Security Technology Group – Cryptographic Standards, Authentication and Infrastructures

Bill Burr
william.burr@nist.gov
Dec. 16, 2003
Security Technology Group

• Cryptographic Standards Team
  – Elaine Barker leader
  – 5 FTE (one addition last FY)

• Authentication and Infrastructure Team
  – Tim Polk leader
  – 6.5 FTE (.5 addition last FY)

• Biometrics Standards
  – Fernando Podio leader
  – 1 FTE at the moment
NIST Cryptographic Standards

• First Federal Information Processing Standard (FIPS) in Cryptography in 1977
  – FIPS 46, The Data Encryption Standard (DES)

• Mandatory for Federal use of cryptography to protect unclassified, sensitive data
  – FIPS 140-2

• Standardize a set of strong cryptographic tools
  – Can’t test and approve every good algorithm/method
    • Too expensive to study each one
  – Too many would confound interoperability
Cryptographic Standards

Security Requirements for Cryptographic Modules
FIPS 140-2

Symmetric Key
* DES (FIPS 46-3)
* 3DES (FIPS 46-3, X9.52)
* AES (FIPS 197)
* Modes of operation
  - SP 800-38A
  - SP 800-38B, C (OMAC, CCM)
* HMAC (FIPS 198)

Public Key
* Dig. Sig. Std. (FIPS 186-2, FIPS 186-3)
  - DSA (X9.30) – bigger keys
  - RSA (X9.31) – PKCS1 pad
  - ECDSA (X9.62)
* Key Establishment Schemes
  - Diffie-Hellman - X9.42
  - RSA - X9.44
  - Elliptic Curves -X9.63
* Key Management Guideline
  - General Guidance
  - Key Management Organization
  - Application-Specific Guidance

Secure Hash
* SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS 180-2)
Toolkit Advantages

- FIPS 140-2 product testing
  - CMVP Laboratory validation testing
  - Known answer testing for many of the tools
- Confidence in the security of the tools
  - Carefully evaluated and monitored
- Interoperability and acceptance
  - Tools very widely implemented and used
  - Seen as the safe choice
- Use by Federal agencies often required
Sources of Standards & Recommendations

- Public submissions with NIST selection
  - DES, AES, new crypto modes
- Standards Bodies
  - ANSI-X9
    - TDES, ECDSA, ECDH and ECMQV, FFDH and FFMQV, RSA variants
  - IETF
    - HMAC
    - perhaps eventually PKIX, TLS, S/MIME, IKE….
- NSA
  - DSA, SHAxxx, proposed AES Key Wrap
Crypto Standards Participation

• X9F1 has been main venue for NIST participation
  – Financial services industry
  – X9F1 standards used in FIPS
    • X9.52 (TDES), X9.62 (ECDSA), X9.31 (rDSA)
      – NIST did much of the work for several of these

• Other important cryptographic standards venues
  – ANSI INCITS T4 (ISO/IEC JCT1 SC27 )
  – IEEE P1363 & IEEE 802.11 tgi (CCM)
  – IETF (HMAC for example comes from RFC 2104)

• NIST can’t afford to play everywhere
  – Which is the best place to participate?
    • Broadest & best participation & exposure
Modes of Operation
Recommendation

• SP 800-38A 2001 ED, Recommendation for Block Cipher Modes of Operation, 2001 (encryption modes)
  – update of FIPS 81
  – 5 modes
    • ECB – Electronic Code Book
    • CBC – Cipher Block Chaining
    • CFB – Cipher Feedback
    • OFB – Output Feedback
    • **Counter**

• Generalized for any block cipher
New Modes on Our Plate

• **Block Cipher Message Authentication Code**
  – Originally proposed RMAC
    • Blocks extension attacks
    • Blocks “birthday” attacks
      – At expense of more tag bits
      – Mainly a problem for TDES
  • Controversy
    – TDES Related key attack
  – Answer: OMAC
    • One key variation on XCBC MAC

