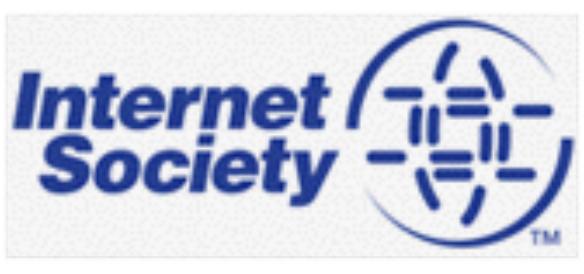


# Collaborative Security

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

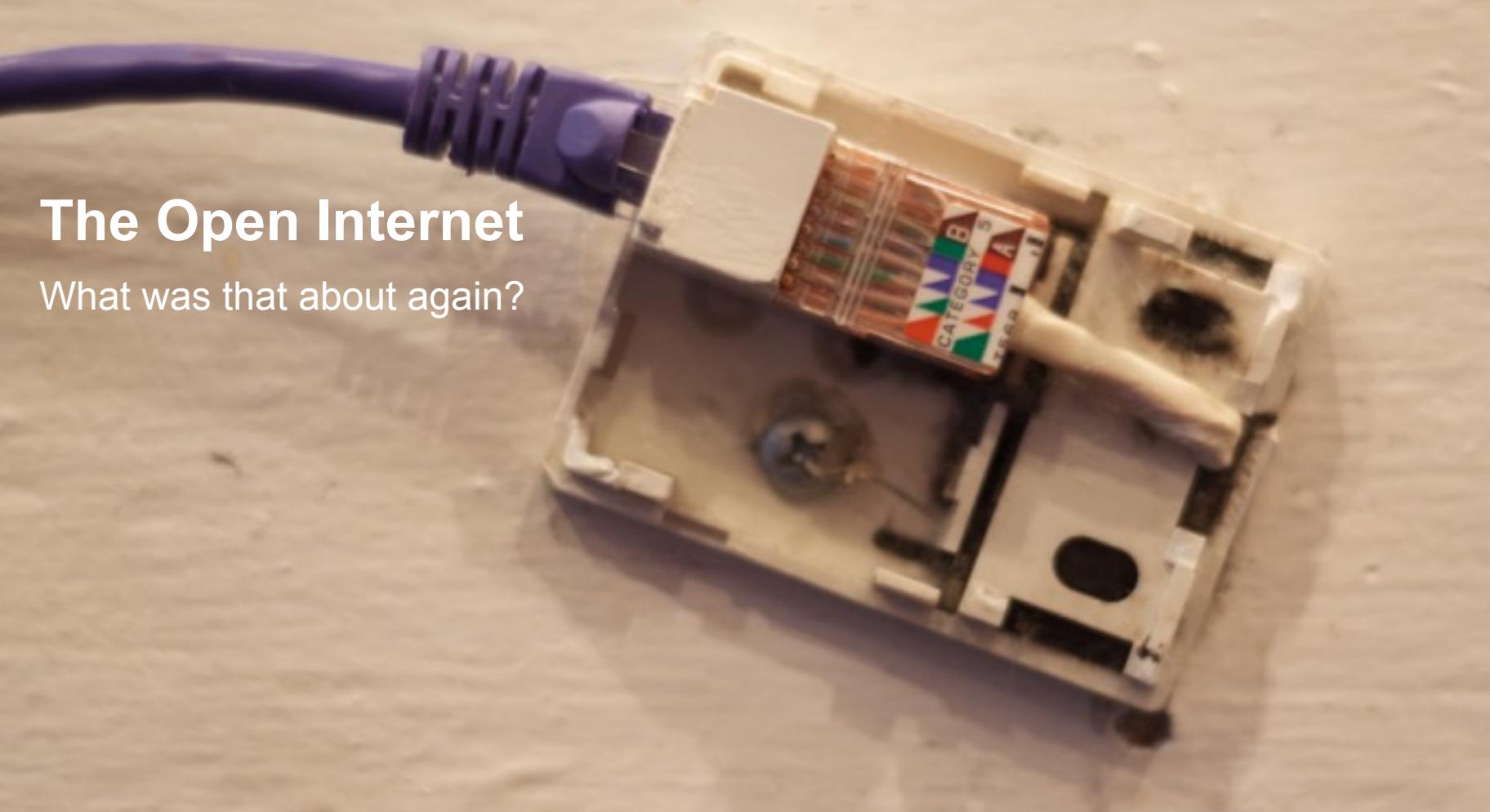
Global and  
Inclusive

Independent and  
