Next Generation Physical Access Control Systems – A Smart Card Alliance Educational Institute Workshop

Cryptography

Nathan Cummings
Director Integration/Applications – HID Global

8th Annual Smart Cards in Government Conference
Washington Dc Convention Center – October 27 – 30, 2009
Security vs. Cryptography

Security is the set of services:

- Data Integrity
  - Ensuring that data has not been modified
- Authentication
  - Verifying attributes of a specific entity
- Confidentiality
  - Concealing data so that it cannot be read
- Non-Repudiation
  - Cannot refute the validity of an action

Cryptography is the set of mathematical algorithms used to implement security
Data Integrity

The assurance that the data has arrived intact, with no tampering or corruption of the bits.

Data Integrity is achieved electronically through the use of cryptographic checksums (one-way hashes) over the data.

- This “hashing” function produces a small value that uniquely represents the data, like a fingerprint. If a single bit is altered the hash value will change.
One Way Hash Functions

Creates a small derived string that uniquely characterizes the data (the message digest/hash)

It is infeasible to find a message that hashes to a particular value (i.e. one cannot recalculate the original message from the hash result)

It is infeasible to find two different messages that hash to the same value

By recalculating a new message digest and comparing it with the received digest the message integrity can be verified

The hash function is not secret

The addition of a key to the hash algorithm creates a Hashed Message Authentication Code (HMAC)
Hashing Algorithm at Work

ALICE

Sample Plaintext Message Originated by Alice

m-dig

MESSAGE DIGEST

SHA-1

HASHING ALGORITHM
Hash/HMAC

Commonly used algorithms

- Secure Hash Standard (SHS)
  - FIPS 180

- Keyed-Hash Message Authentication Code
  - FIPS 198
The binding of the sender’s (or issuer’s) credentials to the data. This process can be likened to your personal signature - it is unique to you and can be recognized (verified) later by all parties involved.
Mutual-Authentication

A means by which two “entities” can determine if they contain a shared secret, without having to transmit the secret on a non-secure channel

Typically done with a “Challenge” and “Response” mechanism that institutes random numbers to prevent against man-in-the-middle or replay attacks
Mutual-Authentication

Commonly used algorithms

- ISO 9798

ISO/IEC 9798 consists of the following parts, under the general title *Information technology . Security techniques . Entity authentication*:
  - Part 1: General
  - Part 2: Mechanisms using symmetric encipherment algorithms
  - Part 3: Mechanisms using digital signature techniques
  - Part 4: Mechanisms using a cryptographic check function
  - Part 5: Mechanisms using zero-knowledge techniques
  - Part 6: Mechanisms using manual data transfer
Confidentiality

Encryption (scrambling) of the data to prevent unauthorized disclosure.
Encryption

- The process of disguising a message in such a way as to hide its substance
- Requires an encryption **ALGORITHM** and an encryption **KEY**
Symmetric Key Systems

Approach
- Same key used to encrypt and decrypt information

Attributes
- Fast
- Key Distribution is Required (physical, electronic)
- Scalability Requires Management Systems
- Compromise is Critical. Loss can be Broad.

Benefits
- Confidentiality, Integrity thru Encryption
Symmetric Encryption/Decryption

Secret Key used to encrypt data
Sender and receiver must have same key
Key distribution and compromise recovery are difficult

Bob

Alice
Symmetric Encryption

Commonly Used Algorithms

- Data Encryption Standard (DES)
  - FIPS 46
    - Covers various key usage (DES, 3DES, etc.)
    - Covers various modes (EBC, CBC, etc.)

- Advanced Encryption Standard (AES)
  - FIPS 197
Non-Repudiation

The fact that a third party can verify your authentication (e.g., your signature) on a transaction means that you cannot deny participation in the transaction.
Public Keys

A public and corresponding private key are mathematically related hence referred to as a public/private key pair.

The private key is kept secret, the public key is published i.e Directory, File, Newspaper, etc.

By knowing the public key, it is mathematically infeasible to calculate the corresponding private key.

Public Key algorithms are less efficient in terms of encryption than symmetric algorithms.

Public Key systems are generally considered to be more flexible and secure than Symmetric Key systems.
Key pair is use in public key cryptography

- Key generation provides the basis for trust
- Public key bound in certificate and shared
- Private key protected and never shared
Using Public Keys to Solve a Problem

The question is how to get the Secret Key to Alice
Let’s take the secret key and treat it as data
Using Secret and Public Key Technologies

This fundamentally demonstrates how public key algorithms can deliver confidentiality.

