CRYPTOGRAPHIC VALIDATION CHALLENGES WITH BRITTLE ALGORITHMS

Apostol Vassilev
NIST
(July, 2015)
Brittle (Dictionary.com):

1) having hardness and rigidity but little tensile strength; breaking readily with a comparatively smooth fracture, as glass.

2) easily damaged or destroyed; fragile; frail.
Brittleness of a cryptographic algorithm

- modern cryptographic algorithms (e.g., block ciphers) are public
  - depend on strong keys and keeping them secret
- characterizes not just the theoretical security properties of the algorithm;
- but also the opportunities an algorithm offers for robust implementations in a variety of environments
EXAMPLE: AES-GCM

• Very efficient and universally liked symmetric cipher

• A NIST standard – SP 800-38D (2007)
  - mandates uniqueness of key/IV pair for security
  - sets specific requirements for acceptable IV construction
Example: AES-GCM (continued)

What happens when the key/IV uniqueness is compromised?
The NIST CMVP

MISSION:

Improve the security and technical quality of cryptographic modules employed by Federal agencies (U.S. and Canada) and industry by

- developing standards;
- research and development of test methods & validation criteria;
- leverage accredited independent third-party testing laboratories
The international aspects of CMVP

- Adoption of CMVP standards into ISO
  - ISO/IEC 19790 Security Requirements for Cryptographic Modules
  - ISO/IEC 24759 Test requirements for cryptographic modules

- Japanese Government Relationship
  - Japan Cryptographic Module Validation Program (JCMVP)
  - Support of dually accredited Japanese testing laboratories
International footprint of the CMVP

Development of standards, test artifacts, proficiency exams and training

NVLAP HB 150-17: Cryptographic and Security Testing
CMVP Testing and Validation Flow

**Vendor**
- Designs and Produces
  - Hardware • Software • Firmware
- Define Boundary
- Define Approved Mode of Operation
- Security Policy

**CST Lab**
- Tests for Conformance
  - Derived Test Requirements
  - CAVP Algorithm Testing
  - Documentation Review
  - Source Code Review
  - Operational and Physical Testing

**CMVP**
- Validates
  - Review Test Results
  - Ongoing NVLAP Assessment
  - Issue Certificates
  - NIST Cost Recovery Fee

**User**
- Specifies and Purchases
  - Security and Assurance
    - Applications or products with embedded modules

NIST and CSEC Validates
- Review Test Results
- Ongoing NVLAP Assessment
- Issue Certificates
- NIST Cost Recovery Fee

CMVP NIST and CSEC
- Validates
  - Review Test Results
  - Ongoing NVLAP Assessment
  - Issue Certificates
  - NIST Cost Recovery Fee

User
- Specifies and Purchases
  - Security and Assurance
    - Applications or products with embedded modules

NIST and CSEC
- Validates
  - Review Test Results
  - Ongoing NVLAP Assessment
  - Issue Certificates
  - NIST Cost Recovery Fee

CMVP
- Validates
  - Review Test Results
  - Ongoing NVLAP Assessment
  - Issue Certificates
  - NIST Cost Recovery Fee

CST Lab
- Tests for Conformance
  - Derived Test Requirements
  - CAVP Algorithm Testing
  - Documentation Review
  - Source Code Review
  - Operational and Physical Testing

Vendor
- Designs and Produces
  - Hardware • Software • Firmware
- Define Boundary
- Define Approved Mode of Operation
- Security Policy

CMVP NIST and CSEC
- Validates
  - Review Test Results
  - Ongoing NVLAP Assessment
  - Issue Certificates
  - NIST Cost Recovery Fee

User
- Specifies and Purchases
  - Security and Assurance
    - Applications or products with embedded modules

NIST and CSEC
- Validates
  - Review Test Results
  - Ongoing NVLAP Assessment
  - Issue Certificates
  - NIST Cost Recovery Fee
Example: AES-GCM (continued)

SP 800-38D requires IV’s be constructed inside the crypto module boundary to guarantee uniqueness of key/IV pairs.

But…

• collides with existing industry crypto standards:
  • CNG
  • PKCS#11
• Protocol implementations:
  - TLS (RFC 5288), IPSec (RFC 5282), etc.
A note on testing AES-GCM in the CMVP

- The key/IV uniqueness requirement is tested by implementation inspection, **not** machine tested
  - a source of trouble for the testing laboratories and vendors
  - requires special attention by the NIST reviewers too
  - potential for confusion among federal users of cryptography
A note on existing industry crypto standards

• The problem discussed on the previous slide should not be taken to indicate that the architecture of these libraries is bad.
  - they predate AES-GCM and have proven track records of adoption
  - hopefully it is a matter of natural evolution and time to adopt this algorithm properly
A SOBERING OBSERVATION:

- AES-GCM - a good but brittle algorithm

Adoption as a NIST standard has led to difficulties for all constituencies:

- vendors of cryptographic technology
- independent accredited third-party testing laboratories
- NIST validation programs
- federal users of cryptography
CONCLUSION:

Someone once said this about standards:

“With ISO 9000 you can … certify a manufacturer that makes life jackets out of concrete”, Richard Buetow, Motorola

Selecting robust lightweight primitives for potential future standardization is important to avoid running into unpleasant unintended consequences

Robustness is more than just classic theoretical security analysis
Questions?