Not-for-Profit

Organizational  
home for the  
IETF

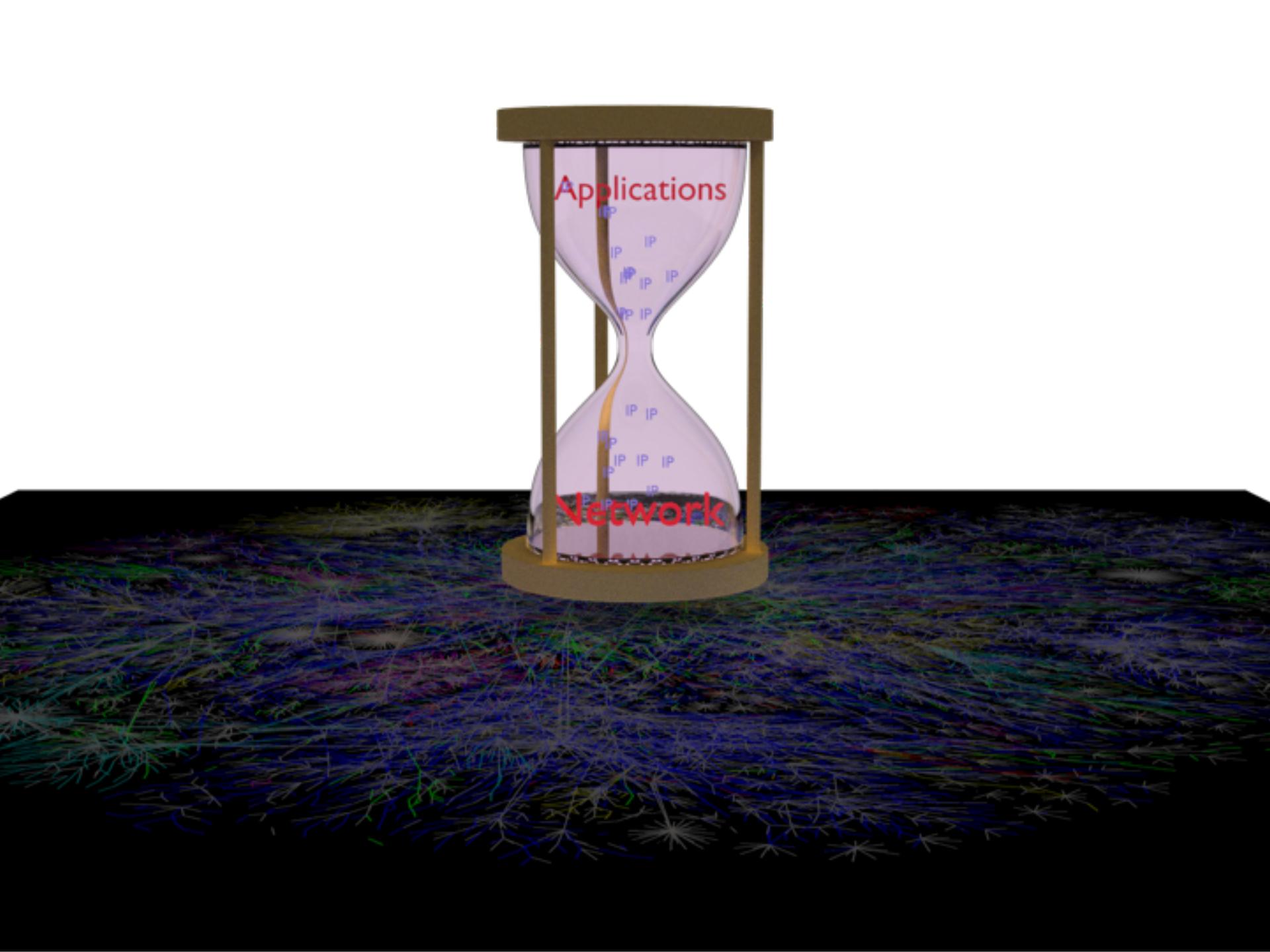
<http://www.internetsociety.org/get-involved/individuals>





# The Open Internet

What was that about again?



