"What Must We Do?"
Industry Reactions to
Pervasive Monitoring Programs

Joe St Sauver, Ph.D (stsauver@fsi.io)

Scientist, Farsight Security, Inc.
Senior Technical Advisor, M^{3}AAWG

SECURECOMM, Dallas TX

https://www.stsauver.com/joe/securecomm/

I. Introduction

Thanks and a Disclaimer

- I'd like to begin by thanking the SECURECOMM Program Committee for the opportunity to speak with you today. It's a real pleasure to be with you here in Dallas today.

- The remarks I'll be sharing with you represent my own opinion, and do not necessarily represent the opinion of any other person or organization.

My Background

- I'm a scientist for Paul Vixie's new company, Farsight Security. Farsight operates DNSDB, the world's most comprehensive source of passive DNS data, collected above recursive resolvers in a privacy-preserving way. (See www.farsightsecurity.com)
- Prior to coming to Farsight, I worked for roughly 28 years at the University of Oregon, including 8 years or so under a UO contract with Internet2 as their Nationwide Security Programs Manager. Internet2 is higher education's high speed nationwide backbone, with most connections running at 10 to 100 Gbps.
- I'm also one of half a dozen Senior Technical Advisor for the Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG).
- More details about me (and copies of many of my talks) are available online at https://www.stsauver.com/joe/

Speaking of My Talks, They Have An Odd Format

- Traditionally, most PowerPoint talks have:
  - A limited amount of text, which then gets "amplified" during delivery
  - That's fine for **non**-technical material and for the people who may be in the audience at the time the talk was delivered. It's a poor fit for technical content (where there can be a lot of detail), or for *post hoc* readers.
- My slides tend to use a different, more detailed, style:
  - I hate being misquoted. Detailed slides reduce the level of misquoting.
  - Because my slides are detailed, you shouldn't need to take notes.
  - Having detailed slides gives me a chance of covering everything I want to cover, and finishing on time. If I nonetheless still somehow fail to stay on track, you'll at least have a copy of what I meant to go over.
  - I'm also committed to making my material accessible to everyone, including non-native English speakers, and the deaf and hard-of-hearing. Thus, think of these slides as providing a transcript or "closed captioning" for my remarks.
  - You're welcome to share these slides with any interested colleagues who weren't able to be here in person today.

Today's Topic

- Today I'll be discussing some of the work that M^{3}AAWG's anti-Pervasive Monitoring Special Interest Group has undertaken, since it is highly relevant to SECURECOMM's focus on secure communications and Internet privacy.

- Before diving into that, I want to first make sure you understand M^{3}AAWG's role, and how the anti-Pervasive Monitoring SIG fits within M^{3}AAWG.

M³AAWG In One Slide

- M³AAWG is the Messaging, Malware and Mobile Anti-Abuse Working Group. It's where the industry works on problems of bots, malware, spam, viruses, DDoS and other online exploitation.
- M³AAWG's leadership: https://www.m3aawg.org/leadership
- Member organizations: https://www.m3aawg.org/about/roster (member organizations represent a billion+ mailboxes worldwide)
- M³AAWG normally meets face-to-face three times a year: in San Francisco, on the East Coast (or in Canada), and in Europe.
- In general, "what happens at M³AAWG stays at M³AAWG" (except for published documents, publicly released videos, and other intentionally-shared content)
- Today's presentation will gives you a "peek behind the curtains," and is offered with the explicit permission of M³AAWG's Executive Director and M³AAWG's anti-Pervasive Monitoring SIG co-chairs.

A Summary of the Anti-Pervasive Monitoring SIG

- Ongoing disclosures about the pervasive monitoring of email, voice and other network traffic remain an industry concern.
- Public and technical communities have increased interest in measures that could protect operational security and customer privacy.
- Leading M^{3}AAWG members have been publicly identified as specific targets for this non-consensual eavesdropping activity.
- An industry-coordinated response to this threat is necessary due to interoperability and "deployability" considerations.
- The M^{3}AAWG anti-Pervasive Monitoring SIG strives to
  - provide technically sound yet approachable advice on complex topics, while
  - providing a balanced perspective and
  - coordinating our efforts with other organizations.

My Personal Perspective On A Few Points

- **OVERARCHING BELIEFS:** The Internet is a transformative invention, and has unique capabilities we must protect & preserve.
  - Messaging (email, IM, VoIP, video, etc.) is a very important part of what the Internet enables
  - Pervasive monitoring is as much of a threat to the continued viability of the Internet as spam, malware, phishing, or other often-mentioned threats.
- Although we all want to be safe from crime, terrorism and war, there must be limits to the means employed, including:
  - Respect for rule of law (e.g.: no torture, no extraordinary renditions, etc.)
  - At least in the United States, respect for the Constitution and the Bill of Rights, including its protections against unreasonable search and seizure
- The greatest risk from terrorism (except terrorism involving weapons of mass destruction) is the damage resulting from over-reaction – we can't allow terrorists to use "mental jujitsu" (forcing us into abandoning hard won liberties in an effort to remain safe).
- Most people are trying to do the right thing (as they understand it)

My Personal Perspective: Service Providers

- **SERVICE PROVIDERS:** SPs are often very large, and may be highly compartmentalized. What one employee does may be unknown to virtually all of the rest of the company, and potentially even to parts of the executive management team or the company's Board of Directors (they may not have clearance or a "need to know").
- We cannot assume, therefore, that any representatives of an SP will have full knowledge about what an SP may in fact be doing.
- SPs require government permission (licenses) for many of their activities, including wireline and cellular operations, international operations (FCC Sec. 214), international cable landing sites (https://transition.fcc.gov/ib/pd/pf/scll.html), etc. These licensing requirements give governments substantial power over SPs (to say nothing of governmental "powers of the purse" w.r.t. contracting)
- We should also note that SPs have the right to monitor/protect their own infrastructure & operations (18 U.S.C. 2702 (b)(5))

Criminal Law Enforcement Officers (LEOs)

- M^{3}AAWG welcomes criminal law enforcement officers, and supports their work to fight spam and phishing, take down botnets, fight online child exploitation, tackle DDoS attacks, etc. M^{3}AAWG expects criminal law enforcement to diligently enforce existing laws, and to do its job in a way that allows all collected evidence to be readily used in prosecutions. We are consistently impressed by the hard work and due diligence we see from them.
- Evidence of this? An FBI agent received M^{3}AAWG's first J.D. Falk Award for his work in establishing the DNS Changer Working Group and protecting end users, see https://www.m3aawg.org/fbi-agent-thomas-x-grasso-receives-first-jd-falk-award-establishing-dns-changer-working-group-and-pr)
- You can also hear Michael Moran of Interpol talking about law enforcement's work fighting online child exploitation at https://www.youtube.com/watch?v=Qc5xBL5NRHA

The Intelligence Community (IC)

- The existence of hostile nations (and hostile organizations abroad) means that foreign intelligence collection needs to be assumed to be a universal reality of modern international relations.
- The IC zealously attempts to collect all available information in an effort to have a fully informed basis for their analyses and policy recommendations, subject solely to technical limitations and any operational limits they choose to accept/acknowledge (effective external oversight may be impossible as a practical matter today).
- Domestic intelligence collection in the United States is, and must remain, subject to 4th Amendment limitations. Domestic dragnet surveillance/pervasive monitoring exceeds those limits, even if done with the most noble of intentions.
- We also must assume that even if the U.S. intelligence community isn't targeting domestic network traffic, foreign intelligence services may nonetheless be attempting to do so.

The Result?

- There's a need for M^{3}AAWG and its member companies to take appropriate action to protect their services and users from attempts at pervasive monitoring, whether done by the U.S. Government or by foreign powers.

II. The Origin of M³AAWG's Anti-Pervasive Monitoring Work: Snowden's Initial Disclosures

M³AAWG 28 Was Being Held In Vienna, Austria, When The First Snowden Article Was Published

https://commons.wikimedia.org/wiki/File:Hotel_Hilton_Vienna_August_2006_001.jpg
https://commons.wikimedia.org/wiki/File:Au-map.png

Remember This Headline? I Sure Do...

NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama

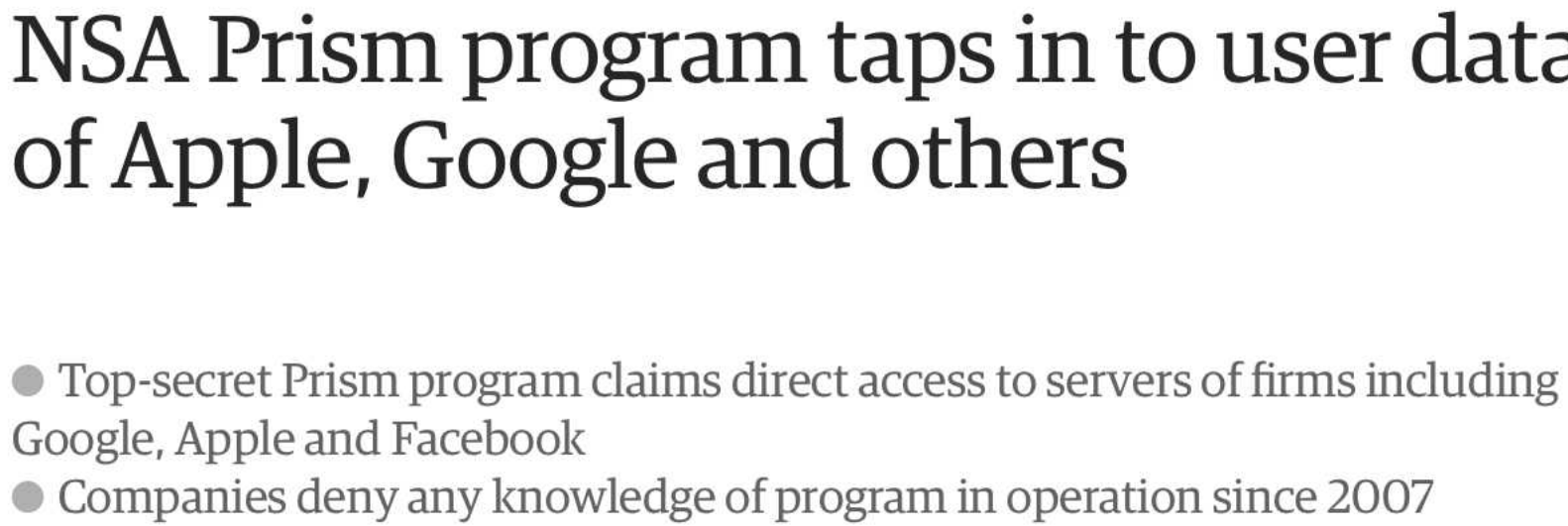
- Read the Verizon court order in full here
- Obama administration justifies surveillance

www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
[notwithstanding the URL, this article was actually published on the 5th of June, see http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline]

Reactions

- Many were angry, shocked, and dismayed over what was reported by *The Guardian* and other news outlets.
- ***Online pervasive monitoring of domestic customer metadata?*** What about Constitutional protections against unreasonable search and seizure? What about Americans' right to privacy?
- This pervasive monitoring was even viewed by some in the community as a *personal affront.* It takes a lot of effort to build and run complex Internet-scale systems. Technical people tend to throw themselves into their work and take great pride in how they build and operate their networks and systems, including the security and privacy thereof. Having that undercut by the U.S. intelligence community felt insulting, dismissive, and violative.
- Many also worried that Snowden's disclosures would cause a loss of customer confidence and be commercially damaging.

