

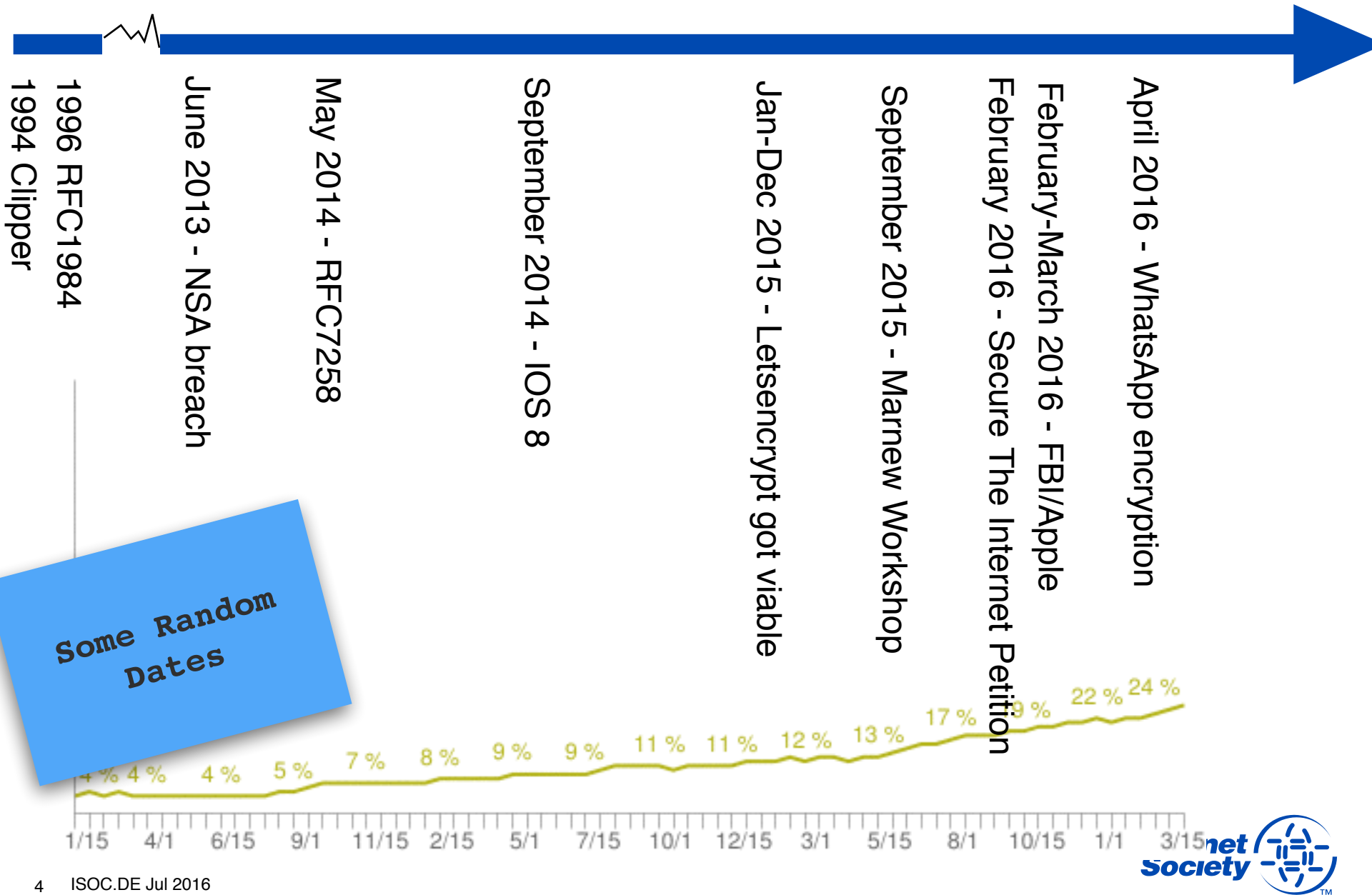
From Encryption to Security

Purpose of the session

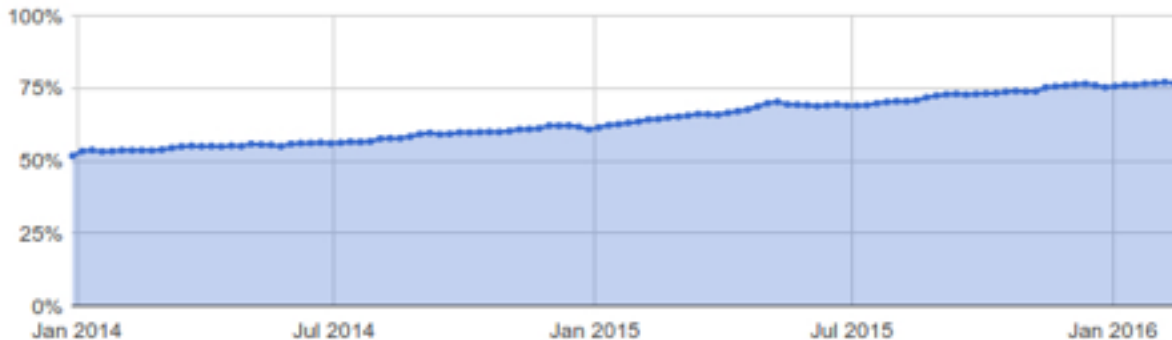
A conversation around where we think the Encryption issue leads to.

