

PKI - Public Key Infrastructure

August 21, 2006

Copyright 2006 by James Lee and Brian Hatch, Onsite
james@onsight.com, bri@onsight.com

PKI

Objectives of This Talk

Topics discussed today:

- an overview of PKI
- PKI and certificates
- DOEGrids and Kerberized CAs
- uses of certificates

Topics not discussed today (covered in the 1/2 day class):

- public key encryption
- creating a good passphrase
- installing certificates
- signed and encrypted e-mail

What is PKI?

What is PKI?

What is PKI?

- Public Key Infrastructure
- an infrastructure that is available for an application to "plug into" and use on an as-needed basis (much like the electricity infrastructure)
- maintains a trustworthy networking environment by knowing who is requesting access or providing service
- can be used by a wide variety of applications including:
 - web browsers
 - email clients
- provides public-key encryption and digital signature services
 - public-key encryption is a way to easily allow people to securely communicate with one another, even if they don't know each other
 - digital signatures are a way to prove to others that you are who you say you are, and you said what we heard you say
- manages keys and certificates
 - a certificate is a digital identifier
 - keys are used to encrypt and decrypt

Why Should I Use PKI?

The Internet can be a dangerous place:

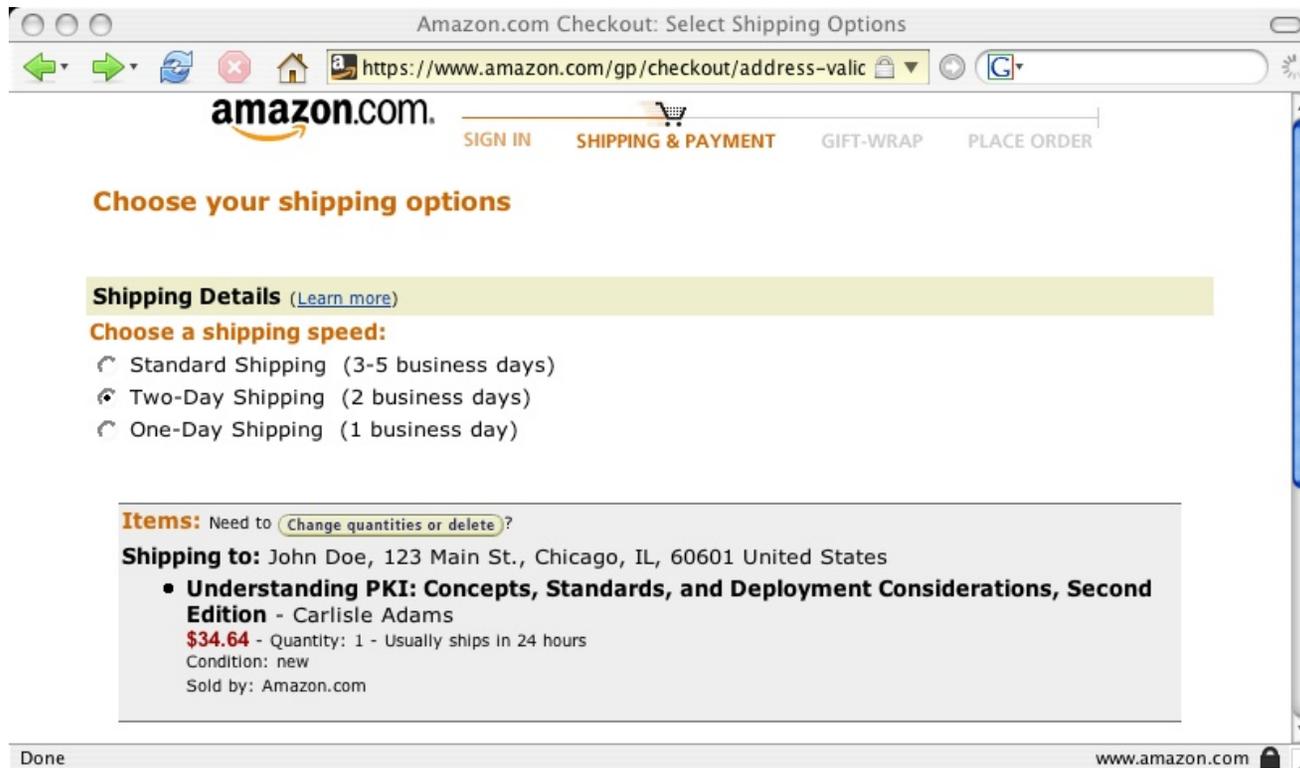


- *identity theft* - loss of good credit, money, sleep
- *data theft* - content of email, usernames, passwords can be sniffed
- *data alteration* - content of emails can be altered between being sent and received
- *confidentiality* - private emails and data can be read, such as emails and sensitive documents

PKI is Used on the Web

If you do any credit card or bank transactions on the Internet, you are probably (should be) using PKI.

