The Data & Identity Protection Journey

Janet Jones (Microsoft Corporation)

- M³AAWG Vice-Chair
- M³AAWG Data & Identity Protection Co-Chair

Thursday, November 8, 2018

Tokyo, Japan

Agenda

- □ Introduction to M^{3}AAWG working groups
- □ Data & Identity Protection
  - ➢ The Journey Travelled
  - ➢ The Road Ahead

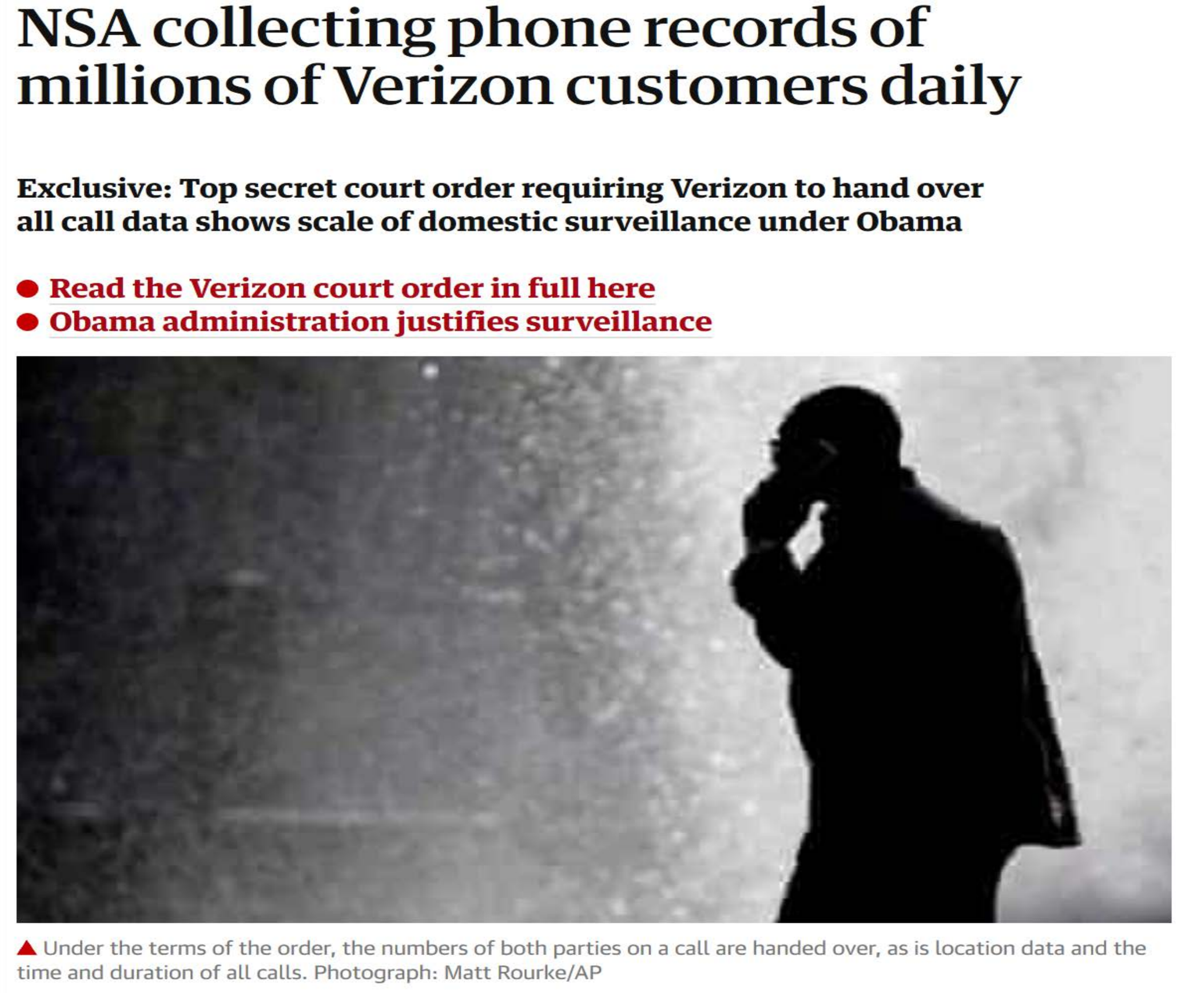
Knowledge to Solutions - **What Working Groups Do**

Committees / SIGs
Technical • Messaging • Malware • Mobile • DDoS SIG • Internet of Things SIG
Collaboration Committee
Abuse Desk Committee
Public Policy Committee
Senders Committee
Data & Identity Protection Committee
Mobile/VTA SIG
Brand SIG
DNS Abuse SIG

Two Primary Activities	
Programming	Informative presentations to the community
Deliverables	Best common practices documents, position papers, white papers
Three Types of Groups	
Birds of Feather (BoFs)	Opportunity to explore a set of problems and solutions that can evolve into SIG, Committee, or document champions
Special Interest Groups (SIGs)	A sustained group developing solutions well-defined problems: Info Sharing, Identity Management and Pervasive Monitoring, etc.
Committees	Long standing topical areas such as Technical, Public Policy, and Collaboration. These core issue areas cross-cut many other areas.

