Trust me, I'm a Root CA!
Analyzing SSL Root CAs in modern Browsers and Operating Systems

Tariq Fadai, Sebastian Schrittwieser
Josef Ressel Center for Unified Threat Intelligence
on Targeted Attacks,
St. Poelten University of Applied Sciences, Austria
Email: [is101005,sebastian.schrittwieser]@fhstp.ac.at

Peter Kieseberg, Martin Mulazzani
SBA Research,
Austria
Email: [pkieseberg,mmulazzani]@sba-research.org

***Abstract*—The security and privacy of our online communications heavily relies on the entity authentication mechanisms provided by SSL. Those mechanisms in turn heavily depend on the trustworthiness of a large number of companies and governmental institutions for attestation of the identity of SSL services providers. In order to offer a wide and unobstructed availability of SSL-enabled services and to remove the need to make a large amount of trust decisions from their users, operating systems and browser manufactures include lists of certification authorities which are trusted for SSL entity authentication by their products. This has the problematic effect that users of such browsers and operating systems implicitly trust those certification authorities with the privacy of their communications while they might not even realize it. The problem is further complicated by the fact that different software vendors trust different companies and governmental institutions, from a variety of countries, which leads to an obscure distribution of trust. To give insight into the trust model used by SSL this thesis explains the various entities and technical processes involved in establishing trust when using SSL communications. It furthermore analyzes the number and origin of companies and governmental institutions trusted by various operating systems and browser vendors and correlates the gathered information to a variety of indexes to illustrate that some of these trusted entities are far from trustworthy. Furthermore it points out the fact that the number of entities we trust with the security of our SSL communications keeps growing over time and displays the negative effects this might have as well as shows that the trust model of SSL is fundamentally broken.**

***Keywords*-PKI, trust, CA**

I. Introduction

As users of modern browsers and operating systems we are heavily dependent on the security mechanisms integrated in these software products, in order to keep our data and communications private. The security of the online services we use in our daily lives heavily depends on the fact that the communication with these services is confidential, in order to protect our data from prying eyes. To achieve an acceptable level of security when using online services, in an era of mass surveillance, we therefore use SSL protected connections for exchanging sensitive data. However, we have to be aware of the fact that the confidentiality of SSL protected communications is dependent on the trustworthiness of various companies and governments. It is therefore of interest to find out which companies we implicitly trust just by using different operating system platforms or browsers. In this paper an analysis of the root certificates included in various browsers and operating systems is introduced. Our main contributions are:

- We performed an in-depth analysis of Root Certificate Authorities in modern operating systems and web browsers
- We correlated them against a variety of trust indexes in order to assess the trustworthiness of the countries represented by these Root Certificate Authorities

The remainder of this paper is organized as follows. In Section II we explain how various browsers and operating systems distribute the certificates of the trust anchors needed by SSL and analyze how many of those certificates exist in the different trust stores. Furthermore, it is analyzed from which countries these trusted certification authorities operate from and how many of these are owned by governmental institutions. In addition the number of trusted root certificates included in the current version of the Firefox web browser have been compared to the number included in previous versions. In Section III the country information gathered during the analysis is correlated against a variety of other indexes and the implications of the results of the conducted analysis are discussed. Finally, Section IV concludes the paper.

II. Root Certificate Programs

To get insight into the amount and type of organizations that users of popular software products such as web browsers and operating systems trust with the security of their private communications, a look at the trust stores of those products is needed. Since every software vendor manages the trusted certificates delivered with their products themselves, the amount of organizations that end users of those products trust by default may vary significantly between different browsers and operating systems. Most software vendors publish information on the Root CAs trusted by their product on their websites. Information on the requirements that need to be satisfied by CAs in order to become/stay a member of the software vendors Root CA Program is also available on those Websites and varies between different software vendors.

