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

Internet Society™

1994 Clipper

1996 RFC1984

June 2013 - NSA breach

May 2014 - RFC7258

September 2014 - IOS 8

Jan-Dec 2015 - Letsencrypt got viable

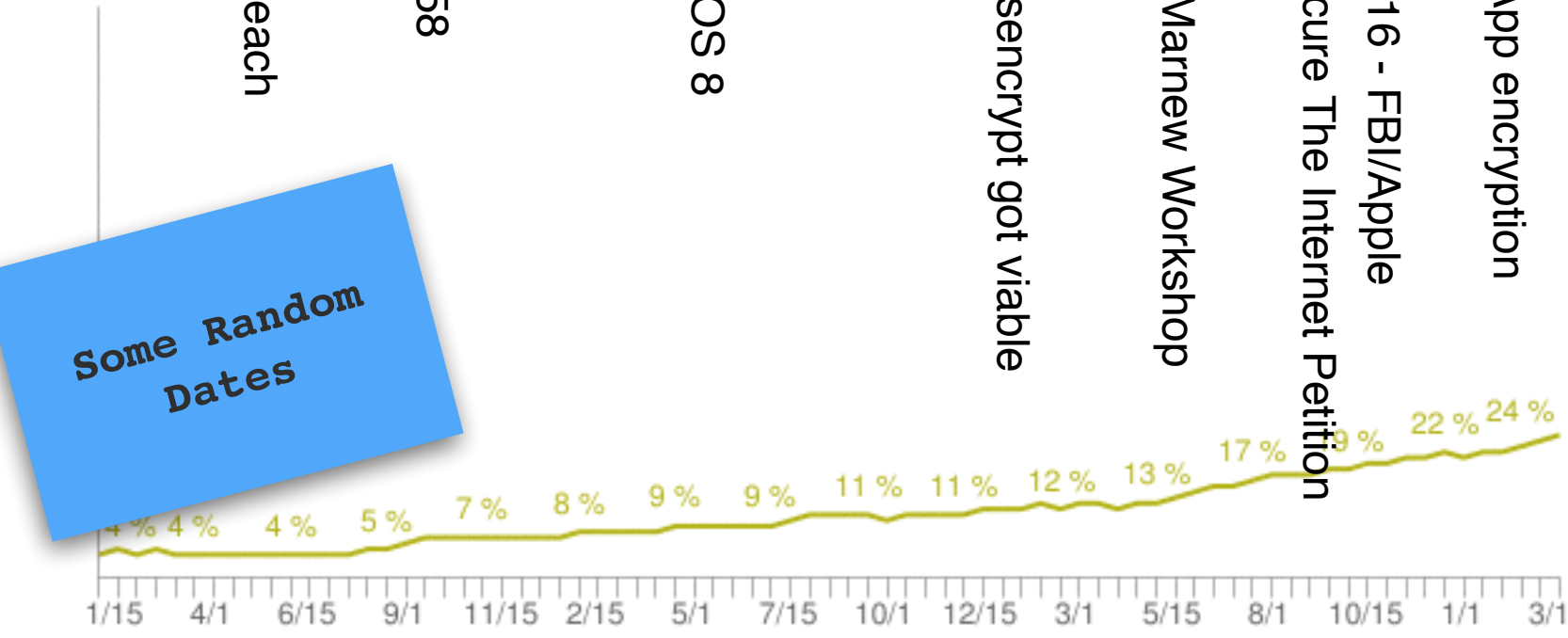
September 2015 - Marnew Workshop

