M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Pervasive Monitoring SIG

Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications

Janet Jones (Microsoft Trustworthy Computing – M3AAWG Pervasive Monitoring Co-Chair)
Josh Benaloh (Microsoft Research – "Keys Under Doormats" report – Co-Author)

October 20, 2015

Attendees Reminder:

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

What occurs in a M3AAWG meeting cannot be shared outside the membership

- Blogging, tweeting, posting is NOT allowed EXCEPT for referencing or citing the specific content on official M3AAWG public sites, which can be reposted or used in articles. The official sites are: www.m3aawg.org/DM3Z, www.Twitter.com/maawg, www.Facebook.com/maawg, https://www.facebook.com/groups/maawg/
- Respect M3AAWG anonymity: No publishing people or company names, except as cited on the official M3AAWG channels listed above
- No use of Wireshark or similar products on the M3AAWG network
- No photography - No video - No audio recording
- Any exception requires written permission from the Executive Director and may require permission from the session members
- All meeting attendees must wear and have their M3AAWG badge visible at all times during the meeting
- Please silence all electronic devices; be courteous to those listening to the presentations
- DO NOT LEAVE YOUR BELONGINGS UNATTENDED. Be aware and cautious at all times

Treat all attendees respectfully in and out of sessions. No less will be tolerated. Please review our meeting Conduct Policy at http://www.m3aawg.org/page/m3aawg-conduct-policy

For questions, please contact Jerry Upton at: jerry.upton@m3aawg.org

Reminders for Our Worldwide Friends

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

All meeting content is confidential: No photos, no video, no recording.
See staff with questions.

L'ensemble du contenu de la réunion est confidentiel : les photos, vidéos et enregistrements sont interdits. Pour toute question, demandez conseil au personnel.

Todo el contenido de la reunión es confidencial: No está permitido sacar fotografías ni grabar vídeo o audio. Consulte con el personal si tiene alguna pregunta.

Der gesamte Inhalt des Meetings ist vertraulich: Keine Fotos, kein Video, keine Tonaufzeichnung. Bei Fragen wenden Sie sich an die Mitarbeiter.

会議の内容はすべて機密扱いです。写真やビデオの撮影、録音は禁止されています。質問がある方は、スタッフまでご連絡ください。

所有会议内容均为保密信息：禁止拍照、录像、录音。如有疑问，请咨询职员。

회의에서 다루는 모든 내용은 기밀입니다. 사진 및 동영상 촬영과 녹음은 금지됩니다. 질문이 있으시면 직원에게 문의해 주십시오.

Pervasive Monitoring SIG

- Ongoing disclosures about the pervasive monitoring of email, voice and other network traffic remains 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 deplorability considerations.
- The 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

Pervasive Monitoring SIG Progress

- Drove industry awareness for importance of adopting Opportunistic TLS as a first-line defense against eavesdropping on user messaging.
  - Published industry guidance
    - *SSL/TLS for Mail: Some Initial M3AAWG Recommendations*
  - Adoption significantly increased since 2014 (~30% to ~80%)
    - *"Massive Growth in SMTP STARTTLS Deployment"*
    - *Google Transparency Report*
- Began working to address the more aggressive man-in-the middle (MITM) attack scenarios for messaging.
  - Published industry guidance
    - *Knowing Who You're Talking To: Addressing the Potential MITM Threat*
  - Evaluating DNSSEC / DANE technologies
  - Creating and evaluating a new protocol "SMTP Strict Transport Security (STS)" in coordination with the IETF

Pervasive Monitoring SIG Roadmap

Deliverable Description	Status	Target
Guidance - *"SSL/TLS for Mail: Some Initial M3AAWG Recommendations"*	Published	December 2014
Guidance – *"Knowing Who You're Talking To: Addressing the Potential MITM Threat"*	Published	February 2015
Endorsement – *"Keys Under Doormats" End-to-End Encryption Recommendations*	Published	August 2015
Guidance – *"Initial Recommendations for Using Forward Secrecy to Secure Data"*	Under final review	October 2015
Guidance - *"Crypto Isn't Free"*	Draft complete	December 2015
Guidance - *"Traffic Analysis"*	Draft complete	February 2016
Protocol - *"SMTP Strict Transport Security (STS)"*	Draft underway	March 2016
Guidance - *"Pervasive Monitoring Threat Model"*	Draft complete	TBD
Guidance - *"Securing Authentication"*	Draft complete	TBD
Guidance - *"Deploying Crypto For Messaging Other Than Email"*	Draft complete	TBD

Pervasive Monitoring SIG Sessions

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

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

Participation Welcomed!

- Join the Pervasive Monitoring SIG working forum via the M3AAWG site and participate in member discussions through email, events, or scheduled conference calls.
  - http://www.m3aawg.org/group/pervasive-monitoring-sig/
- Participate in deliverable planning, draft creation, and review cycles.
- Provide best practice knowledge or solutions where applicable and appropriate for SIG members.

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Keys Under Doormats:

Mandating Insecurity by Requiring Government Access to All Data and Communication

Harold Abelson, Ross Anderson, Steven M. Bellovin,
Josh Benaloh, Matthew Blaze, Whitfield Diffie,
John Gilmore, Matthew Green, Peter G. Neumann,
Susan Landau, Ronald L. Rivest, Jeffrey L. Schiller,
Bruce Schneier, Michael Specter, Daniel J. Weitzner

Our Principal Conclusions

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

We don’t know how to provide law-enforcement authorities the access they seek without further weakening the already fragile security of the Internet.

Our Principal Conclusions

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

We don't *believe* that suitable *exceptional access* can be provided with our current technology and infrastructure without creating undue risks.

What is the Ask?

Access to …

- Communications?
- Stored Data?
  - Held by a service provider?
  - Held on a target device?

Who should have Access?

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Ability to decrypt should be held by

- A single global entity?
- NSA/GCHQ/etc.?
- FBI / Local law enforcement?
- …

Who should have Access?

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Ability to decrypt should be held by

- Private sector …
  - Device manufactures?
  - Service providers?
  - Specialized third-party agents?

Fundamental Impediments

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Incompatibility with best practices
- Increase in complexity
- Concentration of targets

Current Best Practices

- (Perfect) Forward Secrecy
- Authenticated Encryption

Complexity is the Enemy of Security

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Office of Personnel Management
- FBI Trilogy Program
- Healthcare.gov
- …

Complexity is the Enemy of Security

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Sony
- Target
- Heartland Payment Systems
- T. J. Max
- Anthem
- …

Admiral James A. Winnefeld
Vice Chairman, Joint Chiefs of Staff

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

"But I think we would all win if our networks were more secure. And I think I would rather live on the side of secure networks and a harder problem for Mike [NSA Director Mike Rogers] on the intelligence side than very vulnerable networks and an easy problem for Mike and part of that, it's not only the right thing to do, but part of that goes to the fact that we are more vulnerable than any other country in the world, on our dependence on cyber. I'm also very confident that Mike has some very clever people working for him, who might actually still be able to get some good work done."

Admiral James A. Winnefeld
Vice Chairman, Joint Chiefs of Staff

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

"But I think we would all win if our networks were more secure. And I think I would rather live on the side of secure networks and a harder problem for Mike [NSA Director Mike Rogers] on the intelligence side than very vulnerable networks and an easy problem for Mike and part of that, it's not only the right thing to do, but part of that goes to the fact that we are more vulnerable than any other country in the world, on our dependence on cyber. I'm also very confident that Mike has some very clever people working for him, who might actually still be able to get some good work done."

Admiral James A. Winnefeld
Vice Chairman, Joint Chiefs of Staff

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

"But I think we would all win if our networks were more secure. And I think I would rather live on the side of secure networks and a harder problem for Mike [NSA Director Mike Rogers] on the intelligence side than very vulnerable networks and an easy problem for Mike and part of that, it's not only the right thing to do, but part of that goes to the fact that we are more vulnerable than any other country in the world, on our dependence on cyber. I'm also very confident that Mike has some very clever people working for him, who might actually still be able to get some good work done."

Concentration of Targets

- Office of Personnel Management

Apocryphal (but apt) quote attributed to Willie Sutton when asked why he robbed banks – “Because that’s where the money is.”

