Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.2c

Submitted by
Darlene Hill Hardie
(Recently married, I am registered under my maiden name – Hill)

PKI

What is this thing, really?

The world that we exist in today depends on networks. Instantaneous, worldwide, accessibility is the driving force of our economy and ultimately our very existence. To that end is the desire to connect to everyone, everywhere, all the time, and yet still be able to accomplish a private transaction. This can be likened to wanting to have a party to fill a football stadium and having the bathrooms on the fifty-yard line in the center of the field. How do you keep the private things private?

Cryptography is the science and practice of encrypting and decrypting data by using secret codes, and also allows for authentication of the origin and content. Users of cryptography share some known factor or key to encrypt and decrypt the data they wish to exchange. So as you can see, the foundation of good cryptography is the ability to establish a secure communication system in order to initially exchange the shared secret. But how do you do that unless you already have a secure communications system? This is where cipher keys come into play.

There are two types of keys, symmetric and asymmetric. The first of these, symmetric, uses the same key to encrypt and decrypt data. It is almost immediately apparent why this can be a problem. In order to send someone a secure text message you must share the decipher key with them, but you do not want to send them the key unless you can encrypt it with still another shared secret or key. So obviously in order for this type of cryptography to work properly the sender and the receiver must have some way to exchange a key prior to data transmission. Accomplishing this may be difficult or inconvenient in some environments or situations. Additionally, every user must have a key for every other user that they want to share secured information with. Therefore the storage, administration, and maintenance of an even a relatively small number of users and their keys could be a very daunting task for even the most organized person.

Secondly, there are asymmetric keys, which use two, logically different but mathematically connected keys. The mathematic details of how these keys are related and can be used to encrypt and decrypt each other's text will not be discussed here. Sufficed to say that these types of computations are referred to

[1] Reference VII page 17

as "trapdoor functions with high computational complexity."[1] The public key, as the name suggests, is made publicly available and can be stored in a database repository of public keys. The private key is typically stored in a digital certificate or some other media controlled by the user. Rest assured that making the associated public key openly available does not compromise a private key.

Both the public and private key must be stored in some fashion. They can be stored as files, entries in a database, or on a smart card. The public keys must be available and trusted so users can find the key of the entity they wish to exchange data with, and the user can be confident they are exchanging secure transactions with the correct entity. Transversely private keys must be kept secure. As you may have well guessed, keeping the private key a secret is the oil that ensures the concept of public key encryption technologies work.

Now how does all this work? A user has some entity they wish to transmit, in a secure manner, to a recipient. First, the data item is encrypted with the recipient's public key. If the recipient is unknown to the sender they can be relatively confidant that they are sending the item to the correct person because their public key was acquired from a trusted (Certification Authority) CA. The data is encrypted with some cryptographic algorithm, which produces a static block of what appears to be gibberish text. That block is then transmitted to the receiver who decrypts it with their corresponding private key. During transmission if the data block is manipulated in any way the corresponding decryption algorithm will not be able to decrypt the data properly if at all.

As you can see, public key cryptography solves several of the problems associated with symmetric key technologies, but has a few problems of its own. Since public keys are just that, public, how do you validate and trust the owner of a public key? How do address the fact that public keys are susceptible to spoofing and "man-in-middle" attacks? How do you manage the creation, use and termination of key pairs?

> But public key cryptography, on its own, is not enough. We also need security policies, products to generate, store and manage the keys, and procedures to dictate how the keys and certificates should be generated, distributed and used.[2]

Public-Key infrastructure (PKI) is the integration of software, hardware, encryption technologies and services for managing public keys. PKI provides for

[2] Reference I, "What is a Public Key Infrastructure (PKI)?" section

the four basic requirements of a secure system. Confidentiality to keep information private, Integrity to prove that information has not been changed, Authentication to prove the identity of the sender, and Non-repudiation, which ensures that the information originator cannot deny ownership. Cryptography allows data to be transmitted across a vast public network such as the Internet while preserving the confidentiality of its contents. Integrity is ensured because only data that has not been tampered with can be decrypted. The trusted CA that validates the identity of the recipient's public key preserves authenticity. Owner ship of the data cannot be repudiated once it has been signed by the sender's public key.

> There are two basic operations common to all PKI's, certification and validation. Certification is the process of binding a public-key value to an individual, organization or other entity or even to some other piece of information such as a permission or credential. Validation is the process of verifying that a certificate is still valid.[3]

Typically digital certificates are issued to users and servers as means of verifying or authenticating that a specific key belongs to a specific entity. By binding a user to a public key attacks can be mitigated. A digital certificate is the digital equivalent of a state issued identification card. Depending on the type, certificates can contain a plethora of information. At a minimum, they generally have information about the issuer (CA), the owner, the public key algorithm, and the digital signature of the certificate authority (CA), a trusted third party. A digital signature is a block of data (e.g. digital version of CA's signature) encrypted with the sender's private key. This ensures the integrity of the data and the signer's liability for the content cannot be repudiated, because as stated before, if the data is changed in any way the corresponding private key will not be able to decrypt the data.

The main job of PKI is to establish the trust hierarchy between the CA, Registration Authority (RA), and the certificate repository. There can be several RA's, also called Local Registration Authorities (LRA) associated with a single CA. RA's are district supervisors for a CA in order to make certificate management more scalable and often times more cost effective. An RA validates a requestor's identity and issues a new certificate and then a CA signs the certificate with his (CA) private key. The CA is given the authority to issue, accept, and revoke

[3] Reference V, page 480

certificates as well as dictate how keys are generated, registered, certified, stored, and made available in accordance with defined security policy detailed in Certificate Practice Statements.[4] An entire PKI could be rendered untrustworthy and therefore useless should the CA's private key be compromised.

