From: Yesha, Yaacov (Fed)
To: Peralta, Rene C. (Fed); Black, Paul E. (Fed); Bojanova, Irena V. (Fed); Yan Wu; Kelsey, John M. (Fed)
Subject: Re: BF crypto - resources
Date: Thursday, September 15, 2016 5:13:50 PM

This is a very good point. Using plain RSA may be considered
using an adequate algorithm, namely, RSA, without a crucial additional step that is needed for making the whole process adequate. This may be considered a different type of weakness than using an encryption algorithm that is not adequate.

Regards,

Yaacov

From: Peralta, Rene (Fed)
Sent: Thursday, September 15, 2016 9:05:56 AM
To: Black, Paul E. (Fed); Yesha, Yaacov (Fed); Bojanova, Irena V. (Fed); Yan Wu; Kelsey, John M. (Fed)
Subject: Re: BF crypto - resources

I wonder if "inadequate encryption algorithm" is different from
"inadequate use of an (adequate) encryption algorithm". If so, I
would use the latter to describe plain RSA. But I don't really know
the extent of the term "algorithm" in computer security jargon.

Regards, Rene.

From: Black, Paul E. (Fed)
Sent: Wednesday, September 14, 2016 1:40 PM
To: Yesha, Yaacov (Fed); Bojanova, Irena V. (Fed); Yan Wu; Peralta, Rene (Fed); Kelsey, John M. (Fed)
Subject: Re: BF crypto - resources
That's CWE-327 Use of a Broken or Risky Cryptographic Algorithm (2.9)

One can Google CWE and key word, and one often gets a hit.

-paul-
Paul E. Black 100 Bureau Drive, Stop 8970
paul.black@nist.gov Gaithersburg, Maryland 20899-8970
voice: +1 301 975-4794 fax: +1 301 975-6097

http://hissa.nist.gov/~black/ KC7PKT

Curriculum Vitae for Paul E. Black

hissa.nist.gov

Curriculum Vitae for Paul E. Black Personal Data. Name: Paul E. Black; Title: Computer Scientist; Mailing Address: National Institute of Standards and Technology

---

From: Yesha, Yaacov (Fed)
Sent: Wednesday, September 14, 2016 1:37 PM
To: Bojanova, Irena V. (Fed); Black, Paul E. (Fed); Yan Wu; Peralta, Rene (Fed); Kelsey, John M. (Fed)
Subject: RE: BF crypto - resources

Irena,

The following weakness may be already included within one of the items in the resources you provided, but I will mention it anyway:
Using an inadequate encryption algorithm (i.e. one that is vulnerable to a successful attack).
Example: plain RSA (https://en.wikipedia.org/wiki/RSA_(cryptosystem)

Yaacov

From: Bojanova, Irena V. (Fed)
Sent: Monday, September 12, 2016 11:58 AM
To: Black, Paul E. (Fed) <paul.black@nist.gov>; Yesha, Yaacov (Fed) <yaacov.yesha@nist.gov>; Yan Wu <yanwu@bgsu.edu>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Subject: BF crypto - resources

Paul, Yaacov, and Yan, here are some resources that may help our discussion on crypto-related BF classes:

John and Rene, please let us know if some other sources would be useful.

* NIST SP 800-175B Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf):
SECTION 3: CRYPTOGRAPHIC ALGORITHMS
3.1 Cryptographic Hash Functions
3.2 Symmetric-Key Algorithms (Block Cipher Algorithms, Hash-based Symmetric-key Algorithms)
3.3 Asymmetric-Key Algorithms
3.4 Algorithm Security Strength
3.5 Algorithm Lifetime
SECTION 4: CRYPTOGRAPHIC SERVICES

4.1 Data Confidentiality

4.2 Data Integrity and Source Authentication (Hash Functions, Message Authentication Code Algorithms, Digital Signature Algorithms)

4.3 Combining Confidentiality and Authentication in a Block-Cipher Mode of Operation

4.4 Random Bit Generation

4.5 Symmetric vs. Asymmetric Cryptography

SECTION 5: KEY MANAGEMENT

5.1 General Key Management Guidance

5.2 Cryptographic Key Management Systems (Framework, System Profile, Public Key Infrastructure)

5.3 Key Establishment (Generation, Derivation, Agreement, Transport, Wrapping, Derivation from a Password)

5.4 Key Management Issues (Manual vs. Automated Key Establishment, Selecting and Operating a CKMS, Storing and Protecting Keys, Cryptoperiods, