Public Comments on the Second Draft of NIST Special Publication 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (October 15, 2018)

Originally Posted: 12/4/2018
Correction Posted: 3/6/2019

NIST received the following public comments on the Second Draft of Special Publication 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (October 2018). These public comments were received by the November 16, 2018 deadline.

From James DeRienzo:

Greetings:

Consider highlighting the modal auxiliary verbs besides shall, shall not, should and should not.

Consider using highlighting instead of boldface type. The highlight legend can indicate model auxiliary verb expression:

[The following illustrations were provided by the commenter without attribution.]

We use modal verbs to express:

ABILITY - CAPABILITY

I can swim.

I could swim when I was five.

SUGGESTION

You could give Mary some flowers.

Shall we buy her a hat?

a REQUEST

Can I go to the cinema tonight?

Could you lend me £5, please?

May I leave the room?

Would you please close the door?

DEDUCTION-ASSUMPTION

It couldn't have been John because he's in London.

He drives a Ferrari. He must be rich.

PROHIBITION

You mustn't eat any more chocolate.

You should never repeat what you have just said.

NECESSITY

We must buy some more vegetables.

Semi-modals (have to/need to) are often preferred. NOT NECESSARY uses don't have to or don't need to/ needn't

We don't need to buy any more vegetables. (It isn't necessary)

PERMISSION

You can go to the cinema.

In the evenings we could watch TV.

POSSIBILITY

Measles can be quite dangerous.

This vase could be very valuable.

He may be waiting for us at the airport.

John might come to your party.

Would John come with us if we asked him?

SPECULATION

He may have gone to Spain with Mary.

Someone might have already told his father.

What would I have done without you?

Where shall/will we be this time next year?

OBLIGATION

You must / have to study harder!

I should be studying but I'm too tired.

ADVICE

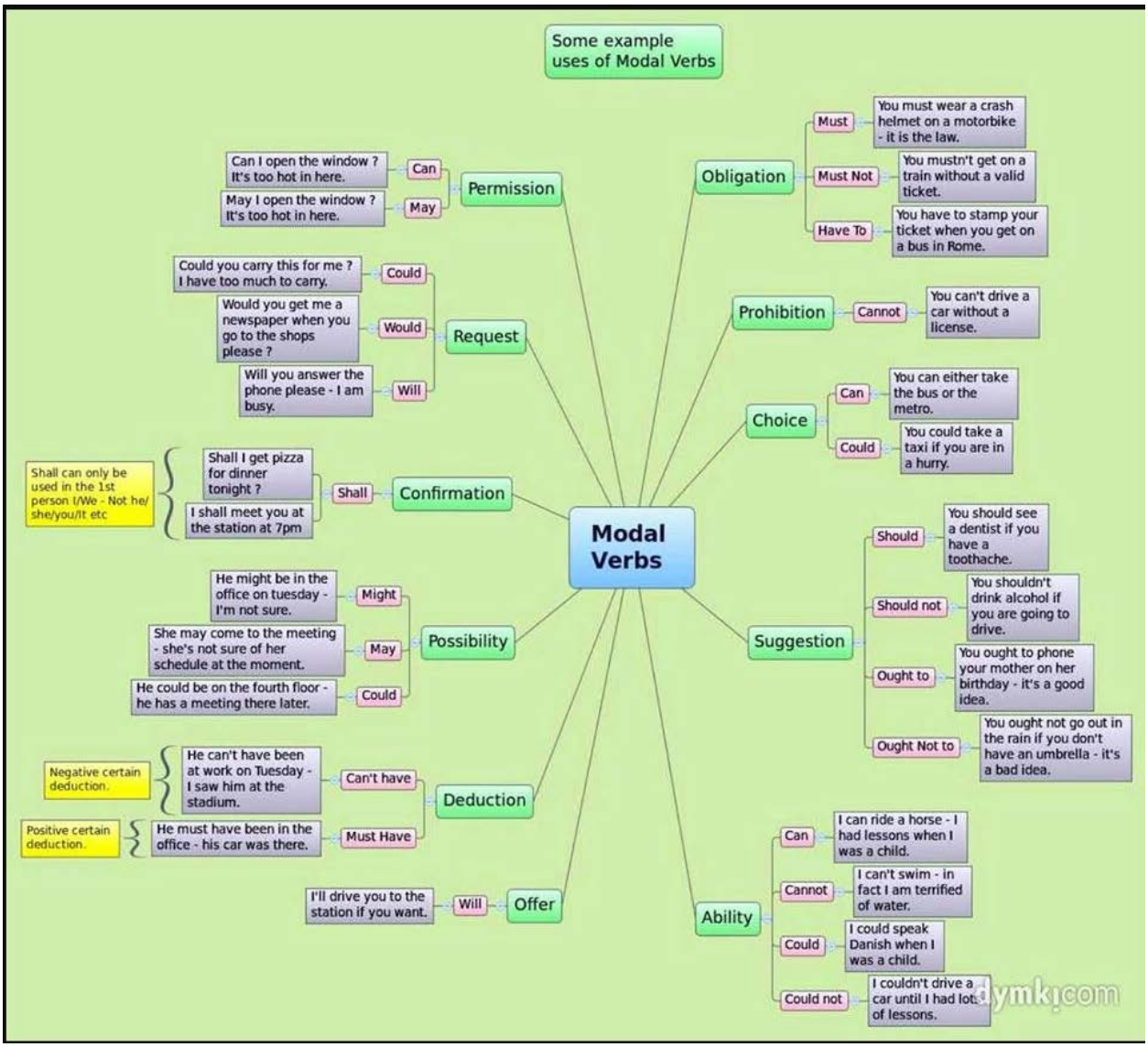
You should go to the doctor's tomorrow.

