Profit loss for website administrators due to HTTPS misconfiguration

Tetsuya Okuda
NTT Secure Platform Laboratories
3-9-11 Midori-Cho,
Musashino-Shi, Tokyo, Japan
okuda.tetsuya@lab.ntt.co.jp

Koha Kinjo
NTT Secure Platform Laboratories
3-9-11 Midori-Cho,
Musashino-Shi, Tokyo, Japan
kinjo.koha@lab.ntt.co.jp

Kazuhiro Hayakawa
NTT Secure Platform Laboratories
3-9-11 Midori-Cho,
Musashino-Shi, Tokyo, Japan
hayakawa.kazuhiro@lab.ntt.co.jp

Toshinori Fukunaga
NTT Secure Platform Laboratories
3-9-11 Midori-Cho,
Musashino-Shi, Tokyo, Japan
fukunaga.toshinori@lab.ntt.co.jp

Ayako Hasegawa
NTT Secure Platform Laboratories
3-9-11 Midori-Cho,
Musashino-Shi, Tokyo, Japan
hasegawa.ayako@lab.ntt.co.jp

Mitsuaki Akiyama
NTT Secure Platform Laboratories
3-9-11 Midori-Cho,
Musashino-Shi, Tokyo, Japan
akiyama@ieee.org

Abstract

The adoption of HTTPS has spread worldwide; however, site misconfiguration can occur anywhere due to complicated Transport Layer Security (TLS) configuration.
We conducted a measurement study of HTTPS misconfiguration and a user study to explore user behavior when facing TLS warning messages. We reveal that 63.7% of the Alexa-Top 100K websites use HTTPS and 11.4% use HTTP Strict Transport Security headers; however, 9.0% use misconfigured HTTPS and may display TLS warning messages. The HTTPS adoption rate is positively correlated with website popularity, while the HTTPS misconfiguration rate is negatively correlated. Although TLS warnings are designed to warn users that a connection is not secure including websites, networks, and browsers, 64.0% of users tend to believe that *the cause of a TLS warning originates from just the website*. In addition, 35.0% of users attribute their decisions of not visiting websites to their “unfamiliarity”. As a result, users are motivated to switch to other websites, so website administrators may lose potential customers and profit.

Author Keywords

HTTPS adoption; HTTPS misconfiguration; TLS warning;

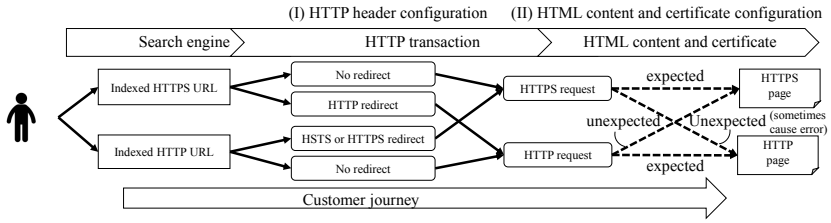

Figure 1: Diagram of customer journey to website

Table 1: HTTPS adoption rate (Alexa Top 100K Sites)

(I) HTTP header configuration	Adoption rate (%)
HTTPS	**63.7**
HTTPS redirect	47.1
HSTS	**11.4**
HSTS preload	2.5
HTTP	42.0
HTTP redirect	3.9

Table 2: Error rate (Alexa Top 100K Sites)

(II) HTML content and certificate configuration	Error rate (%)
TLS error	**9.0**
HTTP error	13.0

Table 3: Comparison of HTTPS adoption and error rates among Alexa Top 1K, 10K, and 100K Sites

(I) and (II) configurations	Top 1K (%)	Top 10K (%)	Top 100K (%)
HTTPS	**79.4**	71.5	63.7
HSTS	**30.2**	16.9	11.4
TLS error	3.4	5.5	**9.0**
HTTP error	7.1	10.2	**13.0**

ACM Classification Keywords

C.2.2 [COMPUTER-COMMUNICATION NETWORKS]: Network Protocols; H.5.m [INFORMATION INTERFACES AND PRESENTATION (e.g., HCI)]: Miscellaneous

Introduction

The adoption of HTTPS has spread worldwide [7]. A major change in Transport Layer Security (TLS) warning messages on browsers motivate a website administrator to adopt HTTPS. Chrome will display a “Not Secure” message in the address bar for all HTTP websites after July 2018 [11].

Since TLS warnings degrade user experience, previous studies have shed light on the root causes of TLS warnings [2][3] and user behavior when faced with such warning messages [10][4][6][12]. Incomplete HTTPS configuration may cause significant problems for website administrators [5][9] as well as end users; it degrades users’ motivation to access those websites, as a result, website administrators may lose potential customers and profit.

We addressed two research questions: (RQ1) How many properly configured and misconfigured HTTPS websites are there? and (RQ2) Why do TLS warning messages on a website degrade a user’s motivation to visit that website? To answer RQ1, we developed a tool to remotely validate HTTPS configurations and conducted a measurement study involving Alexa-Top 100K websites [1]. To answer RQ2, we conducted a user study to explore the reasons users do not visit websites when a TLS warning message is displayed, with reference to the study by Reeder et al. [10].

Our contributions are summarized as follows. Regarding RQ1, 63.7% of Alexa-Top 100K websites use HTTPS and 11.4% use HTTP Strict Transport Security (HSTS) headers [8]; however, 9.0% use misconfigured HTTPS and may display TLS warning messages. The HTTPS adoption rate is positively correlated with website popularity, while the HTTPS misconfiguration rate is negatively correlated. Regarding RQ2, although TLS warnings are designed to warn users that a connection is not secure including websites, networks, and browsers [2], 64.0% of users tend to believe that *the cause of a TLS warning originates from just the website*. In addition, 35.0% of users attribute their decisions of not visiting websites to their “unfamiliarity”. As a result, users are motivated to switch to other websites, so website administrators may lose potential customers and profit.

Our developed tool and measurement study

We shed light on HTTPS misconfiguration during the *customer journey* to/within a website (Figure 1). The connecting protocol can be changed by redirection or a hyperlink on the customer’s journey; however, if there are misconfigurations in these settings, sending an HTTP request on an HTTPS-adopted website and sending an HTTPS request on an HTTP-only website cause problems. In the former case, the customer has an unexpected HTTP connection and loses the secure channel. In the latter case, the customer has an unexpected HTTPS connection and receives a TLS warning even on a familiar site.

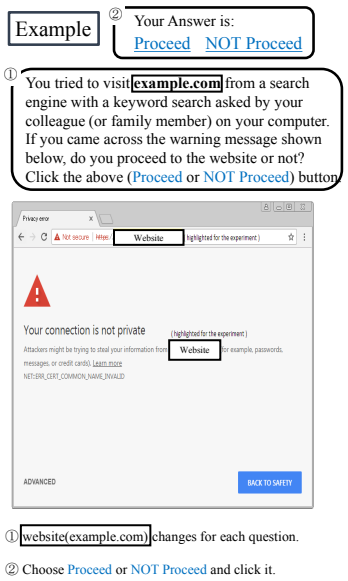

Figure 2: Questionnaire Example

Answers:
- Site: 64.0%
- Network: 36.0%
- Browser: 36.0%

Figure 3: (A) What do you think is the cause of the TLS warning? (multiple choices are allowed) (Choice order is randomized)

Our developed tool

We developed a tool to automatically aggregate the (mis) configuration of HTTPS on websites. The tool involves the following four analytical steps. (i) It first obtains a list of domains from Alexa Top Sites. (ii) To obtain the URL of a website under each domain, the tool retrieves accessible URLs from the search engine results by using the name of the domain as a search keyword and selects the first URL as the top page. (iii) It accesses a top page URL and collects its HTTP header, content, and certificate. It checks for errors, e.g., TLS verification error, HTTP status error, and timeout. It also checks setting information, e.g., HTTP redirect setting and HSTS headers. (iv) The tool outputs a report and statistics. Due to space limitation, the tool architecture will be detailed in our future work.

Measurement study

In 2018, we listed 100,000 domains of the Alexa-Top-Sites list and successfully established a connection with 91,928 websites on either HTTPS or HTTP. We summarize the results as follows.

(1) **HTTPS adoption rate** (Table 1):
(1-1) **HTTPS adoption**: As shown in Table 1, 63.7% (63,714) of websites served HTTPS, 47.1% (47,050) used an HTTPS redirect header, 11.4% (11,355) used an HSTS header, and 2.5% (2,519) used an HSTS preload header. If there is no redirect setting, an HTTP access, which a website administrator does not expect, may occur.
(1-2) **HTTP only**: As shown in Table 1, 42.0% (41,980) of websites served HTTP and did not redirect to HTTPS. When we connected to these websites on HTTPS, there were 3.9% (3,899) sites that were redirected to HTTP reconnection. Some of these sites belong to one of the most familiar IT vendors worldwide and news sites in Japan. It is assumed that HTTP redirect is considered easier than HTTPS adoption by some IT vendors. If there is no redirect setting, an HTTPS access, which a website administrator does not expect, may occur and cause errors.

(2) **Error rate** (Table 2):
(2-1) **TLS verification error**: As shown in Table 2, 9.0% (9,007) of websites had invalid certificates. Most of these were originally HTTP websites; however, they mistakenly opened HTTPS. If the pages were indexed as HTTPS on a search engine, unexpected error may occur for website administrators as well as end users. Due to space limitation, the details of these TLS verification errors and countermeasures will be discussed in our future work.
(2-2) **HTTP status error on HTTPS**: When the tool accesses on HTTPS to a website serving on HTTP, such as https://example.com/, it is expected to be redirected to http://example.com/. Nevertheless, as shown in Table 2, 13.0% (12,971) of websites just replied with an HTTP error status code. Most of these were originally HTTP websites; however, they mistakenly opened HTTPS. If the pages were indexed as HTTPS on a search engine, unexpected error may occur for website administrators as well as end users.

(3) **Comparison** (Table 3): We compared the adoption and error rates from relatively popular sites (Alexa top 1K) to those of other sites (Alexa Top 100K). As shown in Table 3, the HTTPS adoption rate positively correlated with website popularity, which is indicated by the Alexa Top Sites Rank [1], and the HTTPS misconfiguration rate negatively correlated with website popularity.

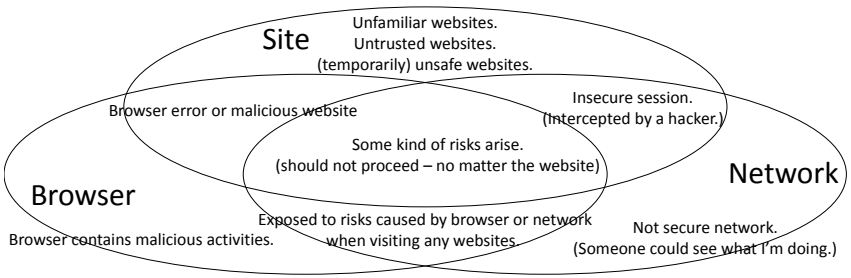

Figure 4: (B) Why did you not proceed? (representative answers)

Other answers:

Reason-"unsafe" websites:
(e.g., "insecure", "risk", "harm", "scared", "stolen", "compromised")

"I was scared to. I would look for the info elsewhere."

"Even if I was at minimal risk, I do not see it being worth it. I could use another site- or wait for them to fix the issue."

Reason-"unfamiliar" websites:
(e.g., "not known", "not heard of", "not recognized", "not visited", "untrusted")

"I chose not to proceed on certain sites because they were unfamiliar to me."

"I would not proceed if I had not previously visited the website or had never heard of the site before."

Figure 5: (B) Why did you not proceed? Describe your specific reasons.

User Study

Method

To understand why a TLS warning message on a website degrades a user's motivation, we conducted a user study for Chrome users recruited from a crowd sourcing service. There were a total of 210 responses. Participants were first given the following directions: *"You tried to visit a website from a search engine with a keyword search asked by your colleague (or family member) on your computer. If you came across the warning message shown below, do you Proceed or Not Proceed to the website?"* We repeatedly asked participants this question regarding ten websites, which were randomly extracted for each participants.

Next, we requested participants who selected "Not Proceed" on at least one website to answer multiple choice questions (Figure 3) and specify their reasons (Figure 5). There were 200 valid responses excluding "All Proceed" users. The choices were "Site", "Network", and "Browser", in accordance with the results by Acer et al. [2], and the choice order was randomized for each participant. The specific reasons were obtained using an open-ended question. Through a debriefing, participants are reminded again that the scenario in this survey is fictional and has nothing to do with the actual system behavior of the sites.

Results

(A) What do you think is the cause of the TLS warning?

As shown in Figure 3, they thought the cause of the warning was "Site" (64.0%), "Network" (36.0%), and "Browser" (36.0%). Although a TLS warning generally warns of a "connection" error including all the above [2], the cause most frequently assumed by participants was "Site". These participants recognized that TLS warnings in the wild are caused by site misconfiguration.

(B) Why did you not proceed? describe your specific reasons.

Representative answers are shown in Figures 4 and 5. Since the most common answer was "Site", 43.5% of the participants referred to keywords such as "(temporarily) unsafe" websites, and 35.0% of the participants referred to keywords such as "unfamiliar" websites in their answers (Figure 5). For website administrators, the answers of "(temporarily) unsafe" websites can mean that users can switch to another sites, causing loss of new and current customers. The answers of "unfamiliar" websites can mean that TLS warning caused loss of new customers, especially for less familiar sites.

Conclusion

Our study showed that 9.0% of the Alexa Top 100K Sites use misconfigured HTTPS and may display TLS warning messages, causing loss of potential customers. The HTTPS misconfiguration rate is negatively correlated with website popularity indicated by Alexa Top Sites Rank, and 64.0% of users tend to believe that *the cause of TLS warning is just the website* and 35.0% attribute their decision of not visiting websites to website "unfamiliarity". As a result, users are motivated to switch to other websites, so website administrators may lose potential customers and profit. Our results will motivate website administrators to adopt properly configured HTTPS.

REFERENCES

1. 2018. Alexa Top Sites (https://aws.amazon.com/alexa-top-sites/). (2018).
2. M. E. Acer, E. Stark, A. P. Felt, S. Fahl, R. Bhargava, B. Dev, M. Braithwaite, R. Sleevi, and P. Tabriz. 2017. Where the Wild Warnings Are: Root Causes of Chrome HTTPS Certificate Errors. In *CCS*. ACM.
3. D. Akhawe, B. Amann, M. Vallentin, and R. Sommer. 2013. Here's My Cert, So Trust Me, Maybe? Understanding TLS Errors on the Web. In *WWW*.
4. D. Akhawe and A. P. Felt. 2013. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *USENIX Security Symposium*.
5. S. Fahl, Y. Acar, H. Perl, and M. Smith. 2014. Why eve and mallory (also) love webmasters: a study on the root causes of SSL misconfigurations. In *CCS*. ACM.
6. A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes. 2015. Improving SSL Warnings: Comprehension and Adherence. In *CHI*. ACM.
7. A. P. Felt, R. Barnes, A. King, C. Palmer, C. Bentzel, and P. Tabriz. 2017. Measuring HTTPS Adoption on the Web. In *USENIX Security Symposium*.
8. J. Hodges, C. Jackson, and A. Barth. 2012. RFC 6797: HTTP Strict Transport Securit (HSTS). (2012).
9. K. Krombholz, W. Mayer, M. Schmiedecker, and E. Weippl. 2017. "I Have No Idea What I'm Doing" - On the Usability of Deploying HTTPS. In *USENIX Security Symposium*. ACM.
10. R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman. 2018. An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In *CHI*. ACM.
11. E. Schechter. 2018. Google Security Blog, A secure web is here to stay. (2018).
12. J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. 2009. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *USENIX Security Symposium*.