Share **thoughts** about the issues.

Encrypted traffic... it is a fact

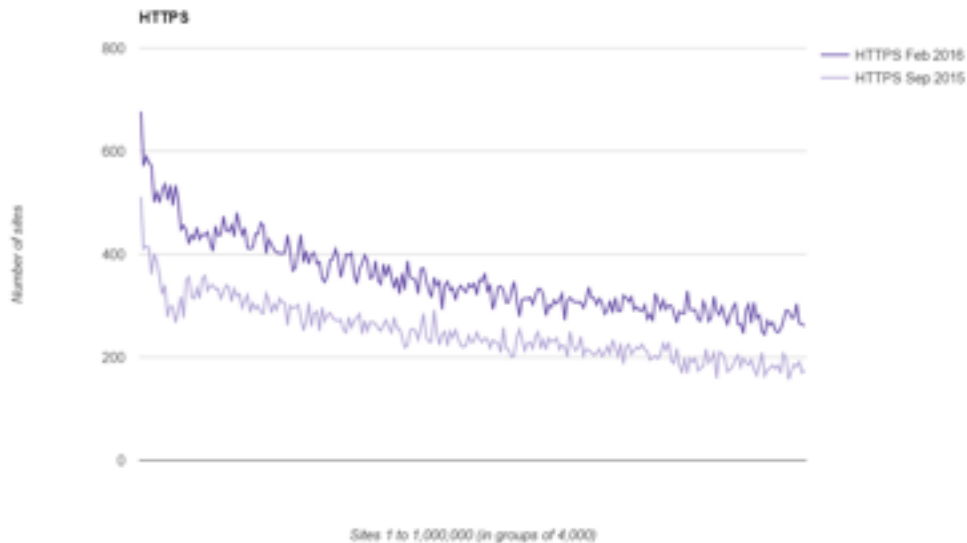


Encrypted Traffic continues growing



Source: Google Blog - Securing the web, together
March 15, 2016

This chart represents the percentage of requests to Google's servers that used encrypted connections. YouTube traffic is currently not included in this data.



