

A decorative network diagram in the top-left corner, featuring a complex web of nodes and edges. Some nodes are highlighted with blue circles, and others with blue dots. The diagram is rendered in a light gray color.

Writing Security Considerations Tutorial

A decorative network diagram in the bottom-right corner, similar to the one in the top-left, featuring a complex web of nodes and edges. Some nodes are highlighted with blue circles, and others with blue dots. The diagram is rendered in a light gray color.

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. Some nodes are represented by solid circles, while others are open circles with concentric rings. The lines connecting them are thin and grey.

1.

Motivation

Why do we write Security Considerations sections?



“


Security is relevant to all protocols, not just those protocols coming from the Security area.

Security Is Important To All Protocols

- ◎ It's obvious why we need protocols like IP, TCP and TLS to be secure.
 - Other protocols depend on them for security properties.
- ◎ That is not enough.
- ◎ Security issues in higher level protocols can compromise the system just as well as issues in TLS. TLS does not solve all your problems.
- ◎ It's mostly about implementation and deployment issues.



Security Is Important To All Protocols

- ◎ The security depends not just on using good crypto, but on dispensing identities and credentials and verifying them.
 - ◎ Example: You are authenticating your nodes with certificates. Great! However:
 - How do you issue certificates?
 - How does the CA verify the identify?
 - How are private keys secured?
 - When one node connects to another, how does it validate the certificate?
How does it validate the name in the certificate?
- 

More Motivation

- ◎ SecDir review is part of the document publication process.
 - All documents go through it.
- ◎ Security Area Directors as well as other ADs will BLOCK or DISCUSS on ignored SecDir review.
- ◎ SecDir reviewers check that the Security Considerations section addresses all that it should.
- ◎ Security Considerations – it's not just a good idea, it's the law.



“

9. Security Considerations Section

All RFCs must contain a section near the end of the document that discusses the security considerations of the protocol or procedures that are the main topic of the RFC.

-- From RFC 2223

Write Them Early

- ◎ Don't leave writing the Security Considerations to the end of the process.
- ◎ Writing down the Security Considerations can help you find issues with your document.
- ◎ SecDir reviews – like any other review – can lead to document changes. If you think there might be an issue, ask for early review.

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by circles of varying sizes, some with solid centers and others with dashed outlines. The lines are thin and gray, connecting the nodes in a non-linear fashion.

2. **History**

How did we get here?

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It shows a cluster of nodes connected by lines, with some nodes having solid centers and others having dashed outlines. The lines are thin and gray.

History

- ◎ Once, RFCs did not have security considerations, and people did not think about security when designing protocols and systems.
- ◎ RFC 2223 required a security considerations section in 1997.
- ◎ RFC 3552 from 2003 had guidance on writing the section and a definition of the Internet Threat Model.
- ◎ An attempt to update RFC 3552 three years ago failed.

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by circles of varying sizes, some with solid centers and others with dashed outlines. The lines are thin and gray, creating a mesh-like structure that extends across the top-left portion of the slide.

3.

The Internet Threat Model

This is your default setting for a threat model

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It shows a cluster of interconnected nodes and lines, with nodes represented by circles of different sizes and line styles (solid and dashed). The lines are thin and gray, forming a network structure that occupies the bottom-right area of the slide.

The Internet Threat Model

- ◎ The Internet Threat Model is described in RFC 3552.
- ◎ An attacker can modify, drop, or spoof any protocol message.
- ◎ Also consider:
 - Off- vs. on-path attackers as in RFC 7430.
A sufficiently powerful off-path attacker can become on-path through DNS poisoning, BGP hijacking, etc.
 - Privacy considerations as in RFC 6973.
 - Pervasive monitoring as in RFC 7258.
 - Trust. Always consider who you trust to do what.



Questions to ask, especially in SEC area



Confidentiality:



Are the protocol messages kept secret from unintended listeners?



