Deployment of Delegated Certification Path Validation in Cloud for Mobile Business

Zhan Wang[1] Luning Xia[1] Jiwu Jing[1] Neng Gao[1]

[1]State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing, 100049, P. R. China

Email: {zwang, halk, jing, gaoneng}@lois.cn

Abstract

Mobile business is one of young promising e-commerce industries. In mobile business scenario, PKI and certifications have been the premier solution to secure mobile transactions. However, client devices with limited computing and storage resources have difficulties to discover and validate the certification path, since this process costs large computing and communication resources. In this paper, we focus on utilizing the distributed and resourceful features of cloud to provide flexible and traceable path validation services for mobile business. This service is compatible with current standard Delegated Certification Validation protocols. All mobile devices can make the validation requests to our "delegation cloud" from world-range locations and get a swift response, regardless how complex the certification path is.

Keywords: Path Validation, Cloud, Mobile Business

1. Introduction

The development of wireless communication technologies and the popularity of e-commerce lend an impetus to the emergence of mobile business, which is a young promising industry.

Either in mobile business or any other forms of e-businesses without face-to-face transactions, security is always the issue of great concern. Especially, macro-payments and account transfers require higher security [5], and for these purposes wireless adaptations of Public Key Infrastructure (PKI) and TLS/SSL (for example, the WAP 2.0 standard contains specifications of WPKI and WTLS) have been developed to enhance the security of mobile transactions (for more information, see [6]).

Therefore, discovering and validating the certification path is the pivotal steps to make certificates effectively secure the transactions.

However, most devices used in mobile business have very limited resources, including CPU, Memory and the battery. We have to ask a delegated server for help to fulfill the task of certification path validation. And the service provider should afford the validation requests from all over the world, meanwhile discover appropriate path along with more than one repositories or LDAP servers which locate all over the world, and give a quick respond to those requests.

Cloud storage and computing become hot topics in both academia and industry recent years. Regardless of all arguments about the concepts of cloud, it truly offers us a choice to fast deploy a distributed delegation service as an experimental

field and achieve above goals. First, cloud computing providers can build large datacenters at low cost due to their expertise in organizing and provisioning computational resources; Second, servers provided by the cloud providers, such as Amazon AWS [7], locate at multiple regions or locations to accelerate the access speed. Hence, we don't need to buy large-scale servers to serve this service and maintain them at different continents.

In this paper, we utilize distributed and resourceful features of cloud to deploy the delegated certificate path validation service and serve the mobile business. This service is compatible with current standard Delegated Certification Validation protocols. All mobile devices can make the validation requests to our "delegation cloud" from world-range locations and get a swift response, regardless how complex the certification path is. The delegation cloud also keeps all validation evidences for later tracing.

The rest of this paper is structured as follows. We describe some issues and findings pertinent to certification path validation in Section 2. In Section 3, we summarize the requirements of deploying the validation service in cloud for mobile business. In Section 4, we describe in detail our deployment scheme.

