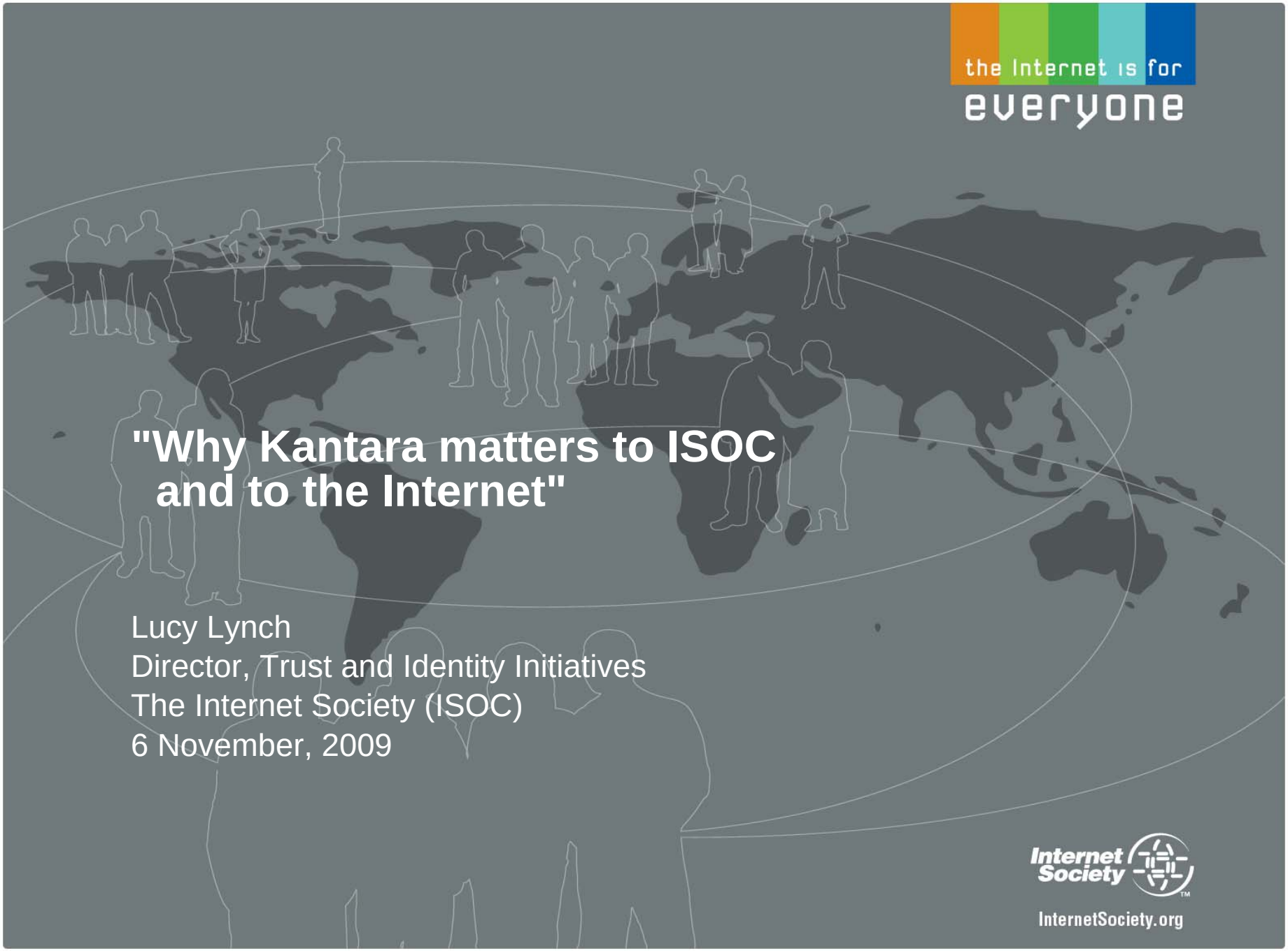


"Why Kantara matters to ISOC and to the Internet"

Lucy Lynch
Director, Trust and Identity Initiatives
The Internet Society (ISOC)
6 November, 2009

Internet Society
InternetSociety.org

Congratulations!

As participants in the Kantara Japan effort you are now helping to address some of the hardest and most persistent problems in the history of the Internet.

In my talk today I will:

- Provide some historical background
- Outline the Internet Society's interests
- Show how the Kantara Initiative can help
- Connect Identity to the continued success of the global Internet

My story is about Trust and the Internet

To understand why we are still working on enabling trust in our networks, we need to understand why trust was “left out” by the early designers.

The short answer is that in the 1960s computing was a very expensive undertaking and access to machines was limited to a small, well educated set of individuals. Access was granted by organizations who already had a strong system of user management controls in place. In other words:

Trust was implemented externally!

There were early causes for concern

In October 1967 a Task Force was organized by the Advanced Research Projects Agency (now the Defense Advanced Research Projects Agency) to study and recommend appropriate computer security safeguards for protecting classified information in multi-access, resource-sharing computer systems.

