Collaborative Security

Reflections about Security and the Open Internet

NLUUG Najaarsconferentie 2015
19 November 2015

independent source of leadership for Internet policy, technology standards, and future development

Mission: To promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world.

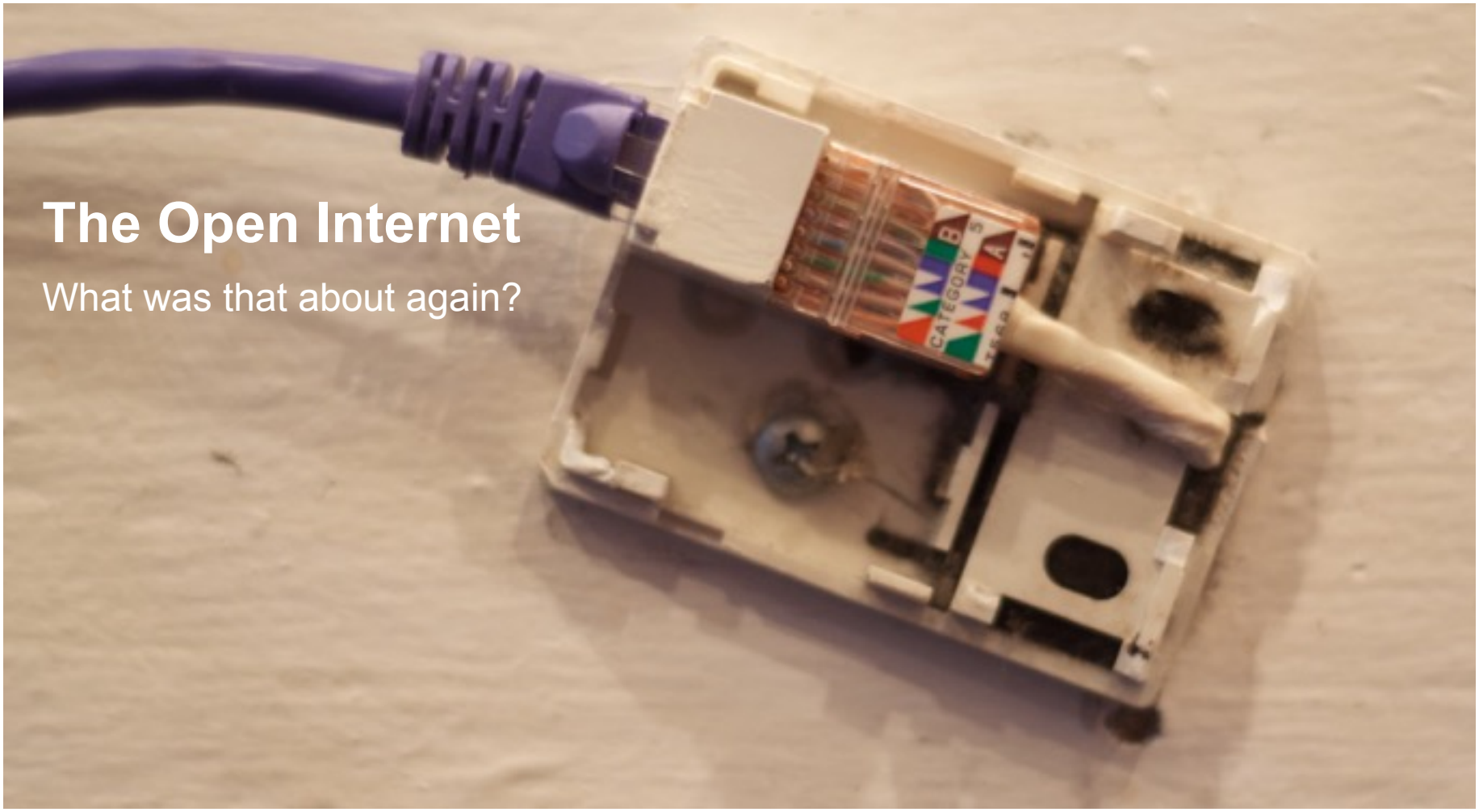
Founded in 1992 by Internet Pioneers

Global and Inclusive

Independent and Not-for-Profit

Organizational home for the IETF

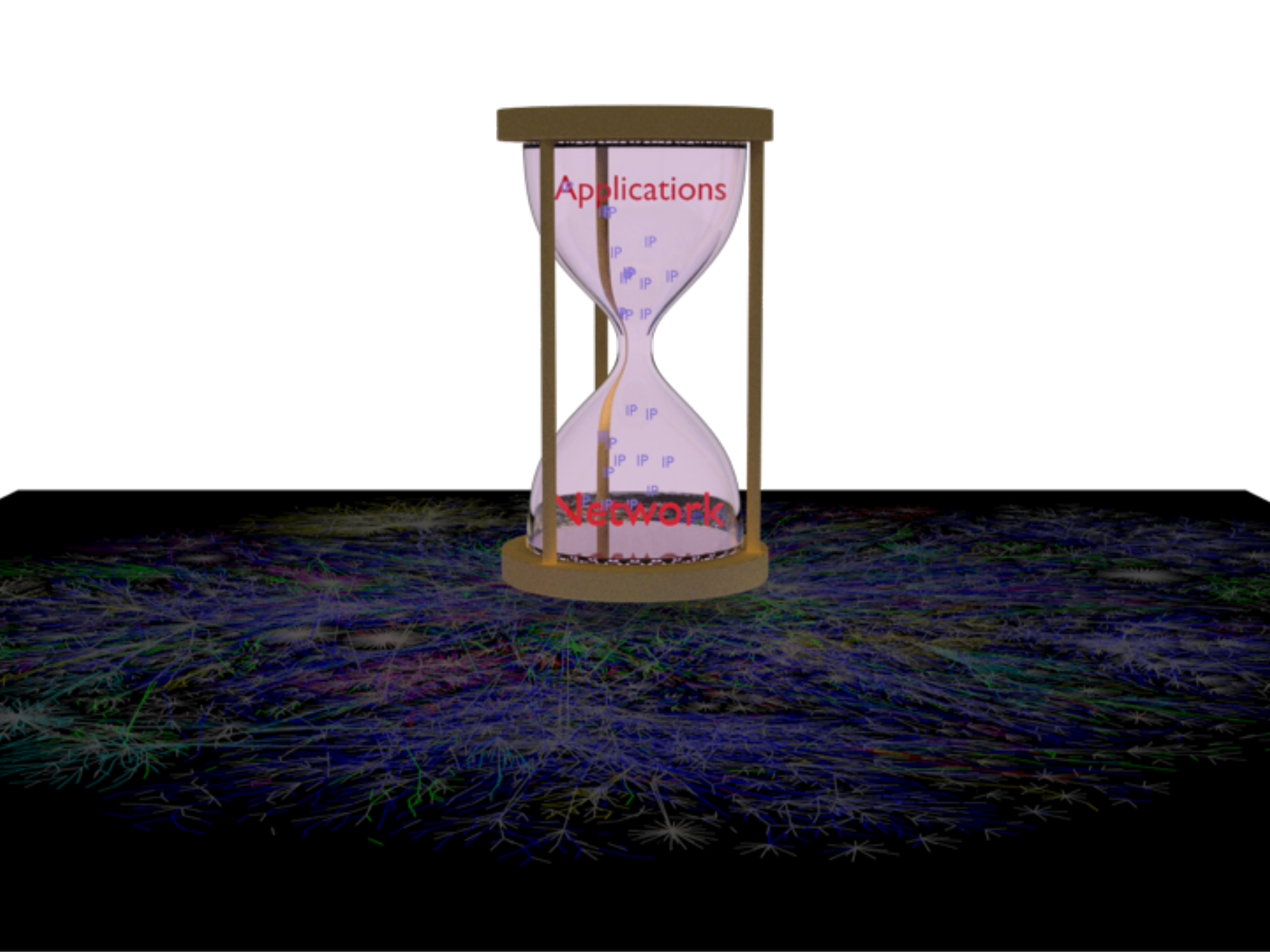
http://www.internetsociety.org/get-involved/individuals



The Open Internet

What was that about again?

