Internet Architecture Board
Open IAB meeting
Seattle, 30 March 1994

AGENDA

- Bash the agenda,
- The status of the ISO liaison
- The IAB Workshop on
  Security in the Internet Architecture

Status of the ISO liaison:

- I2I@sophia.inria.fr:
  - Set up 13 December 1993,
  - 80 participants,
  - 300 messages,
  - the apparence of convergency.
- Meeting of JTC1, February 1994:
  - Agreed on class A liaison,
  - Between JTC1/SC6 and ISOC,
  - Need to prepare an MOU.
- First version of MOU:
  - Sent the 22 March to the I2I list,
  - Few comments received,
  - Second version sent 25 March.

What does the MOU say?

- Mutual Recognition of Standards:
  - Quote the other organization's work,
  - External reference, not "stamping",
  - Maintenance by the originator.
- Information on work programs:
  - Send list of working groups,
  - Complete with RFC, drafts, achievements,
  - Every 6 months.
- Information sharing
  - send list of publications,
  - place technical material on line, accessible.
- Collaborative efforts:
  - Joint meetings of WG allowed,
  - may hold joint workshops.

Security Workshop, Working group "1":

Christian Huitema, INRIA
Steve Bellovin, AT&T
Bob Braden, ISI
John Curran, NEARNET
Phill Gross, ANS
Stev Knowles, FTP Software
Barry Leiner, USRA
Paul Mockapetris, ISI
Yakov Rekhter, IBM
Dave Sincoskie, Bellcore

Summary of retreat:

- Look at proposed scenario,
- Investigate various avenues:
  - Authentication vs. Privacy
  - Privacy without authentication (TCP encryption option?)
  - Use of DNS.
- Reflexion on firewalls:
  - Authentication vs. Authorization,
  - Concur with other groups.
- Study the authentication service.

AN AUTHENTICATION SERVICE?

- Verify the origin of “message”:
  - One time passwords,
  - Access to a firewall..

  basis for “access control”, authorization.

- What shall we name:

domain names:	sophia.inria.fr
machine names:	jupiter.inria.fr
service names:	www.sophia.inria.fr
users:	huitema@sophia.inria.fr
processes:	p112.huitema@sophia.inria.fr
	p112.sophia.inria.fr

  URL:
  http//www.sophia.inria.fr:222/tmp/foobar

Authentication for access control:

- Access control lists:

huitema@sophia.inria.fr
*@sophia.inria.fr
*.inria.fr
*.fr

- Limits to wildcarding:

"member of the IAB?"

- The "distinguished name" approach:
  - An user has one name,
  - Capacities are attached to this name,
  - Cryptographic protections.
- The critic of distinguished names:
  - Validate the name,
  - Validate the "capacity"

  ⇒ requires 2 validations,

  ⇒ two entities to trust,

  ⇒ displays the name.
- A "credit card" alternative?

There is no such thing as a name:

- Users have multiple “credits”:
  - Several bank accounts,
  - Driver licence,
  - Frequent flyer,
  - professional ID,
  - Passport.
- User could have multiple names:
  - Only one validation,
  - Allows wild carding,
  - Allow more privacy.
- A name is a relation:

huitema@sophia.inria.fr
huitema@iab.isoc.org
123456789@cards.amex.com

- A relation is easier to check:
  - Only one name to check,
  - Top certificate is known,
  - Widcarding is easy.

Chosing your credential:

- One communications:
  - Many resources,
  - Different controls,
  - Different tokens, names.
- Cannot pass "all the credentials":
  - Too bulky (messages),
  - Too slow (walk through the list),
  - Too informative (privacy).
  - Need to chose a name:
    - By the user?
    - Resource manager advertize its list?
    - A generic problem of path finding.
- Start with one name only?

Designing the authentication service:

- What is the form of names?
  - X.500 Distinguished names:
    - * Bulky, No name service, Ugly..
  - DNS names:
    - * Too short, alphabet soup..
- What technology should we use:
  - Public keys and certificates:
    - * Patented, computing requirement.
    - * Recent annouces by RSADIR?
  - Symmetric keys (DES, MD5):
    - * No protection against repudiation,
    - * Real time message exchanges.
  - Authentication only (export contol).
- What kind of networking architecture:
  - Rooted hierarchy (as in PEM):
    - * Difficult to deploy, "big brother"..
  - Bottom up growth (as in PGP):
    - * The "friends and family" of security
- Need one working group, maybe two.