2013 - SNOWDEN DISCLOSURES

2013



NSA collecting phone records of millions of Verizon customers daily

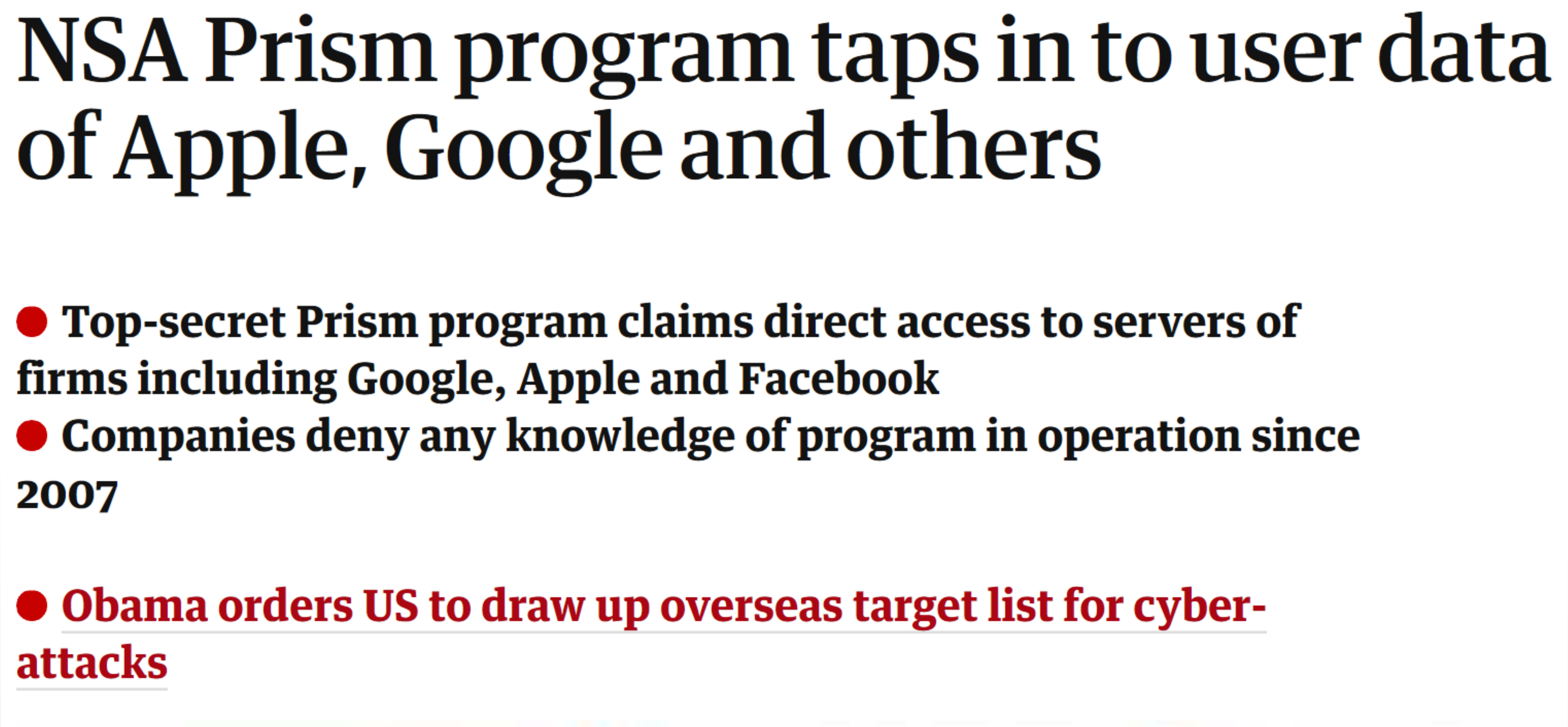
Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama

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

▲ Under the terms of the order, the numbers of both parties on a call are handed over, as is location data and the time and duration of all calls. Photograph: Matt Rourke/AP

https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

2013



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

- Obama orders US to draw up overseas target list for cyber-attacks

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

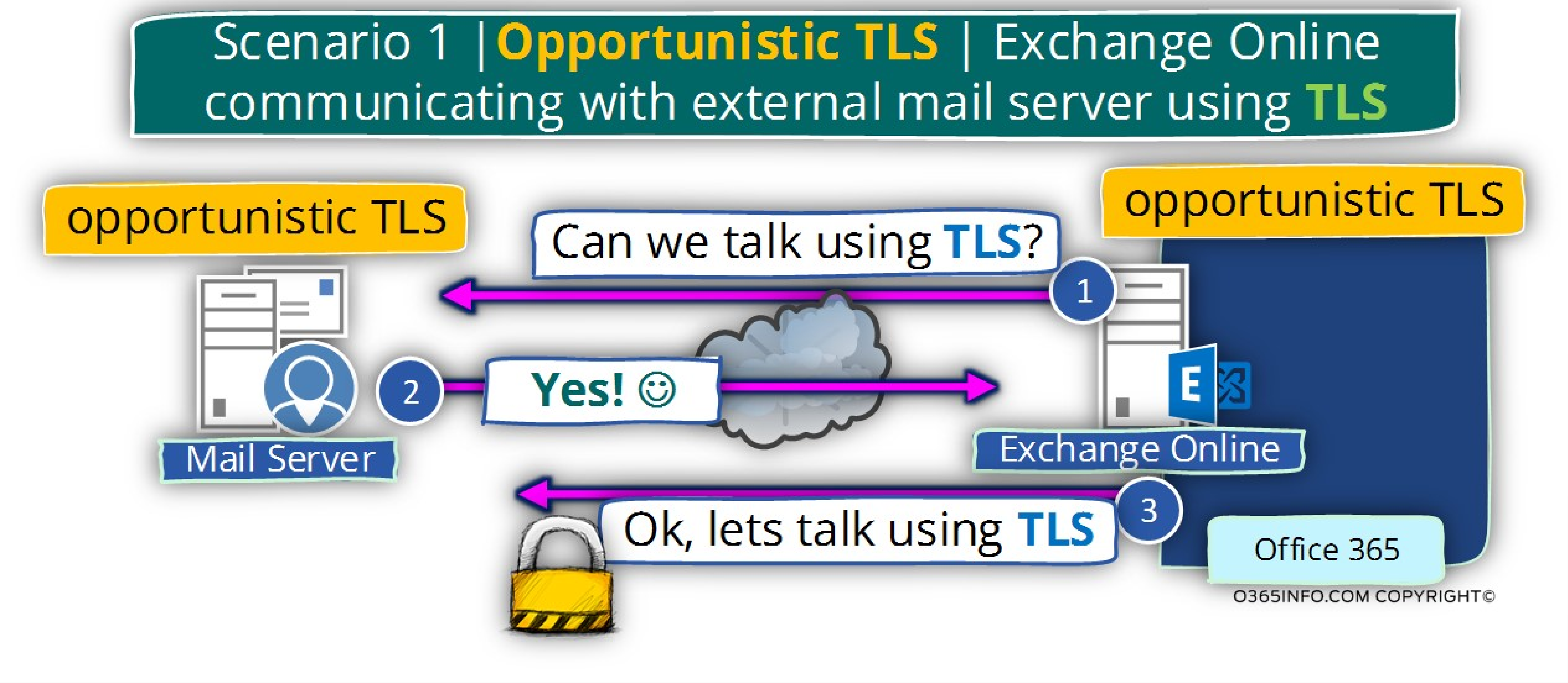
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP

2014 – M^{3}AAWG TAKES ACTION

2014 – M^{3}AAWG Tackles Pervasive Monitoring

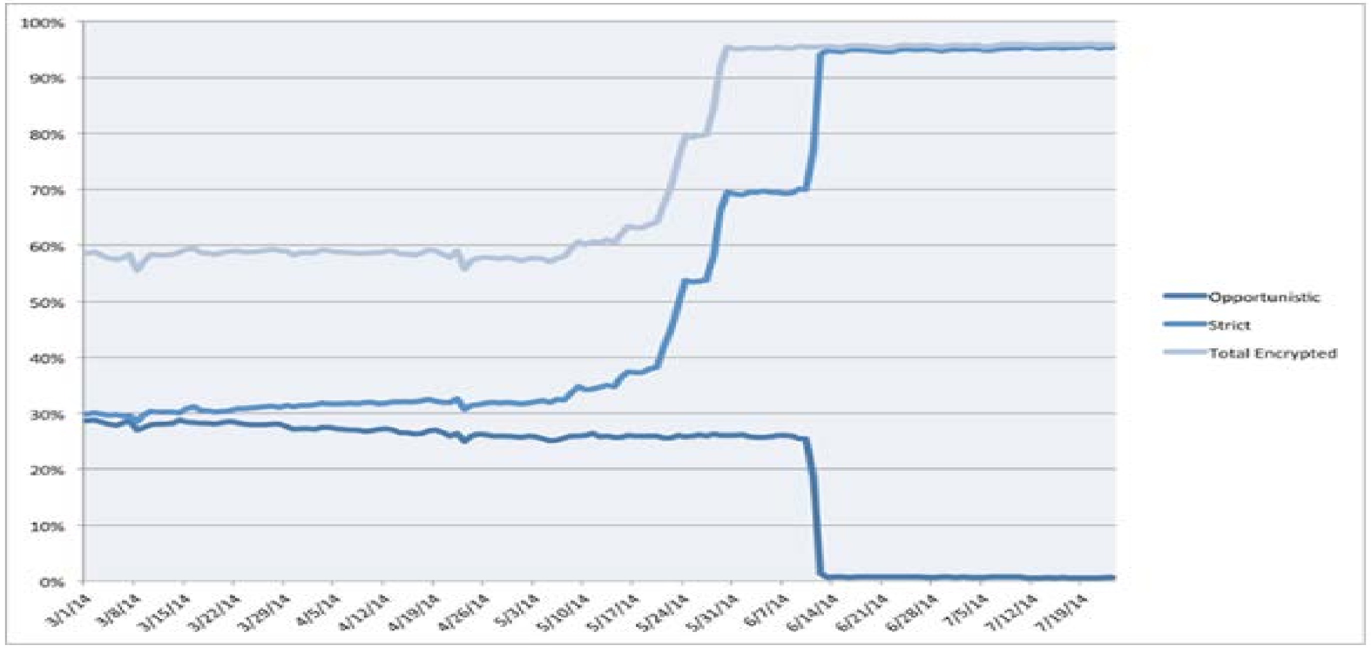
- ✓ M^{3}AAWG creates Pervasive Monitoring Special Interest Group (SIG)
- ✓ M^{3}AAWG Senior Technical Advisor (Stephen Farrell – Trinity College Dublin) co-authors IETF Best Current Practice declaring “Pervasive Monitoring is an Attack” that should be mitigated in the design of IETF protocols, where possible.
- ✓ As you might expect, given that email is a core area of M^{3}AAWG, the first Board-approved anti-pervasive-monitoring recommendation was around "TLS for Mail: M3AAWG Initial Recommendations“
- ✓ This M^{3}AAWG Board-approved document is short, providing 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)

Opportunistic TLS



Opportunistic TLS Deployment Push

- As Facebook Messaging Integrity Engineer and M³AAWG Co-Vice Chairman Mike Adkins reported on August 19th, there was *“Massive Growth in SMTP STARTTLS Deployment”* in a few months timeframe from May 2014 – August 2014 as large providers made progress to deploy Opportunistic TLS.
    - https://www.facebook.com/notes/protect-the-graph/massive-growth-in-smtp-starttls-deployment/1491049534468526



2015 - IS OPPORTUNISTIC TLS ENOUGH?

Man-in-the-Middle Threat

https://elie.net/blog/understanding-how-tls-downgrade-attacks-prevent-email-encryption

July 2015 M^{3}AAWG Publication

- *M3AAWG Initial Recommendations for Addressing a Potential Man-in-the-Middle Threat*

Using Perfect Forward Secrecy with TLS

https://www.expressvpn.com/blog/perfect-forward-secrecy/

January 2016 M^{3}AAWG Publication

M3AAWG Initial Recommendations for Using Forward Secrecy to Secure Data

- "Enabling forward secrecy in conjunction with TLS assists in protecting captured traffic against any possibility of eventual decryption."

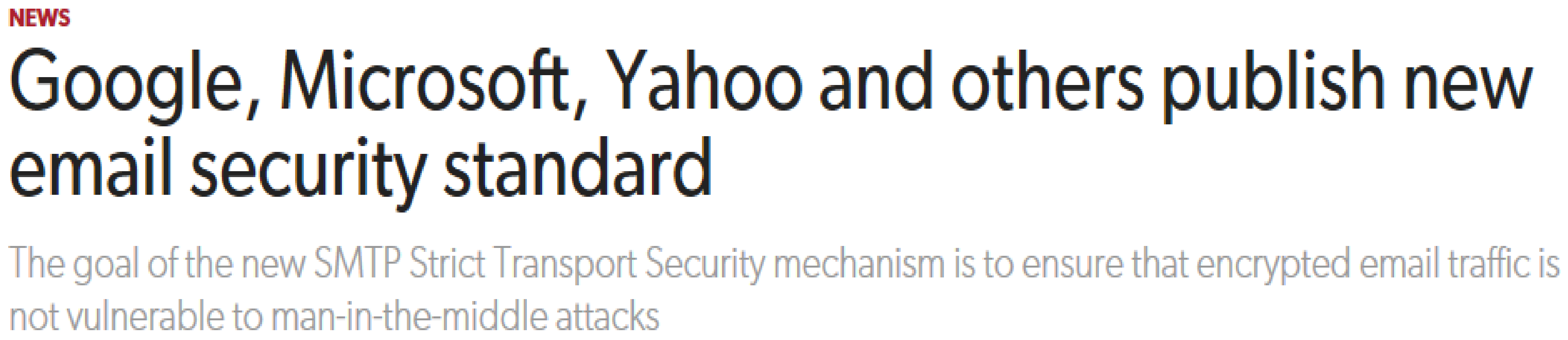
“Keys Under Doormats”

August 2015

“The Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) supports the use of effective, end-to-end encryption. Mechanisms that intentionally compromise encryption put that effectiveness at risk. Therefore M^{3}AAWG endorses the recommendations in the recent paper "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications" written by 15 noted security experts. The widely recognized authors include cryptography expert Bruce Schneier and researchers from MIT, Stanford University, Columbia University, Cambridge University, Johns Hopkins University, Microsoft Research, SRI Worldwide and Worcester Polytechnic Institute.”

2016 - M^{3}AAWG DRAFTS NEW IETF PROTOCOLS

SMTP Strict Transport Security/TLSPRT



NEWS

Google, Microsoft, Yahoo and others publish new email security standard

The goal of the new SMTP Strict Transport Security mechanism is to ensure that encrypted email traffic is not vulnerable to man-in-the-middle attacks

“Devised by engineers from Google, Microsoft, Yahoo, Comcast, LinkedIn and 1&1 Mail & Media Development & Technology, the SMTP Strict Transport Security is a new mechanism that allows email providers to define policies and rules for establishing encrypted email communications.”

https://www.pcworld.com/article/3046484/security/google-microsoft-yahoo-and-others-publish-new-email-security-standard.html

2017 – IDENTITY MANAGEMENT / CRYPTO COSTS

Identity Management

February 2017 M^{3}AAWG Publications

- *M^{3}AAWG Multifactor Authentication Recommendations*

  "M3AAWG urges providers not to wait for the rest of the industry to deploy multifactor authentication before doing so themselves. A critical mass of institutions needs to take a leadership role and set the example for their industry peers—otherwise, deadlocks may result."

- *M^{3}AAWG Password Recommendations for Account Providers*

  "M3AAWG recommendations for ISPs and other providers who continue to rely on passwords. It briefly describes the risk model arising from the use of passwords to provide authorized or secure access to resources. It is intended to improve end-user security by encouraging strong passwords."

