PKI + Channel Security

Friday, February 9, 2018 12:58 PM

Public Key Distribution

- Needs to be securely distributed
- Public Announcement, Publishing Directory, PKI
- Standardised techniques: a trusted entity needed

Public Key Infrastructure

Certificate Authority (CA)

- Root CA -> Hierarchy of Trust in Certificate Chain
- A few trusted CAs in computer
- Expensive to get signed (verifies that you own domain name)

Certificate

- A public key certified by an authority

Limitations

- CVE bug: browsers in C do not display substrings after the "name"
    - Null character "\0" not displayed by browser written in C, which takes it as an end-line
- CA abuse
- Lenovo SuperFish
    - CA allowed MIM attack to show ads even on encrypted pages
- Social Engineering (typosquatting - URL typos)

Strong Authentication

- Challenge-response
- Freshness: m is random (cryptographic nonce, r)
- Unilateral/ mutual? Have to verify both ways
- Mallory = malicious man-in-the-middle, steps in after being "authenticated"
- Eve = sniffing, cannot modify
- Authenticated key exchange
- Long term key = public/ private key (unilateral use)
    - Short term (session) key
- Slide 49 sequence number, check for integrity
    - Confidentiality = k (session key)
    - Integrity = t (MAC)
- Even if LT key is known, session key is unknown (cannot decrypted the STORED encyrpted messages)
- Secret key is encrypted with session key
    - Can get encrypted alice's report (confidentiality + integrity)

Readings

CA abuse
https://www.computerworld.com/article/2501291/internet/trustwave-admits-issuing-man-in-the-middle-digital-certificate--mozilla-debates-punishment.html
CVE browser bug
http://www.ruby-lang.org/en/news/2013/06/27/hostname-check-bypassing-vulnerability-in-openssl-client-cve-2013-4073/

Station to station protocol
https://en.wikipedia.org/wiki/Station-to-Station_protocol
SSL/ TLS handshake = authenticated key exchange; similar to DH
https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm