Introduction to PKI and Certificate Authorities

InterWorks 2001

Session # 23

Ben Rothke, CISSP, CCO
Senior Security Consultant
Baltimore Technologies
ben.rothke@baltimore.com

About me...

- Who I am
  - Senior Security Consultant with Baltimore Technologies
  - Previously with Ernst & Young, Citibank
- Who Baltimore Technologies is
  - Leading e-security company
  - A global leader in e-security products, services & solutions
  - Over 1,200 employees worldwide

Session agenda

This session is:

- An introduction to PKI & certificate authorities (CA)
- Explanation of how a CA operates

This session is not:

- Comprehensive product/vendor investigation
- Vendor bashing
- Legal, privacy or social issues

Technology has changed

- You know the risks, you have seen the pie charts & stats
- The Internet has transformed the entire IT infrastructure
- There is hardly a Fortune 500 company without some type of external public connection
- Internet connectivity, intranets, extranets, WAN & VPN have myriad benefits, and also bring associated security risks
- The language of the Internet is TCP/IP. But security was not added to TCP/IP until version 6 <1998>
- And given that >95% of the Internet is running TCP/IP v4, it's built on and running on an insecure infrastructure.

Goals of Security

- Availability
  - Is the information available to the right people?
- Integrity
  - Is the message received the same as the one sent?
- Confidentiality
  - Can anybody else look at my private information?
- Non-Repudiation
  - Can you deny that you sent this message?

Overview of Information Security

Yesterday		Today
Internal focus Access is granted to employees only	→	**External focus** Suppliers, customers, and prospects all need some form of access
Centralized assets Applications and data are centralized in fortified IT bunkers	→	**Distributed assets** Applications and data are distributed across servers, locations, and business units
Prevent losses The goal of security is to protect against confidentiality breaches	→	**Generate revenue** The goal of security is to enable eCommerce
IT control Security manager decides who gets access	→	**Business control** Business units want the authority to grant access

A matter of trust

- PKI in a nutshell - Establishing digital trust and maintaining that level of assurance
- In the real world, trust is built through a complex web of social, legal, national, international and business interactions that often take years or decades to develop.
  - drivers license
  - ID badges
  - credit cards
  - passports
  - treaties
- What the above provides is trust, underwritten by the providing authority. Unfortunately, that same level of trust is much harder to implement in the electronic world.

Authentication today

- Authentication today = username + password
- Even with tokens, what if half of your users are using SecurID in bypass mode?
- What is wrong with username + password, let me count the ways....

Problems with passwords

- Insecure - Given the choice, people will choose easily remembered and hence easily guessed passwords such as names of relatives, pets, phone numbers, birthdays, hobbies, etc.
- Easily broken - Programs such as crack, SmartPass, PWDUMP, NTCrack & l0phtcrack can easily decrypt Unix, NetWare & NT passwords.
    - Dictionary attacks are only feasible because users choose easily guessed passwords!
- Inconvenient - In an attempt to improve security, organizations often issue users with computer-generated passwords that are difficult, if not impossible to remember
- Repudiable - Unlike a written signature, when a transaction is signed with only a password, there is no real proof as to the identity of the individual that made the transaction

PKI enables Security

Security is an enabler to eCommerce

- integrates multiple information sources and business functions to a single point of access
- allows expansion into new markets and new business capabilities
- selling point for a company's eCommerce services
- increased level of trust and reduced exposure to fraud
- automated vs. procedural security results in more reliable processing and fewer errors
- users unknown to one another can communicate securely
- enables cryptographic services to secure applications over insecure networks

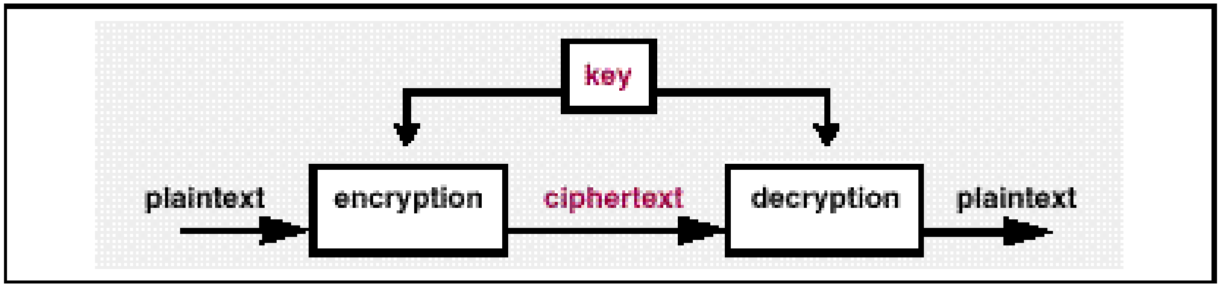
Public-key cryptography

- PKI is built on top of public-key cryptography
  - Public-key cryptography is a form of encryption based on the use of two mathematically related keys (the public key and the private key) such that one key cannot be derived from the other.
- Why use it?
  - User Authentication
  - Data Confidentiality
  - Message Authentication and Integrity
  - Non-Repudiation

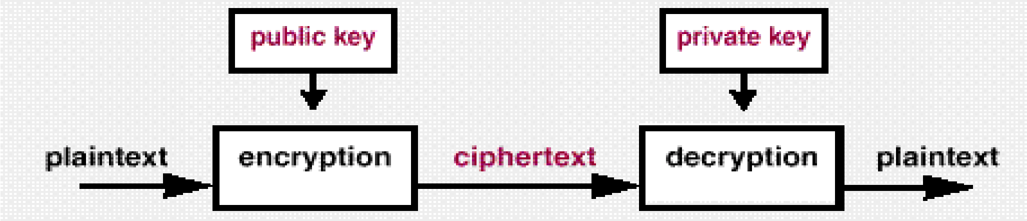
Public-key cryptography

- Conceptual ideas developed by Whitfield Diffie and Martin Hellman in 1976 to solve key management problems.
  - You need a secure channel to set up a secure channel.
  - How do you get the key to the recipient without someone intercepting it?
- First public-key cryptosystem designed by Ron Rivest, Adi Shamir and Len Adleman (RSA) in 1977.
- In a public key system, each user has a publicly known encryption key, and a corresponding private key, known only to that user.
- When sending a private message to someone, you encrypt that message with their *public* key. When they receive it, they decrypt it using their *private* key.
- The private key is used for confidentiality and the public key is used for authentication.

Public vs. private key



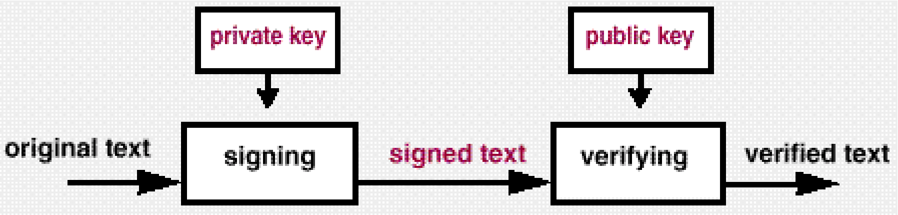
Secret-key (symmetric) encryption



Public-key (asymmetric) encryption

Digital Certificates

- Used to authenticate the identity of the message sender or the signer of a document and to ensure that the original content of the message or document has not be altered.



Just what is a PKI?

A set of technologies that enables an organization to ensure that similar levels and forms of trust that exist in the physical world are implemented in the digital world.

– Secure envelopes	<=>	encryption
– Confidentiality	<=>	encryption
– Ink signatures	<=>	digital signatures
– Passport	<=>	digital certificate
– Issuing authority	<=>	certificate authority

PKI is not an intuitive name

- A problem with PKI is its name.
  - PKI technology is no more complex than any other technology (NT, Unix, Sybase, Norton UnErase, etc.).
- But management often gets confused by the appellation *public-key infrastructure*. PKI is not an intuitive definition
- If we could change the name to *eTrust*, *SafeComputing*, *Don’t Worry – Transact!* or comparable, a lot of the confusion would go away.

