

WHITE PAPER ENCRYPTED TRAFFIC MANAGEMENT

WHITE PAPER

Encrypted Traffic Management January 2016

Raphael Ernst

Martin Lambertz

Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE
in Wachtberg and Bonn.

Project number: 108146

Project partner: Blue Coat Systems Inc.

Contents

1	Introduction	5
2	The spread of SSL	6
3	Safety issues in previous versions of SSL.....	8
4	Malware and SSL	9
5	Encrypted Traffic Management.....	11
5.1	Privacy	12
5.1.1	Requirements.....	12
5.2	Compatibility	12
5.2.1	Requirements.....	12
5.3	Performance	13
5.3.1	Requirements.....	13
5.4	Security.....	13
5.4.1	Requirements.....	14
5.5	Costs	15
6	Conclusion	16
7	Sponsoring.....	17
8	Fraunhofer FKIE.....	18
	Appendix – Short test on Blue Coat Systems Inc. SV2800 appliance.....	19
	Bibliography.....	31

1 Introduction

Encryption using Secure Sockets Layer/Transport Layer Security (SSL/TLS)¹ has become ubiquitous in recent years. Many Internet websites and cloud services, as well as communications within and between companies, are already secured using SSL and the figures are likely to increase.

Increasing use of SSL encryption is extremely advantageous from an information security point of view, however it also presents new challenges to information security professionals. In fact, almost all modern security solutions such as intrusion detection systems (IDS), intrusion prevention systems (IPS), web filters, data loss prevention (DLP) systems or next generation firewalls (NGFW) are reliant on being able to analyse unencrypted data communications. As a result, cyber criminals and malware creators increasingly use encryption to disguise their data communications, complicate analyses and bypass security systems unnoticed using compromised computers.

Faced with these challenges, companies need to answer the question of how they want to deal with encrypted traffic on their networks – so-called “encrypted traffic management” (ETM)². This white paper will start off by explaining the extent to which SSL encryption has managed to proliferate on networks, thereby underscoring the relevance of ETM. After that, it will look at the security issues that accompany the use of SSL, and will quantify how widespread SSL is within the world of cyber crime. Broadly, these observations prove that ETM needs to be a component in modern information security architectures, so the paper will conclude with an explanation of which requirements any appropriate solution will need to meet.

¹ TLS is the successor to SSL, however the abbreviation SSL is also widely used synonymously with TLS. We will therefore use the term SSL in the rest of this white paper for the sake of simplicity. Further information on the name change can be found in blog [37] by Tim Dierks, co-author of RFC 2246 on the standardisation of TLS 1.0. This white paper is not meant as an introduction to SSL. A more comprehensive description of SSL, including theoretical and practical considerations, can be found in [38].

² In addition to SSL, there are also a number of other encryption protocols, however they are much less widespread. This white paper will concentrate solely on SSL.

2 The spread of SSL

SSL/TLS (SSL versions 2.0, 3.0, TLS versions 1.0, 1.1, 1.2 and the forthcoming standard 1.3) is the most common form of end-to-end encryption used over the Internet today. It supports numerous standardised combinations of key exchange algorithms and encryption/hash functions [1] and are therefore able to cover almost all sender/receiver confidentiality, integrity and authenticity requirements. As a result, SSL is used to secure a broad range of applications, from File Transfer Protocol over SSL (FTPS) and e-mail communication over SMTPS and IMAPS, to web browsing over HTTPS. Popular web mail and social media platforms such as Google, Facebook and Twitter, as well as cloud services such as Dropbox, Office 365 or Amazon AWS, also use SSL to encrypt their communications as standard.

Studies on the use of encryption in companies have shown that over 25% of Internet traffic is already encrypted nowadays [2] [3]. In 2012/2013, the use of SSL by the Internet's top 1,000,000 websites grew by 23% [4]. By 2014, the proportion of websites had already reached 45% [5]. The most recent measurements from the ZMap Team at the University of Michigan [6] show that, as of January 2016, almost 70% of the websites included in the rankings use SSL. As the leading search engine provider, Google has seen such significant results from encryption using SSL that it started to use HTTPS as a ranking signal back in 2014 [7]. Thanks to initiatives such as Let's Encrypt, [8] it can also be assumed that even smaller websites will reinforce their encryption in the future, leading to yet more SSL traffic.

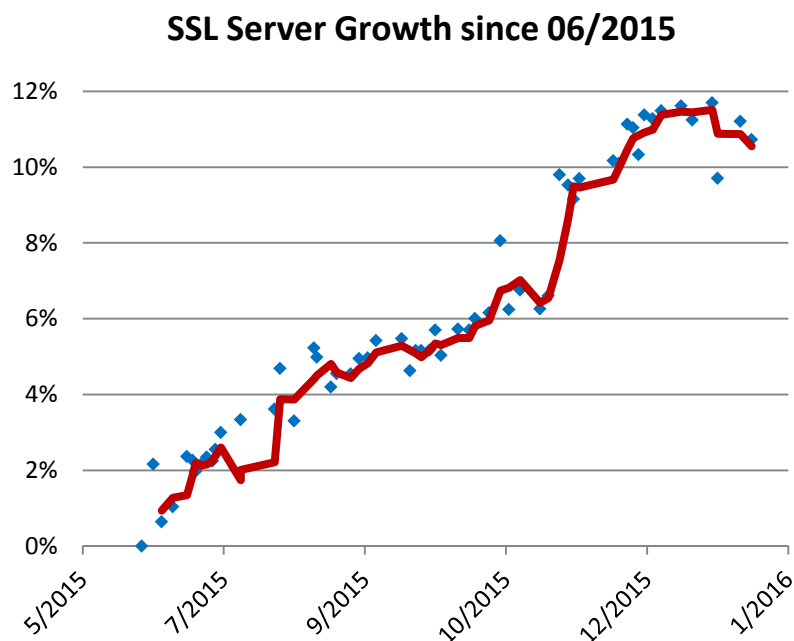


Figure 1: increase in SSL servers on port 443 in the global IPv4 Internet based on measurements by the University of Michigan

The German Federal Office for Information Security (BSI), which is responsible for preventing threats to the security of federal information technology as well as testing and evaluating the security of information technology systems [9], recommends the use of SSL

even under normal circumstances [10]. Germany's Conference of the Data Protection Commissioners of the Federal Government and the *Länder* [11] also demands that personal data be protected according to the very latest standards, i.e. SSL.

The reasons behind the growing use of SSL are varied: even embedded devices can use SSL without a significant drop in performance, meaning that companies are able to secure all communications and therefore thwart possible economic or industrial espionage. The private sphere has also seen awareness of issues regarding data protection increase as encrypted services become increasingly popular. Especially in e-commerce, online banking and messaging, encryption has become an increasingly important selling point.

