IDentity and Trust in Context

Peter G. Neumann
Principal Scientist
SRI International ComputerSciLab
Menlo Park, CA 94025-3493
Neumann@CSL.sri.com
http://www.csl.sri.com/neumann
Telephone 1-650-859-2375
IDes+2 of April 2009, NIST

Outline of This Talk

- The overall context
- Global-scale ID management
- Assessable ID/privacy protection
- Health-care as an example
- Attribute-based encryption
- Attribute-based messaging
- Lattice-based cryptography
- References, URLs, `search words`

IDentity

Something that identifies a person (or class of persons, or process, or piece of hardware, or other computer-related entity) – but not necessarily uniquely.

IDtrust and Trustworthiness

'IDtrust' begs the question: Why trust authentication systems/IDs? Because it's easy? Alternatives are not user-friendly? I'm not paranoid?

Trustworthiness of mechanisms, systems, and people on which you must depend is very important, but difficult to ensure. Risks: errors, ID fraud, spoofing, ... [References]

IDeals and IDylls

In the myth of perfect security, our beliefs are often misplaced. Perfect security does not exist. Instead, we tend to have:

- IDeology: Faith-based security
- IDolatry: Worship of physical security rather than systemic and operational security.

IDiomatic?

Psychoanalytic terms (IDentity types)

- ID: completely unconscious division of the psyche (users!)
- EGO: organized conscious mediation (administrators!)
- SUPEREGO: partially conscious morality/conscience/guilt/... (privacy advocates!)

The Basic IDea

We need holistic total-system trustworthy identity management. IDeally, IDentities should relate to strong system authentication, fine-grained authorization, nonsubvertible accountability, real-time and post-hoc analysis, remediation, revocation, and more.

IDealization

We need to mask underlying complexity to make IDs and ID management more usable – with abstraction, encapsulation, invisible encryption/hash functions, virtualization, sensible interfaces, judicious use of anonymization, and much more.

IDiosyncrasies

Characteristic peculiarities must be accommodated. "One size fits all" is not practical, with many special cases: long names, hyphenated names, foreign languages, alternative spellings non-ASCII characters, ambiguities, false positives/negatives, and much more. Beware of oversimplification!

IDiots and IDleness

- IDiot: Typically, an attribute associated with someone blamed for misusing a dysfunctional human interface or who is dysfunctional.
- IDleness: Inaction that may result in serious risks, typified by laziness with respect to security practices.

IDeograms

IDeograms are symbolic but not literal representations, useful for identification (candidate or party icons in elections), CAPTCHAs (for confirmations), authentication. Caveats: dyslexia, prosopagnosia (face-blindness), other disabilities, user unfriendliness, ...

Global-Scale ID Management

ID management, authentication, authorization, accountability must

- adapt to continual change
- transcend local identities
- transcend centralized control
- transcend untrustworthy systems
- transcend untrustworthy people
- avoid conflicts and ambiguities
- scale to large heterogeneity

Roadmap for Global ID Management

Doug Maughan's R&D roadmap for cybersecurity addresses GIDM as one of 11 hard problems, holistically synergistic with the other 10: scalable trustworthiness, metrics, evaluation life-cycles, insider threats, malware, system survivability, situational awareness, provenance, privacy-aware security, usability.

Assessable IDentity and Privacy Protection

Dartmouth-I3P-funded joint project:

- MITRE (PI Bruce Bakis) *
- Cornell University
- Georgia Tech
- Purdue University *
- SRI International
- University of Illinois Urbana *

[* => project paper presented here.]

Some Health-Care Challenges

Patient and personnel identification, authentication, authorization, accountability; correct up-to-date medical histories; network/system/ data security, integrity, privacy; controlled data access for insurance, medication, research, and analysis.

Health-Care Risks

- System and information misuse; wrong IDs, privacy violations, mal-practice, ... (http://www.risks.org).
- Computer-centric doctors may cause patient depersonalization. (See The Computer Will See You Now, Anne Armstrong-Cohen, *The New York Times,* March 6, 2009, risks-25.60).

Health-Care Risk Avoidance

- Trustworthy systems are essential, but privacy is largely extrinsic. They demand pervasive oversight.
- Well-defined enforceable policies are essential.
- Attribute-based encryption might provide natural mappings between identities and role-based applications.

Attribute-Based Encryption (ABE)

ABE (Brent Waters et al.) involves IDs, role-based-like authorization with expressive access controls, practical usability, collusion resistance, simplifies key management, and is holistically well-suited to applications such as health care (21 papers since 2007). Search: `functional encryption Waters`

Attribute-Based Messaging (ABM)

- UIUC's ABM (Carl Gunter et al.) uses ABE. The messaging system constructively uses access-control attributes that can be systematically derived and automatically managed (10 recent papers). Search: `attribute messaging Gunter`

Lattice-Based Cryptography (LBC)

- LBC (Chris Peikert et al.), based on a problem other than factoring or discrete logs, seems resistant to quantum computing. Uses include strong public-key cryptography and a hash function SWIFFTX with provable properties: a NIST SHA-3 candidate (11 recent papers). Search: `Peikert`

Conclusion

- Local and global IDentities need trustworthy systems and networks with authentication, authorization, accountability, and much more. Enterprise architectures, system engineering, sound operational practices, usability, and people tolerance are all vital to reducing risks.

CSTB Trustworthiness/ID Reports

- NatlResCouncil, www.nap.edu:
  - Toward a Safer and More Secure Cyberspace, 2007
  - IDs Not That Easy: Questions About Nationwide Identity Systems, 2002
  - Trust in Cyberspace, 1998
  - Computers at Risk: Safe Computing in the Information Age, 1990

PGN IDentity Reference

- PGN, Security and Privacy in the Employment Eligibility Verification System (EEVS) ..., House Ways and Means Committee Subcommittee on Social Security, 7 Jun 2007. http://www.csl.sri.com/neumann/house07.pdf

Other Relevant PGN References

- Reflections on System Trustworthiness, Advances in Computing, volume 70, Academic Press, Elsevier, 269–310, 2007
- Principled Assuredly Trustworthy Composable Architectures, 2004: http://www.CSL.sri.com/neumann/chats4.html, .pdf, .ps

More PGN References

- **Holistic Systems,** *ACM SIGSOFT Softw.Eng.Notes,* **Nov. 2006**
  http://www.csl.sri.com/neumann/holistic.pdf
- **Computer-Related Risks, Addison-Wesley, 1995**
- **www.CSL.sri.com/neumann**
- **ACM Risks Forum, www.risks.org**

IDiographic Summary

IDentity
kIDstuff
epIDemic
accIDental
consIDerable
indivIDual
improvIDent
self-evIDent
unconsolIDated
IDeals, offset by
fIDelity and
avIDity slowed by
antIDotes with
fastIDiousness and
coincIDences but with
backslIDing, result in
nonconfIDence or else
overconfIDence!