Concentration of Targets

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Even if decryption capabilities remain in the private sector with device manufactures or service providers, do we really want *golden keys* held by Verizon or Apple or Microsoft?

Scenarios

- Encrypted communications data
- Encrypted stored device data

Traditional Encrypted Communications

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Message m is encrypted with symmetric key k.
- Symmetric key k is encrypted with recipient's asymmetric key r.
- Transmit both $E{\downarrow}k\,(m)$ and $E{\downarrow}r\,(k)$.

Suggested Communications Access

Together with $E{\downarrow}k\,(m)$ and $E{\downarrow}r\,(k)$, transmit $E{\downarrow}g\,(k)$ where g is *golden key* to provide government access.

Suggested Communications Access

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Problem 1: Whose golden key?

- Single entity? Which one?
- Multiple golden keys?

Split keys increase complexity.

Suggested Communications Access

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Problem 2: This data transmission paradigm is being replaced due to weaknesses:

An attacker can collect $[E\downarrow k\,(m), E\downarrow r\,(k)]$ transmissions for years.

One breach can reveal all past data.

Forward Secrecy

Using “Diffie-Hellman” protocol, a new “ephemeral” random key is generated for each transmission.

This ephemeral key is destroyed once the transmission is complete.

Successful attacks must be real-time.

Suggested Communications Access

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Problem 3: *Authenticated encryption* is being adopted to simultaneously give confidentiality and authentication.

But giving a third party access to an authentication key allows that party to impersonate the sender and breaks authentication.

Encrypted Device Data

- One could postulate a regimen to gain access to data on “captured” devices.
- We do have some experience with localized private escrow systems (e.g. BitLocker).

Encrypted Device Data

If access keys are maintained by vendors, they must …

- Authenticate access requests by potentially large numbers of agencies.
- Verify possession of target device.

Encrypted Device Data

If access keys are maintained by law enforcement agents, vendors must …

- Obtain and install correct keys on their devices.
- Store and access extremely valuable and sensitive key material.

Encrypted Device Data

Whoever holds access keys …

- The master key or database is an attractive target.
- Frequent access must be secured.
- Updates are very difficult.

Encrypted Device Data

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

What happens when devices cross borders?

What keys are in my American-designed, Chinese-built mobile phone purchased in the UK and used in Russia to call someone in Syria?

Former NSA director of research

"When it comes to security, complexity is not your friend. Indeed it has been said that complexity is the enemy of security. This is a point that has been made often about cybersecurity in a variety of contexts including, technology, coding and policy. The basic idea is simple: as software systems grow more complex, they will contain more flaws and these flaws will be exploited by cyber adversaries."

Former NSA director of research

"When it comes to security, complexity is not your friend. Indeed it has been said that complexity is the enemy of security. This is a point that has been made often about cybersecurity in a variety of contexts including, technology, coding and policy. The basic idea is simple: as software systems grow more complex, they will contain more flaws and these flaws will be exploited by cyber adversaries."

Implementation

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Implementation is hard!

- A system that is designed to provide exceptional access under some circumstances might also inadvertently provide it elsewhere.
- Perfection cannot be guaranteed.

Competitive Disadvantage

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- U.S. products that provide exceptional law enforcement access will be at a severe competitive disadvantage in countries without access mandates.
- Broad international agreement seems unlikely.

Unanswered Questions

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Scope, Limitations, and Freedoms
- Planning and Design
- Deployment and Operation
- Evaluation, Assessment, and Evolution

Unanswered Questions – Scope (1)

- Are all systems that use encryption covered, or just some?
- Which ones?

Unanswered Questions – Scope (2)

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Do all online communications and information platforms have to provide access to plain text, or merely provide keys to agencies that had already collected ciphertext using technical means?

Unanswered Questions – Scope (3)

- Would individuals, corporations, nonprofit institutions, or governments be allowed to deploy additional encryption services on top of those systems with exceptional access?
- Would those user-installed systems also have to meet exceptional access requirements?

Unanswered Questions – Scope (4)

- Would machine-to-machine systems be covered?
- What about Internet of Things and industrial control (SCADA) systems?

