

Certification Authority Security Requirements and Technologies

Dr. Stephen Kent
Chief Scientist- Information Security

QuickTime™ and a
Photo - JPEG decompressor
are needed to see this picture

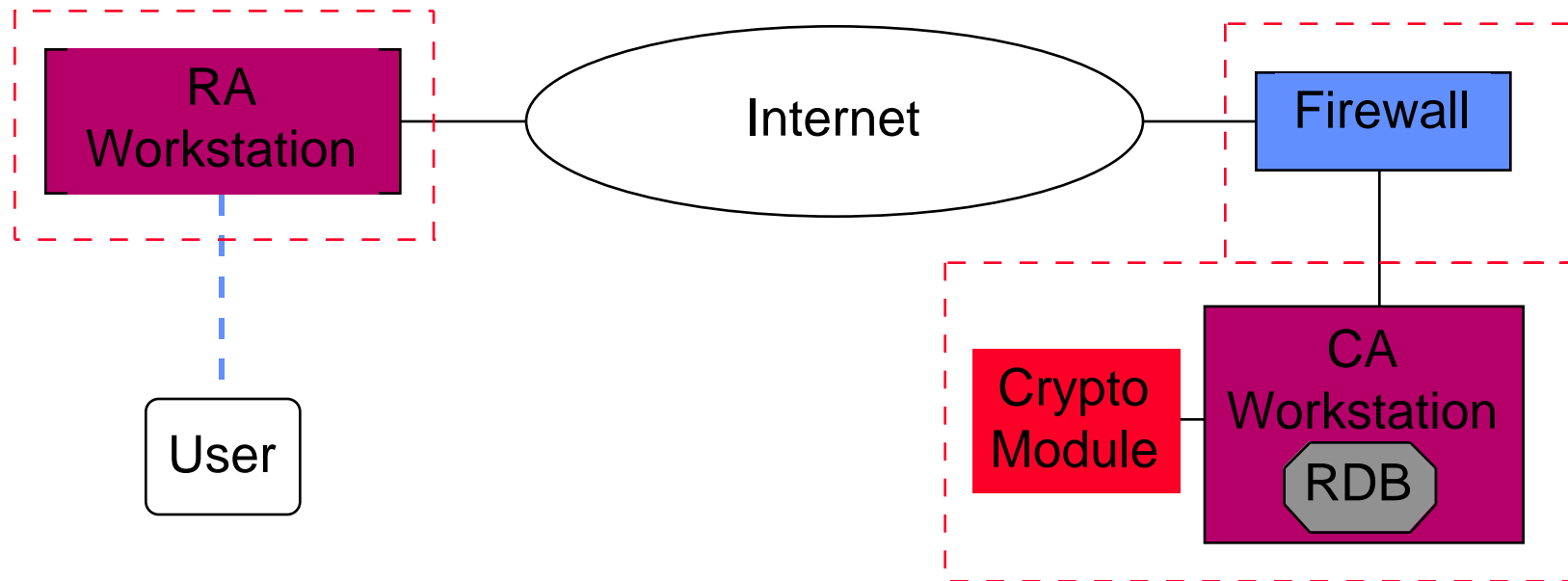
The CA Security Requirement

**Establish and maintain an accurate
binding between attributes and a
public key in a certificate**

Derived Security Requirements

- Protection of CA private keys
 - ◆ confidentiality in the face of a wide range of attacks
 - ◆ support for polyinstantiation
 - ◆ support for key recovery
- Validation of certificate issuance requests
 - ◆ user/organization identification
 - ◆ verification of certificate syntax against rules for a specific CA or RA (basic certificate fields and extensions)
- Validated certification revocation requests*
- Timely CRL distribution*

CA System Components



Adversaries & Capabilities

■ Hackers

- ◆ motivated by recognition (not averse to detection)
- ◆ software-based attacks
- ◆ external access

■ Compromised employees

- ◆ motivated by retribution, greed, ... (averse to detection)
- ◆ internal access
- ◆ may employ software, hardware, physical attacks