Another Shoe Drops



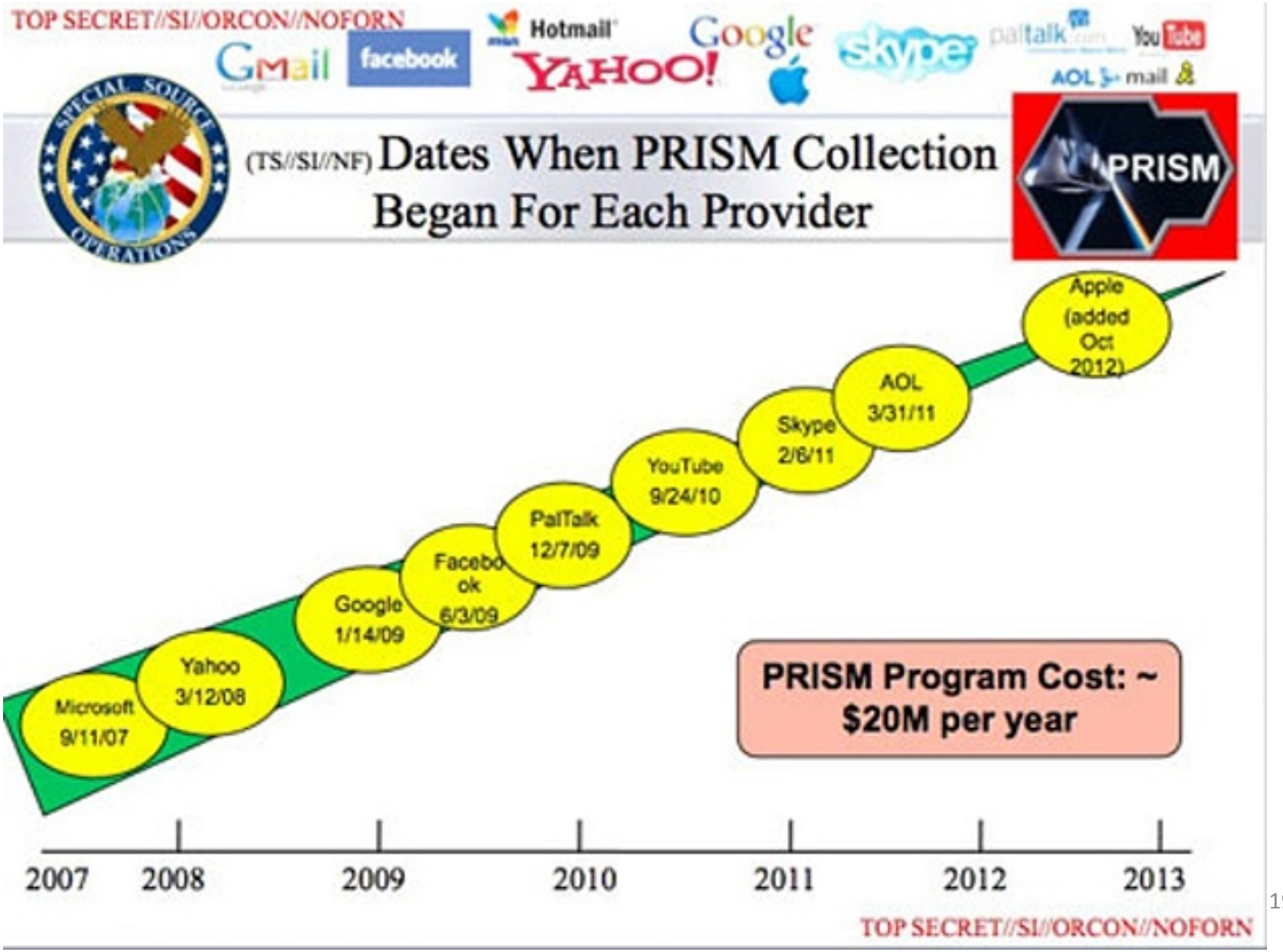
NSA Prism program taps in to user data of Apple, Google and others

- Top-secret Prism program claims direct access to servers of firms including Google, Apple and Facebook
- Companies deny any knowledge of program in operation since 2007

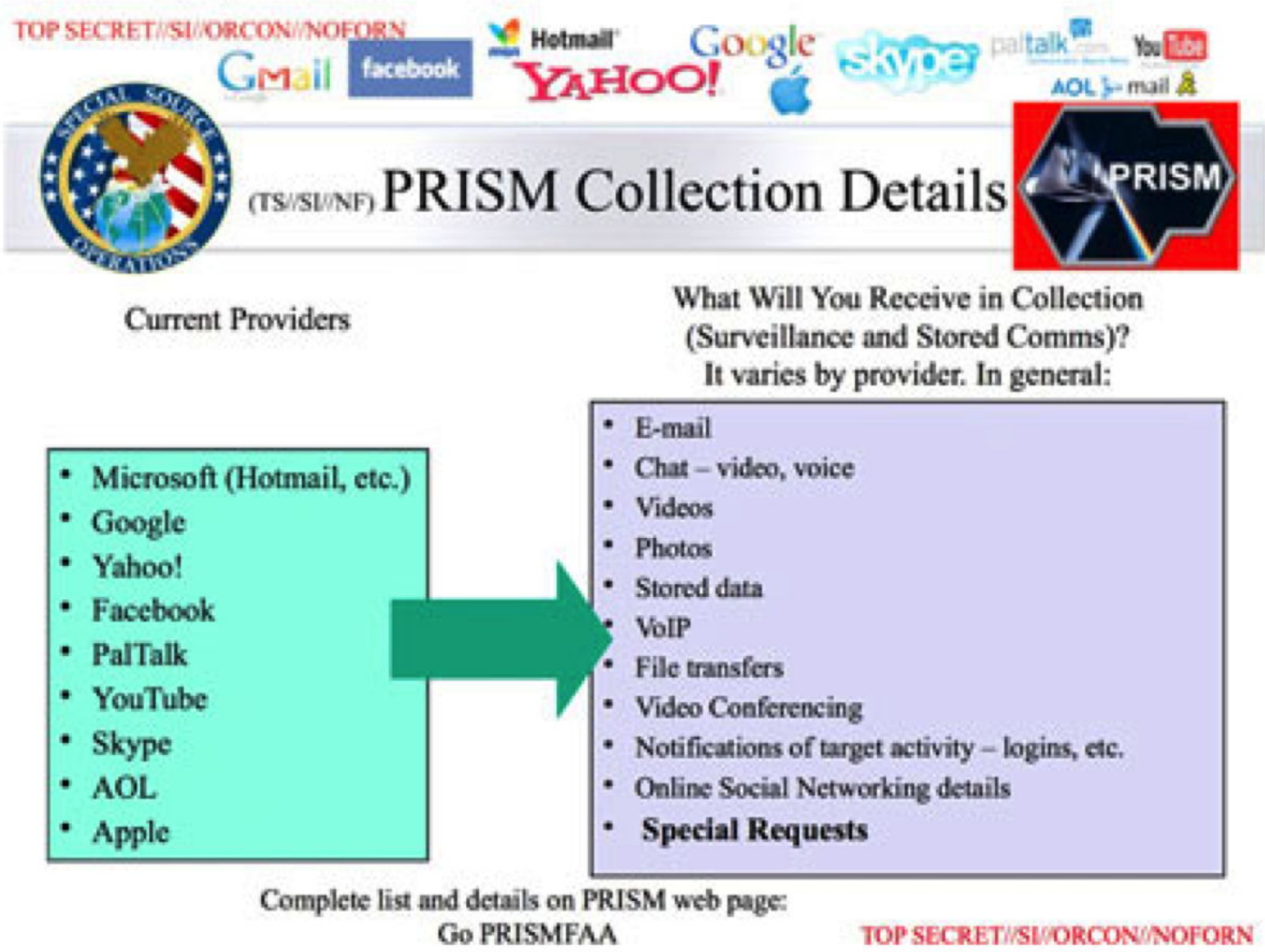
Source: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

- The first Snowden revelation was about the bulk collection of domestic **metadata.** While metadata can be hugely revealing, most average users have no idea of just *how* revealing it can be. Eavesdropping on **full message contents** on the other hand (Snowden's 2nd revelation, as shown here) is the troubling sort of behavior that even non-technical users can readily apprehend.

The PRISM Program Disclosure



What Has The PRISM Program Collected?



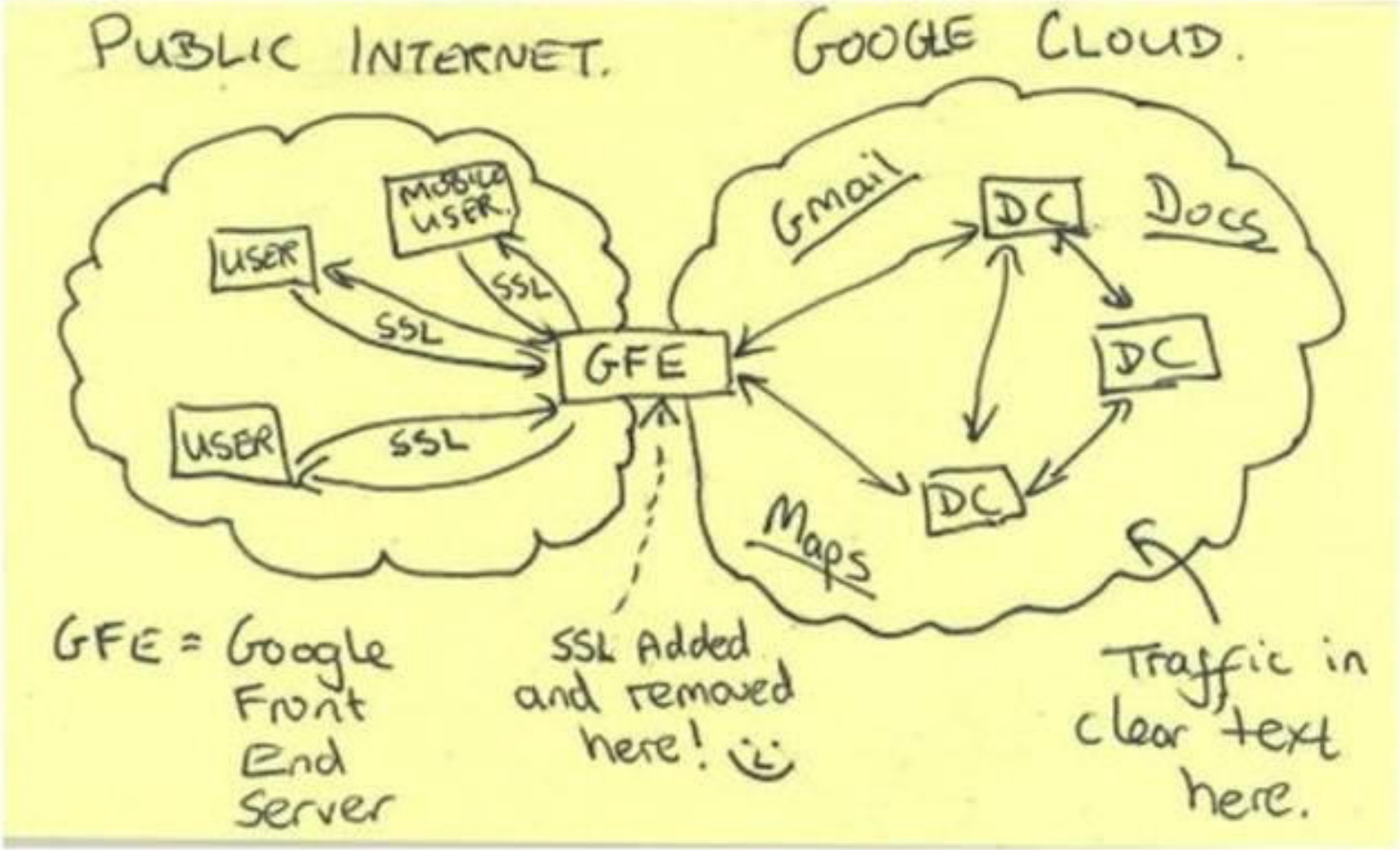
A Third Release (They Just Kept Coming), The Week After M^{3}AAWG 29 In Montreal, Oct 21st-24th

National Security

NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say

Source: Washington Post, October 30th, 2013.

