WHITE PAPER

The Security Engineer's Guidebook to TLS 1.3

The State of SSL/TLS Decryption

A key to success is knowing what you are getting into before you embark on a new journey. Data encryption/decryption is one such example. The Internet Engineering Task Force (IETF) released a new version of its encryption protocol in the last half of 2018. Is this standard something you should adopt immediately?

According to a study by Enterprise Management Associates (EMA), 73% of respondents plan to begin the conversion to TLS 1.3 before mid-year 2019.[1] For many enterprises, especially in the financial industry, this will result in a fundamental change to their security architectures. Any organization that is currently using secure socket layer (SSL) or Transport Layer Security (TLS) for passive SSL decryption will need to change their architecture or lose the ability for deep packet inspection (DPI), threat hunting, data loss prevention (DLP), and the use of intrusion detection systems (IDS)

Any organization that is currently using secure socket layer (SSL) or Transport Layer Security (TLS) for passive SSL decryption will need to change their architecture.

1 Report Summary: TLS 1.3 Adoption in The Enterprise, Enterprise Management Associates. February 2019.

KEYSIGHT TECHNOLOGIES

This white paper addresses three important topics and the full ramifications of how TLS 1.3 data decryption will affect you.

1. TLS 1.3 brings new changes
2. Active testing of TLS/SSL validates security solutions
3. Ongoing monitoring strengthens your encryption strategy

TLS 1.3 Brings New Changes

Encryption is a way to secure connections between web browsers and servers. TLS is the new term for SSL, but the two terms are interchangeable. The IETF approved the latest version of the TLS 1.3 encryption standard (RFC 8446) in August 2018. It is now starting to make its way into corporate networks.

Figure 1 is a summary of the changes to the SSL encryption standard over time.

Version	Released	Deprecated
SSSL1.0	1995 (had flaw)	Immediately
SSSL2.0	1995	2011
SSSL3.0	1996	2015
TLS1.0	1999	Upcoming
TLS1.1	2006	Upcoming
TLS1.2	2008	
TLS1.3	2018	

Figure 1. SSL encryption — a quick overview.

The goal of TLS 1.3 is to fix gaps in the SSL standard and generate the following improvements:

- Improve privacy
- Remove older, less-secure algorithms
- Decrease setup latency

The goal of TLS 1.3 is to fix gaps in the SSL standard and generate the following improvements:

- Improve privacy
- Remove older, less-secure algorithms
- Decrease setup latency

According to the EMA study[2], most individuals involved with security have similar improvement expectations:

- Data security – 73%
- Privacy – 67%
- User experience – 55%

The fundamental question is whether or not these expectations are accurate. A more in-depth analysis of these expectations, will provide the information you need to make decisions about data privacy, security, and visibility within your organization.

Adoption of the new TLS 1.3 security architecture will introduce significant changes for many IT teams, including:

- Data visibility will become a challenge when performing encryption, as many security devices and other tools cannot inspect encrypted data
- Use of encryption will force new programmatic changes within the network
- How and where data inspection occurs will change
- Passive SSL decryption will no longer work

The following architecture changes are necessary to implement TLS1.3 successfully:

- The use of ephemeral keys
- A man-in-the-middle (MITM) architecture
- Elimination of passive SSL decryption
- Reconfiguration of equipment for different key exchange mechanisms and a reduced cipher list

2 Report Summary: TLS 1.3 Adoption in The Enterprise, Enterprise Management Associates. February 2019.

Use of ephemeral keys means that a new key is generated every time encrypted data. Previously, a static key method was an option that could last for hours or days. This item closes the attack vector of stealing keys and using them for a few hours afterward to decrypt network data. Therefore, one of the key components driving the improved security expectation cited earlier is that ephemeral keys are now mandatory.

Ephemeral keys also mean that a MITM approach is now mandatory. The resulting outcome is that passive monitoring is eliminated—you must use active monitoring. This one change will affect many IT engineers because another data point from the survey showed that currently over one-quarter of enterprise IT solutions decrypt data for out-of-band monitoring; meaning they are currently using passive decryption.[3] Since this is no longer allowed within the TLS 1.3 standard, security and operations personnel will need to change this process—the use of DLPs, IDSs, and DPI will all change.

