

On the usefulness of proof-of-possession

2nd Annual PKI Research Workshop
April 28-29, 2003

N. Asokan <n.asokan@nokia.com>

Valtteri Niemi <valtteri.niemi@nokia.com>

Pekka Laitinen <pekka.laitinen@nokia.com>

Nokia Research Center

Presentation outline

- Why am I here, what is our motivation?
I know you're asking
- What is enrollment and proof of possession (PoP) during enrollment?
I know you know
- Attacks prevented (and not prevented) by PoP
- Does PoP do any harm?
- Conclusions
- Questions and Answers

Motivation

- 3GPP work item “support for subscriber certificate”:
 - bootstrapping a PKI infrastructure using cellular authentication
 - more info: <http://www.3gpp.org/>
- Every PKI standard asserts that PoP is essential
 - none of them describe the threats addressed by PoP
- Discussed in standards meetings and mailing lists
- No easily available or commonly known papers or articles
- Examine potential rationales for PoP
- Questions:
 - Should designer of new PKI require PoP during enrollment?
 - Does designer of new public key based application or protocol benefit from having PoP done during enrollment?

Definitions

- enrollment:
process of submitting a certificate request to CA
- proof of possession (PoP) during enrollment:
during enrollment the end entity that submits the public key proves that it knows the corresponding private key
- two primary ways to use the private key:
 - claim (authentication or decryption), user benefits from something
 - commitment (non-repudiation), user commits to something

Attack 1 on Enrollment (1/2)

Replacing public key in enrollment request sent by victim

- Mallory replaces Victor's public key by her own public key
 - possible if security in Victor's device or enrollment process is weak
- Mallory has private key and corresponding certificate belonging Victor

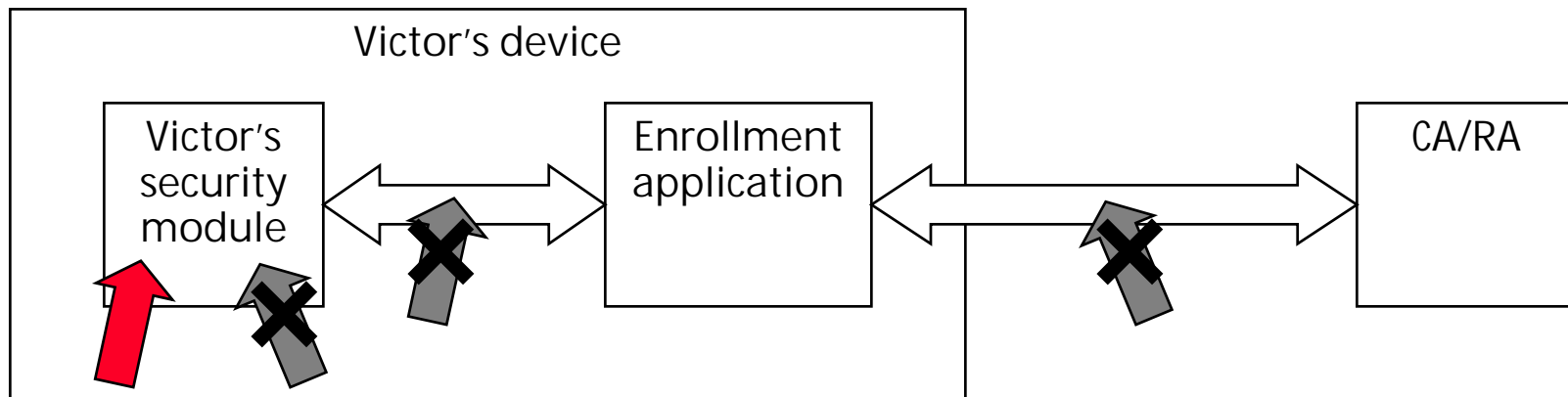
Implications:

- Mallory can mislead Carol to encrypt confidential data intended for Victor
- Mallory can make commitments and leave Victor liable for them

Attack 1 on Enrollment (2/2)

Does PoP help?

- If Victor's device is secure → attack is not possible → PoP is not needed
- PoP useful preventing this attack *iff*:
 - attacker can insert a public key into victim's device, but is unable to
 - insert a private key
 - intercept communication between security mod and application
 - attack enrollment process itself



- PoP has minor role
 - access control on victim's device needs to be faulty in specific and unrealistic manner
- Protection provided by PoP is minimal

Attack 2 (1/2)

Using victim's public key in own enrollment request

- Mallory uses Victor's public key in her own certificate request
 - possible if PoP is not used
- Mallory has certificate for Victor's public key, but not Victor's private key

Implications:

- Attacks on claim type uses if application protocol is designed badly, i.e., Mallory can substitute Victor's certificate with her own, e.g.,
 - Mallory can claim ownership of messages that were signed by Victor
 - Mallory can mislead Carol into revealing private data intended for Victor
- Attacks on commitment type uses:
 - no effective protocol attack
 - claim attacks are also possible if:
 - application does not check the key usage of the certificate
 - certificate is used for multiple purposes

Attack 2 (2/2)

Does PoP help?

- PoP is not needed if applications and protocols are designed “properly”
 - Prevention techniques (= well known rules of thumb of secure design):
 - signer’s identity/certificate is included in signed text
 - software application handles certificate usage restrictions correctly
 - certificate has only one type of use
 - PoP can prevent these attacks, but
 - if prevention techniques are adopted → PoP is not essential
 - certificate does not indicate if PoP was done → developer must not assume it was done → should use prevention techniques anyway
 - In a perfect world PoP is not needed since applications and application protocols would have been designed “properly”
 - However, this is not a perfect world
- PoP is useful during enrollment, although it is not essential

Does PoP do any harm?

- Considered factors:
 - bandwidth
 - PoP increases message size
 - if channel is bandwidth constrained → size of messages matter
 - latency
 - to prevent replay attacks PoP protocol must ensure freshness
 - use timestamps → requires synchronized clocks
 - use challenge-response msgs → procedure contains extra msgs
 - novel applications
 - mandating PoP can preclude new use cases for certificates, e.g., Mallory obtains gift certificate for Victor's public key
- Judgment:
 - enrollment is not done often and it does not have real-time requirements → bandwidth and latency not critical
 - there are other ways of designing novel applications, e.g., SAML assertions instead of gift certificates

→ PoP does no harm

Conclusion

- PoP is useful safety precaution
 - PoP *not essential* for preventing any the identified attacks
- Should designer of new PKI require PoP during enrollment?
 - They should, especially if their PKI will be used with existing applications
- Does designer of new public key based application or protocol benefit from having PoP done during enrollment?
 - They benefit from PoP, but they must not assume that PoP was done during enrollment → they should follow the well known rules of secure protocol design
- *If you have questions about 3GPP's "support for subscriber certificate" WI, feel free to contact us.*