PKI Do's & Dont's

Do:

- Take significant time for research, planning, and designing a strategy for your corporate PKI implementation
- Get all corporate divisions involved
- Get high level (CIO, CEO) support
  - Business needs must drive security agenda
- Expect to do major infrastructure re-engineering
- Have a budget for the project
- Be able to sell this to management without using technical jargon
- Perform a risk analysis
- Know that the technology is not the primary issue

PKI Do’s & Dont’s

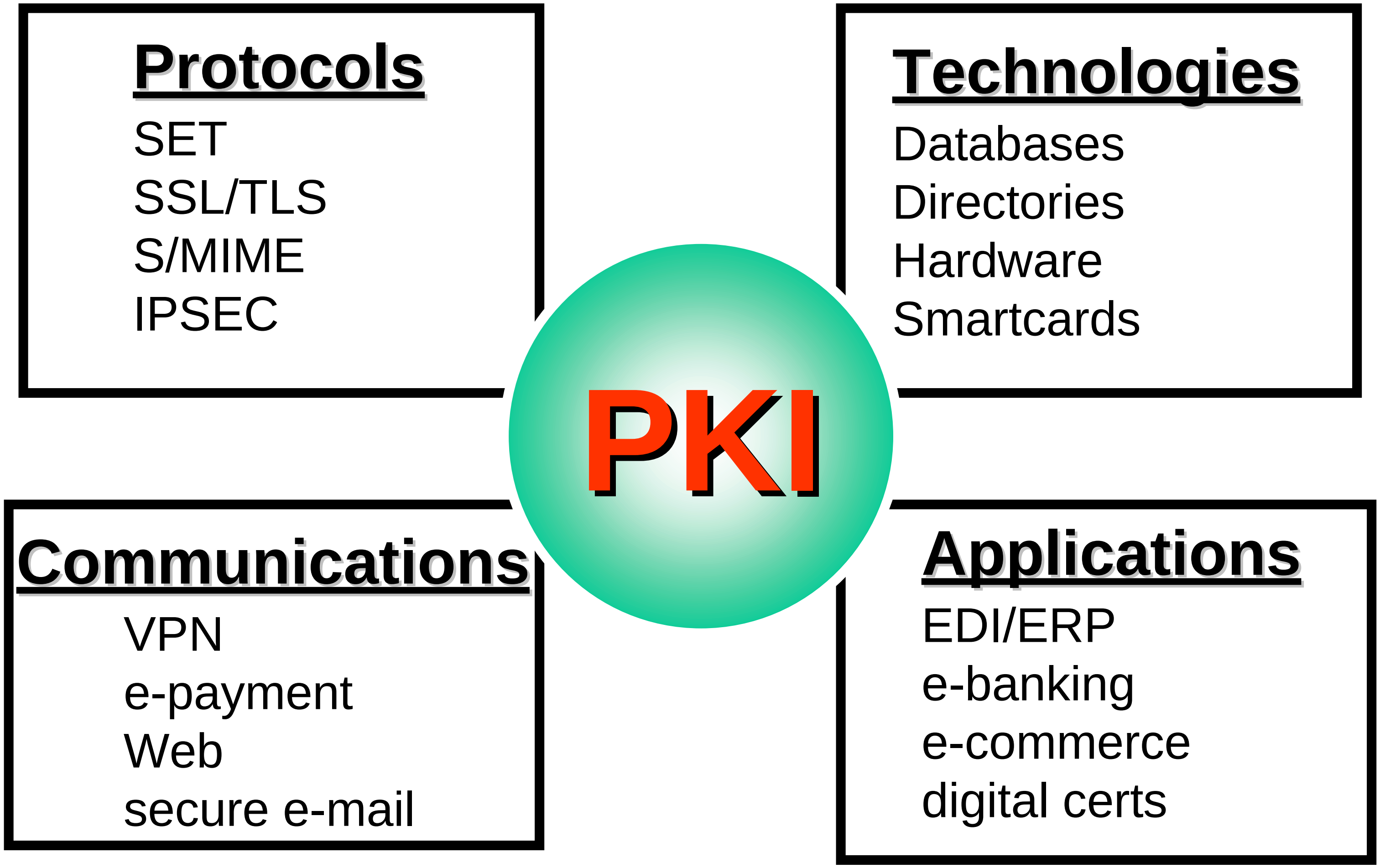
Don’t:

