Protecting Messaging Other Than Email, plus Network Link Protection

Joe St Sauver, Ph.D.
stsauver@fsi.io or joe@stsauver.com
M3AAWG Senior Technical Advisor
Scientist, Farsight Security, Inc.

Gold Ballroom, 1st Floor
M3AAWG 36, San Francisco, California
Wednesday Feb 17th, 2016, 15:30-16:30

https://www.stsauver.com/joe/crypto-other-than-email/

Introduction

- Today's session has two parts:
  - **The first part will consider cryptographic privacy protection for messaging other than email.**
  - **The second part will focus on cryptographic protection of high speed internal links.**
- The common link between the two topics is that in each case, your options are **constrained by what the market offers.** Today's goal is to help you understand why you want protection for these points of exposure, and how to select a solution.
- Both of these topics are the subject of pending draft documents in the Pervasive Monitoring SIG.

I. Messaging Other Than Email

Messaging Other Than Email

- M3AAWG has been working hard on protecting **email** against pervasive monitoring.

- That's very important work, and protecting email privacy is a totally appropriate goal for M3AAWG.

- Although M3AAWG has always had a strong focus on **email**, our charter, as the anti-Pervasive Monitoring SIG of the **Messaging,** Malware, and **Mobile** Anti-Abuse Working Group, includes, or **should include**, protecting mobile voice telephony and mobile applications (such as texting/chat), too.

- Arguably, for many users, secure mobile voice and secure text/ chat is **as important**, or even **more important** than email.

What's The Need/Use Case For Secure Mobile Voice?

- There are many use cases/drivers, including...
- Deterring warrantless pervasive monitoring of voice traffic by foreign or domestic government agencies
- Helping to secure company-confidential info (business leads, new product development work, proprietary research, HR info, etc.)
- Assisting journalists to protect their confidential sources
- Helping attorneys confidentially consult with their clients
- Hardening health-care-related communications WRT HIPAA
- A simple human desire to enjoy the "luxury" of private communication with one's friends or family members
- And if we can have an encrypted experience that's as good as the unencrypted experience, why *shouldn't* we encrypt by default?
- If nothing else, shifting the default may help keep encrypted traffic from being novel and inherently interesting as such...

What About The Bad Guys?

- Some assert that offering strong crypto for voice calls, texts, etc., hinders **LEOs** and the **Intelligence community**, making it harder for them to keep us all safe. There have even been calls for a ban on strong encryption, or for government-accessible "backdoors."
- While such proposals are unquestionably offered with the best of intentions, they represent yet another failure to understand the modern reality – **crypto isn't something that can be effectively controlled on a country-by-country basis.**
- See for example, "Encryption Is Worldwide: Yet Another Reason Why a US Ban Makes No Sense," http://www.wired.com/2016/02/encryption-is-worldwide-yet-another-reason-why-a-us-ban-makes-no-sense/ which noted, "Any laws mandating encryption backdoors will overwhelmingly affect the innocent users of those products, [...] while having little effect on the rogue parties for which the backdoors are intended."

Please Note: We're NOT Talking About Overcoming Local Device Encryption

- This talk is NOT about whether or not a given phone, once seized, can be accessed by the authorities (although see "Judge orders Apple to help FBI hack San Bernardino gunman's cellphone," http://www.washingtontimes.com/news/2016/feb/16/apple-ordered-help-fbi-access-syed-farooks-cellpho/)
- We ARE talking about protecting **network traffic** when it is ***in transit*** between two mobile devices.
- I emphasize: we're NOT talking about keeping investigators from accessing the contents of a device they've seized.
- The American Enterprise Institute has an article that does a nice job of teasing these two issues apart. See the December 2015 piece: "Encryption: Conflating two technical issues in one policy debate," https://www.aei.org/publication/encryption-conflating-two-technical-issues-in-one-policy-debate/

Status Quo

- Much mobile text/voice telephony transit traffic is unencrypted (or, at best, imperfectly encrypted) by default. What do I mean by "imperfectly encrypted?" Well, as one example, see, "The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle," https://theintercept.com/2015/02/19/great-sim-heist/
- Today's talk describes some commercially available **mobile voice telephony** options that are **strongly encrypted end-to-end ("E2E").** Some of those options also include:
  -- end-to-end encrypted chat/text messaging and/or
  -- end-to-end encrypted person-to-person video.
- At one level, given that these are commercially-available products , **"all that people need to do is pick a product and use it."** That sounds easy, but the problem is **non-interoperability** and **the number of products available** for potential adoption.
- This can be a real problem if you're not just **"talking to yourself."**

The Distributed Bi-Lateral Adoption Problem

- In order for me to be able to use a secure mobile voice product that I've selected, **the person on the other end must ALSO must have it installed.**

- **This is the critical problem we face today:**

  -- lots of choices, but no critical mass around any one product
  -- poor/non-existent interoperability between products.

