International Journal of Research in Advent Technology, Vol.7, No.2, February 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Risk in Certificate based Security including both Revocation Factors and Behavioral Trust Management

Dr.R.Murugadoss , Mogal.UmeraJasmine
Professor, St.Ann's College Of Engineering& Technology,chirala.
PG Scholar, St.Ann's College Of Engineering & Technology, Chirala.

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. 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.

Keywords: Risk assessment, certificate validation, trust management, X.509 PKI, mobile applications.

1. INTRODUCTION

Large number of applications and services basecore parts of their security on X.509 digital certificates. They enable secure HTTPScommunications, encrypted Virtual Private Network (VPN)tunnels, and code signing for secure software installation,among others. Hence, protection critically depends on whethercertificates are correctly validated, which includes checkingthat they and the associated certification chain are trusted,non-revoked, unexpired, with valid signatures and deployedon 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.According to the empirical results in [1], only 16% ofthe top one million most popular websites implementedcertificate-based authentication properly. Most failures weredue to domain mismatch, followed by untrusted and expiredcertificates. Similarly, the study performed in [2] showed thatan 68.8% of HTTPS connections from 20 well-known CDN(Content Distribution Network) providers had invalid certificatewarnings and the study performed in [3] demonstrated thatmore than an 8% of certificates used by commercial servers(i.e., about 38,5 millions of IPv4 HTTPS certificates) arerevoked.Revocation works in a similar way: if the certificateis not contained in a revocation list, the check is positive. Butif it is revoked or information cannot be gathered, then thePKC is considered not valid. Thus, it can be seen that lackof 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, whichresulted in the fraudulent issuing of certificates [5], and forwhich there are no effective implemented countermeasuresyet [6], reveal the unsuitability of static trust anchor lists.

Trust evolves and should be managed: we cannot be sureabout the liability of a CA, that we now trust, in the nearfuture. Even if the CA organization acts as a fair CA atthe beginning, this does not mean that the organization willstay honest or will not suffer a breach. Many proposals in
the literature have demonstrated the importance of using trustmanagement for enhancing security in distributed and dynamicenvironments [7]–[9] and Kumar at el. [10]show another rich code that has two stockpiling levels and can be used for record affirmation. This earlier code, named as two levels code, can open and private stockpiling levels.Individuals when all is said in done level is the same as the standard code stockpiling level, along these lines it is fathomable by any settled code application. The private level is worked by supplanting the dull modules by specific completed illustrations. It contains information encoded using question code with a mix-up change constrain.All these issues can be tackled using Security Risk Assessment(SRA) [11], which involves risk identification, analysisand evaluation. Kumar at el. [18] proposed two visual validation protocols: one is

a one-time-password protocol, and another is a password-based validation protocol. Our approach for genuine arrangement: we had the capacity attain to abnormal state of ease of use while fulfilling stringent security necessities. We propose a probabilistic SRA solution.

2. 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 are revoked.

Disadvantages:

1. Clients are frequently not rigorous in the validation process and current interfaces fail to provide effective information to end-users leads to exploitable vulnerabilities.
2. It can be seen that lack of information is treated as certainty of negative information, and trust is still based on static pre-configuration

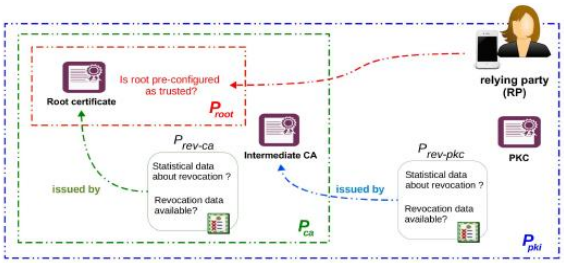
3. PROPOSED SYSTEM

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:

Advantages:

1. Security in communications
2. Secure installation of mobile applications

Architecture:



4. MODULES

Conduction Risk Assessment: 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.

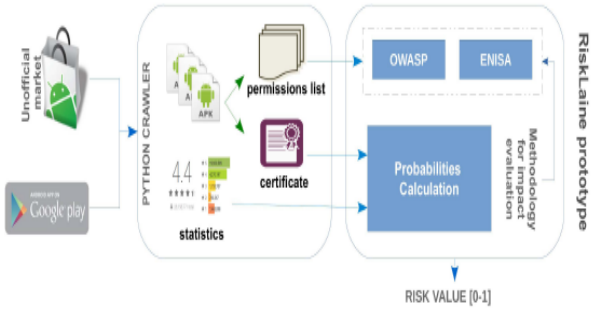
Risk Evaluation: Risk evaluation is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable.

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, 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.
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.