- W. Ware, ed. "*Secure Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security*", RAND Corporation, Santa Monica, CA, 11 February, 1970

- The report pre-dates the ARPANET and is focused on security for single systems.

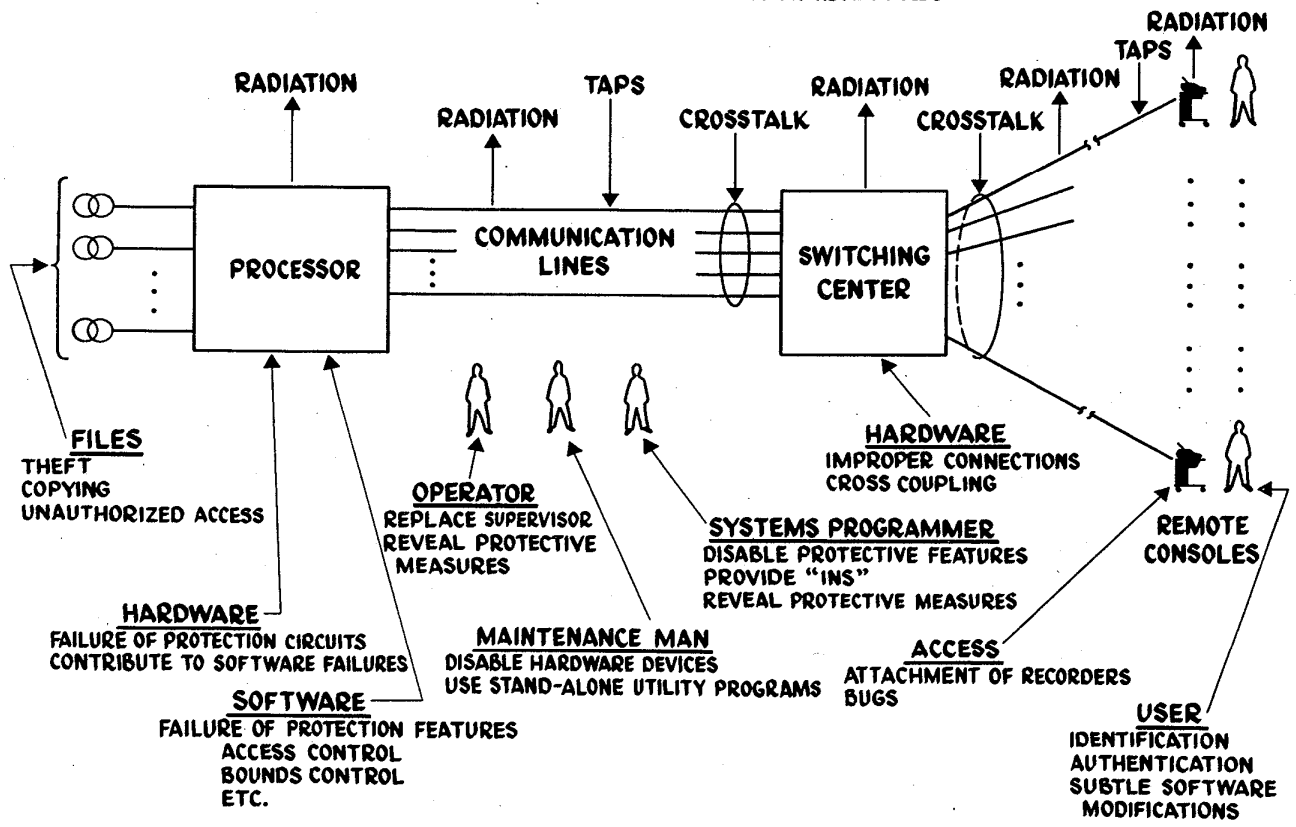

COMPUTER NETWORK VULNERABILITIES
RADIATION
RADIATION
TAPS
CROSSTALK
RADIATION
CROSSTALK
RADIATION
TAPS
RADIATION
PROCESSOR
COMMUNICATION LINES
SWITCHING CENTER
FILES
THEFT
COPYING
UNAUTHORIZED ACCESS
OPERATOR
REPLACE SUPERVISOR
REVEAL PROTECTIVE MEASURES
HARDWARE
IMPROPER CONNECTIONS
CROSS COUPLING
SYSTEMS PROGRAMMER
DISABLE PROTECTIVE FEATURES
PROVIDE "INS"
REVEAL PROTECTIVE MEASURES
REMOTE CONSOLES
HARDWARE
FAILURE OF PROTECTION CIRCUITS
CONTRIBUTE TO SOFTWARE FAILURES
MAINTENANCE MAN
DISABLE HARDWARE DEVICES
USE STAND-ALONE UTILITY PROGRAMS
ACCESS
ATTACHMENT OF RECORDERS
BUGS
SOFTWARE
FAILURE OF PROTECTION FEATURES
ACCESS CONTROL
BOUNDS CONTROL
ETC.
USER
IDENTIFICATION
AUTHENTICATION
SUBTLE SOFTWARE MODIFICATIONS

Figure 3

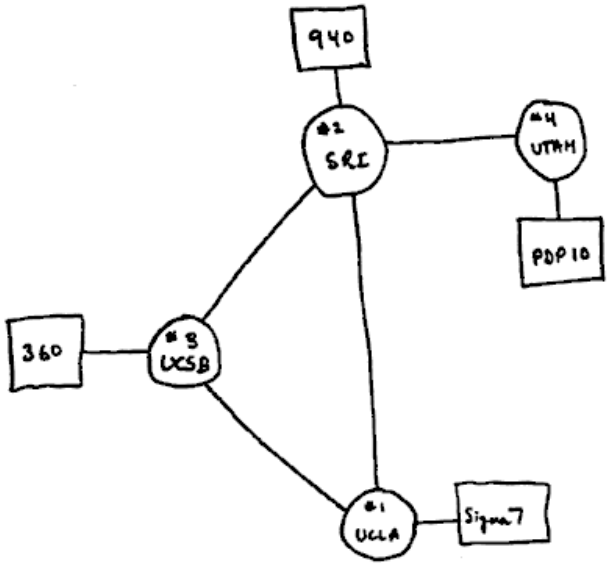
Key finding (and still true today)

- Contemporary technology can provide a secure system acceptably resistant to external attack, accidental disclosures, internal subversion, and denial of use to legitimate users for a closed environment.

- Contemporary technology cannot provide a secure system in an open environment, which includes uncleared users working at physically unprotected consoles connected to the system by unprotected communications.

- It is unwise to incorporate classified or sensitive information in a system functioning in an open environment unless a significant risk of accidental disclosure can be accepted.

Interconnection brought additional complexity



The ARPANET –

40 years ago the first packets were transmitted on 29 October, 1969 between UCLA and SRI.

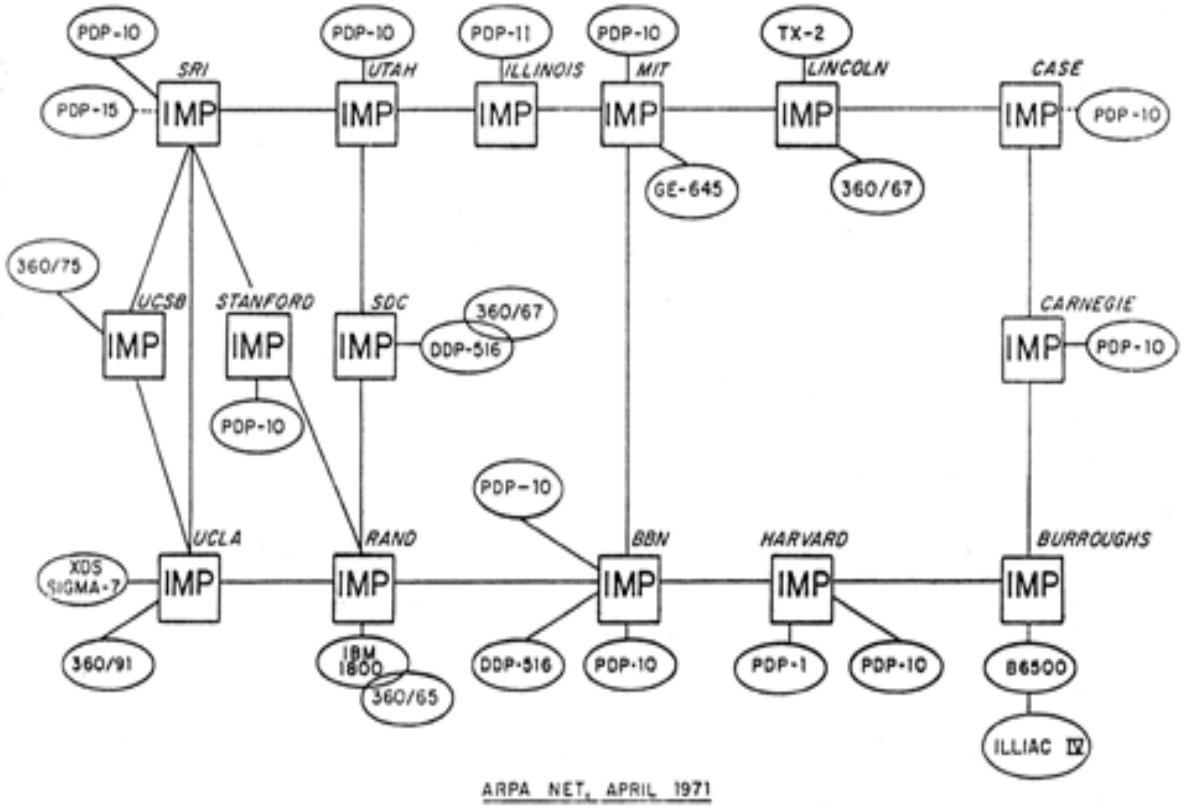
The start of the RFC series

Early ARAPNET documentation becomes the foundation for the Internet Engineering Task Force (IETF)