February 2016 - Secure The Internet Petition

February-March 2016 - FBI/Apple

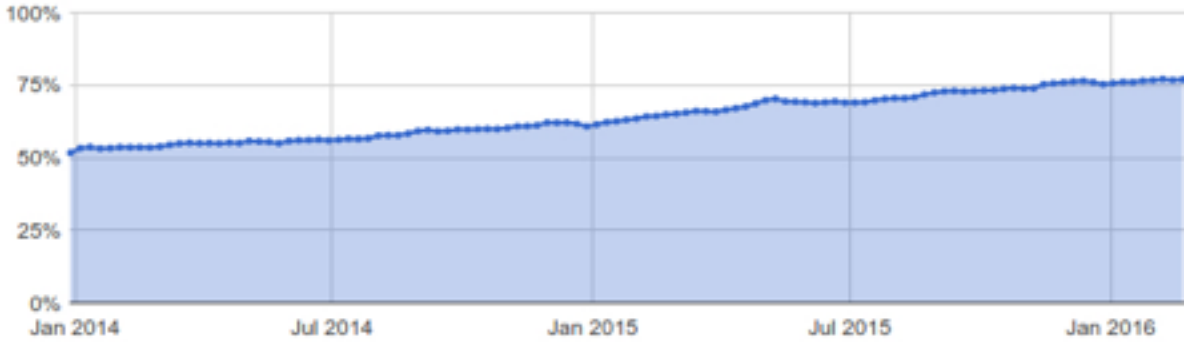
April 2016 - WhatsApp encryption

Some Random Dates

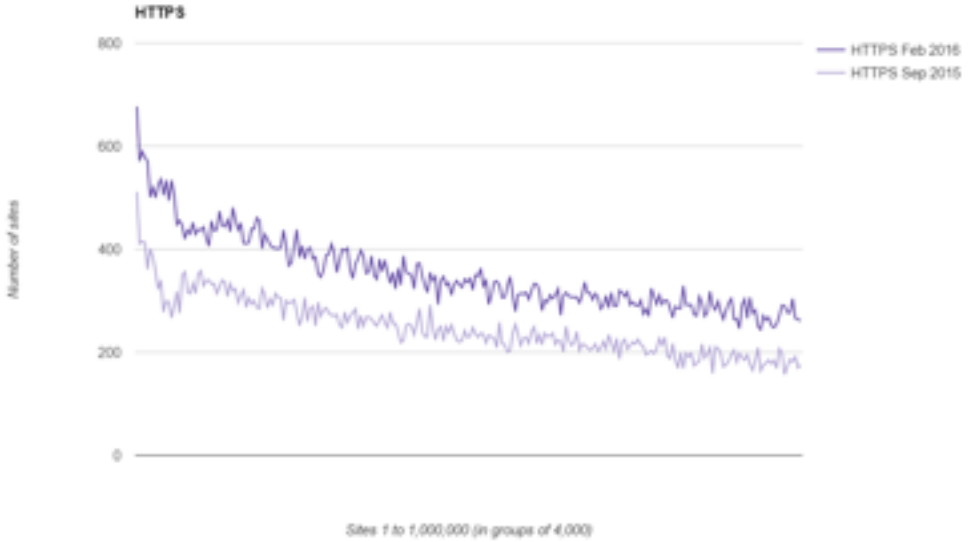


http://httparchive.org/trends.php?s=Top1000&minlabel=Jan+1+2013&maxlabel=Mar+15+2016#perHttps