In the further course of this research the different mechanisms that operating system and browser vendors use to distribute lists of trusted root certificates, as well as options to access those have been analyzed. Then the trust stores of the following browsers and operating systems have been analyzed and compared by the number of certificates included, country of origin of certificate issuers as well as the amount of certificates owned by governmental institutions:

- **Browsers:** Apple Safari, Google Chrome, Microsoft Internet Explorer, Mozilla Firefox
- **Operating Systems:** Google Android Lollipop, Apple iOS 8 & Mac OS X Yosemite, Microsoft Windows & Windows Phone 8, Ubuntu 14.04.1 LTS

Furthermore, since the source code of all versions of Firefox is available on Mozilla's website, older Browser versions have been analyzed by the quantity of certificates included in their trust store and compared against the certificates included in the current release, to determine a possible trend in the quantitative growth and the lifetime of trusted root certificates in Mozilla's trust store.

Finally the findings regarding the originating Countries of Certificate Issuers are correlated against various other indexes such as the perceived levels of corruption, the levels of press freedom prevalent and the legal status of capital punishment in those countries to raise the question of the general trustworthiness of those countries.

A. Distribution of Trusted Root Certificates

iOS, Mac OS X & Safari

Apple products such as their web browser Safari and their Mail application use a common store for root certificates [3]. These certificates are installed by default on devices running them, hence they do not have to be downloaded.

In case of the OS X operating system a list of these certificates can be accessed via the integrated Keychain application. This list is also made available online [2]. For the iOS operating system, the same applies, except that users are not able to inspect the certificates included in the operating system. The only information provided in iOS 8 is the trust store version which can be found under the path *Settings -> General -> About -> Trust Store* as well as a link to the list of included root certificates [4]. It is worth mentioning that the number of certificates included in OS X and iOS differs even if only by a marginal amount.

Google Chrome & Android

The Google Chrome browser attempts to use the trust store of the underlying operating system [10] with the exception of Linux since no central root certificate program exists as part of the various Distributions. It therefore uses the Mozilla Network Security Services Library (NSS) which includes certificates vetted according to Mozilla's Root Certificate program.

Android however comes bundled with its own list of trusted Certificates but it has to be noted that the list may be further altered by device manufacturers. It was therefore only possible to analyze the trusted certificates included in the android source repository, which can be accessed online [11], in order to get a representative overview of androids trust store.

Internet Explorer, Windows & Windows Phone 8

Microsoft manages the distribution of root certificates in a single Program across Desktop and Phone devices [14], since the release of Windows Phone 8. Since the release of Windows Vista Microsoft also changed the way those root certificates are distributed. While previous Versions of Windows had a list of all trusted root certificates installed by default, which could be accessed using the certificate manager snap-in *certmgr.msc*, this is not possible in newer versions of Windows since root certificates are updated automatically [15] when needed by the Windows certificate chain verification software. Microsofts Browser Internet Explorer also utilizes the same trusted list of root certificates. A current list of all included root certificates can be found online [16].

Firefox

Mozilla maintains its own trust store for their products [18]. The default set of trusted root certificates is included in Mozilla's Network Security Services (NSS) which is a set of libraries that supports cross-platform development of security-enabled applications [19] and is part of Mozilla's products such as Firefox and Thunderbird. The source file including these trusted certificates is located in the following path of the Firefox source tree: */mozilla*/security/nss/lib/ckfw/builtins/certdata.txt*. The current source file [20] as well as a spreadsheet [17] containing information on all root certificates can be found online.

Ubuntu

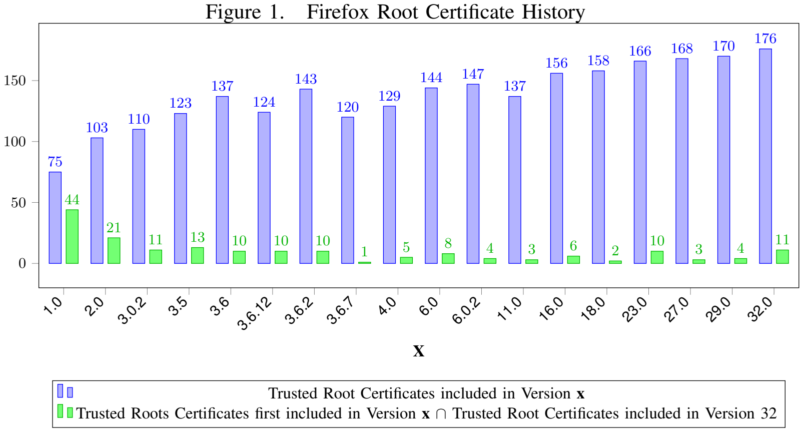
Ubuntu also includes its own list of trusted root certificates. The certificates are part of the package *ca-certificates* [6] which is a modified version [22] of the list included in Mozilla's NSS. The trusted root certificates are located in the following path of the filesystem: */usr/share/ca-certificates/*.

