Incorrect HTTPS Certificate Validation in Samsung Smart TVs

Technical Report TUD-CS-2014-0802
Marco Ghiglieri
May 5, 2014
email: marco.ghiglieri@ec-spride.de

TECHNISCHE UNIVERSITÄT DARMSTADT

Computer Science
Security in Information Technology

CASED

EC SPRIDE

Zusammenfassung (in German)

Fernseher mit Internetfunktionalitäten, auch genannt Smart TVs, erhalten immer mehr Popularität und finden Einzug in fast jeden Haushalt. Einige dieser Geräte bieten über einen Web Browser die Möglichkeit im Internet zu surfen.

Dieser technische Bericht zeigt die Wichtigkeit von korrekt implementierten Sicherheitsfunktionen und deckt Sicherheitsmängel im Web Browser von Samsung Smart TVs auf. Dieses Problem bestand in der von Samsung veröffentlichten Serie E (Modelle aus 2012) und F (Modelle aus 2013). Samsung hat die Schwachstelle im April 2014 bei den genannten Modellen mit einem Update behoben. Die Schwachstelle besteht weiterhin bei Smart TVs mit der Bezeichnung UE55D6500.

Dieser Artikel verdeutlicht weiterhin die immer größer werdende Bedeutung einer durchdachten Updatestrategie auch für Smart Entertainment Geräte.

Abstract

TVs with Internet functionalities, which are commonly called Smart TVs, are gaining more and more popularity and can soon be found in every household. Some of these devices have integrated web browsers that enable consumers to browse the Internet.

This technical report shows how important correctly implemented security features are and uncovers security issues in web browsers on Samsung Smart TVs. These issues have been found on the E series (models from 2012) and F series (models from 2013) of the Samsung Smart TV devices. In April 2014 Samsung distributed a patch for these devices. The older model UE55D6500 (a 2011 model) still does not validate HTTPS certificates properly.

Furthermore, the work shows that a proper update strategy is becoming more and more important, even on smart entertainment devices.

1 Introduction

Nowadays, users can visit web sites on many devices, e.g., on desktop computers, smart phones, tablets or even on smart TVs. Some web sites provide only public content, which does not need to be encrypted, i.e., public content may be seen by every user visiting this web site. However, web sites with sensitive data like online banking or other customer relationship management sites have to be transported in a secure way. For example, passwords should never be sent in plain text over the Internet; they could easily be intercepted by a third party. The protocol used for transporting web sites to the end users in plain text is HTTP (Hypertext Transfer Protocol) and when encrypted it is HTTPS (Hypertext Transfer Protocol Secure).

1.1 HTTPS

Current web browsers on desktop and mobile devices are able to process HTTPS requests. HTTPS is technically HTTP transported over SSL/TLS (see [3]), so after decrypting the HTTPS stream the browser can handle the resulting traffic as HTTP data (see [2]). Thus, HTTPS should guarantee confidentiality and integrity transparently on the route to the user. In the best case the user does not need to take any other action than he/she would on an HTTP web site.

The encryption used for HTTPS is asymmetric; this means that the server has a private key and the client needs the server's public key to negotiate a symmetric key for HTTPS session initiation. An HTTPS certificate (SSL certificate or technically an X.509 certificate) is used to bind the public key to a specific subject, in this case a web server. The subject of an HTTPS certificate is usually the host name of the web server, e.g., ssl1.wsp.lab.sit.cased.de.

A registration authority (RA) is the entity that is responsible for the trusted binding of a specific subject to a public key. Before a certificate authority (CA) issues and cryptographically signs an HTTPS certificate, an RA must verify that the binding is legitimate, i.e., a trusted CA should never issue a certificate for which the legal owner of a host does not provide the public key. In order to ensure that only HTTPS certificates issued by trusted CAs are valid in web browsers, they are bundled with a list of trusted CAs. This shows that the validation of HTTPS certificates by the web browser is essential for the security of HTTPS. Without a trusted HTTPS certificate, a connection must be considered to be insecure. In this work, we will not discuss in detail how an HTTPS certificate is issued or validated correctly. Further information can be found in RFC 3280 [4].

The important part of an HTTPS certificate validation process is the presentation to the users. In web browsers, the user usually gets a lock symbol next to the address bar of the browser (see Figure 1). Current browsers on desktop PCs notify the user if a certificate is valid (1.1.1) or invalid (1.1.2).

