Security Characteristics of Cryptographic Mobility Solutions

Dr. Sarbari Gupta

Electrosoft Services

Tel: (703)757-9096

sarbari@electrosoft-inc.com

http://www.electrosoft-inc.com

Agenda

- What is a Cryptographic Mobility (CM) Solution?
- Functional Architecture
- Phases of Operation
- Characteristics that impact security
- Potential Security Issues
- Usage and Applicability
- Product Sampler
- Concluding Remarks

What is a CM Solution?

Roaming users need access to their cryptographic credentials from a variety of systems/workstations

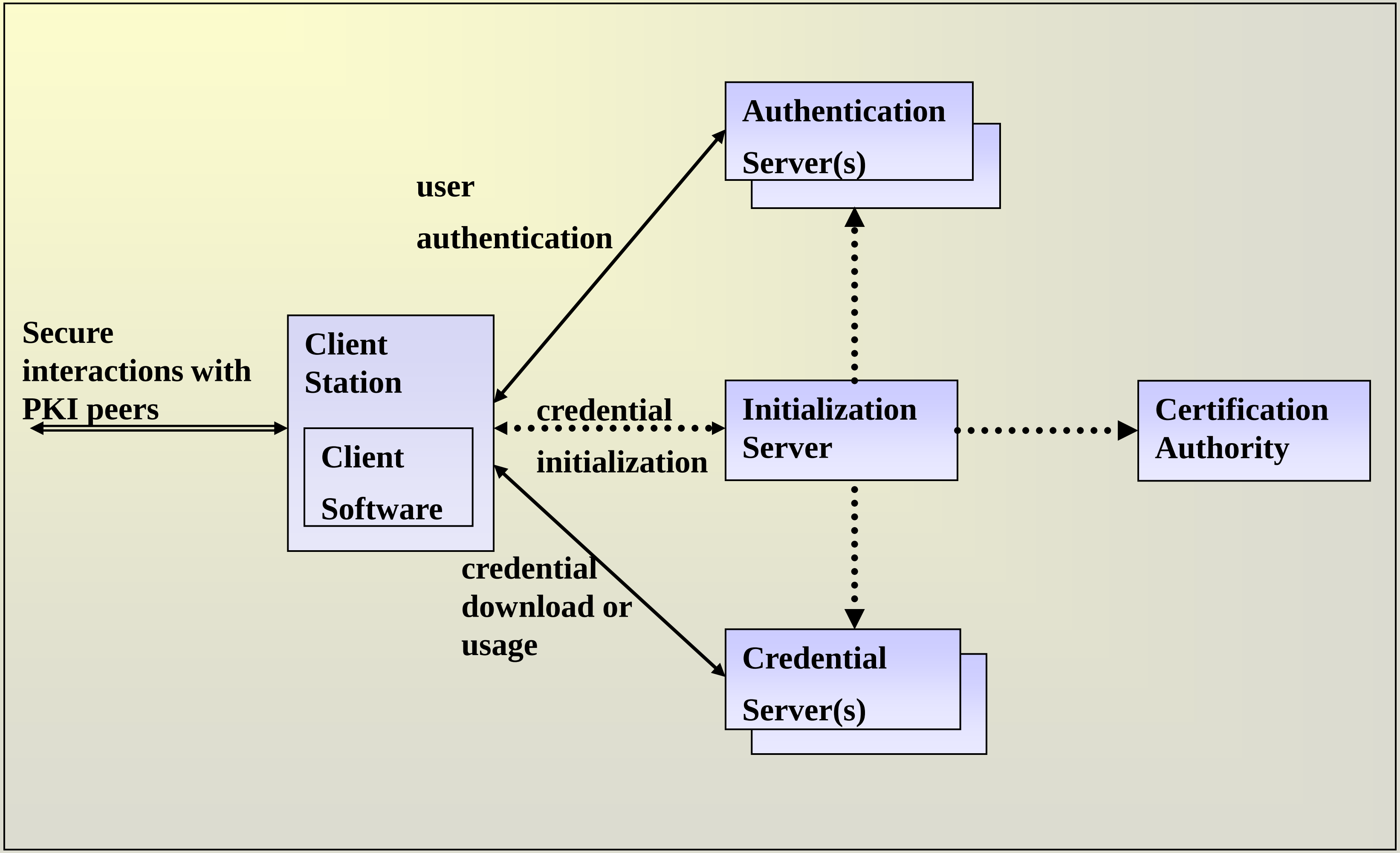
Available mechanisms for Roaming Access:

- *Portable Tokens*
  - Software Tokens
  - Hardware Tokens
- *Credential Server Solutions (**Cryptographic Mobility Solutions**)*

Characteristics of CM Solutions:

- *No hardware or software tokens required*
- *Vendor-specific Client Software may be required*
- *User Credentials (partial or whole) stored on Online Server*
- *User authentication to Online Server to obtain access to credentials*
- *Ability to use crypto credentials from any connected workstation*

Functional Architecture



Authentication Server(s)

user authentication

Secure interactions with PKI peers

Client Station

Client Software

credential initialization

Initialization Server

Certification Authority

credential download or usage

Credential Server(s)

Phases of Operation

- *Credential Initialization*
  - Generation and/or Packaging of credentials for roaming usage
- *Authentication*
  - Roaming user authentication to Remote Servers
- *Credential Download*
  - Part of whole credential downloaded to user local system
- *Credential Usage*
  - Application of credential to secure online transactions
- *Credential Release*
  - Removal of local copy of credential to prevent reuse

Characteristics that Impact Security

- Client Station is shared by multiple users
  - *Low assurance of hardware and OS software*
  - *More vulnerable to hacking if remnants of cryptographic session remain*
- Client software downloaded to Client Station
  - *Vulnerable to spoofing*
  - *Difficult to establish trust*
- Authentication Server available online
  - *Exposed to online attacks on Authentication Database*
  - *Vulnerable to Denial-of-Service attacks*
- Credential Server available online
  - *Vulnerable to online attacks - high value system holding a large number of credentials*
  - *Vulnerable to Denial-of-Service attacks*
- Protocol interactions over untrusted networks
  - *Online protocols may be exposed to attacks*

Potential Security Concerns (I)

- Key Initialization Issues
  - *Key pair generation location*
  - *Mechanism of credential transport to Server*
- Key Storage Issues
  - *Accessibility of private keys to Server*
  - *Cryptographic protection of credentials stored on Server*
  - *Impact of compromise of Credential Server*
- Authentication Issues
  - *Authentication spoofing*
  - *Eavesdropping*
  - *Denial-of-service*
- Credential Download Issues
  - *Capture of credential during download*

Potential Security Concerns (II)

- Credential Usage Issues
  - *Credential usage location – client station or server?*
- Credential Release Issues
  - *Disabling credential reuse*
- Client Station Trust Issues
  - *Establishing trust in Client Software*
  - *Client misuse of User authentication data*
  - *Client misuse of User Credential information*

Usage and Applicability

- Requirements that drive CM Usage
  - *Highly mobile users*
  - *Use of multiple workstations not under organizational control*
  - *Software tokens not practical or secure enough*
  - *Simple user interface needed – account names and passwords*
  - *Strong (PKI) authentication needed by application*

- Contraindications for CM Usage
  - *Strong non-repudiation is a must*
  - *Recovery of encryption keys is essential*
  - *Zero tolerance for denial-of-service*

Product Sampler

- Entrust Roaming PKI
- VeriSign Roaming
- Arcot ID Mobility
- SingleSignOn.Net Appliance
- Microsoft Roaming Profiles
- RSA Security Keon Web Passport
- Baltimore UniCert Option for Roaming
- Hush Communications HushMail

(See paper for brief descriptions)

Concluding Remarks

- No major weaknesses found in the cryptography or the protocols used

- Common Security Concerns Remain:
  - *Basis of trust on Client Station shaky at best*
  - *Susceptibility to Denial-of-Service attacks*
  - *Authentication Servers susceptible to attack/compromise*
  - *Credential Servers represent high value targets*
  - *Non-repudiation is weaker if Servers have direct/indirect access to private keys*

- However, CM Solutions represent:
  - *Much needed functionality*
  - *A category of PKI implementations that are easy to use and deploy*
  - *Improved security compared to software token solutions*
  - *Sufficient security for most online secure transactions*

Thank You!

Questions??