- Pick a PKI vendor until you know your needs
- Believe often exaggerated or useless marketing material
- Get into PKI religious wars (Entrust vs. Verisign, Baltimore vs. Xcert) before performing a complete architecture and technology assessment.
- Rush to get the PKI installed & running
- Expect PKI to solve all of your security problems

Risk analysis

- A study should be undertaken of the process and information flows involved in the proposed PKI system, focusing on the weakest links. These may be individual computer systems with the potential to be hacked, or they may be staff operating under different levels of control.
- Could consider the cost to the organization of a successful attack, and the cost an attacker must pay to mount the attack. Establish the computing power needed for a different types of attacks.
- Since human weaknesses can always be exploited at far lower cost by an adversary, ensure that the risk analysis covers staff roles and responsibilities.

PKI is the glue



Protocols

SET
SSL/TLS
S/MIME
IPSEC

Technologies

Databases
Directories
Hardware
Smartcards

PKI

Communications

VPN
e-payment
Web
secure e-mail

Applications

EDI/ERP
e-banking
e-commerce
digital certs

Certificate authorities

The CA is the mechanism that issues the actual certificates, & implements the defined policies & procedures on how those certificates are to be utilized.

These policies and procedures are detailed in the Certificate Policy (CP) and Certificate Practice Statement (CPS)

What does a CA do:

- Generates, updates & manages certificates
- Signs certificates
- Stores users private keys
- Generates & publishes CRL
- Cross certifies other CA

Certificate authorities

Who can be a certificate authority?

– Any organization that has the ability to verify the binding between a public key and an entity, depending on the application or role.

- A company, for its employees
- DMV, for drivers in the state
- American Express, for its cardholders
- University, for its students and faculty
- United States Government, for its citizens
- Bruce Springsteen for members of the E-Street Band
- You, for your family, relatives and friends

Your own personal CA

- As an example, PGP has no central authority or hierarchical trust, rather it implements a *web of trust* architecture
- Individuals sign each others keys which progressively forms a web of individual public keys interconnected by links formed by these signatures
  - Therefore, any PGP user can act as a CA, and can also validate another PGP user’s public-key

Certificate authorities

As CA begin to proliferate, the main quandary will be how to deal with:

- so many certificate authorities
- users with so many different certificates
- so little trust
- the difficulty of cross certification
- interoperability
- lack of standards
- legal issues
- indemnity issues

Registration Authorities

- The registration authority (RA) which is an optional component in the PKI, is a subordinate server to which a CA can delegate management functions.
- The RA may perform varied authentication tasks, report on revoked certificates, generate keys or archive key pairs.
- RA can be useful in creating implementations that are more scaleable since they allow organizations to distribute functionality across the network.
- While RA offer the advantage of task delegation, they also come with the disadvantage of lengthening the security loop that must be managed.