Internet Society™

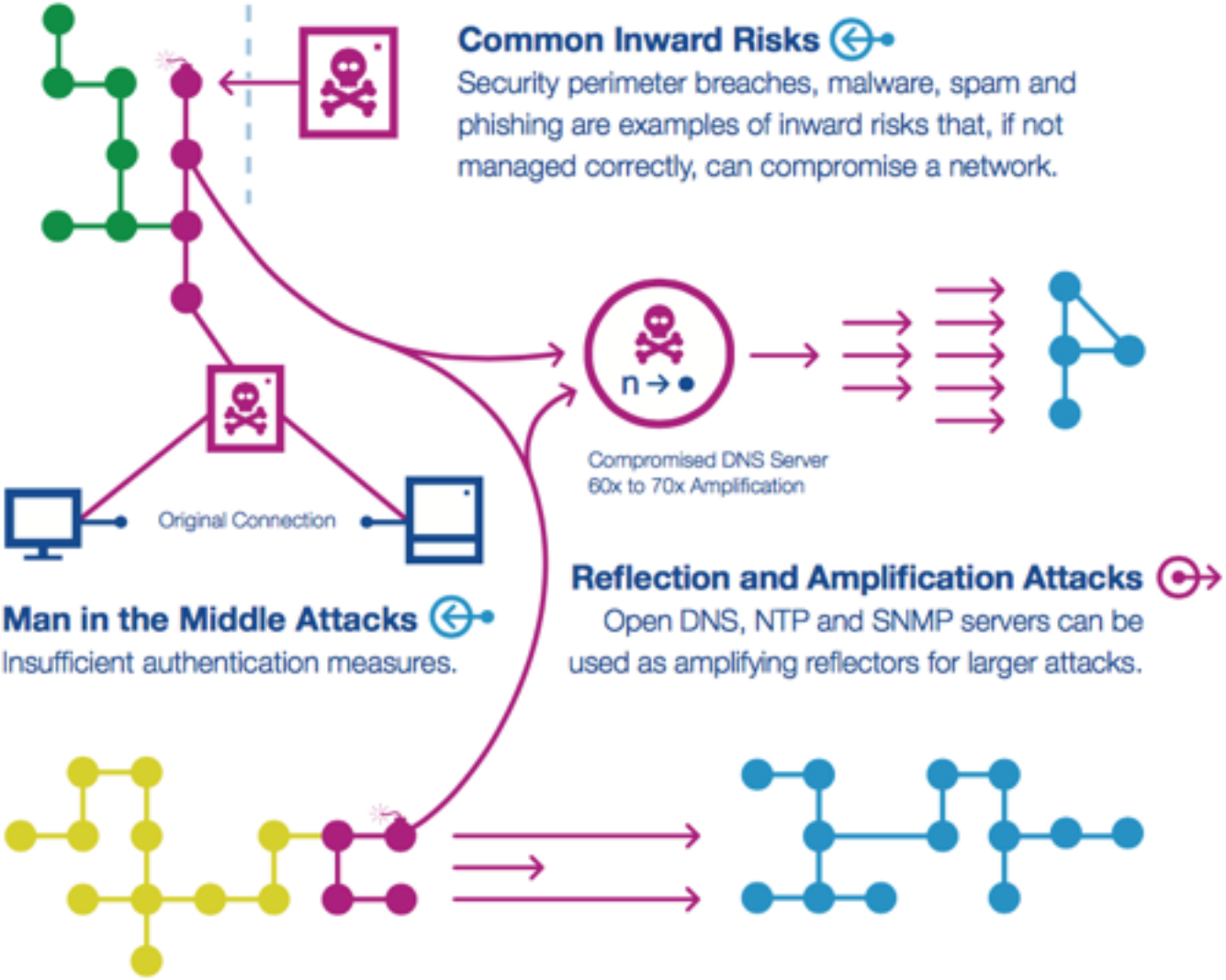

Applications
IP
Network

https://www.flickr.com/photos/worldbank/4725033296/in/album-72157634090168746/


General Purpose
Interoperable Building Blocks
Accessible
Global Reach & Integrity
Interoperability & mutual agreement
Permissionless Innovation
Accessible
Collaboration
No Permanent Favorites
Internet Invariants: What Really Matters
http://www.internetsociety.org/internet-invariants-what-really-matters