- This is the "distributed bi-lateral adoption problem.

- Some people have ideas for overcoming this problem...

Some "Solutions" to Handling "The Other End"

- Some commercial encrypted voice products may offer a free "receive only" client that can act as an inbound call **receiver** (but not an outbound call **initiator).** If you have a calling pattern that's strictly "one way," this might be a convenient solution, but that sort of traffic pattern seems rather improbable.
- Other products may target enterprise markets. In that case, management picks a product, that's what everybody has, and that's what everybody uses. Within the enterprise, the "other end problem" has been solved because everyone has the same thing.
- We're not really interested in either the "free receive-only" option or the enterprise case. **We're interested in options that will work for large Internet-scale populations of random consumer or small business adopters.**
- A free-for-everyone option would seem to be the most straightforward alternative

The Potentially Critical Role of Mobile Carriers

- Mobile carriers have a potentially critical role to play when it comes to promoting secure E2E voice and secure E2E text service.

- **If you're a mobile carrier, and you recommend/promote a secure voice/text option for your customers, that's likely what they'll use. This can help create critical mass/focused adoption.**

- We recognize that some mobile carriers may not be willing or able to choose a product of this sort – I totally get that.

- But, if you are a mobile carrier and you CAN promote a secure mobile voice and secure mobile text solution while your competitors don't, this may serve as a **positive market differentiator** in a noisy/crowded mobile marketplace.

Bet-Your-Life-Grade Protection?

- While some of the applications we'll mention are extraordinarily good at protecting your communications against eavesdropping, **please do NOT "bet your life" on any application mentioned.**
- Even with the best available options, there are still many ways that communication privacy can be potentially undercut for high value targets by determined adversaries, including via untrustworthy communication partners, compromised hardware, or technical eavesdropping measures (such as shotgun microphones) meant to remotely collect conversations *believed* – at least by those talking -- to be happening in privacy.
- If you do decide to rely on one of the solutions we'll mention, **please do your own due diligence** to verify the suitability of that solution for your unique circumstances and exposures. We recommend that you NOT blindly trust any commercially available solution in situations where you could get badly hurt.

Explicitly Excluded From Our Discussion

- We will also NOT consider devices that are intended for use solely by government-approved customers for classified communications over the **Defense Red Switch Network** (http://en.wikipedia.org/wiki/Defense_Red_Switch_Network)

- This means that we will NOT be including products such as

  - http://www.boeing.com/defense/boeing-black/index.page
  - https://gdmissionsystems.com/cyber/products/secure-voice
  - or any other product that relies on NSA "Type 1" (controlled access) crypto technology....

- That exclusion aside, what would we **would like to see in a secure mobile voice solution?**

Winnowing The Remaining Abundance of Options

- **Highly desirable "soft" (end-user-experience) factors:**

  (1) Easy to use
  (2) Free
  (3) HD quality (with low bandwidth utilization)
  (4) Also supports secure text, video and file transfers
  (5) Runs on "everything"

- **Highly desirable "hard" (technical) factors:**

  (1) Proven algorithms
  (2) Cryptographically secure E2E
  (3) Non-attributability (doesn't require linkage to a real identity)
  (4) Avoids opportunities for metadata collection
  (5) Open source for ease of auditing

II. "Soft" Factors:
The End-User Experience

These "soft" factors may be as important, or MORE important, than the "hard" factors...

(1) Easy to Use

- Consumers have been "spoiled" by how easy it is to use many popular unencrypted (or lightly-encrypted) Internet voice or text messaging applications.

- If encrypted alternatives are too hard-to-use, by comparison, most consumers simply won't bother to do so.

- It is hard to overemphasize the importance of this point

- **Cryptographically secure products, to succeed, most be easy to use**

(2) Free

- Users need to be able to afford any potential solution (at least if we want it to be potentially broadly adopted).

- This implies $500+ solutions are likely non-starters for the consumer market, particularly since both sides of a conversation would need to make such an investment.

- Free/open source software is obviously attractive, *IF* it is easily and securely installed and configured.

- Free products also avoid leaving a financial attribution trail ("follow the money")

Free? **How Does** ***That*** **Sort of Business Model Work?**

- A common Internet saying is, "If you're not paying, you're the product being sold," and often there's truth in that observation. There are exceptions, however. At least some cryptographically-protected secure voice products have been produced and distributed as "labors of love," relying on grants and donations.
- Other products may employ the usual set of "pseudo-free" funding approaches, including:
  -- limited free use (N minutes/month are free, more than that? $)
  -- basic product is free; feature-rich "pro" version costs $
  (for example, a voice product may generally be free, except for calls to/from POTS #'s)
  -- give away the product, but sell product support/prof. services
  -- in-app advertising generates revenue
  -- free (for now), maybe not-free later (once you're "hooked")
  -- build market share with an eye towards an eventual buy-out

(3) HD Quality (With Low Bandwidth Utilization)

- If a secure voice solution can't deliver good (virtually "HD") voice quality, it probably won't end up getting used. This means that any encrypted voice solution needs to be able to deliver high quality, low jitter audio.

- Delays (call setup time, and encrypt/transmit/decrypt latencies) also need to be minimized – this can't be like talking to someone on the moon. "Did this finally connect? Can you hear me? Over..." People just won't put up with it.

- AND the application needs to do all this while consuming relatively low amounts of bandwidth.

(4) Supports Secure Text, Video and File Transfers

- While voice is the thing that's often focused upon when it comes to securing mobile devices, mobile devices are often used as a way of transmitting text, files, and video, too.

- If the user's current non-encrypted messaging solution supports sending texts, video and files, they will expect a secure option to do so, too, and may not be willing to accept any option that doesn't deliver this.

(5) Runs on "Everything"

- Many solutions may only be available for limited platforms.
- For example, a solution might only be available for iPhone, or only be available for Android, or just in the form of a proprietary hardened handset.
- Ideally, we'd like a solution that's available for ALL popular handsets and mobile devices, including at least:
  -- Android
  -- iPhones and other iOS devices
  -- Mac OS X
  -- Microsoft Windows
  -- Linux
- We'd even like to see support for:
  -- Windows Phones
  -- Blackberry
  -- etc.

Interoperability: A Practical Necessity

- The desire to have a single product that can work "everywhere" is not some utopian "hippy commune" dream, it's a matter of simple pragmatism.
- If a product **doesn't** support all platforms, either:
  -- some people will not be able to securely communicate,
  -- multiple products will need to be used, or
  -- users may even have to buy and carry multiple devices
- It's a LOT easier if everyone can standardize on one or two mobile products at most (presumably this would mean Android (53.3% of the U.S. smartphone market as of December 2015), plus Apple iOS (42.9% of the US Market),* plus Mac OS X and MS Windows.

---

https://www.comscore.com/Insights/Market-Rankings/comScore-Reports-December-2015-US-Smartphone-Subscriber-Market-Share

III. "Hard" Factors: Technical Requirements

(1) Proven Cryptographic Algorithms

- There's nothing more frightening than use of "home-grown" crypto algorithms in a production system. You need thoroughly scrutinized/soundly implemented crypto protocols, instead.
- In a voice messaging space, this seems to largely devolve to:
  -- sRTP (https://tools.ietf.org/html/rfc3711)
  -- zRTP (https://tools.ietf.org/html/rfc6189)
  [nice FAQ on RTP, sRTP, zRTP at https://jitsi.org/Documentation/ZrtpFAQ , FWIW]
- Plus old friends from previous cryptographic conversations:
  -- TLS (potentially with all its well-loved warts and flaws)
  -- AES
  -- ECC
  -- DHE
  -- etc.

(2) Secure End-To-End

- If you've attended previous anti-Pervasive Monitoring talks, you know the difference between "in transit" or "hop-by-hop" cryptographic protection (as offered by TLS), and end-to-end protection (as offered by PGP/GPG). When it comes to mobile voice or text traffic, we want to be sure that the solution we use encrypts traffic end-to-end, not hop-by-hop.
- Some products claim to be cryptographically secure end-to-end, but then exhibit "anomalies."
- For example, imagine a test "end-to-end encrypted" session that conveyed specially tagged URLs, used NOWHERE ELSE, over an "end-to-end" secure channel.
- If those specially tagged URLs end up getting visited by a third party, as captured in the content of your web server log files, you have "smoking gun" proof that somebody other than the sender and receiver had access to traffic that they shouldn't have.

(3) Non-Attributability/Pseudo-Anonymity

- Because of concerns related to traffic analysis (see "The Enduring Challenges of Traffic Analysis," https://www.stsauver.com/joe/dublin-traffic-analysis/dublin-traffic-analysis.pdf), **it will also be highly desirable for E2E voice traffic not to be attributable to a particular known entity, even if it is securely encrypted.**
- Put simply, **you'd ideally like to be able to acquire a secure mobile voice solution for cash** (or a cash equivalent), and then be able to begin using that device with **no registration** or other linkage to any other online or real-life identity
- This means (ideally):
  -- Product available for over-the-counter retail purchase (or free download for addition to a "burner" phone)
  -- No login required to download or activate software
  -- No required link to a user's telephone number or to an email address

Non-Attributability & The User Discovery Problem

- **If a user does NOT link his or her email address and/or phone number to their encrypted communication tool, it may be hard for potential friends and colleagues to discover how to reach them, except through one-on-one side exchanges.**

- Many services thus offer the ability to link to the user's phone number or email address(es) as an ease-of-use convenience feature for the less-security-paranoid users.

- The good news is that if you do choose to use just a long-and-opaque non-discoverable address, it may be harder for spammers and other abusers to discover and harass you via encrypted messaging channels.

(4) Avoiding Metadata Creation

- Some messaging applications route everything through central servers, client-server style. Central servers are always a scary potential point of compromise and/or monitoring.

- Others route calls directly, "peer-to-peer," even avoiding any use of DNS through the use of distributed hash tables or other non-traditional addressing techniques. This will generally be preferred.

- However, because P2P applications must configure systems to permit at least some direct inbound connections from the Internet if they don't check in with a central rendezvous point, they may potentially be subject to identification by active scanning or through passive flow analysis.

(5) Open Source

- When thinking about closed source/proprietary programs, we often need to largely depend on vendor self-diligence to protect its users against backdoors or accidental flaws (unless the vendor is willing to at least get code audits from trusted third party assessors).

- Open source programs, on the other hand, can be checked by any interested party.

- Of course, to be fair, proponents of closed source products will note that open source products may be heavily scrutinized by hacker/crackers, too...

IV. Your Current Options

As We've Mentioned, There Are MANY Options From Which To Choose...

In alphabetical order by domain name (Note – listing here does NOT mean that the service has been "evaluated" or "endorsed" or "approved" by M3AAWG, these are merely some market options)

- http://www.bitwiseim.com/
- http://www.bleep.pm/
- http://www.bull.com/hoox/
- http://www.cellcrypt.com/
- http://www.celltrust.com/products/celltrust-secureline/#voice
- http://www.coverme.ws/en/index.html
- http://www.crypttalk.com/
- http://esdcryptophone.com/

[continued]

- https://www.gold-lock.com/en/goldlock3g/
- https://gowiper.com/
- http://kryptall.com/
- http://www.kryptoscommunications.com/
- http://voip.kryptotel.net/
- http://www.linphone.org/
- http://www.mocana.com/keytone
- http://wiki.mumble.info/wiki/Main_Page
- http://mysecurephone.us/
- https://ostel.co/about
- http://www.phonecrypt.com/~phonecry/index.php
- https://www.phone-x.net/

[continued]

- http://www.rohde-schwarz.com/en/product/topsec-mobile-productstartpage_63493-10284.html
- https://www.rokacom.com/
- https://safeum.com/
- https://www.securegroup.com/
- https://www.securemobile.com/
- http://www.securevoicegsm.com/
- http://www.secure-voice.com/secure-voice-3g.html
- https://www.seecrypt.com/en/
- https://silentcircle.com/
- https://www.simlar.org/en/
- http://www.tango.me

[continued]

- https://threema.ch/en
- https://www.tivi.com/en/tech/voipsoftcrypt.php
- http://torfone.org/
- https://tox.chat/
- http://www.tutus.se/products/farist-mobile.html
- https://www.vipole.com/en/
- http://www.voiponeclick.com/
- http://voxxpro.com/
- https://whispersystems.org/ ("Signal")
- https://www.wickr.com/
- https://www.wire.com/
- http://www.zoiper.com/en

- **If I've overlooked any encrypted voice options, drop me a note...**

'That's Too Many! Just Mention A Few Free Ones!'