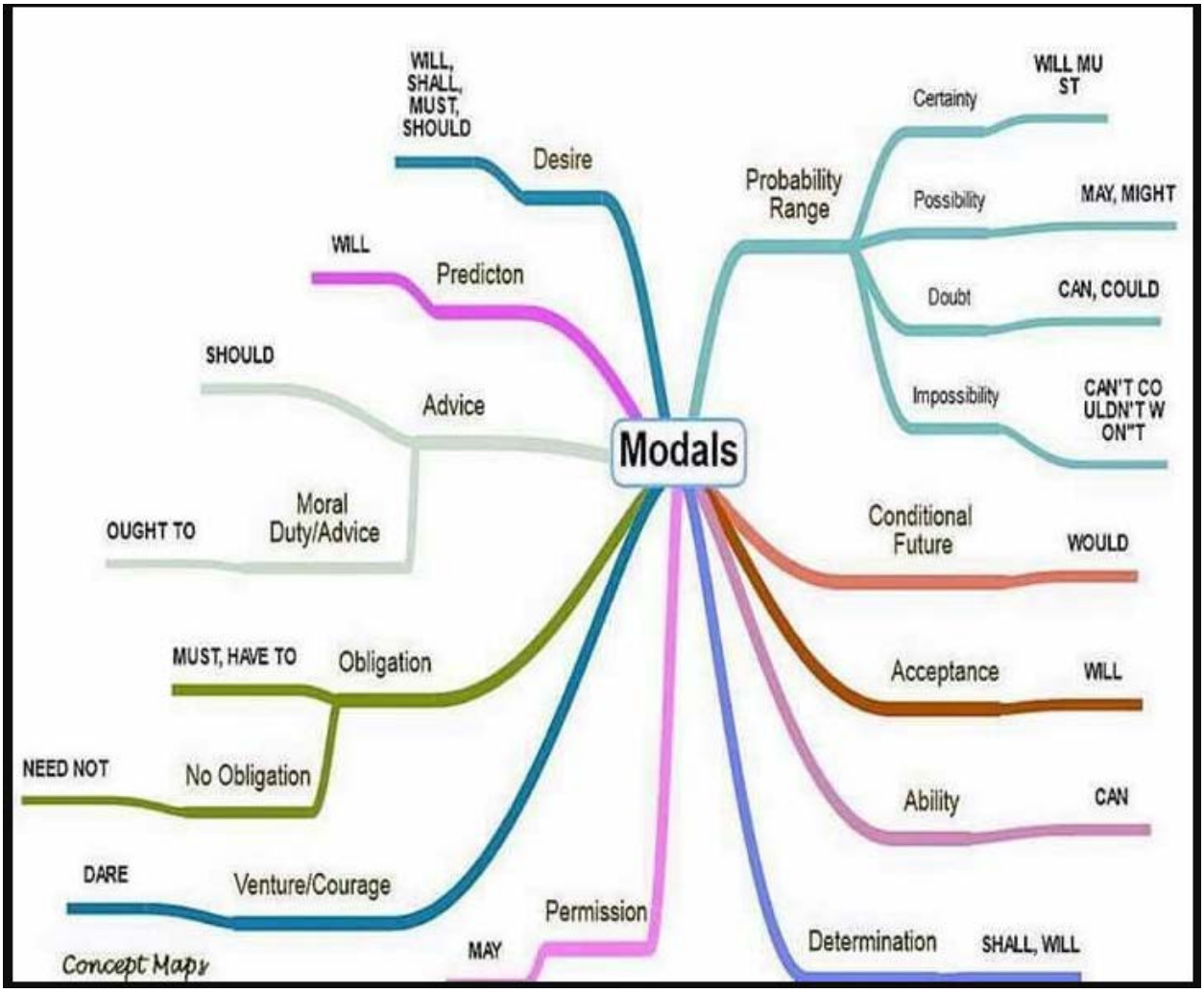
You must go to the doctor's tomorrow! (emphatic advice)

Semi- modals and other forms are often used. However, they sometimes change the level of intensity of the advice given.

You ought to/had better/have to/ . . . . . .

If I were you I would go to the doctor's.


Some example uses of Modal Verbs
Modal Verbs
Permission
Can
Can I open the window ? It's too hot in here.
May
May I open the window ? It's too hot in here.
Request
Could
Could you carry this for me ? I have too much to carry.
Would
Would you get me a newspaper when you go to the shops please ?
Will
Will you answer the phone please - I am busy.
Confirmation
Shall
Shall can only be used in the 1st person I/We - Not he/she/you/It etc
Shall I get pizza for dinner tonight ?
I shall meet you at the station at 7pm
Possibility
Might
He might be in the office on tuesday - I'm not sure.
May
She may come to the meeting - she's not sure of her schedule at the moment.
Could
He could be on the fourth floor - he has a meeting there later.
Deduction
Negative certain deduction.
Can't have
He can't have been at work on Tuesday - I saw him at the stadium.
Positive certain deduction.
Must Have
He must have been in the office - his car was there.
Offer
Will
I'll drive you to the station if you want.
Obligation
Must
You must wear a crash helmet on a motorbike - it is the law.
Must Not
You mustn't get on a train without a valid ticket.
Have To
You have to stamp your ticket when you get on a bus in Rome.
Prohibition
Cannot
You can't drive a car without a license.
Choice
Can
You can either take the bus or the metro.
Could
You could take a taxi if you are in a hurry.
Suggestion
Should
You should see a dentist if you have a toothache.
Should not
You shouldn't drink alcohol if you are going to drive.
Ought to
You ought to phone your mother on her birthday - it's a good idea.
Ought Not to
You ought not go out in the rain if you don't have an umbrella - it's a bad idea.
Ability
Can
I can ride a horse - I had lessons when I was a child.
Cannot
I can't swim - in fact I am terrified of water.
Could
I could speak Danish when I was a child.
Could not
I couldn't drive a car until I had lots of lessons.
dymki.com



At some point, you have to draw the line in the sand:

Modal verbs

Obligation/prohibition

MUST Obligation. Personal opinion. You decide.
*I must study more. You must clean the car.
MUSTN'T Prohibition. Don't do it.
*You mustn't eat in the classroom.
HAVE TO: Obligation. Law or rules.
*I have to wear a uniform. (3rd person: has to)
DON'T HAVE TO: It's not necessary.
*I don't have to work on Sundays.
Don't have to means the same as **NEEDN'T**.
PAST: I had to. **FUTURE**: I will have to.

Ability and permission

ABILITY: CAN
Present: Mary **can** drive.
Past: Mary **couldn't** drive when she was 12.
Future: Mary will **be able to** drive next year.
PERMISSION MAY/MIGHT CAN COULD
Asking for permission:
May/can/could I sit here, please?
Giving permission: You **can/may** use my phone.
Refusing permission: You **can't/may not** use it.
Request: **Can/Could** you pass the water, please?

Advice

Asking for advice. SHOULD
Should is not as strong as **must** or **have to.**
Should I buy this dress? What do you think?

Giving advice. SHOULD / OUGHT TO
Affirmative: You **should** help your mother.
Affirmative: You **ought to** help your mother.
Negative: You **shouldn't** eat unhealthy food.
Negative: You **ought not to** eat unhealthy food.

Deduction

Possibilities for the future: MAY/MIGHT/COULD
It **may/might/could** rain tomorrow.
I **may/might/could** go to Paris next month. (not sure)
Possible explanations: MAY/MIGHT/COULD
Judging by her accent she **may/might/could** be American but I am not sure.
Certainty: CAN'T/COULDN'T/MUST
Her French is bad. She **can't** be French.
He drives a Ferrari. He **must** be rich.

Modals of deduction and speculation with past participle

MUST HAVE-Deduction about something that has happened. You **must have** left your book in the classroom, you haven't been anywhere else and it's not in the car.
CAN'T HAVE-Deduction about something that didn't happen in the past based on present evidence. *You **can't have seen** Mark's sister. She lives in Canada and hasn't been to England for ages.
SHOULD HAVE-Something was desirable or needed but didn't happen.*I **should have called** you but I forgot.
NEEDN'T HAVE-Opposite to 'should have'. Something not necessary was done. You **needn't have bought** more potatoes. We've got plenty.
MIGHT/MAY/COULD HAVE-Something was possible in the past but we're not sure. *I think I saw your sister at the cinema last night but I **may/might/could be** wrong because it was very dark.

The perfect infinitive with modals

MODAL VERB + PERFECT INFINITIVE ((TO) HAVE + PAST PARTICIPLE)

The perfect infinitive is often used after the modal auxiliary verbs to talk about unreal situations

COULD HAVE: I **could have bought** a nice house if I had saved enough money.
SHOULD HAVE: You **should have told** me that before but you didn't. You **shouldn't have kept** the secret.
WOULD HAVE: I **would have gone** to that private university If I had had enough money.
NEEDN'T HAVE: We **needn't have waited** for him (but we did).

Sometimes the perfect infinitive can express certainty.

*She **should have arrived** home by now. *They **will have arrived** home by now. They left so long ago.

English Outside the Box

Modals

Advice

*should (not):
- It is raining, you should take an umbrella.
- You've got a test tomorrow, you shouldn't procrastinate studying!

*ought to
-You ought to call your grandmother, it's her birthday.

*had better (not)
-You had better look both ways before you cross the street.
-You had better not start a fight with that big guy!

Notes:
*These modals are used to speak about the present & future.

*Use should for questions

*Had better (not) is strong/urgent advice: like a warning

*Use should not & had better not for negative statements

Necessity/Obligation

*(don't) have to:
-It's late, so I have to go home now.
-If you're busy, you don't have to help me

*have got to:
-This show is hilarious! You have got to see it!

*must (not):
- You must wear your seat belt while driving and in the car.
- You must not enter that area for staff only, you don't work here!

Notes:
*These modals are used to speak about the present & future.

*For the past, only use "didn't have to": to express something wasn't necessary.

*Use must for the strongest necessity/obligation, especially official signs, laws, rules, etc...

*Use must not to express prohibition, when an action is not allowed.

Ability/Inability

*can (not):
-With many years of training, I can sing very well.
-Even though I can sing, I can't dance at all.

*could (not):
-Last week I hurt my knee, but I could still run 3 miles.
-After surgery, I couldn't walk for 6 weeks.

Notes:
*Use can for ability and can not for inability in the present.

*Use could for past ability and could not for past inability/impossibility.

*"Be able to" is also used to express ability.

Future Possibility

*may (not):
-It may rain tomorrow. Look at those clouds in the sky.
-The movie got bad reviews, so it may not be funny.

*might (not):
-I might finish work and be able to go out tonight.
-I have so much work to do, I might not make it to the party.

*could:
-Lucy could win best new actress, her performance was incredible!

Notes:
*To form questions, it's common to use: "Do you think..." or "will" & "be going to" forms.

*Don't use may, might, could for questions

*Could not is NOT used for possibility, it changes the meaning to past inability/impossibility.

Volition
will
will not
shall
shall not
would

would not
should
should not

Recommendations or suggestions:
should
should not
ought to
have to

A possibility:
might,
might not,
could,
could not,

A strong possibility:
may,
may not,

An obligation:
must,
must not

An ability or inability:
can,
cannot,

Probability
must
might
can't
can
cannot
should
ought to

Permission
can
cannot
could
may
might

Advice
should

ought to
might
shall

Obligation
ought to
must
have to

Need
Need not

Had better

Be able to

From James DeRienzo:

To improve the retention of information, provide an appendix containing a qualitative analysis of action statements by role in structured format. Yes, this requires a significant amount effort to tag the data, scrub the data and convert it into structured format, but others wll find the information more useful, such as finding policy and technology gaps in their own policy. You will be able to reduce stylistic inconsistencies to improve comprehension. You will be able to extract responsibilities by Organization (Agency, Bureau, Department), Program (Mode, Site, CSP, ISP, Partner, Contractor), Operations (Wired and Wireless Networks, Subnet, VLAN, Datacenter), Administrative (Servers, Services, End User Devices, DNS, Performance Monitoring), Identity, Credential and Access Management (PKI, PIV, Remote Access), Development (Web, Database, SOA, SaaS/IaaS/PaaS Applications), Data (National Security, Classified, CUI, HVA, S-PII, H-PII, PII, PCI, HIPAA) and Security (NICE, FISMA 2.0, Risk Management Framework 2.0, Cyber Security Framework 1.1, Cyber Security Engineering, Supply Chain, IoT) roles.

From James DeRienzo:

Other areas of interest:
Some processes and entities.
Take a look at the NIST RMF categorize, select and monitor documents.
They are tagging the paragraph with a frame. You want to tag every discrete sentence and every keyphrase
Strip away all formatting, except line breaks.
Try to find patterns and quantify occurrences.
Compare against NIST SP 800-63 Series and the other Crypto documents
Look for gaps and matches.

From: CERT, Software Engineering Institute, Carnegie Mellon University

Approved algorithms:

- 533-534 and tables 3-1 and 4-1 ecPublicKey - Assuming that Curve25519 and/or Curve448 are still in the approvals process, we should make a note here that when/if they're approved, they may be used for this purpose.
- 656-657,1657 - This puts all our eggs in one basket: AES. There are plenty of secure cipher suites, such as ChaCha20/Poly1305, that just aren't approved yet, and for servers that don't have to be FIPS compliant, there's no need for this restriction.
- 841-842,1320 - Not every server needs to be FIPS compliant, and a lot of good crypto would never get a foothold if this were to always be followed.

Unnecessary weakness:

- 129,502,508,515,1241,1244-1246 - Once TLS 1.3 is widely deployed and supported, there's no reason to keep TLS 1.2 around forever until a major vulnerability is found in it, but that seems to be exactly what these lines are suggesting.
- 155-156,509-510,Appendix F - Make these statements stronger. TLS 1.0 and 1.1 shouldn't be used unless it's absolutely required for interoperability.
- 711-712 - Are there any clients that support these CCM_8 ciphers but not a more secure cipher in this list? If not, why not just ban CCM_8 outright?
- 946,1374 - Not many devices can handle an 80-bit MAC but not a full-length one anyway these days. I don't think this extension is worth the risk.
- 1316 – Why not say "shall" instead of "should" here - no need to allow some side-channel at- tacks if can be prevented.
- General - Mention that OCSP stapling "should" be performed.
- General - Certificate Transparency should be either required or much more strongly recommended.
- General - Cipher suites that don't provide forward secrecy should be forbidden.