- look for the `https://` in the location bar
- uses SSL (Secure Socket Layer) for encrypted communication
- essential if personal information (name, address, credit card, social security number, password) is transmitted



PKI is Used on the Web (cont.)

This is what happens when a secure web page is requested by the browser:

- the browser asks for a web page, such as `https://www.amazon.com/titles`
- the server responds with a *certificate*, a digital identifier, informing the browser of the server's identity by telling the browser who is vouching for the server
- the browser checks to see if it trusts the entity vouching for the server - if so, it tells the server "ok, because I trust who is vouching for you, I trust you"
- the server responds with the HTML page requested
- the browser sends any data, including sensitive data, with the knowledge that it can trust the server

Wouldn't it be nice to communicate with others in a similar trustworthy environment?
That is the purpose of PKI.

What is a Certificate?

A certificate is:

- a digital identifier, verifying the identity of the user or entity
- contains information about the user such as their name, email address, and more
- is "vouched-for" by a trusted entity (called a *Certificate Authority* or CA)

There are two types of certificates used at Fermi:

- DOEGrids
- Kerberos CA (KCA)

More on certificates later.

Will PKI Protect Me?

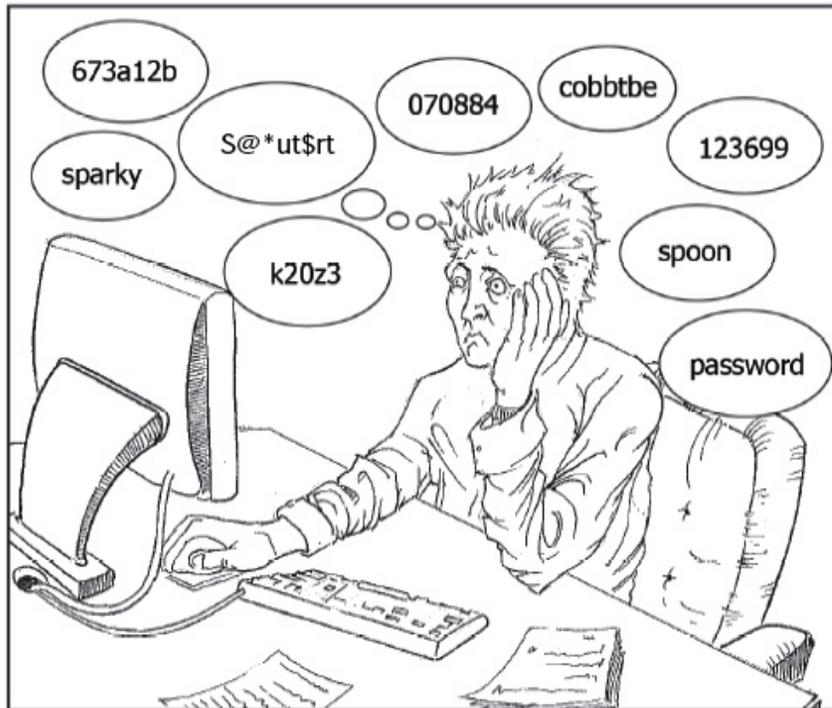
Yes. If a person protects their private key with a strong password, and keeps it secret, then they will be protected.

- provides enhanced two-factor authentication - both a password and a certificate file is required
 - to impersonate you, a cracker needs your password and your computer
 - if the cert is password protected with "", then it is not secure - make sure you have a strong password!
- provides "single sign-on" across multiple websites - your browser can provide your credentials to multiple websites and you only need to remember your one certificate password
- your certificate password never goes across the network - your password is used to decrypt your certificate for your browser, email client, etc, but is never sent across the network, not in the clear, not even in crypto

Personal Benefits of PKI

PKI will benefit an individual:

- *single secure sign-on* - if PKI is used, remembering passwords will become easier:



- *end user transparency* - after setup, using the infrastructure is almost totally transparent to the user (except when there is an error)
- *comprehensive security* - ensures that a single trusted security model is available throughout the environment

Business Benefits of PKI

PKI benefits to the business include:

- *cost savings* - implementing a single security solution is cheaper than implementing multiple solutions.
- *interoperability* - all applications work with all services
- *consistent implementation* - if all applications use the same solution then installation time, management and maintenance costs decrease
- *possibility of achieving security* - consistent handling of security increases the chance of security and decreases insecure workarounds
- *choice of provider* - an open infrastructure means choice of who will provide service

PKI is Recommended at Fermi

PKI will be used at Fermi:

- Fermi websites and computing resources will request PKI authentication
- DOE is demanding that labs be able to prove and produce an audit trail of what human being corresponds to each "username" -- in this case the "common name" in the certificate
- PKI is to the browser and email world what kerberos is at Fermilab for ssh and ftp users

PKI and Certificates

X.509 Basics

- Detailed in RFC-2459, issued in 1998
- PKI standard
- PKI certificate format specification
- can be stored in many different formats:
 - PEM, used by most unix tools
 - PKCS#12, used by most windows tools
 - `openssl` program can convert between them

X.509 Certificate Information

Contains information about the identity of the key owner including:

- owner's name, organization, email address
- URL (for server keys)
- key serial number (for key revocation)
- date key signed (becomes valid)
- date key expires (no longer valid)

X.509 Certificate Information (cont.)

Here is an example X.509 certificate:

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 4 (0x4)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=US, ST=Washington, O=True You, LLP, OU=True You CA, CN=True You
CA/emailAddress=RootCA@verily_sign.com

Validity

Not Before: **Jun 29 21:37:23 2006 GMT**

Not After : **Jun 26 21:37:23 2016 GMT**

Subject: C=US, ST=Washington, O=Example.com Seattle Branch, OU=IT Department,
CN=**John Doe (jdoe)**/emailAddress=j.doe@example.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:d5:d6:30:5b:b9:8e:4e:23:2d:c6:dc:31:7d:76:
08:81:e8:45:d9:e6:e3:7a:7d:6f:72:24:e0:25:11:
36:11:a5:ee:35:ca:52:4a:e4:17:d7:27:ce:6b:17:
0a:09:97:ca:0a:19:f4:00:d7:11:ad:99:f6:c9:af:
1e:64:2d:50:82:69:7f:b1:b0:99:e7:78:bc:ca:49:
3d:0b:c8:c4:e7:18:10:9c:3b:8c:82:ea:c2:47:1c:
7d:80:8c:cb:5c:0c:48:63:a7:86:0c:f6:a0:d9:dc:
b9:3e:27:61:18:db:75:80:44:23:2e:ff:32:1f:3b:
cf:60:eb:24:82:2c:6f:bd:f9

Exponent: 65537 (0x10001)

X.509 Certificate Information (cont.)

```
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  Netscape Cert Type:
    SSL Client, SSL Server, S/MIME
  Netscape Comment:
    OpenSSL Generated Certificate
  X509v3 Subject Key Identifier:
    90:C3:F3:24:DE:DE:9E:1D:B3:2E:0A:94:D1:03:E9:75:33:0C:57:2D
  X509v3 Authority Key Identifier:
    keyid:21:DE:0B:28:F5:94:90:1F:96:75:54:09:D9:C9:D9:8C:25:5B:4B:F5
    DirName:/C=US/ST=Washington/L=Seattle/O=VerilySign, Inc/OU=Certificates
    Department/emailAddress=RootCA@verily_sign.com
    serial:01
  Signature Algorithm: md5WithRSAEncryption
    8b:33:b3:b3:9a:66:b4:13:07:81:68:ed:ed:9e:62:7d:dc:4b:
    51:4d:83:55:50:20:47:4c:a0:8b:2b:9f:64:f0:f1:f2:97:bc:
    15:bf:73:cf:ff:68:08:90:e0:8d:92:47:f6:c1:de:37:b2:c6:
    68:86:c7:54:30:07:a1:08:75:f4:a5:44:72:2a:8d:ed:d0:23:
    d1:14:b8:66:cd:d1:c8:94:05:c6:a3:32:c1:1b:bb:b0:0b:ab:
    38:b7:67:30:b7:3c:5c:46:99:5e:6c:d9:ca:0a:bf:fd:0c:3e:
    f0:d7:3b:4f:b6:47:02:93:8a:67:6f:0d:43:5a:fe:01:c6:49:
    43:ff
```

X.509 Certificate Information (cont.)

-----BEGIN CERTIFICATE-----

```
MIID2DCCA0GgAwIBAgIBBDANBgkqhkiG9w0BAQQFADCBjTELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCldhc2hpbmd0b24xZjAUBgNVBAoTDVRYdWUgWW91LCBMTFaxFDAS
BgNVBAstClRydWUgWW91IENBMRQwEgYDVQQDEwtUcnVlIFlvdSBDQTElMCMGCSqG
SIb3DQEJARYWUm9vdENBQHZlcm1seV9zaWduLmNvbTAeFw0wNjA2MjkyMTM3MjNa
Fw0xNjA2MjYyMTM3MjNaMIGbMQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGlu
Z3Rvb2EjMCEGA1UEChMARXhhbXBsZS5jb20gU2VhdHRsZSBCcmFuY2gxZjAUBgNV
BAsTDU1UIERlcGFydG11bnQxGDAWBgNVBAMTD0pvaG4gRG91IChqZG91KTEgMB4G
CSqGSIb3DQEJARYRai5kb2VAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANXWMFu5jk4jLcbcMX12CIHoRdnm43p9b3Ik4CURNhG17jXKUkrk
F9cnzmsXCgmXygoZ9ADXEa2Z9smvHmQtUIJpf7Gwmed4vMpJPQvIxOcYEJw7jILq
wkccfYCMylwMSGOnhgZ2oNncuT4nYRjbdYBEIy7/Mh87z2DrJIIIsb735AgMBAAGj
ggE2MIIBMjAJBgNVHRMEAjAAMBEGCWCgsAGG+EIBAQQEAwIF4DAsBg1ghkgBhvhC
AQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydG1maWNhdGUwHQYDVR0OBBYEFJDD
8yTe3p4dsy4K1NED6XUzDFctMIHEBgNVHSMGgbwwgbmAFChEcyj11JAflnVUCdnJ
2Yw1W0v1oYGdpIGaMIGXMqswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3Rv
bjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UEChMPVmVyaWx5U2lnbiwgSW5jMSAw
HgYDVQQLExdDZXJ0aWZpY2F0ZXMGZGVwYXJ0bWVudDElMCMGCSqGSIb3DQEJARYW
Um9vdENBQHZlcm1seV9zaWduLmNvbYIBATANBgkqhkiG9w0BAQQFAAOBgQCLM7Oz
mma0EweBaO3tnmJ93EtRTYNVUCBHTKCLK59k8PHyl7wVv3PP/2gIkOCNkkf2wd43
ssZohsdUMAehCHX0pURyKo3t0CPRFLhmzdHIlAXGozLBG7uwC6s4t2cwtzxcRple
bNnKCr/9DD7w1ztPtkcCk4pnbw1DWv4BxklD/w==
```

-----END CERTIFICATE-----

X.509 Certificate Revocation

Certificate revocation occurs when an entity loses its privilege to authenticate:

- revoke a key if it becomes compromised
- revoke a key if it becomes lost, before a new one is issued
- lists of revoked serial numbers are available

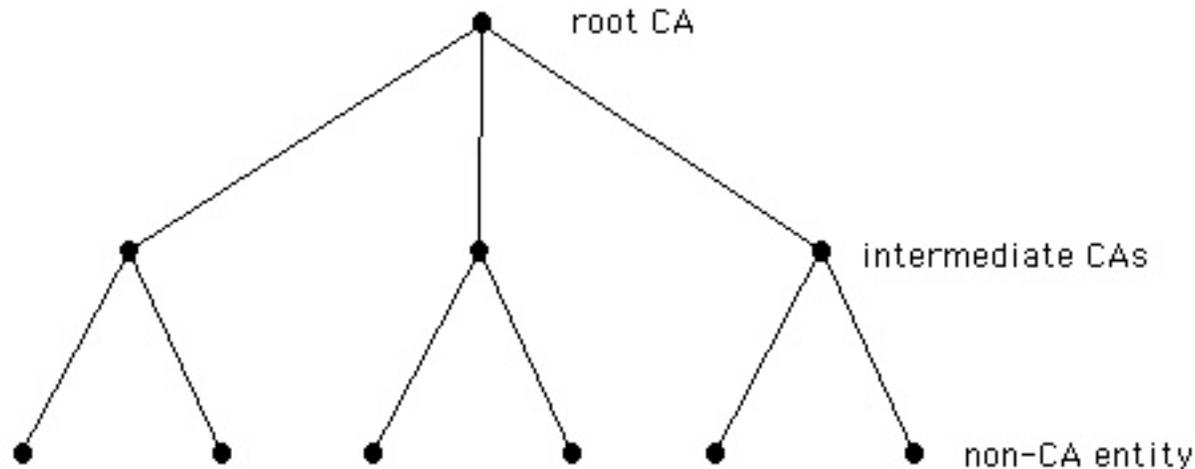
A *certificate revocation list* (CRL) is a list of all certificate serial numbers that have been revoked by a CA. DOEGrids uses a CRL, KCA does not.

Certificate Authorities

- also known as CAs
- the "trusted 3rd parties" that sign keys
- issues digital certificates stating the CA attests to the entity's identity
- here are a few public CAs:
 - VeriSign
 - Thawte
 - GeoTrust
 - DigiCert
 - CAcert.org

Trust Relations Between CAs

- top level (*Root CA*) keys are trusted by virtue of being installed and trusted in your browser or other application.
- root CAs can sign CA keys of other trusted CAs - these are called *intermediate CAs*
- root CAs or intermediate CAs can sign X.509 certificates for entities
 - this creates a *certificate chain*
 - proving your identity means proving you have your public/private key pair, and providing your certificate and every intermediate CA certificate up the certificate chain for verification



Applications that Validate Certificates

There are many applications that support the use of certificates:

- web browsers (Firefox, IE, Opera, etc.)
- email clients (Thunderbird, Outlook, Mutt, etc.)

DOEGrids and Kerberized CAs

DOEGrids and KCAs

DOEGrids:

- service run by ESnet
- long-term personal certificates (1 year)
- required for DOE-related grid computing
- required for access to many restricted DOE websites
- recommended for signing email
- open to a wider audience than just Fermilab
- also provides SSL server certificates

DOEGrids and KCAs (cont.)

KCA at Fermilab:

- provides you an X.509 certificate by virtue of having authenticated against Kerberos
- short-term certificate lifetime, maximum of 1 week - renewed frequently
- more convenient to obtain than DOEGrids cert
- grid access and web page authentication
- not recommended for email signing (life span too short)
- uses KX.509:
 - an open-source means of obtaining short-term X.509 certs using Kerberos
 - issued by Fermilab's KCA and is tied to the user's FNAL.GOV Kerberos principal
 - requires that the user possess current, valid Kerberos credentials

DOEGrids and KCAs

How to choose KCA certs vs DOEGrids certs:

	KCA	DOEGrids
life span	7 days	1 year
access grid resources?	yes	yes
signing email?	not recommended	recommended
access websites and some Fermi resources?	some Fermi	various
use Nessus scanner?	yes	no

Note: not all Fermi websites accept KCA certs.

Uses of Certificates

Web Page Access

Websites can allow authentication via various means:

- form/cookie based authentication (custom CGIs and application code)
- popup username/password dialog boxes (HTTP Basic authentication)
- X.509 certificates

X.509 certificates are better for several reasons:

- requires two-factor authentication - the X.509 cert, and the password
- doesn't require application logic
- simple configuration in Apache and IIS
- authorization can be done via webserver or applications, as desired
- you can use the same cert for multiple web sites
- don't need to close your browser to use a different cert, you do need to close your browser to forget HTTP authentication or cookies.

Other Uses of Certificates

Here are some other uses of X.509 certs:

- URL verification
 - SSL-protected websites signed by a trusted CA can be guaranteed to provide secure access
 - no popup dialog boxes asking you to trust the certificate
 - requires you trust the CA that signed the website certificate
- email signing and encrypting
 - S/MIME standard
- grid resource authentication (grid jobs)

Fermi Platform and Tools

Fermilab uses broad range of platforms and tools:

- OSes include Windows, Linux and Mac OS X
- email is implemented with IMAP servers - NOT Exchange
- email clients include:
 - Outlook Express/Outlook
 - Netscape/Mozilla/SeaMonkey/Thunderbird
 - Eudora
 - .Mail under MacOS
- Browsers include:
 - IE
 - Safari under Mac
 - Firefox/Mozilla/SeaMonkey/Opera under all OSes

In Summary

To summarize about PKI and certificates at Fermi:

- PKI is recommended at Fermi
- PKI has both business and personal benefits
- there are two types of certificates at Fermi: DOEGrids and KCA
- PKI is used for web access and signed/encrypted email

To Learn More About PKI

If you want to learn more about PKI, attend the 1/2 day class. We will talk about these additional topics:

- public key encryption
- creating a good passphrase
- installing certificates
- signed and encrypted e-mail

Check out <http://security.fnal.gov/pki/> for some excellent information about PKI and certificates at Fermi.