We do not use public key technology against the message itself because of basic inefficiencies (slow).
Bob uses his own private key to sign
Alice uses Bob’s public key to verify
Result is Pass or Fail
Anybody can use Bob’s public key and recover message
Hash results are compared
Message integrity, authentication and sender non-
repudiation are achieved.
Putting it All Together - Signing & Encrypting

Bob

Alice

Key Generation

Secret

Public Key Algorithm

DES

M-Dig

Bob’s Token

Bob’s Private Key

Hashing Algorithm

Alice’s Certificate

Alice’s Public Key

Alice’s Private Key

Alice’s Token

Secret Key

Public Key Algorithm

DES

M-Dig

Bob’s Certificate

This is plain text. It can be a document, image, or any other data file

12A7BC544109FD00A6293FECC7293B9BCAA12020384AC6F4D93B8

This is plain text. It can be a document, image, or any other data file

DES

M-Dig

M-Dig

M-Dig

Property of the Smart Card Alliance © 2009
Asymmetric Encryption

Commonly used algorithms

- Digital Signature Standard (DSS)
  - FIPS 186
  - Includes; RSA, DSA, and ECC
PKI

Public Key Infrastructure
Public Key Infrastructure

- Public Key Certificates
- Certification Authorities
- PKI Services
- X.509
- Certificate Management
- Public Key Management
- Token Management
- Registration Management
- Information Dist. & Mgmt

Property of the Smart Card Alliance © 2009
Definition:

- “Data structure associated with a Certification Authority(s) which hosts public key certificates for use by PKI population.”

Functions:

- Support publication of certificates from CA(s)
- Support publication of certificate revocation lists from CA(s)
- Service subscriber/relying party requests for cert and CRL info
- High availability – application transactional services
- Trusted operations, high integrity
Digital Certificates

Certification Authority acts as a trusted third party:
  ➢ **Binds user information to public key.**
  ➢ **Issues an unforgeable certificate.**

Digital certificates can be published in a public directory/repository.

Digital certificates can be used to provide the required security services: integrity, confidentiality, authentication, authorization, and non-repudiation.

ITU Recommendation X.509 is the accepted standard for digital certificates in Government and industry.
X.509 Certificates (cont.)

X.509 Version 3 certificates:

- Defined extensions that can be added to the base certificate:
  - public key information
  - policy information
  - additional subject attribute information
  - constraint information
  - CRL information
- Widely accepted in Gov’t and industry.
- Commercial and Gov’t implementations.
Digital Certificates

Definition

Information about a public key owner that is “bound” together via a digital signature with owner (subject) information by a trusted authority called a “Certification Authority”

Values:
- Authentication of parties in e-Business transactions
Certificate Issuance

1. Generate Subject Public/Private Key Pair
2. Collect Subject Information
3. Authenticate Subject and Key Binding Info
4. Generate Certificate
5. Digitally Sign Certificate

Validate Certificate Request

Produce Certificate

6. Distribute Certificate To Subject
7. Publish Certificate To Repository
8. Create CA Database Entry & Audit Record

Distribute and Publish Certificate
Certificate Revocation List

A listing of public key certificates which are no longer valid

Typically placed in public directories so that applications may check the revocation status of a certificate before trusting

Examples

- Compromise
- Affiliation change
- Superseded

Reference

- RFC 3280
Identity Federation

- Boeing
- Lockheed Martin
- Northrop Grumman
- ARINC
- CertiPath Common Policy Root CA
- GPO SSP
- DoJ
- DoE
- SITA
- Exostar
- US PTO
- VDoT
- DEA
- Dept. of State
- State of Illinois
- Wells Fargo
- Higher Ed Bridge CA
- Federal Bridge CA
- SAFE Bridge CA
- SAFE Root CA
- Fed Common Policy Root CA
- VeriSign SSP
- US Treasury SSP
- DoD Interoperability Root
- DoD
- DoT
- HUD
- SSA
- NASA
- DHS
- EOP
- HHS
- VA
- Entrust MSO
- GSA

Trust Anchor
Key Management

There are good and bad secrets. Example: an ATM PIN of 1234 is bad

All secrets should be securely stored and backed-up in case of disaster

There must be a secure way to share secrets with authorized users

A secret should not last forever. Its usage should expire at some point

All references to the secret are completely erased
Security is based on:

- The strength of open cryptography (algorithms)
  - Algorithms are published which allows for academic peer review to ensure strength and dependability

- The strength of the secrets (keys)
  - Because the algorithms are public, the strength of the algorithm depends on the generation, length, quality, and secrecy of the key

- Multiple layers
  - Just as in physical security, cryptographic strength depends on a layered approach rather than a single point of failure, the solution is only as strong as the weakest component

A balance must be achieved that provides for risk appropriate security along with the conveniences users have come to expect with RF enable physical access control.
Speaker Contact Information

Nathan Cummings  
HID Global  
ncummings@hidglobal.com · Phone: (949) 732-2068  
www.hidglobal.com