

Trust and Public Key Infrastructure

Sangyoon Oh

Computer Science Dept.
Florida State University
oh@cs.fsu.edu

Abstract

In the current rocket-speed growing E-commerce market, certain infrastructure, which enables users to exchange information and money securely over the Internet, is essential. Unfortunately, Internet is mere a cloud of connections of nodes. There is no organization to operate and manage. So the Internet itself is not responsible for any malicious frauds and attacks, and failures caused by reliability problems. Public Key Infrastructure (PKI) has been the solution to insecure communication over the network including above E-commerce problem. PKI is indispensable in the present Internet environment. This paper summarizes papers about secure communication over network using PKI as well as reviews the infrastructure and the role of Public Key in current Internet.

1 Introduction

After Diffie, Helloman, and Merkle invented Public-key cryptography in 1976, Rivest, Shamir, and Adleman proposed the algorithms in 1977 that enables to do encryption and authentication [RSA1]. But the big success story of Public-key cryptography had come along with current success of Internet, which changed every life-style of people in the world. 1) Customers buy products on the Business Web site and pay with plastic money. 2) A company branch in Seoul, Korea sends confidential sales report to the head quarter in New York by E-mail. 3) A research center needs a secure and trust communication channel to another center to discuss a research issue. 4) Critical information is backup-ed and that backup should be protected from disclosure and alternation. 5) Alice tries to communicate with Bob but does not trust the nodes on the path to Bob. As we see above, all kinds of open

network environment need a securely guaranteed method to communicate. The PKI has been treated as an answer for the trustworthiness problems. In section 2, we review the Public Key Infrastructure (history, architecture, the models, and structures). In section 3, the questions, which are brought up recently about PKI and how to choose the right PKI to our system. In section 4, two good papers about using certificate in open network to find trust path are reviewed.

2 Public Key Infrastructure

2.1 Private key system and Public key system

Even though we had a cipher method before the PKI, PKI has many advantages over the open network. Before the PKI, the private key system has existed and it provides security by encryption/decryption and authentication. The private key system, symmetric cryptography, is exchanging secret key to communicate each other with cipher text over the un-trust open network. As far as mutual trust is working, we don't have to have extra certifying system for transaction between Alice and Bob. But it is impossible to setup an independent trust to all the other party. So the PKI system provide plain ways to communicate securely rather than exchanging secret key with every trader like looking up public phone book.

2.2 Architecture of PKI

PKI introduced Certified Authority (CA) that issues and verify someone's public-key (In most case, it is called digital signature)[PKI]. Like we make a signature on the letter and 3rd party certifies that signature, the Public Key Infrastructure certifies public-key/digital signature. For the privacy, Alice sends an encrypted message using Bob's public key. Bob receives and decrypts message using Bob's own private key. In this case, any active trial to eavesdrop the message won't work, because Bob's secret key is not public and eavesdropper cannot decrypt message. For the integrity (digital signature), Alice sends signed message using Alice's private key. Bob receives the message and verifies the message using Alice's public key, which is held in the directory of Certified Authority. As far as Alice's private key keep in secret, eavesdropper cannot impersonate. PKI also have to have certificate management system and the directory where the certificates are held. User has the risk that the CA is lying about the contents of the certificate [ES].

So Registered Authority (RA) that acts as the verifier for the CA before a digital certificate is issued to the requester [PKI].

2.3 Several PKI structures and models

2.3.1 X500/X509

X.500 Directory service is developed originally for the global directory of Internet address. It is hierarchically structured look-up table. It is organized under a common root directory, Root Certification Authority (RCA) in a tree hierarchy. All the users in the network assume to know it by CA. All the entities do not have trust same RCA. One may use hierarchical authentication structure with several RCAs [ABD]. X.500 is popular but is fragile when the RCA is hacked and exposed. Pretty Good Privacy does not have specific structure rather, which we see in section 2.3.4.

2.3.2 Trust Graph

Certificates are used to model the confidence of an open-network in its public keys by a directed trust-graph [ABD]. The confidence is established by either direct trust (acquired by non-cryptographic method, such as checking identity) or induced trust (acquired only when the each node on the trust-path certifies the authenticity of the public key of the next node. It is very important not to confusing communication network and trust-graph. They may or may not be the same, since the communication network is based on the links of physical connection rather than confidence. Trust graph is core concept of the modeling of trust valuation in open network like the Internet [BBK][BD]. In the section 3, we see how this concept is applied.

2.3.3 PGP

Pretty Good Privacy is E-mail program, developed by Phil Zimmerman. It offers a reasonable degree of security for E-mail by using encryption and decryption under un-specific structured authentication infrastructure. Users are free to choose whom they are going to trust. Then, this trusting makes the trust chain grow. It is called key ring, which is a set of all public key that someone has [PFL]. The way it works is identical with Public key system, since it is originated from Public key system.