Unnecessary banning of things that aren't necessarily insecure:

- 1080,1474 - It's possible to use Raw Public Key in a secure way if you're doing your own validation that the key is correct. Why ban it outright?
- 1549-1550 - False Start isn't as dangerous as it's made to sound like here. This should be a "should not" at most.
- 1654-1656 - The second "shall not" here is too strong. It's possible to use pre-shared keys securely, even with non-government systems. It should be a "should not" at most.

Responsibility for intermediate certificates:

- 1182-1185 - An empty hints list is a bad idea, as when users have multiple client certificates, it will often lead to them choosing the wrong one, and today's browsers make it very difficult to change this choice after it's made.

- 1477-1483 - It's always the responsibility of the entity providing their own certificate to pro- vide the intermediates along with it. Why make allowances here for broken programs?
- 1499-1509 - Clarify that it's okay to have whatever certificates sitting around for path building, as long as they're not trusted as anchors.
- 1543-1544 - Clients shouldn't give up useful functionality just because the server might be misconfigured.

Minor wording fixes:

- 1243 - Say "shall be configured to not use" rather than "shall not be configured to use", in case some programs have insecure default configurations.
- Appendix A - 3DES is entered only as if it were TDEA, leaving out that "S" stands for "Standard"

Other:

- Tables 3-1 and 4-1 - For ecPublicKey, specifying curve parameters instead of a name should be allowed.
- 535 - Sentence effectively means nothing, as even a self-signed certificate takes the role of a CA for itself.
- 1291 - DANE doesn't seem like a good replacement for revocation checking. Also, saying things "in lieu of" revocation checking goes against saying that servers "shall" do it.
- 1327 - Saying "not needed" here is too broad, as a lot of TLS extensions aren't strictly necessary but are offering some large benefit. Perhaps "not serving a useful purpose" would be bet- ter.
- General - The "post_handshake_auth" extension should be supported as a replacement for one of the common uses of renegotiation in TLS 1.3.
- General - Encrypted SNI should be mentioned in appendix E.

From: ETSI Enterprise Transport Security (ETS) Specification Rapporteur

16 November 2018

Charles H Romine
Director, Information Technology Laboratory National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: **Comments:**
SP 800-52 Rev. 2 (DRAFT), Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (2nd Draft)

Dear Dr. Romine:

I am filing comments in this NIST public proceeding on behalf of the Enterprise TLS standard development group within the ETSI Cybersecurity Technical Committee (TC CYBER) as the Group's Rapporteur responsible for the work.

In addition to the comments, attachments include the relevant published Technical Specification, preceding Technical Report, and links to a variety of materials including a related webinar, Hot Middlebox workshop, Hackathon, repository of the standards team's materials, public announcement, and a presentation by UK's NCSC at the May 2018 U.S. government, Integrated Adaptive Cyber Defense (IACD) workshop.

We also understand that U.S. Bank has briefed your Chief Cybersecurity Advisor, Donna Dodson, on the matter.

Respectfully submitted,

/s/

Anthony M. Rutkowski
ETSI TC CYBER MSP Part 3 Rapporteur Yaana Technologies LLC
542 Gibraltar Dr
Milpitas CA 95035
tel: +1 703.999.8270 mailto:tony@yaana.com

cc: Donna Dodson, Chief Cybersecurity Advisor

Attachments:

ETSI TR 103421, *Network Gateway Cyber Defence*

ETSI TS 103 523-3, *Middlebox Security Protocol; Part 3: Profile for enterprise network and data centre access control*

Comments

SP 800-52 Rev. 2 (DRAFT), Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (2nd Draft)

Summary:

ETSI as a global standards body has been engaged for the past three years in developing Transport Layer Security implementation technical standards similar to those published in the draft, but tailored to meet specific use cases of considerable importance to industry and public users. The work entailed considerable outreach to and involvement of industry and government organizations and academic institutes worldwide, as well as research into best-of-breed, functional solutions to meet the most important use cases.

The most important and urgent use case was that of enterprise networks and data centers operating in closed environments similar to those of Federal Agencies, government contractors, and regulated industries. The platform advanced was one which was already developed by U.S. Bank and further perfected over a six-month period of intensive team work. The resulting platform was formally adopted by ETSI and published in October 2018 as Technical Standard 103523-3, Middlebox Security Protocol; Part 3: Profile for enterprise network and data centre access control. It is also known as eTLS (Enterprise TLS). NetScout Systems also contributed running code to demonstrate the functionality and effectiveness of the specification.

A publicized ETSI webinar was subsequently held demonstrating the use of eTLS in practice by U.S. Bank. The presentations notably included a session on how the use of TLS 1.3 implementations suggested in the draft SP 800-52 Rev. 2 Guidelines would eliminate the ability of enterprise security experts to see cybersecurity threats by an adversary. The potential for significant damaging information exfiltration and placement of malware were apparent. These harms are in addition to the inability of private and government enterprise networks to meet multiple regulatory obligations that include auditing of their own communication transactions.

NIST is strongly urged in this proceeding to explicitly consider: 1) actual enterprise network and data center use cases, 2) the significant harms potentially resulting from NIST proposed TLS 1.3 implementations, and 3) alternatives such as eTLS and any others found similarly effective. It is realized that such action might entail additional delay in finalizing the Special Publication. However, the enormity of the potential harms and costs involved to industry and government systems, as well as an implementation date that is already in 2024, calls for more considered analysis and action.