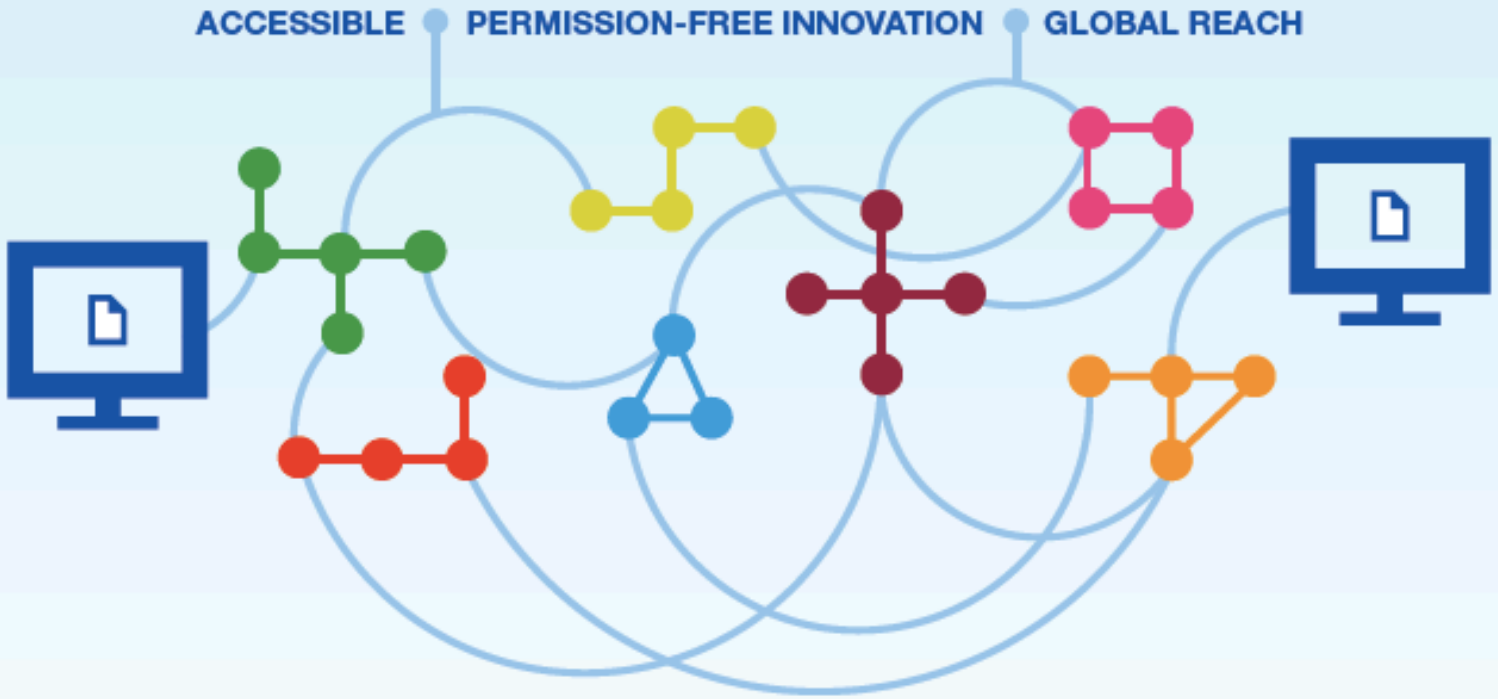
Security, stupid


Open Platform
Open for attack and intrusion
Permission less innovation
Malware development & deployment
Global Reach
Attacks and crime are cross-border
Voluntary collaboration
Hard to mandate


Common Inward Risks
Security perimeter breaches, malware, spam and phishing are examples of inward risks that, if not managed correctly, can compromise a network.
n→●
Compromised DNS Server
60x to 70x Amplification
Original Connection
Man in the Middle Attacks
Insufficient authentication measures.
Reflection and Amplification Attacks
Open DNS, NTP and SNMP servers can be used as amplifying reflectors for larger attacks.

The Internet is open, interconnected and interdependent

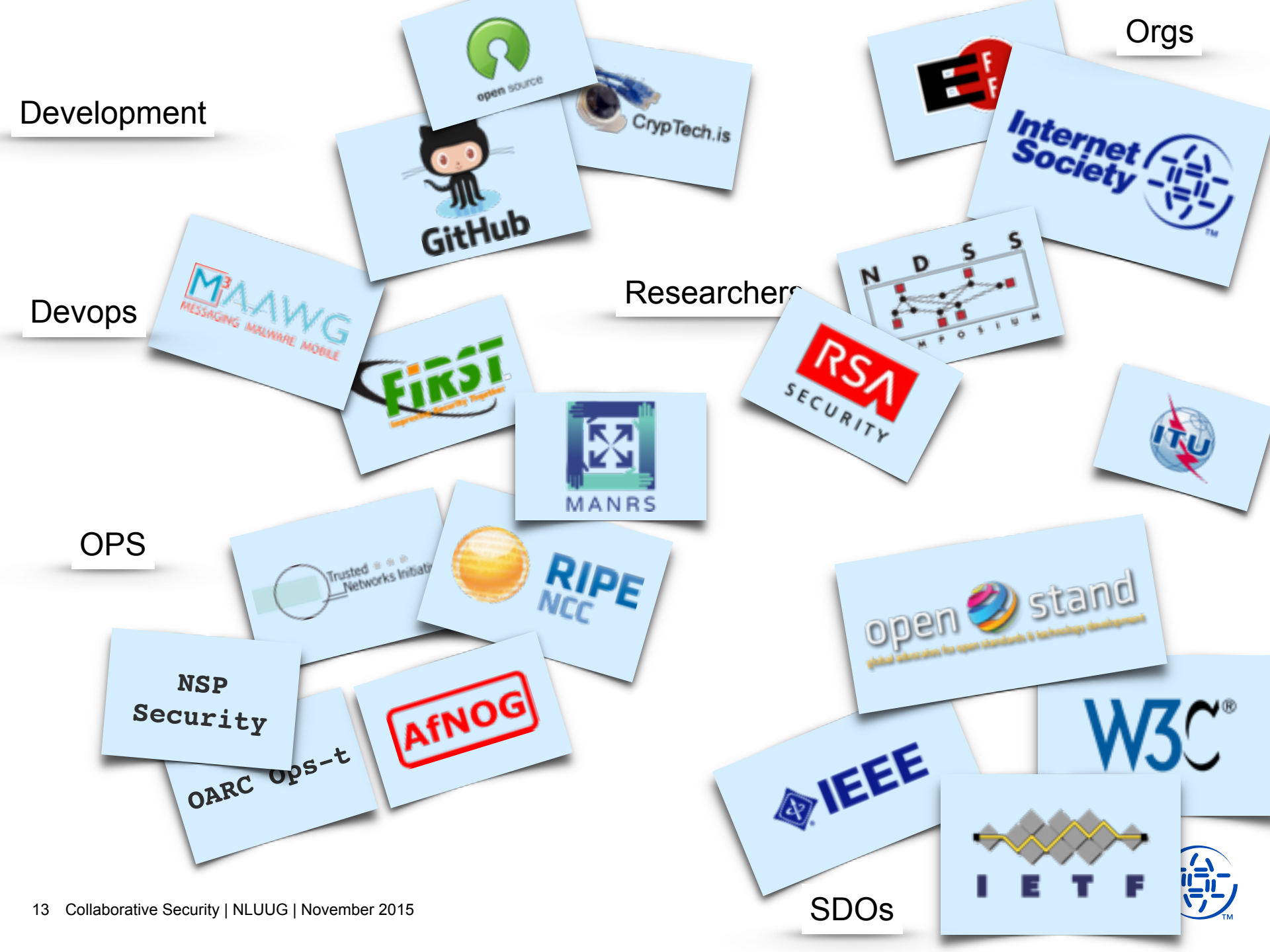
It's an ecosystem based on collaboration and shared responsibility



Each network is responsible not only for its own security, but also contributes to the overall security of the medium. The challenge is to create a culture of collective responsibility to make the Internet more secure and resilient.


Fostering Confidence and Protecting Opportunities
Fundamental Properties and Values
Collaborative Security
An approach to tackling Internet Security issues
APRIL 2015
Collective Responsibility
Think Globally Act Locally
Evolution and Consensus
Internet Society

Where the rubber meets the road.


Development
Orgs
Devops
Researchers
OPS
SDOs
open source
GitHub
CrypTech.is
Internet Society
M3AAWG
MESSAGING MALWARE MOBILE
FIRST
MANRS
RSA SECURITY
NDSS
ITU
Trusted Networks Initiative
RIPE NCC
NSP Security
OARC Ops-t
AfNOG
open stand
IEEE
W3C
IETF

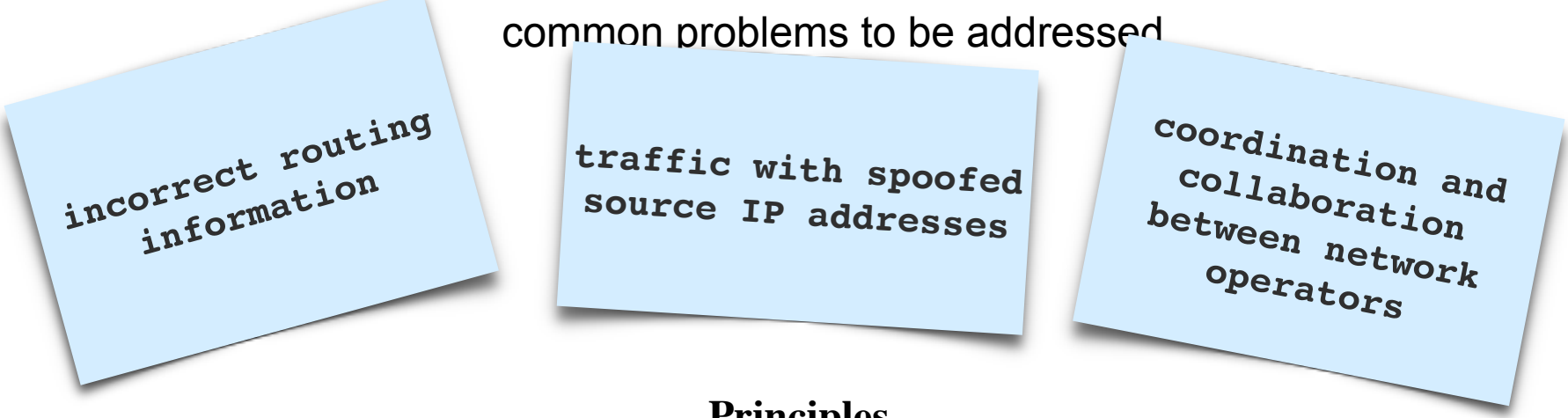
Mutually Agreed Norms for Routing Security (MANRS)

Stimulate visible improvements in security and resilience of Internet Routing by changing towards a culture of collective responsibility

MANRS

Internet Society

common problems to be addressed



Principles

1. The organization (ISP/network operator) recognizes the interdependent nature of the global routing system and its own role in contributing to a secure and resilient Internet.
2. The organization integrates best current practices related to routing security and resilience in its network management processes in line with the Actions.
3. The organization is committed to preventing, detecting and mitigating routing incidents through collaboration and coordination with peers and other ISPs in line with the Actions.
4. The organization encourages its customers and peers to adopt these Principles and Actions.

MANRS

Internet Society

Prevent propagation of incorrect routing information.

Prevent traffic with spoofed source IP addresses.

Facilitate global operational communication and coordination between network operators.

Facilitate validation of routing information on a global scale.

MANRS

Internet Society

Please have this conversation with your stakeholders

http://www.routingmanifesto.org/

or

http://manrs.org/

Contact routingmanifesto@ISOC.org

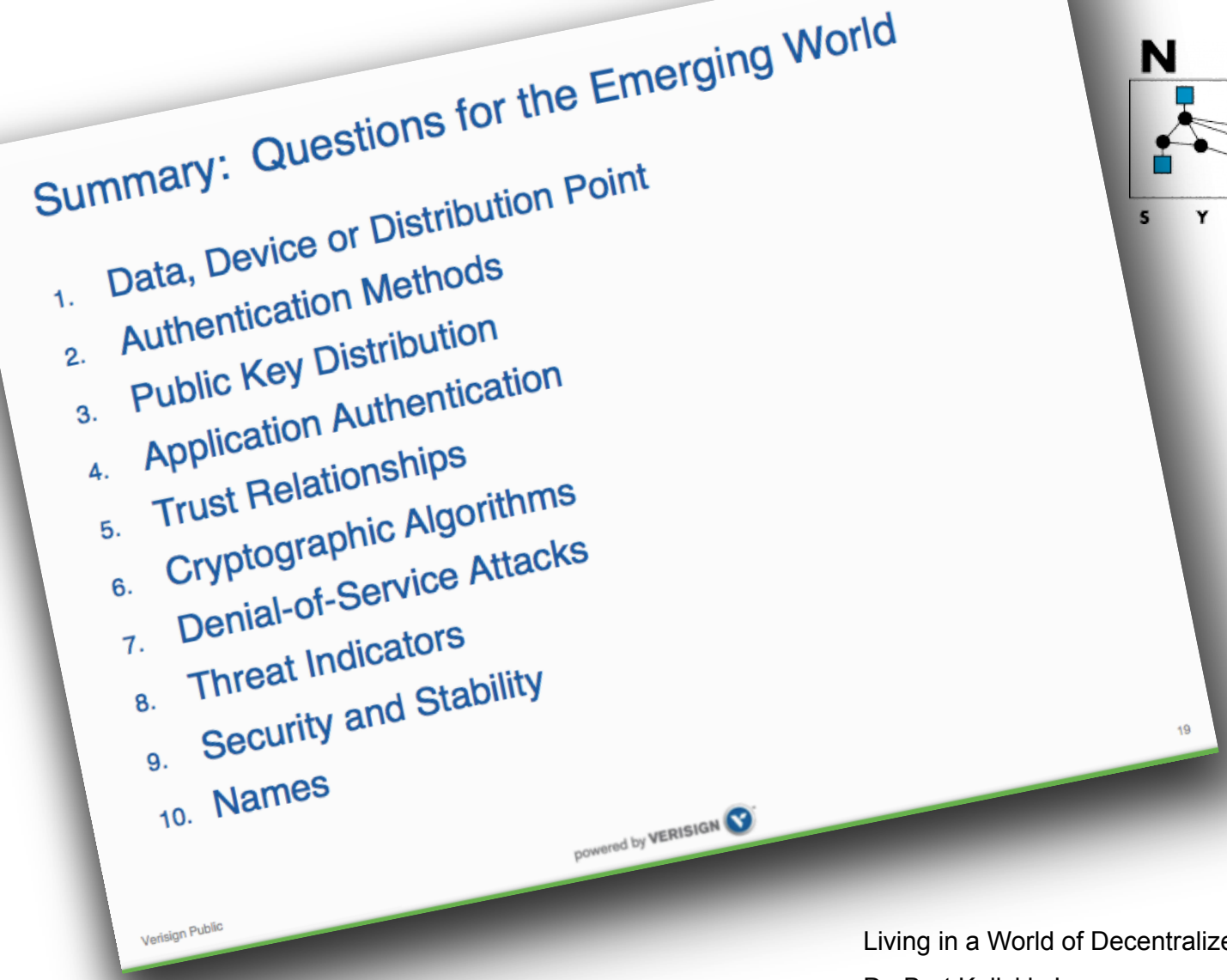
MANRS

Internet Society

http://www.internetsociety.org/iot/

Collaborative Security and the Internet of Things

Internet Society



N D S S '15 S Y M P O S I U M

Living in a World of Decentralized Data

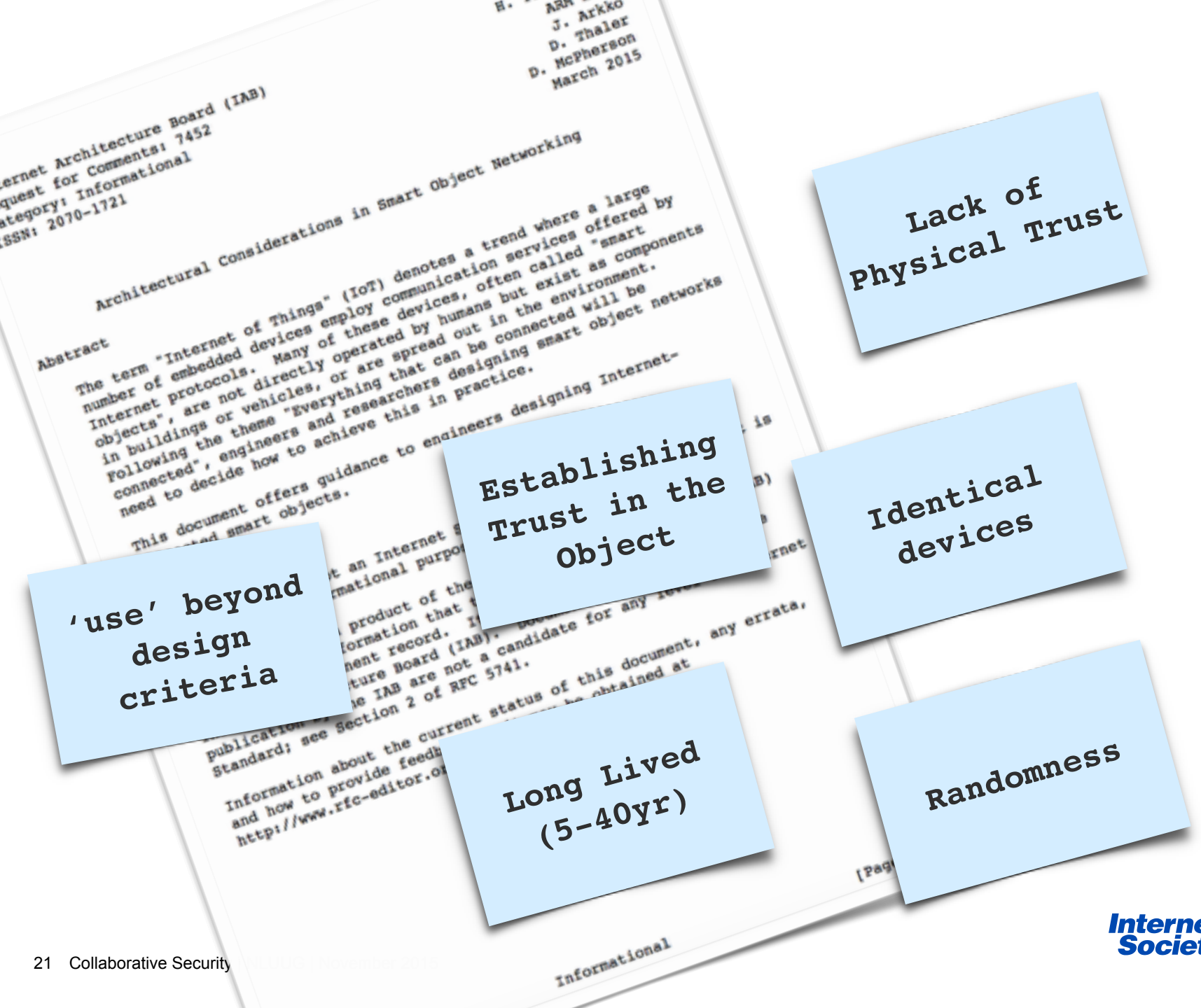
Dr. Burt Kaliski, Jr.

Senior Vice President and CTO, Verisign

NDSS Workshop on Security of Emerging Networking Technologies (SENT)