All of the above has led to SSL encryption becoming very widely used. Faced with increasing security requirements, current developments and the ease of access, the spread of encryption will in all likelihood continue to rise in the coming years.

.....
The spread of SSL
.....

3 Security issues in previous versions of SSL

In the past, the complexity of SSL led to the need for greater numbers of fixes, e.g. to optimise the protocol or to solve issues with implementation errors which were weakening the process. Studies have shown, however, that these improvements were often only implemented at a much later date, as manufacturers were not updating their software or devices [12]. By way of an example, we will now look at a few well-known vulnerabilities and implementation errors in order to illustrate the threat.

The "Browser Exploit Against SSL/TLS (BEAST)" [13] exploit affects SSL 3.0 and TLS 1.0. It uses predictable values to identify parts of the plain text within encrypted traffic. BEAST was proven capable of cracking an encrypted HTTP session cookie. As a result, users were advised to upgrade to version 1.1 of TLS or to encrypt data using RC4, which BEAST was not capable of cracking.

Documented attacks on RC4 [14] have shown, however, that this process provides insufficient protection. As a result, RFC 7465 prohibited the use of RC4 in all versions of TLS, and therefore can't be used as a measure to protect against BEAST.

In addition to problems with the SSL protocol and in the encryption algorithms that were being used, implementation errors were also discovered. A particularly serious example of this was the so-called Heartbleed bug in OpenSSL [15] [16]. Unlike outdated protocol versions or weak ciphers, the affected keys or systems cannot immediately be recognised, meaning that security can be massively compromised [17]. Even in such serious cases, protective measures are still often taken far too late [4].

These examples show that the use of SSL on its own is insufficient. It is essential to ensure that current protocol versions and secure implementations are also used.

4 Malware and SSL

In the beginning, malware used unencrypted communication, but then later implemented its own encryption procedures to disguise data traffic. Recently, however, there has been a noticeable increase in the use of SSL encryption by malware [18] [19] [20]. Experts at Cisco established that in 2015 12.26% of malware communications were using the TLS protocol [21].

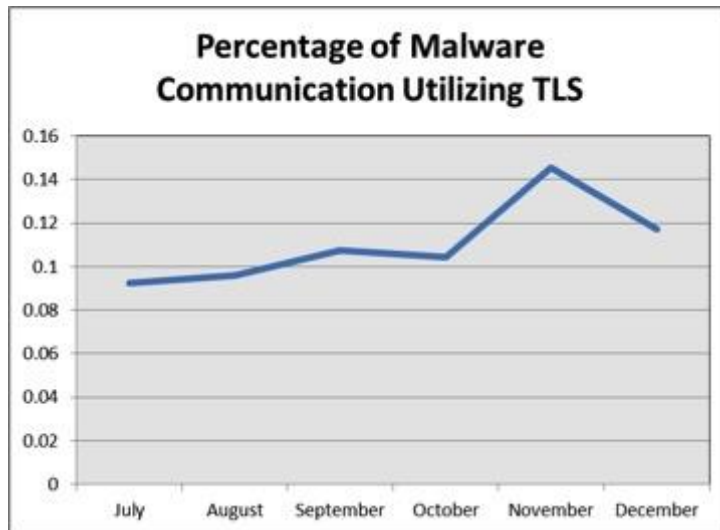


Fig. 2: use of TLS in malware communication between July-December 2015. Cisco Systems, Inc., 2016 [22].

For malware, the use of SSL has several advantages: first of all, the growing prevalence of the protocol ensures that malware traffic cannot be differentiated from regular traffic. In addition, there is no longer the need for proprietary encryption solutions – instead, tried and tested libraries and existing infrastructures such as web proxies can be used, which are explicitly for SSL transport. In fact, Cisco noted that 98.25% of malicious TLS traffic used HTTPS standard port 443 [22].

Blue Coat Systems Inc. has also made similar observations¹: between January 2014 and September 2015, a whole range of malware families and command and control (C&C) servers which were known to use SSL were active. Each month, an average of over 500 samples of these malware families were found. In the remaining three months of 2015, this value rose to almost 29,000 samples per month². A similar explosion was also noticeable on well-known C&C servers: in the 3rd quarter of 2014, Blue Coat Systems Inc. had identified around 1,000 C&C servers which communicated with the malware families; by the 3rd quarter of 2015, over 200,000 were known. Although these figures are likely to fluctuate, they are still an important indicator that SSL/TLS will be used more and more in the future to hide attacks.

Another emerging trend is the distribution of malicious software over advertising networks [23] [24] [25]. In such cases, attackers inject malware-laden software into legitimate

¹ Data provided by Blue Coat Inc. to the authors of this study.

² Based on figures from the SSL Blacklist project (<https://sslbl.abuse.ch>)

advertising networks which take advantage of vulnerabilities in the victim's system. As advertising networks also encrypt their content, common security software cannot recognise the malicious code from the transport alone. This is particularly dangerous as it is not only small or specially-prepared websites that are affected. Even popular websites such as eBay [26], Yahoo [24] and Weather.com [25] have already been shown to spread malware.

Known SSL C&C Servers

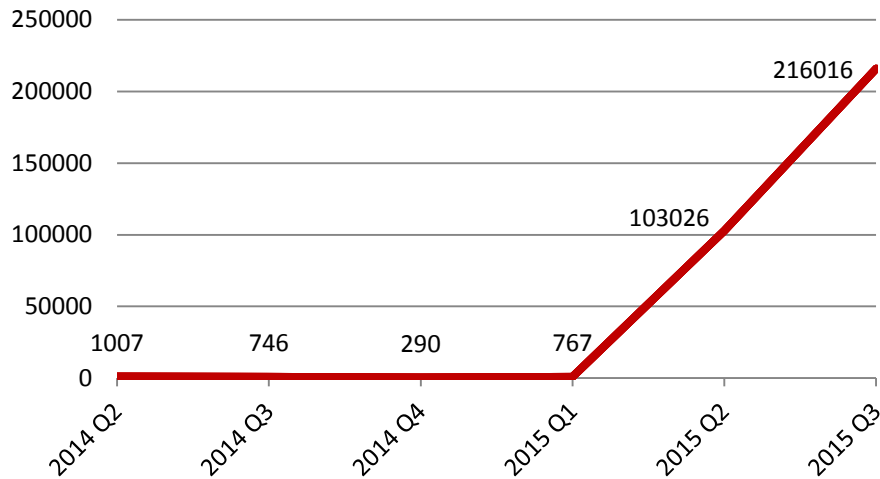


Figure 3: number of C&C servers detected by Blue Coat Systems Inc.

Malware Samples with SSL per Month

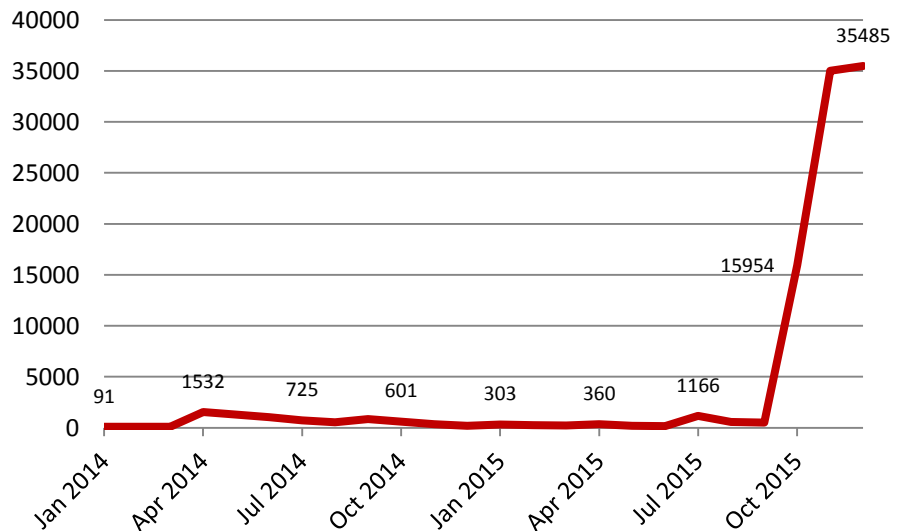


Figure 4: number of malware samples including SSL detected by Blue Coat Systems Inc.

5 Encrypted Traffic Management

The sections above have proven the importance of having a comprehensive ETM approach for handling encrypted traffic. Without ETM, many established security measures are either of limited or no use whatsoever. When implementing such a strategy, it is essential to take into account privacy policies, legal requirements, works agreements and even technical aspects such as performance levels of the different products.

A study by Securosis [27] looked at questions of privacy and the performance of different types of device. Their conclusion? “What you don’t see can kill you”. Consequently, Securosis recommends analysing encrypted traffic. It is just as important that measures are taken to ensure that personal data is not decrypted, or is examined as little as possible. In an analyst brief [3], NSS Labs analysed how great the loss in performance was for NGFWs when decrypting SSL traffic, highlighting the advantages and disadvantages of such a solution. Their conclusion was that thorough investigation of the requirements and performance during SSL analysis is necessary in certain specific cases. Just like Securosis in [27], NSS Labs also came to the conclusion that policies should be applied to except certain data from decryption.

In [2], ESG published the results of a questionnaire of 150 “IT and information security professionals” regarding “Network Encryption and its Impact on Network Security” and [2] offered important considerations that readers could implement in their own organisation. This white paper builds upon this background information by providing a comprehensive list of the security measures and requirements needed for an ETM solution. The main requirements can be divided into the categories of privacy, compatibility, performance, security and cost, although some of them cannot be assigned to just one single category. To explain these requirements in a little more detail, we will now look at an example of an ETM solution with a dedicated SSL visibility appliance (such as in [27] and [28]). Similar considerations and requirements are also applicable for other types of deployment.

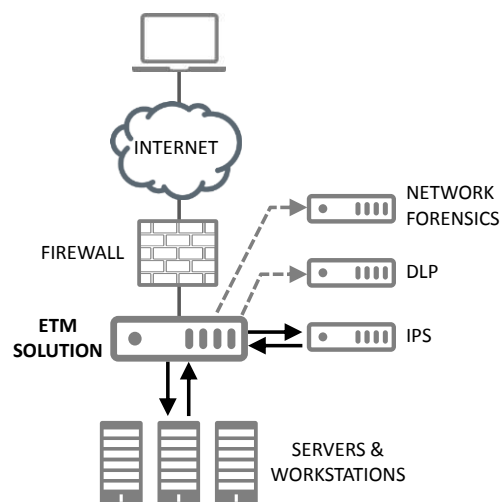


Figure 5: both incoming and outgoing traffic from/to servers and workstations are decrypted first by the ETM solution and then passed onto connected security solutions. Active solutions such as IPS can terminate suspicious connections, whereas purely passive solutions such as IDS just read the data traffic and send alerts.

5.1 Privacy

One of the reasons for the rise in the use of encryption is the increasing importance of protecting individuals by making it harder to link them to the content of their communications. In corporate environments, this is generally only secondary to protecting confidential information. Nevertheless, an ETM solution must still be able to differentiate between different groups of people such as management, HR department or clerks, and be capable of implementing the respective corporate policy requirements, legal obligations and works agreements. Furthermore, it must be able to distinguish separate content: online banking must be handled very differently to social networks, for example.

5.1.1 Requirements

1. **Filtering according to source:** the decision whether or not to decrypt traffic should be dependent on the source of the query. Different groups of people can be managed according to the demands of their position.
2. **Filtering according to destination:** the decision whether or not to decrypt traffic should be dependent on the destination of the query, e.g. online banking will be handled differently to social networks.
3. **Selective forwarding:** regardless of the decision on whether or not to decrypt the data, it must be possible to configure which security systems the data are forwarded to for further analysis.
4. **Block lists and reputation databases:** comprehensive reputation and classification databases consist of enormous data repositories which must be updated constantly. Management of these databases is normally carried out by specialised service providers, and the ETM solution should be capable of integrating with them.

5.2 Compatibility

There are many versions of SSL available. Each of them can utilise a wide range of different cipher suites which, in turn, can be configured according to a wide selection of parameters. An ETM appliance must be capable of supporting all common permutations. On top of that, SSL can be used with all kinds of protocols depending on the application. The ETM solution must be equally capable of supporting both standard and non-standard configurations.

5.2.1 Requirements

5. **Support for all relevant SSL/TLS versions:** SSL 2.0, 3.0 and TLS 1.0, 1.1, 1.2 – and soon TLS 1.3 – should all be supported.
6. **Support for all relevant cipher suites:** the IANA provides a registry of all cipher suites in RFCs at [1]. All of these should be supported.
7. **Support for relevant cipher suite parameters:** this primarily affects the supported key sizes. Currently the majority of keys are between 512 and 8192 bits. Occasionally there are also instances where larger keys are used.
8. **Support for common protocols at a transport and network level:** especially IPv4, IPv6 and TCP or UDP (which is still used infrequently).