In order to allow for enterprise wide access to public keys, certificates are often stored in a repository known as a directory server. Additionally revoked certificates, those that are no longer valid, are place in a Certificate Revocation List (CRL) database. The CRL should be referenced when a certificate is requested, because a revoked certificate would not exactly ensure a secure communication. Note that repeated attempts to use a revoked certificate could be evident of an attack or at least suspicious activity.

PKI sounds like the solution to the digital world's security problems. So what is the catch?

"Security is only as strong as the weakest link."[5] In a Public Key Infrastructure there are several potential weak links, such as hardware, software, and the ever-present human factor. The CA is defined as the "trusted" third party. Who is authenticating and certifying the reliability and identity of the CA or the RA's certificate issuing system? How does is the identity of a certificate requestor verified before issuing them a certificate?

First lets address the ever present and always unpredictable human factor. Users usually have their private keys stored on computer systems that they leave vulnerable to attack. Or they use on smart cards that can be lost or stolen. And more often then not, if they even use password protection it is weak at best. So this forces you to consider how the users are protecting, or not protecting, their private keys?

The biggest obstacle for most organization is that implementing a PKI solution is currently far too costly and complex. Most likely all of the PKI components that you wish to implement will not be available from a single supplier. So interoperability issues abound. To make matters worse PKI standards are still in the embryonic stages an in some instances are non-existent. Widespread implementation of PKI is still not a reality and therefore the cost can be a pretty heavy burden for some organizations to bear.

The government is probably the biggest proponent of PKI and is pushing hard for standardization. With huge coffers, and no need to actually turn a profit, the government may be the break that PKI needs. Time and money resources can prove invaluable for a fledgling technology. A standard single source PKI solution

[4] Reference I
[5] Reference VIII, page 1

may be on the horizon with the help of government research and development dollars.

Ultimately PKI may be viewed at the underlying technology to support authentication, integrity, confidentiality and non-repudiation. But there are limitations that must be considered. There is no such thing as a single all inclusive security solution. Information, vigilance, and patience are the best tools at our disposal in unlimited supply at no charge. Management can't argue with that.

References

[I] Baltimore Learning Center. "Introduction to PKI." 2001.
URL: http://www.baltimore.com/library/pki//pki-security.html (4/20/01).

[II] Hurwicz, Michael "A PKI Primer." Web Tools. February 26, 2001.
URL: http://www.webtools.com/story/TLS20010222S0001 (4/19/01).

[III] Verisign "Understanding PKI."
URL: http://verisign.netscape.com/security/pki/understanding.html (4/20/01)

[IV] Verisign "Benefits of PKI."
URL: http://verisign.netscape.com/security/pki/benefits/index.html (4/20/01)

[V] Tipton, Harold F. and Krause, Micki. Information Security Management Handbook, 4th Edition. Auerback Publications, 2000.

[VI] Tipton, Harold F. and Krause, Micki. Information Security Management Handbook, 4th Edition, Volume 2. Auerback Publications, 1999.

[VII] Adams, Carlisle and Lloyd, Steve. Understanding Public Key Infrastructure Concepts, Standards, and Deployment. MacMillan Technical Publishing, 1999.

[VIII] Ellison, C. and Schneire, B. "Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure." Computer Security Journal, v16, n1, 2000
URL: http://www.counterpane.com/pki-risks.html (4/20/01).

Multiple Choice Questions:

1. Q: The three basic requirements of a secure system are:
   a: Confidentiality, Integrity, Authentication, and Non-repudiation
   b: Confidentiality, Integrity, Validation, and Non-repudiation
   c: Integrity, Validation, Repudiation, and Asymmetric Cryptography
   A: (a) PKI provides for the three basic requirements of a secure system. Confidentiality to keep information private, Integrity to prove that information has not been changed, Authentication to prove the identity of the sender, and Non-repudiation, which ensures that the information originator cannot deny ownership.

2. Q: Digital certificates that are no longer valid are keep where?
   a: a locked storage room with an audited control mechanisms
   b: on the Certificate Revocation List (CRL)
   c: on the Certificate Invalidation Listing (CIL)
   A: (b) Revoked certificates, those that are no longer valid, are placed in the Certificate Revocation List (CRL).

3. Q: A symmetric key is defined as:
   a: using a public key to encrypt and a private key to decrypt
   b: using a private key to encrypt and a public key to decrypt
   c: using the same key to encrypt and decrypt
   A: (c) Symmetric key cryptography uses the same key to encrypt and decrypt.

4. Q: An asymmetric key is defined as:
   a: using a public key to encrypt and a private key to decrypt
   b: using a private key to encrypt and a public key to decrypt
   c: using the same key to encrypt and decrypt
   A: (a) Asymmetric key cryptography is a key pair where a user uses someone public key to encrypt a message and the recipient uses their private key to decrypt..

4. Q: The only security risk associated with a system that most likely will never be able to be mitigated with 100% assurance is:
   a: certificate authorities
   b: users
   c: smart cards
   A: (a) System users (the human factor) will be ever present and always unpredictable.

True/False Questions

1. Q: Certification and Authentication are the two basic operations common to all PKI's. A: False - Certification and Validation are the two basic operations common to all PKI's.

2. Q: The RA is defined as "trusted" third party. A: False - The CA is defined as "trusted" third party.

3. Q: Cryptography is the science and practice of encrypting and decrypting data. A: True.

4. Q: It is critical to keep the public key of a key pair well guarded to prevent spoofing or "man-in-middle" attacks. A: False – It is imperative to keep the private key of a key pair private in order to secure your data transmissions. You must however make your public key available or public in order to utilize the benefits of asymmetric cryptography. Certificates are used to mitigate attacks on public keys.

5. Q: PKI can be viewed as the single all inclusive security solution. A: False – no such animal exists..

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event