B. Comparison of Root CA Programs

The analysis of the certificates included in the trust stores of the previously mentioned browsers and operating systems has yielded the following results[1]. The Microsoft trust store contains by far the highest amount of trusted root certificates, almost twice as much as those included in the iOS trust store,

[1] Bermuda has been considered part of Great Britain, Hong Kong and Macao have been considered part of China in all statistics

Figure 1. Firefox Root Certificate History



which includes the second largest amount of trusted root certificates. It also includes the largest amount of distinct countries of certificate issuer origin and by far the highest amount of certificates owned by governmental institutions. Furthermore it includes more than twice as much root certificates owned by distinct governments than any other of the Root CA Programs it was compared to. It also represents 16 countries of certificate issuer origin that are not represented in any other Root CA Program of which the governments of 11 of those countries own a trusted root certificate in this program. The following is a list of the countries that are only represented in Microsoft's trust store:

- Australia, Brazil, Bulgaria, Chile, India, Lithuania, Luxembourg, Malaysia, Mexico, Portugal, Saudi Arabia, Serbia, Singapore, Slovenia, Tunisia, Uruguay

Other interesting observations were made while comparing the certificates contained in the iOS trust store to the ones contained in the OS X trust store. The iOS trust store includes three more trusted root certificates than OS X's. While two of these 3 certificates can also be found in other Root CA programs one particular, government owned root CA, sticks out since it is neither included in any other Root CA Program nor included in the OS X trust store: *U.S. Government ECA Root CA* (owned by the US Department of Defense). When comparing the trusted certificates included in Ubuntu another certificate unique to this trust store was found: *spi-inc.org Root CA* (owned by the SPI non profit organization). The complete statistics of the conducted analysis are illustrated in Figure 2.

C. *Firefox Certificate History*

To determine a possible trend in the quantitative growth and the lifetime of the certificates included in Mozilla's trust store, certificates included in previous versions of Firefox have been analyzed and compared against the ones present in version 32. In order to save time during the analysis the following methodology was applied: First a look at the published spreadsheet containing detailed information on the trusted certificates included in the current release was taken [17]. The information provided on when those certificates were first included in the trust store was then used to narrow down versions of interest. Then the source code of these versions was downloaded, the *certdata.txt* file contained in the source tree was extracted and subsequently analyzed, to determine the amount of certificates included in those versions. Finally the gathered information was cross checked against the certificates currently included in Firefox. Figure 1 illustrates the results[2] of the analysis. The results show that even though the number of root certificates trusted for server authentication purposes dropped on three occasions, the total development over time shows the trend is growth of the number of trusted root certificates. Furthermore they illustrate the longevity of certificates included in the Mozilla's Root CA Program between release versions. The majority of certificates currently included in Firefox's trust store (137 out of 176) was already included by the release of version 6.0.2 but the time elapsed between those releases is not too significant (roughly three years) considering the fact that the average validity period of the certificates included is about 23 years.

III. Correlation of Country Information with other Indexes

In order to get insight into as how trustworthy the various countries represented in the previously analyzed root CA programs can be perceived in general, the country information gathered was compared against the following indexes:

- **Corruption Perception Index:** The Corruption Perception Index is an annually released index that captures the informed views [27] of analysts, business people and experts from currently 175 different countries and territories in order to measure the perceived levels of public sector corruption present in those countries.

[2] Only certificates that are trusted for server authentication purposes were considered during the analysis

It is compiled by the Germany-based non-governmental institution Transparency International and scores countries on a scale from 0 (highly corrupt) to 100 (very clean). There is currently no country that scores a perfect 100.

- **Freedom on the Net Index:** The Freedom on the Net Index lists numerical ratings for 65 countries worldwide [9] [8] that were chosen to provide a representative sample with regards to geographical diversity and economic development, as well as varying levels of political and media freedom and aims to measure each country's level of internet and digital media freedom. It is published by the U.S.-based non governmental Institution Freedom House and examines the level of internet freedom by analyzing obstacles to access, limitations on content and the violation of user rights in those countries. Countries are scored from 0 (best) to 100 (worst), where countries with scores up to 30 are considered as having a "Free" internet and digital media environment, those with scores from 31 to 60 as "Partly Free" and those with scores higher than 60 as "Not Free".
- **World Press Freedom Index:** The World Press Freedom Index is an annually released report published by the French-based non-governmental non-profit organization Reporters Without Borders [23] and contains information about 180 countries [24] on the amount of freedom that journalists, news agencies and internet users enjoy in these countries, as well as the efforts made by the countries authorities to ensure respect for this freedom. Countries are scored from 0 (best) to 100 (worst).
- **Legal Status of Capital Punishment:** To determine the legality of Capital Punishment in the countries represented in the various Root CA Programs, Amnesty Internationals Death Sentences and Executions Report [1] was used. Any country that legally allows capital punishment, independent of the type of crime committed or the fact of actual executions practiced recently, has been considered in the comparison.

The results illustrated in Figure 3 show that all of the Root CA programs analyzed contain certificates originating from countries which are known to either have problems with public sector corruption, to respect press freedom or who actively censor the internet connections of their citizens. They even contain certificates originating from countries who legally violate the basic human right to life by employing the death penalty.

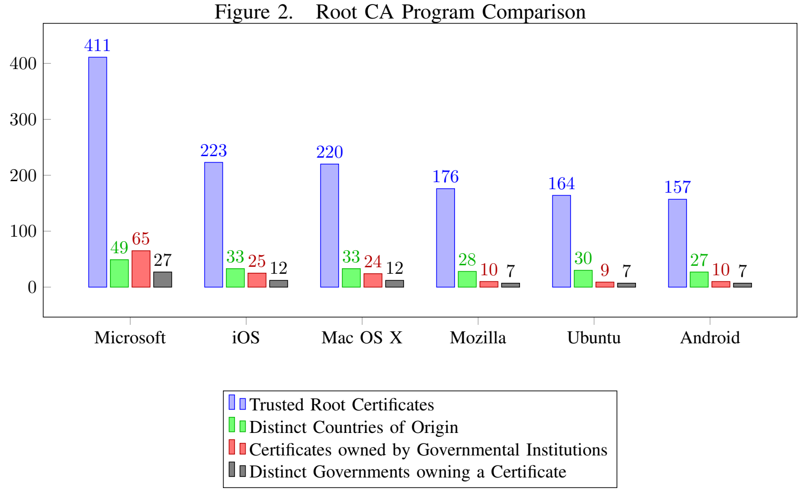
While multiple countries score bad on some of the considered indexes, the only two countries scoring bad on all indexes and employing the death penalty are Saudi Arabia and China. While the Saudi Arabian certificate authority is only present in Mircosoft's trust store, Chinese certificate authorities are present in every trust store analyzed.

A. *Implications*

As explained earlier the entire authentication model of the X.509 PKI utilized by SSL enabled browsers and operating systems is based on the unconditional trust in various certificate authorities which for some reason are trusted by application manufacturers. Therefore the entire security of the PKI is based on the security of the weakest link [7] in the infrastructure meaning that if a single CA [26] gets compromised, the entire authentication process of SSL can be subverted and has to be considered as potentially compromised, since an attackers would be able to issue trusted certificates to any domain of their choice, if they managed to steal the private keys of a trusted root certificate authority or an intermediate CA that chains up to a root trusted by the application manufacturers.

This property is also referred to as *weakest link property* [5] and to this day there have been multiple occurrences where intermediate CAs or in one instance even a root CA have been compromised, and forged certificates for high profile domains have been issued as a consequence of the security breach [5]. The previously conducted analysis showed that users of operating systems and browsers trust hundreds of such certificate authorities by default and the comparison of the analysis results to other research [12] [21] showed that not only the trust store of Mozilla's applications keeps growing, but also those of any other browser or operating system. This of course introduces even more weak links to the CA-based authentication model. Furthermore these trusted CAs and their subsidiaries are owned by a large number of companies [5] who operate from various countries and jurisdictions. Since ordinary users of applications that rely on SSL might not even be aware of the existence of certificate authorities, it is rather impractical to expect them to choose which of those companies or countries these CAs operate from they would like to trust with the ability to protect their sensitive data. Even more problematic is the fact that users of SSL enabled web services actually accept the relying party agreement [25] [7] of the CA that issued the SSL certificate to the provider of the web service, which contains a significant liability disclaimer to end-users that seeks to minimize the end-user's right to rely on the authentication process used by SSL. The user's consent is not asked during this process since he agrees to this liability disclaimer by just visiting a web service utilizing an SSL certificate issued by such a CA. The vendors of SSL-based application also face a hard decision [5] in case a trusted root CA gets compromised, since the removal of such an authority from their trust store would automatically invalidate all certificates issued by it and its intermediaries which could lead to the inaccessibility of a myriad of services for users

Figure 2. Root CA Program Comparison



of their applications. In case a really big CA (one that issued hundreds of thousand certificates) gets compromised, the application vendors might not be able to remove the trust in this authority since they would need to choose the availability of the affected services to the end user, over security, which would make the compromised CA *too big to fail*. Considering the fact that the majority of end entity SSL certificates is issued only by a minority [5] of the trusted CA's this scenario is not of hypothetical nature.

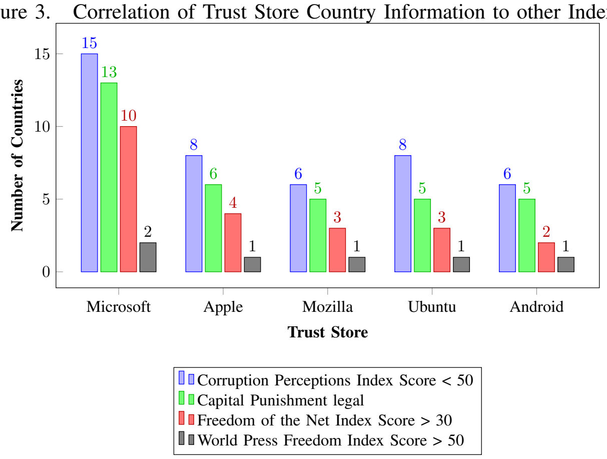
The fact that the root CAs included in the various trust stores analyzed are originating from a variety of countries, some of which might not be considered as trustworthy [25] when looking at the results of the correlation to other indexes made, introduces further problems. Also intermediate CA's created by those roots add some more countries to those results [5]. Even if assumed that all certificate authorities are totally secure and immune against security breaches by hackers, they are still bound to the legislature of the country they operate from. Since the governments of those countries have the legal power [28] [26] to allow their authorities to intercept the communication of their citizens and to legally retrieve communications data from service providers and other companies located in their country, even the best security practices can be subverted by them.

As a result of such legislation companies can be forced to assist local government authorities with the interception of communications traffic, and to provide infrastructure to facilitate such interception while withdrawing those companies the right to inform the public about the existence of such conduct or systems, by threatening them with punitive measures. A certificate authority therefore might be forced [26] by a governmental authority to hand over their signature key or to issue an intermediary CA certificate to such an authority. This is also referred to as *compelled certificate creation attack*.

It is important to understand that this gives the governments of any country a trusted root CA operates from the ability to perform man-in-the-middle attacks [13] on the otherwise encrypted communication of their citizens, which could lead to a total loss of the end users privacy. While this ability might only be exploited in emergency situations e.g. to avoid attacks on the security of their nation by some governments, oppressive regimes might use this ability to spy on the communication of political dissidents, which could result in serious, maybe even life threatening situations for those who were spied on.

While the analysis results displayed in Figure 2 might lead to the assumption that the government owned CAs included in the various programs would be used for such conduct other research argues [26] that this is unlikely since governments could compel another trusted certificate authority falling under their legislation to issue an intermediary CA certificate to them, without the risk of having the trust removed from their own CA or facing damages of reputation in case such an attack is noticed. Governments who don't have any other trusted root CAs than their own tangible in their jurisdiction might as well use their own CAs to issue fraudulent certificates. The growth of the trust stores analyzed is therefore very problematic since it equips more and more governments with the power to eavesdrop on the private communication of internet users over time. This is concerning especially since various countries have passed new legislation [8] enabling them to increase surveillance or restrict user anonymity in the last years. Additionally other researchers [21] have shown that every trust store that was analyzed in this work contains a number of certificates (in the case of Microsoft roughly a third of the included certificates) that were never used to issue SSL certificates and argue that they therefore only pose unnecessary risks for users of SSL-based applications.

Figure 3. Correlation of Trust Store Country Information to other Indexes



IV. Conclusions

This paper showed that users of modern operating systems and browsers, that utilize SSL, have to trust a large number of companies and governmental institutions with the privacy of their online communications, in order to have an unobstructed user experience, while using SSL-enabled services. It further highlighted that different software manufacturers include very different certificate authorities from a variety of countries in their trust stores and argued that some of these authorities might not be trustworthy considering their country of origin. This results in the unsatisfying situation that while the SSL trust model might protect a users privacy from ordinary attackers, it also enables government authorities to conduct large scale surveillance operations.

Acknowledgments

This work has been supported by the Austrian Research Promotion Agency under grant 846028 and COMET K1. The financial support by the Austrian Federal Ministry of Science, Research and Economy and the National Foundation for Research, Technology and Development is gratefully acknowledged.

References

[1] Amnesty International. Death Sentences and Executions 2013, 2013.

[2] Apple. OS X Yosemite: List of available trusted root certificates.

[3] Apple. Apple Root Certificate Program, 2014.

[4] Apple. iOS 8: List of available trusted root certificates, 2014.

[5] H. Ashgari, M. Van Eeten, A. Arnbak, and N. Van Eijk. Security Economics in the HTTPS Value Chain. In *The Twelfth Workshop on the Economics of Information Security (WEIS 2013)*, November 2013.

[6] Canonical. Information on package ca-certificates.

[7] C. Ellison and B. Schneier. Ten Risks of PKI: What You're not Beeing Told about Public Key Infrastructure. *Computer Security Journal*, 16(1):1 – 7, 2000.

[8] Freedom House. Freedom on the Net Report - Summary of Findings, 2014.

[9] Freedom House. Freedom on the Net Report 2014 - Methodology, 2014.

[10] Google Inc. Google Chrome Root Certificate Policy.

[11] Google Inc. Root Certificates Included in current Android release (Source), 2014.

[12] R. Holz, L. Braun, N. Kammenhuber, and G. Carle. The SSL Landscape: A Thorough Analysis of the x.509 PKI Using Active and Passive Measurements. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, IMC '11, pages 427–444, New York, NY, USA, 2011. ACM.

[13] L. S. Huang, A. Rice, E. Ellingsen, and C. Jackson. Analyzing Forged SSL Certificates in the Wild. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*. IEEE, 2014.

[14] Microsoft Corporation. Windows and Windows Phone 8 SSL Root Certificate Program (Member CAs).

[15] Microsoft Corporation. Microsoft Root Certificate Program, January 2009.

[16] Microsoft Corporation. Windows Root Certificate Program Members, September 2014.

[17] Mozilla Corporation. Mozilla Built In Certificate Authorities.

[18] Mozilla Corporation. Mozilla CA Certificate Policy V2.2.

[19] Mozilla Corporation. Network Security Services.

[20] Mozilla Corporation. Mozilla Cross-Reference - Source of certdata.txt, 2014.

[21] H. Perl, S. Fahl, and M. Smith. You Won't Be Needing These Any More: On Removing Unused Certificates From Trust Stores. In *Financial Cryptography and Data Security 2014*, 2014.

[22] Philipp Kern. Copyright of package ca-certificates.

[23] Reporters without Borders. World Press Freedom Index '14.

[24] Reporters without Borders. World Press Freedom Index - Methodology, 2014.

[25] S. B. Roosa and S. Schultze. The "Certificate Authority" Trust Model for SSL: A Defective Foundation for Encrypted Web Traffic and a Legal Quagmire. *Intellectual Property & Technology Law Journal*, 22(11):3 – 8, November 2010.

[26] C. Soghoian and S. Stamm. Certified Lies: Detecting and Defeating Government Interception Attacks against SSL. In *Financial Cryptography and Data Security*, volume 7035 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2012.

[27] Transparency International. Corruption Perceptions Index, 2014.

[28] Vodafone Group Plc. Sustainability Report 13/14, 06 2014.