• **Counter with CBC-MAC mode**
  – To be mandatory to implement in 802.11

• **AES Key Wrap**
  – TDES too?
802.11 WEP Debacle & CCM

• 802.11 wireless Ethernet is huge success, but
  – Wired Equivalency Protocol (WEP) was a disaster
    • Vulnerable to almost every attack known to cryptologists
      – Keystream is more or less guaranteed to repeat
      – “Side-channel” attack exploits non-cryptographic checksum
      – Weak RC4 encryption – can recover the key
      – Encryption but no authentication
    • Can do only so much to patch this
• This is fundamental infrastructure
  – it’s worth getting it right
• 802.11i and 802.1x are addressing the problem
  – NIST plans to adopt the CCM mode
Data Transfer

CCM Mode Overview

- Use CBC-MAC to compute a MIC (Message Integrity Code) on the plaintext header, length of the plaintext header, and the payload
- Use CTR mode to encrypt the payload
  - Counter values 1, 2, 3, …
- Use CTR mode to encrypt the MIC
  - Counter value 0
Key Management

• Most current drafts posted for comment
  – Key Establishment Schemes: NIST SP 800-56 Basic public key methods
    • RSA is still the missing piece
  – Guidance: NIST SP 800-57
    • General guidance
    • Best practice for key management organization
    • Application specific guidance (not posted yet)

• Proposed 80-bit crypto end of use date: 2010
  – Stop using 1024-bit RSA/DSA or 160-bit EC by 2010
Random Number Generation

• ANSI X9.82: Consists of three parts
  – Part 1: Overview and Basic Principles
  – Part 2: Non-deterministic Random Bit Generators
  – Part 3: Deterministic Random Bit Generators
• Workshop being planned for Summer 2004
• Draft to be made available prior to workshop
### Comparable Strengths

<table>
<thead>
<tr>
<th></th>
<th>Sym. Key</th>
<th>Hash</th>
<th>MAC</th>
<th>RSA/DSA</th>
<th>EC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size in bits</td>
<td>56</td>
<td>160</td>
<td>64</td>
<td>512</td>
<td>160</td>
</tr>
<tr>
<td>Sym. Key</td>
<td>80</td>
<td>224</td>
<td>160</td>
<td>1k</td>
<td>224</td>
</tr>
<tr>
<td>Sym. Key</td>
<td>112</td>
<td>256</td>
<td></td>
<td>2k</td>
<td>256</td>
</tr>
<tr>
<td>Sym. Key</td>
<td>128</td>
<td>384</td>
<td></td>
<td>3k</td>
<td>384</td>
</tr>
<tr>
<td>Sym. Key</td>
<td>192</td>
<td></td>
<td></td>
<td>7.5k</td>
<td>512</td>
</tr>
<tr>
<td>Sym. Key</td>
<td>256</td>
<td></td>
<td></td>
<td>15k</td>
<td>512</td>
</tr>
</tbody>
</table>

**Sym. Key:** Symmetric key encryption algorithms  
**MAC:** Message Authentication code  
**RSA/DSA:** Factoring or discrete log based public key algorithms using FF arithmetic  
**EC:** Elliptic Curve discrete log based public key algorithms  
**White background:** currently approved FIPS  
**Yellow background:** under development  
**Black background:** not secure now
## NIST Crypto Standards Status

<table>
<thead>
<tr>
<th>Sym. Key</th>
<th>56</th>
<th>80</th>
<th>112</th>
<th>128</th>
<th>192</th>
<th>256</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>46-3</td>
<td>185</td>
<td>46-3</td>
<td>FIPS 197 (AES)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modes</td>
<td>81</td>
<td></td>
<td></td>
<td>SP 800-38A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash</td>
<td>180-1</td>
<td>180-2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td>FIPS 198 (HMAC)/SP 800-38B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA, DSA, EC-DSA</td>
<td>186-2</td>
<td>186-3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DH/RSA</td>
<td></td>
<td></td>
<td></td>
<td>Key Management FIPS:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EC-DH</td>
<td></td>
<td></td>
<td></td>
<td>Scheme and Guidance</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Colors:**
- White: FIPS approved
- Red: working draft phase
- Black: no longer secure
- Yellow: draft in progress
- Gray: initial recommendation published, more to come
Authentication & Infrastructure Team: Scope of Current Efforts

- Three overlapping technology areas:
  - Authentication Technologies
  - Cryptographic Infrastructures
  - Crypto-enabled Applications

- Four General Activities
  - Research
  - Standardization & Guidance
  - Testing (Interoperability, Conformance, & Assurance)
  - Deployment
Authentication Technologies, I

- **Research**
  - Knowledge-based Authentication
  - Strength of Passwords

- **Standardization & Guidance**
  - E-Authentication Guidance establishes framework for selection of e-Auth mechanisms
  - Updating NIST’s password guidance
  - Subject Identification Method standard (with KISA)
Authentication Technologies, II

• Testing & Tools
  – Reference Implementation of the Subject Identification Method standard

• Deployment
  – SAML-based infrastructure for e-Authentication for Federal Government applications
Cryptographic Infrastructures

• Research Activities
  – 3rd Annual PKI R&D Workshop co-sponsored with Internet II

• Standards
  – PKI Standards are mature
  – IETF and ISO PKI standards activities are winding down
Cryptographic Infrastructures, II

• NIST leading PKI Testing Efforts
  – Interoperability testing for IETF PKI standards
  – PKI client conformance tests (Path Validation)
  – Protection Profiles for CAs and PKI clients

• Key Participant in FPKI Deployment Efforts
  – FPKI Policy Authority and Certificate Policy Working Group (Federal Bridge CA)
  – Shared Service Provider Working Group (managed PKI services for Government Smart Card)
  – Path Validation & Discovery Working Group
FPKI Architecture

Legend:
SSP = Qualified Shared Service Providers
Federal Identity Credentialing Committee (FICC)

- Common physical & logical credentials for Physical & logical access
  - Federal employees & associates
- Combines Federal PKI Steering Committee, HR and Physical Security
- NIST provides technical support
  - Smart card/badge, biometrics & certificate
    - NIST lead in Certificate Policy WG
- Website: http://www.cio.gov/ficc
Crypto-Enabled Applications

• Standards & Guidance
  – High Level API for Cryptographic Services
  – S/MIME Functional Profile
  – SSL/TLS Selection and Implementation Guidance

• Testing Tools and Services
  – Reference Implementation for High Level API
  – S/MIME Interoperability and Conformance Testing

• Assisting Agencies in Application Deployment
  – FDIC, Army Corps of Engineers, Treasury/Financial Management System
E-Authentication Tech Guidance

• Will Be NIST Recommendation SP800-63
• Puts technical flesh on OMB generated e-Authentication policy guidance
  – Federal Register announcement for comment in July; revised announcement pending
  – Four levels of assurance
    • Defined in terms of the possible risks and consequences of authentication error
Assurance Levels

• OMB guidance defines 4 assurance levels
  – Level 1 is lowest, Level 4 is highest

• Assurance level needed determined by consequences of authentication error
  – Inconvenience, distress & damage to reputation
  – Financial loss
  – Harm to agency programs or reputation
  – Civil or criminal violations
  – Personal safety
Technical Guidance Constraints

• Technology neutral
  – Required (if practical) by e-Sign, Paperwork Elimination and other laws
  – Difficult: many technologies, apples and oranges comparisons

• Practical with COTS technology
  – To serve public must take advantage of existing password based solutions and relationships

• Only for remote network authentication

• Only about identity authentication
  – not about attributes or authorization or access control
E-Auth Guidance Scope