Security Architecture Changes and Options

Several security architectures support TLS 1.3, and some are much better than others.

Over one-quarter of enterprise IT solutions decrypt data for out-of-band monitoring, meaning they are currently using passive decryption.

Architecture option 1

One process change is to support inline data monitoring and decryption. This allows you to perform MITM decryption. Figure 2 illustrates the new monitoring/decryption architecture with the removal of out-of-band decryption.

An easy way to enable active decryption and inline monitoring is to use a network packet broker (NPB). With the deployment of an NPB, it is possible to connect an SSL decryption appliance to handle high-volume data decryption. Decrypted data is relayed back to the NPB and then gets forwarded to the correct security appliance for analysis.

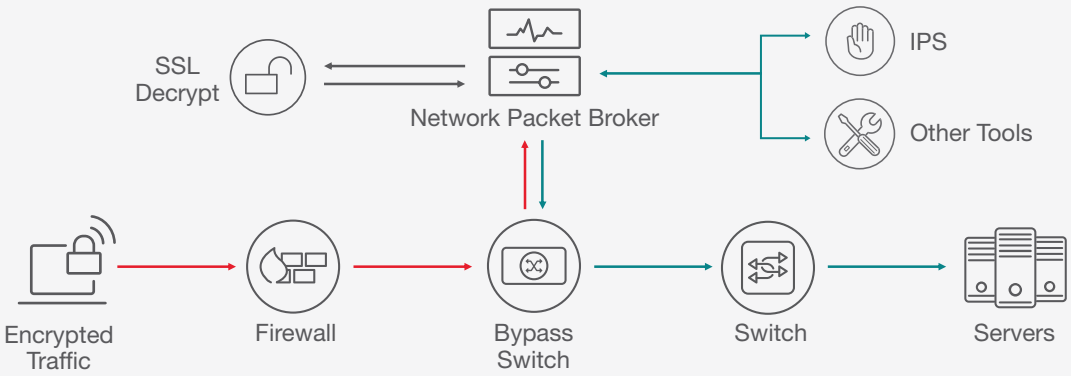


Figure 2. SSL decryption with a stand-alone appliance.

3 Report Summary: TLS 1.3 Adoption in The Enterprise, Enterprise Management Associates. February 2019.

Architecture option 2

An improvement to the architecture in option 1 is to include SSL decryption within the packet broker. This reduces complexity and costs by providing one integrated source for decryption before the inline security tool inspection process and data re-encryption.

Figure 3 illustrates an integrated decryption approach. The NPB decrypts the data and forwards it straight to special-purpose tools. The NPB does not impact application performance. Data that passes analysis by the security appliances is re-encrypted and sent into the network core.

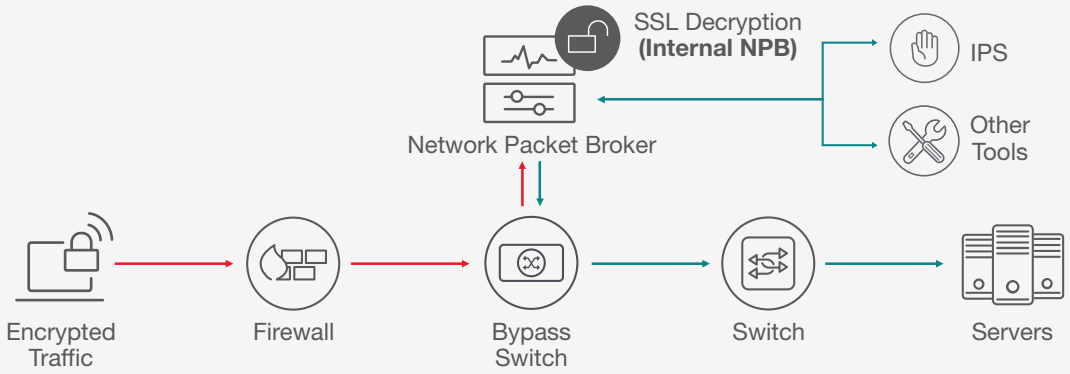


Figure 3. SSL decryption integrated into an NPB.

