Public Key Infrastructure
PKI

Michael Maass and Blase Ur

Outline

- Intro to cryptography
- Intro to PKI / Davis reading
- Current issues
- Gaw reading
- PKI in the enterprise
- Discussion

Introduction to Encryption

- We want to send a secret message
  - Plaintext → Ciphertext
- A **key** is the “secret”
  - BlaseMichael → leahciMesalB
  - BlaseMichael → CmbtfNjdibfm

Types of Keys

- Instructions on how to modify the plaintext
- How many “letters” to shift (Caesar cipher)
- A->C, B->Z, C->J, D->H (Substitution cipher)

...

- Random bit (1 or 0) for every bit of the original (One Time Pad)

Other symmetric systems

- Stream ciphers
- Block ciphers e.g. DES / AES, Twofish

Disadvantages of Symmetric Enc.

- The key is “shared secret”
- Codebooks

Asymmetric Encryption

- “Public Key Encryption”
- Whitfield Diffie and Martin Hellman- 1976
  - (Discrete logarithm is hard)
- Ellis, Cocks, Williamson- 1973

RSA

- Rivest, Shamir, Adelman- 1978
- Public Key- known to everyone
- Private Key- known only to the person who can decrypt the message

Sending Rich my CC#

- Amazon's public key is widely known.

- E(Message, Rich's Public Key)

→ Encrypted message

- D(Encrypted message, Rich's Private Key)

→ Message

Rich's Signature

- Message- “I said this”

- F(Message, Rich's Private Key)

→ Signature

- V(Message, Signature, Rich's Public Key)

→ I believe them

How do we Know Rich's Key

- How do we know Rich's public key?
- Ask him?
- Man In The Middle

Introduction to PKIs

- What is a PKI?
- What do PKIs get right?
- What do PKIs get wrong?

What is a PKI?

- PKI = Public Key Infrastructure
- PKIs bind an identity to a public key
- PKIs come in many forms:
  - Certificate Authority Based – Most familiar
  - Web of Trust Based – PGP's model
  - More we won't talk about...
- PKIs enable encryption and sender authentication for email, authentication of servers to browsers, authentication of users to applications, etc.

Security and Usability, Chapter 16 Making the Impossible Easy: Usable PKI (D. Balfanz, G. Durfee, and D.K. Smetters)

Certificate Authority Model

- A Certificate Authority (CA) sits at the top of a trust hierarchy
- CAs issue digital certificates that contain identity information about the subject, expiration and revocation information, and the subject's public key
- CAs sign digital certificates they issue. If you trust a CA, you trust any certificate they sign that hasn't expired or been revoked
- CAs can be internal to a business, government, or organization or they can be they can be large for-profit multi-national corporations

What do PKIs get right?

- PKIs require less trust than approaches based on symmetric keys
- PKIs have low availability demands
- PKIs are highly reliable
- PKIs are high performance

What do PKIs get wrong?

- PKIs are complicated and loosely defined enough that users don't understand them
  - Users don't understand public key cryptography and therefore the need for PKIs
  - Users don't understand what certificates are for
  - Users don't understand what role PKIs play in what they want to accomplish
- PKIs establish a root of trust that, when compromised, erase the security of any system in which the PKI is required to link identities to public keys
- PKIs suffer from a number of compliance defects

Compliance Defects in PKIs

- It is difficult to authenticate subjects that cannot be issued certificates face-to-face. This reduces trust in the attestation provided by a CA that allows remote registration
- Authenticating the public key for a root CA is onerous. Not authenticating the key can allow an attacker to replace it, causing an application to accept forged certificates
- There are scaling issues in distributing certificate revocation lists quickly and securely
- The users private key must typically be cached in memory to ensure usability, which opens the key up to attack
- Quality properties for passwords and other controls defending a user's private keys cannot be enforced

D. Davis. Compliance Defects in Public-Key Cryptography. USENIX Security 1996.

Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted Email

Shirley Gaw, Edward W. Felten, Patricia Fernandez-Kelly

CHI 2006

Interviews with 9 employees of “ActivistCorp”

Practices for encrypting email

Secrecy, Flagging, and Paranoia...

Social stigma, not just usability, limits adoption

Used for financial and direct action planning

Woodward- didn't trust plugins. Manually encrypted

Abe- financial data

Secrecy, Flagging, and Paranoia...

"You felt a bit like a secret agent"

"Fear of attackers was less important than ease of use. It if was easier to encrypt everything. [Abe] would"

(Referencing PGP rep) "It was too over-the-top and definitely too complicated. It was like a movie"

Secrecy, Flagging, and Paranoia...

“Jenny emphasizes `normal people.' *Normal* people wouldn't encrypt normal messages.”

“I work with somebody... and he sends *every-single-message* of his is encrypted”

“Equating encryption with confidentiality might disappear if encryption was invisible to the user”

Current Issues

- DigiNotar, Comodo
- Stuxnet, Duqu
- Windows 8
- SecurID

Comodo- March 2011

Comodo- a certificate authority

"The login.live.com domain used for logging in to Windows Live accounts was one of the domains compromised by the rogue Comodo certificates."

"Google, Skype, Yahoo Targeted by Rogue Comodo SSL Certificates."

http://www.pcworld.com/businesscenter/article/223147/google_skype_yahoo_targeted_by_rogue_comodo_ssl_certificates.html

DigiNotar- August 2011

DigiNotar- Dutch CA

531 certificates compromised

Covertly revoked certificates

“Trust in all certificates issued by DigiNotar was revoked by most major browser and operating system manufacturers”

http://www.cio.co.uk/opinion/ferguson/2011/10/18/diginotar-where-did-our-trust-go/?intcmp=HPF2

Browsers' CAs

https://spreadsheets.google.com/pub?key=ttwCVzDV

“Sadly, the state of digital certificates is such a mess that it probably matters little either way. Legitimate companies with legitimate sites often have improper or expired certificates. Users are already jaded and conditioned to simply accept erroneous certificates and bypass browser and operating system warning messages.”

http://www.pcworld.com/businesscenter/article/239682/apple_silent_on_diginotar_certificates_hack.html

Stuxnet

June 2010 Malware that attacks Siemens PLC

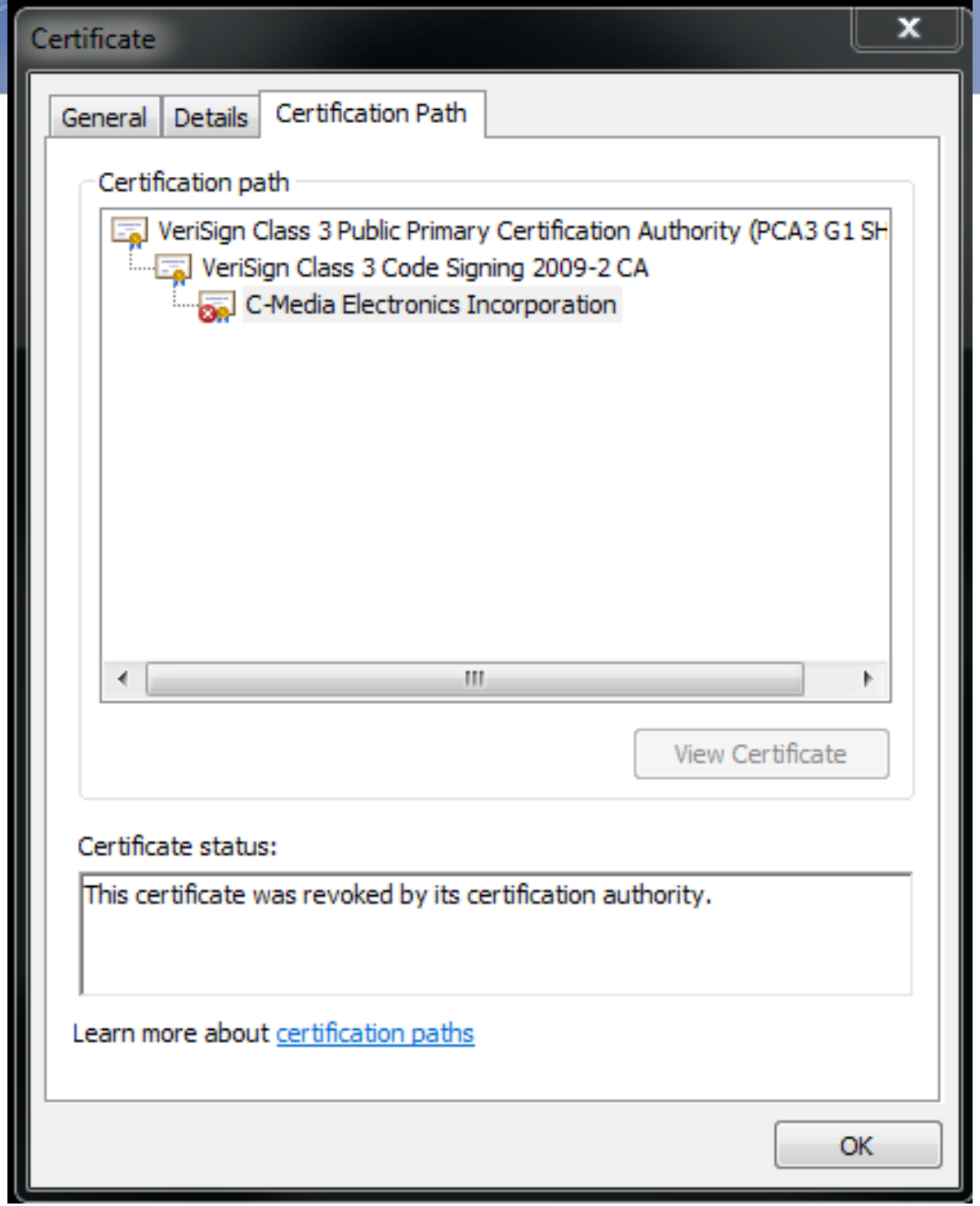
Suspected target: Iranian Nuclear Program

Rumored creator: USA/Israel

“The malware is digitally signed with legitimate certificates stolen from two certificate authorities.”

http://www.wired.com/threatlevel/2010/09/stuxnet/


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
•Ensures software came from software publisher
•Protects software from alteration after publication
* Refer to the certification authority's statement for details.
Issued to: C-Media Electronics Incorporation
Issued by: VeriSign Class 3 Code Signing 2009-2 CA
Valid from 8/2/2009 to 8/2/2012
Install Certificate...
Issuer Statement
OK


Certificate
General
Details
Certification Path
Certification path
VeriSign Class 3 Public Primary Certification Authority (PCA3 G1 SH
VeriSign Class 3 Code Signing 2009-2 CA
C-Media Electronics Incorporation
View Certificate
Certificate status:
This certificate was revoked by its certification authority.
Learn more about certification paths
OK

Duqu

Keylogger

"McAfee Labs advises Certificate Authorities to carefully verify if their systems might have been affected by this threat or any variations."

http://blogs.mcafee.com/mcafee-labs/the-day-of-the-golden-jackal-%E2%80%93-further-tales-of-the-stuxnet-files

After analyzing the captured code, researchers believe that Duqu is specifically designed to target certificate authorities.

http://www.pcworld.com/businesscenter/article/242114/duqu_new_malware_is_stuxnet_20.html

Duqu

"The trojan-spy is able to record keystrokes and collect various details of system information. The collected information is saved to an encrypted file, which the attackers can retrieve via the CC server."

http://www.f-secure.com/v-descs/backdoor_w32_duqu.shtml

"Duqu has a driver signed with a stolen certificate belonging to a Taiwanese company called C-Media Electronics Incorporation. The driver still claims to be from JMicron, though."

http://www.f-secure.com/weblog/archives/00002255.html

Windows 8

Windows 8- PKI-based Secure Boot

Is this a good idea?

http://www.zdnet.co.uk/news/desktop-os/2011/09/23/microsoft-explains-windows-8-boot-to-quell-linux-fears-40094017/

SecurID Breach

March 2011-

"While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack." http://www.rsa.com/node.aspx?id=3872

SecurID Breach

June 2011- “The company’s admission of the RSA tokens’ vulnerability on Monday was a shock to many customers because it came so long after a hacking attack on RSA in March and one on Lockheed Martin last month. The concern of customers and consultants over the way RSA, a unit of the tech giant EMC, communicated also raises the possibility that many customers will seek alternative solutions to safeguard remote access to their computer networks.”

http://www.nytimes.com/2011/06/08/business/08security.html?pagewanted=all

SecurID Breach

Rumor: cryptographic seeds compromised

Rumor: Lockheed Martin break-in

RSA claim: nation state

http://arstechnica.com/business/news/2011/10/rsa-details-march-cyber-attack-blames-nation-state-for-securid-breach.ars

PKIs in the Enterprise

- How do enterprises use PKIs?
- What usability issues do enterprises suffer from?
- How do enterprises address PKI usability issues?

How do enterprises use PKIs?

