http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

OPEN ACCESS Information Technology Journal

ISSN 1812-5638
DOI: 10.3923/itj.2017.79.84

Research Article
Efficient Approaches to Ensure Certificate Authenticity for Public Key Infrastructure

[1]John Barclay, [1]Vijay Kansara, [1]Eknath Eswar, [1]Khaled Elleithy and [2]Laiali Almazaydeh

[1]Department of Computer Science and Engineering, University of Bridgeport, Bridgeport, Connecticut, United States of America
[2]Faculty of Information Technology, Al-Hussein Bin Talal University, Ma'an, Jordan

Abstract

Background and Objective: The public key infrastructure provides secure digital certificates required to establish secure transactions over the networks. The certificates are intended to act as the sole item needed to authenticate an entity. However, fraudulent certificates become one of the challenges faced by the public key infrastructure, which have impacted the users' trust in certificates. A user must validate the certificate with the issuing certificate authority. Checking every certificate with the certificate authority is costly in time and bandwidth. It also eliminates one of the benefits of certificates, which is offline authentication. In this study, different methods were explored for deciding when to contact the certificate authority for authorization with a focus on minimizing the risk of accepting a fraudulent certificate while maintaining the benefit of offline authentication. **Materials and Methods:** This study analyzed Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) requests. Most of the related approaches can roughly provide potential options for increasing the scalability of the Public Key Infrastructure (PKI). Nevertheless, only few recent approaches addressed a tradeoff risk versus cost. As it is well known, at the point when reducing one's risk, it is almost that cost is increased. **Results:** Simulation results showed the relationship between risk and changes in criteria through generated graph from the experiment. With that hybrid technique for checking the revocation status of a certificate, this research ponders on a relationship between risk and cost that is non-linear. Based on experiment results, policies could be created that provide the best risk to cost ratio for specific environments. **Conclusion:** From results it is concluded that checking certificates based on the age of a cached certificate revocation lists provided the best relationship between cost and security. Combining it with other features will either reduce the potential cost to security ratio or reduce the flexibility of the method.

Key words: Public key infrastructure, certificate revocation list, online certificate, protocol, delta CRL, certificate authority, directory access protocol, CRL distribution points

Received: January 17, 2017 Accepted: February 21, 2017 Published: March 15, 2017

Citation: John Barclay, Vijay Kansara, Eknath Eswar, Khaled Elleithy and Laiali Almazaydeh, 2017. Efficient approaches to ensure certificate authenticity for public key infrastructure. Inform. Technol. J., 16: 79-84.

Corresponding Author: Laiali Almazaydeh, Faculty of Information Technology, Al-Hussein Bin Talal University, Ma'an, Jordan Tel: +962 (77) 6245243

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

With public key cryptography, users can exchange encrypted data over insecure networks while ensuring confidentiality and integrity of that data. However, public key cryptography by itself does not ensure authentication of the identity of the other party. There would be no assurance that the public key is generated from a reputable source. Thus, to both securely exchange data over networks and reliably authenticate the identity of the other party, a Public Key Infrastructure (PKI) is used[1-3].

The PKI was developed to manage and validate the encryption keys using digital certificates. PKI is serviced by a number of trusted Certificate Authorities (CA) that provides certificates to organizations to identify them. A user knows that a certificate is signed by a CA they trust by checking the digital signature. This digital signature consists of the certificate holder's public key encrypted using the CA's private key. This method allows the user to ensure the certificate is valid without the need to check with the CA for every certificate they accept[4].

One problem with this method which has endangered the security of PKI is when CA is compromised by entities that have issued fraudulent certificates[5]. These incidents have required the creation of Certificate Revocation Lists (CRLs). A user can request a CRL from the CA or use Online Certificate Status Protocol (OCSP) to ensure a certificate is valid. However, this impacts the benefit of offline authentication[6,7].

It is clear that the users could check with a CA whenever they need to accept a certificate, which will lead to impact the efficiency of using certificates. Therefore, there are two opposing goals that need to be met: Security vs. efficiency. Maximizing efficiency will result that the user accepts some certificates that have been revoked. On the other hand, maximizing security will result in a drain on resources as users make constant requests to CAs for certificate validation. This study explores different methods to strike a balance between security and efficiency by outlining conditions for contacting the CA for appropriate authorization.

MATERIALS AND METHODS

Related work and schemes: Several models of PKI have been suggested for validation of certificate to solve the scalability related issue. One of the most common PKI trust models is Internet X.509 Public Key Infrastructure (PKIX), which has focused on reducing the cost of issuing CRL's. In PKIX model, the information about the status of the certificates was maintained by the CA which includes the support of the certificate revocation. The CA can revoke any certificate as it becomes invalid due to any reason. As reported by Choi *et al.*[8], certificate revocation has resulted in the creation of different approaches such as CRL distribution points, delta-CRL and freshest-CRL. As an example, the delta-CRL methodology is to only publish the most recent additions to the CRL, but this still result in a high number of simultaneous connections to the CRL provider[9].

Certificate Revocation List (CRL): An issued certificate with a validity period of one or two years defined by CA is a Certificate Revocation List (CRL). The validity period of a certificate should be checked whenever a certificate was presented as a part of an authentication dialog[10]. The key problem of this scheme was when there is a large domain involve, the list will become huge in size as the number of revoked certificates was proportional to the size of the domain. As the CRL size becomes large due to the domain size, the network load increases when the end-users download the list. In this regards, the end-users need to cache the CRL as long as the CRL has not yet expired, but because of the frequency of updates, then the obtained list may not always be fresh.

Delta-CRL: Traditional CRL is expected to have small refresh period in order to get the freshness of the CRL. A Delta-CRL works as an extension to CRL. A delta-CRL was periodically updated and it serves as an up-to-date certificate status information of the previously issued CRL. So, the user can obtain the newest revocation information from delta-CRL instead of downloading the latest full CRL. Thus, less load and improved response time can be obtained[11,12].

CRL Distribution Points (CDPs): As an extension to the CRL scheme, CRL Distribution Points (CDPs) approach addresses the maximum size of a CRL. The size of a CRL subject population is restricted by partitioning the total population for a CA into a number of segments. All these segments were associated with CDP, which can be located on various hosts and/or directories on the same host. Each certificate has a pointer to the location of its CDP[4]. The location of certificate checking information was controlled by the CA and will generally be at a location convenient to the CA, which may not be ideal for the end-user all the time.

Lightweight Directory Access Protocol (LDAP): Lightweight Directory Access Protocol (LDAP) server was required in PKI system to provide the CRL query and downloading, which was stored as binary sort tree structure. It improves the efficiency of querying the certificates and decreases the number of mobile records. The LDAP was superficially similar to directory based approach in which end users can use a local directory server providing efficient high performance access. Most CAs support LDAP CRL publishing[11,13].

Online Certificate Status Protocol (OCSP): Online Certificate Status Protocol (OCSP) was designed as a protocol that provides online validation of a certificate's revocation status without requesting an entire CRL. An OCSP responder will keep a database of CRLs. It will only return a response to the requester whether the certificate has been revoked or not. However, it was not able to act as the primary method of checking on certificate's revocation status because of issues of convergence[14].

Zhang and Wang[11] have attempted to solve the problem by reducing the resources needed to verify a current certificate. These methods generally attempt to reduce the burden placed upon the CA by reducing the size of the response or lowering the needed number of revocation requests. On the other hand, although CRLs were signed by few trusted authorities, they can be distributed by un-trusted entities. Therefore, other research works, such as by Qiu *et al.*[15] has even been done on distributing CRL's through Peer-to-Peer networks. However, the former will only offload the bandwidth usage to many users rather than actually reducing it.

Proposed solution: Concerning the aforementioned related approaches, they can be roughly provide potential options for increasing the scalability of the PKI, but, until recently, they have not addressed the problem from the position of risk versus cost. As it was well known, at the point when reducing one's risk, it is almost that cost was increased. Noteworthy, as the risk reduced the cost increases.

Two above-mentioned CRL retrieval methods were analyzed. At one end of the spectrum, every certificate would be checked for revocation status. At the other end, no certificate would be checked for revocation status. The former method would result in the least amount of risk and the maximum cost. The later method, would result in the maximum amount of risk and essentially zero cost.