1.1.1 Valid Certificates in Browsers

Figure 1 (b) shows a web site requested via HTTP and (a) a web site via HTTPS. Therefore, the green lock in the address bar of the browser clearly indicates a correct HTTPS connection, i.e., the HTTPS certificate is valid.

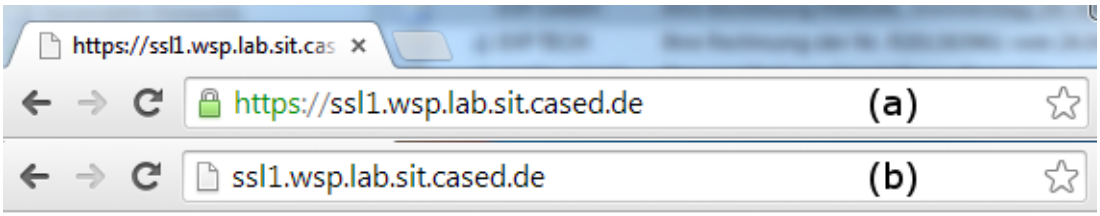

Figure 1: Google Chrome - (a) web site with valid HTTPS certificate; (b) web site with HTTP

The HTTP connection does not show the prefix **http://** nor a green lock symbol.

In both cases more information will be displayed when clicking on the symbol in front of the address. In the case of HTTPS the user can verify the certificate information presented. A manual HTTPS certificate check is possible by comparing the public key hash code; but end users do often not do this. The integrated automatic validation is performed with the trusted list of CAs and is updated regularly since a malicious CA could lead to a security problem. If a CA is not in the list, the certificate will not be marked as valid. However, users can always import their own certificates, which will then be considered to be secure only on their own system.

The list of trusted CAs for certificates can be found in the browser options. In mobile devices it is located in the main settings. This option is essential for users to see which certificate authorities are trusted.

1.1.2 Invalid Certificates in Browsers

There are different reasons why a certificate will be marked as invalid in the web browser. All current web browsers show a qualified warning in addition if a certificate is invalid. With this information the user can decide weather to trust the requested web site nevertheless.

Figure 2 shows two different cases: (1) the subject (web server) in the HTTPS certificate does not match with the web server delivering the web site and (2) the HTTPS certificate is not trusted because it has been self-signed. Both warnings notify the user that these requested sites are considered to be insecure. The address bar additionally strikes out *https* and the text color is changed to red. This indication will remain even if you click on *Proceed anyway*, so a user is always able to see if the page is considered to be secure.