- Remote Authentication over open networks
  - Does not address in-person authentication
- Consequence is that biometrics are only useful in identity proofing, because
  - Protocols for remote network authentication are based on secret tokens (typically passwords or keys), but;
    » Biometrics make bad secrets
E-Auth Guidance

- SP 800-63
  - ID Proofing
  - Tokens, credentials and assertions
  - Protocols
    - Required properties at each level
    - Password strength model
ID Proofing

• Level 1
  – Self assertion, minimal records

• Level 2
  – More or less instant gratification possible
    • Some confirmation of address or phone number

• Level 3
  – Substantial checking, multiple sources

• Level 4
  – Level 3 plus in-person appearance
    • Record biometric, give token to a warm body
## Token Type by Level

### Allowed Token Types

<table>
<thead>
<tr>
<th>Allowed Token Types</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard crypto token</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Soft crypto token</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Zero knowledge password</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Strong password</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIN</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Required Protections by Level

<table>
<thead>
<tr>
<th>Protection Against</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eavesdropper</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Replay</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>On-line guessing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Verifier Impersonation</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Man-in-the-middle</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session Hijacking</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
## Auth. Protocol Type by Level

### Allowed Protocol Types

<table>
<thead>
<tr>
<th>Protocol Type</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private key PoP</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Symmetric key PoP</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Zero knowledge password</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunneled password</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Challenge-reply password</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Required Protocol Properties by Level

<table>
<thead>
<tr>
<th>Required properties</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared secrets not revealed to 3(^{rd}) parties</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Session Data transfer authenticated</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>
Biometric Standards - Plan for 2004

- Lead national (INCITS M1) & international (JTC 1 SC 37) Biometric standard developments
- Coordinate & participate in the development of an initial portfolio of interoperability & data interchange standards to:
  - ANSI approval status (through M1):
    - Data interchange formats: finger-image, pattern, & minutiae; iris image; face
    - Application profiles: transportation workers, border management
  - Draft international standard status (through SC 37):
    - BioAPI specification (ANSI INCITS 358-2002)
    - Common Biometric Exchange Formats Framework (CBEFF)
    - Data interchange formats (finger-image, pattern, minutiae; iris image & face)
Biometric Standards - Plan for 2004

- NISP role in the Biometric Consortium (BC) and the BioAPI Consortium
  - Co-chair the Biometric Consortium (with NSA)
    - Annual conference: Week of September 20th.
  - Member of the BioAPI Consortium Steering Committee

- Leverage of Consortia Standards developed by NIST/BC Biometric WG:
  - Complete development of the Common Biometric Exchange Framework Format (CBEFF):
    - Publish as NISTIR 6529-A & submit to INCITS
    - Publish biometric identifier protection and usage techniques as a NISTIR & submit to INCITS T4

- Identify biometric interoperability testing requirements
Questions
Links

• NIST Cryptographic Toolkit
• Federal PKI Steering Committee
  – http://www.cio.gov/fpkisc/
• E-gov project
  – http://www.whitehouse.gov/omb/egov/
• E-authentication
• Federal Identity Credentialing Committee
  – http://www.cio.gov/ficc/
Crypto FIPS

• FIPS 46-3, Data Encryption Standard -1999
  – refers to ANSI X9.52-1998 for triple DES
  – expect to kill 56-bit DES with 46-4 due in 94
• FIPS 81, DES Modes of Operation – 1980
• FIPS 113, Computer Data Authentication - 1985
  – DES MAC for financial apps.
• FIPS 117, Key Management using ANSI X9.17
  – being withdrawn
• FIPS 180-2, Secure Hash Standard – 2002
  – SHA1, SHA-256, SHA-384, SHA-512
Crypto FIPS

- FIPS 185, Escrowed Encryption Alg. – 1994
  - Skipjack
- FIPS 186-2, Digital Signature Standard
  - DSS, RSA: X9.31 & PKCS#1, ECDSA: X9.62
- FIPS 197, Advanced Encryption Standard (AES) 2001