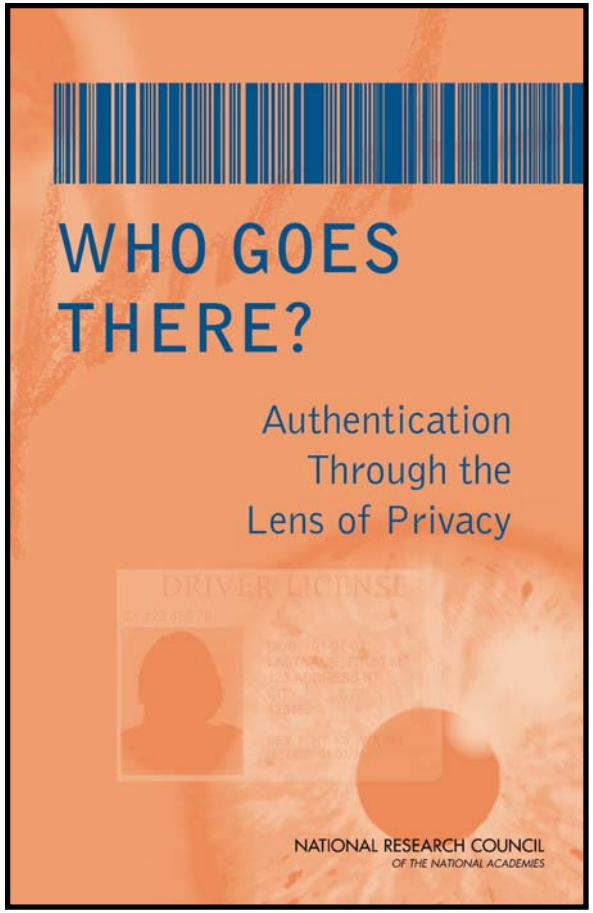

Who Goes There? Authentication Through the Lens of Privacy

Committee on Authentication Technologies and Their Privacy Implications

Computer Science and Telecommunications Board
The National Academies
Washington, D.C.
http://cstb.org/

CSTB • Computer Science and Telecommunications Board

THE NATIONAL ACADEMIES
Advisers to the Nation on Science, Engineering, and Medicine

Study Committee

Stephen T. Kent, ***Chair***
BBN Technologies

Michael Angelo
Compaq Computer Corporation

Steven M. Bellovin
AT&T Labs Research

Bob Blakley
IBM

Drew Dean
SRI International

Barbara Fox
Microsoft Corporation

Stephen H. Holden
University of Maryland, Baltimore County

Deirdre Mulligan
University of California, Berkeley

Judith S. Olson
University of Michigan

Joe Pato
Hewlett Packard Labs

Radia Perlman
Sun Microsystems

Priscilla Regan
George Mason University

Jeffrey Schiller
Massachusetts Institute of Technology

Soumitra Sengupta
Columbia University

James Wayman
San Jose State University

Daniel J. Weitzner
W3C/Massachusetts Institute of Technology

Lynette I. Millett, *Study Director (CSTB)*
Jennifer M. Bishop, *Sr. Project Assistant (CSTB)*

Study Process

- March 2001 launch meeting
- Briefings, deliberations at 7 plenary meetings in 2001-2002
- Issuance of extraordinary report on nationwide identity systems in April 2002: *IDs—Not That Easy*
  - Self-initiated (committee and CSTB) after 9/11/01
  - Called "A must read for anyone involved in the debate." – Bruce Schneier
- Consensus development
- Blind peer-review process (12 reviewers + CSTB)
- Writing, rewriting, rewriting, and rewriting
- NRC approval

Motivations

- Authentication ever more ubiquitous
  - Both for business and government
- Privacy a growing concern in general
- Committee asked to look at how authentication technologies affect privacy
- Note that *affecting* privacy is not always a *violation* of privacy

Overview

- Terminology is central (making analysis abstract):
  - Agreed-upon terminology is critical for productive discussion
  - Inconsistent usage confuses the issue
  - Terms are not as they seem colloquially
  - Authentication is not a simple concept
- Technologies subordinate to system choices and policies
  - Some choices more privacy-problematic than others
- Government has unique role(s)
- As noted in the committee's interim report: It's not that easy.

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
- Toolkit includes checklist for evaluating/designing authentication systems

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

System Considerations

- In all cases, design and implementation choices affect efficacy and privacy issues related to authentication
- Understand the threat model and why authentication is being used
- The base technology (biometrics, PKI, smartcards, etc.) matters less than how it is deployed within a larger systems context
- The broader the scope of the system, the greater the potential privacy impact
  - Bulk compromise of private information used in large-scale system can have large-scale adverse effects

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

Assessing Privacy Implications of Authentication Systems

- Toolkit with checklist of questions around four big design decisions
  - Attribute Choice
  - Identifier Choice
  - Identity Selection
  - Authentication Phase
- Examine each decision against the four types of privacy implications
  - Information privacy
  - Bodily integrity
  - Decisional privacy
  - Communications privacy

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

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

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