Applications

Network



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

General  
Purpose

## Interoperable Building Blocks

Global Reach &  
Integrity

Permissionless  
Innovation

Accessible

No Permanent  
Favorites

## Internet Invariants: What Really Matters

Interoperability  
& mutual  
agreement

Collaboration

The Internet has seen significant change since it was established as a research network forty years ago. On one front, it has gone from being a network run by a mixture of government and researchers to facilitate their collaboration, to being run by a mixture of research and commercial interests as a curiosity, an informal electronic communications medium, and a cornerstone of considerable importance for both commerce and individuals' daily lives. On another front, the technologies supporting the network has evolved commensurately with computing power, and network architectures and services have followed the changing requirements and uses. And on yet another front, Internet applications and services have been transformative, continuously challenging expectations (for example, no one predicted the impact and popularity of Facebook).

In the light of those considerations, it's important to understand what is actually important and unchanging about the Internet – the invariants that have been true to date. This paper describes several invariant properties of the Internet, which have enabled the Internet to serve as a platform for seemingly limitless innovation, outline not only its technology, but also its shape in terms of global impact and social structures.

### What really matters about the Internet

The Internet is a worldwide interconnection of computers and computer networks that facilitate the sharing of information among users. The unchanging properties of that system have included features of the underlying networks, technologies and standards, as well as emergent properties that impact users and uses of the Internet.

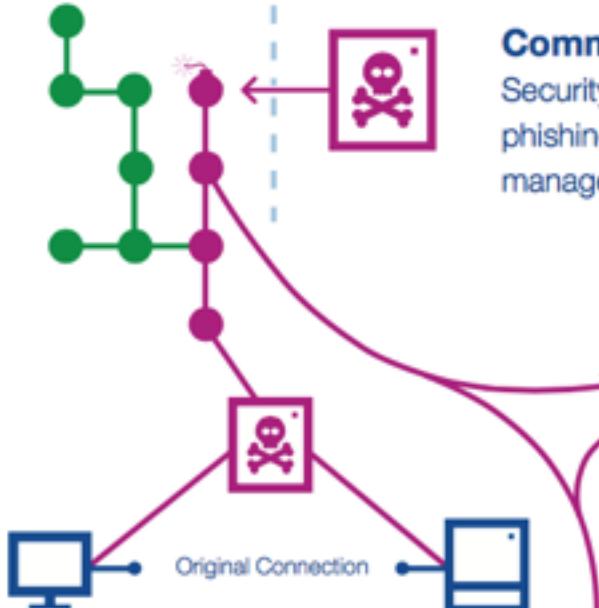
The Internet has global reach and integrity, and is not constrained in terms of supported services and applications:

- **Global reach, Integrity:** Any endpoint of the Internet can address any other endpoint, wherever the receiver information received at one endpoint is as intended by the sender, whenever the receiver connects to the Internet. Implicit in this is the requirement of global, managed addressing and naming services.
- **General purpose:** The Internet is capable of supporting a wide range of demands for its use, while some networks within it may be optimized for certain traffic patterns or expected uses, the technology does not place inherent limitations on the applications or services that make use of it.

<http://www.internetsociety.org/internet-invariants-what-really-matters>

# Security, stupid



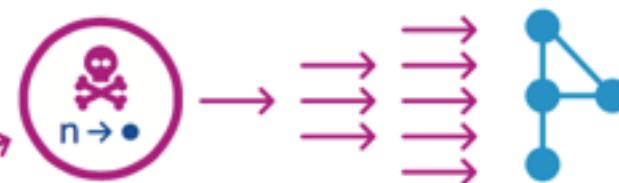


### Man in the Middle Attacks ⚡

Insufficient authentication measures.

