Authentication and Identity Management

Donna F Dodson
Division Chief, Computer Security Division
National Institute of Standards and Technology

Authentication & Access Control

- We *authenticate* people in order to treat them *differently*
- If we cannot authenticate people, they will all be treated the same way
  - i.e., we will "trust no one," "trust everyone," or "trust arbitrarily"
- An access decision is only as good as its authentication decision

NIST

NIST SP 800-63

- Companion to US Federal Government Policy, OMB M-04-04 Guidance for e-authentication
- Technical authentication framework for remote e-authentication
  - Establishes technical requirements for 4 levels of M-04-04 for
    - Authentication protocols and mechanisms
    - Identity proofing

NIST

Authentication: The players

- Token: is a secret, or holds a secret used in a remote authentication protocol
- Authentication Service Provider (ASP): A trusted authority who issues identity or attribute tokens
- Subscriber: A party whose identity or name (and possibly other attributes) is known to some authority

Authentication: The players

- Registration Authority (RA): registers a person with some ASP
  - Has a trusted relationship with ASP
- Claimant: claims identity or a name of a subscriber
- Relying party: relies on claimant's identity or attributes
- Verifier: verifies claimant's identity
  - May be associated with either the ASP or relying party

Authentication: Local vs Remote

- Local authentication
  - Verifier control and supervision is comparatively easy
    - Verifier controls entire authentication system
    - Claimant may be supervised (to various degrees) or unsupervised
    - Verifier knows just where claimant physically is

NIST

Authentication: Local vs Remote

- Verifier control and supervision is harder
  - Claimant generally uses his own system, controls his own software
  - Claimant is generally unsupervised
  - Network access: verifier knows only that claimant has network access
  - Hardware tokens improve supervision and extend verifier control
  - NIST SP 800-63 applies to remote authentication

Authentication Factors

- Something you know
  - Typically some kind of password
- Something you have
  - For local authentication typically an ID card
  - For remote authentication typically a cryptographic key
    - “hard” & “soft” tokens
- Something you are
  - A biometric
    - Problematic without supervision
    - Capture can deter fraud even if not checked in authentication process
- The more factors, the stronger the authentication

Four Levels of SP 800-63

- Level 1
  - Single factor: typically a password
  - Can’t send password in the clear
    - May still be vulnerable to eavesdroppers
  - Moderate password guessing difficulty requirements

Four Levels of SP 800-63

- Level 2
  - Single factor: typically a password
    - Must block eavesdroppers (e.g password tunneled through TLS)
    - Fairly strong password guessing difficulty requirements
    - May fall to main-in-the middle attacks, social engineering & phishing attacks

NIST

Four Levels of SP 800-63

- Level 3
  - 2 factors, typically a key encrypted under a password (soft token)
  - Must resist eavesdroppers
  - May be vulnerable to man-in-the-middle attacks (e.g. phishing & decoy websites), but must not divulge authentication key

NIST

Four Levels of Sp800-63

- Level 4
  - 2 factors: “hard token” unlocked by a password or biometric
  - Must resist eavesdroppers
  - Must resist man-in-the-middle attacks
  - Critical data transfer must be authenticated with a key bound to authentication

NIST

Attacks

- Eavesdropper – listens in
- Decoy sites, access points and terminals,
  - Impersonate a real site and either facilitate a man-in-the-middle attack or capture password tokens
  - Facilitated by browser limitations and ability of websites to control the user's screen appearance
  - Phishing brings victim to the decoy

NIST

Attacks (cont)

- Man-in-the-middle - communications go through the attacker
  - Can yield attacker some tokens, allow attacker to eavesdrop, or can allow session hijacking
- Social Engineering – attacker persuades user to do something insecure
  - Probably no remote authentication method is entirely immune to this
- Malware & intrusion – bad software introduced on claimant' computer
  - Copied token: some tokens are easy to copy and the user will never know

NIST

PIV Presidential Policy Driver

Homeland Security Presidential Directive 12

HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors (8/27/04)

http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

General Objectives

- Common, secure, reliable identification for all government employees and contractors.
- Identification to be used for access to federal resources (physical – fed. buildings, logical to federal IT resources).
- Interoperable identification across Departments and agencies.

NIST

FIPS 201 Specifications - Personal Identity Verification (PIV) for Government Employees and Contractors

- A smart card-based solution (PIV card)
  - Common on-card credential for logical and physical access
  - Card Edge Interface: Credential access through a small subset of ISO/IEC 7816 (contact) and ISO/IEC 14443 (contactless) card commands/APDUs
  - Application Interface: access through common set of Client API
  - PIV Middleware as the Client API-to-APDU translator.

FIPS 201 REQUIREMENTS
PIV Electronically Stored Data

- Mandatory:
- PIN (proves the identity of the cardholder to the card) (Something you know)
- Cardholder Unique Identifier (CHUID) - for contactless physical access
- PIV Authentication Credential (asymmetric key pair and corresponding PKI certificate) for logical access
- **Two biometric fingerprints (something you are)**

Optional:

- Additional cryptographic keys

Digital Images vs. Templates

- FIPS 201/Special Publication 800-76 specify format for storing fingerprint information on Personal Identity Verification (PIV) Cards.
- All major users strongly preferred minutiae or pattern template formats for storage of fingerprint information on PIV Cards.
  - Storage requirement advantage
  - Processing advantage
  - Perceived advantage associated with privacy protection of information subset over full digital image

Template Concept

Template Interoperability Issues

- Initial implementations of the national standard for fingerprint templates (ANSI INCITS 378) were immature. Different products meeting the standard were initially not 100% compatible (they were imperfectly interoperable).
- If both the extractor (uses the extraction algorithm) and the matcher (uses the matching algorithm) were produced by the same vendor, highly satisfactory matching accuracy resulted. That is, there was a high probability that a person who has just provided the live sample was indeed the person whose biometric template is found on the card.
- If extractor and matcher were from two different vendors, testing to a common standard was required to provide a level of confidence in matching results.

MINEX Dependency

- NIST sought to generate ‘empirical matching accuracy data’ through the MINEX project.
- The MINEX project generated data on matching accuracies for various combinations of extraction and matching algorithms using a large set of samples.
- When MINEX was completed, assurance on template-based matching accuracy became available.

Governing Principles

- Maximizing privacy by minimizing amount of personal information stored on and communicated by credential (within Federal programs).
- Maximizing efficiency and safety by fostering interoperability among organizations in use of Federal credentials.
- Providing technical foundation for more global interoperability consistent with the policy environment.
- Participating in standards bodies is a key element in achieving the technical potential for global interoperability.

NIST

Thank you!

http://csrc.nist.gov