- Workstation Logon – Via Smart Cards
- Email Encryption/Signing – Via Soft Certs
- Assigning Identities to Applications – Via Soft Certs
- Identifying Websites – Via HTTPS
- Establishing Secure Channels – Via HTTPS/SSL/FTPS
- Code Signing – Via Hardware Managed or Soft Certs

How do enterprises use PKIs?

- There are many ways to structure CAs, but the following make particular sense for an enterprise:
  - Maintain a root CA for internal use, but utilize intermediate CAs to actually issue certificates
  - Maintain a root CA for major product silos (e.g., employee badges, secure messaging, etc.), and utilize intermediate CAs to issue certificates when appropriate

Usability Issues for Users

- Users don't understand issuance process
  - Badges can't be used until users have visited a website with their smart card in their reader to initialize the badge
  - Enrolling in and configuring encrypted email for Outlook can take 5+ steps, each more confusing than the last
- Users don't understand CA scoping issues
  - You can't necessarily send an encrypted email outside of the company and have it work
  - Browsers installed from the wild won't necessarily be configured by default to trust the internal CA

Usability Issues for Devs/SAs

- Developers and System Administrators may manage so many certificates they can't manually keep track of them all
  - When certificates expire, systems and applications become inaccessible
- Acquiring new soft certificates can be a trying process (6+ steps with 4+ required switches per step, each more confusing than the last)
- Root certificates expire and have to be replaced everywhere they are located
- Error messages for programming libraries that make use of certificates and cryptography tend to be beyond terrible (I am being nice...)
- Cryptographic APIs are very complicated

Usability Issues for Devs/SAs

- Using an assumed nominal rate of $170, this error message cost one of my former employers ~$31,000:

SUN.SECURITY.VALIDATOR.VALIDATOREXCEPTION: PKIX PATH BUILDING FAILED: SUN.SECURITY.PROVIDER.CERTPATH.SUNCERTPATHBUILDEREXCEPTION: UNABLE TO FIND VALID CERTIFICATE PATH TO REQUESTED TARGET

Usability Issues for Devs/SAs

- Java's cryptography libraries are some of the easiest to use in the industry
- The Java Cryptographic Architecture takes 66 printed pages to specify
- Java's JavaDocs for Cryptographic Classes generally assume a strong vocabulary in:
  - Block Cipher Internals
  - Cipher Modes
  - Public Key Encryption Internals
  - Certificate Specifications
  - Key Specifications
  - On and on and on...
- Encrypting a byte buffer with AES requires 9 lines of code, using 7 classes documented over 44 printed pages of JavaDoc

http://download.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html

Dealing with Usability Issues

- Automation:
  - Make enrollment processes as point and click as possible
  - Provide online tools to issue certificates for applications, secure channels, etc.
    - Utilize these tools to automatically warn certificate managers when their certificates are about to expire
    - Utilize these tools to convert certificates or encode keys to whatever format is needed in a particular context
  - Provide a central authority for acquiring new root certificates out of band (perhaps the same tool as above)
  - Utilize configuration management to push out certificate updates
- Provide error messages humans can comprehend

Discussion

Convergence

Black Hat 8/2010

“Marlinspike's Convergence is radically different from the situation today where the web of trust is based on a SSL server certificate signed by a certificate authority and recognized by the user's browser, based on recognition of the certificate authority that's programmed in by the browser vendors. “

“The idea is that the Convergence notaries, based on the user's own selection of which ones they prefer, electronically inform the user if the SSL certificate is considered valid.”

http://www.networkworld.com/news/2011/101211-ssl-moxie-marlinspike-251882.html?hpg1=bn

SSL Security

“Dr Taher Elgamal, the creator of the widely used security protocol [SSL], said that little has been done to bump up SSL security since the attacks, which means 'it could happen again'.

He said that the problem was less an issue of technology and more to do with people, particularly in terms of how many SSL certificate authorities are out there. 'There's way too many of them,' he said. 'Nobody asked the question of what to do if a certificate authority turns out to be bad.'”

http://www.theinquirer.net/inquirer/news/2117943/ssl-creator-warns-attacks

Sir Tim Berners-Lee

"I'm amazed I still can't do public key-encrypted email with people in the local community," Berners-Lee said at an RSA Conference press event on Thursday. "The things that public key cryptography promised us are not actually there in practice... Certain email services, such as Gmail, already allow users to send and receive encrypted email within the service. Berners-Lee envisages an overarching public key infrastructure system that would allow encrypted emails between different services and pieces of software. "

http://www.zdnet.co.uk/news/security-management/2011/10/17/berners-lee-we-need-pgp-for-the-people-40094198/