Current Efforts - Google



Domestic Bulk Metadata Collection Had Been Going On For Years BEFORE Snowden's Revelations

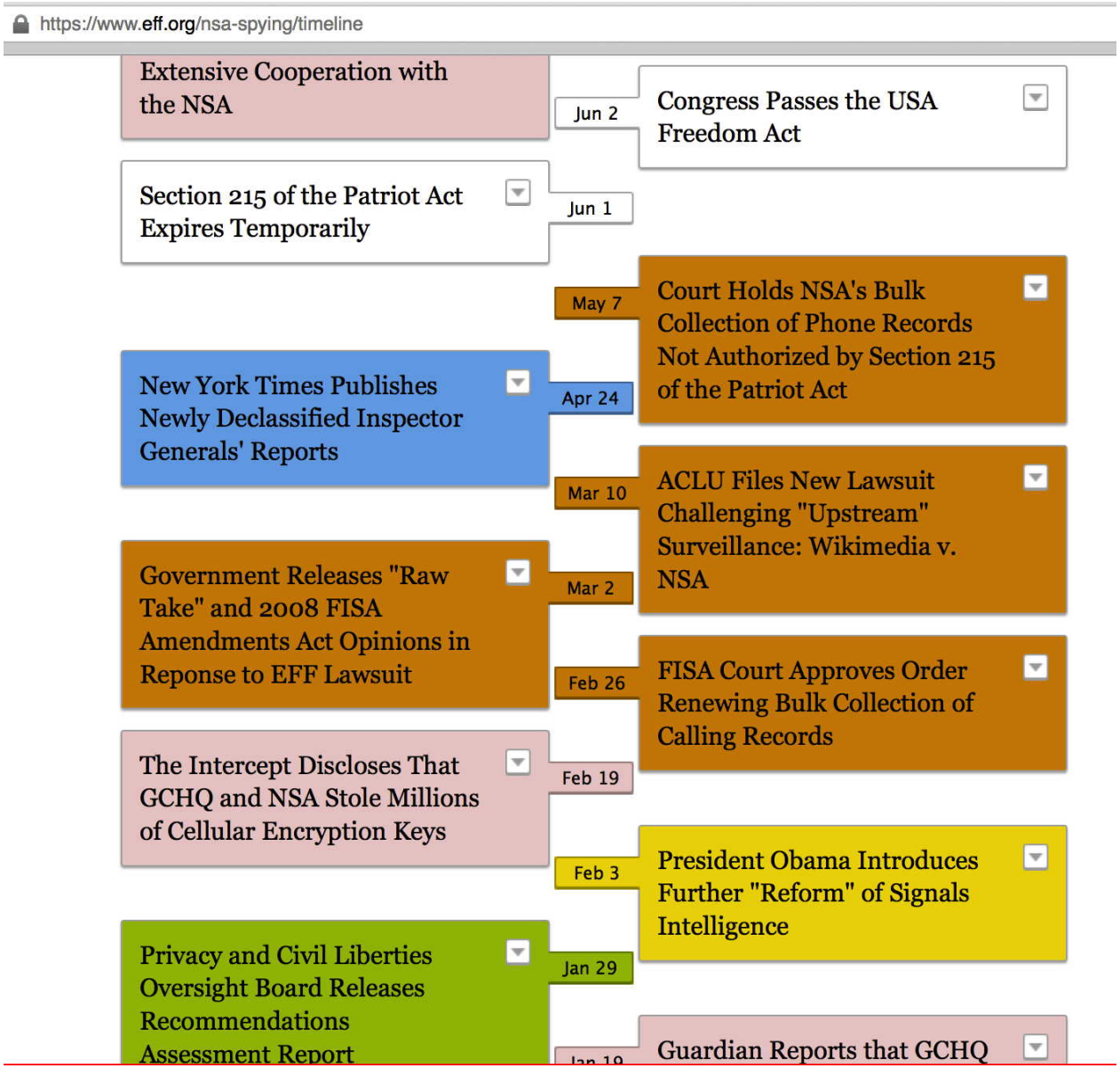
- On May 10th, 2006 USA Today published:

  "NSA has massive database of Americans' phone calls,"
  http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm

- That was **SEVEN YEARS** before Snowden's revelations.

- Even that report was **FIVE YEARS** after the President's Surveillance Program first began, shortly after the attacks of 9/11 occurred. See http://www.nytimes.com/interactive/2015/04/25/us/25stellarwind-ig-report.html

https://www.eff.org/nsa-spying/timeline



M³AAWG Reaction to All These Revelations

- M³AAWG's membership and leadership decided to create an anti-Pervasive Monitoring Special Interest Group.
- First output? The draft of a new document: "SSL/TLS for Mail: Some Initial M³AAWG Recommendations"
- More generally, M³AAWG also has proceeded to:
  -- identify and invite relevant speakers as guests,
  -- arrange for cryptographic training sessions,
  -- develop a broad "crypto roadmap"/work plan, and
  -- draft additional anti-pervasive monitoring documents.
- The remainder of this talk will discuss those efforts.
- As you listen to that program of work, please think about what you might suggest we add (or suggest we change).
- Perhaps you might even want to become involved with M³AAWG and its work in this important area.

III. Anti-Pervasive Monitoring-Related Videotaped Keynotes, Training Session Videos And Other Video Content

M³AAWG Public Videos

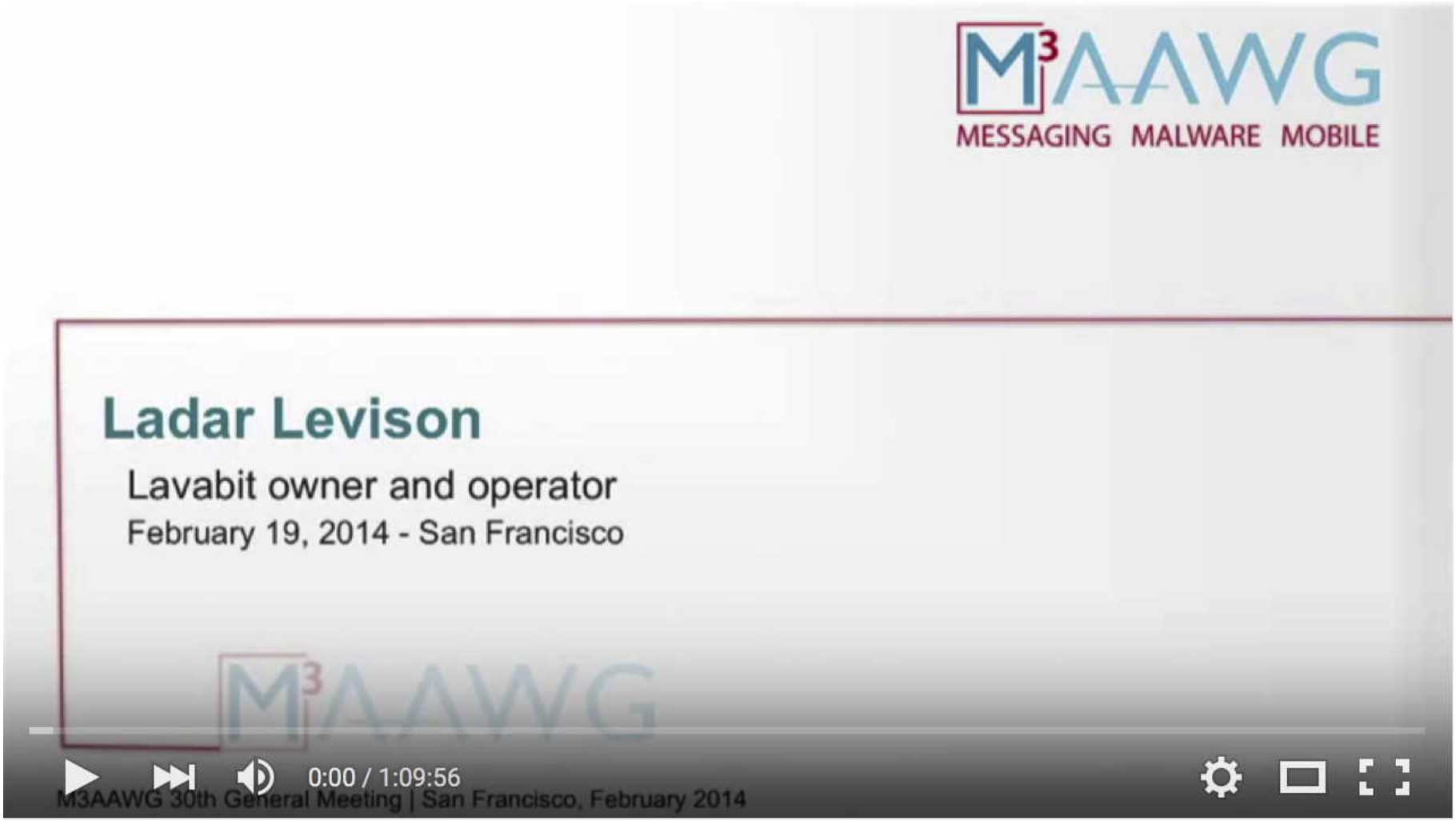
- M³AAWG meetings include a variety of types of sessions, including invited keynotes and in-depth training sessions.

- M³AAWG's public videos give you a unique opportunity to view selected meeting content that you would normally not be able to hear, and to hear from invited experts or M³AAWG's leadership.

- As you'll see in the following slides, a relatively large number of videos are available for topics related to M³AAWG's anti-pervasive monitoring work.

- Additional videos will continue to be added at https://www.youtube.com/user/MAAWG/videos

Keynote: M³AAWG San Francisco, February 19, 2014



Watch it at https://www.youtube.com/watch?v=kF-nnyDUOV8

Ladar Levison and Lavabit

- If you're not familiar with Ladar Levison and Lavabit, Lavabit was Edward Snowden's ISP, offering specially encrypted email services.

- After Snowden's revelations began to occur, the government surreptitiously sought to compel Lavabit to release their SSL/TLS certificate and associated private key. This would have completely undercut the security of all Lavabit users.

- This keynote talk described what happened during that incident, and makes for a fascinating session to watch.

Training: M³AAWG Brussels, June 9th, 2014

Part 1: https://www.youtube.com/watch?v=GmhSCH6TfSw
Part 2: https://www.youtube.com/watch?v=WLpipaCyCRg

Brussels Crypto Sessions

- As a practical matter, one of the things service providers need to harden their crypto posture is technical advice about how to best configure their crypto-enabled web servers, mail servers, etc.

- The Better Crypto Applied Crypto Hardening training was an excellent source of advice for the community, and the Better Crypto handbook remains available online at

  https://bettercrypto.org/static/applied-crypto-hardening.pdf

- During the Brussels meeting, we were also fortunate to have Christopher Meyer do a track session on the state of TLS. Video from that session is also available, see the next slide.

Track Session: M³AAWG Brussels, June 10th, 2014

Watch it at https://www.youtube.com/watch?v=bsv_v_E_TpA

The Boston, October 2014, Keynotes

- Three pervasive monitoring-related keynote video sessions are available from the Boston M^{3}AAWG meeting.
- One session was by Brian D. Snow, retired NSA Senior Technical Director. As noted at http://synaptic-labs.com/resources/security-bibliography/87-biographies/191-bio-brian-snow.html , "In all of his positions, he insisted that the actions NSA took to provide intelligence for our national and military leaders should not put U.S. persons or their rights at risk."
- A second session was by Dan Geer, a widely well-regarded cyber security expert. Wikipedia states that "Geer is currently the chief information security officer for In-Q-Tel, a not-for-profit venture capital firm that invests in technology to support the Central Intelligence Agency."
- The third session is a joint Q&A for both keynote speakers.

Keynote: M³AAWG Boston, October 22nd, 2014

Watch it at https://www.youtube.com/watch?v=tM_c7_GOU1Q

Keynote: M³AAWG Boston, October 22nd, 2014

Watch it at https://www.youtube.com/watch?v=WvW9dVzz_Kg

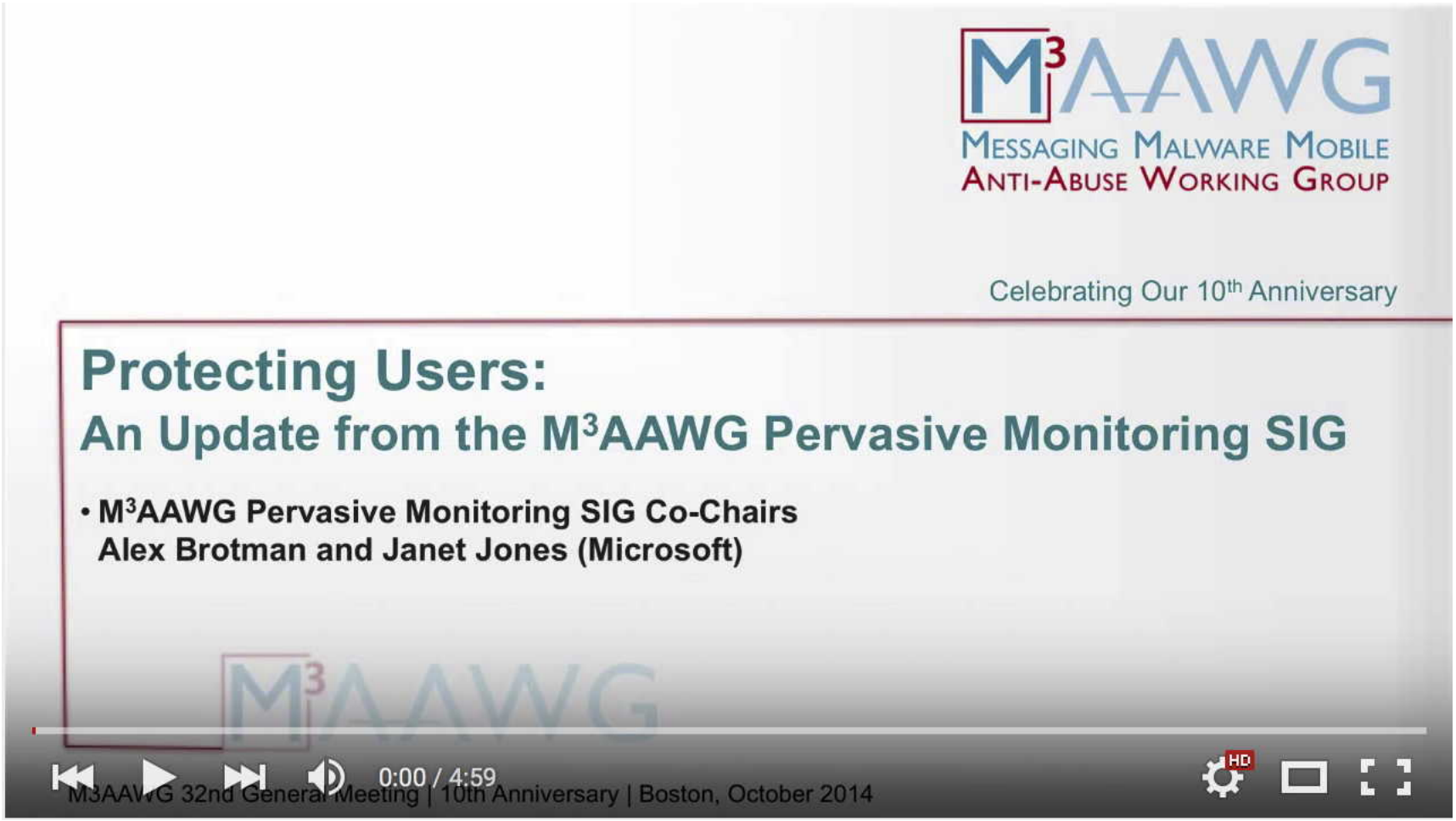
Keynote Q&A: M³AAWG Boston, October 22nd, 2014

Watch it at https://www.youtube.com/watch?v=vM2pcRtOb6Y

Other Videos

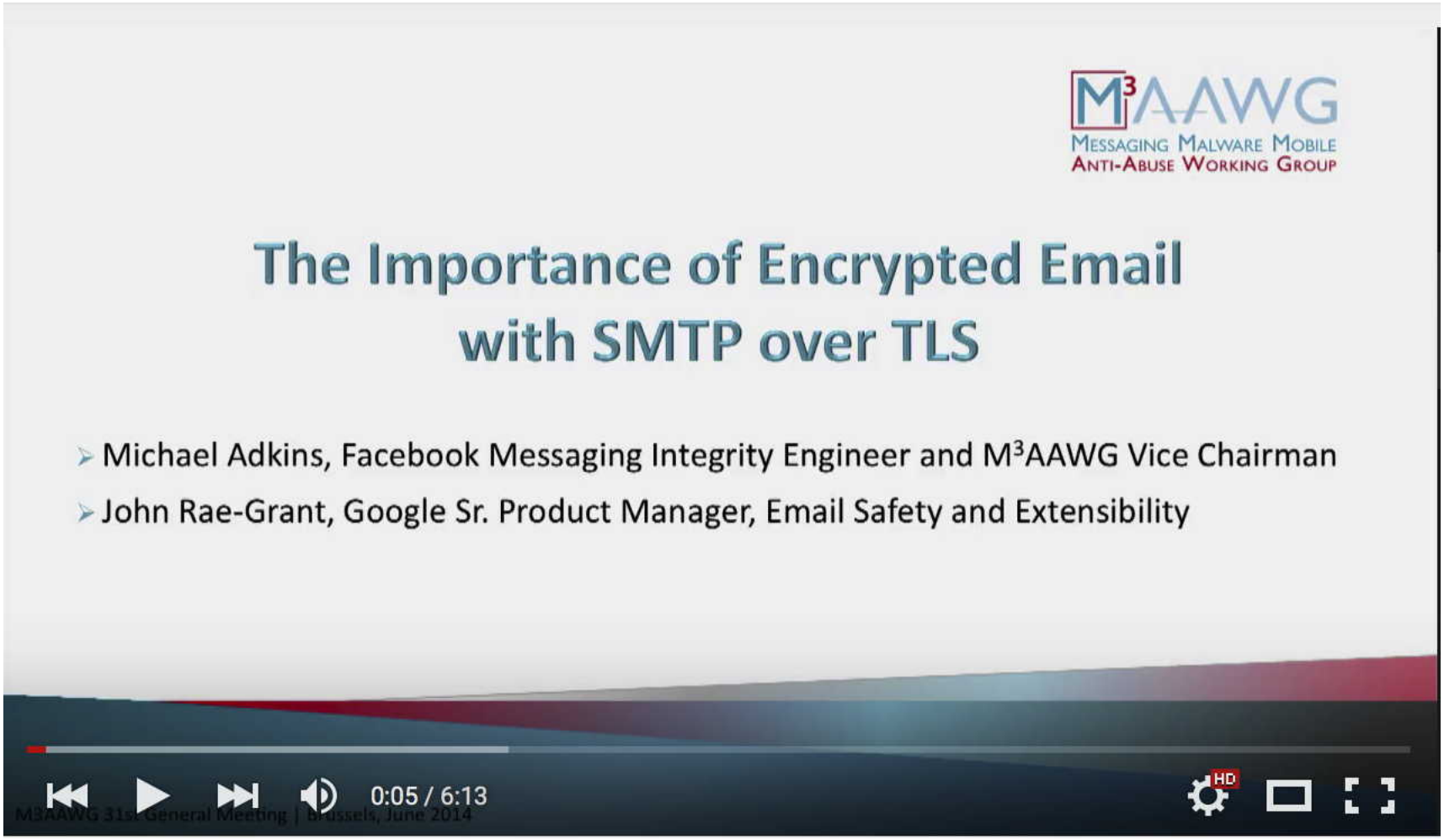
- A number of other shorter M^{3}AAWG videos are also available, including ones featuring:
  - The co-chairs of the anti-Pervasive Monitoring SIG explaining some of the SIG's work
  - Another talking about the importance of enabling opportunistic encryption for SMTP traffic
  - A third talking about Facebook's experience with opportunistic encryption
  - And a fourth that talks about using DNSSEC and DANE to secure email.
- We hope to have additional anti-Pervasive Monitoring videos publicly available in the future.

Short Video: Pervasive Monitoring SIG Update



Watch it at https://www.youtube.com/watch?v=ckL2qqSZ2kE

Short Video: SMTP over TLS

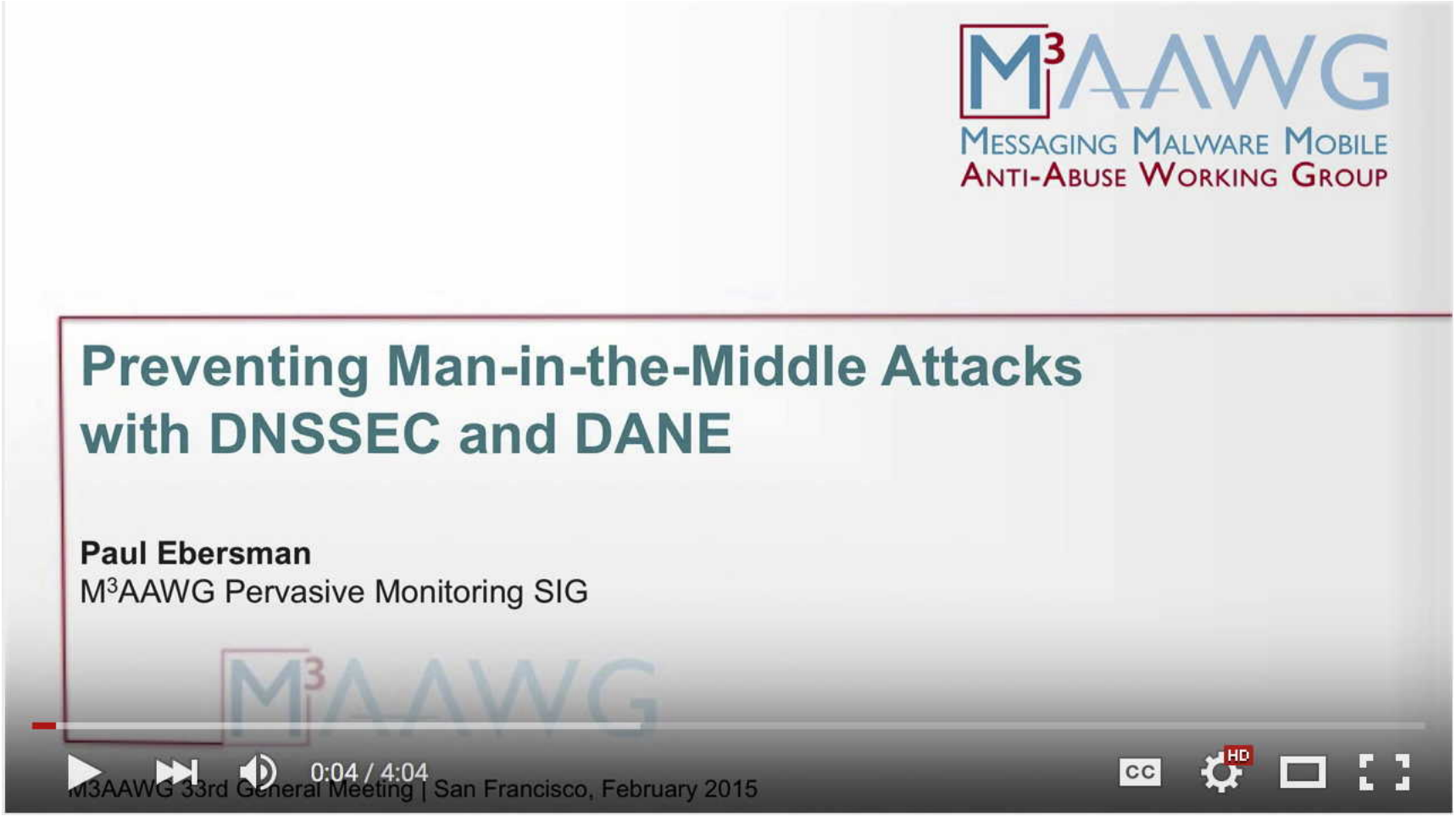


Watch it at https://www.youtube.com/watch?v=vrfSdka1jjo

Short Video: The Facebook Encrypted Email Study

Watch it at https://www.youtube.com/watch?v=f9qyYDvCbLs

Short Video: MITM Attacks, DNSSEC, and DANE



Watch it at https://www.youtube.com/watch?v=rCpEDVm962Q

Pervasive Monitoring SIG Sessions From The Most Recent M³AAWG Meeting In Atlanta, Some of Which May Be Available Soon In Video Form

Session	Date	Time
SMTP Transport Security: Past, Present, Future	10/20/2015	1:00 pm – 2:00 pm
Keys Under Doormats	10/20/2015	3:30 pm – 4:30 pm
Hardening Opportunistic TLS: Enforcing Transport Encryption for Messaging	10/20/2015	4:30 pm – 5:30 pm
Messaging Encryption: A Technical BCP Discussion	10/21/2015	4:30 pm – 5:30 pm
NIST Email Security Improvements	10/22/2015	3:30 pm – 5:30 pm

IV. Digging In A Little: What's "In Scope" For M³AAWG's Anti-Pervasive Monitoring Work? Why Focus on Intelligence Community Surveillance?

Norms For Performing Intercepts in the U.S.

- While there is a tendency in some quarters to treat all monitoring or network interceptions as interchangeable, in fact, there are important differences between:

  -- provider monitoring done for self-protection,
  -- monitoring done in a criminal law enforcement context, and
  -- monitoring done by the intelligence community.

- I wanted to take a few minutes to highlight some of those differences, both because I think they're important, and because they help to provide context for the reaction of the technical community to Snowden's disclosures.

Provider Monitoring

- It is routine for providers to monitor their own systems and networks for a variety of purposes, including:
  - Billing purposes
  - Engineering and planning
  - Detecting outages, operational faults, and other errors
  - Identifying intrusions and other unauthorized access by third parties, and
  - Blocking spam, phishing, malware, denial of service attacks, etc.
- This activity is subject to careful limitation under the Electronic Communication Privacy Act (ECPA), as well as contractual agreements entered into between providers and their customers. This is not the sort of monitoring M^{3}AAWG's worried about.

Other Areas Out Of Scope

- Online tracking for marketing and related purposes
- Untrustworthy end-user systems (e.g, systems compromised by malware due to being unpatched, etc.)
- Monitoring the Internet activity of minors by parents/schools
- Monitoring done with the consent of a party or both parties to the communication (requirements depend on whether a "single party notification" or "double party notification" state is involved)
- Monitoring of employee Internet activity by their employers
- Monitoring of academic institutional networks for research purposes (particularly if anonymized, and done with IRB approval)
- Lawful interception done for criminal investigation purposes, if narrowly targeted and done pursuant to a valid court order, etc. See the next slide...

Criminal Law Enforcement Wiretaps

- In a criminal investigation, the use of wiretaps is subject to extensive limitations and protections, see the discussion in the U.S. Attorney's Manual at http://www.justice.gov/usam/usam-9-7000-electronic-surveillance and the Criminal Resource Manual at http://www.justice.gov/usam/criminal-resource-manual-27-electronic-surveillance

- If appropriate electronic surveillance procedures aren't followed, criminal, civil and administrative sanctions may apply, and any evidence improperly collected may end up being tossed out at trial.

- Thus, significant limitations and protections normally apply to the use of wiretaps in domestic criminal investigations.

Limitations Applicable to Criminal Law Enforcement

- **Only a comparative handful of offenses are serious enough** to justify electronic interception orders (89% of wiretaps involved illegal drugs, with the next highest reason being homicide at 4%)
- **Intercept orders are limited to 30 days** (although extensions can be requested from the courts if required)
- **Targets of the surveillance must be identified with specificity**
- **Interceptions must be minimized** to just the approved targets
- **Normal investigative procedures must be impossible, or too dangerous to use**
- Requests are subject to review by a U.S. Attorney or AUSA, and by the Attorney General or Deputy Assistant Attorney General for the Criminal Division, prior to being submitted to the Courts
- See http://www.justice.gov/usam/criminal-resource-manual-28-electronic-surveillance-title-iii-applications

Net Result? Relatively Few Criminal Investigations Actually Involve Wiretaps

- "The number of federal and state wiretaps reported in 2014 decreased 1 percent from 2013. A total of 3,554 wiretaps were reported as authorized in 2014, with 1,279 authorized by federal judges and 2,275 authorized by state judges." See http://www.uscourts.gov/statistics-reports/wiretap-report-2014

- For context (and a sense of relative magnitude): "At yearend 2014, the United States held an estimated 1,561,500 prisoners in state and federal correctional facilities," of which 1,508,600 were sentenced to more than 1 year. See http://www.bjs.gov/content/pub/pdf/p14.pdf

- Thus wiretaps in criminal investigations represent a relatively rare activity, and one we're not particularly worried about.

And For The Record, Use of Encryption Has Seldom Been An Impediment To Wiretaps in Criminal Cases

- "The number of state wiretaps in which encryption was encountered decreased from 41 in 2013 to 22 in 2014. **In two of these wiretaps, officials were unable to decipher the plain text of the messages.** Three federal wiretaps were reported as being encrypted in 2014, of which **two could not be decrypted.** Encryption was also reported for five federal wiretaps that were conducted during previous years, but reported to the AO for the first time in 2014. **Officials were able to decipher the plain text of the communications in four of the five intercepts."**

  http://www.uscourts.gov/statistics-reports/wiretap-report-2014 [emphasis added]

OK, So What About the "Intelligence Community?"

- "During calendar year 2014, the Government made 1,416 applications to the Foreign Intelligence Surveillance Court (hereinafter "FISC") for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. [...] **1,379 applications included requests for authority to conduct electronic surveillance."**

- "In 2014, the FBI made **12,452 NSL [National Security Letter]** requests (excluding requests for subscriber information only) for information concerning United States persons. These sought information pertaining to 4,699 different United States persons."

  "FISA Annual Report to Congress,"
  http://fas.org/irp/agency/doj/fisa/2014rept.pdf

An Aside: "What Are National Security Letters?"

- *See 18 USC 2709:* "The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may, using a term that specifically identifies a person, entity, telephone number, or account as the basis for a request—
- (1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; [continues]

The Problem With All Those Statistics?

- We now know that some FISC-approved intelligence community monitoring programs were so broad as to include virtually everyone, including large numbers of law-abiding Americans. Those are the sort of pervasive monitoring programs that give many people (including me) pause.
- While our discussion has been and largely will be couched in terms of domestic pervasive monitoring, there is no reason to believe that Internet traffic isn't potentially subject to similar nation-state monitoring by the intelligence services of other countries, too, whether as part of the "Five Eyes" consortium (US, UK, Canada, Australia, and New Zealand), or otherwise.
- There was thus a need for action.
- Opportunistic encryption was the first area selected for attention.

V. Encrypting Email In Transit

Opportunistic Encryption of Email In Transit

- As you might expect, given that email is a core area of M³AAWG attention, M³AAWG's first Board-approved anti-pervasive-monitoring recommendation was around:

  "TLS for Mail: M³AAWG Initial Recommendations"
  https://www.m3aawg.org/sites/default/files/document/M3AAWG_TLS_Initial_Recommendations-2014-12.pdf

- This **M³AAWG Board-approved document** is short (just two pages) with some pretty basic recommendations:
  - Protect mail flows between providers with opportunistic TLS
  - Protect intracompany network traffic from eavesdropping
  - Protect user passwords from eavesdropping (IMAPS/POPS/SMTP Submit/web email interface)

IS Email Getting Encrypted In Transit? Why Yes, It Is

Below is the percentage of email encrypted for the top domains in terms of volume of email to and from Gmail, in alphabetical order.

Select Region World

Top domains by region, inbound

Domain	%
From: amazonses.com	99%
From: facebookmail.com via facebook.com	99.99%
From: grouponmail.{...}	< 50%
From: linkedin.com	99%
From: mandrillapp.com	100%
From: mcdlv.net	0%
From: mcsv.net	0%
From: sailthru.com	> 95%
From: twitter.com	99.9%
From: yahoo.{...}	99%

Monday, October 5, 2015

Top domains by region, outbound

Domain	%
To: aol.com	99.99%
To: comcast.net	99.99%
To: craigslist.org	100%
To: hotmail.{...}	100%
To: live.{...} via hotmail.{...}	100%
To: mail.ru	99.99%
To: msn.com via hotmail.{...}	100%
To: orange.fr	100%
To: outlook.com via hotmail.{...}	100%
To: yahoo.{...} via yahoodns.net	100%