Digital Signatures & Certificates

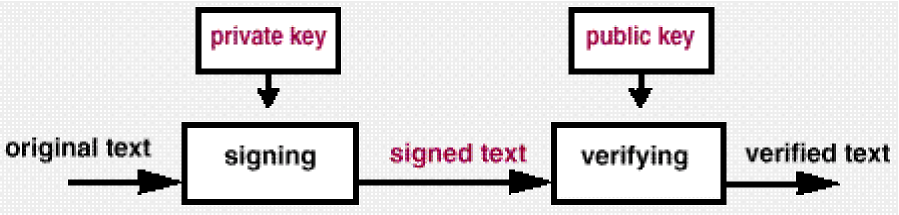
- Digital Signature - The encryption of a message with a private key.
- Digital Certificate - An electronic document binding pieces of information together; generally:
  - name
  - serial number
  - expiration dates
  - copy of the certificate holder's public key
  - digital signature of the CA. So that a recipient can verify that the certificate is real.

Digital Signatures & Certificates

- A digital certificate is simply an electronic credential.
- Used to authenticate the identity of the message sender or the signer of a document and to ensure that the original content of the message or document has not be altered.
- The certificate is protected by a users private/public key pair and a passcode.
  - So even if someone obtains your certificate, that is not enough without your passcode.
- The value of the certificate is determined by the CA that issues it. Just as it is possible to get a worthless identification card in Times Square, so is it possible to get a worthless, albeit cryptographically strong digital certificate.

Digital Signatures & Certificates

- Used to authenticate the identify of the message sender or the signer of a document and to ensure that the original content of the message or document has not been altered.
- The process of digitally signing starts by taking a mathematical summary (called a hash code) of the file. A hash code is a uniquely-identifying digital fingerprint of the file. If even a single bit of the file changes, the hash code will change. The next step in creating a digital signature is to sign the hash code with your private key. This signed hash code is then appended to the file.



Digital Signature verification

- The recipient of the file can verify the hash code sent by using the public key.
- At the same time, a new hash code can be created from the received file and compared with the original signed hash code.
- If the hash codes match, then the recipient has verified that the file has not been altered.
- The recipient also knows that only the sender could have sent the file because *only the sender has the private key that signed the original hash code.*

What’s in the digital certificate?

- User’s name
  - In the format of a distinguished name (DN), which specifies the user’s name and any additional attributes required to uniquely identify the user (for example, the DN could contain the user’s SSN, employee number, etc.)
- Public key of the user
  - Required so that others can verify the user’s digital signature
- Validity period (lifetime) of the certificate
  - Start & end date
- Approved operations
  - For which the public key is to be used (whether for encrypting data, verifying digital signatures, or both)

