International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 24th Feb 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-02

Title: **DIGITAL CERTIFICATE VERIFICATION BY USING RISK ASSESMENT**

Volume 08, Issue 02, Pages: 69–73.

Paper Authors

MR.K.SRINIVASA RAO, B.ANIL KUMAR

Vignan's Lara Institute of Technology & Science

International Journal for Innovative Engineering and Management Research ★

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

DIGITAL CERTIFICATE VERIFICATION BY USING RISK ASSESMENT

MR.K.SRINIVASA RAO[1], B.ANIL KUMAR[2]
Assistant Professor[1], Department of M.C.A ,Vignan's Lara Institute of Technology & Science
M.C.A Student[2],Department of M.C.A ,Vignan's Lara Institute of Technology & Science

Abstract:

Digital certificates, based on X.509 PKI standard, are located at the core of many security mechanisms implemented in services and applications. However, the usage of certificates has revealed flaws in the certificate validation process (e.g., possibility of unavailable or non-updated data). This fact implies security risks that are not assessed. In order to address these issues that such flaws entail, we propose a novel probabilistic approach for quantitative risk assessment in X.509 PKI, together with trust management when there is uncertainty. We have evaluated our risk assessment approach and demonstrated its usage, considering as a use case the secure installation of mobile applications. The results show that our approach provides more granularity, appropriate values according to the impact, and relevant information in the risk calculation than other approaches

Introduction

A LARGE number of applications and services base core parts of their security on X.509 digital certificates (PKCs, Public Key Certificates). They enable secure HTTPS communications, encrypted Virtual Private Network (VPN) tunnels, and code signing for secure software installation, among others. Hence, protection critically depends on whether certificates are correctly validated, which includes checking that they and the associated certification chain are trusted, non-revoked, unexpired, with valid signatures and deployed on proper domains and for the right purpose. Recent studies however have unveiled that the state of Public Key Infrastructure (PKI) deployment is far from perfect.Similarly, the study performed in [2] showed that an 68.8% of HTTPS connections from 20 well-known CDN (Content Distribution Network) providers had invalid certificate warningsandthe studyperformedin [3] demonstratedthat more than an 8% of certificates used by commercial servers (i.e., about 38,5 millions of IPv4 HTTPS certificates) are revoked. But even if these errors exist, clients are frequently not rigorousin the validationprocess and currentinterfaces fail to provide effective information to end-users [4], which leads to exploitable vulnerabilities. According to [3], no browser in its default configuration checked all revocations or rejected certificates if current revocation information was not available. The situation is even worse with mobile browsers or application delivery managers, as they state [3]: “not one of the major mobile browsers checked to see if a certificate was valid or had been revoked”. Another issue is that the checks to be conducted when validating a certificate are static and output binary values. This means that e.g., if the Certificate Authority (CA) signing the certificate under validation is trusted (configuredas such), then the certificateis also trusted,otherwiseit is nottrustedand thus invalid. Revocation works in a similar way: if the certificate is not contained in a revocation list, the check is positive. But if it is revoked or information cannot be gathered, then the PKC is considered not valid. Thus, it can be seen that lack of information is treated as certainty of negative information, and trust is still based on static pre-configuration. Indeed, incidents as the DigiNotar’s security breach, which resulted in the fraudulent issuing of certificates [5], and for which there are no effective implemented countermeasures yet [6], reveal the unsuitability of static trust anchor lists. Trust evolves and should be managed: we cannot be sure about the liability of a CA, that we now trust, in the near future. Even if the CA organization acts as a fair CA at the beginning, this does not mean that the organization will stay honest or will not suffer a breach. Many proposals in the literature have demonstrated the importance of using trust managementfor enhancingsecurity in distributed and dynamic environments [7]–[9] and [10]. All these issues can be tackled using Security Risk Assessment (SRA) [11], which involves risk identification, analysis and evaluation. We propose a probabilistic SRA solution . for digital certificate validation together with dynamic trust management, called RiskLaine. Our solution allows users to determine the faced risks posed by a particular certificate at usage time. RiskLaine can be applied to enhance several scenarios wherecertificate-baseddecisions must be performed: • security in communications is a critical scenario, where digital certificates are commonly used for authentication, encryption and key exchange. In the HTTPS scenario, for example, secure websites often involve links to nonsecure elements from remote sites. The validation in this case results in “warning” messages that may confuse users. Risk quantification can help in making educated decisions upon transactions over a connection secured with certificates. • secure installation of mobile applications is another significant scenario, given the continuously growing size of app markets and the increasing interest it has attracted from all sectors. There is a risk when mobile applications signed with certificates are installed by users [12]–[15], because they do not know if the downloaded app is authentic and trusted. Hence, risk quantification can aid in better decision making. The rest of the paper is organized as follows. In Section II we describe our SRA approach, explaining how risks are identified, the metrics defined for quantitative analysis, and an overview of the risk evaluation process. Two main components are formulated as part of the general risk computation: risk probability on PKI, and risk probability on trust. Accordingly, the detailed calculus of both probabilities is given in Sections III and IV. Section V describes how to calculate the impacts associated to these risk probabilities. Next, in Section VI, we evaluate our approach using the scenario of mobile applications installation, in order to show how risk could be computed and applied for decision making. We performed evaluation using two different impact frameworks, and we also compared our approach with risk computation tools in the literature