	Bleep	Signal	Wickr*
E2E Encrypted 1:1 Voice	Yes	Yes	Voice Messages
E2E Encrypted 1:1 Text	Yes	Yes	Yes
iPhone	Yes	Yes	Yes
Android	Yes	Yes	Yes
Mac OS X	Yes	Beta	Yes
MS Windows	Yes	No	Yes
Linux	No	No	Yes
Peer to Peer	Yes	No	No
Open Source	No	Yes	No
Linked to Email	Optional	No	Optional
Linked to Tel #	Optional	Yes	Optional
Cost	Free	Free	Free

* Wickr is included here despite not offering a true real-time voice option to ensure that at least one easy-to-use cross-platform option with Linux support gets included.

"But Joe! You Should Have Picked..."

- Think that I picked the "wrong" three products to show in that table? Entirely possible. I **don't** claim to have any overarching ability to pick the best thing for everyone to use.

- I will say that I DO think that you should

  -- PICK SOMETHING,
  -- TRY IT, AND
  -- ENCOURAGE THOSE YOU COMMUNICATE WITH TO TRY IT, TOO!

- Let's move on and talk a little about encrypting high speed point-to-point network links now.

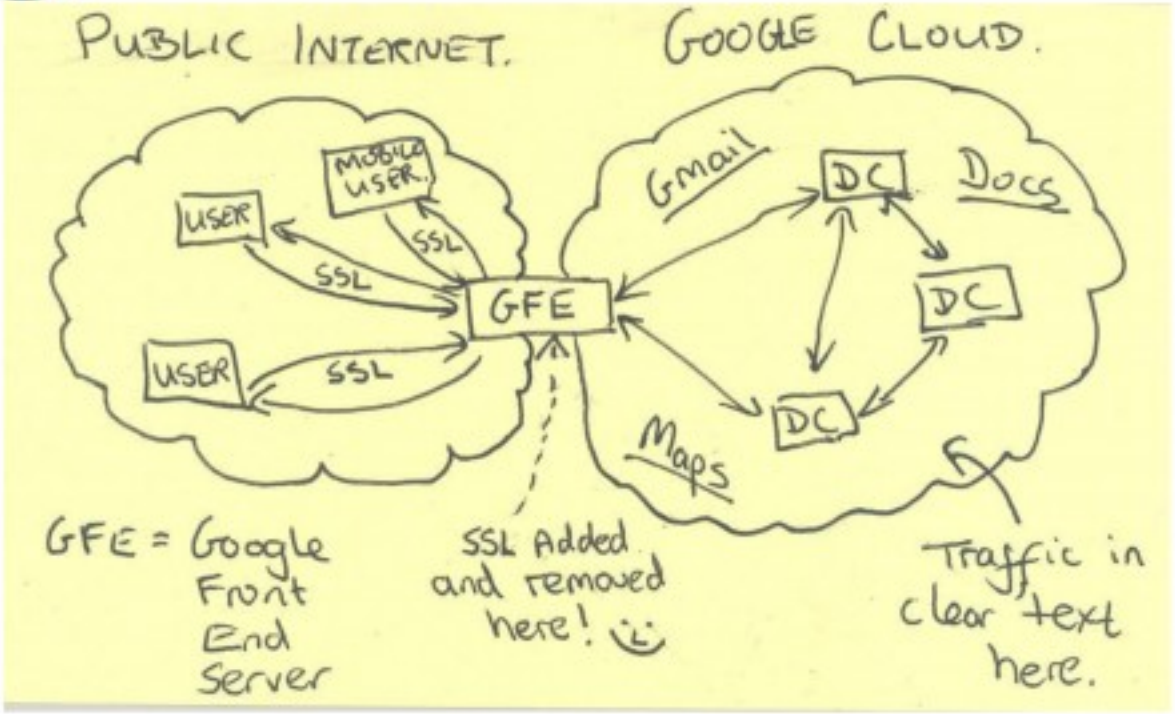
V. Protecting Point-to-Point Network Links

[This section is meant for you to use to spur discussions with your network engineering team]

The Need For This Work -- "Traffic is in clear text here."

TOP SECRET//SI//NOFORN

Current Efforts - Google



TOP SECRET//SI//NOFORN

For The Record

- The victim network targeted in the preceding slide has now reportedly addressed that vulnerability, see, for example: http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network/

  See also:

- http://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/
- http://www.pcworld.com/article/2139440/yahoo-turns-on-encryption-between-data-centers.html

- **But what about <u>your</u> company's internal network links? Are they encrypted, too?**

M3AAWG Members Typically Need Solutions That START At 10 Gbps and Go On Up

- Just to make sure we're talking about the right scale, these days many M3AAWG members' internal network links likely start at 10 Gigabit per second and just keep going up from there.

- The speed of those links can be important because cryptographic options at those speeds may be relatively limited.