Cryptography Costs

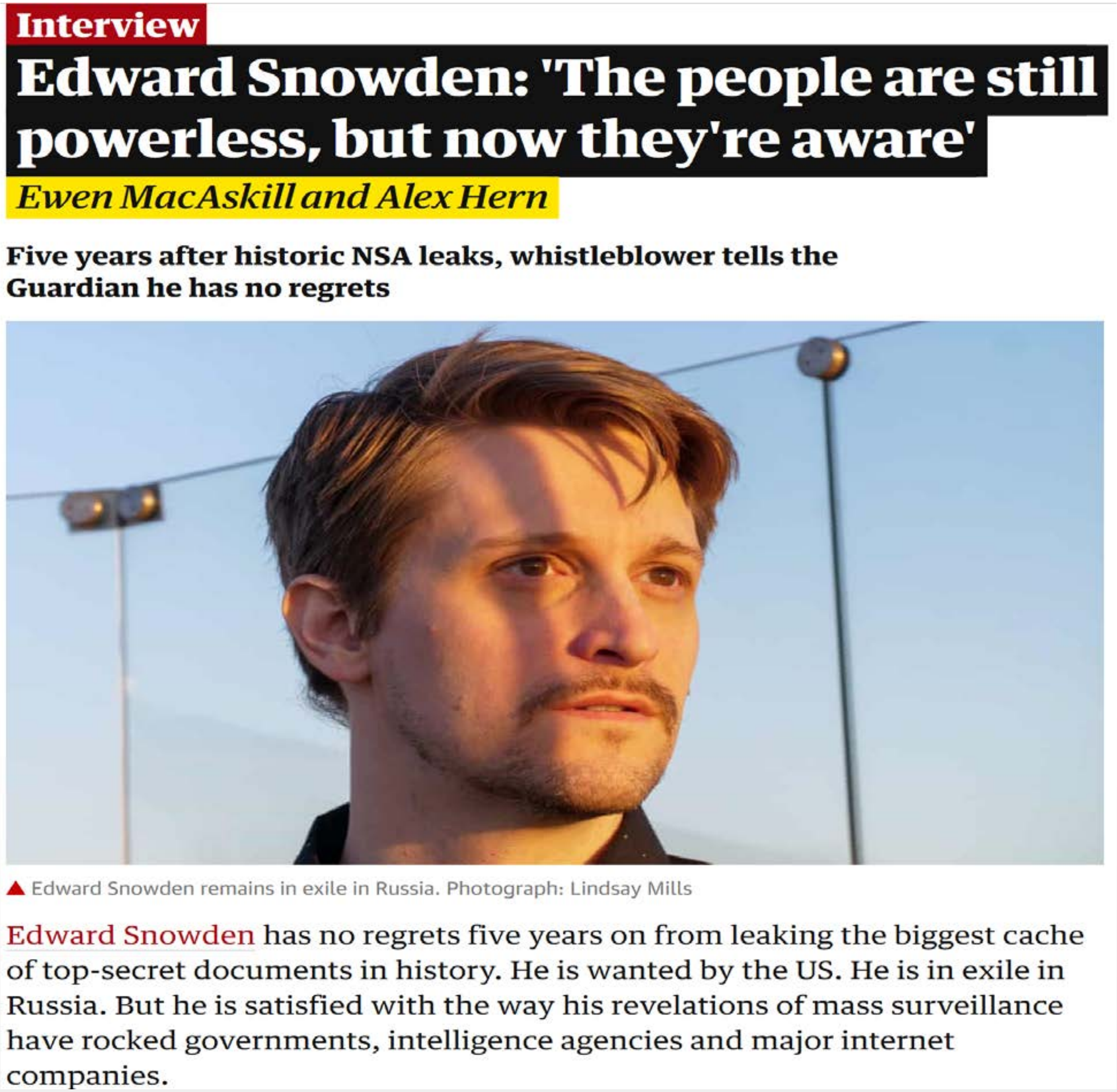
March 2017 M^{3}AAWG Publication

- *M3AAWG Describes Costs Associated with Using Crypto*

  “While there are "costs" to doing anything and everything, the Messaging, Malware and Mobile Anti-Abuse Working Group believes the "costs" associated with deploying encryption should not be a "show stopper," that is, should not be a barrier to employing encryption.”

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

2018 – 5 YEARS POST SNOWDEN DISCLOSURES



Interview

Edward Snowden: 'The people are still powerless, but now they're aware'

Ewen MacAskill and Alex Hern

Five years after historic NSA leaks, whistleblower tells the Guardian he has no regrets

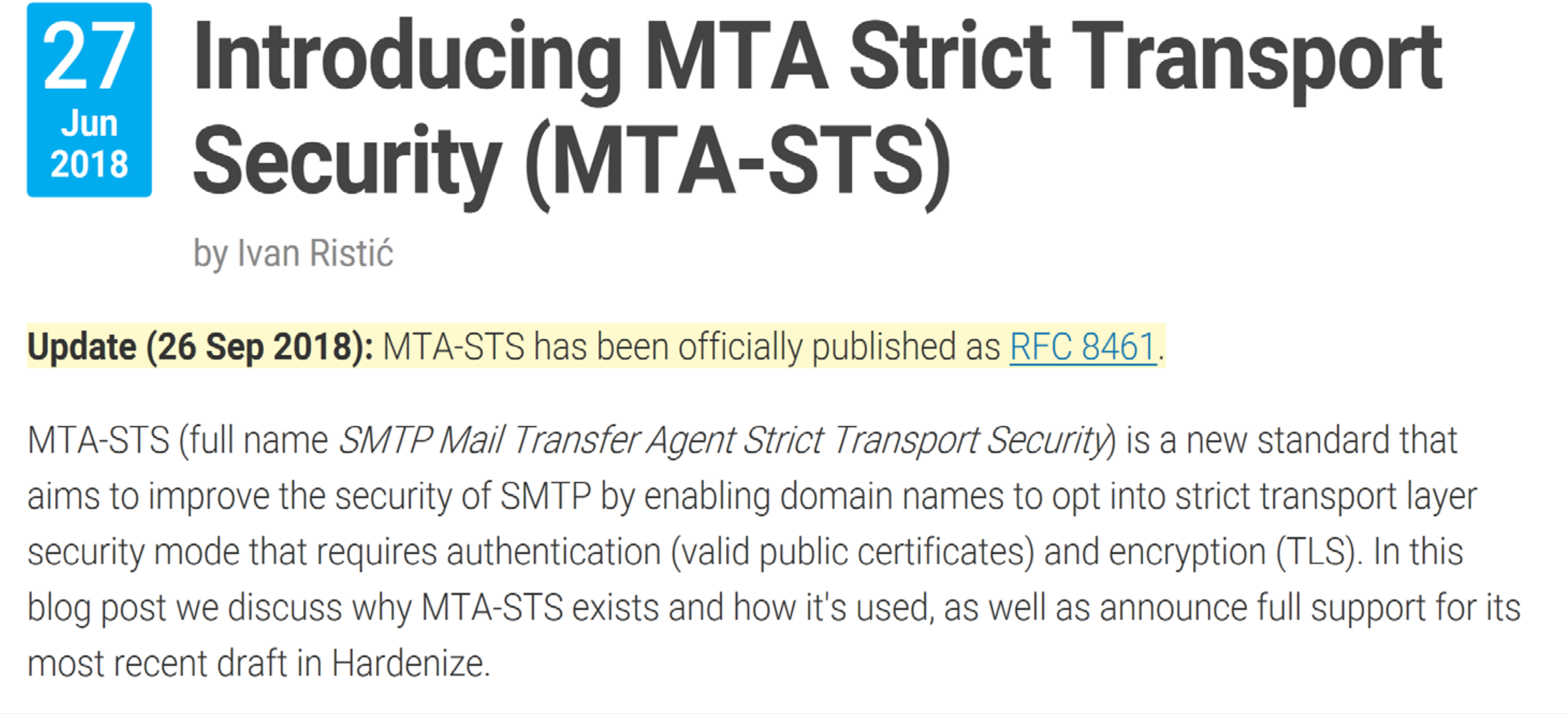
▲ Edward Snowden remains in exile in Russia. Photograph: Lindsay Mills

Edward Snowden has no regrets five years on from leaking the biggest cache of top-secret documents in history. He is wanted by the US. He is in exile in Russia. But he is satisfied with the way his revelations of mass surveillance have rocked governments, intelligence agencies and major internet companies.

https://www.theguardian.com/us-news/2018/jun/04/edward-snowden-people-still-powerless-but-aware

2018 – NEW IETF EMAIL SECURITY STANDARDS PUBLISHED

Adoption of New Email Security Standards



27
Jun
2018

Introducing MTA Strict Transport Security (MTA-STS)

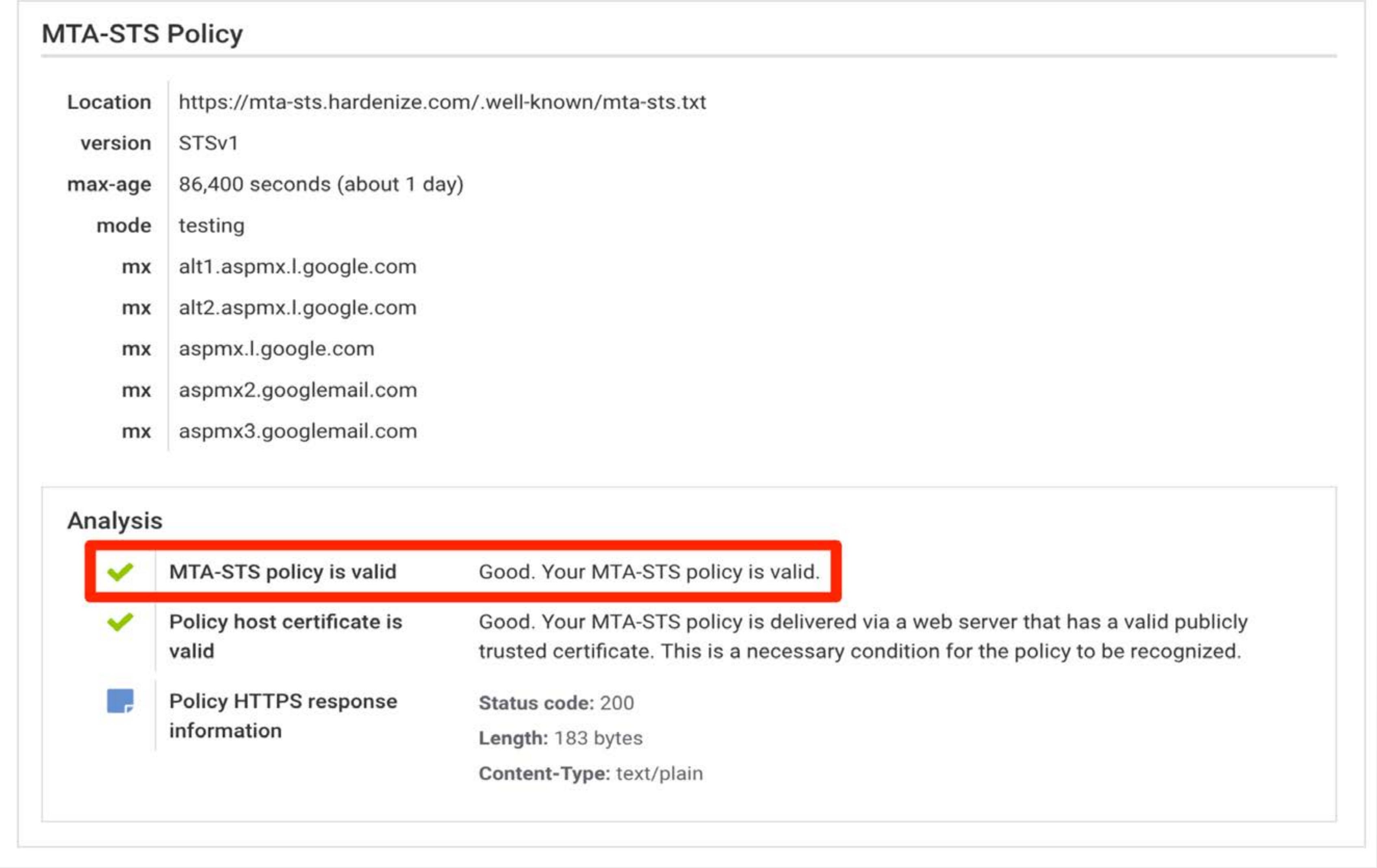
by Ivan Ristić

Update (26 Sep 2018): MTA-STS has been officially published as RFC 8461.