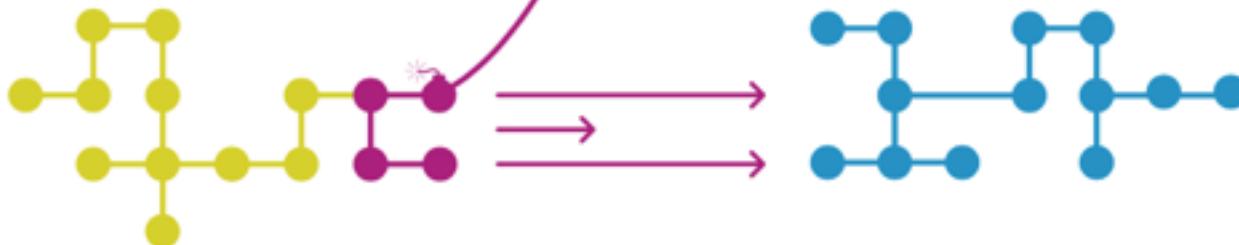
### Common Inward Risks ⚡

Security perimeter breaches, malware, spam and phishing are examples of inward risks that, if not managed correctly, can compromise a network.



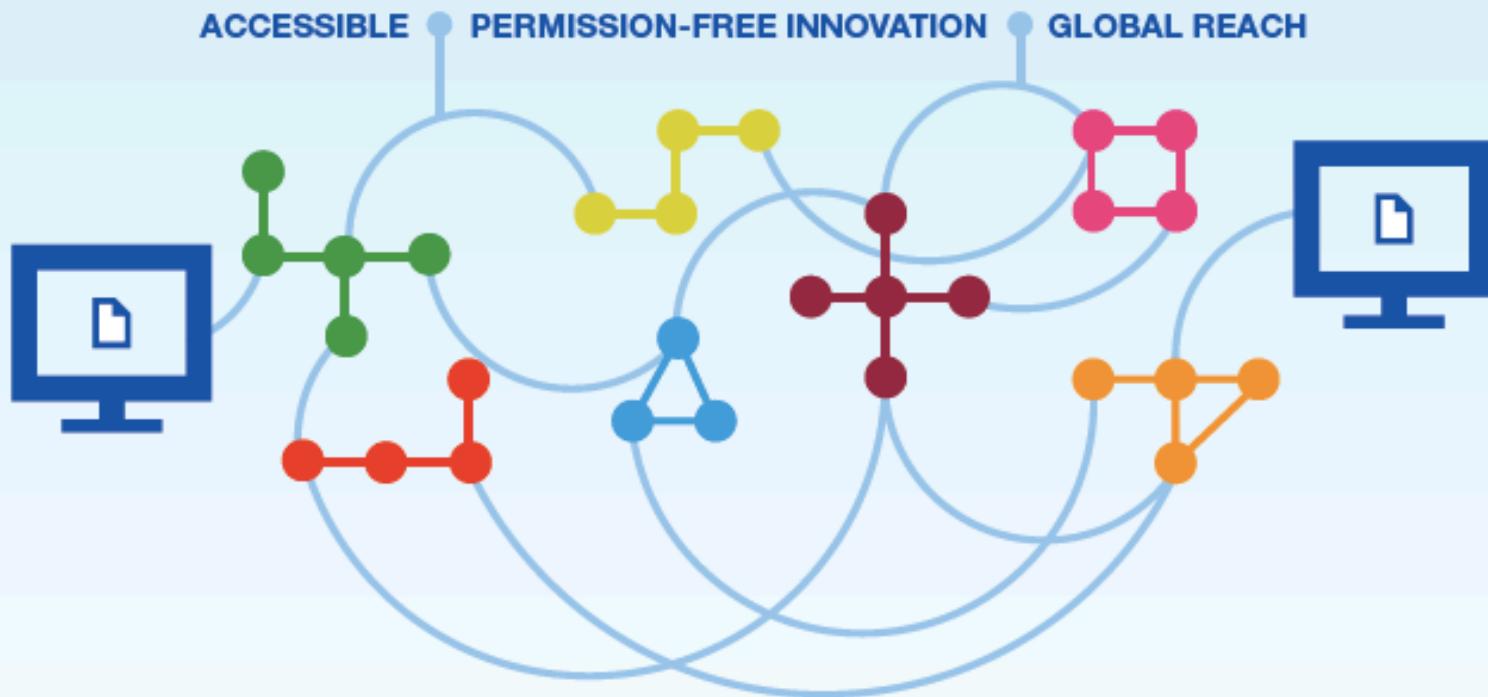
### Reflection and Amplification Attacks ⚡

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

Collective  
Responsibility

Evolution and  
Consensus

# Collaborative Security

An approach to tackling Internet Security issues

APRIL 2015

Fundamental  
Properties and  
Values

Think Globally  
Act Locally



# Where the rubber meets the road.

Orgs

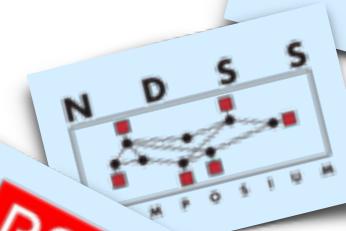
Development



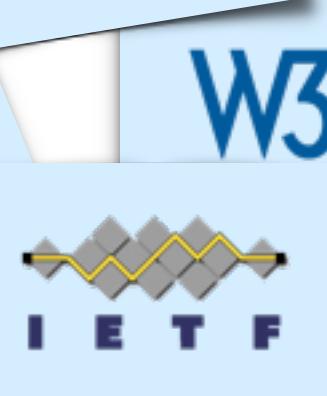
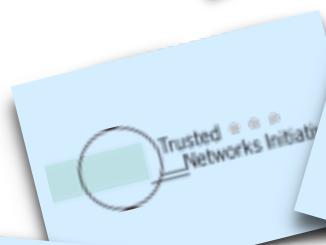
Devops



Researchers



OPS



SDOs





# 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

*incorrect routing  
information*

*common problems to be addressed*

*traffic with spoofed  
source IP addresses*

*coordination and  
collaboration  
between network  
operators*

## **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.**

Action 1

**Prevent propagation of incorrect routing information.**

Action 2

**Prevent traffic with spoofed source IP addresses.**

Action 3

**Facilitate global operational communication and coordination between network operators.**

Advanced  
Action 4

**Facilitate validation of routing information on a global scale.**

Please have this  
conversation with  
your stakeholders



<http://www.routingmanifesto.org/>

or

<http://manrs.org/>

Contact  
[routingmanifesto@ISOC.org](mailto:routingmanifesto@ISOC.org)

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

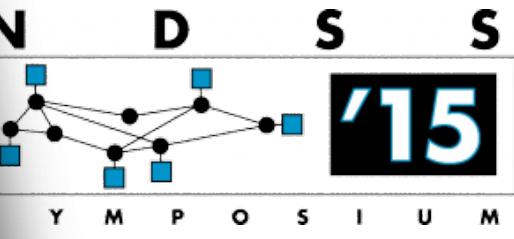


# Summary: Questions for the Emerging World

1. Data, Device or Distribution Point
2. Authentication Methods
3. Public Key Distribution
4. Application Authentication
5. Trust Relationships
6. Cryptographic Algorithms
7. Denial-of-Service Attacks
8. Threat Indicators
9. Security and Stability
10. Names

powered by  VERISIGN

Verisign Public



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



## Abstract

The term "Internet of Things" (IoT) denotes a trend where a large number of embedded devices employ communication services offered by Internet protocols. Many of these devices, often called "smart objects", are not directly operated by humans but exist as components in buildings or vehicles, or are spread out in the environment. Following the theme "Everything that can be connected will be connected", engineers and researchers designing smart object networks need to decide how to achieve this in practice.

This document offers guidance to engineers designing Internet-connected smart objects.