Encrypted Traffic continues growing



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



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

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

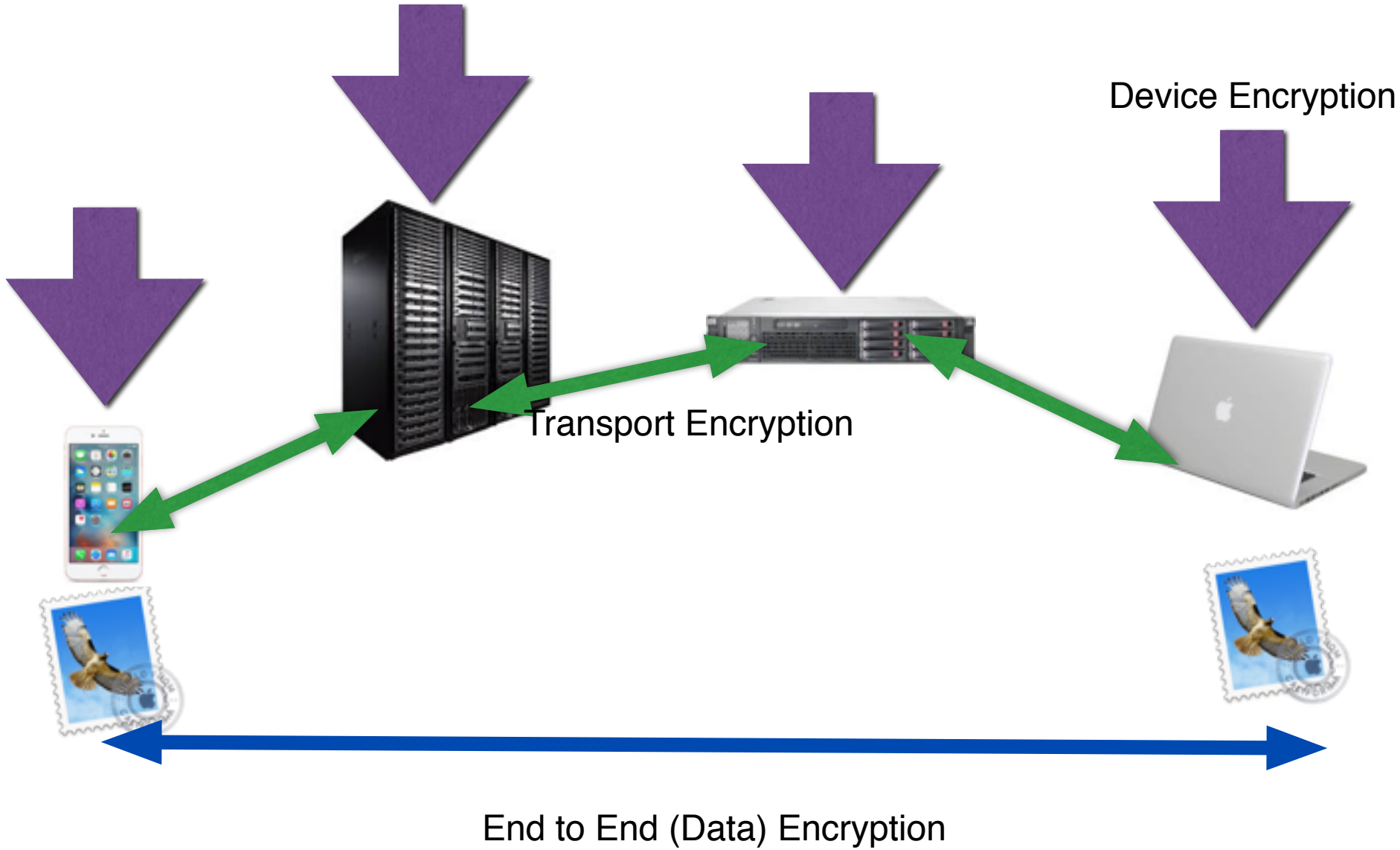