Architecture option 3

An alternative approach to a single SSL decryption device is to use decryption within every security tool. Unfortunately, this is the worst-case scenario. Figure 4 illustrates how each device has to perform MITM decryption and re-encryption, which increases costs because decryption capability is required on each device. The process slows down the flow of traffic considerably compared to the “decrypt once and inspect the data with multiple tools” approach. This option creates unnecessary complexity in the data monitoring process.

The biggest challenge with changing from passive decryption to active decryption is the inability to support security tools like DLPs, IDSs, threat hunting, and other DPI solutions out-of-band. This means the common solution in the Figure 5 process is no longer valid.

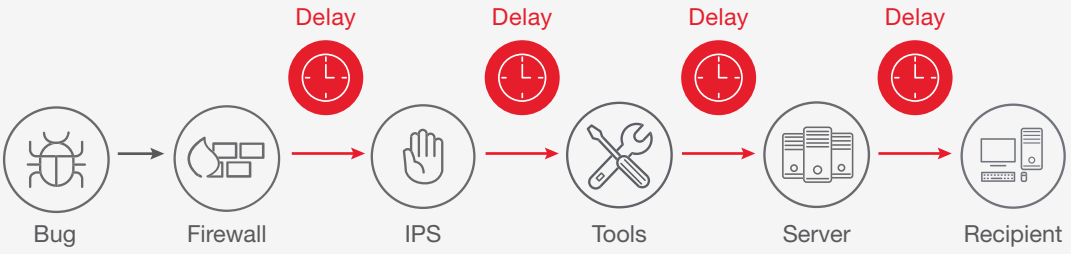


Figure 4. SSL decryption built into multiple appliances — not the architecture of choice.

Architecture option 4

The biggest challenge with changing from passive decryption to active decryption is the inability to support security tools like DLPs, IDSs, threat hunting, and other DPI solutions out-of-band. This means the common solution shown in Figure 5 is no longer valid.

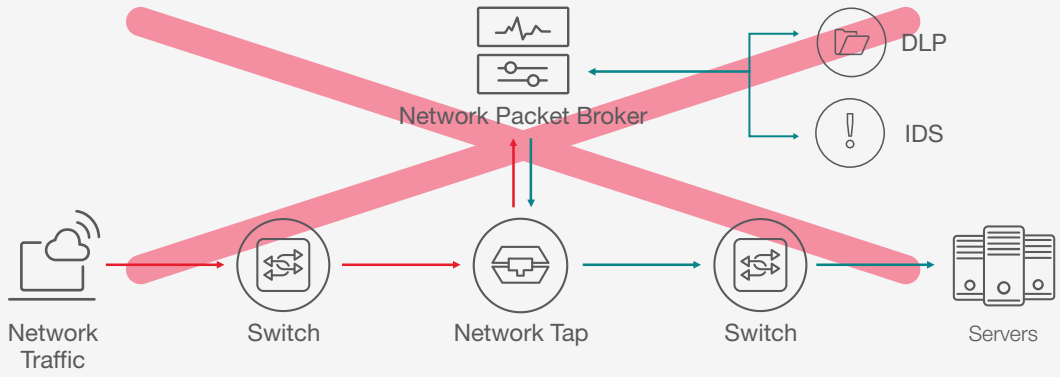


Figure 5. Now obsolete out-of-band security monitoring use case.

There is an alternative approach. Figure 6 illustrates a modification, so the NPB replicates a stream of data and sends that data to out-of-band tools. The out-of-band solution continues to work as before — this monitoring data is just a copy — no real-time actions are performed to stop threats. An extensive deep dive analysis can provide insight into well-hidden threats. Data can also migrate to a data lake for storage.