2.3.4 Virtual Private Network

Virtual Private Network is not exactly one of the PKI structure. But VPN is very popular infrastructure, which is using PKI. It is necessary to review it. Virtual Private Networks enable to establish secure connection through Public Internet Line, Network service Providers or Private Network. Tunneling (with Tunneling Protocol), Encryption, Authentication and Access Control enable this VPN over Public Line. The VPN needs encryption. To make a Virtual Tunnel (such as driving car to destination with Black cover, not to expose type of car) confidential, all the data/information should be encrypted with encrypt algorithms such as RSA [RSA]. Network Service Providers and Virtual Private Networks Equipment vendors provide these encryption features. Authentication is especially important when the remote access is using VPN. Since, before establish tunnel (Logically partitioned connection between two points over shared resource), Company should verify user information (Authentication) and give proper permission to use Company resource (It can be physical hardware resource and also information) to prevent unexpected user get into Corporation system, strong authentication is essential. Digital Certificate using PKI is used for verifying user information.

3 Questions in PKI and the Right PKI

3.1 Questions and weaknesses

Nevertheless PKI does crucial part in the Internet and open network communication, some bring up the questions of the need of PKI. Ellison and Schneier question the security of PKI system itself [ES]. Since security builds up from the chains of component, how strong the security is upon the weakest link. They insist that the link of the component of CA system is not all encrypted. So the weak point of link always exists and exposed to the attacks. They even doubt about needs of PKI. They listed several possible -flaw of PKI system. Since keeping the private key safe is under the responsibility of the user, PKI system does not have obligation to any security failure by stolen private key, even though the most of private key user computer is very vulnerable to hacking. The hacker gets the Root Certification Authority (RCA: The top-placed certificate on the tree structure) can be another possible stolen certification story. Once hacker has it, it certifies everything he wants to do. Another one Ellison and Schneier pointed is

finding certificate from CA directory with 'Name'. If the certificate holder has common name, there is possibility to get incorrect certificate. (Rivest suggest remedy in the SDSI presentation [SDSI]. He insists the uniqueness of public key than individual name). Also they indicate that there are the weaker links in the PKI and they makes they infrastructure vulnerable to malicious attack. The link between CA and RA is one of them and it is worse than either CA or RA. The certificate itself is not perfect securing either. The CA needs to identify certificate applicant before issuing certificate. But information, which they depend on, may not be the one they look for or may be the one altered. Because of case above, the use of PKI system has to be designed and implemented properly.

3.2 Right PKI

By Adams [ABD], the right PKI should be considered from two factor, 'definition' and 'application' perspectives. It should provide real applications and tools. And should be transparent to the day-to-day operation for the common users. The PKI has to have the tools to manage key and certificates (if it is beyond valid period, it may deny the certificates). If it does all this, 'definition' perspective is satisfied. For the application perspective, the right application of right PKI structure achieves high level of security. The most of transactions can be categorized into Business-to-Business (B2B), single Business (B), Business-to-Customer (B2C) categories, and individual (I). X.509 is the right PKI according to the 'definition' and 'application' perspective. But every category has own right choice. A PKI does not have to be the right PKI for all the categories. For instance, (I) hierarchical PKI, such as X.509 may not be necessary for the individual. However, it is suited for B2B and B categories. The 3rd party certifier model is the possible best choice for B2C, since transactions are through browsers.

Three essential approaches that may be used to support the security of PKI by Burmester [ABD] are a stochastic approach, a security policy management approach, and a structural approach. A stochastic approach, which is using probabilistic models, is based on the statistics data to assign the trust profiles and assurance level to the entities. It controls reliability faults. For the malicious attack, combination of a security policy management and a structural approach will work as far as properly implemented. A many attacks can be prevented by well-implemented security policy, but not all. Appropriate structure of PKI helps. As Adams states, right structure topologies are very necessary for the security. Horizontal structure will be the right

choice for the malicious attack. If a bounded number (k) of penetrations attacked the vertex-disjoint path, it is secure as far as $2k + 1$ disjoint path is connected. All three aspects are indispensable to obtain secure PKI.

As an inventor of PGP, Zimmerman insist that PGP structure can be the right PKI choice for many case. The de-centralized structure of PGP does not need the CA and prevent weaknesses of PKI, which arises from flaws of CA system. He put the PGP on the web as a freeware to insist users to use it. Then, the public key ring gets bigger and wider secure communication accomplished.

4 Trust of open network

The Internet is an open network. Communication in open network requires trustworthiness information of the other party, because there is not guarantee that single Certificate Authority (Authentication Server: AS in Beth, Borchering, and Klein [BBK]) can serve all the time. It may not have the information or it may be under control of malicious attacker. Beth, Borchering, and Klein introduced [BBK] the logics and protocol to decide the trustworthiness of path not only considering either trust or not but also the 'degrees of trust'. Based on previous models, Burmester and Desmedt introduced [BD] the algorithms for the sender to compute a good approximation of the trust graph if the disjoint connectivity of trust-graph is at least $2k + 1$, where k is the upper bound on the number of faulty (Byzantine) processor (vertex).