Unanswered Questions – Scope (5)

- How would cross-border regulatory differences be resolved?
- Would technology developers have to meet different exceptional access requirements in each jurisdiction where their systems are used?
- Or would there be a globally harmonized set of regulatory requirements?

Unanswered Questions – Scope (6)

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- How can the technical design of an exceptional access system prevent mass surveillance that would covertly violate the rights of entire populations, while still allowing covert targeted surveillance of small numbers of suspects as an actual “exception” to a general rule of citizen privacy?

Unanswered Questions – Scope (7)

- Would there be an exception for research and teaching?

Unanswered Questions – Scope (8)

- Could companies refuse to comply with exceptional access rules based on a fear of violating human rights?

Unanswered Questions – Scope (9)

- Would anonymous communications, widely recognized as vital to democratic societies, be allowed?

Unanswered Questions – Design (1)

- What are the target cost and benefit estimates for such a program?

Unanswered Questions – Design (2)

- What security and reliability measures would be established for the design?
- How would system prototypes be tested?
- How long would companies have to comply with exceptional access rules?

Unanswered Questions – Design (3)

- How would existing services and products be treated if they do not comply with exceptional access rules?
- Would providers have to redesign their systems?
- What if those systems cannot accommodate exceptional access requirements?

Unanswered Questions – Design (4)

- Who would be involved in the design of the systems and procedures — just the US government, or would other governments be invited to participate?
- Could foreign technology providers such as Huawei participate in the design discussions?

Unanswered Questions – Design (5)

- Would the technical details of the program be made public and open for technical review?
- What level of assurance would be provided for the design?

Unanswered Questions – Operation (1a)

- Who would supervise compliance?
- Would an existing regulatory agency such as the FCC be given jurisdiction over the entire process?
- How would other countries regulate US domestic and foreign services?

Unanswered Questions – Operation (1b)

- Would there be a global harmonization of rules regulation and enforcement?
- Would the International Telecommunications Union have a role in setting and enforcing requirements?

Unanswered Questions – Operation (2a)

- Would global technical standards be required?
- How would these be developed and enforced?
- How would be such standards be changed/improved/patched?

Unanswered Questions – Operation (2b)

- Would traditional standards bodies such as the UN International Telecommunications Union T-sector or ISO set standards, or would the world look to Internet standards bodies such as the IETF and the World Wide Web Consortium?
- How would the world converge on one set of standards?

Unanswered Questions – Operation (3)

- Would the US government provide reference software libraries implementing the desired functionality?

Unanswered Questions – Operation (4)

- Would programs and apps need to be certified before they were allowed to be sold?
- Who would test or certify that programs produced operate as intended?

Unanswered Questions – Operation (5a)

- Who would be liable if the plaintext-disclosure mechanisms were buggy (either in design or in implementation), causing the disclosure of all citizens' information?

Unanswered Questions – Operation (5b)

- More generally, what would happen when (not if) critical secret information was revealed, such as the private keys that allow encrypted data to be read by anyone, that destroyed the privileged position of law enforcement?

Unanswered Questions – Operation (6)

- How many companies would withdraw all but local sales staff from markets where exceptional access was mandated in ways that clashed with their business strategies or the rights of users in other countries, as Google already has done from China and Russia?

Unanswered Questions – Evolution (1)

- What oversight program would be required to monitor the effectiveness, cost, benefits, and abuse of exceptional access?

Unanswered Questions – Evolution (2)

- What sunset provisions would be build into legislation for such a program?
- What conditions would be in place for its termination (e.g., for lack of sufficient benefit, for excessive cost, or for excessive abuse)?

Unanswered Questions – Evolution (3)

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- One unintended consequence of such a program may be a much-reduced use of crypto altogether. This would further weaken our already fragile and insecure information infrastructure, so how do we incentivize companies to continue encrypting sensitive user communications?

Unanswered Questions – Evolution (4)

- How will [the negative] economic impacts be assessed before an exceptional access program is mandated?
- Further, what economic effect would be considered too impactful for exceptional access to be considered worthwhile?

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Further questions???

Discussion

Arguments

Rebuttals