Protecting Administrative Credentials

Mingchao Ma
OSCT
GridPP Security Officer
STFC - RAL

Introduction

- What?
- Why?
- How?

What?

- **Password**
  - Root
- **SSH and SSH Keys**
  - SSH server configuration and SSH Private keys
- **X.509 Certificate**
  - Private key
- **Proxy Certificate/Delegated Proxy Certificate**
  - Private key
- **… …**

Why?

- **High valuable target**
- **High risk**
- **Larger damage**
- **Hard to detect**
- **Things can go wrong in many different ways**
  - Growing complexity of system
  - OS security holes
  - Application bugs
  - Mis-configuration
  - Virus/Malwares/Spywares
  - Network traffic sniffing
  - Shoulder surfing
  - Phishing
  - Social engineering
  - … …

Why (cont.)?

- **A stolen administrative credential**
  - Unauthorized access to the WHOLE comprised system(s)
  - Unauthorized access to the Grid
  - Remote control of a site or a part of a site
  - Unauthorized access confidential information
  - … …
  - The attacker can do almost everything that a system administrator can

How?

- Patch (OS & Application)
- Anti-virus software
- Firewall (site or host)
- Install only needed software and applications
- Disable unused network services
- Install software only from trusted source
- Verify signature/hash value of software before installed
- Be aware of malicious software such as Root kit, Troyes Horse, Keystroke-loggers …
- … …

Password?

- **Password**
  - Be aware of your local security policy
  - at least 8 characters (minimal requirement)
  - Including numbers, letters and at least one special character
  - As random as possible (no vocabularies/common names)
  - Consider some tools – e.g. *mkpassed*

    mkpasswd -l 15 -d 3 -C 5

    creates a 15-character password that contains at least 3 digits and 5 uppercase characters
  - Password cracking tool to verify security & strength of password
    - Disable any account with a week password
  - Do NOT write it down
  - Do NOT use the same password for different accounts

Password (cont.)

- **Password encryption on Linux/Unix**
  - MD5 hash
    - One way hash function
      - *Not reversible*
      - *Fast & Easy*
    - Encrypted password:
      - *HASH=MD5 (“password”, “salt”)*

  OR

  - Use *crypt* routine to encrypt user’s passwords
    - It is a modified one-way DES encryption
    - It encrypt a password with a “salt”
    - In RedHat/Scientific Linux: with *Python* interpreter
      - *Import crypt; print crypt.crypt (“your password”, “salt”)*
- **Both are subject to dictionary attack/brute force attack**
- **It is absolutely necessary to protect encrypted password!**

Password (cont.)?

- **Shadow password enabled:**
  - cd /etc
  - chown root:root passwd shadow group
  - chmod 644 passwd group
  - chmod 400 shadow
- **Shadow file only root readable**
- **Prevent from “offline” password cracking (e.g. dictionary attack, brute force attack)**
  - Try different combination until have a match
- **Pre-computation/Lookup table: speed up attacking dramatically**
  - Many online pre-computation password databases;
  - Some database achieves nearly 1,000,000,000 alphanumeric MD5 hashes;
  - Rainbow tables, RainbowCrack (http://www.antsight.com/zsl/rainbowcrack/) can generate and use rainbow tables to attack LM Hash, MD5 and SHA1

Password (cont.)

- **Disable rlogin/rsh/rcp**
- **Disable Telnet**
- **Disable FTP**
- **All use clear text password protocol**
  - Network sniffing: Ethreal/Wireshark, tcpdump, Ettercap
  - Even in a switched LAN network (Ettercap) http://ettercap.sourceforge.net/
    - Arp poisoning
    - Man-In-The-Middle attack
- **It is also possible to sniff/wiretap WAN (DNS spoofing)**
- **Send out CLEAR password over network is a bad practice**
- **Instead, use more secure SSH/SCP**
  - An end-to-end secure, cryptographic channel

SSH and SSH keys

- **Be aware of problems with the default setup**
  - SSH version 1 protocol is not secure
- **Be aware of online SSH dictionary/brute force attack**
  - Automatically attempt to login
  - Check /var/log/security for failure login (RedHat/SL)
- **Hardening SSH server:**
  - SSH version 2 protocol only;
  - Disable root login – “PermitRootLogin no”;
  - Disable password login whenever applicable – “PasswordAuthentication no”;
  - SSH key authentication if possible;
- **Consider to deploy one bastion host for SSH connection; all other SSH servers are behind a firewall**

SSH and SSH keys (cont.)

- **Be aware of SSH man-in-the-middle (MITM) attack**
  - Make sure to have server SSH public key from trusted source;
  - Verify the fingerprint of the server SSH key if possible
  - Be alert of “new server key warning message”
  - Password-based login is subject to MITM;
- **SSH keys**
  - Multiple ssh keys?
  - Where are the private keys?
  - How many copies of each private key?
  - Encrypted the private keys with GOOD password/passphrase
  - Set file permission of the private key to 0400 (Linux/Unix)
- **An encrypted private key is still subject to dictionary attack and brute force attack**

X. 509 Certificate

- **X.509 Certificate**
  - Your digital ID in the Grid world
  - At least at two places:
    - Web browser (s) – mutual authentication
    - UI – access grid (e.g. submit a job)
  - Used by SSL/TLS and Grid middleware (etc. Globus, gLite)
- **Set a GOOD/STRONG password/passphrase on private key**
  - Web browser
    - IE: make sure to set a password when you import the certificate and private key by choose *Set Security Level* to high
    - Firefox (WXP): Tools=>Options=>Security: use a master password
    - Firefox (Linux):Edit=>Preferences=>Privacy=>Passwords: Set Master Password
  - UI
    - ~/.globus/userkey.pem =>private key
    - Set the key only readable by owner: chmod 0400 userkey.pem
    - Protect private key with a password:
      - *grid-change-pass-phrase userkey.pem*
- **Encrypted any backup of private key and know where they are**

X.509 Certificate (cont.)

- **Man-in-the-middle (MITM) attack**
  - Server authentication is subject to MITM
    - HTTPS protocol with server authentication ONLY
    - A third-party pretends to be the server you connect to and relay information between your web browser and your intended server
    - The web browser will alert you that server certificate can not be verified, but most user will click yes and proceed anyway!
  - Import ONLY trusted root CA certificates into your browser from **TRUSTED** source
  - Do NOT trust unverified server certificate
  - Be alert of any warning message about server certificate
- **A encrypted private key/certificate is still subject to dictionary attack and brute force attack**

Proxy Certificate

- **Proxy certificate is issued by your standard X.509 certificate:**
  - grid-proxy-init, or
  - voms-proxy-init
- **Delegated proxy certificate is issued by your proxy certificate**
  - myproxy-init
  - myproxy-get-delegation
  - X.509 Certificate=>Proxy Certificate =>Delegated Proxy Certificate

Proxy Certificate (cont.)

- **Technically, they are the same as the standard X.509 Certificate, but:**
  - Very short valid time, typically 12 hours
  - In subject field, it has something like "/CN=my name**/CN=proxy**"
  - It can not be revoked (no CRL)
- **Proxy certificate also comes with a PRIVATE key, but,**
- **No password on proxy or delegated proxy certificate**
  - Password will break Grid middleware


```
-----BEGIN CERTIFICATE-----
MIICfDCCAWSgAwIBAgICLTQwDQYJKoZIhvcNAQEEBQAwUzELMAkGA1UEBhMCVUsx
... ... ... ...
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIBOAIBAAJBAKmq+yV=jl+bX/sLseu6ub+GjVo9MJHBIa1sDyoSwgU1qjGN46Iu
hq07fVtooc7gI4UV5QVtPEpRT6R/yC6FgdECAwEAAQJAUvvztlT94bkm6qy/quI7
```

Proxy Certificate (cont.)

- **Proxy/Delegated certificates are as important as the standard X.509 certificate**
  - A stolen proxy certificate can be used by others to submit a job
  - You can NOT prove it is not you who abuse the Grid with YOUR certificate
- **Everyone should take care of his/her certificates**
  - Do not create proxy certificate if you do not use it;
  - Do not create delegate certificate if you do not use it;
  - Try not to allow anonymous delegation if possible;
  - Destroy proxy/delegated certificate if necessary
    - Grid-proxy-destroy/voms-proxy-destroy/myproxy-destroy
- **System administrators and managers need to take extra-cautions**
  - They have **more** privilege than regular users
  - Might cause larger damage than a regular user

More … …

- **Other OSCT training talks cover different topics**
  - Introduction: Grid and security
  - Grid systems installation and configuration
  - Centralised logging
  - Testing and monitoring Grid systems
  - Incident response (policies and procedures)

Conclusion

- No network, system, device, software and or hardware can be made fully secure
- Security is a chain, it is only as secure as the weakest link
- Multiple layers – defence depth