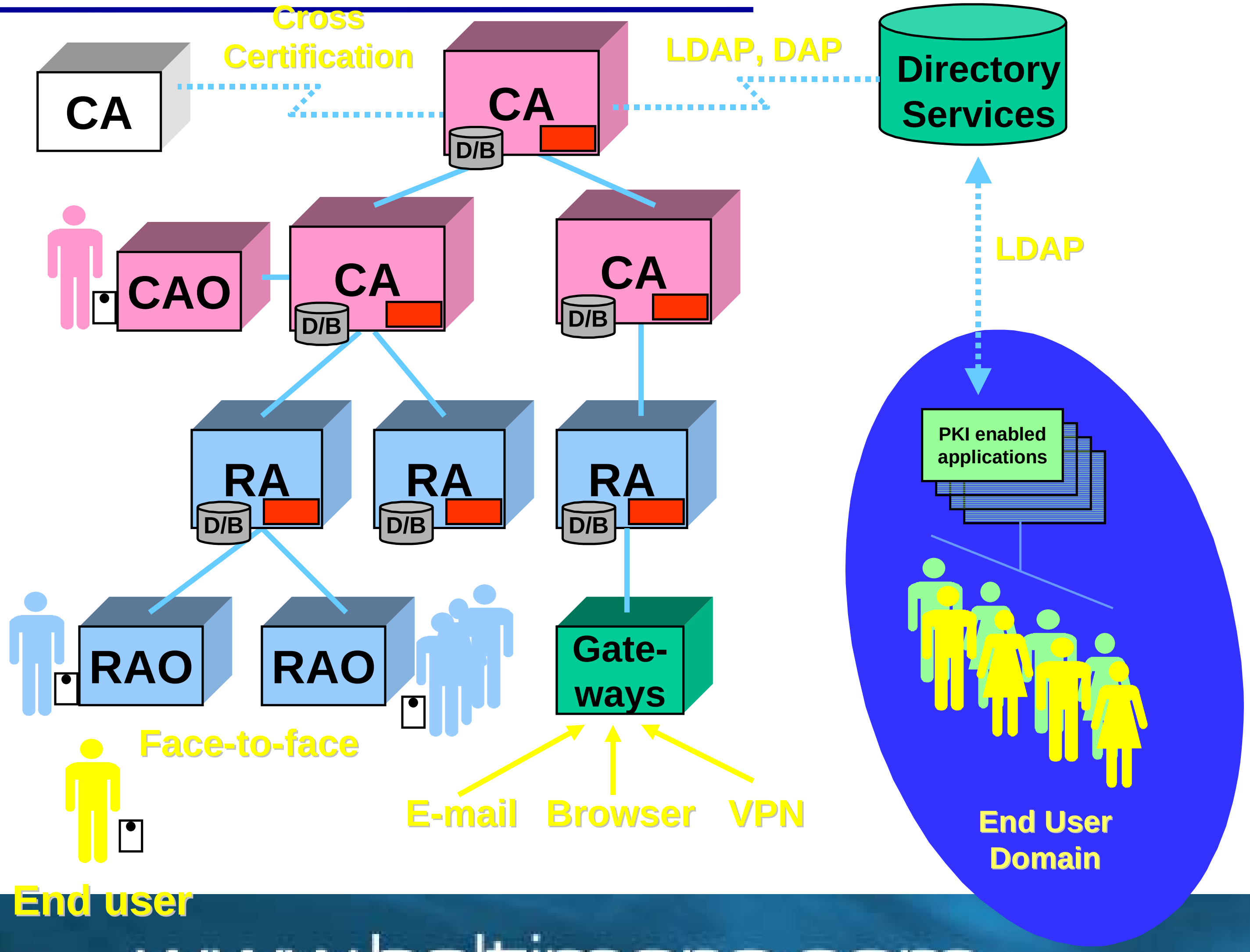
Directories

- Since the CA is the trusted 3rd-party, it must have a means to distribute certificates so they can be used by users and applications. A directory is a certificate repository that stores certificates so applications can retrieve them on behalf of users.
- LDAP (Lightweight Directory Access Protocol) has become the de facto directory of choice for many PKI systems.
- LDAP is a preferred solution due to many factors:
  - can support huge amount of users
  - very scaleable & distributed
  - responds efficiently to search requests
  - an open standard (RFC 1777)
- LDAP is based on X.500, which is a huge, complex protocol that is overkill for PKI

Directories

- Directories provide an efficient means for certificate storage and retrieval within a PKI system.
- The CA populates its directories with certificates and Certificate Revocation Lists (CRL).
- Client applications can then use the directory to retrieve the certificate based on a parameter such as name or e-mail address.
- Additionally, clients can check the CRL to determine whether a individual certificate is revoked or not.

A pictorial view



Certificate revocation

- Since many certificates have a long lifetime, certificates that are no longer trustworthy and have not expired must be revoked by the CA. Why may a certificate revoked?
  - Compromised or stolen private key
  - user forgets passphrase
  - user resigns or is terminated
  - change in corporate policy
- Users & applications must be informed that the continued use of the certificate is no longer considered secure.
- The revocation status of a certificate must be checked prior to each use. As a result, the PKI must incorporate some type of revocation system.

Certificate revocation

- The CA must be able to securely publish information regarding the status of each certificate in the system.
- Application software, on behalf of users, must then verify the revocation information prior to each use of a certificate.
- The most popular means for distributing certificate revocation information is for the CA to create secure (via digital signature) certificate revocation lists (CRL) and push these CRL to the directory

Certificate revocation

- CRL specify the unique serial numbers of all revoked certificates.
- Prior to using a certificate, the client-side application must check the appropriate CRL to determine if the certificate is still trustworthy.
- Client-side applications must check for revoked certificates consistently and transparently on behalf of users.

Problems with CRL

- Since the CRL issued by a CA must include all valid certificates issued by that CA that have been subsequently revoked, it can become extremely large.
- The size of the CRL is proportional to the size of the user base, lifetime of the certificates, and the probability of a revocation.
- For large CA, the bandwidth to support the CRL can become huge, and it is becoming impractical for large organizations to support standard CRL
- CRL do not contain a positive response. The absence of a certificate from a CRL indicates that it isn’t revoked

More effective CRL solutions

- CRL Distribution Points
  - Fragment the full set of certificates issued by the CA into sub-sets, so that each fragment can have its own smaller CRL. Certificates can have a pointer to the CRL fragment where its revocation status is indicated
- OCSP (Online Certificate Status Protocol)
  - IETF working group designing a better CRL system that provides users with revocation information for individual certificates. Users do not receive information about certificates they have no need for.
- Delta CRL
  - Uses a base CRL. Delta CRL are then issued more frequently and only contain updates to the base CRL. Since they are small, they can provide timely information without unduly consuming network resources

Cross certification

- An extension of 3rd-party trust in which two CA securely exchange keying information so that each can certify the integrity of the other’s keys
- Before cross certifying, each company must understand the others security policies, and have assurance that their security policies will be followed on the remote side.
  - In a nutshell, Company A says to Company B “Trust Me”
- When two CA cross-certify, each CA requests cross-certification from the other. When that request is received, each CA signs the other’s verification public key in a cross-certificate. The result is two-cross certificates.
  - Mutual cross-certification (bilateral)
  - Unilateral cross-certification

Policy

Policy is a critical element in the effective and successful operation of a PKI. A PKI can’t be effective unless it is deployed it in the context of working policies that govern the use, administration, and management of certificates.

In a similar vein, Marcus Ranum defines a firewall as:

“the implementation of your Internet security policy. If you haven’t got a security policy, you haven’t got a firewall. Instead, you’ve got a thing that’s sort of doing something, but you don’t know what it’s trying to do because no one has told you what it should do”.

Policy

Certificate policy

- Controls use of certificates
- X.509 defines certificate policy as: a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Certificate practice statement (CPS)

- Assertion of the practices that a CA employs in managing the certificates that it issues. The CPS should describe how the certificate policy is interpreted in the context of the system architecture and operating procedures of the organization
- Without a CPS, there will be a ambiguity and confusion as to who is responsible for what

Certificate practice statement

1. Introduction

Overview

Identification

Community & Applicability

Contact Details

References

Definitions

2. General Provisions

Obligations

CA Obligations

RA Obligations

End User Obligations

Interpretation and Enforcement

3. Identification and Authentication

Initial Registration

Identity verification process

Identity Verification Check

Certificate Renewal

Revocation Request

4. Operational Requirements

Physical & logical controls

5. Technical Security Controls

Key properties

Key Strength

Private key distribution

Confidentiality key archive

Evidence required to retrieve a key

Compromise of CA keys

6. Certificate and CRL Profiles

Certificate Profile

CRL Profile

7. Specification Administration

Specification Change Procedures

Publication and Notification Procedures

8. Policy Status

From: www.baltimore.com/download/index.html
Also see Certificate Policies and Certification Practice Statements at:
www.entrust.com/downloads/pdf/cps.pdf
www.verisign.com/repository/CPS/CPS-1_2-009.doc

PKI standards

- PKIX (Public-Key Infrastructure)
  - Proposed IETF standard that provides a framework to integrate the various public key tools into a PKI based on X.509
- SPKI (Simple Public Key Infrastructure)
  - Competing standard to PKIX. Being developed by another working group within the IETF. SPKI is simpler than PKIX and oriented towards privilege authorizations.
- PKCS (Public Key Cryptography Standards)
  - Series of standards developed & maintained by RSA. In lieu of any formal standards availability, PKCS has served as a practical guide for design & implementation of public key encryption technology.
- SESAME (Secure European System for Applications in a Distributed Multi-vendor Environment)
  - European effort that encompasses PKI and Kerberos. Developed by RACE, Bull SA, ICL & Siemens-Nixdorf. Much broader than PKIX and backed by European countries.

Physical Security Requirements

- Access to the building/floor/room in which the CA servers are located
- Physical access controls for backup tapes, media containing cryptographic keying material
- Fire-suppression systems
- UPS
- Water/flood alert devices exist
- Other environmental or physical access controls
- Background checks for information security staff

Misc. legal issues

- The law has not yet had time to adapt
  - Lack of precedents
  - Establishing autonomy
- Legal effect
  - Validity
  - Admissibility
  - Enforceability
- Multiple and overlapping jurisdictions
  - local, state, federal, international
- Liability and indemnity

For further information

- Understanding the Public-Key Infrastructure
  - Carlisle Adams, Steve Lloyd New Riders Publishing 1999; ISBN: 157870166X
- Applied Cryptography: Protocols, Algorithms, and Source Code in C
  - by Bruce Schneier John Wiley & Sons 1995 ISBN: 0471117099
- Secure Electronic Commerce: Building the Infrastructure
  - Warwick Ford & Michael Baum Prentice Hal 1977 ISBN: 0134763424
- Ten Risks of PKI
  - www.counterpane.com/pki-risks.html
- Why Cryptography Is Harder Than It Looks
  - www.counterpane.com/whycrypto.html
- Security Pitfalls in Cryptography
  - www.counterpane.com/pitfalls.html

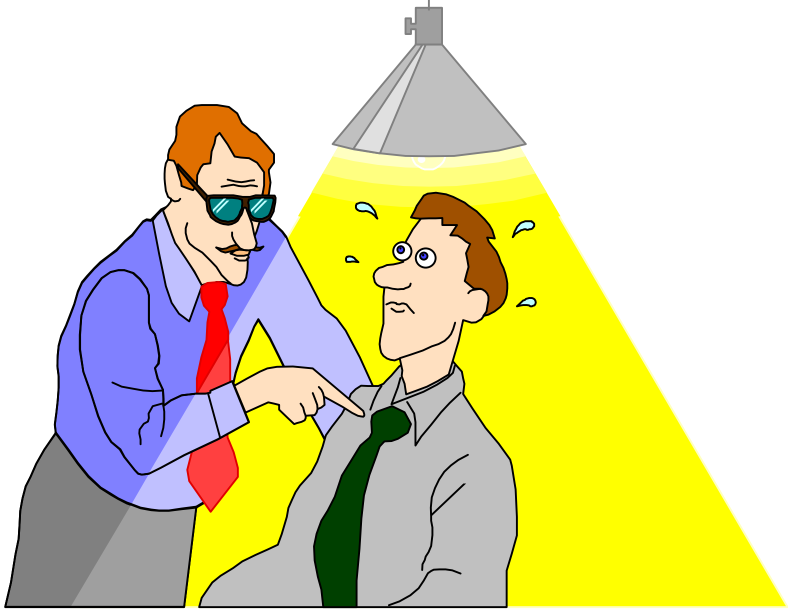
Conclusion

PKI is one of the hottest technologies around and is the foundation of an effective e-commerce infrastructure. Yet PKI means a lot of different things to different people.

By better understanding what PKI can, and can't achieve, your move towards PKI implementation will be more effective.

Thanks for attending

- Any questions? comments?
- Please fill out your evaluation sheets



Ben Rothke, CISSP, CCO

Senior Security Consultant

Baltimore Technologies

ben.rothke@baltimore.com

973/202-7921