4.1 4.1. Valuation of trust in open network

In the paper, Beth, Borchering, and Klein [BBK] narrows the definition of direct trust and recommended trust (induced trust in section 2.3.2) specifically. The formal definition of direct trust is that a direct relationship exists if all experiences with Q with regard to trust class x which P knows about are all positives [BD]. There are mediators, which consist the sequence between P and Q . The value of the trust relationship, V is computed by the probability of the reliability of Q . The recommendation trust is a relationship exist if P is willing to accept reports from Q about experiences with 3rd parties with respect to the trust class x [BD]. This trust is restricted to the experience with target set by path set. (By an example by Desmedt, if P is the group of employer, Target set is computer science graduates when Q is a group of faculty who recommend target set to P .) According to the

definition above, the example in the paper illustrates how the trustworthiness of given entities are computed. If the each vertex between two entities has whether direct trust or recommended trust and the value, derive direct trust relationship and recommendation trust relationship. The rules of derivation are in the paper. The recommendation trust is derived from the sequence of recommendation trust and recommendation trust. The values are multiplied and assigned to the new relationship. And the direct trust is from the sequence of recommendation trust and direct trust. The computation of new direct trust requires formula, $V1$ and $V2$ from the previous relationships are applied to $1 - a \cdot (V1 * p)$. In the example, there are two distinct paths from A to G. So the combination of direct trust relationships are computed also with formulas in the paper, since the valuation of trust should consider all possible distinct paths' values. The last step is to use that value to decide whether or not an entity is trustworthy with respect to the certain task [BBK]. It is the function of probability a , we've used above, value that introduced from the combination of relations, and the unit (Beth, Borcharding, and Klein assume that the value can be measured in units) number that we wish to entrust. In the example, if we want to entrust a task worth 100 units, the risk we will have is 49.5 units.

4.2 Secure communication in an unknown network using certificates

Based on a previous effort like Beth, Borcharding, and Klein [BBK], Burmester and Desmedt present a protocol with which secure communication can be achieved by providing information about the trust graph is sufficiently connected [BD]. They assumed that the structure of trust graph is not known to sender and receiver. Only Faulty processor (It is corrupted node, which is under attacker's control.) has information about the structure and is lying about the their neighbors. This lying chain provides false information to the user to prevent finding the trust-graph. A good approximation of trust-graph G is the subset of G , where the edge of faulty processor has removed. Suppose vertex b wants to construct a good approximation of the trust graph to communicate by querying all its neighbors in un-known trust graph G . And the neighbor asks to the neighbors. Vertexes are returning a neighbor list of a faulty vertex. According to the list received, the good approximation of the trust graph is gotten. But to compute a good approximation of the trust graph in a polynomial time, constructing protocol is used, because in the first case we've seen, there is no halting strategy. So Burmester and

Desmedt propose the general case of Constructing a communication network problems. In this case, the query is flooded in the round-robin fashion to prevent the jam caused by faulty processor [BD]. After certain time elapse, some vertices finish the list and return it. Then, that vertex is labeled as "replied". Others are "replying". If the vertex is linked to b eventually, it is labeled "linked", else are labeled "not-yet-linked". Upon the list and the labels the vertex have, the protocol computes a good approximation of the trust graph in polynomial time.

References

- [ABD] Carlisle Adams, Mike Burmester, Yvo Desmedt (2000)
Which PKI (Public Key Infrastructure) is the right one?
CCS '00 Athens, Greece
- [BBK] Thomas Beth, Malte Borcherding, Birgit Klein (1994)
Valuation of Trust in Open Networks
European Symposium on Research in Computer Security, pp 3-18
- [BD] M. Burmester and Y. Desmedt. (1999)
Secure communication in an unknown network using certificates.
Advances in Cryptology – Asiacrypt '99, pp. 274-287.
- [ES] Carl Ellison, Bruce Schneier (2000)
Ten Risks of PKI: What you're not being told about Public Key Infrastructure.
Computer Security Journal, 16(1): 1-7
- [PFL] Charles P. Pfleeger
Security in Computing, 2nd
- [PGP] Pretty Good Privacy <http://whatis.com>
- [PKI] Public Key Infrastructure <http://whatis.com>
- [RSA1] Rivest, R. L., Shamir, A., and Adleman, L. (1978).
A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.
Communications of the ACM, 21(2): 120-126.
- [RSA2] Rivest-Shamir-Adleman Algorithm <http://whatis.com>

- [SDSI] Ronald L. Rivest (1997)
SPKI/SDSI 2.0 A Simple Distributed Security Infrastructure
Maryland Computer Science Day Presentation
- [VPN1] Cris Banson (1999)
Virtual Private Networks
http://www.ntsistemas.com/db_area/archive/1999/9905/305s1.shtml
- [VPN2] Paul Ferguson, Geoff Huston (1998)
What is a VPN?
<http://www.employees.org/~ferguson/vpn.pdf>