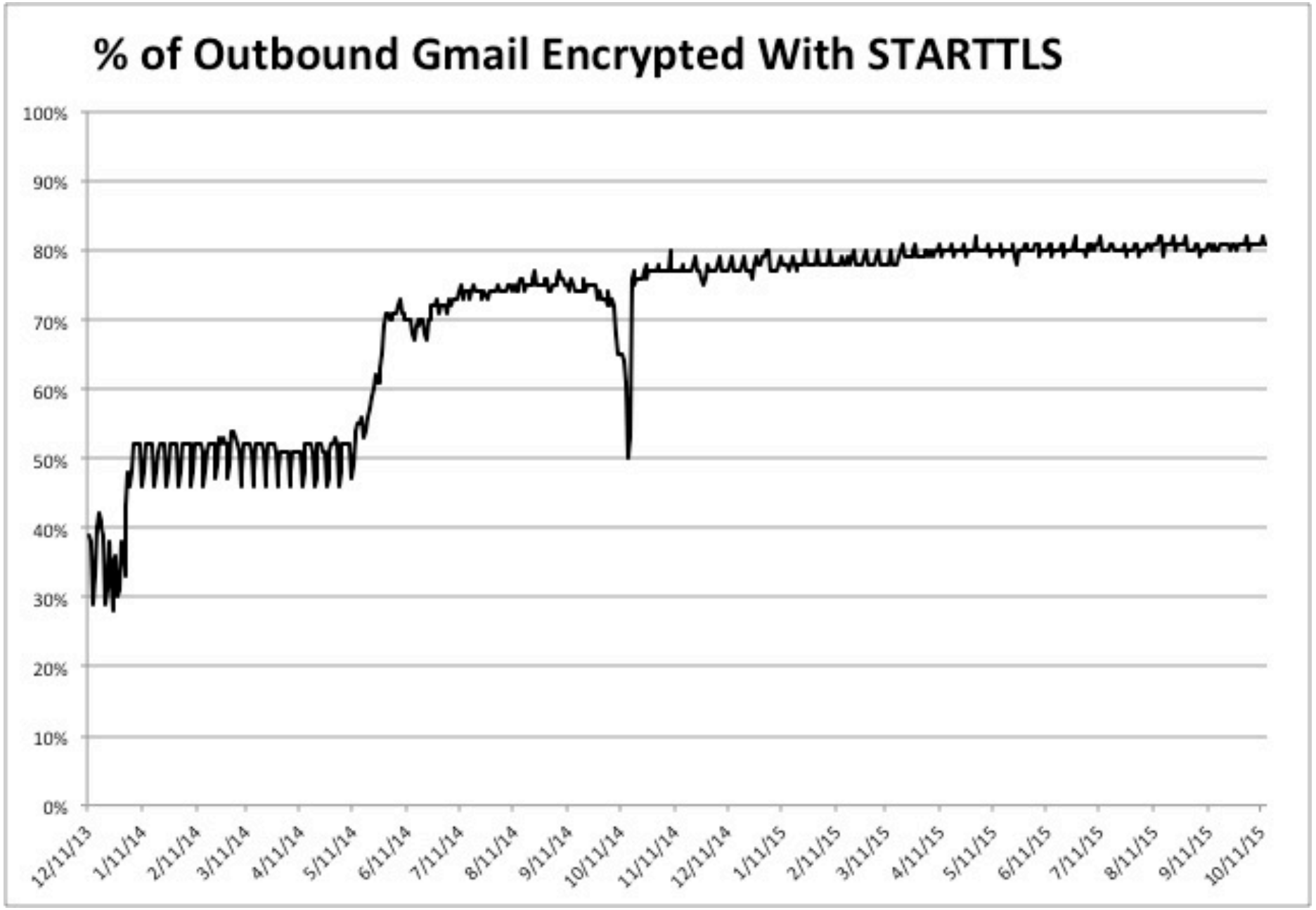
https://www.google.com/transparencyreport/saferemail/#region=001

All Those 100%'s and 99.99%'s? Those Numbers Represent A Bit of a Miracle...

- Few security technologies have *ever* successfully deployed at Internet scale.

- **PGP/GPG?** Great, but only used by a tiny subset of all users.
- **IPSec?** Never deployed (except for some *ad hoc* VPN usage)
- **DNSSEC?** Deployment of DNSSEC still trails
- **RPKI?** Another security technology that's had a slow start.

- But ***encryption of email in transit*****? THAT's** an example of a security technology that **HAS** deployed at scale. We've gone from 30-40% opportunistic encryption of outbound email from Google a year ago to fully 80% in just a year. See the graph on the next slide.



https://www.google.com/transparencyreport/saferemail/google-starttls-percentages.csv

A Couple of Notes About The Google Numbers

- There's a noticeable difference between inbound email and outbound email in the Google Email Transparency report. The largest sources of unencrypted inbound traffic tends to be **marketing-related email**. If something has to be unencrypted, that's probably the best content to have traveling in plain text.

- **Some regions/some ISPs are better than others** when it comes to encrypting email traffic in transit. Explore the Google Safer Email Transparency Report at https://www.google.com/transparencyreport/saferemail/ to see for yourself the differences between the various regions of the world. **Is your region of the world deploying TLS to protect email? If not, why not?** Most of the big North American and European ISPs are already successfully doing so.

Does This Mean That Gmail Is "Going Dark?" NO!

- "Going dark" is short hand for "LEOs will no longer be able to conduct court-ordered lawful interceptions." That notion forms the basis for law enforcement "push back" against encryption (see for example http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course by FBI Director James B. Comey from October 16th, 2014).
- The preceding graph is NOT an example of "going dark" even with 80% of outbound Gmail now encrypted in transit. Why? That 80% protection refers to email on the network *in transit*. Law enforcement is still free to obtain a court order for access to the email of a specific user on the ISP's *email servers*.
- So why bother encrypting in transit? ***Answer: It becomes far harder for foreign and domestic intelligence agencies, and any hacker/crackers that may be sitting on the wire, to potentially vacuum up EVERYONE's SMTP traffic indiscriminately.***

VI. MITM Attacks

MITM Attacks

- Opportunistic SSL/TLS (as described in the initial M^{3}AAWG recommendations) protects against passive monitoring, but does nothing to address an active "man in the middle" attack.
- There are many ways that an attacker can MITM a conversation. **The SIG's 2nd Board-Approved document,** on MITM, (see https://www.m3aawg.org/sites/default/files/M3AAWG-Man-in-the-Middle-Recommendations2015-07.pdf) mentions:
  - ARP spoofing
  - Rogue DHCP servers
  - Use of Web Cache Control Protocol (WCCP)
  - Web Proxy Autodiscovery Protocol (WPAD)
  - Spoofed WiFi wireless access points ("evil twin" access points)
  - DNS poisoning
  - BGP route injection
  - Physical (inline) network traffic interception devices

Our Assessment of the Risks of MITM Attacks

- If an adversary can successfully execute a MITM attack against unencrypted/ unsigned network traffic, the adversary will be able to:
  - eavesdrop upon the traffic,
  - modify the traffic, and
  - impersonate parties to the communication.

- **If the traffic is encrypted in transport, but endpoints are NOT cryptographically protected against MITM attacks, an adversary can execute the same attacks against encrypted traffic as it can against unencrypted traffic.**

- It is therefore extremely important that cryptographically "protected" transmissions be robust to MITM attacks.

The Basic Problem With Opportunistic Encryption

- Opportunistic encryption "does the best it can" to protect email from eavesdropping. However, that may **not** be **good enough.**
- **To understand why this is true, think about what typically happen if opportunistic encryption is deemed to NOT be "good enough:" in that case, MTA-to-MTA transmissions normally fall back to sending email traffic in plain text, e.g., totally unencrypted.**
- In that sort of scenario, your "choice" may devolve to tolerating "best effort crypto" (including crypto that's vulnerable to MITM attacks), living with "no crypto at all," or not transfering the message. None of those choices is very good. For example, even if "best effort" crypto is thought to be better than "no crypto at all," a MITM attacker with a self-signed cert may easily impersonate a real server.

What We Need: A Rigorous Alternative

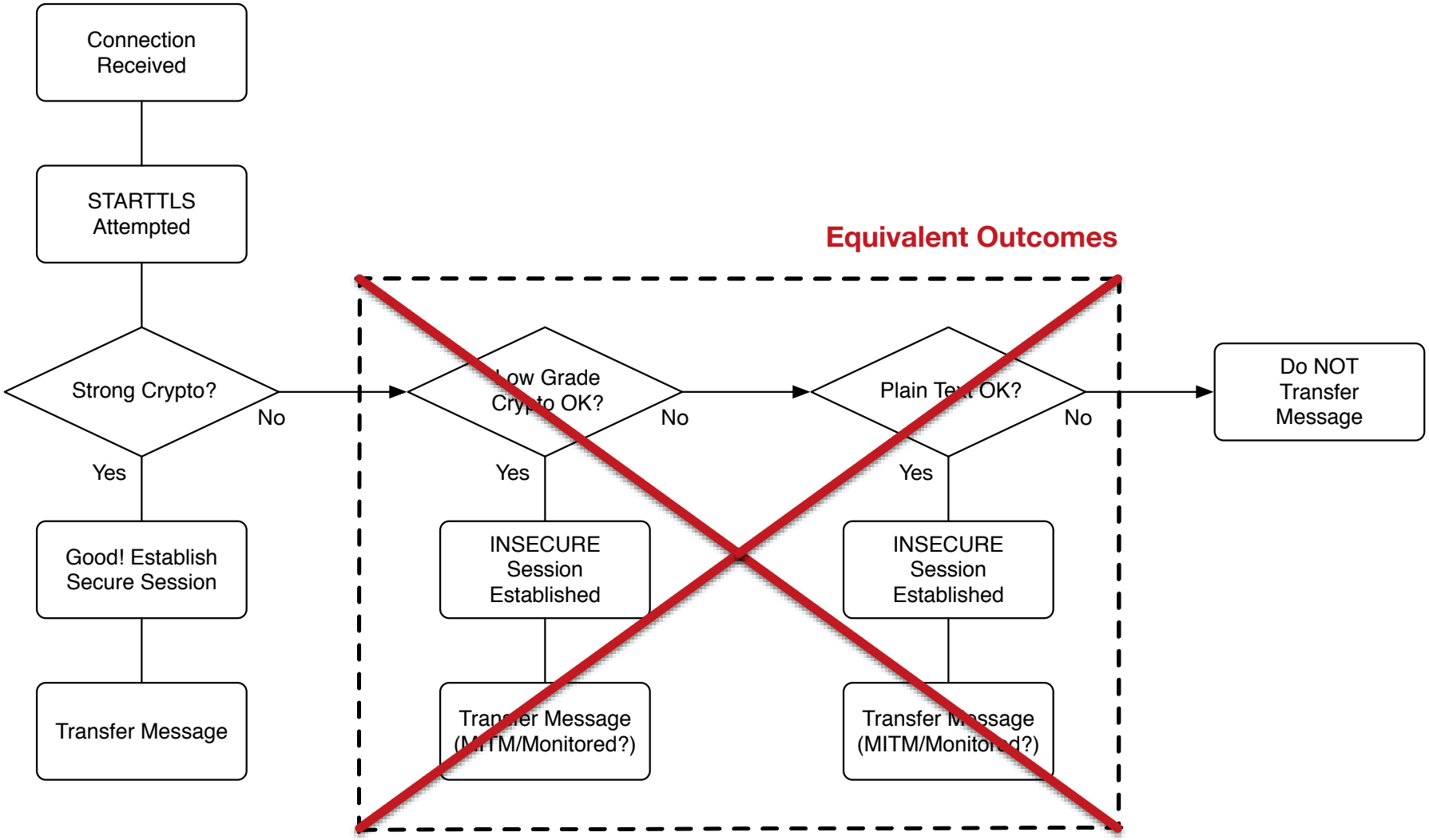
- Mail servers identify themselves using a globally trustworthy certificate (e.g., the server is using a commercially-procured certificate that chains to a globally-trusted root; **the server is NOT using a self-signed certificate**)
- The name of the server correspond to one of the domain names for which the certificate was issued (**the server and certificate "match"**)
- Checking Online Certificate Status Protocol (OCSP) and/or a Certificate Revocation List (CRL), **the certificate can be seen to not have been revoked.**
- **The certificate is not being used before it is first valid, nor after it has expired.**
- The certificate is **signed using a (now-industry-standard) SHA-2 signature.**

The Rigorous Alternative (continued)

- The certificate covers a **strong (2048 or 4096 bit) RSA key pair.**
- The originating and receiving mail server support the most recent version of the TLS protocol (**TLS 1.2** at the time this document was drafted)
- The servers mutually agree upon using a cipher suite that supports **forward secrecy** for the purpose of key exchange (normally Ephemeral Diffie Hellman (EDH) or Elliptic Curve Diffie Hellman Ephemeral (ECDHE)
- A strong symmetric cipher is negotiated (ideally **AES-128 or AES-256**).
- **If ANY of the preceding conditions are not satisfied between the sending MTA and the receiving MTA, the sending server cannot be sure that it can safely transfer the message.**

What If A Message CAN'T Be Securely Conveyed?