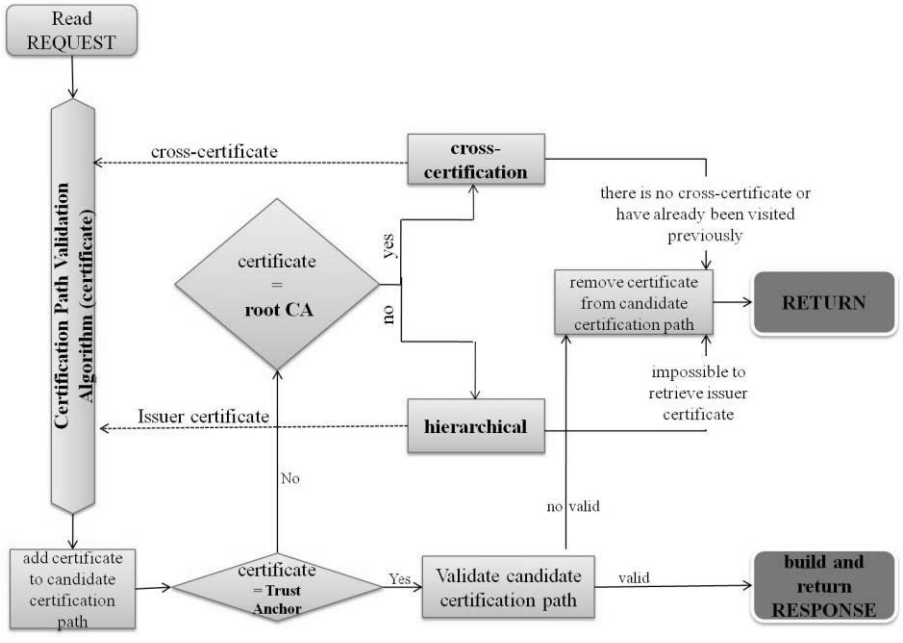

Fig. 1: Certificate Path Validation Workflow.

2. Backgrounds and Related Work

2.1. Certification Path Validation

PKI supports a number of security-related services, including data confidentiality, data integrity, and end-entity authentication. Fundamentally, these services are based on the proper use of public/private key pairs. The public component of this key pair is issued in the form of a public key certificate and, in association with the appropriate algorithm(s), it may be used to verify a digital signature or encrypt data. Before a certificate can be used, it

must be validated. In order to validate such a certificate, a chain of certificates or a *certification path* between the certificate and an established point of trust must be established, and every certificate within that path must be checked. This process is referred to as *certification path Validation.* [1].

In this paper, certification path validation generally includes path discovery and the certification checking. We don't deal with them separately when we refer certification path validation. Fig. 1 shows the workflow of certification path validation. We can find that the path discovery ends with encountering the certificate as the trust anchor. And when we meet a root CA certificate, which is not the trust anchor in the candidate path, it indicates that cross-certificates may be involved in the path. All these processes cost large computing and communication resources to acquire and add appropriate certificates into the candidate path. Additionally, validation checking process requires verifying CRL and each signature of the certificates those construct the path. It is also a time-consuming work.

Due to the limitation of end-devices in mobile business, some efforts have been made to design lightweight certification path validation protocol to adapt mobile environment, such as [2]. Although they have to tradeoff between the complexity and functionality, handheld devices still have difficulties to cope with communicating with diverse repository interfaces. Another standardized solution is delegated certification path validation.

2.2. Delegated Certification Path Validation

Certificate path validation is the task that often cannot be carried out by entities that have limited resources [2]. As a result, these tasks can be assigned to trusted entities that perform Delegated Path Discovery (DPD) and Validation (DPV) on behalf of the requesting party.

In 2002, RFC 3357 [3] has standardized the DPD and DPV protocol requirements. But these delegated services earn attentions till recent years. Some CAs offer delegated validation service under the range of their trust domains. In this case, the process of path discovery is extremely simple, since the delegated server can easy to find the PKI structure and do not need to communicate with different repositories. However, for the end-devices in mobile business, in order to validate all kinds of certificates, they have to interact with different servers, which bring extra costs.

To our best knowledge, there isn't any delegated validation service which serves global path validation. With the rapid development of mobile business, the delegation requirement will become urgent. And it is impossible to establish one delegation server which faces more than one trust domains even hundreds and millions, interacts with diverse PKI structures and repository interfaces. From the user perspective, they may make validation requests from every corner of the world and expect a quick response. We have to find another distributed solution to deploy such global validation service.

2.3. Cloud Storage and Computing

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud [4]. In sum, cloud seems to be a manager of the resources pool and waits for explorers to exploit.

Due to the resourceful feature of cloud, utilizing the storage and computing resources offered by the cloud, we can use

the original standard validation protocols to provide delegation services. That means no need to tailor the protocol and balance the complexity and functionality for mobile scenario.

In the delegation service of mobile business, one certificate path may include CA certificates that belong to several different CAs, and these CA certificates may locate at different regions. All mobile devices also locate all over the world. The distributed feature of cloud makes it good at coping with this situation.

For further mitigate the communication pressure of the end-devices, part of storage work can also hand over the cloud, such as trust anchors and validation policies. This also can accelerate the response speed, since end-devices don't need to submit the trust anchors along with each request, and more interactions are accomplished within the cloud.

Therefore, with deploying the validation services in a manageable cloud, mobile end-devices can acquire the high quality and flexible validation service with lowest storage, computing and communication cost.

3. Features and Requirements

In mobile business scenarios, the delegated certification path validation request has the following features:

- Devices of end-users cannot afford heavy load of computing, storage and communication
- All validation requests may come from every corner of the world
- For a specific handheld device, it may initial requests from different locations
- CAs involved in a certification path may locate at very different regions, such as at different continents
- Applications of mobile business are divers, end-users may apply different validation policies

According to above feature, the delegation service for mobile business scenario should satisfy the following requirements：

- Transparency. Mitigating the cost of end-devices is a premier task. End-users are unnecessary to know the complex PKI structures, such as cross-certification.
- Distributed service. Because two important entities involved in the delegation service are end-user devices which are mobile and CA Repositories which locate at very different regions.
- Flexibility. End-users have the right to determine whether or not to trust the delegation. Allowing
- Efficiency. Mobile business is a new style of commerce. The principle, time is money, is still adoptable.
- Compatibility. Adopting current standard protocols to realize the delegation service can provide a full service to mobile business.
- Traceability. Validation service should provide users chances to trace the evidences when dispute occurs.

4. Our Deployment

In order to satisfy the requirement of certification path validation for mobile business, we deploy the delegated service in the cloud; we call it "delegation cloud". As shown in Fig. 2, each mobile end-device can request the validation to the cloud and get a swift respond from the cloud regardless how complex the path is.

We will introduce our deployment from two views. One is looking inside the "delegation cloud". The other is the degree of trust between end-devices and the delegation cloud. Finally, we propose a prototype plan for the deployment.

4.1. Inside the Cloud

Each organization or CA will have to define an internal certification model (single, hierarchical or peer-to-peer cross-certification), and the mechanism to establish external security relationships. As shown in the upper part of Fig. 2, delegation server cannot predict the structure of PKI and the potential path at the beginning. However, cloud provider has the power to discover distributed resources. For example, delegation cloud received a request to validate a certificate issued by CA1 that locates in America. Delegation cloud asks servers located at different regions to reach related repositories. Relative fast responds are obtained from the servers nearby the CA repositories or its LDAP servers. Delegation cloud also can record this process, and optimize the discovery process next time. As shown in Fig.3, all servers collaborate with each other to return quick responds to the client.

Cloud provider can also provide unlimited storage space. Each end-device can register in the cloud and configure their separate policies. Another scenario to apply this function is that groups wish to execute uniform policy. When the policies are stored in the delegation cloud, the validation process becomes faster since the communication inside the cloud has already optimized by the cloud providers. Additionally, cloud storage also offers the possibility to retain all validation evidences for global users for certain duration, which satisfies the traceability requirement.

4.2. Three Levels Trust

The delegation cloud provides flexible services to users. According to RFC 3359, users can select to trust the delegated server or not. In our deployment, we provide three levels of trust between the requesting user and the delegation cloud. Two of them are compatible with the standard; the third one is a special case of the standard:

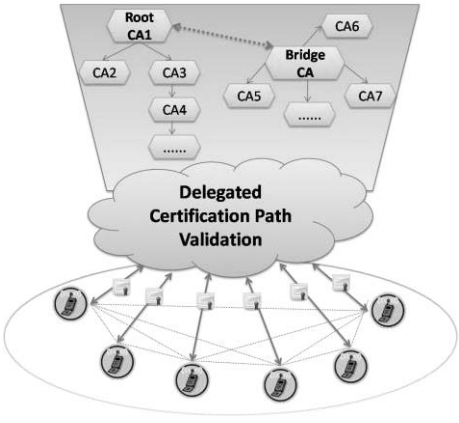

Fig. 1: Structure of delegated certification validation in cloud.

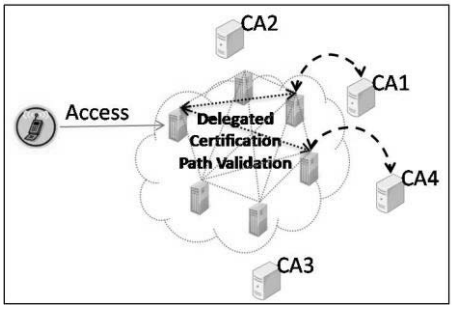

Fig. 2: Interactions inside the delegation cloud.