9. **Support for non-standard configurations:** if only standard ports are examined, a large proportion of communication remains uninspected. As a result, the solution needs to be able to identify and examine traffic through all ports.
10. **Application-independent handling:** when decrypting, an ETM solution should not only be able to manage common uses such as web browsing and e-mail, but must also be able to decrypt traffic regardless of the application – it is important to also scan for malware incidents that communicate via their own protocols.
11. **Statistical data:** new findings in cryptography and more powerful hardware frequently result in changes in the key sizes and the procedures used. An ETM solution should provide statistical information on the traffic analysed in order to detect and react to changes in data traffic in a timely fashion.

5.3 Performance

Among the most important benchmarks regarding performance in security solutions are throughput and latency. Both of these variables are also relevant when evaluating ETM solutions. Other important factors are the maximum number of connections established per second and the maximum number of parallel connections the solution can handle.

5.3.1 Requirements

12. **Low latency:** low latencies are particularly important for real-time applications such as video or telephony systems. If an ETM solution is monitoring all traffic or connections via VPN tunnels, it is essential to ensure that the additional latency does not have a negative effect on them.
13. **High throughput:** high throughput plays an important role in many situations to avoid network bottlenecks, particularly when synchronising large quantities of data, e.g. when carrying out backups or accessing databases.
14. **Sufficiently high numbers of connections per second:** in addition to latency and throughput, a decisive factor in ETM solutions is the amount of connections they can handle in short periods of time. As a result of the increasing prevalence of encryption on the Internet, the majority of web requests also involve the setting up of SSL connections. If the ETM solution cannot handle these requests quickly enough, the connections are affected by high latencies. In the case of short-lived connections, only a low throughput is achieved.
15. **Sufficient parallel connections:** an ETM system must, as a rule, analyse all active SSL connections. Once the limit has been reached, no further connections can be accepted, meaning that any additional incoming connections are either rejected or not handled.
16. **Scalability:** operations in enterprise networks require efficient support for multiple network segments. The scalability of an ETM solution must therefore apply both to the number of hosts and the complexity of the network infrastructure.

5.4 Security

An ETM strategy should, on the one hand, make it possible for existing security systems to examine encrypted traffic, but should also contribute actively to data confidentiality. The solution must enforce minimum standards for encryption and ensure continued operations in case of failures.

5.4.1

Requirements

17. **No downgrading of cipher suites:** decryption and analysis of SSL traffic must not compromise the security level of the SSL session. Many solutions such as NGFWs do not support perfect forward secrecy. An ETM solution must support at least the same SSL features as the client and server have negotiated for the session.
18. **Blocking of weak cipher suites:** new findings from the last few years in cryptography and protocol analysis have revealed more and more weak spots, making certain protocol versions or algorithms liable to attack. These versions should be replaced immediately, but often remain in use for a long time due to a variety of reasons (such as configuration issues). An ETM solution should support policies which either warn users of the issue or even prevent their use.
19. **Upgrading of weak connections:** under certain circumstances, ciphers will need to be used which have been classified as insecure, as it is not possible to update the affected devices or software. In these situations, the ETM solution should be able to accept the weak connection and then establish its own secure connection to the remote location. This will make it possible to considerably increase security.

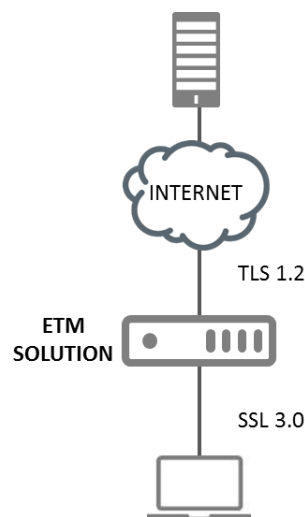


Figure 6: a legacy client in a company only supports SSL 3.0, whereas the queried server can handle TLS 1.2. The policy employed by the ETM solution on the company network will allow the SSL 3.0 encryption – even though it has been classified as insecure – but will establish the connection to the server using TLS 1.2 in order to ensure maximum security.

20. **Accessibility to other products:** the main task of an ETM solution is to provide decrypted data for analysis by other systems such as IPS, IDS, NGFW or DLP. Particularly in the case of active connections, the option must be provided to make changes to the data traffic (e.g. the termination of a connection).
21. **Multi-layer SSL:** theoretically, it is possible to establish further SSL connections from inside of an existing SSL connection. This function can be abused, however, to circumvent filters or blocking mechanisms and exfiltrate data past a DLP system. As a result, an ETM solution must also be capable of handling multi-layer SSL connections. Alternatively, policies in downstream systems (such as an IPS) can prevent connections of this type from being established or re-sent to the ETM solution.
22. **Certificate revocation lists (CRLs) and certificate blocking lists:** upon connection, many clients verify whether the endpoint is actually the requested server. As clients do not actually communicate directly with the endpoint in ETM solutions, it is up to the ETM solution to ensure that the destination server has a

- valid certificate. This, in particular, involves checking CRLs and certificate blocking lists and warning the client if an invalid certificate is detected.
23. **Invalid certificates:** a warning must be generated or a suitable policy must be configurable in the ETM solution in case a client attempts to connect to an endpoint which either has an invalid or self-signed certificate.
 24. **Certificate pinning:** certificate pinning offers the client the possibility of verifying the endpoint's certificate directly without the need for a CA. In such scenarios, a trusted man-in-the-middle, as used in ETM solutions, is not possible. It must be possible to define a policy which allows the client to establish connections, even if they cannot be analysed ¹, even if this is at the expense of transparency and could pose a risk of data theft. Alternatively, it is an option to simply block the connection.
 25. **Warning messages in case of decryption errors:** some targeted attacks to overcome security systems make use of buggy implementations that cannot be processed by the security solution. Fault-tolerant clients are, however, capable of interpreting the data, meaning that an ETM solution should generate a warning in the case of errors.
 26. **Availability in the event of failure or overload:** just like with any other product, ETM solutions are also susceptible to failures, a fact which needs to be taken into account in advance. There are three possible solutions in such cases:
 1. If there is a failure, the solution can automatically discard all traffic. Depending on the configuration, this can be used to discard all passing traffic, not just SSL-encrypted data.
 2. Alternatively, the data traffic can be forwarded unprocessed (and still encrypted) to connected security products. In some situations, these products continue to offer limited functionality for encrypted data.
 3. The third option is a bypass, whereby the data is forwarded directly onto the outgoing network device.
 27. **Patch management and updates:** their central position in the network and access to otherwise encrypted data make ETM solutions a very attractive target for attackers. ETM solution vendors need to react quickly to security issues with the ETM solution itself and must offer appropriate maintenance contracts. This is also applicable to the updates required when protocol versions change. Downtimes resulting from update processes must be kept to a minimum.

5.5 Costs

As with all security solutions, it is a question of weighing up the costs and the benefits for the customer. It is initially a question of clarifying whether it is better to deploy a dedicated appliance or adding the ETM functionality to existing security tools. In addition to capital expenditure (additional hardware, expanding existing solutions), the operational costs (greater configuration costs, increase architecture complexity) must also be taken into account. On top of that, other factors such as the required licences for integrating host reputation services and personnel costs must be factored in.

¹ Chrome [39] and Firefox [40] browsers have the option of bypassing certificate pinning through local settings.

6 Conclusion

The use of SSL and TLS is set to continue rising across the globe. At the same time, the number of advanced malware and cases of data theft using SSL/TLS will also increase. This means that encrypted traffic management (ETM) has been given an increasingly important role in safeguarding infrastructures. Nevertheless, companies need to find ETM solutions capable of satisfying their needs with regard to data privacy, compatibility, security, performance, scalability and cost effectiveness, all in equal measure.

The FKIE has carried out a series of tests on Blue Coat Systems' SSL Visibility Appliance in order to determine whether it successfully meets these demands. The appendix to this white paper contains a description of these tests and the results.

7 Sponsoring

This white paper was sponsored by Blue Coat Systems Inc.



8 Fraunhofer FKIE

The Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE is a leading institute in the field of security related information and communication technology. Conducting applied science they create practical and innovative solutions. They cover various research fields, ranging from sensor data and information fusion, information technology for command & control, cyber security, robust and secure communications systems and networks, software defined and cognitive radio, to robotics and ergonomics.

Appendix – Short test on Blue Coat Systems Inc. SV2800 Appliance

Contents

1	Introduction	20
2	Test setup	21
3	Tests	22
3.1	Scenario 01: simple functional tests	22
3.2	Scenario 2: non-standard configurations.....	22
3.3	Scenario 3: multi-layer SSL and SSL VPNs	23
3.4	Scenario 4: different cipher suites	24
3.5	Scenario 5: exception handling for defined endpoints	25
3.6	Scenario 6: malware	26
3.7	Scenario 7: weak cipher suites	27
3.8	Scenario 8: invalid certificates	27
3.9	Scenario 9: Active-Inline test.....	28
3.10	Scenario 10: failsafe operation	28
3.11	Limitations of SSL TMITM appliances	29
3.12	Test matrix	29
	Bibliography.....	31

1 Introduction

As part of the drafting of the white paper entitled “Encrypted Traffic Management” [29], Blue Coat Systems Inc. provided the authors with an SSL Visibility Appliance SV2800 for the purpose of testing. This meant that scenarios could be tested under laboratory conditions using a real appliance.

The short tests demonstrated in this document cover a number of the requirements considered in the white paper [29], however they were not meant to address the issue of performance tests or comparisons with other products. As a result, the short tests were only meant to represent a comparison between the requirements and an existing product on the market.

The tests were carried out with the support of and in consultation with Blue Coat Systems Inc. Blue Coat Systems Inc. was given the opportunity to provide suggestions and clarifications to the individual tests or results.

Hereinafter, Blue Coat Systems Inc. will be referred to simply as “Blue Coat” and the SSL Visibility Appliance SV2800 as “SSLV”.

2 Test setup

Figure 2 shows a schematic representation of the structure of the test scenarios covered in the following sections. Encrypted connections are shown in red; decrypted traffic in green. The client sends SSL-encrypted data to a server. These are then routed via the SSLV to which an intrusion detection system (IDS) is connected. Unless specified otherwise, the appliance is run in "Passive-Inline"¹ mode. In this mode, the application is run transparently between the client and server, simply forwarding the decrypted traffic to the IDS without intervening actively in the connections.

To validate the decrypted traffic, an IDS system is used, which only logs the traffic incoming from the appliance. The recorded data is then compared to the data created on the client. On the server side, checks are made to ensure that the connection was carried out with the desired encryption.

For each test scenario, the requirements as listed in [29] are tested according to the specifications. A short description of the test and a graph of the results are also given. Green, orange and red markings indicate successful, partially-successful and failed sections of the test. A short explanation of the results is then given.

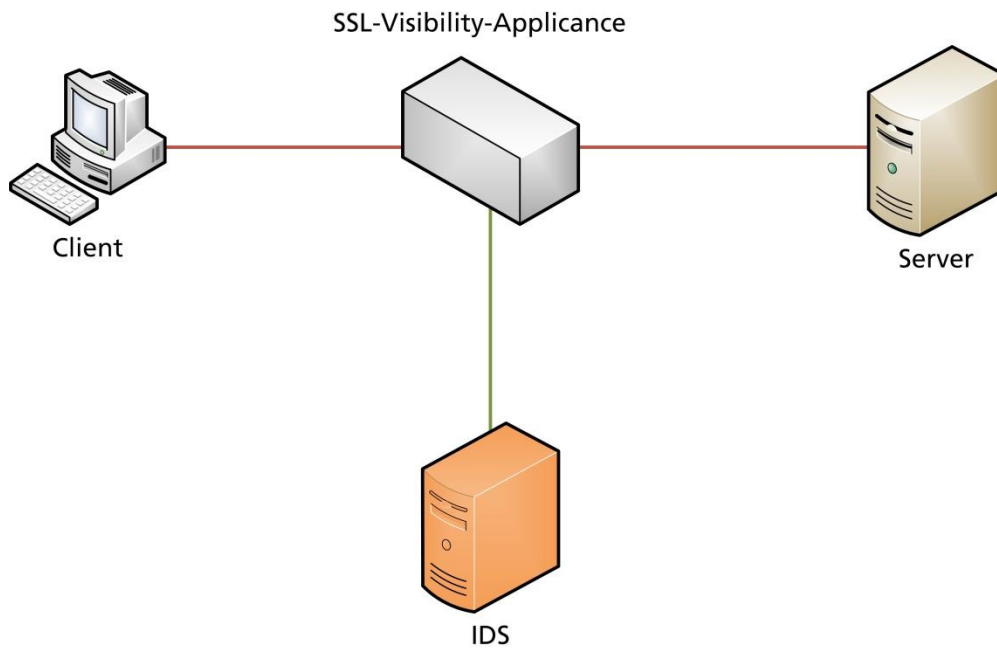


Figure 2: Schematic diagram of the test structure








¹ Passive-Inline is one of the three possible modes supported by the SSLV. The other options are "Passive-Tap" and "Active-Inline". All three modes are described in the administrator's manual [34].

3 Tests

3.1 Scenario 01: simple functional tests

Requirements tested: 10

Description: this scenario is intended to check the basic functionality of the SSLV. It involves establishing connections between the client and server using different standard protocols/services which are usually encrypted using SSL.






Protocol	Network protocol	Port	Result
HTTPS	IPv4	443	
POP3S	IPv4	995	
POP3/STARTTLS	IPv4	110	
IMAPS	IPv4	993	
IMAP/STARTTLS	IPv4	143	
SMTPS	IPv4	465	
SMTP/STARTTLS	IPv4	25	







Note: all connections were encrypted both on the client and the server; on the IDS, however, they were in plain text. The results seem to prove that the basic functionality of the SSLV is ensured in the case of standard protocols.

3.2 Scenario 2: non-standard configurations

Requirements tested: 8, 9, 10

Description: in this scenario, the tests from scenario 01 were repeated but using unusual ports. In the test sections with stunnel, the LINUX tool stunnel was used to establish an SSL connection to the destination. Data was then transferred via this tunnel.

Protocol	Network protocol	Port	Result
HTTPS	IPv4	37331	
POP3S	IPv4	21993	
POP3/STARTTLS	IPv4	23658	
IMAPS	IPv4	64768	
IMAP/STARTTLS	IPv4	61251	

				Tests
SMTPS	IPv4	59224		
SMTP/STARTTLS	IPv4	30237		
rsync over stunnel	IPv4	873		
netcat over stunnel	IPv4	4443		
netcat over stunnel	IPv6	4443		
ncat1 with SSL over Sctp2	IPv4	54321		

Note: as with the previous scenario, the usual TCP applications returned the expected results. It appears that the port running the protocol does not seem to play any role in the success of the SSLV.


In addition to the tests with IPv4, one test segment included an evaluation with IPv6. In this scenario, the SSLV also forwarded the traffic to the connected IDS in decrypted form. Only in the last test, in which the Stream Control Transmission Protocol (SCTP) was used instead of TCP, was the connection not decrypted. This is, however, a niche protocol which is not used very often. As a result, this was not evaluated negatively in the concluding list in the test matrix.

3.3 Scenario 3: multi-layer SSL and SSL VPNs

Requirements tested: 21

Description: As an example of a test case in which SSL traffic takes place within an already encrypted SSL connection, a website was opened via HTTPS over stunnel. This is a recognised procedure for circumventing company firewalls with the help of HTTPS proxies and stunnel.

Some types of VPN connection are also cases where an SSL connection takes place within another connection.

Layers	Result
HTTPS over stunnel	

Note: in this test, no plain text data in the proper sense was received by the IDS. the SSLV was only able to remove the outer SSL layer. This means the IDS received the encrypted HTTPS connection.

Blue Coat confirmed when asked that the SSLV is not intended for scenarios in which multiple SSL layers are used. As a suggestion for a possible solution, a proxy can be installed before the SSLV which will refuse such SSL connections. In this case, an inspection of the plain text is not possible either, however circumventing the policy by using several SSL layers can be successfully prevented.

¹ ncat is a netcat implementation in port scanner which supports native SSL over Sctp.













² SCTP is an alternative transport protocol such as TCP or UDP.

In the case of VPN connections – another scenario with multi-layer SSL connections – the same is true whereby only the outer layer can be removed. In the document entitled “Encrypted Traffic Management For Dummies” [30] Blue Coat explains that in these cases, a TMITM appliance should be installed internally (i.e. behind the VPN endpoint) if the traffic needs to be inspected. The National Institute of Standards and Technology (NIST) also recommends ensuring access to decrypted data to the security solution [31]. Both follow the NIST recommendations for the deployment of SSL VPNs [32]. In this scenario, each connection was processed by the SSLV. The additional VPN encryption layer would not have any consequences as it was already removed by the VPN endpoint. This case covers the majority of VPN connections in a company. Attackers that have already gained access to the inside of the network can, however, establish unauthorised tunnels to exfiltrate data. Scenarios in which employees establish VPN connections to other companies in order to, for example, use their services are not covered either. Attackers can be prevented from establishing connections with the correct use of suitable policies, whereas different measures must be taken in the case of employees.

3.4 Scenario 4: different cipher suites

Requirements tested: 6

Description: this scenario verifies whether the SSLV can handle different cipher suites. The cipher suites tested are those with forward secrecy recommended by the BSI (cf. [33], Table 1, p. 6).

Cipher suite	Result
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256



Tests

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256



TLS_DHE_RSA_WITH_AES_256_CBC_SHA256



TLS_DHE_RSA_WITH_AES_256_GCM_SHA384



Note: the results correspond to the details given in the "Administration & Deployment Guide" [34] for the SSLV. That document states clearly that neither "static DH (Diffie-Hellman) key exchange" nor "DSS (Digital Signature Standard) authentication" are supported (it contains a list of all supported cipher suites). It should be noted here that the corresponding connections were recognised as SSL traffic. In practice, it is possible to configure policies in the SSLV which can either terminate such connections or direct the traffic through in encrypted form.

3.5 Scenario 5: exception handling for defined endpoints

Requirements tested: 1, 2, 4

Description: to check source/destination filtering, a simple company-wide guideline was defined which allowed private surfing but blocked all pornographic material. In this case, confidential connections from a workstation computer (Host A) – for example, in the case of online banking and other similar services – should not be decrypted, pages with pornographic content should be blocked and all other connections should be forwarded to the IDS in unencrypted form. In addition, in the case of certain source hosts (Host B) the entire communication should be decrypted. Host B represents systems with particularly sensitive internal company information which are not permitted for any private use.

Source	Destination	Expected	Result
Host A	www.deutsche-bank.de	encrypted	encrypted
Host A	www.sparkasse.de	encrypted	encrypted
Host A	www.paypal.de	encrypted	encrypted
Host A	www.ebay.de	encrypted	encrypted
Host A	www.gmx.net	encrypted	encrypted
Host A	www.google.com	decrypted	decrypted
Host A	www.gutefrage.net	decrypted	decrypted
Host A	www.youporn.com	blocked	blocked
Host A	livejasmin.com	blocked	blocked

Tests

Host B	www.deutsche-bank.de	decrypted	decrypted
Host B	www.sparkasse.de	decrypted	decrypted
Host B	www.paypal.de	decrypted	decrypted
Host B	www.ebay.de	decrypted	decrypted

Note: this overall guideline was implemented using a combination of “host categorisation list”¹, “subject/domain names list” and source IP filters. It was simple to cover bank websites, Paypal and eBay as well as web pages suitable for all audiences with simple host categorisation. GMX, web.de and Outlook.com were used randomly and interchangeably as mail servers². They were all, as expected, categorised correctly as confidential. In some cases it was possible to register a new e-mail address, however access was then blocked. When validating the results, it became obvious that different components of a website can come under different categories when using host categorisation. To name one example, the majority of Sparkasse bank web pages came under the “financial services” category, however this was not the case for the chat service offered on the same page. In summary, the host categorisation list is a very good basis on which to implement a basic guideline. It will, however, require perfecting with additional filter functionalities and may require validation via testing. The SSLV supports filters based on domain name and IP addresses, cipher suites, certificate subjects and traffic classes as well as many others. The current version of the SSLV does not support any local block lists or reputation databases. Domain and IP lists can be set up manually, however scalability is limited once a certain database size is reached. Blue Coat noted that local, user-defined databases should also be supported in future versions.