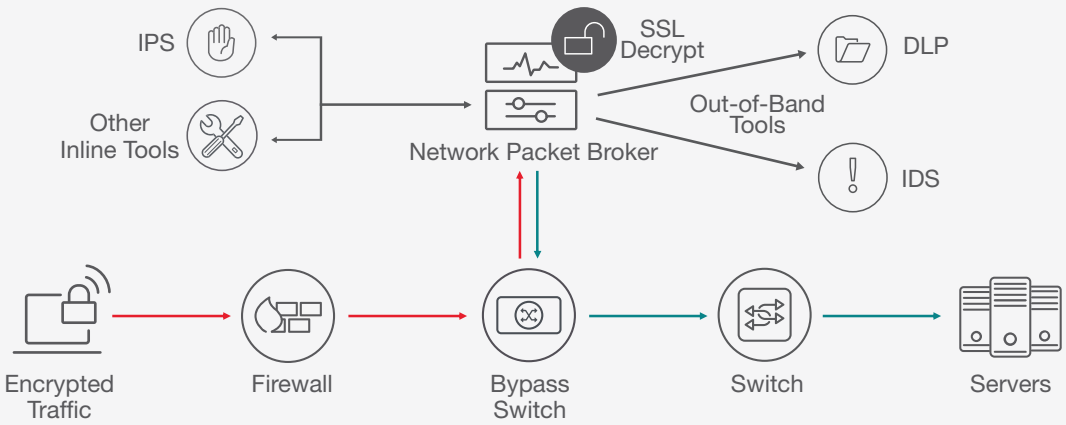


Figure 6. Inline and out-of-band security monitoring now combined.

Ciphers and Ephemeral Keys

Another fundamental change from the TLS 1.3 standard is the suite of allowed ciphers. TLS 1.3 only allows five ciphers. This is a significant difference from TLS 1.2 that allowed 37 ciphers, or from previous versions that allowed 319 ciphers. If any of the older ciphers are in use, then web servers must be reconfigured for the proper ciphers.

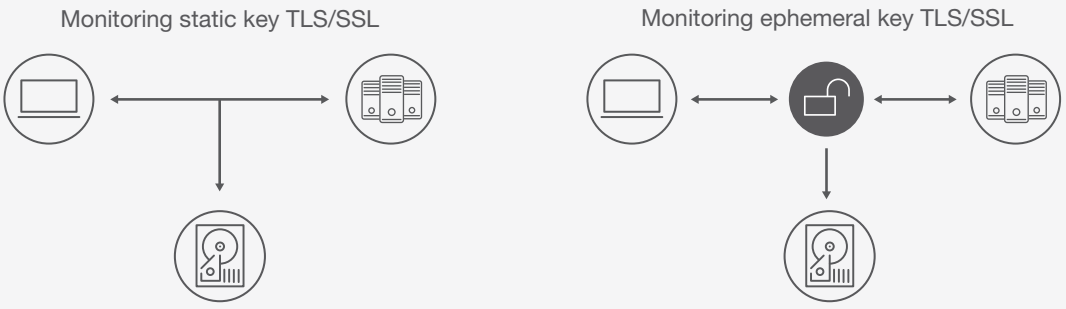
Here is the list of supported ciphers in TLS 1.3:

- ECDHE-ECDSA-CHACHA20-POLY1305-SHA256
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-CHACHA20-POLY1305

Until everyone adopts TLS 1.3, you may find that the actual keys your web servers need to use are still part of the TLS 1.2 standard.

Every additional security mechanism adds complexity to a security architecture. As Figure 7 illustrates, the movement from static keys to ephemeral keys comes at an engineering cost.

Another fundamental change from the TLS 1.3 standard is the suite of allowed ciphers. TLS 1.3 only allows five ciphers now This is a major difference from TLS 1.2 that allowed 37 ciphers, or the 319 ciphers allowed in previous versions...



- Can attach to a Tap or SPAN port
- Stream directly to disk and decrypt later
- No impact on original encrypted connection
- Requires monitoring device to have a copy of server's encryption keys

- Must be inline
- Must be an active part of the SSL connection— a "proxy"
- Add some latency / potential failure point
- Client must trust SSL inspection device

Figure 7. Comparison of static and ephemeral key decryption.

While the benefits of this new approach outweigh the disadvantages, it is necessary to account for the complexity. A way to mitigate the complexity in the short-term is to deploy decryption in stages. Identify architecture zones and then deploy decryption within a specific zone. A staged approach minimizes implementation issues, reduces time delays, and tests the security appliance processor load before implementing a mass cutover.

Active Testing of TLS/SSL Validates Security Solutions

Whether you currently deploy encryption or plan to, create a plan to validate SSL performance and efficacy. The first step for a security engineer is to investigate the equipment that is already in place. It is essential to know what you are testing and the ramifications of those tests. Which encryption protocols are running across the network? Which encryption keys are in use? Which parts of the network use encryption/decryption? When finished with your assessment, you will have a baseline of current encryption capabilities.

As you move forward to deploy TLS 1.3 across your network, you need to validate your TLS upgrade implementation. Is the decryption accurate? Is it 100% effective or did encrypted packets slip by unnoticed? This type of TLS testing covers firewalls, IDS, IPS, SSL offload, web servers, and other SSL points within a large data center architecture.

One critical concern is that decryption has the potential to change the underlying performance of the devices — throughput and session increases/decreases. The impact is sometimes substantial. According to a study performed by ZK Research, 45% of respondents admitted to turning off security features in devices to improve performance. SSL decryption was the central culprit of the problem.[4]

A test tool, such as Ixia's BreakingPoint, is required to investigate the decryption level of various network function points. This type of test system is a combined traffic and malware generator. It creates simulated traffic to mimic the type and amount of load on a network, as well as create encrypted malware. It is possible to retest these points prior to the TLS 1.3 upgrade (as a baseline) and then after.

According to a study performed by ZK Research, 45% of respondents admitted to turning off security features in devices to improve performance. SSL decryption was the central culprit of the problem.

4 Simplified Programming of a Visibility Layer Can Have a Big Impact on Application Performance, ZK Research 2016

Test 1: Application throughput with encryption

The first test includes using a security testing device to generate realistic network traffic, like that from YouTube, Facebook, Twitter, and other applications, to determine the throughput. Next, activate TLS 1.3 encryption and examine the throughput delta. It is common to see a 20 to 40% drop in throughput because of encryption. The important point is to factor this performance loss into your security architecture.

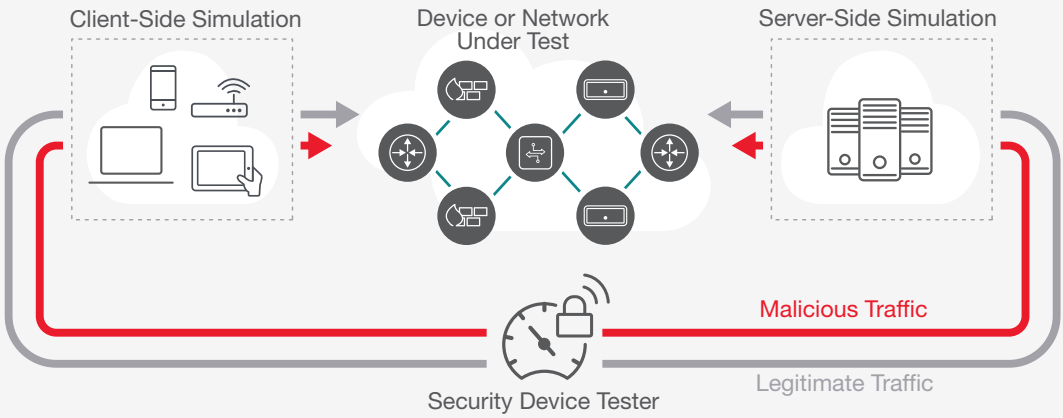


Figure 8. SSL decryption efficacy testing.

This type of testing allows you to validate the decryption capabilities of your equipment and the ability of your inline tools to catch malware.

Test 2: Performance variance with different ciphers

A second test is performance-related as well. A security testing device needs to create traffic using different ciphers to see the performance penalty created based upon cipher choice. For example, to test network operation of each of the five different ciphers that TLS 1.3 supports, or the impact of TLS 1.2 ciphers on the network.

Test 3: Efficacy of detecting encrypted malware

The third test to consider uses your security device tester to create encrypted malware and then send that traffic into your security infrastructure. Typically, this test is not performed on a live network. Most security engineering teams will create a realistic representation of their network in a lab environment to perform any tests that could impact the network. A device, or set of devices like inline threat detection tools (firewall, IPS, decryption solution, next generation firewall), can then be examined to see if those devices work as specified.

Test 4: Strength of decryption capabilities

This test probes your security architecture for weak decryption capabilities. Specifically, you can look at the key length of the bulk cipher, not the handshake keys, to determine if the system is using strong or weak keys. For instance, are all parts of your network running at TLS 1.3? Are some parts defaulting back to an earlier version (TLS 1.2 or 1.1) for some unknown reason?

There are tools available, like the Ixia SecureStack solution, that passively looks at the encryption keys in use on the network. The resulting information is exported as extensions to NetFlow metadata so that you can "see" the decryption capability across your network. A dashboard can display NetFlow data to provide a visual display of your network's capabilities. Such information enables you to restrict connections to sites with weak encryption; servers that are using keys that are too short.

Network monitoring may be a bigger challenge than anticipated. For instance, the EMA survey reported that 57% of respondents are currently unable to monitor security applications due to encryption. This indicates that network visibility actually decreased with the addition of decryption.

Ongoing Monitoring Strengthens Your Encryption Strategy

After introducing decryption, network monitoring may be a bigger challenge than anticipated. For example, the EMA survey reported that 57% of respondents are currently unable to monitor security applications due to encryption.[5] This indicates that network visibility actually decreased with the addition of decryption.

Once the transformation to TLS 1.3 is complete, ongoing monitoring is necessary to:

- Validate that inline and out-of-band security tools work as specified
- Validate that SSL decryption appliances are running at optimum speed
- Validate that TLS decryption and encryption is taking place accurately
- Verify that no malware has infiltrated the decryption process
- Ensure that the network is performing decryption as planned

Validation that all security tools work correctly is a major ongoing task. This means sending periodic encrypted malware tests to ensure that inline security tools continue to capture relevant threats. It also means that unencrypted data continues to flow to out-of-band tools for deep inspection, especially as the equipment is reconfigured over the following year or two.

In addition, periodic monitoring using a packet broker to create NetFlow data to look at encryption levels allows you to assess how well the decryption solution performs. A NetFlow collector forwards data from NetFlow logs for long-term analysis. As an example, if you have chosen the 512-bit cipher, you can determine if any device is not using that cipher. If someone in the organization creates a new server on the internal network with old software that is using weak encryption, you can easily spot that anomaly.

5 Report Summary: TLS 1.3 Adoption in The Enterprise, Enterprise Management Associates. February 2019.

Conclusion

TLS version 1.3 is the latest update to the SSL/TLS encryption standard and is intended to increase data security and user privacy.

Figure 9 summarizes the results of the changes introduced by TLS 1.3:

Static Keys		Ephemeral Keys
One for each client server pair	Session Key	New key every session
If you have session key, you can read all sessions	Forward secrecy	Having the key for one session doesn't let you see others
OK	Privacy	Much better
Straightforward	Legitimate monitoring	Problematic
Can listen passively	How to monitor?	Must participate in session
Only option up to TLS1.1	What TLS versions?	Optional in TLS1.2 Mandatory in TLS1.3

Figure 9. Summary of typical TLS 1.3 decryption changes for an enterprise

The new TLS standard should improve data privacy. However, performance will suffer, depending upon how fast the network was before decryption was employed. I t is possible to see a 20% to 40% drop in performance for most enterprise networks.

As the chart indicates, the new standard improves data privacy. It is difficult to simply perform a packet capture and look at the data. However, performance will suffer, depending upon how fast the network was before decryption was employed. It is possible to see a 20% to 40% drop in performance for most enterprise networks. Complexity will also increase, and sanctioned data monitoring will be more problematic. Enterprises currently using passive decryption to perform deep packet inspection and threat hunting will need to rearchitect their monitoring network to continue those types of activities.

So, after looking at all of this, do you really get improved security from decryption? The answer is probably not. Depending upon budget and resources, decryption may make your network less secure in the short-term while you rearchitect the network and purchase additional security solutions. What you really get is improved data privacy.

Ixia network visibility and security test solutions are a powerful way to optimize your network encryption and monitoring architecture. These include decryption solutions, inline bypasses and NPBs, TLS testing solutions, network monitoring, and intelligence solutions. Ixia can help you strengthen network security.

Additional Resources

For more information on network monitoring solutions, visit www.ixiacom.com/solutions/network-visibility.

For more information on network security test solutions, visit https://www.ixiacom.com/products/network-security-testing-breakingpoint.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES