Poster – TLS Proxies: Friend or Foe?

Mark O'Neill, Scott Ruoti, Kent Seamons, Daniel Zappala
Brigham Young University
Computer Science Department
Provo, UT 84602
mto@byu.edu, ruoti@isrl.byu.edu, seamons@cs.byu.edu, zappala@cs.byu.edu

ABSTRACT

The use of TLS proxies to intercept encrypted traffic is controversial since the same mechanism can be used for both benevolent purposes, such as protecting against malware, and for malicious purposes, such as identity theft or warrantless government surveillance. To understand the prevalence and uses of these proxies, we build a TLS proxy measurement tool and deploy it via a Google AdWords campaign. We generate 2.9 million certificate tests and find that 1 in 250 TLS connections are proxied. The majority of these proxies appear to be benevolent, however we identify over 1,000 cases where three malware products are using this technology nefariously. We also find numerous instances of negligent and duplicitous behavior, some of which degrade security for users without their knowledge.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General - Security and protection

Keywords

TLS proxy; measurement; man-in-the-middle attack

1. INTRODUCTION

Communicating securely over the Internet requires authenticating the identity of a website to establish trust. Web browsers authenticate a site by validating a chain of trust from the site's certificate back to one of a set of trusted root certificates. These certificates comprise the root store and are typically bundled with the operating system or browser.

This validation system is currently being compromised by the use of TLS proxies, which can act as a man-in-the-middle (MitM) for TLS connections. Companies typically employ TLS proxies for benevolent reasons, particularly to protect intellectual property and to protect their network from intruders. Personal firewalls use similar techniques to protect users from malware and phishing attempts. Despite their benevolent uses, TLS proxies can also be used by a malicious entity to steal a user's private information, such as a credit card number, or by a government to snoop on encrypted traffic. The most dangerous aspect of TLS proxies is that the user is entirely unaware that encrypted traffic is being intercepted by an organization or attacker. Current browser software shows a reassuring lock icon during such sessions, which could lead most users to assume they are having a confidential conversation with the website. Essentially, in the name of providing increased security, TLS proxies have violated the authentication guarantees TLS was designed to create.

Although TLS proxies subvert the security of a TLS connection, little work has been done to characterize the prevalence and use of these proxies. Huang et al. measured the prevalence of TLS proxies using measurements deployed at Facebook [4], finding 0.20% of TLS connections are proxied, mostly by corporate Internet filters and personal antivirus software. In addition, a small number of connections were found to be intercepted by malware.

The focus of our research is to better understand the current uses of TLS proxies through a large-scale measurement of TLS proxies found in the wild. We have developed a tool to automatically measure the presence of TLS proxies, using the Flash runtime. Our method requires no user action and silently runs to determine whether a proxy is present whenever the user visits our web site. Using this tool, we conducted a measurement study of TLS proxies using a novel Google AdWords campaign. With this campaign, we automatically scan TLS connections when Google serves our ad, without any user involvement. Our study found 11,764 proxied connections out of 2.9 million total measurements (0.41% of all connections) spanning 142 countries. Most substitute certificates claim to be from benevolent TLS proxies, however we also found numerous instances of negligent and malicious behavior, affecting thousands of systems.

We developed our tool and conducted our measurement study independently and prior to Huang's publication [4]. The advantage of Huang's methodology is that they find proxies specifically targeting Facebook, whereas the advantage of our methodology is that we can collect results without the cooperation of a major website and find proxies that may have whitelisted Facebook or other high-profile sites. As compared to Huang, we find that TLS proxies are twice as common, we find some additional malware, we find evidence of spammers using TLS proxies, and we find that one parental filter weakens security for its users by opening them up to a MitM attack.

CCS'14, November 3–7, 2014, Scottsdale, Arizona, USA.
ACM 978-1-4503-2957-6/14/11.
http://dx.doi.org/10.1145/2660267.2662393.

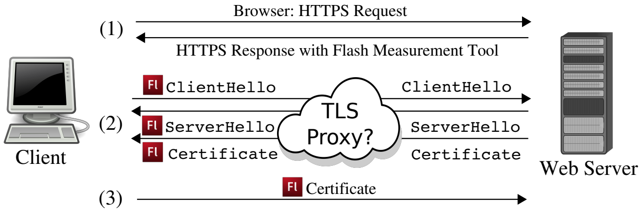

Figure 1: TLS Proxy Measurement

2. MEASUREMENT STUDY

We have developed a tool to measure the prevalence of TLS proxies using existing, widely-deployed technologies. The tool runs silently from the perspective of the user; no user action is required, either to install any software or to interact with the tool. This is a significant advantage as compared to other work that requires client-side software installation [6, 5, 1, 3, 2], since it enables us to quickly deploy our measurement tool and obtain millions of measurements within a week. We do not need to encourage users to adopt our tool in order to obtain measurements. The primarily limiting factor regarding how fast we collect data is the amount of money we wish to spend on Google's ad network.