- Very high speed crypto solutions can also be surprisingly expensive (at least in some cases).

- There are other considerations, too...

Encrypt at *What Layer*?

- Network link encryption can be handled by options running at layer 1,[1] layer 2,[2] or layer 3[3] of the OSI[4] model.
  Given uncertainties about various attacks against encryption technologies, some sites may even decide that they want to run *multiple* encryption products 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 doesn't preclude *also* doing encryption at layer 6[5]
  (e.g., opportunistic SSL/TLS), or encryption at layer 7[6]
  (end-to-end encryption), as well.

---

1 http://en.wikipedia.org/wiki/Physical_layer
2 http://en.wikipedia.org/wiki/Data_link_layer
3 http://en.wikipedia.org/wiki/Network_layer
4 http://en.wikipedia.org/wiki/OSI_model
5 https://en.wikipedia.org/wiki/Presentation_layer
6 http://en.wikipedia.org/wiki/Application_layer

The OSI Model

OSI Model				
Layer		Protocol data unit (PDU)	Function[3]	Examples
Host layers	7. Application	Data	High-level APIs, including resource sharing, remote file access, directory services and virtual terminals	TLS, FTP, HTTP, HTTPS, SMTP, SSH, Telnet
	6. Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption	CSS, GIF, HTML, XML, JSON
	5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes	RPC, SCP, PAP
	4. Transport	Segment (TCP) / Datagram (UDP)	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing	NETBEUI, TCP, UDP
Media layers	3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control	AppleTalk, ICMP, IPsec, IPv4, IPv6
	2. Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer	IEEE 802.2, L2TP, LLDP, MAC, PPP
	1. Physical	Bit	Transmission and reception of raw bit streams over a physical medium	DOCSIS, DSL, Ethernet physical layer, ISDN, USB

Source: https://en.wikipedia.org/wiki/OSI_model

You Must Be At Least /This Tall/ To Ride

- To be considered here, network encryption solutions must support a minimum of AES-256. This rules out, for example, products that only support less-strong AES-128.
- While there has long been discussion in the industry around whether or not AES-128 is "good enough," guidance from the NSA itself now clarifies its position on recommended key lengths. See for example "... it is prudent to use larger key sizes in algorithms [...] in many systems (especially, smaller scale systems). Additionally, IAD customers using layered commercial solutions to protect classified national security information with a long intelligence life should begin implementing a layer of quantum resistant protection. Such protection may be implemented today through the use of large symmetric keys..." The guidance specifically calls out AES-256. See https://www.nsa.gov/ia/programs/suiteb_cryptography/

Is It Available To Non-Governmental Entities?

- Products must also be available for sale to non-governmental entities. This means excluding HAIPE[1]-compliant devices such as:

  https://gdmissionsystems.com/cyber/products/taclane-network-encryption/taclane-10g-encryptor/ and

  http://www2.l-3com.com/cs-east/pdf/kg245x.pdf

  both of which are 10Gbps, but which use classified NSA Suite A[2] crypto algorithms restricted to just government and military users.

---

1 https://en.wikipedia.org/wiki/High_Assurance_Internet_Protocol_Encryptor
2 http://en.wikipedia.org/wiki/NSA_Suite_A_Cryptography

You *Will* Be Buying A Commercial Solution

- Solutions in this space are normally delivered in the form of hardware from commercial vendors (you can't role your own 10gig-or-faster crypto appliances in software)
- In enumerating the products discussed herein, neither M3AAWG nor I are a position to say which competing vendor's solution may be "best," nor do we assert that ANY vendor solution will be adequate to meet a particular site's needs.
- Each company must do its own due diligence when it comes to evaluating network cryptographic options in light of its own unique requirements.
- **This document is meant as a collection of starting points, nothing more.** Available products may change from time-to-time, so please always consult vendors of interest for the latest options. Typically I'll only mention one product per vendor per category; see each vendor for other potential possibilities.

We're Talking About Domestic Networks

- The network infrastructure cryptographic products discussed in this talk are assumed to be meant for use within the United States.

- If these devices are needed for use abroad, they will typically subject to U.S. export controls, and the devices may be subject to international controls as well. See the excerpt on the following slide as an example of one relevant U.S. provision.

- Please consult an attorney for authoritative information.

