NIST Computer Security Division Update

Donna F Dodson
Deputy Chief Cyber Security Advisor
donna.dodson@nist.gov
Agenda

- Organizational Update
- FIPS 140-3 Update
- Hash Competition Update
- Secure Web Services Guide Discussion
- New Publications
Organizational Update

• Chief Cyber Security Advisor – W. Curt Barker

• Cyber Security – Tim Grance

• Identity Management System – James Dray

• Trustworthy Network – Tom Karygianis
FIPS 140-2 and FIPS 140-3

**FIPS 140-2**
- Cryptographic Module Specification
- Cryptographic Module Ports and Interfaces
- Roles, Services, and Authentication
- Finite State Model
- Physical Security
- Operational Environment
- Cryptographic Key Management
- EMI/EMC
- Self Tests
- Design Assurance
- Mitigation of Other Attacks

**FIPS 140-3**
- Cryptographic Module Specification
- Cryptographic Module Ports and Interfaces
- Roles, Authentication and Services
- Software Security
- Operational Environment
- Physical Security – Invasive
- Physical Security – Non-Invasive
- Sensitive Security Parameter (SSP) Management
- Self Tests
- Life-Cycle Assurance
- Mitigation of Other Attacks

*Slide content is subject to change*
FIPS 140-3: Highlights

- New Security Level 5
- Non-Invasive Attacks
- Software Security Section
- Life-Cycle Assurance
- EFP at Level 5
- Detached from CC
- SSPs, CSPs and PSPs
- Key Management Clarified
- Pre-operational tests

*Slide content is subject to change*
# FIPS 140-3 Schedule

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/12/2005</td>
<td>Federal Register Notice Announcement Announcing Development of FIPS 140-3</td>
</tr>
<tr>
<td>02/28/2005</td>
<td>Comments received on FIPS 140-2</td>
</tr>
<tr>
<td>09/26/2005</td>
<td>Physical Security Workshop</td>
</tr>
<tr>
<td>03/31/2007</td>
<td>First Public Draft of FIPS 140-3 – Internal Review and Approval</td>
</tr>
<tr>
<td>07/13/2007</td>
<td>First Public Draft of FIPS 140-3 Released</td>
</tr>
<tr>
<td>10/11/2007</td>
<td>First Public Draft comment period ends</td>
</tr>
<tr>
<td>2008</td>
<td>Public Workshop</td>
</tr>
<tr>
<td>2008</td>
<td>Second Public Draft of FIPS 140-3 Released</td>
</tr>
<tr>
<td>2008</td>
<td>Second Public Draft comment period ends</td>
</tr>
<tr>
<td>2008</td>
<td>Final Release of FIPS 140-3</td>
</tr>
<tr>
<td>2008</td>
<td>Signed by the Secretary of the Department of Commerce</td>
</tr>
<tr>
<td>+6 Months</td>
<td>FIPS 140-3 Effective</td>
</tr>
<tr>
<td>+6 Months</td>
<td>Transition from FIPS 140-2 to FIPS 140-3 ends</td>
</tr>
</tbody>
</table>
SHA-3 Hash Function Competition

• Motivated by collision attacks on most of the commonly used hash algorithms, particularly MD5 & SHA-1
  – No actual collisions yet announced on SHA-1
• Held 2 hash function workshops
• Jan 2007 proposed criteria for new hash function comment period
• Many comments received
• Announcement for “SHA-3” Competition Nov. 2, 2007
Minimum Acceptability Requirements

• Publically disclosed and available worldwide without royalties or intellectual property restrictions
• Algorithm implementable in a wide range of hardware and software
• Support message digest sizes 224, 256, 384, and 512 bits
• Support maximum message length of at least $2^{64-1}$ bits
Evaluation Criteria

• Security
• Cost
  – Computational Efficiency
  – Memory Requirements
• Flexibility
• Simplicity
Submission Package

• Name of submitters
• Algorithm Specification
• Supporting Documentation
• Known Answer Tests
• Reference Implementation
• Statement by Patent Owner (if applicable)
SHA-3 Competition Timeline

- 1Q07 draft submission criteria published
- 11/2/07 Federal Register Announcement
- 8/31/08 Preliminary submissions:
  - NIST will review for completeness by 9/30/08
- 10/31/08 Final submissions due
- 2Q09 First Candidate Conference
- 2Q10 Second Candidate Conference
- 3Q10 Announce Finalist Candidates
- 4Q10 Final Tweaks of Candidates
- 1Q12 Last Candidate Conference
- 2Q12 Announce Winner
- 4Q 12 FIPS package to Secretary of Commerce
NIST Hash Function Policy

• Federal Users may use SHA-2 family hash functions (SHA-224, SHA-256, SHA-384, & SHA-512) for all hash function applications.
• For digital signatures and other apps that require collision resistance, Federal users:
  – Should convert to SHA-2 as soon as practical, but
  – Must stop using SHA-1 for these apps by end of 2010
• Federal users may use SHA-1 after 2010 for:
  – HMAC
  – Key derivation
  – Random number generation
  – To verify old signatures (signed before 2011)
Guide to Secure Web Services

• Web Services and their Relation to Security
• Dimensions for Secure Web Services
• Web Services Security Standards
• Challenges for Secure Web Services
• Recommendations
• Conclusions
Web Service Example

User → Web Portal

1. User accesses the Web Portal

2. Web Portal interacts with Loan Service

3. Loan Service returns data to Web Portal

4. Web Portal returns data to User
Web Service Example (Cont)
Web Service Example (Cont)
Advantages of Web Services

- Web services provide interoperability between various software applications running on various platforms.
  - “vendor, platform, and language neutral”
- Web services leverage open standards and protocols. Protocols and data formats are text based where possible
  - Easy for developers to understand what is going on.
- By piggybacking on HTTP, web services can work through many common firewall security measures without requiring changes to their filtering rules.
Threat Facing Web Services

- **Message Alteration:**
  The message information is altered by modifying the information.

- **Loss of Confidentiality:**
  Information in the message can be viewed by unintended participants.

- **Falsified Messages:**
  Fake messages are constructed and sent to the receiver.

- **Man in the middle:**
  A party poses as the other participant to the real sender and receiver in order to fool both participants.
Threats (Cont)

• Principal Spoofing:
  A message is sent which appears to be from another principal.

• Forged Claims: A message is sent in which the security claims are forged to gain access to otherwise unauthorized information

• Replay of Message Parts:
  A message is sent which includes portions of another message in an effort to gain access to otherwise unauthorized information

• Denial of Service:
  An attacker forces the service to exhaust its resources
Security Services

- Authorization
- Integrity
- Non-repudiation
- Confidentiality
- Authentication
- Availability
Web Service Security Functions

- Service to Service Authentication
- Identity Management
- Establishing Trust between Services
- Authorization and Access Management
- Confidentiality and Integrity of Service to Service Interchange
- Accountability End-to-End throughout a Service Chain
- Availability of Web services
- Security The Discovery Service
# Web Security Services

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Requirement</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messaging</td>
<td>Confidentiality and Integrity</td>
<td>WS-Security (XML DSig/Enc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSL/TLS (HTTPS)</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>WS-Security (SAML, X.509)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSL/TLS (X.509)</td>
</tr>
<tr>
<td>Resource</td>
<td>Authorization</td>
<td>XACML</td>
</tr>
<tr>
<td></td>
<td></td>
<td>XrML</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RBAC</td>
</tr>
<tr>
<td></td>
<td>Privacy</td>
<td>EPAL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>XACML</td>
</tr>
<tr>
<td></td>
<td>Accountability</td>
<td>Auditing</td>
</tr>
<tr>
<td>Discovery</td>
<td>Registries</td>
<td>UDDI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ebXML</td>
</tr>
</tbody>
</table>
Secure Implementation Tools and Technologies

• Web Services Developer Toolkits
• XML Parsers
• Languages for Secure Web Service Development
• Security Testing Tools and Techniques
Some Publications in Development

• Draft Special Publication 800-53, Revision 2, Recommended Security Controls for Federal Information Systems Special Update
• NIST Special Publication 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
• Draft Special Publication 800-39, Managing Risk from Information Systems: An Organizational Perspective
• Draft NIST Special Publication 800-73-2, Interfaces for Personal Identity Verification
• Draft NIST Interagency Report 7328, Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information System
• Draft SP 800-61 Revision 1, Computer Security Incident Handling Guide