Data Integrity:



Is there any chance of protocol messages being tampered or altered by attackers?



Peer Entity Authentication:



Are the messages really from the expected peers, not from attackers?



Are the messages really sent to the expected peers? Not to attackers?



the Security Considerations section needs to explain:

1. which attacks are out of scope (and why!)

2. which attacks are in-scope

2.1 and the protocol is susceptible to

2.2 and the protocol protects against



Attacks to be considered



Targets:

- Even walled-In systems, such as routers & switches in cages, are susceptible to those Internet threats, especially when they have ports facing external .
- More vulnerable targets: Shared media, such as Ethernet, WIFI (e.g. 802.11)



Passive Attacks (reads packets off the network but does not write them):

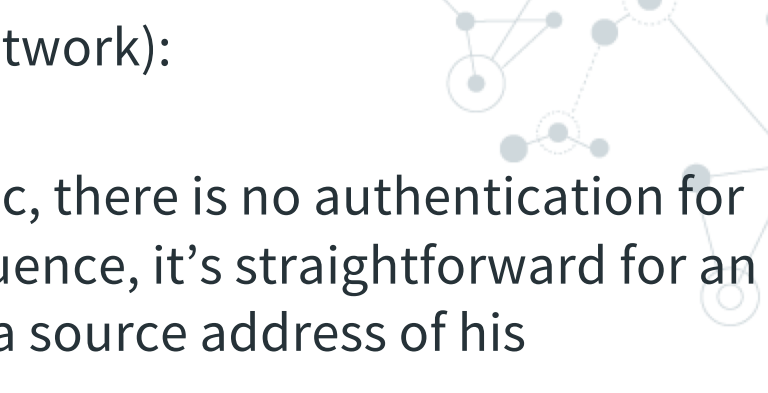
- sniffing some inherently private data off of the wire
- Password Sniffing
- Offline Cryptographic Attacks: the attacker recovers data which has been processed using the victim's secret key and then mounts a cryptanalytic attack on that key




Common Issues:

- Shared Keys, Key Distribution Centers;
- Certificates
- Downgrade attacks
- Denial of Service attacks
- Firewalls: the most serious security threats is from insiders, not outsiders!

Attacks to be considered

- 
- **Active Attacks** (writing data to the network):
 - **SPOOFING ATTACK:**

E.g. When IP is used without IPsec, there is no authentication for the sender address. As a consequence, it's straightforward for an attacker to create a packet with a source address of his choosing.
 - **Replay attacks**
 - **Message Insertion, modification or deletion**

E.g. If IPsec ESP is used without any MAC then it is possible for the attacker to read traffic encrypted for a victim on the same machine. The attacker attaches an IP header corresponding to a port he controls onto the encrypted IP packet. When the packet is received by the host it will automatically be decrypted and forwarded to the attacker's port.
 - **Man-In-The-Middle attacks**
- 

A decorative background graphic consisting of a network of nodes and lines. The nodes are represented by small circles, some of which are solid grey and others are hollow with a grey outline. They are interconnected by thin, light grey lines, forming a complex, web-like structure that spans the entire slide. The density of the network is higher on the left side and tapers off towards the right.


4.

What Goes in the Security Considerations Section?

Security-related stuff that is new
to this document.

About the Threat Environment

A decorative network diagram in the top right corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in blue and others in grey.

- ◎ A TCP client that is anywhere on the Internet, including behind a NAT talking to a server in the cloud is the Internet Threat Model.
 - ◎ Any other environment that changes the attack surface should be called out and described in the Security Considerations section.
- 
- A decorative network diagram in the bottom left corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in blue and others in grey.

About the Threat Environment

This protocol variation inherits all the security properties of regular ESP as described in [RFC4303].

- ◎ This one's from draft-xu-tictoc-security-for-synchronization-02
- ◎ It's about protecting IEEE-1588
- ◎ IEEE-1588 requires consistent latency down to sub-microsecond or sub-nanosecond jitter.
- ◎ It can't run through a router, because those introduce jitter.
- ◎ This is not the Internet.