1. Background

ETSI and its precursors for decades - both for its own standards as well as for GSM radio – have been engaged in a broad array of cryptographic developments that date back to their earliest implementations for communication and data networks in the 1970s. Examples of continued cryptographic activities today include the ETSI committee SAGE (Security Algorithms Group of Experts) which is responsible for creating reports (containing confidential specifications) in the area of cryptographic algorithms and protocols specific to fraud prevention/unauthorized access to public/private telecommunications networks and user data privacy. The Cyber Security Technical Committee's Working Group for Quantum-Safe Cryptography is also the leading global collaborative industry standards mechanism for related study and specifications.

In early 2016, with the exponentially increasing deployment malware via encrypted traffic paths, TC CYBER started a work item to exhaustively examine every dimension of the challenges and ecosystem to prepare a Technical Report making several recommendations. Published in early 2017, ETSI TR 103421, Network Gateway Cyber Defence, included an ambitious effort to develop an extensible set of specifications under a common framework, subsequently named the Middlebox Security Protocol. The Report also recommended to the European Union that these platforms for addressing cyberthreats via encrypted traffic would be essential for effective cyber security.

Beginning in 2017, a team of experts began to pursue the development of an initial four-part specification for effectively managing - in a secure and trusted manner - how physical and virtual middleboxes processing encrypted traffic are discovered and their observability of traffic tuned. The name Middlebox Security Protocol (MSP) was given to the ensemble of specifications, with the ability to extend the specification parts to deal with any kind of encryption platform.

The work concentrated on three subtasks: Part 1) producing a generic requirements specification, Part 2) an implementation profile for TLS 1.2 middlebox processing instantiations in network transport paths, and Part 3) an implementation profile for TLS 1.3 within closed enterprise networks and data centers. After extensive surveys of work in other standards bodies, and within known R&D institutes, the group settled on the joint U.S.- European R&D collaboration that produced a platform commonly known as mcTLS for Part 2. For Part 3, the group settled on a platform developed by U.S. Bank that was designated eTLS (Enterprise TLS).

The work proceeded using the ETSI standards development process that relied on a combination of Face-to-Face plenary meetings at 4 month periods, and virtual meetings at 2-4 week intervals. They were enhanced with constant surveys of the literature, outreach to the R&D community, liaisons on all interested standards bodies including 3GPP (5G security), GSMA, IEEE, IETF, ITU-T, and the NFV ISG.

The outreach also included open venues of the U.S. national security community – notably a presentation at the Integrated Adaptive Cyber Defense (IACD) workshop held at the Johns Hopkins University Applied Physics Laboratory in May 2018. A Hot Middlebox workshop was held in conjunction with ETSI's annual Security Week in June 2018, along with a related Middlebox Security Protocol Hackathon. The draft standards were also made available publicly to all interested parties, and became the basis for work at Microsoft and INRIA R&D centers which identified vulnerabilities that were subsequently mitigated.

The specification Part which had immediate urgency was eTLS because of the heightened concerns of the financial services industry about their inability to perform essential cybersecurity functions and to meet regulatory obligations imposed on the industry. After U.S. Bank initially vetted the platform in the IETF in 2017, its TLS group with its management approval, made the decision to bar enterprise network and data center security use cases and suggested the work be done elsewhere. The ETSI TC CYBER committee agreed to assume responsibility for the work with the active involvement of U.S. Bank and other supporting organizations such as NetScout Systems which helped perfect the protocol and develop running code for demonstrating functionality.

After multiple published iterations, the resulting eTLS platform was formally adopted by ETSI and published in October 2018 as Technical Standard 103523-3, Middlebox Security Protocol; Part 3: Profile for enterprise network and data centre access control. ETSI plans to also use its PlugTest interoperability center as well as feedback on implementation of the Specification from users to evolve and perfect it as needed. One related work item is already underway, CYBER DTS/CYBER-0040 (TS 103651), Critical Security Controls for MSP middlebox defence.

Following adoption, a publicized ETSI webinar was held to demonstrate the use of eTLS in practice by U.S. Bank. The presentations notably included a session on how the use of TLS 1.3 implementations suggested in NIST's draft SP 800-52 Rev. 2 Guidelines would eliminate the ability of enterprise security experts to see cybersecurity threats by an adversary. The potential for significant damaging information exfiltration and placement of malware were apparent. These harms are in addition to the inability of private and government enterprise networks to meet multiple regulatory obligations that include auditing of their own communication transactions.

2. NIST's SP 800-52 Rev 2 and Recommended Action

The appearance of the subject NIST draft in October 2018 on the agency's website came as both a surprise and mystery to those in industry venues working on the significant challenges posed by the IETF's Pervasive Encryption initiatives of which TLS 1.3 is the centerpiece. Those multiple IETF initiatives - although seen by some parties as useful for improving a theoretical enhancement of encryption capabilities between arbitrary network endpoints - are causing considerable concern bordering on havoc within industry network provider communities as security capabilities go dark and network management systems fail.