- Options hypothetically include:
  - The message can be **rejected outright,** and returned to the sender for his or her processing (assuming the sending host and the receiving host reach an agreement that they CANNOT securely exchange a message while a connection is still established); messages that cannot be securely delivered must NOT be bounced to apparent message body senders (due to spoofed apparent senders).
  - Alternatively, the message can be **temporarily queued, and retried one or more times thereafter,** thereby helping to address transient non-deliverability issues.
  - After that, **the message must be summarily dropped.** (This presumes that the sender has an application-level delivery confirmation mechanism that will detect silent non-deliveries if/when they occur)


Connection Received
STARTTLS Attempted
Strong Crypto?
No
Yes
Good! Establish Secure Session
Transfer Message
Low Grade Crypto OK?
No
Yes
INSECURE Session Established
Transfer Message (MITM/Monitored?)
Plain Text OK?
No
Yes
INSECURE Session Established
Transfer Message (MITM/Monitored?)
Equivalent Outcomes
Do NOT Transfer Message

Yes, We Know

- This is really a brutal way of doing business, much like DNSSEC (it's either cryptographically right, or it just doesn't happen).
- We also know that if we support plain text SMTP traffic as well as encrypted SMTP traffic, there's a risk of STARTTLS stripping
- Yes, he rigorous approach relies on the commercial certificate authority infrastructure, with all of its admitted shortcomings (the alternative, DANE, is lightly supported by available software)
- It mandates OCSP or CRL checking, which is another area where many rightfully don't feel all warm and fuzzy (see for example: https://www.imperialviolet.org/2014/04/19/revchecking.html); yes, there is an increased risk of denial of service attacks.
- There may be some scenarios where it is difficult to talk about "matching" certificate names to machines (e.g., consider an MX server that is meant to answer for hundreds if not thousands of unique domains)

VII. M³AAWG's 2015 J.D. Falk Award

"Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications"

J.D. Falk Award

- The M^{3}AAWG J.D. Falk Award seeks to recognize people who are committed to making a better online world. Nominees will have demonstrated dedication to improving the Internet experience and protecting end-users.
- The award seeks to recognize efforts for a particularly meritorious item of work rather than recognizing a lifetime of achievement. (The M^{3}AAWG Mary Litynsky Award honors lifetime achievement.)
- Examples of worthy accomplishments to be considered for the J.D. Falk Award include developing a service, authoring a specification or related documentation, inventing a security mechanism or other technology, mentoring a community, or pursuing notable research. The work can be in an academic or corporate context and can be an individual, group or institutional effort. Simply put, M^{3}AAWG wants to recognize cool work that reduces online abuse and improves the Internet.
- The recipient must also embody the spirit of J.D.'s volunteerism and community building. The J.D. Falk Award winners have a vigilant eye on the broader perspective of Internet systems and communities and call upon thoughtful humor when things get tough.

The 2015 J.D. Falk Award Recipient

https://www.m3aawg.org/news/keys-under-doormats-authors-receive-m3aawg-jd-falk-award-for-clarifying-insecurity-of

"KEYS UNDER DOORMATS" AUTHORS RECEIVE M^{3}AAWG J.D. FALK AWARD FOR CLARIFYING INSECURITY OF GOVERNMENT-MANDATED ACCESS TO DOCUMENTS

Home › News ›

"Keys Under Doormats" Authors Receive M^{3}AAWG J.D. Falk Award for Clarifying Insecurity of Government-Mandated Access to Documents

Atlanta, M^{3}AAWG 35th General Meeting, October 21, 2015 – The 15 highly-respected computer scientists and security experts who came together to outline how law enforcement's proposed requirement for "backdoor" access to all encrypted files would actually make the Internet more vulnerable to crime and deception were recognized for their work today with the M^{3}AAWG 2015 J.D. Falk Award. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications" explains how the government's request for a system that would allow it to access any secured file would set back Internet security, raise legal and ethical questions, and be impractical to implement.

The anti-Pervasive Monitoring SIG is delighted to see this work by leading cryptographers receive the recognition it deserves! Congratulations to all 15 authors!

VIII. Forward Secrecy

The Non-Forward Secrecy Risk Model

- We now move into some of the currently pending work.

- Normally public key crypto (relatively time consuming/expensive) is used to bootstrap agreement about a shared symmetric key. That approach generally works fine, with one exception:

  - An adversary intercepts & retains some or all of your TLS-encrypted traffic
  - The adversary ALSO manages to obtain a copy of your private key.

- If that happens, and you've NOT been using a cipher suite that has forward secrecy, then your adversary has everything they need to retrospectively decrypt ALL the traffic they may have squirreled away, associated with that key.

Is Encrypted Traffic Being Retained? Yes...

Forbes / Security

JUN 20, 2013 @ 06:21 PM 40,298 VIEWS

Leaked NSA Doc Says It Can Collect And Keep Your Encrypted Data As Long As It Takes To Crack It

Andy Greenberg, FORBES STAFF

Covering the worlds of data security, privacy and hacker culture.

FOLLOW ON FORBES (1413)

Opinions expressed by Forbes Contributors are their own.

Forbes, June 20th, 2013

Are Private Keys Really At Risk of Disclosure?

https://blog.cloudflare.com/the-results-of-the-cloudflare-challenge/

The Results of the CloudFlare Challenge

11 Apr 2014 by Nick Sullivan.

Earlier today we announced the Heartbleed Challenge. We set up a nginx server with a vulnerable version of OpenSSL and challenged the community to steal its private key. The world was up to the task: two people independently retrieved private keys using the Heartbleed exploit.

The first valid submission was received at 16:22:01PST by Software Engineer Fedor Indutny. He sent at least 2.5 million requests over the course of the day. The second was submitted at 17:12:19PST by Ilkka Mattila at NCSC-FI, who sent around a hundred thousand requests over the same period of time.

UPDATE: Two more confirmed winners: Rubin Xu, PhD student in the Security group of Cambridge University submitted at 04:11:09PST on 04/12; and Ben Murphy, Security Researcher submitted at 7:28:50PST on 04/12.

We confirmed that all individuals used only the Heartbleed exploit to obtain the private key.

Alternative Means of Obtaining Private Keys

- Since many sites just store their private key in a regular file, rather than using a hardware security module (HSM), anyone who can arrange to access to the keys stored in that regular file would then be able to decrypt any associated encrypted traffic.

- Strategies for getting access might include:

  - Subornation of a system administrator or other privileged user (bribery, extortion, physical coercion, etc.),
  - A court order compelling disclosure (*ala* Lavabit)
  - Access to a poorly-secured copy of that file (e.g., perhaps access to an unencrypted backup stored at a third party site, or the system gets hacked/cracked by a cyber intruder who's after that critical file's contents).

The Solution: Forward Secrecy

- Fortunately there is a solution to this problem, and that's ephemeral key exchange.

- If a site uses a key exchange mechanism that offers forward secrecy, such as Diffie Hellman Ephemeral (DHE) or Elliptic Curve Diffie Hellman Ephemeral (ECDHE), a new public/private key pair is created for each connection and then discarded immediately after use.

- With that approach, even if traffic does get captured and the security of the RSA private key is compromised, those adverse events won't result in an adversary being able to do retrospective decryption.

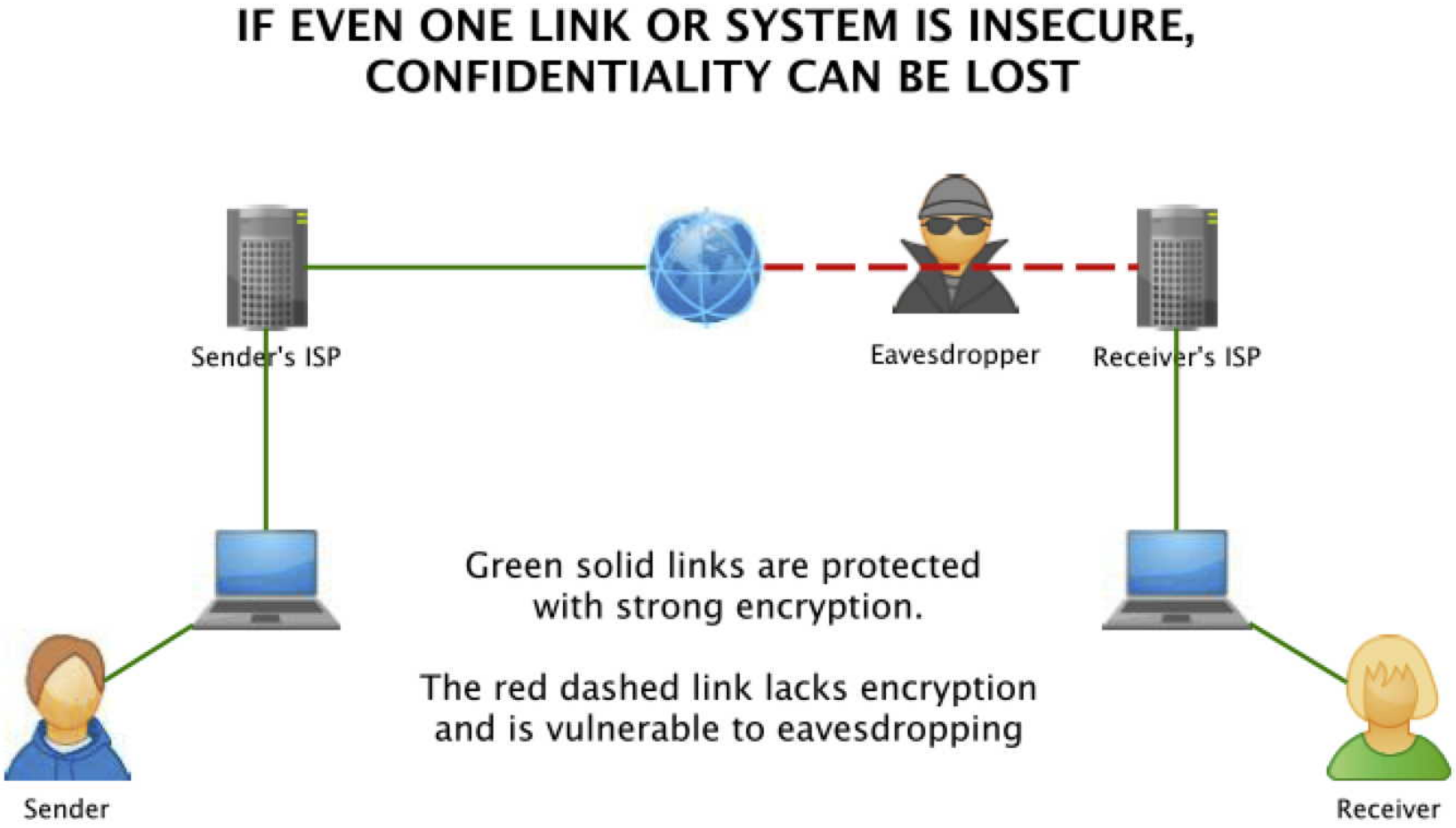
Diffie-Hellman Parameters

- In using ephemeral key exchange mechanisms, some care must be taken to ensure that long/strong Diffie-Hellman parameters get used. At least in some circumstances, the default Diffie-Hellman parameters may only be 1024 bits long. Fortunately, current versions of popular cryptographic libraries such as OpenSSL now allow even 4096 bit DH parameters.

- Please note, too, the recent article "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice," https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf

IX. End-To-End Encryption
(Draft in Circulation)

Introduction: A typical message will routinely pass through many systems and networks on its way from sender to recipient. If that message is NOT protected by *end-to-end encryption*, the privacy of that message depends on the protection the message receives from EACH individual system or network through which it passes. If any ONE of those systems or networks is untrustworthy, the message may no longer be confidential.



Why *Doesn't* Everyone Use End-to-End Crypto?