Source: Scott Helme - Security headers in the Alexa Top 1 Million

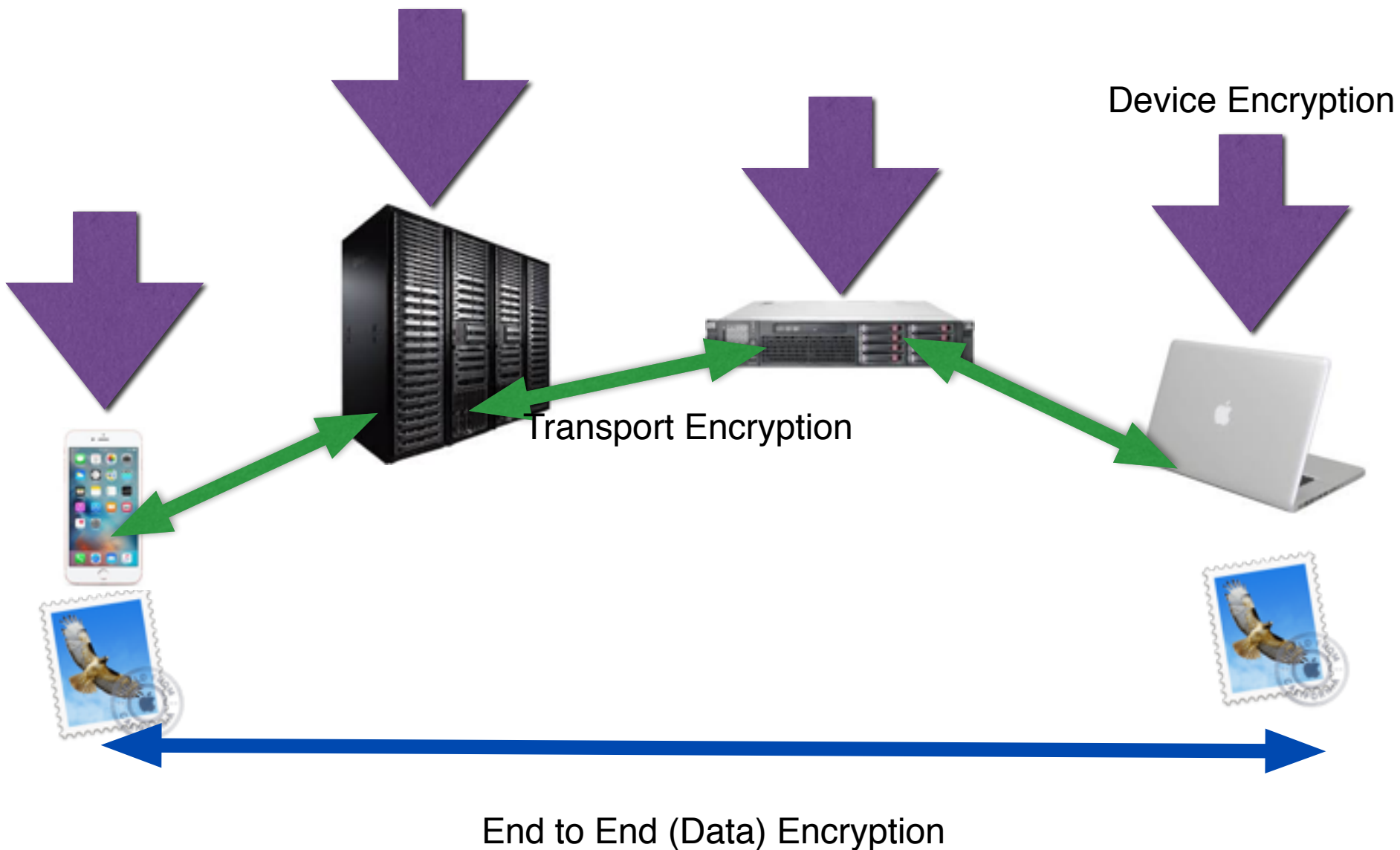
Encrypted traffic

Protects users from ‘the Bad™’ and protects their confidential information and their privacy.

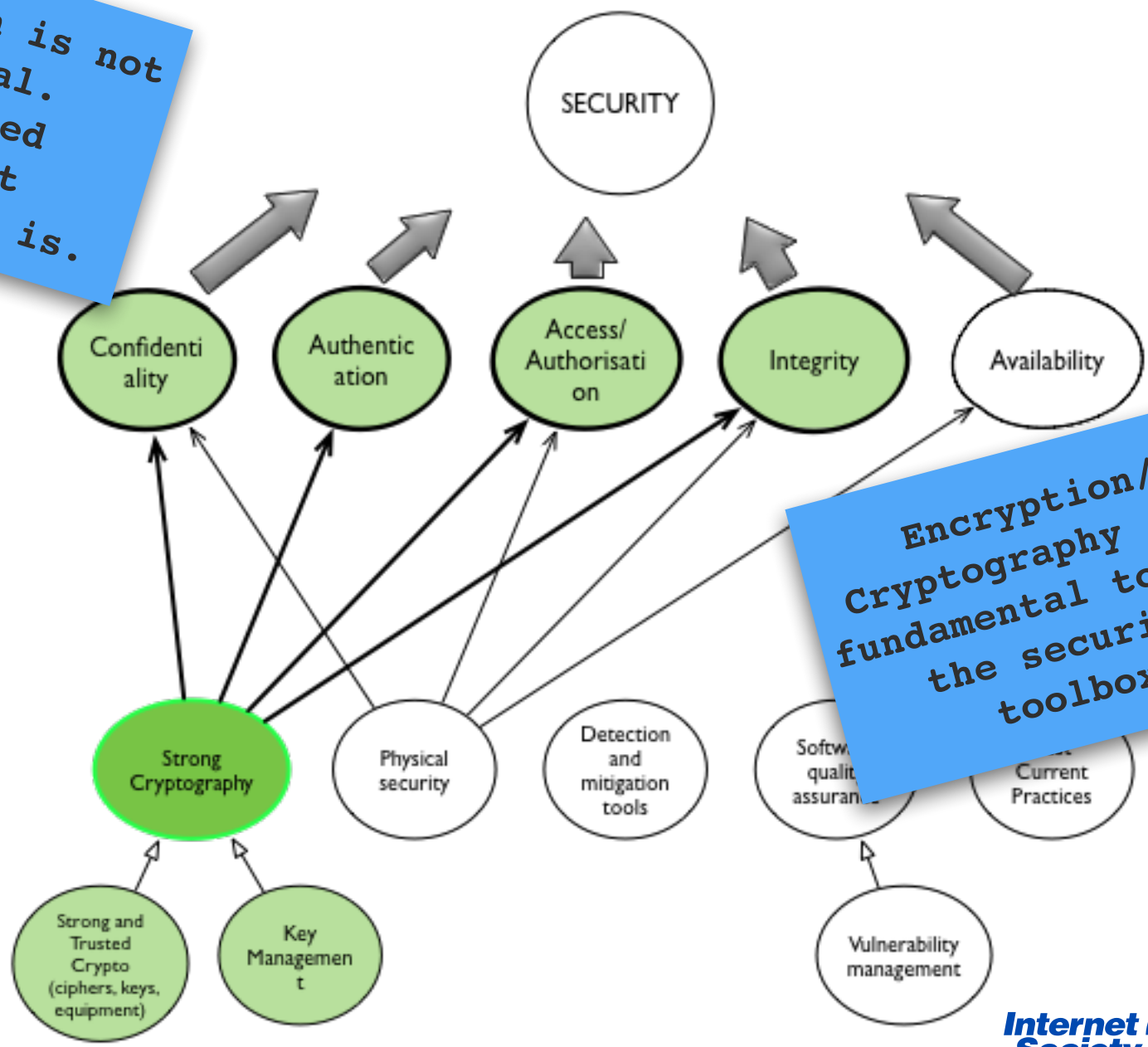
The Economy depends on Encrypted Traffic