- Non-trust: clients only utilize the delegation cloud to discover the certificate path without validation. In this case, clients need to offer the certificate to validate and validation policies to follow, and don't need to trust the delegation. As illustrated in Fig. 4-a, delegation only provide all necessary elements used to validate the certificate, including certificate chain, CRL and all CA certificate involved on the chain. All above elements are sign by related CA，the tasks of verify-

ing these signature are left for the end-user. The merit of this level is that end-user needn't to trust the delegation and only consider the delegation as a search tool.

- Trust: clients utilize the delegation cloud to discover the certificate path and then validate it according to the policies provided by clients. In this case, clients have to trust the delegation to some extend and accept any responds from the delegation according the policy provided by clients. As illustrated in Fig.4-b, the delegation accords to the validation Policies return the end-device a final result.
- Complete trust: clients utilize the delegation cloud to discover the certificate path and then validate it according to the preplaced policies. As illustrated in Fig. 4-c, clients don't need to send the policies to the delegation. An organization can make contract with the delegation cloud to implement uniform validation policy. In this case, clients are unnecessary to provide the trust anchors, which will save the communication costs.

4.3. Prototype Plan

Till now, we have got a big picture of our deployment of delegation cloud. According our current project status, we have well analyzed the related delegated path validation protocols and have a prototype plan. We experiment to use Amazon AWS to create a country-level delegation service to serve the mobile business within the country, which will give us a good proof and feedback about the feasibility. And establishing world-level service is the next phase.

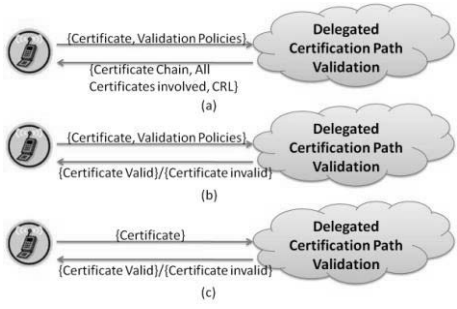

Fig. 4: Three levels of trust.

5. Summary and Future Work

In this paper, we propose a new deployment scheme of delegated certification path validation, which can well serve mobile business transactions. Comparing to traditional centralized delegated certification path validation, we deploy the validation service in a distributed and manageable environment, named "delegation cloud". Utilizing cloud technologies including cloud storage and computing, distributed end-devices can access the service with lowest communication and computing cost.

In Future, we will focus on detailing the world-level delegation service, including how to utilize the cloud storage resource to cache the history path and further accelerate the delegated respond speed.

Acknowledgements

This work was supported by grants from the National Key Technology R&D Program (ID: 2008BAH22B03), knowledge innovation program of Chinese Academy of (Grant No. YYYJ-1013), National Natural Science Foundation of China (70890084/G021102), "863" program (Grant No. 2006AA01Z454) and 2009 national information security standards development project (Certification Delegation and Path Validation Standard).

References

[1] PKI Forum, Inc, "Understanding Certification Path Construction", White Paper, September 2002.

[2] K. Papapanagiotou, G. F. Marias, and P. Georgiadis, "Revising centralized certificate validation standards for mobile and wireless communications", Computer Standards & Interfaces 32 , pp. 281-287, 2010.

[3] D. Pinkas and R. Housley, "Delegated Path Validation and Delegated Path Discovery Protocol Requirements", RFC 3379, IETF, 2002.

[4] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "Above the clouds: A Berkeley View of Cloud Computing", Tech. Rep. UCB/EECS-2009-28, EECS Department, University of California, Berkeley, February 2009.

[5] N. Mallat, M. Rossi and V.K. Tuunainen, "Mobile Banking Services", Communications of the ACM, Vol. 47, No. 5, pp. 42-46, May 2004.

[6] J. Claessens, V. Dem, D. De Cock, B. Preneel and J. Vandewalle, "On the security of today's online electronic banking systems", Computers and Security Vol. 21, No. 3, pp. 257–269, 2002.

[7] Amazon AWS, http://aws.amazon.com/