- There are many reasons....

- In order to do end-to-end, both sender and receiver must be willing to go through the extra work involved; unfortunately, non-technical people may find the process complex or confusing, or believe that their traffic doesn't need cryptographic protection.

- In order to be able to send an encrypted message to someone, you first need their public key; discovering and managing keys for random Internet correspondents can be burdensome.

Why Not End-to-End? (continued)

- While end-to-end encryption can protect messages against eavesdropping or unauthorized modification, and those are very important benefits, end-to-end encryption also brings with it some non-negligible new risks, too:

  – If access to the required private key is lost, and that private key hasn't been backed up or escrowed, the messages or files encrypted with that key will be irrecoverably lost.

  – Because encrypted messages are opaque to everyone except the recipient, the recipient needs to be responsible for managing any unwanted or malicious content, including dealing with messages that contain malware, phishing, or spam content.

Why Not End-to-End? (continued)

- Some risks arise as a result of expectations around use of strong crypto, including particularly the expectation that what's being sent encrypted will not (ever) be able to be read by an unauthorized party. Unfortunately:
  - Due to **user error**, sensitive content that was meant to be sent encrypted may end up accidentally being sent unencrypted. ("Oops...")
  - **End-to-end encryption may not encrypt "everything."** For instance, it is common for message "Subject" lines to be sent in plain text even if the body of the message is fully-encrypted. The unencrypted contents of the Subject line may disclose operationally sensitive information if the sender isn't scrupulously careful in limiting what gets put into the Subject line.
  - If the sender or receiver is using an insecure computer (e.g., one or the other of those systems is infected with malware, or has had a hardware keystroke grabber installed), **encrypted content may be intercepted prior to encryption, or after decryption has taken place,** thereby undercutting the confidentiality of the message's content.
    [continued on next slide]

Why Not End-to-End? (continued)

- Even if end-to-end encryption is used in an operationally flawless way, that encrypted traffic will still be subject to **traffic analysis.** For example, if you're working in a sensitive government position and you send an encrypted message to an investigative journalist or to a representative of a hostile foreign intelligence service, and that's noticed, the sheer fact you sent ANY such message, regardless of what the message might actually contain, will still likely be enough to trigger a review.

- **The sender or the receiver may be compelled to disclose the plain text, or the private key,** either by force of law, or through so-called "rubber hose cryptography."

- **A flaw or a cryptographic breakthrough, may unexpectedly nullify the protection** formerly offered by any given cryptographic system, allowing collected traffic to be suddenly decrypted en masse.

- Bottom line, end-to-end crypto is currenty relatively little used.

How **Little Used?**

- End-to-end cryptography (e.g., PGP/GPG or S/MIME) is probably used for no more than 1/100th of 1% of all messages currently traversing the Internet. That is, if we assume a daily traffic volume of 300 billion email messages a day, 1/100th of that 1% would be 30 million end-to-end encrypted messages a day.

- At that level of market penetration, end-to-end encryption isn't a particularly significant technology relative to opportunistic encryption (given that opportunistic encryption is currently protecting over 80% of all outbound traffic from one major Internet mail provider, albeit not end-to-end)

- That said, this same provider is working to make end-to-end encryption easier to use in a cross-provider initiative, too.

In The Mean Time, We'll Teach People To Use The Tools That Are Available, S/MIME and PGP Alike

- *Client Certs and S/MIME Signing and Encryption: An Introduction*
  Feb 20, 2012, M^{3}AAWG 24, San Francisco
  https://www.stsauver.com/joe/maawg24/maawg24.pdf
  (142 slides)

- *Pretty Good Privacy (PGP) & GNU Privacy Guard (GPG): Just Enough Training To Make You Dangerous*, June 8, 2015, M^{3}AAWG 34, Dublin, Ireland
  https://www.stsauver.com/joe/pgp-tutorial/pgp-tutorial.pdf
  (184 slides)

X. Traffic Analysis
(Draft In Circulation)

The Traffic Analysis Problem

- Even if an adversary can't see the contents of your message, simply knowing the sender and the receiver, when a communication was sent, how large the communication was, etc., can still yield important information to a trained analyst.

- Traffic analysis the fundamental reason why metadata gets collected. It can be an exceptionally powerful technique.

- In addition to the draft guidance that's currently in circulation, I did a talk on traffic analysis for M^3AAWG this summer, see:

  The Enduring Challenge of Traffic Analysis, June 11th, 2015, https://www.stsauver.com/joe/dublin-traffic-analysis/dublin-traffic-analysis.pdf (108 slides)

XI. Securing Authentication
(Draft In Circulation)

The Problem of Weak User Authentication

- A user's credentials (username and password, or sometimes username/password and a 2nd factor) are normally all that stands between the user's saved messages and a snoopy world. What authentication-related steps should users and M^{3}AAWG member companies be taking to ensure that unauthorized 3rd parties can't get their hands on unencrypted saved content?
- The six page draft document in circulation discusses recommendations around:
  - passwords and passphrases
  - multifactor authentication (and reasons why multifactor uptake is still low)
  - use of password manager applications,
  - and more...
- This document may be supplanted by a pair of password management documents now being finalized by M^{3}AAWG's Identity Management SIG.

XII. "Crypto Isn't Free"
(Draft In Circulation)

Everything Has a "Cost," Including Crypto

- There are very real tradeoffs/"costs" to using cryptography to protect your traffic This document will describe those considerations so you can make an informed decision about what you do (or don't!) want to do when it comes to deploying encryption. Areas covered in the draft document include:
  1) If Needed, Spam and Malware Filtering Has To Be Done On-System, Not Passively On Network Links
  2) Other Potential Loss of Functionality (e.g., mail spool searchability; lack of mailing list support for encryption; debugging encrypted connections becomes more difficult)
  3) Potential Irrecoverable Loss of Encrypted Contents
  4) Incrementally Increased Effort/Inconvenience
  5) Potential Loss of Anonymity
  6) Cryptographic "Failure Modes" Often Tend To Be Brittle, and Failures Are Often Undifferentiated
  7) Computational Overhead? (Not That Big Of A Deal These Days)

XIII. "I Need To Protect Higher Bandwidth Internal ISP Links -- What Are My Options?" (Draft In Circulation)

This Document Is A Reaction to the MUSCULAR Revelations ("SSL Added/Removed Here")

- Many M^{3}AAWG service provider members have already publicly announced that they've encrypted their internal network links to avoid surreptitious passive monitoring of those links.
- See for example:
  - http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network/
  - http://yahoo.tumblr.com/post/81529518520/status-update-encryption-at-yahoo
  - http://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/ ("All of our key platform, productivity and communications services will encrypt customer content as it moves between our data centers.")
- At least some other major providers, however, plus many supporting-tier providers, have not yet done so.

The Draft Document

- The draft document currently in circulation describes cryptographic options at higher speeds that are relevant to larger service providers, e.g., 10Gbps/40Gbps/100Gbps (although your options may be limited, and increasingly expensive, the faster you need to go).
- Network encryption can be handled by options running at network layer 1, layer 2, or layer 3 of the network model. Given uncertainties about various attacks against encryption technologies, some sites may even decide that they want to run redundant encryption products, each at different network layers, for security in depth and reduced risk of unexpected exposure.
- Of course, doing network-based encryption at layers 1, 2, or 3 does not also preclude doing encryption at layer 4 (e.g., opportunistic SSL/TLS), or encryption at layer 7 (end-to-end encryption with PGP/GPG or S/MIME), as well.

Product Eligibility

- To be considered for listing in the draft document in addition to supporting at least 10Gbps speeds, network encryption solutions must support a minimum of AES-256. This rules out, for example, products that only support AES-128 (or weaker) crypto.

- Products must also be available for sale to non-governmental entities (e.g., High Assurance Internet Protocol Encryptor (HAIPE)-compliant devices such as the http://www.gdc4s.com/taclane-10g-%28kg-175x%29.html using classified NSA Suite A crypto algorithms are not available for use in the commercial/unclassified market, and hence, these sort of products will not be included in the options mentioned in the draft document)

Product Categories

- Listings are provided for Layer 1 (optical) encryption solutions running at speeds of up to 100Gbps, but optical encryption solutions may be limited by the optical platform you've deployed.
- There are 15 Layer 2 encryption options (often referred to as "MACsec" or LinkSec or 802.1AE). Low overhead, low latency, protocol agnostic and relatively well-standardized, MACsec is a popular option that's normally deployed as a point-to-point protocol, protecting switch-to-switch, switch-to-router, or switch-to-server links. Layer 2 encryption is typically one of the *least expensive* 10Gbps encryption solutions.
- Layer 3 encryption generally means doing IPsec, probably in tunnel model rather than transport mode. Doing IPsec at 10Gbps can be quite challenging/expensive, and is subject to both materials latency issues and substantial overhead-related impacts. Nonetheless, some 10Gbps+ options are mentioned in the draft.

XIV. "Deploying Crypto For Voice Telephony and Chat/Text Messaging" (Draft In Circulation)

It's Not All About Email

- While most of M^{3}AAWG's anti-pervasive monitoring/pro-crypto work has been focused on email, there are other messaging modalities/devices/protocols that are also potentially in need of cryptographic protection, including telephony and chat. This draft document considers encryption for those non-email applications.
- Most voice telephony is unencrypted. This draft document describes some one-to-one voice telephony options that are encrypted end-to-end ("E2E"), and which may also offer one-to-one end-to-end encrypted chat/text messaging and/or one-to-one end-to-end encrypted video.
- Products that are not available to the commercial and/or consumer market are considered out of scope (for example, http://www.boeing.com/defense/boeing-black/index.page and http://www.gdc4s.com/products/secure-voice-and-data-products-catergory-listing/secure-voice-%28prodland%29.html)

The Challenge of Interoperability

- Most secure voice and secure chat solutions do not interoperate. This is an obvious disadvantage: either "everyone" needs to standardize on a single common solution, or individuals need to buy and use multiple discrete devices.
- The draft points to 53 known alternatives, and offers a comparative chart for 4 representative alternatives. Factors driving users to select one product or another might include:
  - Need for voice? video? text/chat?
  - Platform used? (Android, iPhone, Mac OS X, Windows, etc.)
  - Crypto used? (zRTP? SSL/TLS? AES? ECC?)
  - Source code available?
  - Call logging/metadata collected?
  - Password recovery possible?
  - Tied to real world identity? (logged-in download, POTS #/email, etc.)
  - Interoperate with POTS/employ POTS for transport?
  - Cost? (paid-for client? subscription charges?)

XV. "The Potential Role of DANE TLSA in Securing MTA-to-MTA Flows" (Draft In Circulation)

DANE TLSA

- DANE TLSA has the potential to deter 3rd parties from using improperly-obtained globally-trusted certificates, however it depends on sites having:
  - DNSSEC
  - MTAs with support for DANE

- Deployment of DANE TLSA has been slow to date. You can check sites of interest using the tester that's available at:

  https://dane.sys4.de/

  Example of a site that **does** do DANE: ietf.org
  Example of a site that does DNSSEC, but **not** DANE: icann.org
  Example of sites that do neither: [lots of those, sadly!]

Conclusion

- You've now had a bit of a "whirlwind tour" of some of M^{3}AAWG's work against Pervasive Monitoring.
- You now know why we're working, and working hard, in this particular area.
- You've learned that there are M^{3}AAWG videos you can watch, if you'd like to learn more, plus pointers to some M^{3}AAWG crypto training materials.
- You've also learned about M^{3}AAWG anti-pervasive monitoring documents that have been published, and others that are still in the queue in draft form.
- Perhaps this is work you'd like to become involved with, too?

- **Thanks for the chance to talk! Are there any questions?**