'use' beyond  
design  
criteria

Establishing  
Trust in the  
Object

Lack of  
Physical Trust

Identical  
devices

Randomness

Long Lived  
(5-40yr)

# 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

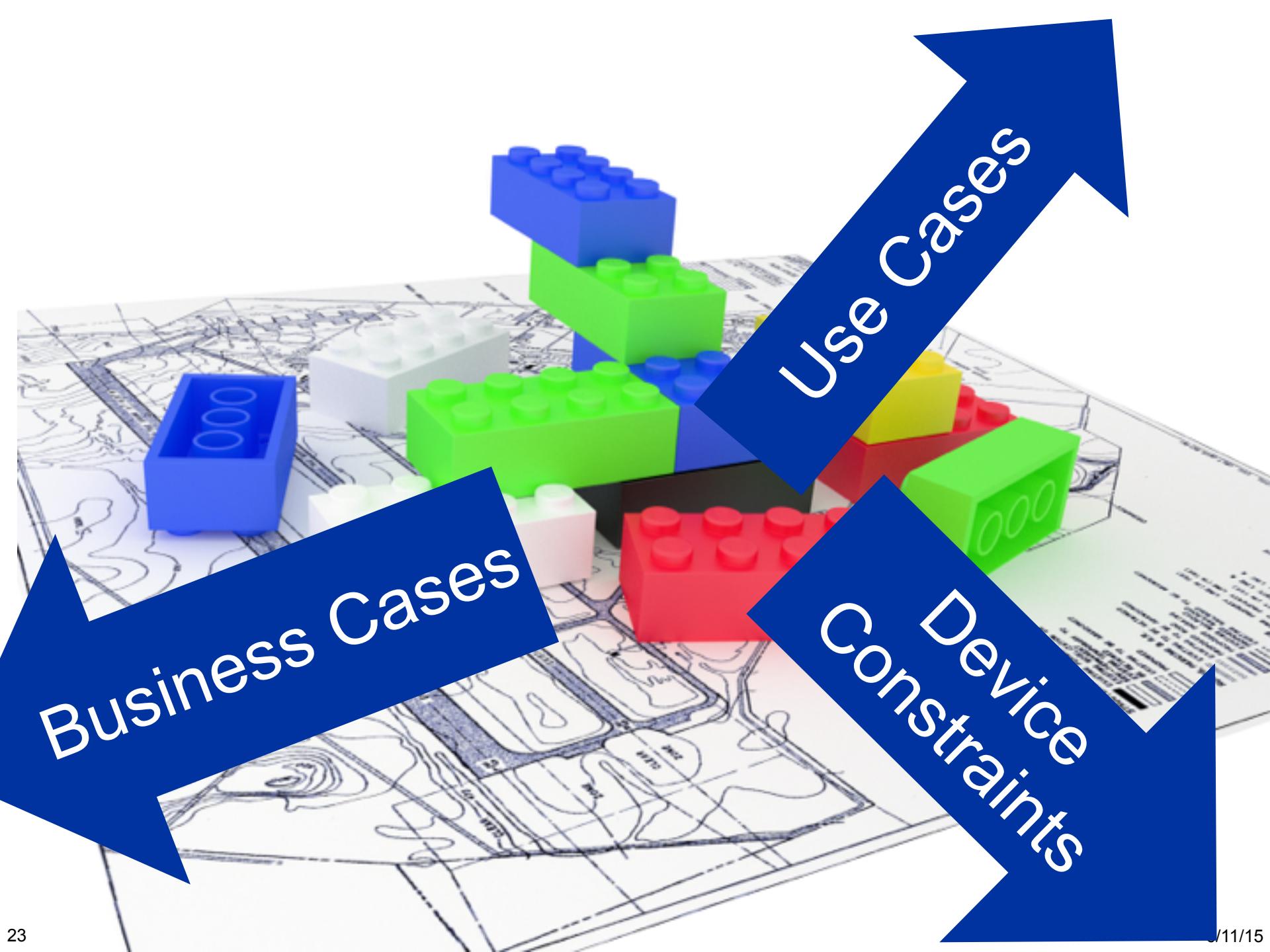
Buffer overflow attacks, poor UI or other usability problems, poor choice of hardware

Deployment

Enabled debug ports, missing deployment of security mechanisms

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





Business Cases

Device  
Constraints

Use Cases

000

000

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

## Some Practical Recommendations

### 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.

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](mailto:Kolkman@isoc.org)  
twitter: @kolkman