February 8, 2015

Internet Society

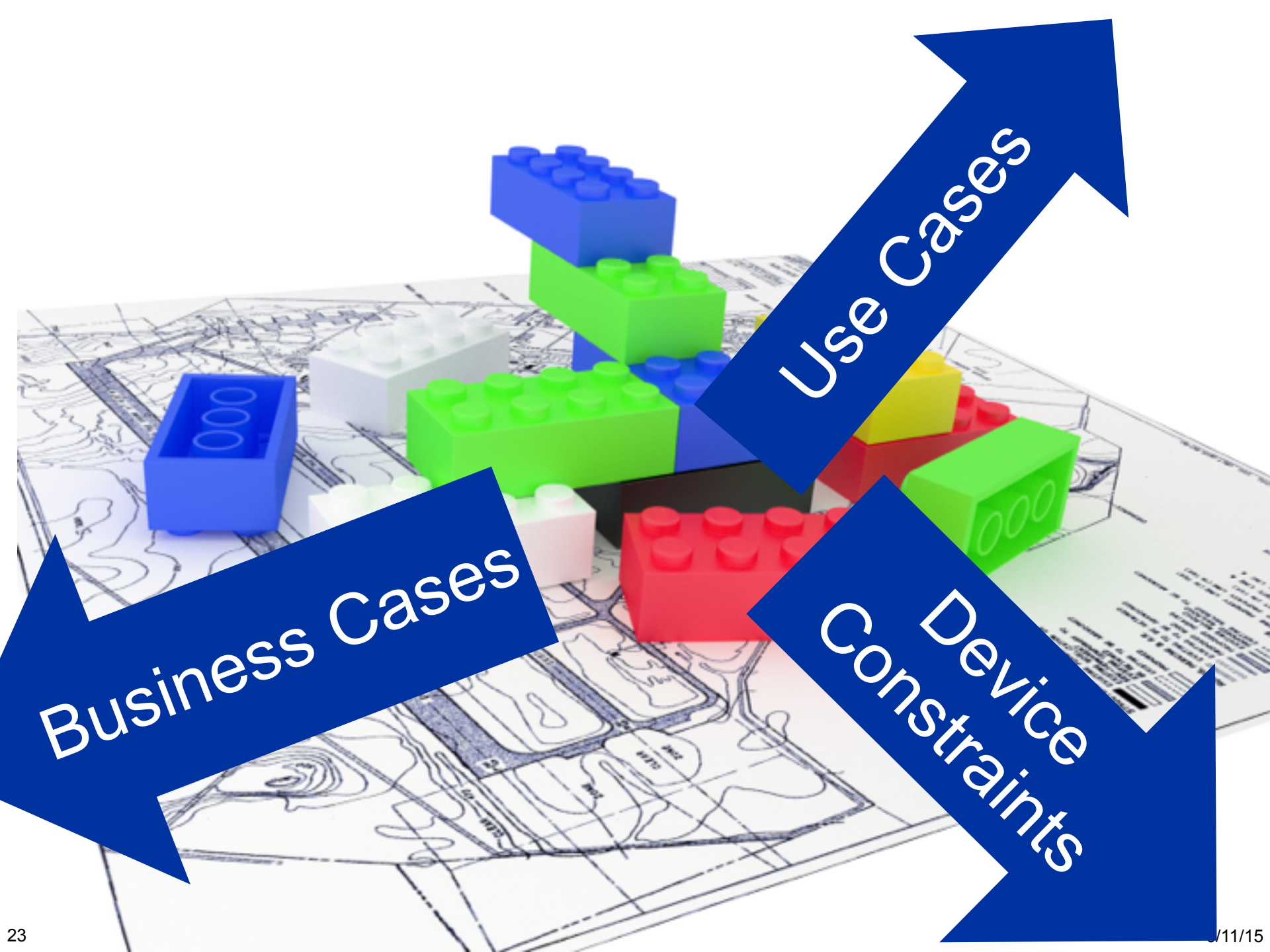

Lack of Physical Trust
Establishing Trust in the Object
Identical devices
'use' beyond design criteria
Long Lived (5-40yr)
Randomness
Architectural Considerations in Smart Object Networking
Abstract
Informational

Areas of Responsibility

	Examples of Problems
Cryptographic Primitives	Improved algorithms for integer factorization, too small key size.
Protocol Specifications and Architecture	No end-to-end security, complexity in specifications, insecure authentication protocols
Implementation	Buffer overflow attacks, poor UI or other usability problems, poor choice of hardware
Deployment	Enabled debug ports, missing deployment of security mechanisms

Understanding the distributed nature of the development process is essential for tackling security problems.

Courtesy: Tschofenig et al, IETF 92 Technical Plenary


Use Cases
Business Cases
Device Constraints

Can you do responsible security on a € 0.04 margin device?

Re-use Internet security technologies:

- Use state-of-the-art key length
- Always use well-analysed security protocols.
- Use encryption to improve resistance against pervasive monitoring.
- Support automatic key management and per-device keys.

Additional IoT relevant security aspects:

- Crypto agility is a hard decision and you need to think deeply about it.
- Integrate a software update mechanism and leave enough “head room”
- Include a hardware-based random number generator.
- Threat analysis must take physical attacks into account.
- Use modern operating system concepts to avoid system-wide compromise due to a single software bug.

Some Practical Recommendations

See RFC7452

Smart Connected Objects

These objects will have a profound impact on our lives.

Important Security Questions have not been answered while we deploy.

The Collaborative Security Approach has properties that will help to make a positive impact

Foster Confidence and Protect Opportunities

Evolution and Consensus

Fundamental Properties and Values

Collective Responsibility

Think Globally, Act Locally

Olaf M. Kolkman

Chief Internet Technology Officer

Kolkman@isoc.org
twitter: @kolkman

Internet Society™