Existing system:

X.509 digital certificates (PKCs, Public Key Certificates). They enable secure HTTPS communications, encrypted Virtual Private Network (VPN) tunnels, and code signing for secure software installation, among others. Hence, protection critically depends on whether certificates are correctly validated, which includes checking that they and the associated certification chain are trusted, non-revoked, unexpired, with valid signatures and deployed on proper domains and for the right purpose. Recent studies however have unveiled that the state of Public Key Infrastructure (PKI) deployment is far from perfect. Most failures were due to domain mismatch, followed by untrusted and expired certificates. Similarly, the study performed in [2] showed that an 68.8% of HTTPS connections from 20 well-known CDN (Content Distribution Network) providers had invalid certificate warnings and the study performed in [3] demonstrated that more than an 8% of certificates used by commercial servers (i.e., about 38,5 millions of IPv4 HTTPS certificates) are revoked.

Proposed system:

All these issues can be tackled using Security Risk Assessment (SRA), which involves risk identification, analysis and evaluation. We propose a probabilistic SRA solution for digital certificate validation together with dynamic trust management, called RiskLaine. Our solution allows users to determine the faced risks posed by a particular certificate at usage time. RiskLaine can be applied to enhance several scenarios where certificate-based decisions must be performed

Modules:

Conduction Risk Assesment

Risk assessment is made up of three sub-processes, namely: risk identification, risk analysis, and risk evaluation. In the following, we detail how RiskLaine covers these three aspects as defined in ISO 31000

Risk Identification

The starting point for SRA is determining which are the applicable risks considering the scope of the assessment and clarifying the assumptions under which the assessment is conducted. In our case, the scope is the procedure of certificate validation. Furthermore, we assume a flexible PKI validation model where: 1) the PKI validation checks are not binary and its value can be probabilistically estimated depending on the available information; and 2) apart from the PKI preconfigured trust on CAs, behavioural trust is also evaluated, taking continuous values calculated using a dynamic trust management approach.

Risk Analysis

Risk analysis is a process that is used to understand the nature, sources, and causes of the risks previously identified and to estimate the associated level of risk.

Risk Evaluation

Risk evaluation is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable.

Probability Calculation on PKI

In this section, we calculate the uncertainty associated to the PKI processes that could have an influence on security risks (*Ppki (t)*), as explained above. As shown in Figure 1, this probability value will be estimated based on metrics M2, M4 and M6, which are built on certificate,revocation and time information.

Root CA Uncertainty

Following the traditional PKI binary behaviour, if a root CA is considered trusted by users (i.e., by pre-configuration), uncertainty on the root is 0. This is the case for example in web scenarios, where root certificates are installed by web browser companies and considered trusted by default. On the contrary, if a root is unknown by users, uncertainty is maximum and equal to 1, and the root is considered untrusted.

Revocation Uncertainty

In order to calculate the probability that a certificate is revoked (M4), we consider three different situations quantified in equation 9: 1) the relying party (RP) has no revocation data, 2) RP has revocation data and the certificate is not revoked, and 3) RP has revocation data and the certificate is revoked.