- RCF 1: Host Software (7 April 1969)
  - Establishing a connection
  - Focus is on interoperability and shared code

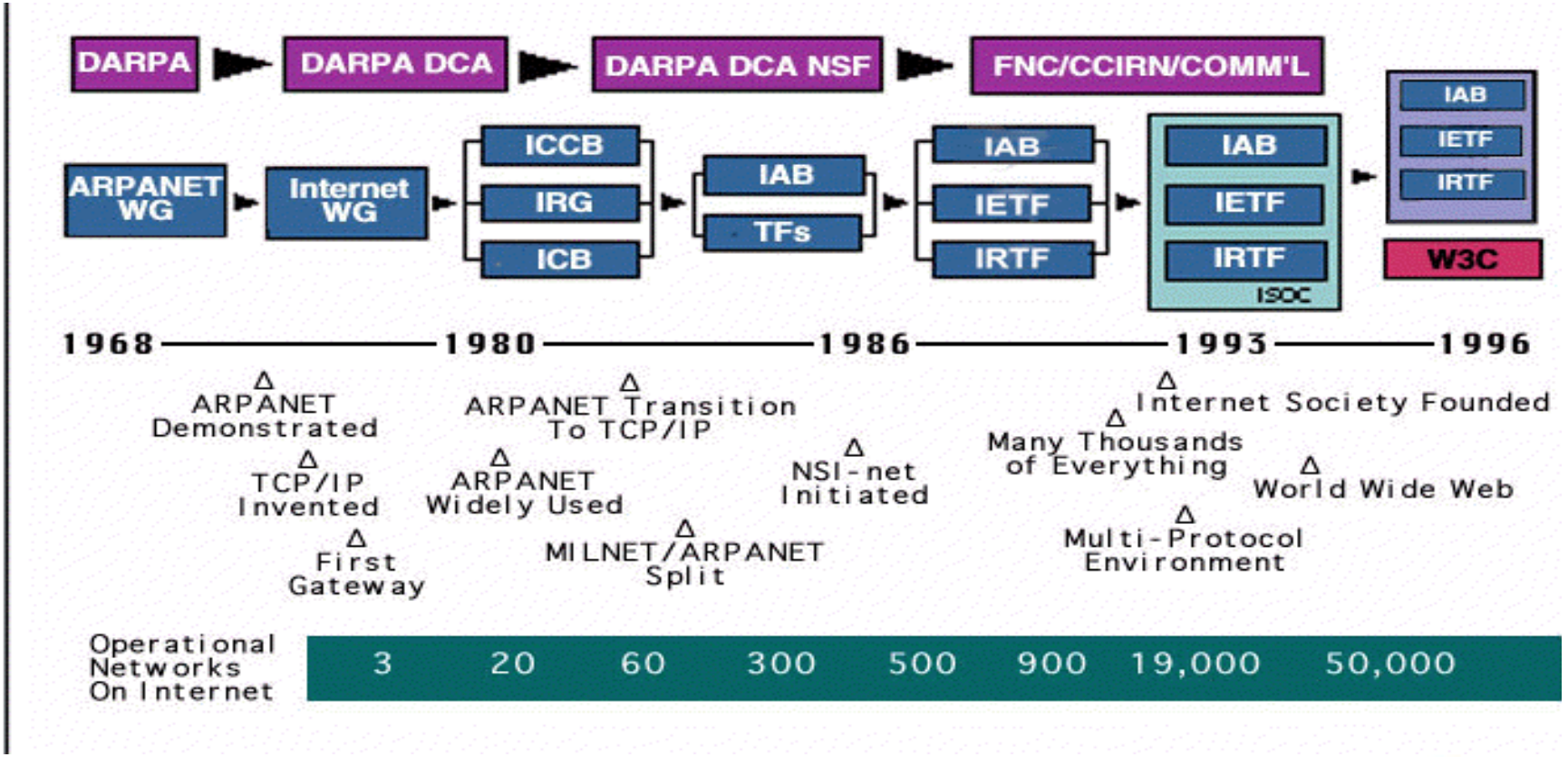
- RFC 76: Connection-By-Name: User-Oriented Protocol (28 October 1970)
  - “An important characteristic of most of the users at our Center is a lack of sophistication about data communication techniques and practices. The user will eventually be in the majority of those using the network from all nodes but the problem is ours, almost from the start.”

And growth, even before TCP/IP



ARPA NET, APRIL 1971

A long period of development led to...



A global networks of networks

The Internet is the world-wide network of interconnected computer networks (e.g., commercial, academic and government) that operates using a standardized set of communications protocols called TCP/IP (transmission control protocol/Internet protocol) or the Internet protocol suite.