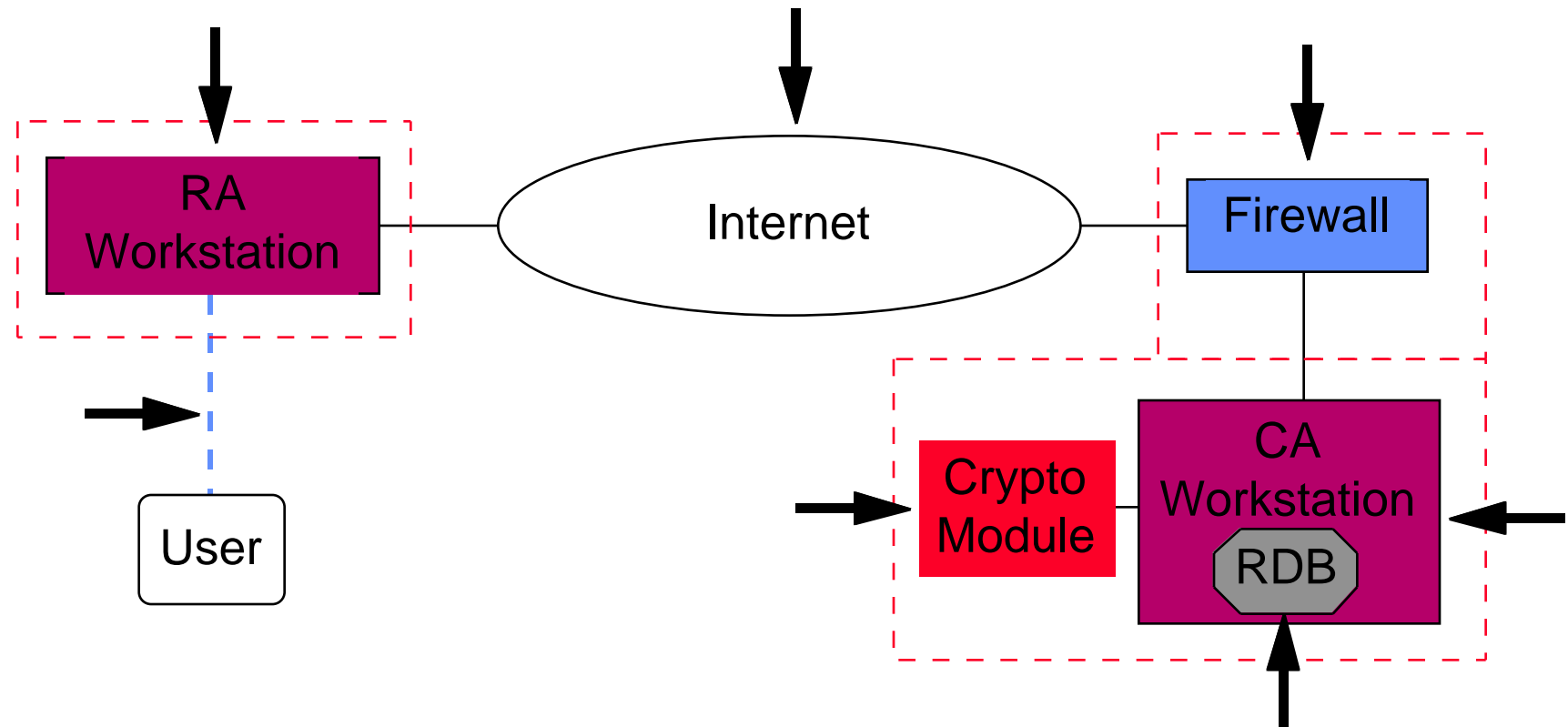
■ Criminals

- ◆ motivated by greed (averse to detection)
- ◆ external or internal access (bribe employees, break in, ...)
- ◆ may employ software, hardware, physical attacks

Attacks Against CAs

- Passive and active wiretapping
 - ◆ user/RA path
 - ◆ RA/CA path
- Personnel compromise
- CA workstation attacks
 - ◆ OS penetration
 - ◆ CA software or database manipulation
- Crypto module attacks
 - ◆ simple physical tampering
 - ◆ module theft/swapping
 - ◆ close-in attacks (TEMPEST, temperature, timing analysis, differential fault analysis, ...)

Attack Points



Protecting CAs

- Physical security
- Personnel security
- Procedural security
- OS and application security
- Network security
- Crypto module security

Countermeasures

- Locks, sensors, guards, guns, dogs, ...
- Personnel background checks
- Audit trails
- Multi-party authorization
- Certificate syntax filtering against rules
- Operating system security
- Software configuration control
- Signed/encrypted RA-CA communication
- Firewalls
- Crypto module security

Crypto Implementation Options

- Software crypto
- Generic crypto hardware (e.g., PC and smart cards)
- Specialized crypto hardware

Software Crypto

■ Advantages

- ◆ low cost
- ◆ easy upgrade for new algorithms

■ Limitations

- ◆ vulnerable to CA key compromise via software or physical attacks on workstation
- ◆ poor key generation (no hardware RNG)
- ◆ poor audit trail security
- ◆ low entropy PINs, PIN exposure to workstation
- ◆ vulnerable to personnel (RA/CA) security compromise
- ◆ vulnerable to close-in monitoring attacks?

Generic Crypto

■ Advantages

- ◆ modest cost
- ◆ keys protected from compromise of workstation software or physical attacks against the workstation
- ◆ hardware RNG for key generation
- ◆ multi-party authorization possible with split-key systems

■ Limitations

- ◆ algorithm upgrade may be more difficult
- ◆ poor support for CA key polyinstantiation & recovery
- ◆ low entropy PINs, PIN exposure to workstation
- ◆ vulnerable to close-in monitoring attacks
- ◆ no certificate syntax validation
- ◆ limited or no audit
- ◆ vulnerable to theft & device swapping attacks

Specialized Crypto

■ Advantages

- ◆ keys protected from compromise of workstation software or physical attacks against the workstation
- ◆ hardware RNG for key generation
- ◆ multi-party authorization via high entropy keys
- ◆ secure polyinstantiation/recovery for CA keys
- ◆ protection against close-in monitoring/tampering
- ◆ some certificate syntax validation
- ◆ potential for secure audit

■ Limitations

- ◆ higher device cost
- ◆ algorithm upgrade may be more difficult (as above)
- ◆ limited certificate rule checking (in current devices)

CA Security Recommendations

- Establish high quality personnel, physical, and procedural security standards for CA operations
- Use a crypto module specialized for support of CA functions, with suitable provisions for CA key recovery, polyinstantiation, & multi-party authorization
- Employ a high assurance workstation for the CA
- Protect RA-CA communications with cryptography

Summary

- The fundamental security requirement for CAs is simple to state, but hard to achieve in the face of a wide range of attack scenarios
- Software crypto for CAs is highly vulnerable
- Hardware crypto can limit the range of attacks against CA keys, but generic crypto devices still leave CAs vulnerable to many attacks
- Specialized hardware crypto, designed for CA support, offers the greatest potential for high assurance CA operation, but it's not a complete solution
- Identity attribute validation is still “outside the system”