Analysis for CRL and OSCP requests were performed. However, the cost is measured in the required bandwidth. Although, the size of a CRL is variable, the basis provided by Lakshminarayanan *et al.*[16] is used. The size of the CRL is equal to the following:

180 bytes+9 bytes per CRL entry

The study carried out by Lakshminarayanan *et al.*[16] assumed 200 revocations were added to the CRL per day and remained in the CRL for half of their lifetime. This resulted in a base CRL of 321 kb. Therefore, to determine whether the size of the CRL affects the performance relationship between issuing CRLs and using OCSP, simulations with various sizes for the CRL were conducted. Validation requests through OCSP assume a size of 1 kb.

A hybrid technique for checking the revocation status of a certificate was provided while running different scenarios in with the simulation; every individual feature and a combination of two separate features. The features will include the followings:

- **Age of the certificate:** There is a period of time during which an improperly issued certificate exists but has not been added to a revocation list. Even checking the certificates revocation list does not prevent a user from accepting this certificate. Therefore, it can be assumed that there was some time period early in the certificate's lifetime during which it would be more efficient to not check its status
- **Significance of the certificate:** For certain online services such as banking and shopping services, it was a crucial step that a user does not accept a fraudulent certificate. Therefore, it was desirable that these certificates be checked for revocation status more regularly
- **Previously acquired CRL:** If a CRL has been recently acquired from a CA, a fraudulent certificate was likely has already been in the CRL. For checking certificates from the same CA, assuming there was a time period during which a cached CRL will be useful rather than needing to reacquire one
- **Random check:** While it was rudimentary, choosing to check a random percentage of certificates for their revocation status will result in the rejection of some fraudulent certificates in many cases

As part of running the experiment with simulation, it was assumed that there are twenty CAs and the clients requests certificates. These certificates were assigned random characteristics including age, issuing CA and significance.

Based on these characteristics, the client makes an evaluation of whether the revocation status of the certificate should be checked. Meanwhile, a running counter is kept to track revocation status requests, rejected fraudulent certificates and fraudulent certificates which were accepted.

Using the aforementioned proposed data, the relationship between risk and changes in criteria through generated graph from the experiment simulation was demonstrated. With that hybrid technique for checking the revocation status of a certificate, a non-linear tradeoff between risk and cost was implemented. Based on the experiment results, policies could be created that provide the best risk to cost ratio for specific environments.

Mathematical model: As part of the experiment simulation, the following assumptions were made:

- Certificates are granted for 365 days
- Ten percent of certificates were fraudulent and will be added to a certificate revocation list
- Fraudulent certificates will exist for 1-180 days without being added to a certificate revocation list
- There were 20 certificate authorities
- There were 20 end users that everyone deals with 20 certificates each day for 365 day
- The results are used to show a relationship between security and cost

Security was measured based on the percentage of fraudulent certificates that were rejected. These simulations were not conducted under real world conditions, the specific calculated cost in bytes is not necessarily relevant. Thus, rather than use this raw value, a baseline cost was established. This baseline came from checking every single certificate. All methods eventually reach 100% cost.

As a note, this baseline does not result in 100% of fraudulent certificates being rejected. However, as part of the simulation, the fraudulent certificates can exist but not as a part of a certificate revocation list. In addition, even checking every certificate does not result in 100% security.

RESULTS AND DISCUSSION

In this experiment two scenarios were considered, the first scenario was every individual feature simulation and the second scenario was a combination of two separate features simulation.

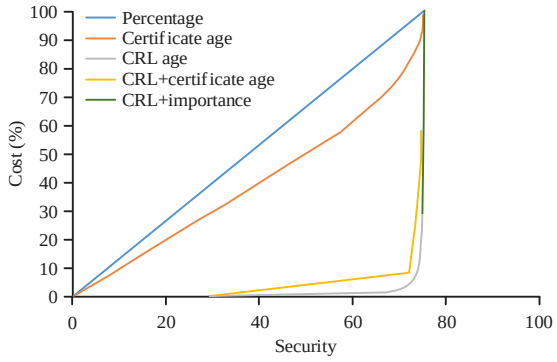

Fig. 1: Simulation results of checking based on certificate age and checking based on importance

The first experiment simulation was based on checking a certain percentage of certificates. Several cases were investigated from 0-100% with 10% increments. Every 1% increase in cost resulted in approximately three quarters of a percent increase in security. At maximum cost, this method resulted in seventy-five percent of fraudulent certificates being rejected. This series of simulations is represented by the blue line in Fig. 1.

