Certificate Authorities (CA) and SSL Certificates

Presented by: Laith Mohammad Hamasha
Supervised by: Dr. Monther Aldwairi
Student ID: 8308
INCS 745: Intrusion Detection and Hacker Exploits
NYIT - Jordan

Agenda

- What is a CA?
- Issues regarding CAs
- Attack Types
- Certificate verification errors
- Countermeasures
- Questions and discussion
- References

What is a CA?

- Certification authority serve as a regulator facilitating identifying entities.
- Certificates are digitally signed documents by the CA that attest that the entity is who it claims it is.
- A certificate can be verified by decrypting it using the public key of the CA.
- Major CAs include: VeriSign, eTRUST, Comodo, DigiNotar.

Issues regarding CAs

- The scheme used proved to be insecure. E.g. Google Iran MITM attack September 2011 and nine top-tier websites certificates forged issued by Comodo.
- The enormous number of CAs (around 650) which is too much.
- Usage of SSL contains many operational flaws exploited by attackers: User legitimacy judgment, invalid certificate overriding mechanism

Attack Types

- Eavesdropping
  - Shared media
  - Unencrypted packets
- Man-In-The-Middle (MITM)
  - Interception of packets
  - ARP Spoofing (IP to MAC)
  - DNS Spoofing (Domain to IP)
- ARP poisoning
  - Altering ARP cache table in router
- Certificate Spoofing and forgery
  - Impersonate the client and later can legitimately access the server or impersonate it also.

Certificate verification errors

- These errors trigger the predictable behavior in SSL (overriding)
- Causes:
  - Self-signed certificate (private CA)
  - Expired certificate
  - Domain name mismatch
- Can be exploited through MITM & Certificate spoofing

Countermeasures

- User' Legitimacy Judgment
  - Responsibility of user to check clues and depend mainly on user security awareness.
  - Prefix (HTTPS), Padlock, Spelling and content of website
  - Currently assumed in the implementation of SSL and browsers nowadays.
- SSLock
  - No interaction from the user
  - Implemented in the more security-cautious firms
  - Generic (FTPS, SMTP), light-weight (<50 LOC), Privacy-preserving (No cookies), idiot-proof
  - Banks and secure entities must opt-in first

Countermeasures (continued)

- Context Sensitive Certificate Verification (CSCV)
  - Cannot be overridden interface
  - Security awarness
  - User provide certificate manually (USB, Floppy)
  - Contact information of system admin
  - Proven to be very successful in experiment
- Specific Password Warnings (SPW)
  - Triggered by unencrypted passwords only
  - Security awareness
  - Can be overridden (HTTP web mail)

Countermeasures (continued)

- Veiled Certificates (VC)
  - New to the literature
  - Multi-dimensional (Many credentials)
  - Provide privacy (Preserve personal information)
  - Adhere to legal reporting requirement
  - Can be aggregated
  - Introduce the concept of VC token (owner ID + User certificate specific public key)
  - Local key management is essential (Many VC tokens)

Questions & Discussion

References

- [1] Iranian Man-in-the-Middle Attack Against Google Demonstrates Dangerous Weakness of Certificate Authorities, Commentary by Seth Schoen and Eva Galperin, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2011/08/iranian-man-middle-attack-against-google
- [2] The flawed certificate authority system, Angela Moscaritolo, From the October 2011 Issue of SCMagazine, http://www.scmagazineus.com/the-flawed-certificate-authority-system/article/212015/
- [3] SSLock: Sustaining the Trust on Entities Brought by SSL, Adonis P.H. Fung, K.W. Cheung,
- [4] Hardening Web Browsers Against ManintheMiddle and Eavesdropping Attacks, Haidong Xia and Jos´e Carlos Brustoloni.
- [5] Analysis and Countermeasures of Security Vulnerability on Portal Sites, Kyoungju Kwak, Kwangwoo Lee, Dongho Won, Seungjoo Kim,
- [6] Privacy-Preserving Multi-Dimensional Credentialing Using Veiled Certificates, Chin-Tser Huang, John H. Gerdes, Jr.
- [7] When Private Keys are Public: Results from the 2008 Debian OpenSSL Vulnerability, Scott Yilek, Eric Rescorla, Hovav Shacham, Brandon Enright, Stefan Savage