3.6 Scenario 6: malware

Requirements tested: 10

Description: Certain malware families exploit SSL to disguise communication activities. In this scenario, the example of the following sample (hash: 006744efeg90cc666cca8c23ba759ba4d3721f910c03a7a8e29e0bde3bode0e52) was used to verify whether the data traffic was decrypted by the SSLV.

Sample	Result
006744efeg90cc666cca8c23ba759ba4d3721f910c03a7a8e29e0bde3bode0e52	

¹ The host categorisation service is an add-on subject to a licence fee which contains predefined lists with categorised websites. An overview of the different categories can be found in [5].

² This test proved that host categorisation is highly fine-tuned. Even if the “e-mail” group is blocked, it is still possible to access certain pages within GMX.



Note: data traffic was decrypted. The connected IDS was capable of evaluating the HTTP-GET request from the malware.

Tests

3.7 Scenario 7: weak cipher suites

Requirements tested: 18, 19

Description: certain legacy clients only support weak cipher suites. The aim of this test is to verify whether the SSLV can block such connections, or even carry out an upgrade of the cipher suite on devices with weaker protection.





Handling of weak cipher suites	Result
Block	
Upgrade	

Note: it was possible to implement the blocking of weak cipher suites by creating a list of explicitly permitted cipher suites (once more we referred to the recommendations of the BSI [3]) and defining the catch-all policy as "Reject". According to the information provided by Blue Coat, the technical design of the SSLV prevents modifications to the cipher suite, meaning that neither upgrades nor downgrades can be carried out.

3.8 Scenario 8: invalid certificates

Requirements tested: 22, 23

Description: this scenario tested how the SSLV behaved when confronted with invalid certificates. As explained in the white paper [29], in such cases the user should be shown an appropriate warning.

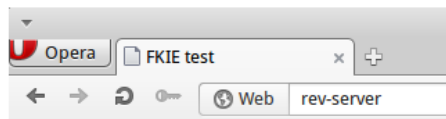
Reason why invalid	Result
Expired certificate	
Certificate valid in the future	
Neither CN nor SANs coincide with the requested domain	
Certificate revoked (OCSP)	

Note: in cases where the certificate had expired or was not yet valid, the user was correctly shown a warning. In such cases, the SSLV gave the correct warning that the certificate was invalid. The same was true for situations in which neither the common name nor the subject alternative name coincided with the requested host name. In the case of the revoked certificate, an Opera browser was used to establish an HTTPS connection to a web server. The certificate that had been used was revoked and this information was made available to the online certificate status protocol (OCSP). An OCSP request on the responsible server was recorded when opening the site without active SSLV, and the connection was no longer classed as secure. No OCSP request was recorded with active SSLV and so the HTTPS connection was classed as secure (cf. Figure 3). The

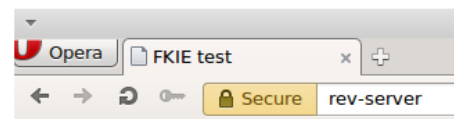
reason behind this seems to be that the part of the certificate containing the OCSP information is no longer available in the certificate issued by the SSLV.

As a matter of principle, the SSL TMITM application needs to remove the parts with the OCSP information from the original certificate, as the OCSP receiver would not accept a certificate that has been re-signed by the TMITM application as valid. Nevertheless, it is essential to protect the user from visiting websites with revoked certificates. This means the SSL TMITM needs to be capable of warning the client in case of revoked certificates, e.g. by transmitting the corresponding requests and answers via a proxy which takes on the role of CA.

Blue Coat commented on this issue and informed the authors that their SSLV would be able to present stapled OCSP responses to a client. The reason for Opera (or the SSLV) not initiating the OCSP check could not be clarified completely before the finalization of this whitepaper due to timing constraints.



This is our test page for the SSLV test.



This is our test page for the SSLV test.

Figure 3: website secured with OCSP. Left: no access without the SSLV; right: with the SSLV.

3.9 Scenario 9: Active-Inline test

Requirements tested: 20

Description: In this scenario, the SSLV is run in Active-Inline mode. Instead of a purely passive IDS, a Suricata instance was deployed. In this case, no decrypted SSL connections were blocked (cf. scenario 04).

In another test, an additional web content filter (Squid) was used to remove or prevent certain components and/or services on one website. As part of the test, JavaScript should be removed from all websites as an example.

Active components	Result
IPS (Suricata)	
Web content filter (Squid)	

Note: once the SSLV detects that the active security tool has discarded decrypted data or when the tool with a TCP reset indicates that malicious content has been found, it terminates the corresponding SSL flow. This prevents the malicious content reaching its destination. It is not possible at the moment, however, to modify packets, e.g. with Squid removing scripts.

3.10 Scenario 10: failsafe operation



Requirements tested: 26

Description: This test scenario simulates a failure in the SSLV. The aim is to test whether the failure results in all communications being interrupted, or whether it simply becomes impossible to continue inspecting SSL traffic.

The SSLV offers different modes in case of failure. Additionally, different policies can be defined in case of software errors, overload and when the appliance loses power. The

policies can basically be summarised into “allow all data” (where applicable, with or without forwarding to connected security appliances) and “block all data”. The test is limited to checking “Power-Off” mode. This involved disconnecting the power once with and once without “Power-Off Fail-To-Wire” active. It was checked whether communications between the client and server were possible.

 Tests







Mode	Expected	Result
Power-Off Fail-To-Wire active	Communication possible	
Power-Off Fail-To-Wire not active	No communication possible	









3.11 Limitations of SSL TMITM appliances

Scenarios in which decryption is not possible with any SSL TMITM appliance due to the characteristics of SSL were not tested. This includes, for example, setups with pre-shared keys in which the appliance does not have the corresponding key. Likewise, no scenarios were considered in which the client checks the certificate using fingerprints. In both cases, the appliance could not function as a TMITM with the current state of research.

The situation is the same for HTTP public key pinning (HKPK): TMITM is also generally not possible. One exception are scenarios in which web browsers (such as Firefox or Chrome) ignore the pinning if the verification of the certificate chain ends with a local trusted certificate authority (cf. [35] [36]). If the CA used to sign the certificates on the SSLV is on file on the client systems as a trusted CA, it is also possible to run a TMITM in these cases.