Some attributes of the communication are not encrypted.

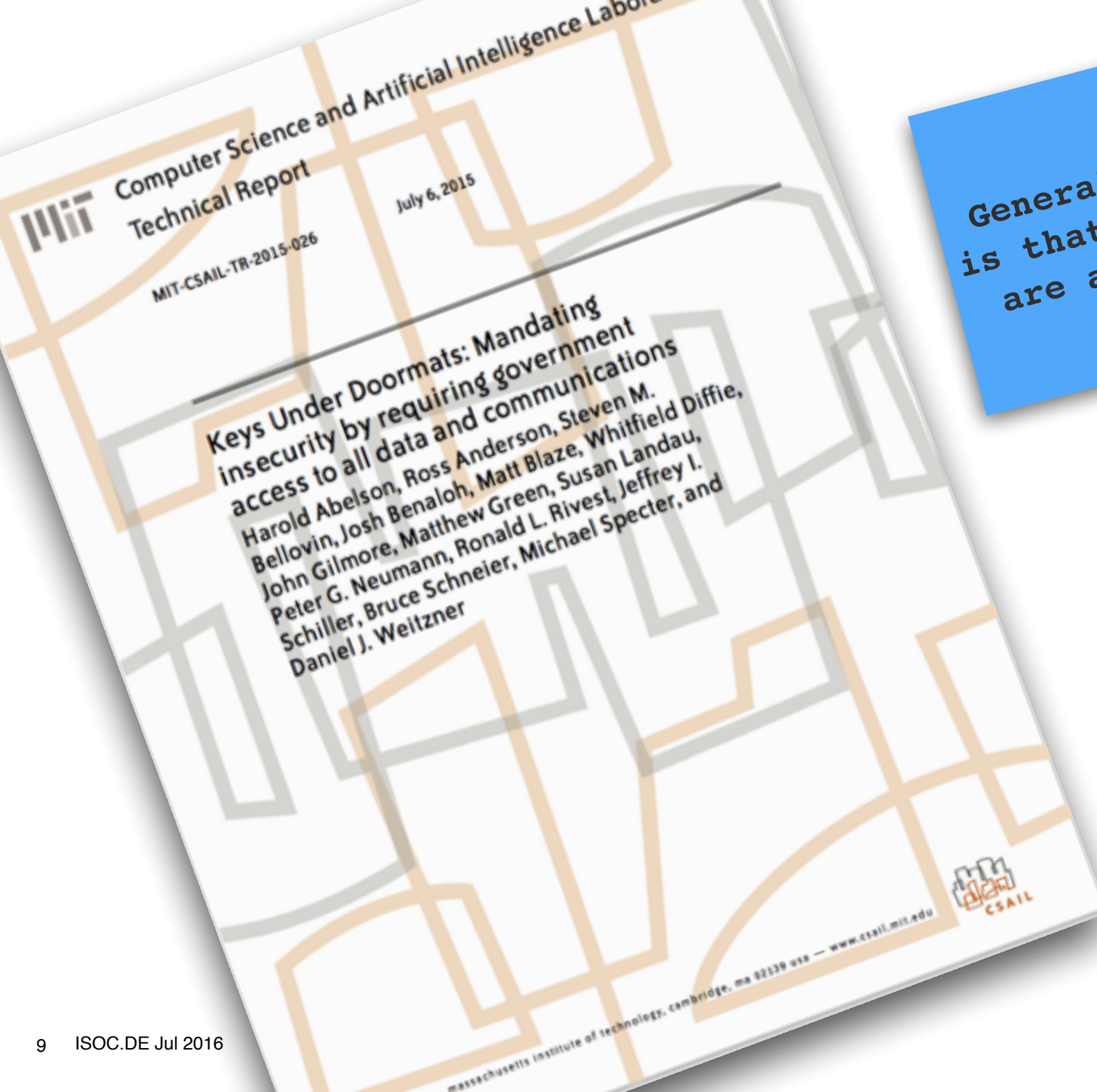
The evolution impacts what law enforcement sees and how operators perform some network management functions.



Encryption is not the goal.
A trusted Internet environment is.



Encryption/ cryptography is a fundamental tool in the security toolbox



General consensus
is that 'backdoors'
are a no go area

Roles and responsibilities in an encrypted world

PROMPT

Right now, law enforcement and intelligence agencies around the world are mining data, re-routing internet traffic, and hacking into devices and systems, sometimes on a mass scale. While these tactics may present an alternative to undermining encryption, they each come with their own costs, including serious costs to human rights. Discussants in this track will explore without prejudice the rumored, public, or potential methods and tools that are available to government surveillance agencies; where and how they are explicitly authorized; their costs and benefits; and high-level safeguards that need to be in place if they are carried out.

DISCUSSION LEADERS

Jamie Tomasello, Access Now
Shauna Dillavou, Community Red

SPECIFIC OUTCOMES

Identified **24** techniques or alternatives to obtain encrypted data.

- Targeted and bulk "lawful" hacking
- Crypto-analysis
- Brute force
- Creating backdoors
- Not encrypting
- Undermining infrastructure
- Underseas fibers
- Exploiting global networks (getting data overseas)
- Spoofing target
- Man In The Middle attacks
- Impersonation
- Exploit supply chain vulnerabilities
- Metadata analysis
- Social graph analysis
- Compelled decryption
- Physical intrusion
- Human intelligence
- Black bags
- Extralegal decryption
- Subpoena/Legal process
- Social engineering
- Stealing keys/certificates
- Informants
- Legal/Court mechanisms

Identified **14** factors by which to consider alternate techniques to obtain encrypted data.

- Severity of the crime
- Necessity of employing the technique
- Proportionality of the crime compared to the severity of the technique
- Credibility of evidence
- Legality of the alternative
- Potential for unintended consequences
- Nature of unintended effects
- Balance of equities
- Resources required
- Breadth (targeted or bulk)
- Abuse — to what extent could the technique be abused once created
- Oversight and accountability
- Efficiency
- Viability

Are all doors closed then?

Source: <https://www.accessnow.org>

lets talk Trust and the Internet

Approaching this from a Trust Perspective

Collaborative Security

An approach to tackling Internet Security issues

APRIL 2015

Executive Summary

People are what ultimately hold the Internet together. The Internet's development has been based on voluntary cooperation and collaboration. Cooperation and collaboration remain the essential factors for Internet's prosperity and potential.

Collaborative Security is an approach that is characterized by five key elements:

- **Fostering confidence and protecting opportunities:** The objective of security is to foster confidence in the Internet and to ensure the continued success of the Internet as a driver for economic and social innovation.
- **Collective Responsibility:** Internet participants share a responsibility towards the system as a whole.
- **Fundamental Properties and Values:** Security solutions should be compatible with fundamental human rights and preserve the fundamental properties of the Internet — the *Internet Invariants*.
- **Evolution and Consensus:** Effective security relies on agile evolutionary steps based on the expertise of a broad set of stakeholders.
- **Think Globally, act Locally:** It is through voluntary bottom-up self-organization that the most impactful solutions are likely to be reached.

Introduction

Any cybersecurity framework needs to start with an Internet (open standards, voluntary collaboration and global reach ("the cybersecurity landscape" and social processes of trust).

The FBI/Apple Case was not about Encryption: It was about circumventing device security

Can a company be compelled to weaken its products security?

The next door to knock on

A few thoughts...

About roles and responsibilities with respect to the **highest** standards of device security

System Security Principles

It is *my** belief that:

***Industry* is best place to assess risks, cost and benefits, and viable technical solutions hence they have a primary responsibility for their system's security**

They should be empowered to create the best possible security solutions for their products and services

Industry should, under parameters of rule of law, cooperate with law enforcement, whilst not sacrificing the principles above.

Governments should create the best circumstances for improving System Security.

* This is not (yet) ISOC's position

System Security Principles

It is my* belief that:

Not just a Law-
Enforcement
issue

place to assess risks, cost and benefits, and
solutions hence they have a primary
for the system's security

They should be empowered to find the best possible security
solutions for their products and services

A general Cyber
Security issue

Industry should, under parameters of rule of law, cooperate with
law enforcement, whilst not sacrificing the principles above.

Governments should create the best environment for
improving System Security.

Broadly
applicable

Including
IOT

* This is not (yet) ISOC's position

Some Questions and observations

Governments should create the best circumstances for improving System Security.

That means: Responsible disclosure, bug bounties, procure for security, setting high security expectations, etc, etc.

That does not mean: prevent the general public from ‘*tinkering*’, ‘*hacking*’, and security research

But how does that relate to the use of exploit kits by law enforcement?

Nothing prevents proliferation of the exploits of vulnerabilities

Nothing prevents proliferation of the tools to enable strong system security such as encryption

Some Questions and observations

Industry is best place to assess risks, cost and benefits, and viable technical solutions hence they have a primary responsibility for their system's security

For sure they are not the only actors: system security is the responsibility of many parties, including governments (public safety) and users themselves

**Collaborative
Security**

**The
responsibility
of minimum
standards?**

**Companies put a
lot of crap out
there too...**

Some Questions and observations

Industry should, under parameters of rule of law, cooperate with law enforcement, whilst not sacrificing the principles above.

What are the needs for industry to work with law enforcements and vice-versa

Additional nuance is needed. There is a difference between cooperation/assistance and becoming a tool of the government

How about the procurement and use of (existing) exploits by law enforcement?

Premise: recognize
the role of Law
Enforcement in
public safety

trade-offs

Premise: recognize
the role of system
security in public
safety

Some Questions and observations

Industry is best place to assess risks, cost and benefits, and viable technical solutions hence they have a primary responsibility for their system's security

Does that work in global context: what are the specific issues in cross-border cooperation?



**Clearly some
tension**

TXkIdbsHSVWaIdwZvYImcBo4taN0hpp9zmQd3EgyG1+60vLtPXMgMhQwOQ900ECUeo3+HdqnoVqs77rzPOMPcHNoZAQVPgrImXTYfGh17gsWfzOxF
Y954CC5QeHoG+11oUmJLu5uRu358TaG1YbH17CG7mBk+fedEhmRc7+VJL8co3A7W2xyqzN
+AADV09FxeWRp5i8vSsOibxJCwFzOknQmHXcXG80KtNsKaMACRWZPaWTB84b1HI
+9D23XhYeCmzhzaHqRjivQuBpC7KS5hf1odjjmOk0f6rEIkAgE4QQ4H2wKwelsp6p1ESKYmUdAx9ik2nlqbLxDneZJG4xNfSR0D0X9gX8/
ay8TTRWf7oH8GmfOebcFGtLbXvkRv2YjumPvNRmScPfzml3ouQahXlj+0IqypHq7J9NA5hppQr0DQ1FWOC1PQIm92Td0/
bJOIqjRlgdYYkJBXJWQZtnLZpqi/sDuAGag5kbLPVAoGT3rDLQ0uQpopR/
zJKVAcnfXFFWofQLTPz4t03xHK2rm4kwcgVL18quzRn5ZRZXU26TGpM7iCNkrihhL5R1hPjIXwCRSaowVd81XuM/
QgF68h1oTla8Yb100q1Iis3qp1ZhuP33LgELyKbhak9x20ZC/t+P7Vf9rh9K4o/3RN19Tv60Cp885i40IynFwWEbaDzQTVoV3rGHwz5mjQHSy/

What are your thoughts?

iiigPchPZTg94yck18astDFdSvguUT0536jBazfuLOZwaadw1Edoz6trK9YK13yysPcBXIRUQXRpKkI/Zs/
MHtVKXP769AZTHmicrV9pvnXAYSVBcuLLwQLpez9HcQTBSTyFW46WwAcYvVEvE8F0hAp+ju0g6sVUsz3SnHGmP6/
TXkIdbsHSVWaIdwZvYImcBo4taN0hpp9zmQd3EgyG1+60vLtPXMfIUOX11jv1/5zni5j/zc+bZLbL4x+5ZBCfi3hu7vyI
+IhQSuMqLEYFWGHIHicxnoZj6AXj3b6t9xkqd37Q37WdscBR8hfoQcjwxY2nzCW7DWYtCpD0CgrLwQzR574g040te/
kz5veOrNXjQ8AUaVRh2zFJC2/+vcjcnIvNtsb1lgI764EgRcNcbvX17s0+insjOd3wiQLnNUKArLW0Elji6mFuguQABYXdIFCDVf6qDQPaQIf6v0JGjAMzWwCu6D7kXj
lRK3DZdzOEZK+fd4zZHTADwusNFPddCp3QUlKp0R5/Wl+wDnZef53Fh+eQkdGjpEVv11fCKYa9kZMSw3LaMjc1/L5c7c5RZgD4q6vXFPDGuxoEJmRmVDnPiW
+gxOm71xuWgnNbpTwSqrGEiQrfdDsc1U5gTk8TCmJqGkxWcTDEJdw0jHplAF1Jub84cd7nDJObxVPWQXz2CI/ndT...RSH2Iop1e7YWJx03kF3L
+YrPtqXyBki8cBWUg7rJQj3zr7myFXTHkGkiOB5x47q53rHdqyxEWtmdNXA3s...
+mCnzlNoSqE4DLz56VIjrbavnlZwityr9oRWq7AsNiVPVXUAX6MfgjL7avi...UIJff/
mzdNz4EcdmLOUpWznR2p133yJyF2hw9csDtmVcv8d9XFSqluFPnqaxjEaRae3YwIcGuVnO...8qSdiJZHwWSdo/jkRRyGsn/
32McAhXQYE7KBeTD3aoHCufHVSQjunhxOLSd96D2lzfNLSQSjXh1CYmTqqQTSQ...ludIBNXD+zligYJ
+JvhdCCIsDyGOEHkz8Yt70QbG/lg89jhC6nAxEgaaFhpRiC6nNeFU...mEnE/
gMhQwOQ900ECUeo3+HdqnoVqs77rzPOMPcHNoZAQVPgrImXTYfGh17gsWfzOxF...aG1YbH17CG7mBk
+fedEhmRc7+VJL8co3A7W2xyqzN+AADV09FxeWRp5i8vSsOibxJCwFz...
+9D23XhYeCmzhzaHqRjivQuBpC7KS5hf1odjjmOk0f6rEIkAgE4QQ4H2wKwelsp6...X8/
ay8TTRWf7oH8GmfOebcFGtLbXvkRv2YjumPvNRmScPfzml3ouQahXlj+0IqypHq7J9NA5hppQr0DQ1FWOC...WQZtnLZpqi/
sDuAGag5kbLPVAoGT3rDLQ0uQpopR/zJKVAcnfXFFWofQLTPz4t03xHK2rm4kwcgVL18quzRn5ZRZXU2...owVd81XuM/
QgF68h1oTla8Yb100q1Iis3qp1ZhuP33LgELyKbhak9x20ZC/t+P7Vf9rh9K4o/3RN19Tv60Cp885i40...y/DL5jJvt/
...aOfYIARbHhw3zT/
...d8gGOWthYdRxmAI
...3GC0krUEUJJWT
...WNdXkznln9KXwv
...bmPh5a
...mc8g4/
EkyLg4FzHrSmow+3REM...

Technical

Societal

Political

Operational

With Global impact

These are questions that cannot be answered in isolation





Backup

Internet Society Resources on encryption

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

IGF 2015 Brazil, Joao Pessoa (November 2015)

REPORT:

Workshop 141 - Law enforcement in a world pervasive encryption

Report by: Nicolas Seidler

with input from Jairus P

Encryption

An Internet Society Public Policy Briefing

Encryption technologies allow Internet users to protect the confidentiality of their data and communications from unwanted observation and intrusion. Encryption is also a technical foundation for trust in the Internet. Encryption enables freedom of expression, commerce, privacy, user trust and helps protect users' data from bad actors. For this reason, the Internet Society believes that encryption should be the norm for Internet traffic and data storage.

Some law enforcement agencies have expressed concern that encryption to hide their activities or hijack users' data (e.g. user trust and helps protect users' data from bad actors. For this reason, the Internet Society believes that encryption should be the norm for Internet traffic and data storage.

Some law enforcement agencies have expressed concern that encryption to hide their activities or hijack users' data (e.g. user trust and helps protect users' data from bad actors. For this reason, the Internet Society believes that encryption should be the norm for Internet traffic and data storage.



Who We Are

Home | Connect Login | Become a Member | Find a Chapter | Blog

What We Do

Why It Matters
How We Work
Where We Work

Issues

Access
Children and the Internet
DNSSEC
DNS
Encryption
Human Rights
Innovation
Interconnection and Traffic Exchange
Intellectual Property
Internet Governance