The NIST draft notes that its intended purpose is a "...guideline for the cost-effective security and privacy of other than national security-related information in federal information systems." However, the stated purpose of the IETF TLS 1.3 protocol is to create an unobservable information/code transport capability between any arbitrary TCP/IP endpoint worldwide and users within an organization's network or data center. That IETF use case seems plainly antithetical to the secure operation of federal information systems.

Deployment of TLS 1.3 as described in the NIST draft appears to introduce a rather significant, large-scale vulnerability by design into federal information systems that would ironically be additionally costly for system operators to manage and mitigate.

Indeed, at a national policy level, so-called “pervasive encryption initiatives” such at TLS 1.3 raise significant concerns that are amplified almost every week by new revelations of foreign adversaries using the platforms to exfiltrate commercial data, classified information, and manipulation of U.S. elections. See also, Symantec’s White Paper and IETF discussion group detailing how implanting malware on host servers using encrypted tunnels has become a massive cybersecurity threat. See
https://www.ietf.org/mail-archive/web/patient/current/pdfoDl1SNF3iS.pdf

One of the significant inadequacies of NIST’s guideline process here is that unlike mainstream industry standards bodies, there is no use case process, nor are use cases even discussed. The omission is especially significant where the federal system use cases are not only not apparent, but where the proffered specification requirement for TLS 1.3 use is seemingly antithetical to the interests of federal agencies.

NIST is strongly urged in this proceeding to take four actions:
1) engage in a process of considering actual enterprise network and data center use cases,

2) engage in Red Team exercises that consider the significant harms potentially resulting from the NIST proposed TLS 1.3 implementations in federal networks and data centers,

3) work closely with operators of enterprise networks and data centers, as well as industry standards bodies such as ETSI TC CYBER who are addressing the same needs on a large scale, and

4) move forward with alternative solutions that better fit federal systems needs such as eTLS and any others found similarly effective

It is realized that such action might entail additional delay in finalizing the Special Publication. However, the enormity of the potential harms and costs incurred by government systems and industry contractors, as well as an implementation date that is already in 2024, calls for more considered analysis and action.

Links to Additional Materials

- ETSI releases standards for enterprise security and data centre management, Sophia Antipolis, 5 November 2018, https://www.etsi.org/news-events/news/1358-2018-11-press-etsi-releases-standards-for-enterprise-security-and-data-centre-management

- Webinar - Middlebox Security Protocol explained, 15 Oct 2018, https://www.etsi.org/news-events/events/1338-2018-10-webinar-middlebox-security- protocol-explained

- Hot Topics in Middlebox Security, Tuesday 12 June 2018, https://www.etsi.org/etsi-security-week-2018/middlebox-security

- Middlebox Hackathon, Sophia Antipolis, Tuesday 12 June 2018, https://www.etsi.org/etsi-security-week-2018/middlebox-hackathon

- NCSC presentation, Integrated Adaptive Cyber Defense (IACD) workshop, Johns Hopkins University Applied Physics Laboratory, May 2018, https://www.iacdautomate.org/may-2018-integrated-cyber

- Repository of the standards team's materials, https://portal.etsi.org/tb.aspx?tbid=824&SubTB=824

From: Boeing

Comments

- When enabling FIPS compliance on some types of devices and services, it defaults to TLS 1.0 and changing it requires manual intervention. This could potentially cause a great deal of disruptions if newer versions of TLS are required, or if TLS 1.0 is deprecated.

Questions

- Is there an estimated time for when versions prior to TLS 1.2 will be depreciated?
- Is there a way to disable 0-RTT and/or the Pre-Shared Key extension in TLS 1.3 to improve security?
    - If yes, is there a way to remotely audit that is actually disabled?

From: NIH

#	Page #	Line # (Req'd)	Comment (Include rationale for comment)	Suggested change
0	-	-	The NIH appreciated the opportunity to review the guidance for the Final Public Draft NIST SP 800-52 Rev 2,"Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations." This document is very helpful to ensure that a security and privacy review occur before publication.	-
1	N/A	N/A	Token Binding TLS extension is not discussed (RFC 8471, RFC 8472, RFC 8473, etc.). As a tool for increasing security of TLS sessions with and between Federal systems Token Binding offers great opportunity.	Suggest adding text specifying how Token Binding should be implemented if an agency decides to adopt it.
2	54	1762	Use of TLS 1.0 or 1.1 represent significant risk to Federal systems. As such a requirement for tracking, remediating, or mitigating that risk should be strongly recommended.	Where TLS 1.0 or 1.1 are selected for use a POA&M should be created to track the risk and eventually address it.
3	54	1780	DAP is one suggested tool, but encouraging the logging of the information required to determine whether TLS 1.0 or 1.1 are needed is recommended.	Include guidance on ensuring that servers are configured to log the appropriate TLS usage data.