MTA-STS (full name *SMTP Mail Transfer Agent Strict Transport Security*) is a new standard that aims to improve the security of SMTP by enabling domain names to opt into strict transport layer security mode that requires authentication (valid public certificates) and encryption (TLS). In this blog post we discuss why MTA-STS exists and how it's used, as well as announce full support for its most recent draft in Hardenize.

https://www.hardenize.com/blog/mta-sts

Sample MTA-STS Policy



MTA-STS Policy

Location	https://mta-sts.hardenize.com/.well-known/mta-sts.txt
version	STSv1
max-age	86,400 seconds (about 1 day)
mode	testing
mx	alt1.aspmx.l.google.com
mx	alt2.aspmx.l.google.com
mx	aspmx.l.google.com
mx	aspmx2.googlemail.com
mx	aspmx3.googlemail.com

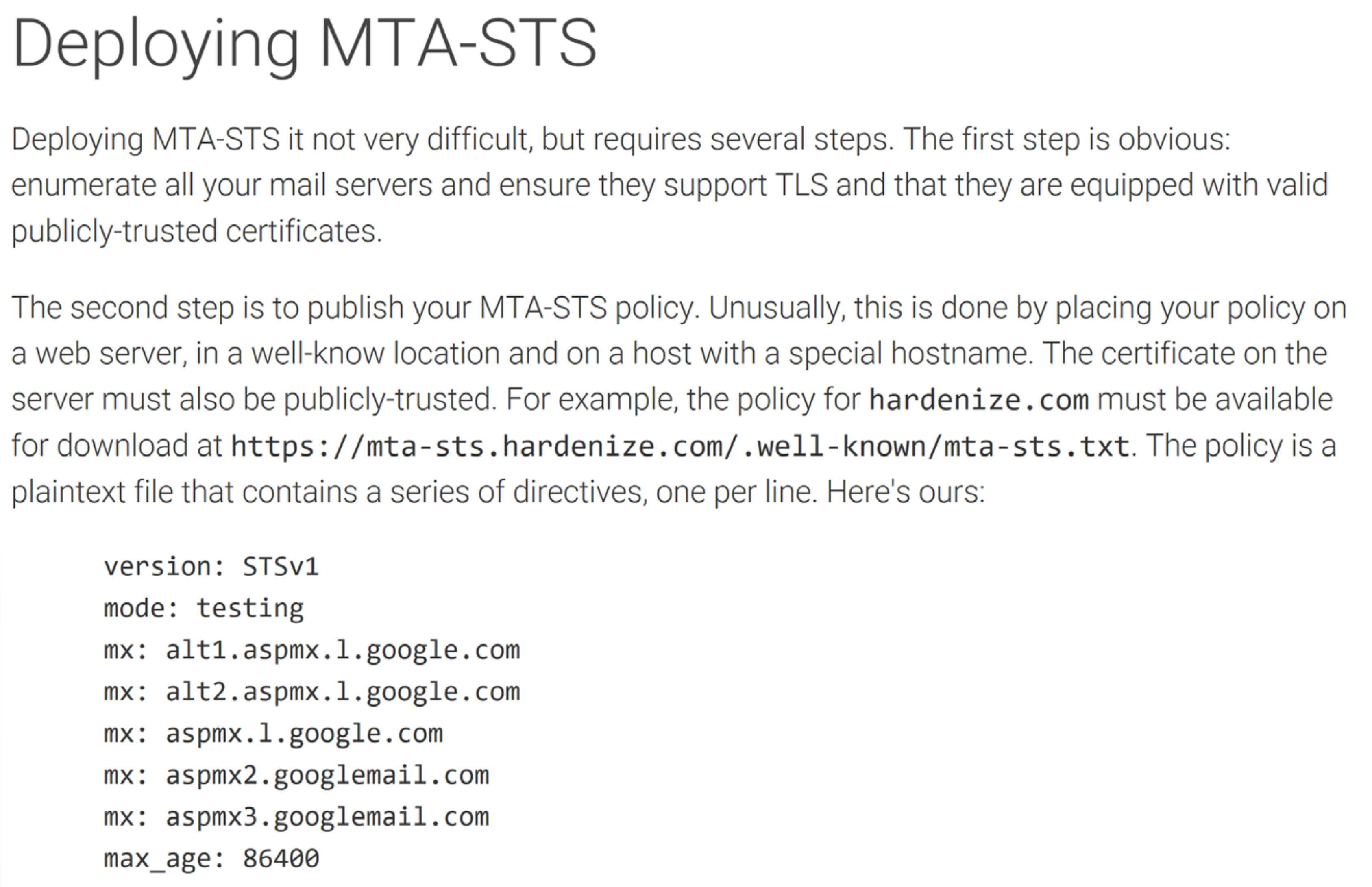
Analysis

✓	**MTA-STS policy is valid**	Good. Your MTA-STS policy is valid.
✓	**Policy host certificate is valid**	Good. Your MTA-STS policy is delivered via a web server that has a valid publicly trusted certificate. This is a necessary condition for the policy to be recognized.
▪	**Policy HTTPS response information**	**Status code:** 200 **Length:** 183 bytes **Content-Type:** text/plain

https://www.hardenize.com/blog/mta-sts

MTA-STS Deployment Steps

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group



Deploying MTA-STS

Deploying MTA-STS it not very difficult, but requires several steps. The first step is obvious: enumerate all your mail servers and ensure they support TLS and that they are equipped with valid publicly-trusted certificates.