An internet (spelled with a lower case i) is a network that is composed of a number of smaller computer networks. The Internet (spelled with an upper case I) is an internet that is vastly larger than any other internet and can be considered to be the ultimate internet; it connects thousands of networks and hundreds of millions of computers throughout the world.

http://www.linfo.org/internet.html

Security comes late in the process

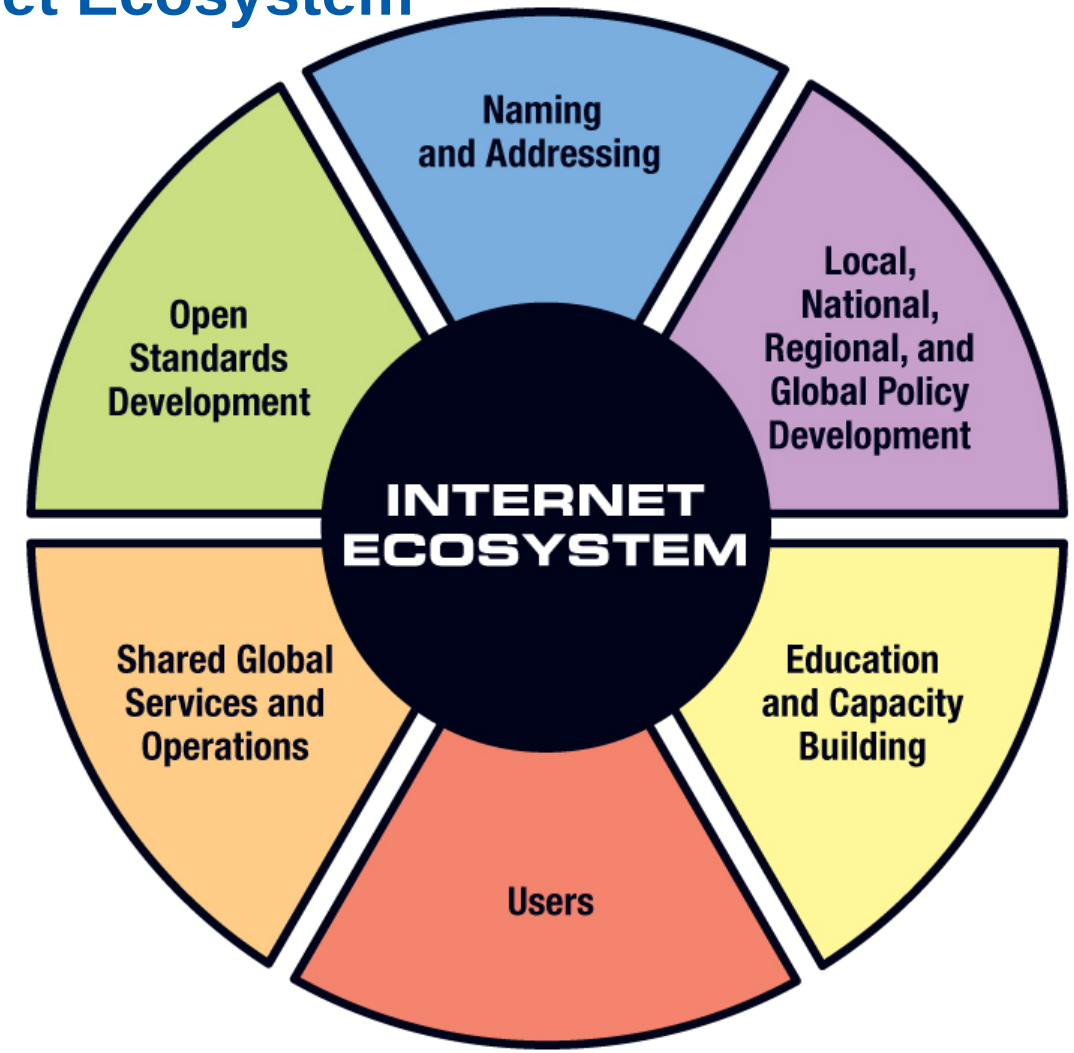
RFC 1281: Guidelines for the Secure Operation of the Internet (November 1991)

- "Each participating network takes responsibility for its own operation. Service providers, private network operators, users and vendors all cooperate to keep the system functioning."

- "It is important to recognize that the voluntary nature of the Internet system is both its strength and, perhaps, its most fragile aspect."

- Security Considerations
  - "If security considerations had not been so widely ignored in the Internet, this memo would not have been possible."

Internet Ecosystem



Internet Society
InternetSociety.org

The Internet Society

- The Internet Society (ISOC) is a nonprofit organization founded in 1992 to provide leadership in Internet related standards, education, and policy. With offices in Washington D.C., USA, and Geneva, Switzerland, it is dedicated to ensuring the open development, evolution and use of the Internet for the benefit of people throughout the world.

- The Internet Society provides leadership in addressing issues that confront the future of the Internet, and is the organizational home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB).

Activities are driven by the following principles:

- Open, unencumbered, beneficial use of the Internet.
- Self-regulated content providers; no prior censorship of on-line communications.
- On-line free expression is not restricted by other indirect means such as excessively restrictive governmental or private controls over computer hardware or software, telecommunications infrastructure, or other essential components of the Internet.
- Open forum for the development of standards and Internet technology.

ISOC principles continued

- No discrimination in use of the Internet on the basis of race, color, gender, disability, language, religion, political or other opinion, national or social origin, property, birth, or other status.
- Personal information generated on the Internet is neither misused nor used by another without informed consent of the principal.
- Internet users may encrypt their communication and information without restriction.
- Encouragement of cooperation between networks: connectivity is its own reward, therefore network providers are rewarded by cooperating with each other.

The ISOC Trust and Identity Initiative

- The Internet Society's Trust and Identity initiative recognises that in order to be trusted, the Internet must provide channels for secure, reliable, private, communication between entities, which can be clearly authenticated in a mutually understood manner. The mechanisms that provide this level of assurance must support both the end-to-end nature of Internet architecture and reasonable means for entities to manage and protect their own identity details.

- A trusted Internet takes into account security, transaction protection, and identity assertion and management. Trust must be a primary design element at every layer of the architecture, and in some cases, existing elements may need to be redesigned or improved to meet emerging requirements.

The Initiative includes three programs

- Identity and Trust:
  - Elevating "Identity" to a core issue in network research and standards development
- Architecture and Trust:
  - Implementing open trust mechanisms throughout the full cycle of Internet research, standardization, development and deployment
- Operationalizing Trust:
  - Mitigating the social, policy, and economic factors that may hinder development and deployment for trust enabling technologies

Goals for the Trust and Identity work

- End users understand their options for identity management and demand appropriate tools and services to support the full range of use cases.
- Developers think in terms of trust, interaction, and sustaining global reach (end-to-end) when designing the next generation of reliance technologies and standards.
- ISOC continues to support the open, transparent, bottom up nature of Internet development and is an active partner in the standards process as the Internet Model expands.
- ISOC acts as a primary advocate for architectural issues that support and increase the value of the Internet as well as an active promoter of "best current practices" for the deployment of key Internet technologies.

ISOC's entry into the Identity community

- Throughout 2008 ISOC worked to build a strong technical and social foundation in the identity sphere.
- We partnered with Internet 2, Liberty Alliance, and the Identity Commons on small projects and worked to expand those relationships.
- We pursed a course of broad-based technical and community engagement to increase our own understanding of “User Managed Identity”.
- We followed with interest the early efforts by Liberty Alliance to transform their organization into a more inclusive home for “identity layer” work.

We found a rich identity layer

But something was missing

There was no clear unified voice for Identity.

ISOC concluded that:

- Liberty's proposed IDTBD structure appeared to have a good chance of achieving a stable, inclusive, neutral base for identity technologies to address a wider audience.

- The core principals outlined for the new organization were well aligned with ISOC values.

- In December of 2008 ISOC joined the Liberty Alliance Management Board in order to support the transition to what would become the Kantara Initiative

ISOC and the Kantara Initiative today

In addition to our continuing role on the Management Board, ISOC staff have been active in the Leadership Council, individual Working Groups, and in project funding. Our participation allows ISOC to help support the organization in ways that:

- encourage and support new entrants, especially from some of the more open communities,
- shelter interesting work from small projects that will need access to both an organizational structure and funding,
- encourage and promote interoperability, and
- provide a unified voice on identity questions from those outside the current development sphere.

Kantara participant interests include:

Kantara Japan:

- Japan (DG and WG)

Discussion Groups:

- Concordia
- Identity Community Update

Working Groups:

- Clients
- Consumer Identity
- eGovernment

Working Groups (cont.)

- Health Identity Assurance
- Identity Assurance
- IdP Selection
- ID-WSF Evolution
- Information Sharing
- Privacy and Public Policy
- Universal Login Experience
- User Managed Access

Many hard problems still to tackle

Although a significant amount of technical work has been done in the last ten years there are still a number of Identity management issues that are poorly understood and in many cases left untouched.

Some examples:

- The business case for the Identity Provider (IdP)
- Inter-federation and reconciliation of regional policy
- User consent, data portability, transparent terms
- Levels of assurance
- Reputation, repudiation, and remediation

Adoption will be user driven

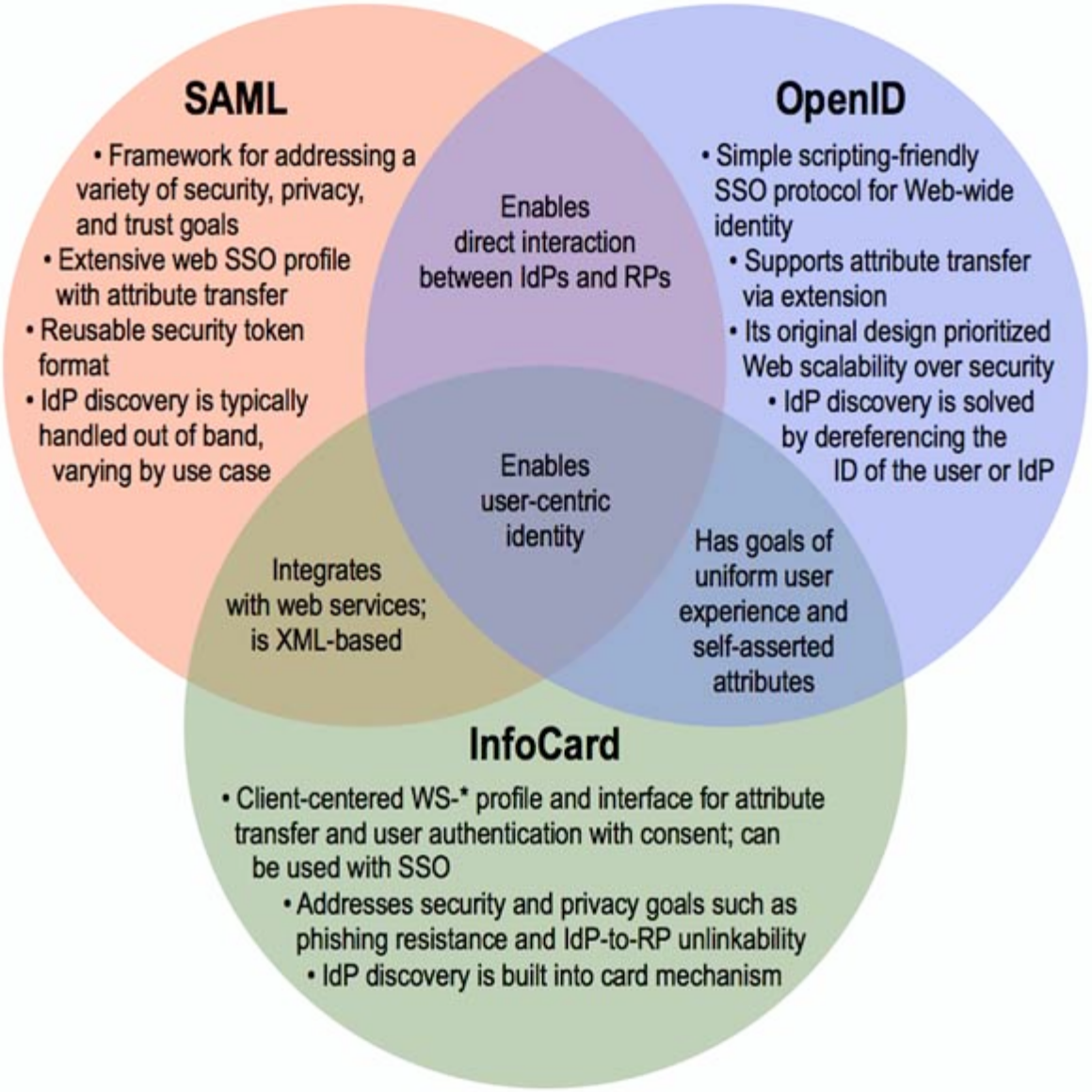
None of the existing Identity solutions has achieved Internet scale deployment. User understanding and education are needed and technologists must recognize that users often have conflicting goals.

Users want:

- Persistence (and a customized experience)
- Consistency (applications are predictable)
- Simplicity (and will trade security for convenience)
- Clarity (limited options requiring judgment)
- Safety (shielded from natural consequences)
- Versatility (anonymity, pseudonymous, strong privacy)

A test: Can we have multiple Identity solutions...

- SAML (OASIS)
  - exchanging authentication, authorization and related data, generally between secured domains
- OpenID (OpenID Foundation)
  - decentralized standard for authentication, primarily for access control
- OAuth (IETF)
  - distributed, secure API-style authorization for access to services and data over HTTP
- InfoCards (Information Card Foundation)
  - user-centric authentication, authorization and attribute exchanging, focus on privacy