Conclusion:

We can concludethat, thoughthere is no global solution that can avoid any security breach related to certificate trust and validation features, risk assessment can help in significantly reducing these breaches. Our solution can be used for this purpose in several ways, which will be the subject of future research: 1) as an integrated component in smartphone operating systems or web browsers that shows risk information to the users for better decision-making; 2) as a tool that runs real-timerisk assessments in the backgroundandautomatically triggers different countermeasures depending on the risk-level, e.g., blocking a website or preventing installation of risky apps; or 3) as a complement to other security controls, e.g., used in combination with security policies in Mobile Device Management systems. Finally, based on the described findings, a research roadmap for enhancing risk assessment in certificate-based security should cover the following aspects: automation of tools for risk computationandits integrationwith user interfaces, adaptability to different certificate-based scenarios, mechanisms for gathering information for risk computation both online and offline, study of additional risk factors, and analysis of the suitability of different impact quantification frameworks.

References

1. N. Vratonjic, J. Freudiger, V. Bindschaedler, and J.-P. Hubaux, "The inconvenient truth about web certificates," in Economics of Information Security and Privacy III. New York, NY, USA: Springer, 2013, pp. 79–117.

2. J. Liang, J. Jiang, H. Duan, K. Li, T. Wan, and J. Wu, "When HTTPS meets CDN: A case of authentication in delegated service," in Proc. 35th IEEE Symp. Secure. Privacy, San Jose, CA, USA, May 2014, pp. 67–82.

3. Y. Liu et al., "An end-to-end measurement of certificate revocation in the Web's PKI," in Proc. ACM Internet Meas. Conf., Oct. 2015, pp. 183–196.

4.D. Akhawe and A. P. Felt, "Alice in warningland: A large-scale field study of browser security warning effectiveness," in Proc. 22nd USENIX Conf. Secur., Aug. 2013, pp. 257–272.

5. N. Leavitt, "Internet security under attack: The undermining of digital certificates," Computer, vol. 44, no. 12, pp. 17–20, Dec. 2011.

6. J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, and R. Holz, "Mission accomplished: HTTPS security after diginotar," in Proc. Internet Meas. Conf. (IMC), London, U.K., Nov. 2017, pp. 325–340

7. O. Khalid et al., "Comparative study of trust and reputation systems for wireless sensor networks," Secur. Commun. Netw., vol. 6, no. 6, pp. 669–688, Jun. 2013. [Online]. Available: http://dx.doi.org/ 10.1002/sec.597 8.J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Commun. Surveys Tuts., vol. 13, no. 4, pp. 562–583, 4th Quart., 2011.

9. F. Almenarez, M. F. Hinarejos, A. Marín, J.-L. Ferrer-Gomila, and D. D. Sánchez, "PECEVA: An adaptable and energy-saving credential validation solution for pervasive networks," Inf. Sci., vol. 354, pp. 41–59, Aug. 2016.

10. Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," J. Netw. Comput. Appl., vol. 42, pp. 120–134, Jun. 2014.

11. G. Purdy, "ISO 31000:2009—Setting a new standard for risk management," Risk Analysis, vol. 30, no. 6, pp. 881–886, Jun. 2010.

12. L. Davi, A. Dmitrienko, A.-R. Sadeghi, and M. Winandy, "Privilege escalation attacks on Android," in Proc. Int. Conf. Inf. Secur. (ISC), Oct. 2011, pp. 346–360.

13.S. Bugiel, L. Davi, A. Dmitrienko, T. Fischer, and A.-R. Sadeghi, "XManDroid: A new Android evolution to mitigate privilege escalation attacks," Center Adv. Secur. Res. Darmstadt, Tech. Univ. Darmstadt, Darmstadt, Germany, Tech. Rep. TR-2011-04, Jun. 2011.

14. P. P. Chan, L. C. Hui, and S. M. Yiu, "Droidchecker: Analyzing Android applications for capability leak," in Proc. 5th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WISEC), Apr. 2012, pp. 125–136.

15. M. Rangwala, P. Zhang, X. Zou, and F. Li, "A taxonomy of privilege escalation attacks in Android applications," Int. J. Secur. Netw., vol. 9, no. 1, pp. 40–55, Feb. 2014.