Risk Laine Architecture:



OWASP Methodology: The OWASP risk methodology defines two kindsof impact: a "technical impact", and a "business impact".Each impact includes factors with a set of options, and eachoption has an impact rating from 0 to 9 associated with it.On the one hand, technical impact factors are aligned with thetraditional security areas: confidentiality, integrity, availabilityand accountability.

5. CONCLUSION

We proposed a novel approach to assess risk in certificate based security including both revocation factors and behavioral trust management. With the clear definition of the risk approach scope, assumptions, steps and the rationale for the assessed risk factors values, we set the basis for increasing the reproducibility and repeatability of risk assessments in this field. Furthermore, the presented approach is applicable to any certificate based scenario and flexible to integrate different impact quantification frameworks.

REFERENCES

[1] D. Akhawe and A. P. Felt, "Alice in warningland: A large-scale fieldstudy of browser security warning effectiveness," in Proc. 22nd USENIX Conf. Secur., Aug. 2013, pp. 257–272.
[2] N. Leavitt, "Internet security under attack: The undermining of digitalcertificates," Computer, vol. 44, no. 12, pp. 17–20, Dec. 2011.
[3] J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, and R. Holz,"Mission accomplished: HTTPS security after diginotar," in Proc. InternetMeas. Conf., London, U.K., Nov. 2017, pp. 325–340
[4] O. Khalid et al., "Comparative study of trust and reputation systemsfor wireless sensor networks," Secur. Commun. Netw., vol. 6,no. 6, pp. 669–688, Jun. 2013.
[5] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust managementfor mobile ad hoc networks," IEEE Commun. Surveys Tuts., vol. 13,no. 4, pp. 562–583, 4th Quart., 2011.
[6] F. Almenarez, M. F. Hinarejos, A. Marín, J.-L. Ferrer-Gomila, andD. D. Sánchez, "PECEVA: An adaptable and energy-saving credentialvalidation solution for pervasive networks," Inf. Sci., vol. 354, pp. 41–59,Aug. 2016.
[7] Maddali M.V.M. Kumar,D. Venkatesh, "Increasing the Storage Capacity of the Classical Quick Response code Reading Level using 2LQR", International Journal of Scientific Engineering and Technology Research, Vol. –06; No. - 10; ISSN: 2319-8885; pp. 2087-2089, March 2017
[8] G. Purdy, "ISO 31000:2009—Setting a new standard for risk management,"Risk Analysis, vol. 30, no. 6, pp. 881–886, Jun. 2010.
[9] L. Davi, A. Dmitrienko, A.-R. Sadeghi, and M. Winandy, "Privilegeescalation attacks on Android," in Proc. Int. Conf. Inf. Secur. (ISC),Oct. 2011, pp. 346–360.
[10] S. Bugiel, L. Davi, A. Dmitrienko, T. Fischer, and A.-R. Sadeghi,"XManDroid: A new Android evolution to mitigate privilege escalationattacks," Center Adv. Secur. Res. Darmstadt, Tech. Univ. Darmstadt,Darmstadt, Germany, Tech. Rep., Jun. 2011.
[11] P. P. Chan, L. C. Hui, and S. M. Yiu, "Droidchecker: Analyzing Androidapplications for capability leak," in Proc. 5th ACM Conf. Secur. PrivacyWireless Mobile Netw. (WISEC), Apr. 2012, pp. 125–136.

[12] M. Rangwala, P. Zhang, X. Zou, and F. Li, "A taxonomy of privilegeescalation attacks in Android applications," Int. J. Secur. Netw., vol. 9,no. 1, pp. 40–55, February. 2014.
[13] L. Hayden, IT Security Metrics: A Practical Framework for MeasuringSecurity & Protecting Data. New York, NY, USA: McGraw-Hill, 2010.
[14] F. Almenárez et al., "Trust management for multimedia P2P applicationsin autonomic networking," Ad Hoc Netw., vol. 9, no. 4, pp. 687–697,Jun. 2011.
[15] Maddali M.V.M. Kumar,J. Babichaitanya, "Secured System for Keylogging – Resilient Virtual Validation", International Journal of Advanced Research in Computer Science and Software Engineering Vol. – 05; No. - 08; ISSN: 2277-128X; pp: 691-695; August 2015
[16] C. Gañán, J. Mata-Díaz, J. L. Muñoz, J. Hernández-Serrano, O. Esparza,and J. Alins, "A modeling of certificate revocation and its applicationto synthesis of revocation traces," IEEE Trans. Inf. Forensics Security,vol. 7, no. 6, pp. 1673–1686, Dec. 2012.

About Authors:

Dr.R.Murugadoss

He is working as a professor at St.Ann's College Of Engineering & Technology ,Chirala.15years of experience and his research interest is soft computing, deeplearning, computer networks.

M.UmeraJasmine

She is currently pursuing MCA in St. Ann's College Of Engineering & Technology, Chirala. She received her Bachelor of science from ANU.