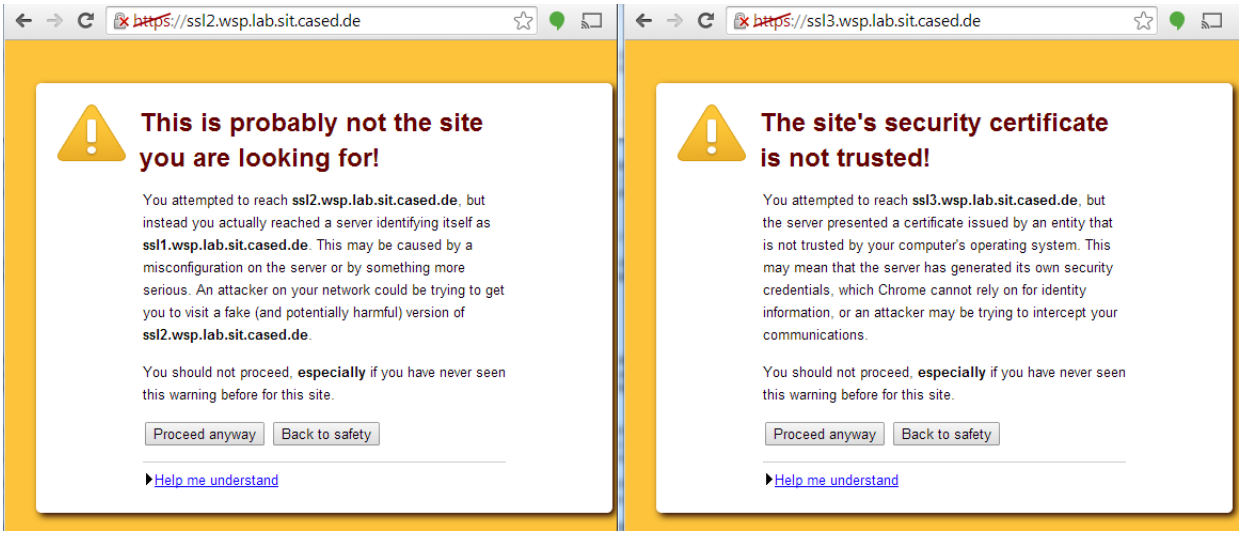

Figure 2: Google Chrome - both certificates are invalid for the specific host

In the past, some hackers had stolen valid CA certificates to create new HTTPS certificates for known web sites [5]. This led to a huge wave of revocations. If an attacker gets a valid certificate or gets the user to accept a wrong certificate, the attacker can collect sensitive data on a faked, so called phishing web site (see [1] for more details on that topic).

1.2 Smart Entertainment Devices

Smart entertainment devices like smart TVs, blu-ray players and set-top boxes are a new class of devices which often have an interface to connect to the Internet. Therefore, many of these devices can be used to browse the Internet via a web browser application. Currently, most of the basic applications cannot be replaced by third party apps. For example, on Samsung Smart TVs the web browser cannot be replaced by another browser. This may become possible in future devices.

We noticed that the current generation of web browsers on smart entertainment devices are light versions of browsers when compared to browsers known from desktop computers, i.e., functions that are commonly known from web browsers are not found for example on Smart TVs. For example we found no possibility to list the HTTPS certificates available on our Smart TVs. However, the functionality of HTTPS is implemented to execute web sites with sensitive data. Without HTTPS many web applications could not be used by consumers.

2 HTTPS on Smart TV

HTTPS on Smart TVs is used in many subsystems where secure updates or retrieval of data is needed. For example, firmware upgrades or login procedures should always be transported via HTTPS or at least encrypted and signed. If a malicious firmware upgrade can be installed on a device with microphone and camera, it can be converted into a spy device, which can secretly record audio and/or video. Thus, it is very important to have a minimum of security methods implemented.

The web browsers integrated on many Smart TVs can be used to browse the Internet like consumers know from a desktop computer. Since no HTTPS support in the web browser would directly break web sites, HTTPS is an essential part to give the consumers a desktop-like browse-feeling. In this work, we found on Smart TV models of the D,E and F series from Samsung that HTTPS certificates have always been marked as valid. Even invalid certificates have been shown as valid without any security warning. The test devices were UE55D6500, UE40ES6300 and UE46F6640. In all of them we found the same issue. As shown in Figure 3, a lock symbol was always displayed next to the address bar, so consumers had no chance to detect an invalid certificate. We directly communicated this issue to Samsung in October 2012.

The E and F series Smart TV models have been patched in April 2014 by an online update. This patch changed the behavior so that consumers get a warning like the one shown in Figure 4 (in German). This warning states that a

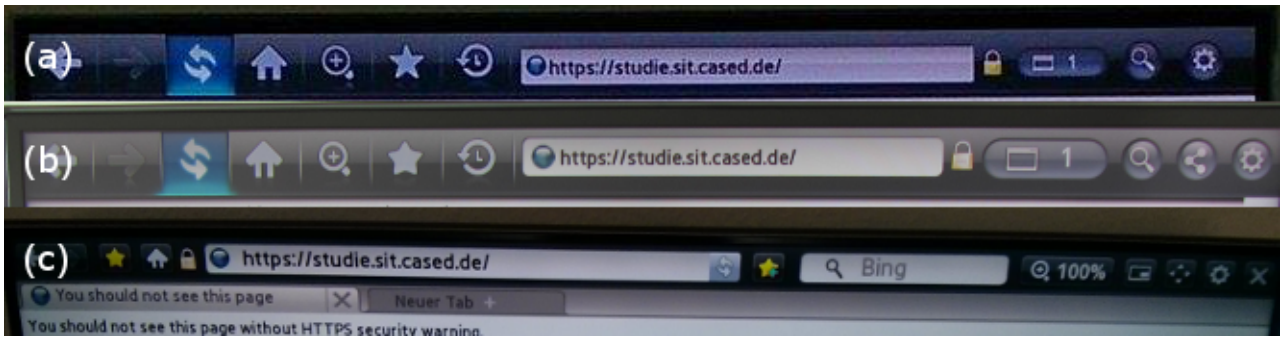

Figure 3: (a) UE55D6300 (b) UE40ES6300 (c) UE46F6640

problem with the HTTPS certificate has occurred, which is correct. However, ignoring this warning by using the button *open anyway* (*Trotzdem öffnen*, left button) presents the web site as a secure one to the consumer. The lock sign next to the address bar stil does not indicate an invalid certificate. It is very important that the consumer is aware that the Smart TV handles HTTPS connections that way.

The older D series model does still not warn consumers if a certificate is invalid, so consumers cannot directly see if the web site is trusted. It is unknown if a patch will ever be made available.

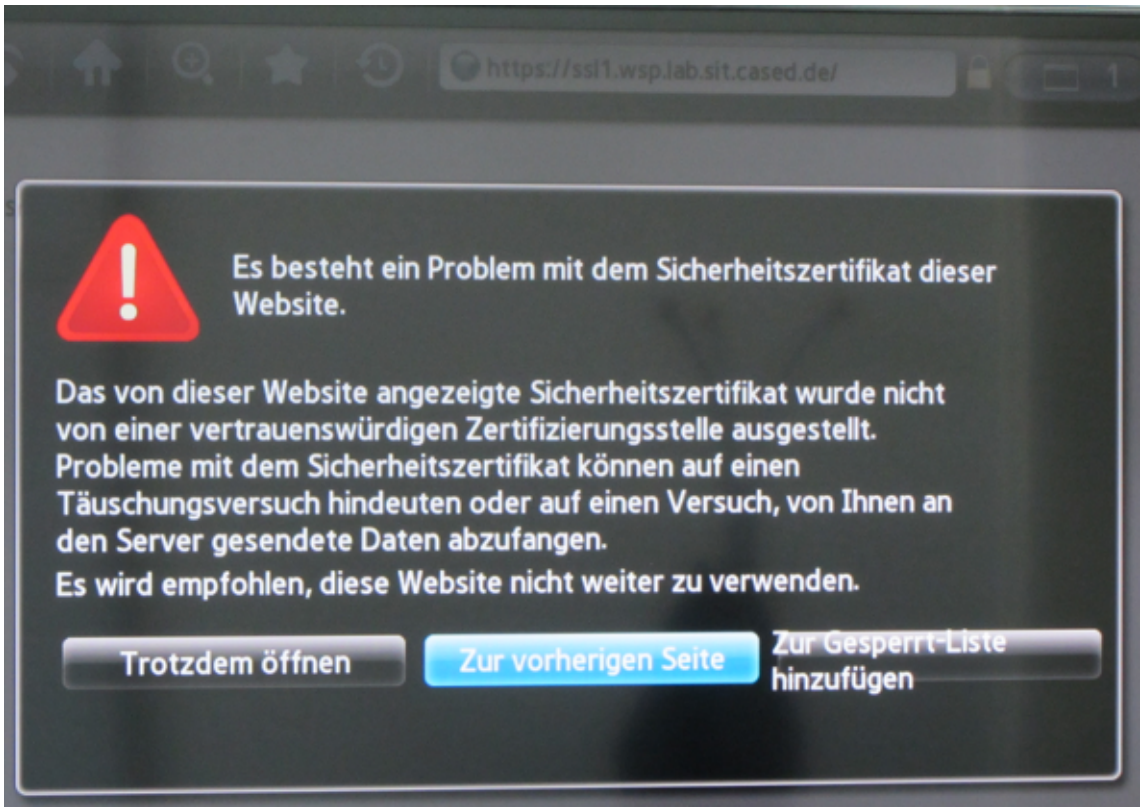

Figure 4: Security Warning on Samsung Smart TV UE40ES6300 (in German only)

For testing purposes we firstly set up a web site `https://studie.sit.cased.de`[1] which delivered an invalid HTTPS certificate to the web browser. The certificate has been issued for a different host name and so it should be handled as invalid in web browsers. In section 3 more URLs are listed that can be used to check a device.

Our tested Smart TVs have fewer functions to adjust the security level than a web browser on desktop computers. We found no option to display a list of HTTPS certificates that are trusted. Extensions and plugins could not be installed.

Conventional TVs were often rolled out but never updated. They did not need a security update since interfaces to other parties or the Internet were not available. Now it is very important, that smart TVs can be updated in a convenient

[1] This test case has been moved to `https://ssl2.wsp.lab.sit.cased.de`

way since consumers do not want to search and update manually, e.g., via USB or other devices. The best way for this is to automatically bring the update to the device over the Internet; especially security updates must be distributed fast and automatically. Usually It is not possible to develop software in such a way that an update will never be necessary.

3 How Can I Test My Device ?

We have configured three web sites which deliver different test cases for HTTPS validation. All web sites can be retrieved on any device having a web browser.

https://ssl1.wsp.lab.sit.cased.de
This is the only URL in the test cases that should be retrieved without any error. It provides a valid HTTPS certificate to the client, so the lock symbol should be displayed and no security warning shown.

https://ssl2.wsp.lab.sit.cased.de
This web site provides a valid certificate on a different host. In fact, we deployed the certificate from `https://ssl1.wsp.lab.sit.cased.de` on `https://ssl2.wsp.lab.sit.cased.de` which should lead to a security warning. Some browsers give reasons for the invalid certificate. Here, the web browser may mention that this is not the web site you are looking for (see Figure 2 left).

https://ssl3.wsp.lab.sit.cased.de
The HTTPS certificate on this web site is self-signed that means that the CA should not be in the trust list of web browsers. All other parameters like date or subject are valid. If you add the issuing CA to your browser it will validate the certificate correctly.

Some other cases where the certificate is valid but outdated were not checked in our test cases. However, in a more complete test environment these should be checked as well.

4 Conclusion and Outlook

In this work we showed that basic security techniques on desktop devices are becoming more and more important on Smart Entertainment devices. Soon Smart TVs will have processors like they are integrated in smart phones today. The software is becoming more complex and the abilities to connect to other devices increase. Hence, updates are essential and an appropriate update strategy must be developed before launching the product on the market. At the moment it is not conductive to harden software against all attacks, since it would lead to an undesired increase of product development effort. This is why important updates must be performed during the product lifetime. Consumers are increasingly putting a greater emphasis on a guaranteed time of support. For example, today's TVs are used for more than five years and have an even longer lifespan technically [6], so security updates for the devices should be provided for a while at least.

Furthermore, it is important that security updates can be provided easily. Updates via USB are not recommended for example, since many people would never update a TV this way. At the moment most consumers are not aware that security updates must be made even on smart entertainment devices, it is therefore very important to find the right measures so that the consumers can get familiar with them. On the other side, companies must test their smart devices for security and privacy as well since they directly affect a person's private life.

In our case, we communicated the issue to Samsung in October 2012. In April 2014 a patch was made available for some devices (E and F series). Hopefully, the D series will be patched soon as well, since our test model is only three years old.

Acknowledgments

We thank Florian Oswald, who wrote his Bachelor's thesis within the context of this project. Moreover, we thank Michael Waidner for his support to make this project possible. This work was supported by the European Center for Security and Privacy by Design (EC SPRIDE), funded by the German Federal Ministry of Education and Research (BMBF), and the Center for Advanced Security Research Darmstadt (CASED), funded by the LOEWE program of the Hessian Ministry for Science and the Arts (HMWK).

References

[1] BSI für Bürger. Phishing. `https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/phishing_node.html`, accessed on April 25,2014.

[2] Network Working Group. RFC2616 - HTTP/1.1, 06 1999. `https://tools.ietf.org/html/rfc2616`, accessed on April 24, 2014.

[3] Network Working Group. RFC2818 - HTTP Over TLS, 05 2000. https://tools.ietf.org/html/rfc2818, accessed on April 22, 2014.

[4] Network Working Group. RFC3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 04 2002. https://tools.ietf.org/html/rfc3280, accessed on April 25, 2014.

[5] Gregg Keizer. Hackers steal SSL certificates for CIA, MI6, Mossad, 09 2011. http://www.computerworld.com/s/article/9219727/Hackers_steal_SSL_certificates_for_CIA_MI6_Mossad, accessed on April 25,2014.

[6] Geoffrey Morrison. How long do TVs last? (Morrison's Mailbag), 02 2012. http://www.cnet.com/news/how-long-do-tvs-last-morrisons-mailbag/, accessed on April 26, 2014.