The second simulation was based on certificate age which runs in 30 days increments from 365-0 days with 30 days increments. Certificates would only be checked if they were older than the entered date. For this series of simulations, cost and security initially increased at a one to one rate. This relationship began to break down around the simulation time of 155 days. At this point, there were severe diminishing security increases for large cost increases. Based on the analysis carried out, this breakpoint occurs based on the assumption that fraudulent certificates were not immediately added to a certificate revocation list. The maximum age at which a certificate was added to a certificate revocation list was 180 days. When no certificates younger than this were checked, there was never a situation in which a fraudulent certificate is checked that has not yet been added to a certificate revocation list.

The third set of simulations was based on the age of the certificate revocation list. An end-user would not download a new certificate revocation list until the cached certificate revocation list was at a certain age. All certificates would be checked against this cached certificate revocation list, but there would be no increase in cost. To maintain consistency with the previous set of simulations, these tests were also run with ages ranging from 365-0 days with 30 days increments. This resulted in a vastly superior cost to security line as demonstrated in Fig. 1. At the highest values, each end-user would only download a single certificate revocation

list from each of the twenty certificate authorities. Since any given certificate can be up to a year old, this certificate revocation list continued to provide some good results for the entire year. This resulted in a minimum of 29% of fraudulent certificates being rejected. In the results of simulation, a breakpoint occurred around day 35. At this point, costs began increasing greatly with little increase in security. From a maximum age of 35 days to a maximum age of 0 days, there was only a 5% increase in security for a 97% increase in cost.

From the individual feature simulations, it was obvious that the simulation based on certificate revocation list age resulted in the best option for reducing costs without severely impacting security.

The second scenario of experiment was a combination of two separate features simulation.

The first run of simulations combined checking based on certificate age and certificate revocation list age. Even if the current certificate revocation list was valid based on maximum certificate revocation list age, the certificate would still be checked if it was older than the maximum certificate age. This approach did not yield any worthwhile improvement. While combining the two certificates did increase the security for certain values of each method, there was no point at which there were better results than those provided by checking based on certificate revocation list age.

The second run of simulations was based on certificate importance. Simulations based on importance alone were not seen as a valid method. It would provide similar results as testing only a certain percentage of certificates. For the purposes of this simulation, 20% of all certificates were labeled as important. Then, for accepting or rejecting fraudulent certificates, important certificates were weighted as two certificates. Since, combining the certificate revocation list age and certificate age methods had given us poor results. Therefore, using the certificate revocation list age was only used to test the importance of a certificate as criteria.

In this approach, several simulation tests were carried out to identify characteristics that impact both security and cost. Checking the importance of certificates, gave us similar results to checking based solely on the certificate revocation list age. However, there was a limit to the minimum cost and minimum security that could be provided. Using importance and certificate revocation list age resulted in a minimum cost of 30% and a minimum security of 74%. Ultimately, this was no better than only checking based on certificate revocation list age, while having reduced flexibility. Therefore, there was no option to reduce cost in exchange for a reduction in security.

After a thorough review of state-of-the-art literature, the simulation model contained herein, including analysis of CRL and OSCP requests from the position of risk versus cost, has not been suggested so far in literature. As most recent studies carried out by Koschuch and Wagner[17] and Ganan *et al.*[12] did not address the same analysis.

CONCLUSION

Checking certificates based on the age of a cached certificate revocation lists provided the best relationship between cost and security. This study introduced different methods to balance security and cost. The simulation results demonstrated the effectiveness of the introduced methods to reach this goal. The simulations could be refined to determine the real world percentage of fraudulent certificates that would be correctly rejected.

SIGNIFICANCE STATEMENTS

This study demonstrates a hybrid technique for checking the revocation status of a certificate with the implementation of different simulation scenarios. Simulation results showed the non-linear relationship between risk and cost through generated graph from the experiment.

ACKNOWLEDGMENTS

The authors acknowledge the support received from the University of Bridgeport and Al-Hussein Bin Talal University to complete this research.

REFERENCES

1. Albarqi, A., E. Alzaid, F. Al Ghamdi, S. Asiri and J. Kar, 2015. Public key infrastructure: A survey. J. Inform. Secur., 6: 31-37.
2. Maurer, U., 1996. Modelling a Public-Key Infrastructure. In: European Symposium on Research in Computer Security, Bertino, E., H. Kurth, G. Martella and E. Montolivo (Eds.). Springer, Berlin, Germany, pp: 325-350.
3. Ramadan, M., G. Du and C. Xu, 2016. A survey of public key infrastructure-based security for mobile communication systems. Symmetry, 8: 1-17.
4. Benantar, M., 2001. The Internet public key infrastructure. IBM Syst. J., 40: 648-665.
5. Paterson, K.G. and G. Price, 2003. A comparison between traditional public key infrastructures and identity-based cryptography. Inf. Secur. Tech. Rep., 8: 57-72.
6. Shivajyothi, G., 2013. Certificate revocation using Online Certificate Status Protocol (OCSP). Int. J. Res. Comput. Technol., 5: 1-8.

7. Satoshi, K. and S. Kouichi, 2005. Proposal and analysis of a distributed online certificate status protocol with low communication cost. IEICE Trans., A88: 247-254.
8. Choi, J.H., S.S. Lim and K.D. Zeilenga, 2005. A new on-line certificate validation method using LDAP component matching technology. Proceedings of the 6th Annual IEEE SMC Information Assurance Workshop, June 15-17, 2005, West Point, NY., USA., pp: 280-285.
9. Tan, H., M. Ma, H. Labiod, A. Boudguiga, J. Zhang and P.H.J. Chong, 2016. A Secure and Authenticated Key Management Protocol (SA-KMP) for vehicular networks. IEEE Trans. Veh. Technol., 65: 9570-9584.
10. Sujitha, T. and T. Hemalatha, 2015. Analysis on certificate validation mechanisms in public key infrastructure. Int. J. Adv. Comput. Sci. Technol., 4: 166-170.
11. Zhang, S. and H. Wang, 2008. An improved delta and over-issued certificate revocation mechanism. Proceedings of the ISECS International Colloquium on Computing, Communication, Control and Management, August 3-4, 2008, Guangzhou, China, pp: 346-350.
12. Ganan, C., J. Mata-Diaz, J.L. Munoz, J. Hernandez-Serrano, O. Esparza and J. Alins, 2012. A modeling of certificate revocation and its application to synthesis of revocation traces. IEEE Trans. Inf. Forensics Secur., 7: 1673-1686.
13. Lim, S.S., J.H. Choi and K.D. Zeilenga, 2008. Design, implementation and performance analysis of PKI certificate repository using LDAP component matching. J. Software Pract. Exp., 38: 827-851.
14. Lee, Y. and Y. Shin, 2008. A proposal of real-time status management protocol for structural desperation of a certificate verification service. Proceedings of the International Conference on Security Technology, December 13-15, 2008. Sanya, China, pp: 87-90.
15. Qiu, Z., M. Chen and J. Huang, 2010. A study on CRL issue by P2P network. Proceedings of the 3rd International Symposium on Intelligent Information Technology and Security Informatics, April 2-4, 2010, Jian, China, pp: 526-529.
16. Lakshminarayanan, A., A. Liviandi, L. Lee and W. Chui, 2006. Can CRLs provide bandwidth-efficient online certificate status? Proceedings of the 31st IEEE Conference on Local Computer Networks, November 14-16, 2006, Tampa, FL., USA., pp: 203-210.
17. Koschuch, M. and R. Wagner, 2014. Papers, Please…: X.509 certificate revocation in practice. Proceedings of the 5th International Conference on Data Communication Networking, August 28-30, 2014, Vienna, Austria, pp: 1-5.