3.12 Test matrix

#	Requirement	Scenario	Result
1	Filtering according to source	05	
2	Filtering according to destination	05	
3	Selective forwarding		Not tested
4	Block lists and reputation databases	05	
5	Support for all relevant SSL/TLS versions		Not comprehensively tested
6	Support for relevant cipher suites	04	
7	Support for relevant cipher suite parameters		Not tested
8	Support for common protocols at a transport and network level	02	
9	Support for non-standard configurations	02	

Tests			
10	Application-independent handling	01, 02, 06	
11	Statistical data		Not tested
12	Low latency		Not tested
13	High throughput		Not tested
14	High numbers of connections per second		Not tested
15	High numbers of parallel connections		Not tested
16	Scalability		Not tested
17	No downgrading of cipher suites		Not tested
18	Blocking of weak cipher suites	07	
19	Upgrading of weak connections	07	
20	Accessibility to other products	09	
21	Multi-layer SSL	03	
22	CRLs and certificate blocking lists	08	
23	Invalid certificates	08	
24	Certificate pinning		Not tested
25	Warning message on decryption errors		Not tested
26	Reliability in case of errors or overload	10	
27	Patch management and updates		Not tested

Bibliography

- [1] IANA, 7 2015. [Online]. Available: <http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml>.
- [2] J. Oltsik, "Network Encryption and Its Impact on Enterprise Security," Enterprise Strategy Group, 2015.
- [3] J. W. Pirc, "SSL Performance Problems: Significant SSL Performance Loss Leaves Much Room for Improvement," 2013.
- [4] Z. Durumeric, E. Wustrow and J. A. Halderman, *Proc. of USENIX Security Symposium: ZMap: Fast Internet-wide Scanning and Its Security Applications*, 2013, Washington, D.C., USA.
- [5] J. Vehent, 1 2014. [Online]. Available: https://jve.linuxwall.info/blog/index.php?post/TLS_Survey.
- [6] Z. T. a. t. U. o. Michigan, 1 2015. [Online]. Available: <https://scans.io/>.
- [7] Z. A. Bahajji and G. Illyes, 8 2014. [Online]. Available: <https://googlewebmastercentral.blogspot.de/2014/08/https-as-ranking-signal.html>.
- [8] 1 2015. [Online]. Available: <https://letsencrypt.org/>.
- [9] Bundesgesetzblatt, 8 2009. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/bsiges2009_pdf.pdf?__blob=publicationFile.
- [10] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Migrationsleitfaden auf TLS 1.2 - Version 1.1," 2015.
- [11] 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, "Gewährleistung der Menschenrechte bei der elektronischen Kommunikation," 2014.
- [12] Qualys SSL Labs, 1 2015. [Online]. Available: <https://www.ssllabs.com/ssltest/clients.html>.
- [13] T. Duong and J. Rizzo, 5 2011. [Online]. Available: <http://www.hit.bme.hu/~buttyan/courses/EIT-SEC/abib/04-TLS/BEAST.pdf>.
- [14] N. J. AlFardan, D. J. Bernstein, K. G. Paterson, B. Poettering and J. C. N. Schuldt, 7 2013. [Online]. Available: <http://www.isg.rhul.ac.uk/tls/RC4biases.pdf>.
- [15] Codenomicon, 4 2014. [Online]. Available: <http://heartbleed.com/>.
- [16] Bundesamt für Sicherheit in der Informationstechnik (BSI), 4 2014. [Online].

- Available:
https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Heartbleed_Bug_16042014.html.
- [17] Debian.org, 5 2008. [Online]. Available: <https://www.debian.org/security/2008/dsa-1571>.
- [18] Trend Micro, 4 2013. [Online]. Available: <http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-campaign-hides-behind-ssl-communication/>.
- [19] abuse.ch, 1 2016. [Online]. Available: <https://sslbl.abuse.ch/>.
- [20] Venafi, "Are Cybercriminals Hiding in Your SSL Traffic?," 2015.
- [21] Cisco Systems Inc., "Cisco 2016 Annual Security Report," January 2016.
- [22] Cisco Systems Inc., "Hiding in Plain Sight: Malware's Use of TLS and Encryption," January 2016. [Online]. Available: <http://blogs.cisco.com/security/malwares-use-of-tls-and-encryption>.
- [23] J. Segura, 8 2015. [Online]. Available: <https://blog.malwarebytes.org/malvertising-2/2015/09/ssl-malvertising-campaign-targets-top-adult-sites/>.
- [24] J. Segura, 8 2015. [Online]. Available: <https://blog.malwarebytes.org/malvertising-2/2015/08/large-malvertising-campaign-takes-on-yahoo/>.
- [25] J. Segura, 8 2015. [Online]. Available: <https://blog.malwarebytes.org/malvertising-2/2015/08/ssl-malvertising-campaign-continues/>.
- [26] D. Schirmacher, 10 2015. [Online]. Available: http://www.heise.de/security/meldung/Malvertising-Kampagne-verteilt-Exploit-Kit-ueber-ebay-de-2853882.html?wt_mc=rss.security.beitrag.atom.
- [27] M. Rothman, "Security and Privacy on the Encrypted Network - Version 1.5," 2015.
- [28] J. M. Butler, "Finding Hidden Threats by Decrypting SSL," 2013.
- [29] R. Ernst and M. Lambertz, "Encrypted Traffic Management," 2015.
- [30] S. Piper, Encrypted Traffic Management For Dummies, 2015.
- [31] K. Scarfone, P. Hoffman and M. Souppaya, "Guide to Enterprise Telework and Remote Access Security (SP 800-46)," 2009.
- [32] S. Frank, P. Hoffman, A. Orebaugh and R. Park, "Guide to SSL VPNs (SP 800-113)," 2008.
- [33] Bundesamt für Sicherheit in der Informationstechnik (BSI), "TR-02102-2; Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2015-01," 2015.

- [34] Blue Coat System Inc., "Blue Coat Systems, Inc.: SSL Visibility Appliance Administration & Deployment Guide. Software: v 3.9.x.x," 2015.
- [35] The Chromium Projects, 1 2015. [Online]. Available: <http://www.chromium.org/Home/chromium-security/security-faq#TOC-How-does-key-pinning-interact-with-local-proxies-and-filters->.
- [36] Mozilla Developer Network and individual contributors, 1 2015. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/Security/Public_Key_Pinning.
- [37] T. Dierks, 5 2014. [Online]. Available: <http://tim.dierks.org/2014/05/security-standards-and-name-changes-in.html>.
- [38] I. Ristić, Bulletproof SSL and TLS, F. D. Ltd, Ed., London, 2015.
- [39] The Chromium Projects, 1 2015. [Online]. Available: <https://www.chromium.org/Home/chromium-security/security-faq>.
- [40] Mozilla Developer Network and individual contributors, 1 2015. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/Security/Public_Key_Pinning.