edu