Legend

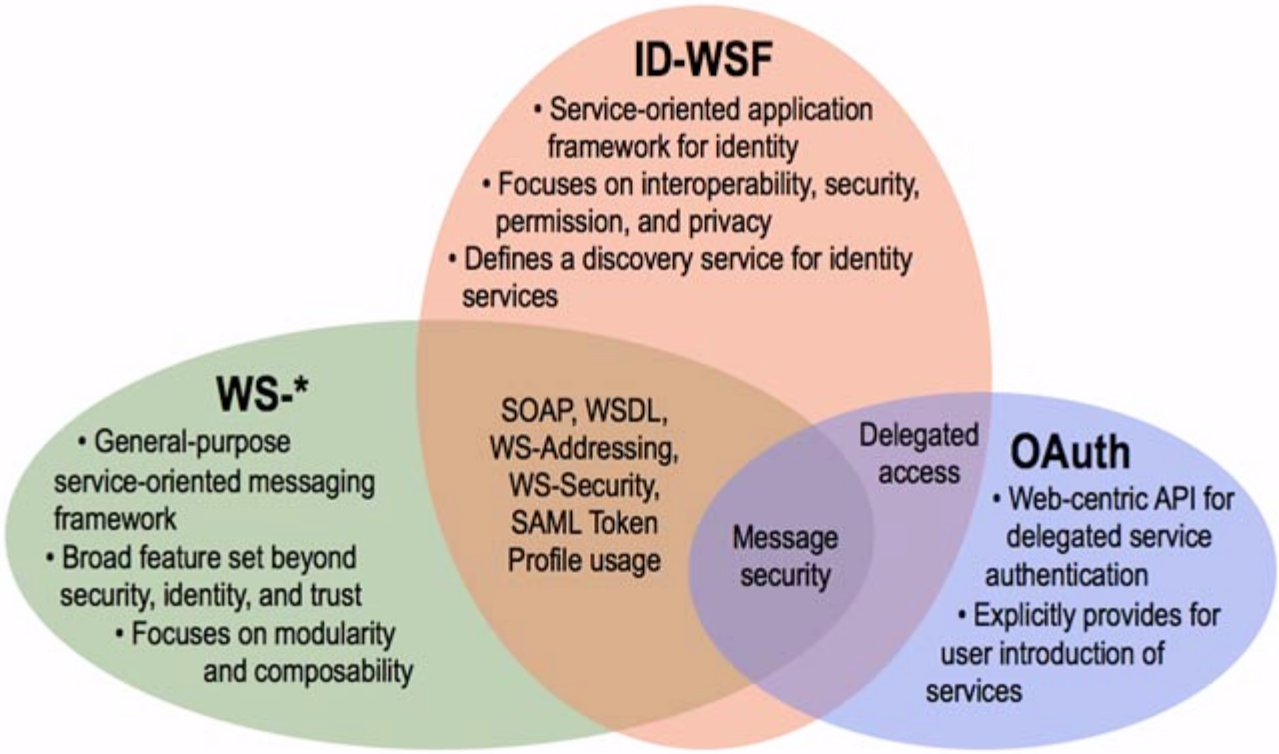
IdP	Identity provider
RP	Relying party
SSO	Single sign-on

The Venn of Identity

September 2009

Eve Maler – VennOfIdentity.org

Acknowledgments: Gary Ellison, Johannes Ernst, Paul Madsen, Jeff Hodges, Ashish Jain, many others



Eve Maler – October 2009 – VennOfIdentity.org

Acknowledgments: Paul Madsen, Domenico Catalano

And accomplish the Kantara mission?

"To foster identity community harmonization, interoperability, innovation, and broad adoption through the development of open identity specifications, operational frameworks, education programs, deployment and usage best practices for privacy-respecting, secure access to online services."

My answer?

Only by recognizing that each of these technologies can be used to address some (but not all) of the Identity problems. Given the number of hard problems still in front of us, cooperation is vital.

Trust is essential to the Internet

For 2010 ISOC has committed itself to the active promotion of network confidence through the development of open standards, technologies, applications, and policies that engender trust in networked environments.

Trust is not just a technical problem, it is a human problem as well and the Identity layer makes the perfect laboratory to test solutions that address both realms. It is our hope that the lessons learned at the Identity layer will also be useful when addressing security, policy, and deployment issues within the network.

We see Kantara as a important and strategic partner in the on-going effort to build trust into the Internet.

Questions?

the Internet is for everyone

InternetSociety.org

info@InternetSociety.org

Internet Society

References:

the Internet is for everyone

The Computer History Museum
http://www.computerhistory.org/

Early Computer Security Papers
http://csrc.nist.gov/publications/history/

IETF Documents:
http://tools.ietf.org/html/

Cooperative Association for Internet Data Analysis
http://www.caida.org/home/

The Kantara Initiative wiki:
http://kantarainitiative.org/confluence/

Eve Mahler on the Venn of Identity
http://www.xmlgrrl.com/blog/categories/venn/

Internet Society
InternetSociety.org

- **Confidence**
  - *noun* 1. the belief that one can have faith in or rely on someone or something. 2. self-assurance arising from an appreciation of one's abilities. 3. the telling of private matters or secrets with mutual trust. 4. a secret or private matter told to someone under a condition of trust.
    - http://www.askoxford.com/concise_oed/

The Internet Society is an international cause-related organization that works for the open development and evolution of the Internet for all people. We do so through work across the areas of technical standards, education, and capacity-building, as well as public policy.

Internet Society

InternetSociety.org

IPv4 & IPv6
INTERNET TOPOLOGY MAP
JANUARY 2009

AS-level INTERNET GRAPH