In-Scope and Out-of-Scope Threats


- ◎ It's fine for a document to leave some security aspects, especially the preventions of certain attacks out of scope.
- ◎ The document should call this out and say how those threats are mitigated.

◎ Example:

Protecting the endpoint against flooding attacks is out-of-scope for this document. It should be mitigated with normal network management procedures.



Security of the Authentication

- ◎ How is the authentication protected?
 - ◎ How are credentials generated?
 - ◎ How are credentials dispersed?
 - ◎ How are credentials and verifiers protected?
 - ◎ This is hardly ever obvious
 - ◎ Even the world wide web has a whole other SDO called the CA/Browser Forum for regulating credentials management.
- 

Residual Risk

- ◎ If the security mechanisms in the document do not handle all risks that you are aware of, spell this out.
- ◎ This is from RFC 5246 (TLS 1.2):
 - Too bad it wasn't in the Security Considerations section.

This leaves a small timing channel, since MAC performance depends to some extent on the size of the data fragment, but it is not believed to be large enough to be exploitable, due to the large block size of existing MACs and the small size of the timing signal.

Risks from Foreseen Mis-application or Mis-deployment

When using ECDSA with SHAKEs, the ECDSA curve order SHOULD be chosen in line with the SHAKE output length. NIST has defined appropriate use of the hash functions in terms of the algorithm strengths and expected time frames for secure use in Special Publications (SPs) [SP800-78-4] and [SP800-107]. These documents can be used as guides to choose appropriate key sizes for various security scenarios. In the context of this document `id-ecdsa-with-shake128` is RECOMMENDED for curves with group order of 256-bits. `id-ecdsa-with-shake256` is RECOMMENDED for curves with group order of 384-bits or more.

- ◎ This is from the SHAKEs document. Note that combining SHAKEs with signatures is not part of this document.
- ◎ If you can anticipate people implementing or deploying in an insecure fashion, call it out. In this case, people might use the new hash function with older, smaller curves.



Call Out Information That is Sent Out

- ◎ This is especially important for extensions.
- ◎ If your extension is sending information that the base protocol did not, call this out.
- ◎ We'll see a good example in the **Pitfalls** part of this presentation.



5.

What Does Not Go in the Security Considerations Section



RFC 2119 Language

- ◎ Requirement language goes in the main part of the document.
- ◎ Wrong:
 - The uniqString value mentioned in section 4 MUST be 256 high quality random bits.
 - The RSA key in section 4.1 MUST be at least 3072 bits in length and MUST be chosen using one of the approved methods described in [SP800-56B]
- ◎ Right:
 - Section 4 requires uniqString to be 256 high quality random bits to avoid birthday attacks.
 - The key length and generation requirements in section 4.1 represent the current state of the art assuming an attacker not equipped with a large-scale quantum computer.

Motivation

- ◎ Remember the IEEE-1588 draft? Here's the rest of the security considerations:

This document describes the modification or extension for the WESP for the additional application. The approach described in this document requires the ESP endpoints to be modified to support the new protocol. It allows the ESP receiver or intermediate node not only to distinguish encrypted and unencrypted traffic deterministically, but also identify whether the encrypted packets are the common packets or the time packets by a simpler implementation for the transport node.

- ◎ We see this a lot. That is what the Introduction is for, not the Security Considerations.

Random Musings

© From draft-ietf-lamps-pkix-08:

The SHAKEs are deterministic functions. Like any other deterministic function, executing multiple times with the same input will produce the same output. Therefore, users should not expect unrelated outputs (with the same or different output lengths) from running a SHAKE function with the same input multiple times. The shorter of any two outputs produced from a SHAKE with the same input is a prefix of the longer one. It is a similar situation as truncating a 512-bit output of SHA-512 by taking its 256 left-most bits. These 256 left-most bits are a prefix of the 512-bit output.