Encrypted traffic

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

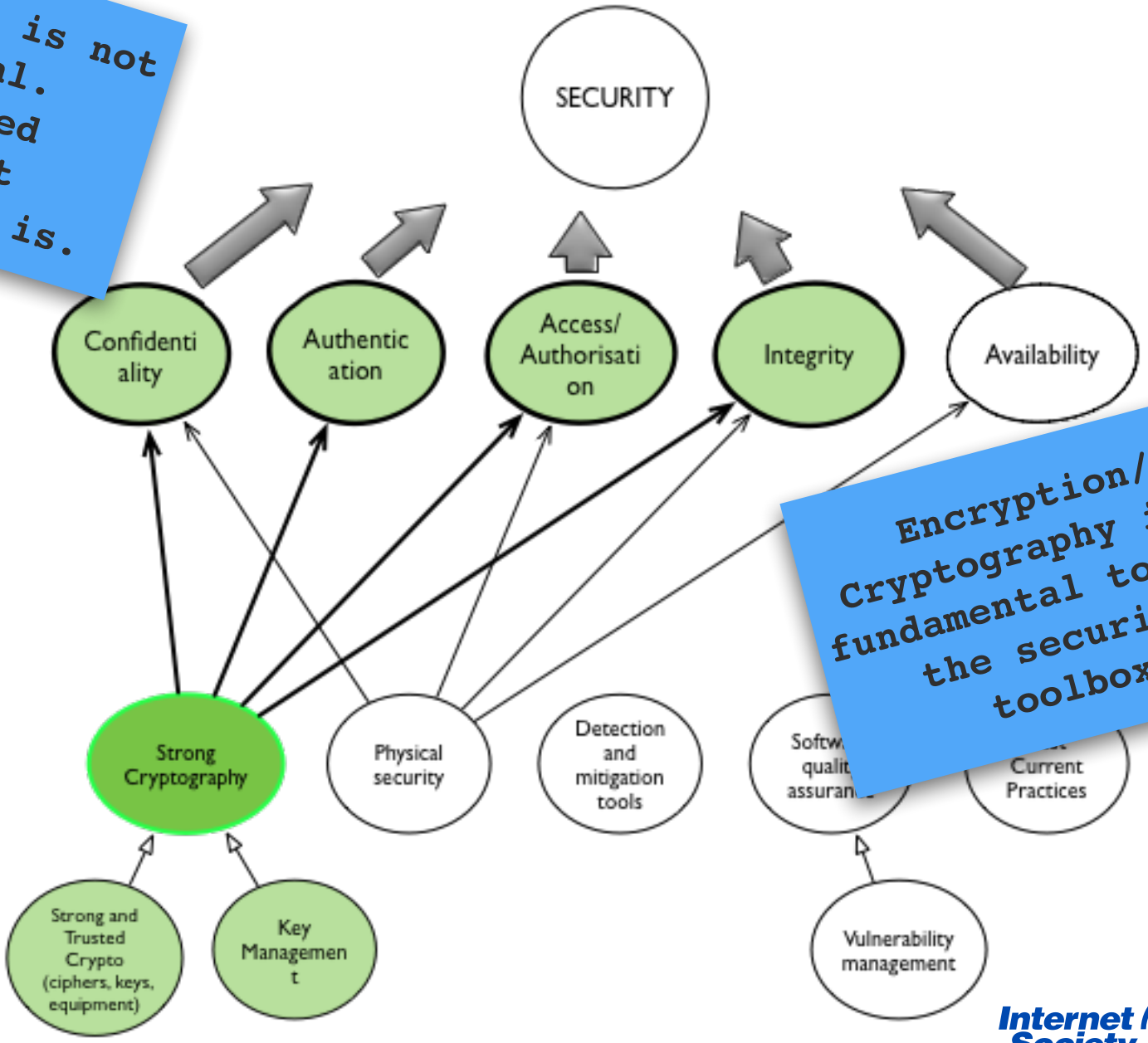
The Economy depends on Encrypted Traffic

Some attributes of the communication are not encrypted.

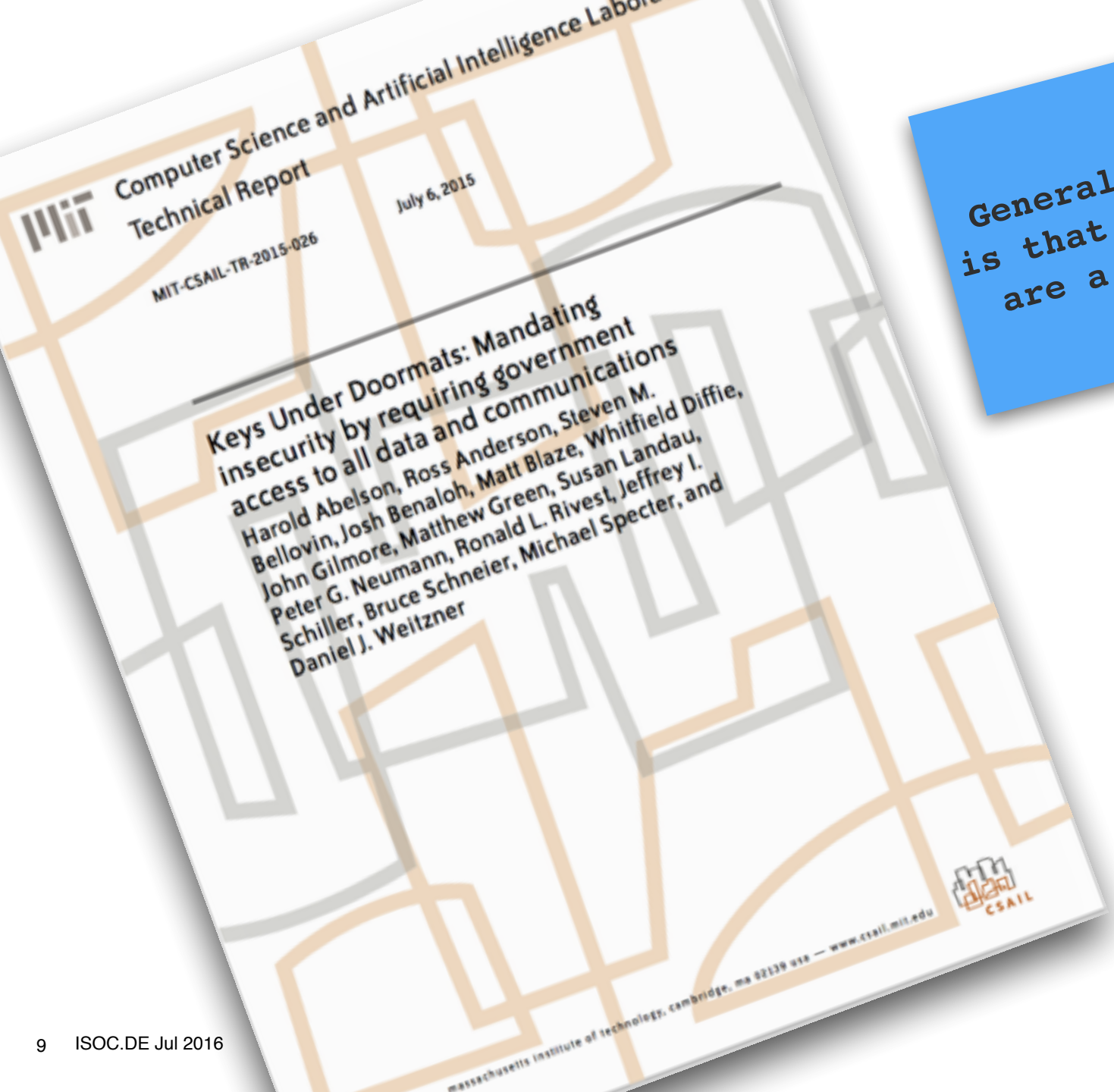
The evolution impacts what law enforcement sees and how operators perform some network management functions.


Device Encryption
Transport Encryption
End to End (Data) Encryption

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

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 reached.

Introduction

Any cybersecurity framework needs to start with a
Internet (open standards, voluntary collab
innovation and global reach ("the
cybersecurity landscape
and social pro
of tru

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

Can a company be compelled to weaken its products security?

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:

…place to assess risks, cost and benefits, and …al solutions hence they have a primary …or the …m's security

They should be empow… …he best possible security solutions for their p… …vices

Industry should, under parameters … rule of law … …operate with law enforcement, whilst not sacrifi… …les above.

Governments should create the best … …or improving System Security.

Not just a Law-Enforcement issue

A general Cyber Security issue

Broadly applicable

Including IOT

* This is not (yet) ISOC's position

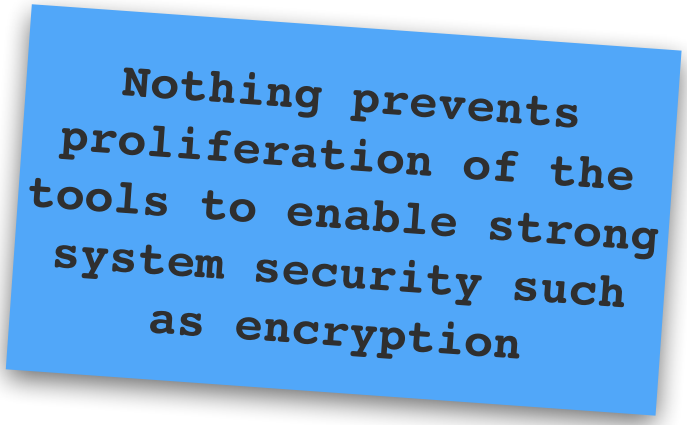
Some Questions and observations

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

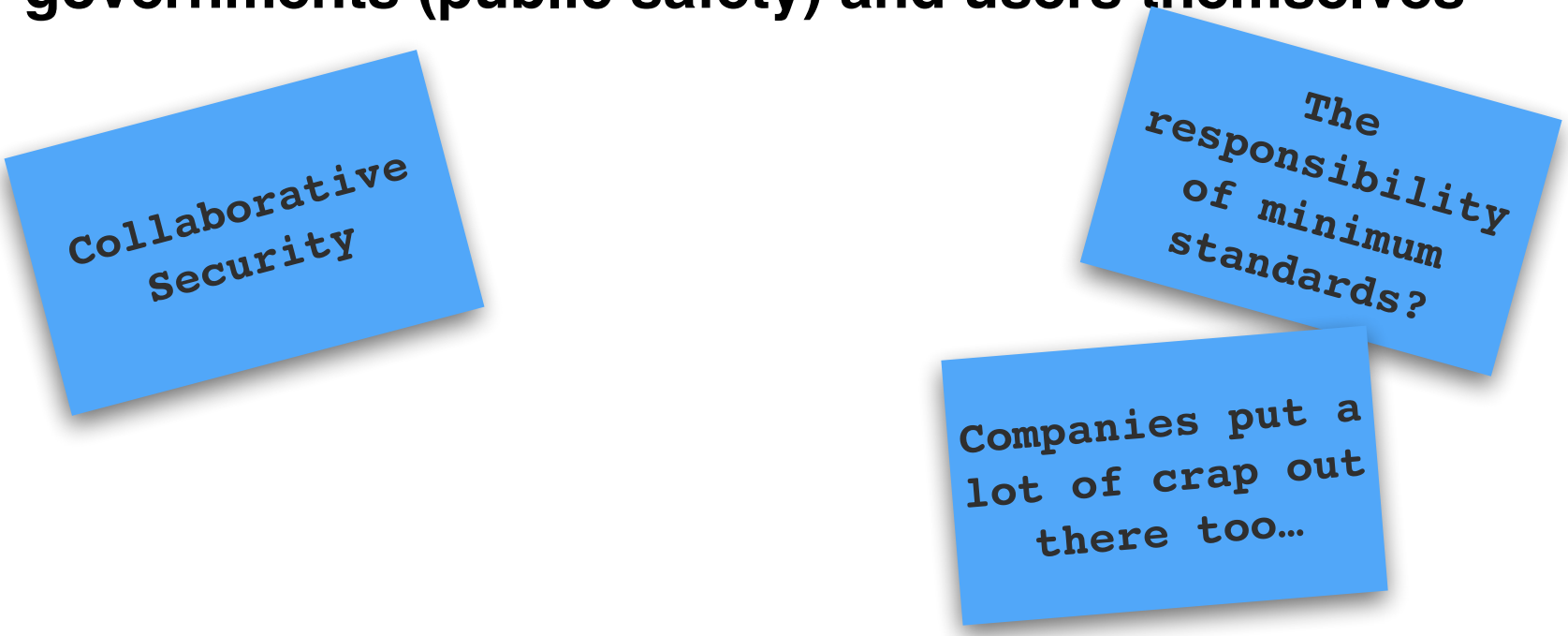
But how does that relate to the use of exploit kits by law enforcement?



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



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

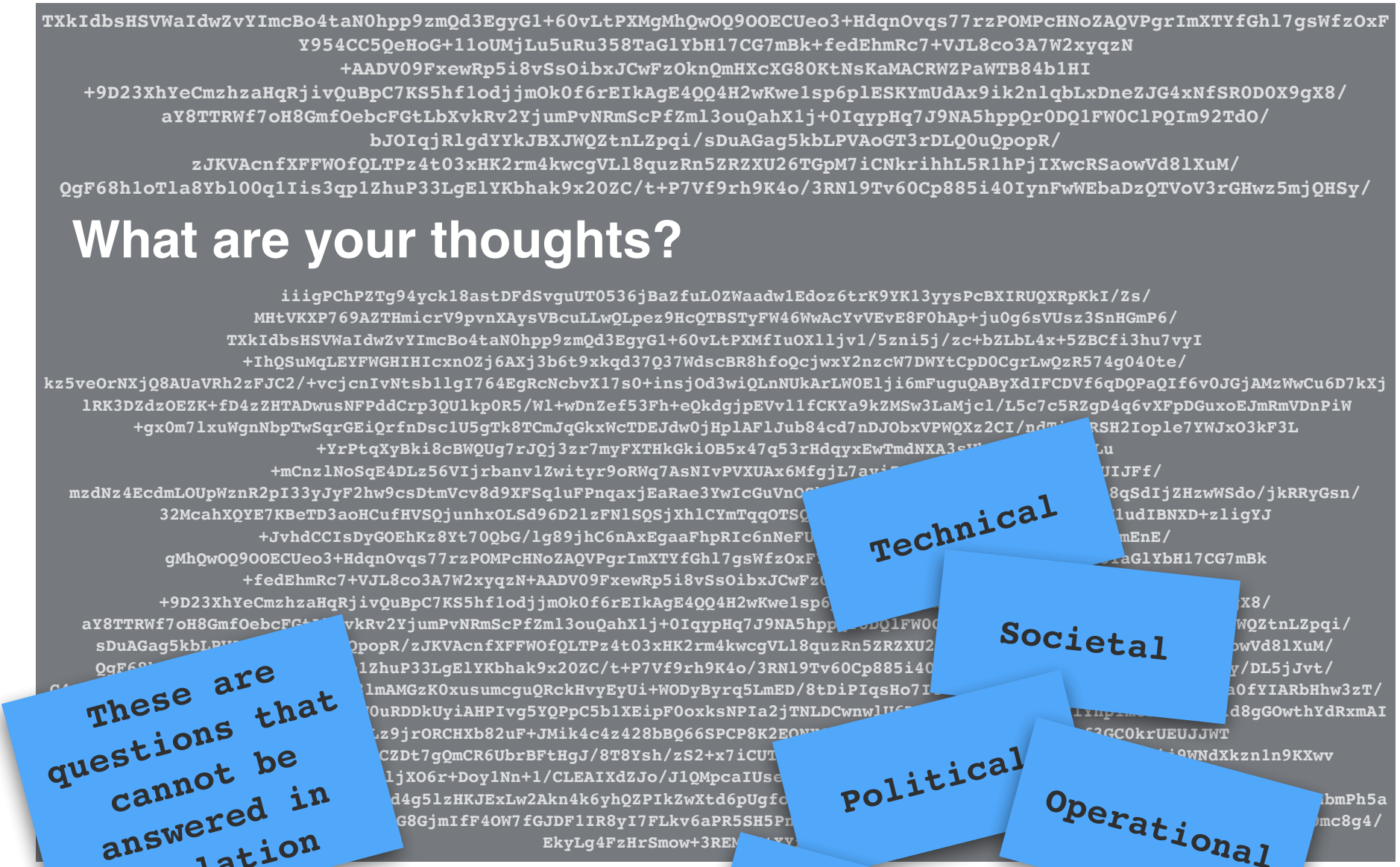
How about the procurement and use of (existing) exploits by law enforcement?

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?

What are your thoughts?



Backup

Internet Society Resources on encryption

http://www.internetsociety.org/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-iab-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.

itted in full conformance with the

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

Internet Society™

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

Internet Society