From: NSA

Comments on Draft (2nd) NIST Special Publication 800-52 Revision 2					
#	Location			Comment	Proposed Resolution
	Page	Section	Paragraph/Line		
1	2	1.1	Paragraph 3 Line 293	Missing “of” between “SHA-2 family” and “algorithms”.	Add text to make line 293 read “the area of hash functions, with the ability to use or specify the SHA-2 family of algorithms for”
2	4	2.1	Paragraph 3 Lines 381-382	As written it’s not clear the extent to which server and client authentication are orthogonal.	Replace the text with “The handshake protocol is used to optionally exchange X.509 public-key certificates to authenticate the server to the client and/or the client to the server.”
3	8	3.1	Paragraph 1	Is there any plan to move TLS 1.1 capability to shall not for government only applications? If so, this is a good place to mention it. If not, why not?	
4	8	3.1	Paragraph 3	As written it appears that TLS 1.2 will remain acceptable long-term. NIST should clarify their plans (if any) for deprecating TLS 1.2.	
5	8	3.0/3.1	Section 3.0 Section 3.1 Paragraph 4	NIST shouldn’t be listing specific implementation issues to avoid as shall not statements. It would be better to require (as a shall statement) that server implementations are correct, with possibly a separate list of common implementation problems to keep an eye out for.	Add text to Section 3.0 saying “Federal agencies shall procure TLS server implementations that correctly implement all supported protocol versions.”
6	9	3.2	Paragraph 2 Line 528	What does “expected to be configured with ECDSA or RSA certificates...” mean? Does it mean that servers shouldn’t use (EC)DH or DSA certificates? Are (EC)DH or DSA certificates forbidden for externally facing severs?	Clarify the text.
7	14/15	3.3.1	Paragraph 3	This paragraph can be simplified by removing discussion of cipher suite ordering on both the client and server sides. Having that content doesn’t add anything helpful here.	Replace the paragraph with “When negotiating a cipher suite, the client sends a handshake message with a list of cipher suites it will accept. The server chooses from the list

					and sends a handshake message back indicating which cipher suite to use. The server may choose any of the cipher suites proposed by the client. There is no guarantee that the negotiation will settle on the strongest common suite. If no cipher suites are common to the client and server the connection is aborted.
8	15	3.3.1	Paragraph 6	Does NIST have a timeline in mind for deprecating RSA key transport? Will this deprecation include prohibitions on RSA key transport for servers running TLS versions 1.0 or 1.1?	To the extent possible, give the relevant information here or point to where it can be found.
9	15	3.3.1	Paragraph 7	Will NIST also deprecate static DH and ECDH?	If not, mention that in this paragraph. With respect to TLS it seems better to deprecate all non-forward secure cipher suites, not just RSA key transport.
10	19/20	3.3.2	Paragraph 2	This would be a good place to require correct implementations.	See Proposed Resolution for Comment 5.
11	20	3.3.2	Paragraph 3 Line 822	Why is constant-time decryption a should?	Unless NIST is aware of a situation where constant-time decryption is not desirable, or not possible, change should to shall.
12	20	3.3.2	Paragraph 4	Same as Comment 5. Note that this does not apply to paragraphs 2 or 3, since those paragraphs describe behaviors that correct servers can have, but that should be avoided.	Same as Comment 5.
13	29	3.5.1	Paragraph 5	It's not clear what "applications" are referenced here.	Change to say "The server shall be able to provide the client certificate, and the certificate policies for which the client certification path is valid, to consuming applications in order to support access control decisions."
14	29	3.5.2	Paragraph 2 Lines 1150-1151	By definition the server trusts any trust anchor with which it is configured. I think the intent here is to say that the server should only be configured with	Change to say "The server shall be configured only with trust anchors that the system owner trusts..."

				trust anchors that the system owner trusts.	
15	29	3.5.2	Paragraph 2 Lines 1155-1156	There may be more than one enterprise and/or PKI service provider trust anchor required.	Change to say “Some specific enterprise and/or PKI service trust anchors may need to be added.”
16	29	3.5.2	Paragraphs 2 and 4	There is some duplication of content here.	Remove the last sentence from paragraph 4, as it’s already covered by the first sentence of paragraph 2.
17	32	4	Paragraph 2	As on the server side, NIST should require correct client implementations.	Add text to the effect of “Federal agencies shall procure TLS client implementations that correctly implement all supported TLS protocol version.”
18	32	4.1	Paragraph 1 Lines 1245-1246	Does NIST intend TLS 1.2 and 1.3 to coexist indefinitely? Or is there a deprecation plan for TLS 1.2?	In either case, mention that here. It’s helpful information for system owners.
19	32	4.2.1	Paragraph 1	It’s unclear whether the certificate profile given in this section is required or not. On the one hand it says “...the client shall be configured with a certificate that adheres to the recommendations presented in this section”. But it also says “In the absence of an agency-specific client certificate profile, this profile should be used for client certificates.”	Make clear what parts of the section are shall requirements and what parts are should recommendations.
20	35	4.3.1	Paragraph 2	Is it intentional that servers shall not be configured to use cipher suites other than those listed in Section 3.3.1, Appendix C, or Appendix D, and that clients should not be configured to use other cipher suites?	If the two are meant to be different, add a rationale for the difference.
21	41	4.5.1	Paragraph 2	Is it NISTs intent that the client must either perform name constraint checking or use the features discussed in Appendix E.1?	The language here should be clarified in either direction. Either the should applies to doing at least one of name constraint checking or using

					one or more of the features discussed in Appendix E.1; or the “As an alternative” really means federal agencies shall do at least one of name constraint checking or one or more of the features discussed in Appendix E.1.