What We Do

Events

Publications

The Internet

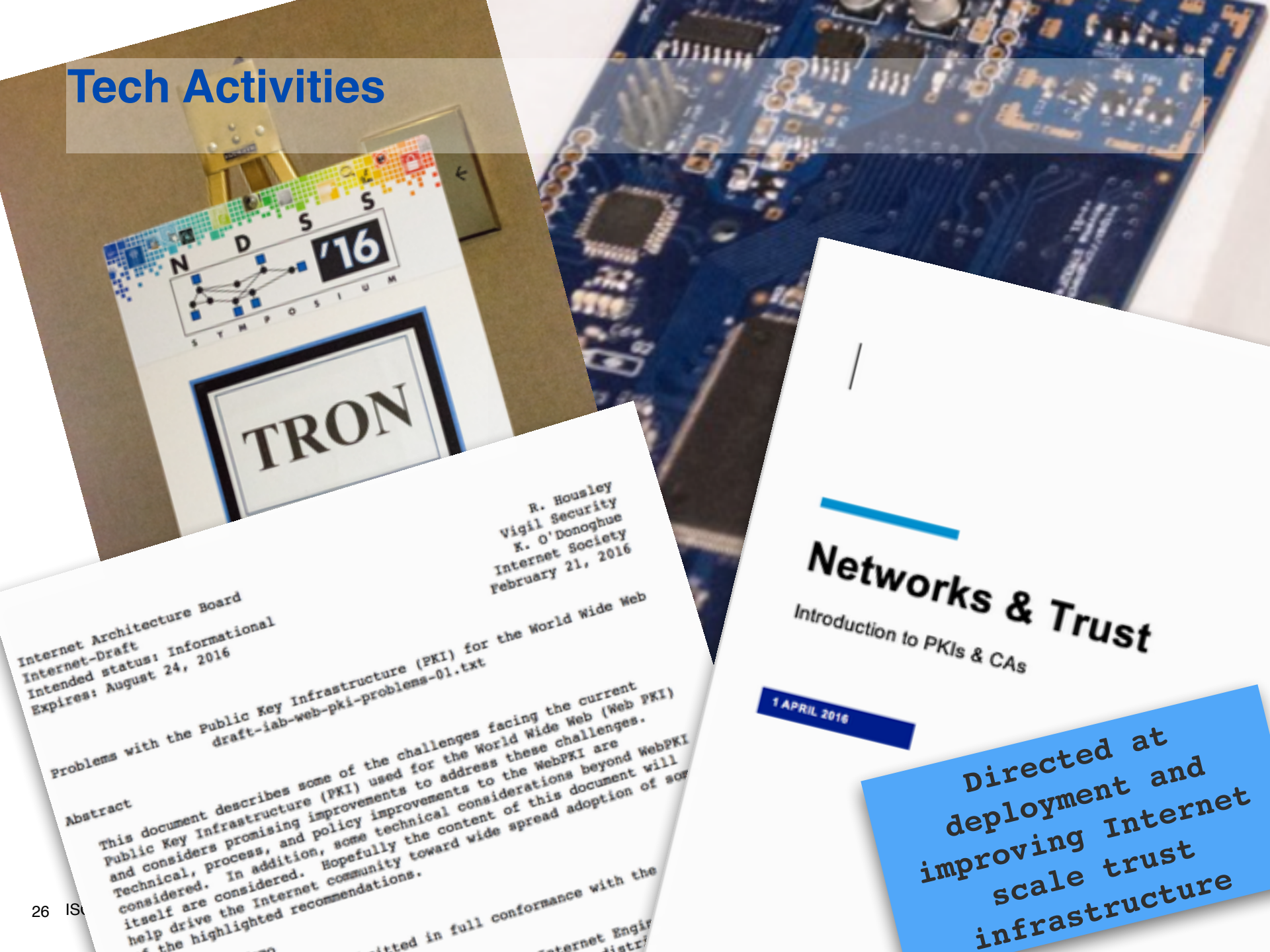
Home • What We Do • Issues • Encryption

Encryption



Policy Brief on Encryption is being finalized after review period ended April 1

Tech Activities



Internet Architecture Board
Internet-Draft
Intended status: Informational
Expires: August 24, 2016

R. Housley
Vigil Security
K. O'Donoghue
Internet Society
February 21, 2016

Problems with the Public Key Infrastructure (PKI) for the World Wide Web
draft-iaab-web-pki-problems-01.txt

Abstract

This document describes some of the challenges facing the current Public Key Infrastructure (PKI) used for the World Wide Web (Web PKI) and considers promising improvements to address these challenges. Technical, process, and policy improvements to the WebPKI are considered. In addition, some technical considerations beyond WebPKI itself are considered. Hopefully the content of this document will help drive the Internet community toward wide spread adoption of some of the highlighted recommendations.

Submitted in full conformance with the
Internet Engineering Task Force (IETF) Policy on Intellectual Property Rights

Networks & Trust

Introduction to PKIs & CAs

1 APRIL 2016

Directed at
deployment and
improving Internet
scale trust
infrastructure

Olaf M. Kolkman

Chief Internet Technology
Officer

Kolkman@isoc.org

twitter: @kolkman

ISOC's General Principles

Encryption should be the norm for Internet Traffic

Weak Encryption is as bad as no encryption

There is a strong technical consensus in the tech community that Cryptographic backdoors are no-go territory.

Nuances

Encryption impacts operations and law enforcement activities