Our tool detects TLS proxies in three steps, illustrated in Figure 1. We take advantage of the widespread deployment and transparency afforded by the Adobe Flash runtime. The Flash application runs without any user interaction and need not even be visible to the user. The application sends a `ClientHello` message to a TLS-enabled server and records the `ServerHello` and `Certificate` messages received in response. The retrieved certificates are then forwarded to the Web server, which compares the certificate received with the original sent and reports a mismatch as a TLS proxy.

To determine the prevalence and uses of TLS proxies, we conducted an advertising campaign using Google AdWords. We uploaded our tool as part of a Flash advertisement so that it runs automatically on any client that views our ad. Our advertising campaign ran from January 6, 2014 to January 30, 2014. During the duration of our ad campaign, we served 4.6 million ads and successfully completed 2.9 million measurements. In total we spent $5,101.88. Along with the certificate, we also recorded the IP address of the client tested. This IP address was then used to query the MaxMind GeoLite database to gather geolocation information. Of those tests, 11,764 returned a different X.509 certificate than was served by our secure web server, indicating the presence of a TLS proxy.

The proxies identified by our campaign originated in 142 countries and from 8,589 distinct IP addresses. Due to the targeting algorithms used by Google AdWords, our tool's exposure to these countries is not uniformly distributed. Connections from the United States and Brazil account for 36% of all proxies. Some countries have significantly higher percentages of proxied connections than the average, including France (1.09%), Canada (0.87%), Belgium (0.81%), the United States (0.79%), and Romania (0.74%).

2.1 Analysis of Issuer Organization

We first analyze the contents of the Issuer Organization in the substitute certificates we collected. We use OpenSSL to decode the certificates and store them in a database, where we can run queries. We also manually inspect the contents of the relevant fields to identify the issuing organization and their software products, using web searches to determine their identity. We emphasize that our results in this section are based on the intercepting proxy self-identifying themselves in the certificate. It is certainly possible that malicious proxies have hidden their tracks by masquerading as a legitimate organization in the Issuer Organization field, and we cannot detect this.

Rank	Issuer Organization	Connections
1	Bitdefender	4,788
2	PSafe Tecnologia S.A.	1,200
3	Sendori Inc	966
4	ESET spol. s r. o.	927
5	Null	829
6	Kaspersky Lab ZAO	589
7	Fortinet	310
8	Kurupira.NET	267
9	POSCO	167
10	Qustodio	109
11	WebMakerPlus Ltd	95
12	Southern Company Services	62
13	NordNet	61
14	Target Corporation	52
15	DigiCert Inc	49
16	ContentWatch, Inc.	42
17	NetSpark, Inc.	42
18	Sweesh LTD	39
19	IBRD	26
20	Cloud Services	23
	Other (332)	1,121

Table 1: Issuer Organization field values

Proxy Type	Connections	Percent
Personal Firewall	6,384	54.27%
Enterprise Firewall	463	3.94%
Personal/Enterprise Firewall	1,528	12.99%
Organization	1,448	12.31%
Malware/Spam	1,141	9.70%
Unknown	800	6.80%

Table 2: Classification of claimed issuer

Table 1 shows the values for the Issuer Organization field of the substitute certificates. Table 2 provides a breakdown of values present in the Issuer Organization field of the substitute certificates. The majority of certificates from proxied connections have an Issuer Organization field matching the name of a personal or enterprise firewall (71.2%). Another 12.3% have the name of an organization set as the Issuer Organization (e.g., Lawrence Livermore National Laboratory, Lincoln Financial Group). Additionally, 6.8% (800) of the substitute certificates have null values for the Issuer Organization field.

The most suspicious activities discovered were revealed by certificates with an Issuer Organization that matched the names of malware. “Sendori, Inc”, “WebMakerPlus Ltd”, and “IopFailZeroAccessCreate” appeared in 966, 95, and 21 Issuer Organization fields, respectively. Sendori poses as a legitimate enterprise, however they produce software that compromises the DNS lookup of infected machines, allowing them to redirect users to improper hosts. A TLS proxy component is used to bypass host authenticity warnings in the browser. The substitute certificates generated by the TLS proxy are signed by a root authority that was added to the root store of the local machine at the time of infection. Substitute certificates issued by Sendori originated from 30 distinct countries.

The WebMakerPlus malware is primarily associated with inserting advertisements into Web pages. Since modern browsers issue warnings when insecure content is queried from secure connections, we hypothesize that WebMakerPlus uses a TLS proxy to simulate that their advertisements are served from a secure connection. Substitute certificates containing markings for WebMakerPlus originated from 16 distinct countries.

Manual Internet queries revealed that malware was responsible for an Issuer Common Name field value of “IopFailZeroAccessCreate”. The certificates containing this value originated from 14 distinct countries. Disturbingly, each certificate contained the same 512-bit public key. This malware was also reported by [4].

In addition to malware discoveries, we found that the names of two companies highly associated with spam were also present in numerous Issuer Organization fields. The names “Sweesh LTD”, and “AtomPark Software Inc” were found in 39 and 20 substitute certificates, respectively. AtomPark offers tools for spammers including “email extractors” and “bulk mailers”. Sweesh offers services to spammers to overcome “hurdles” faced by advertisers and publishers. Internet searches reveal that Sweesh may be responsible for the development of WebMakerPlus.

2.2 Negligent Behavior

Where possible, we installed and characterized personal firewall software from many of the most common companies whose names were provided in the Issuer Organization, Issuer Organizational Unit, and Issuer Common Name fields of our collected certificates. We characterized the behavior of these solutions when running behind our own TLS proxy which issued certificates signed by an untrusted CA. While most solutions properly rejected our forged certificates, Kurupira, a parental filter that is responsible for 267 proxied connections in our dataset, did not. When visiting `google.com` and `gmail.com`, Kurupira replaced our untrusted certificate with a signed trusted one, thus allowing attackers to perform a transparent man-in-the-middle attack against Kurupira users without having to compromise root stores. In contrast, BitDefender not only blocked this forged certificate, but also blocked a forged certificate that resolved to a new root we installed in the victim machine’s root store.

Among the negligent behavior we found are TLS proxies that generate substitute certificates with weak cryptographic strength. Our original certificate has a public key size of 2048 bits. However, we find that 5,951 (50.59%) substitute certificates have public key sizes of 1024 bits and 21 certificates have public key sizes of 512 bits. 23 (0.20%) TLS proxies generated substitute certificates that used MD5 for signing, 21 (0.18%) which were also 512 bit keys. Interestingly, some TLS proxies generated certificates that have better cryptographic strength than our certificate. Seven (0.06%) used certificates with a key size of 2432 and five (0.04%) used SHA-256 for signing.

In addition to problems with cryptographic strength, we discovered that 49 (0.42%) substitute certificates claim to be signed by DigiCert, though none of them actually are. The original certificate from our secure web server is issued by DigiCert High Assurance CA-3, indicating the TLS proxy likely copied this field when creating the substitute.

Finally, we note that 110 substitute certificates have modifications to the subject field. For 51 (0.43%) certificates, the subject did not match our website’s domain. In many cases a wildcarded IP address was used that only designated the subnet of our website. In two cases the substitute certificate is issued to the wrong domain entirely: `mail.google.com` and `urs.microsoft.com`. These certificates appear to be legitimate for those domains and properly validate back to GeoTrust and Cybertrusts roots, respectively.

3. CONCLUSION

Using an automatic measurement tool and a Google AdWords campaign, we show that corporations and a surprising number of individuals are deploying proxies to protect against malware, phishing, and other undesirable practices. However, our study also shows that malware is using this same technique, comprising 9.70% of all proxied connections, and that spammers are using TLS proxies in their products. In some cases a personal firewall acting as a TLS proxy may weaken user security. Our analysis of the Kurupira parental filter finds that it masks forged certificates from an attacker, allowing the attacker to easily perform a MitM attack against the firewall’s users. We also find numerous other suspicious or negligent circumstances in substitute certificates, such as a null Issuer Organization, falsified DigiCert signatures, and downgraded public key sizes.

4. REFERENCES

[1] M. Alicherry and A. D. Keromytis. Doublecheck: Multi-path verification against man-in-the-middle attacks. In *14th IEEE Symposium on Computers and Communications (ISCC)*, pages 557–563. IEEE, 2009.

[2] B. Amann, M. Vallentin, S. Hall, and R. Sommer. Extracting certificates from live traffic: A near real-time SSL notary service. Technical report, TR-12-014, ICSI Nov. 2012, 2012.

[3] R. Holz, T. Riedmaier, N. Kammenhuber, and G. Carle. X.509 forensics: Detecting and localising the SSL/TLS men-in-the-middle. In *17th European Symposium on Research in Computer Security (ESORICS)*, pages 217–234. Springer, 2012.

[4] L.-S. Huang, A. Rice, E. Ellingsen, and C. Jackson. Analyzing forged ssl certificates in the wild. In *IEEE Symposium on Security and Privacy*, 2014.

[5] M. Marlinspike. SSL and the future of authenticity. *Black Hat USA*, 2011.

[6] D. Wendlandt, D. G. Andersen, and A. Perrig. Perspectives: Improving SSH-style host authentication with multi-path probing. In *USENIX Annual Technical Conference*, pages 321–334, 2008.