The network hardware solutions identified in this talk generally are:

"(A) **Network infrastructure software and commodities** and components thereof (including commodities and software necessary to activate or enable cryptographic functionality in network infrastructure products) **providing secure Wide Area Network (WAN), Metropolitan Area Network (MAN), Virtual Private Network (VPN)**, satellite, digital packet telephony/media (voice, video, data) over Internet protocol, cellular or trunked communications meeting any of the following **with key lengths exceeding 80-bits for symmetric algorithms:**

(1) **Aggregate encrypted WAN, MAN, VPN or backhaul throughput** (including communications through wireless network elements such as gateways, mobile switches, and controllers) **greater than 90 Mbps;**
(2) **Wire (line), cable or fiber-optic WAN, MAN or VPN single-channel input data rate exceeding 154 Mbps**; [...]"

See 15 C.F.R. 740.17 (b) (2), http://www.law.cornell.edu/cfr/text/15/740.17 (emphasis added). **Such items are subject to special export licensing/controls.**

VI. Layer 1 Encryption

Encryption at the Optical Layer

- In the layer 1 encryption case, encryption is handled on a point-to-point (or ring-by-ring) basis at the optical layer.

- This choice imposes the least network overhead and the lowest latency, and has the advantage of being protocol independent. It also supports some of the highest network bit rates available. See https://meetings.internet2.edu/media/medialibrary/2015/04/29/Internet2_Global_ADVA_Optical_Networking-Final.pdf

- Interoperability between/across vendors may be limited.
  This may constrain layer 1 optical encryption choices to what's available from your current optical vendor, at least if you're a site that have already deployed extensive optical infrastructure.

Some Sample Layer 1 Encryption Options

- "**ADVA** Optical Networking Launches Industry First with 100G Metro and Built-in Encryption," May 14, 2014, http://www.advaoptical.com/en/newsroom/press-releases-english/20140514
- "**Alcatel** Secure Solutions for Data Center Connect," http://resources.alcatel-lucent.com/?cid=154976
- "**Arista** 7500 Series," https://www.arista.com/en/products/7500-series
- "New Encryption Solution from **Ciena** Decreases Data Breach Risks Across Metro and Long-Haul Networks," http://newswire.telecomramblings.com/2016/01/new-encryption-solution-from-ciena-decreases-data-breach-risks-across-metro-and-long-haul-networks/
- "**Cisco** Transport Layer Encryption," http://www.slideshare.net/CiscoPublicSector/encryption-ponc-33

Physical Protection, Too?

- In addition to encrypting your network traffic at layer 1, you may also want anti-tampering protections, too.

- See the discussion in "Physical Security of Advanced Network and Systems Infrastructure," https://www.stsauver.com/~joe/phys-sec-i2mm/phys-sec-i2mm.pdf

VII. Layer 2 Encryption: MacSec/LinkSec

Layer 2 Encryption

- Layer 2 encryption is now often referred to as "MACsec," 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.

- Nice MacSec overview in "Using MACsec to Protect High-Speed Ethernet Links," http://www.ethernetsummit.com/English/Collaterals/Proceedings/2015/20150416_A201_Singer.pdf

Some Layer 2 Encryption Options

- "**Atmedia** 10G Ethernet Encryptor," http://www.atmedia.de/en/products/atmedia-10g-ethernet-encryptor.html
- "**Certes** Networks Secure Data Center Interconnect," http://certesnetworks.com/solutions/secure-data-center-interconnect/
- "**Cisco** Catalyst 6900 Series 40 Gigabit Ethernet Interface Module for Cisco Catalyst 6500 Series Switches Data Sheet," http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/data_sheet_c78-696623.html
- "**Crypto Link** HC-8682 100G ," http://www.crypto.ch/en/products-and-services/products/crypto-link-hc-8682-100g

[continued]

Some Layer 2 Encryption Options (cont)

- "**Cube Optics** Transport Cube Encryption Unit," http://www.cubeoptics.com/uploads/tx_cuboproducts/D-5121-Rev.A_Encryption_TRANSPORT_CUBE.pdf
- "**ID Quantique** Centauris Layer 2 Encryptors (CN8000)," http://www.idquantique.com/quantum-safe-crypto/network-encryption/centauris-layer-2-encryptors.html
- "**Juniper** EX4200 Ethernet Switches," http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000215-en.pdf
- "**NEC** COMCIPHER XL2B," http://jpn.nec.com/access/prod/xl2b/index.html
- "**Rodhe & Schwartz** SITLine ETH Ethernet Encryptor," http://www.sit.rohde-schwarz.com/en/Products/SITLine_ETH.html

[continued]

Some Layer 2 Encryption Options (cont)