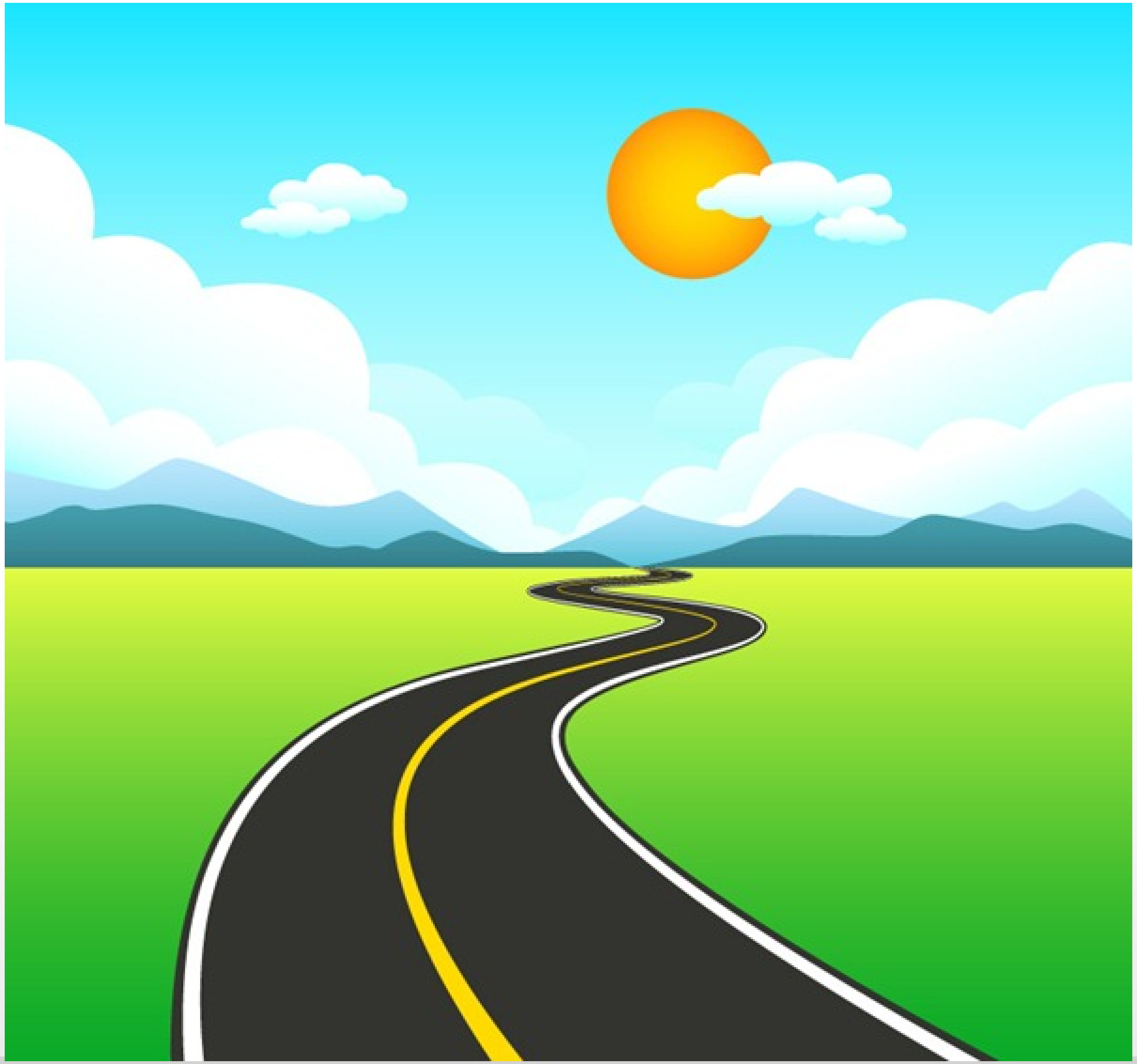
The second step is to publish your MTA-STS policy. Unusually, this is done by placing your policy on a web server, in a well-know location and on a host with a special hostname. The certificate on the server must also be publicly-trusted. For example, the policy for `hardenize.com` must be available for download at `https://mta-sts.hardenize.com/.well-known/mta-sts.txt`. The policy is a plaintext file that contains a series of directives, one per line. Here's ours:

```
version: STSv1
mode: testing
mx: alt1.aspmx.l.google.com
mx: alt2.aspmx.l.google.com
mx: aspmx.l.google.com
mx: aspmx2.googlemail.com
mx: aspmx3.googlemail.com
max_age: 86400
```

https://www.hardenize.com/blog/mta-sts

2018 – M^{3}AAWG PERVASIVE MONITORING SIG BECOMES DATA AND IDENTITY PROTECTION COMMITTEE

The Road Ahead



Upcoming Focus

- Continue working with industry partners on implementation SMTP MTA Strict Transport Security (MTA-STS) and SMTP TLS Reporting
- Working across the member community to understand impact for the upcoming Transport Layer Security (TLS) Protocol Version 1.3 release
- Working with M³AAWG's IETF liaison to evaluate the Deprecating TLSv1.0 and TLSv1.1 and Messaging Layer Security (MLS) Protocol to determine how the member community should contribute
- Upcoming focus on Identity Management and non-email messaging security

How can JP AAWG help?

- Partner on implementation of SMTP MTA Strict Transport Security (MTA-STS) and SMTP TLS Reporting standards
- Participate in future M³AAWG meetings
- Submit topics for upcoming meetings
- Engage with M³AAWG Committee Chairs to collaborate on initiatives

Acknowledgements / Contact Information

Data and Identity Protection Committee Leadership

- Alex Brotman (Co-Chair - Comcast)
- Joe St. Sauver (Senior Technical Advisor – Farsight Security)
- Stephen Farrell (Senior Technical Advisor – Trinity College Dublin)

Contact Information

- Janet.Jones@Microsoft.com

THANK YOU!