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. Some nodes are represented by solid grey circles, while others are open circles with a smaller solid circle inside. The lines connecting them are thin and grey, creating a web-like structure that extends from the top-left towards the center.

6. **Pitfalls**

Learn from the mistakes of others

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It shows a cluster of nodes connected by lines, with some nodes being solid grey circles and others being open circles with a smaller solid circle inside. The lines are thin and grey, forming a web-like pattern that extends from the bottom-right towards the center.

Security Considerations by Reference

The mapping extensions described in this document do not provide any security services beyond those described by EPP [RFC5730], the EPP domain name mapping [RFC5731], and protocol layers used by EPP. The security considerations described in these other specifications apply to this specification as well.

- ◎ Well, if nothing's changed, why did you write draft-ietf-regext-epp-fees?
- ◎ The draft adds financial information to a registration protocol that did not have it before.
- ◎ Something has definitely changed.
- ◎ Claims that X has the same security properties as Y need to be defensible.
- ◎ Don't do >1 level of indirection.

Security Considerations by Reference

Procedures and protocol extensions defined in this document do not affect the BGP security model. See the 'Security Considerations' section of [RFC4271] for a discussion of BGP security. Also refer to [RFC4272] and [RFC6952] for analysis of security issues for BGP.

© This is draft-ietf-idr-te-pm-bgp-13. RFC 4271 is BGP.

The TLVs introduced in this document are used to propagate IGP defined information ([RFC7810] and [RFC7471].) These TLVs represent the state and resources availability of the IGP link. The IGP instances originating these TLVs are assumed to have all the required security and authentication mechanism (as described in [RFC7810] and [RFC7471]) in order to prevent any security issue when propagating the TLVs into BGP-LS.

© RFC 7810 and 7471 describe sending traffic engineering (TE) information in IS-IS and OSPF respectively.

Security Considerations by Reference

- ◎ But it's not all the same, because BGP is not the same as IS-IS and OSPF. You can't just reference those documents.
 - IS-IS and OSPF run on corporate networks all owned by the same entity. BGP runs on the Internet with somebody else's router.
- ◎ It is not obvious that sending TE information on BGP is fine just because it's fine to do it on OSPF and IS-IS.

Security In Another Layer

- ◎ This is the delegation of security to another protocol:
 - Just use IPsec.
 - Just use TLS.
 - Just use HTTPS
 - Just use IPsec with I2NSF.
 - Just use TLS with ACME.
- ◎ Each of those requires a bunch of infrastructure to deploy. They are not trivial.
- ◎ Even the Web PKI is only trivial to use because a lot of companies have done a lot of heavy lifting for you.
- ◎ If you tell people to use a security layer – tell them how.

Security In Another Layer

- ◎ Who and how do you provide credentials?
 - Who gets a credential?
 - How do you authenticate them when granting them a credential?
- ◎ How do you validate a certificate?
- ◎ Who is authorized to do what?
 - A common mistake is the “anyone with a certificate can do anything” model.
 - If you want to trust any certificate holder in a corporate LDAP environment, remember that the printer has a certificate.

More Specific Pitfalls

- ◎ YANG models

<https://trac.ietf.org/trac/ops/wiki/yang-security-guidelines>

- ◎ URIs (using them to locate resources)

Section 7 of RFC 3986

- ◎ Time and replay

- ◎ Broken constraints

Attackers are not bound by RFCs

- ◎ Cryptographic Agility

- ◎ More at [Typical SEC Area Issues](#).

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by circles of varying sizes, some with solid centers and others with dashed outlines. The lines are thin and gray, creating a dense, organic structure that resembles a molecular or biological network.

7. Questions?

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It features a complex web of interconnected nodes and lines. The nodes are represented by circles of varying sizes, some with solid centers and others with dashed outlines. The lines are thin and gray, creating a dense, organic structure that resembles a molecular or biological network.