- "**Safenet** CN 6100 0 Gbps Ethernet Encryptor," http://www.safenet-inc.com/resources/product-brief/data-protection/SafeNet-CN6100-Ethernet-Encryptor_Product_Brief/?utm_source=press-release&utm_medium=pr-link&utm_campaign=new-hse-products
- "**Senetas** CN6100," http://www.senetas.com/_uploads/files/Technical-Paper_Understanding_Senetas_Layer_2_Encryption.pdf
- "**Secunet** SINA L2 Encryption Box," http://www.secunet.com/fileadmin/sina_downloads/Produktinfo_englisch/SINA_L2_Brochure_en_final.pdf
- "**Thales** e-Security Datacryptor Ethernet Layer 2," http://images.go.thales-esecurity.com/Web/ThalesEsecurity/%7B36be2461-0a58-4395-bfe0-75b4c1063432%7D_Datacryptor_Ethernet_Layer_2_ds.pdf

10Gbps+ NICs and LinkSec/MacSec Support

- At 10Gbps and above, our focus is generally on enclave-to-enclave links within the data center, and on datacenter-to-datacenter links.

- However, if you need to push layer two crypto all the way to the server, be sure you're using a network adapter/NIC card that supports MACsec.

- While there are many NICs that support MACsec at one Gbps speeds, at this time, we're only aware of a few that indicate that they're able to do so at 10Gbps or faster speeds.

Some 10Gbps+ NICs Supporting LinkSec/MacSec

- "Advantech MIC-3666 Dual 10 Gigabit Ethernet XMC," http://downloadt.advantech.com/ProductFile/PIS/MIC-3666/Product%20-%20Datasheet/MIC-3666_DS20120626175504.pdf

- "Hotlava Systems Multi-Port 10 Gigabit Ethernet Network Adapters," http://www.hotlavasystems.com/pdfs/HLS_TamboraDS.pdf

- "Intel Ethernet Converged Network Adapter X520," http://www.intel.com/content/dam/doc/product-brief/ethernet-x520-server-adapters-brief.pdf

- "Niagara 32716 Hex Port Fiber 10 Gigabit Ethernet NIC," http://www.interfacemasters.com/pdf/Niagara_32716.pdf

VIII. Layer 3 Encryption: IPSec

Layer 3 Encryption

- Layer 3 encryption generally means doing IPsec.[1]
- We will assume a desire to do IPsec in tunnel mode[2] (rather than transport mode). Tunnel mode encapsulates and protects the entire IP packet.
- Doing IPsec at 10Gbps can be quite challenging/expensive, and is subject to both materials latency issues and substantial overhead-related impacts. That's why network encryption is typically done at layer 1 or layer 2, instead of layer 3.
- However, we include pointers to at least a couple layer 3 10Gbps+ IPsec options here for completeness, and for situations where encryption at layer 3 might be desirable as a complement to encryption at other layers. IPsec is also often suggested as the correct way to protect MPLS traffic from eavesdropping.

---

1 http://en.wikipedia.org/wiki/IPsec
2 http://en.wikipedia.org/wiki/IPsec#Tunnel_mode

A Couple of Sample Layer 3 Encryption Options

- "Brocade MLX 4-Port 10 GBE IPsec Module," http://www.brocade.com/downloads/documents/data_sheets/product_data_sheets/brocade-mlx-ipsec-module-ds.pdf

- "Fortinet FortiGate 5000 Series," http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-5101C.pdf

IETF MPLS Encryption Draft

- Those who have extensive MPLS networks may also want to check out

  "Opportunistic Security in MPLS Networks," draft-ietf-mpls-opportunistic-encrypt-00.txt (expires January 23rd, 2016), https://tools.ietf.org/html/draft-ietf-mpls-opportunistic-encrypt-00

- You may also want to visit with M3AAWG Sr Technical Advisor Stephen Farrell, since he's one of the authors of that draft!

IX. Conclusion

One Slide Takeaway

- Traditionally, M3AAWG has focused on hardening email against pervasive monitoring, and we've made good progress. However, our work isn't done.

- For example, regular mobile voice and text traffic isn't adequately protected from eavesdropping. You should select and employ a commercially available mobile encryption product (such as Bleep, Signal, or Wickr, among others) to improve the security and privacy of your mobile voice and messaging traffic.

- Another area where encryption is needed is on intra-data center and inter-data center links. While those links may be running at 10Gbps, 40Gbps or even 100Gbps, there are now commercially available encryption solutions that will evenwork at those speeds. You should be using those solutions to protect your links.

Thanks for The Chance To Talk Today

- Are there any questions?