To: INCITS Technical Committee T10
From: Gideon Avida, Decru
Date: August 25, 2006
Document: T10/06-389r0
Subject: Using Public-Key Cryptography for Key Wrapping

1 Revision History

Revision 0 (06-r0): Posted to the T10 web site on August 25, 2006.

- Proposal overview for discussion in the Nashua meeting.

2 Introduction

Public-Key Cryptography enables sending secretes securely without requiring a prior shared secret.
There are several advantages for this approach:

1. There is no need to generate and maintain a secure channel and its related security association.
2. Keys can be generated/stored and wrapped away from the application client. This reduces key exposure as there may be multiple client servers (usually running a general purpose OS) and only a few key management servers.
3. There is flexibility in complexity vs. security.

The proposed algorithms are PKCS #1 v2.1 RSAES-OAEP and ECIES.

3 References

1. The IEEE P1363 Standard Specifications For Public-Key Cryptography — Amendment 1: Additional Techniques
   http://grouper.ieee.org/groups/1363/tradPK/index.html
2. ANSI 9.63-2001
   http://webstore.ansi.org/ansidocstore/subscriptions/product.asp?sku=ANSI+X9.63-2001
3. PKCS #1 v2.1: RSA Cryptography Standard
   ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf

4 Overview

4.1 Complexity vs. security

Public-Key cryptography allows for a flexible implementation than can support multiple levels of security:

4.1.1 Confidentiality

Each device server has a secret private key and a public key. The public key is used for wrapping key material sent to the device server. The private key is used by the device server to unwrap the keys sent to it. The entity wrapping the encryption key is assured that only the device server that owns the private portion of this public key can unwrap the encryption key.
At this level, the device server cannot authenticate the entity wrapping the encryption key or detect replay attacks. However, this mode is simple to implement and is an improvement over the current scheme (keys in plain-text). The weaknesses of this approach can be mitigated by relaying on the lower protocols (e.g. ipsec for iSCSI of FC-SP for Fibre-Channel) or on physical security of the connection.
Note that integrity checking is included.

4.1.2 Confidentiality and Sender Authentication

In addition to its private/public key pair, each device server stores the public keys of the entities from which it can receive encryption keys. While these public keys are not secret, the device server shall store them in a way that will prevent and attacker from modifying a public key or even injecting his own (such operations will grant the attacker the ability to send wrapped keys to the device server. In addition, there must be controls on how public keys are introduced. This can be done out of band in a vendor specific way.
The device server's public key is used for the encryption operation of the wrapping, and the wrapping entity's private key is used for the signing operation of the wrapping. By verifying the signature, the device server is assured of the sender's identity.
At this level it is trivial to add protection from replay attacks by requesting a random nonce from the device server prior to wrapping and including this value in the signing operation.
Note that the same message format can be used in both modes. In the "confidentiality assurance only" mode, the nonce and signature fields may not be populated by wrapper, and are not check by the device server.

4.2 No protocol negotiation

Similar to the approach taken in 06-103r2, there will be no protocol negotiation. The client application will discover the wrapping format supported by requesting the Supported Key Formats page (see ssc3r03 8.5.2.5). The wrapping entity is required to support all formats.

4.3 Management of Public Keys

While the public keys are not secret, installing a public key in an entity authorizes that entity to receive from (in the case of device server) or send to (in the case of the key wrapping entity) the owner of that public key. Therefore this process should be controlled.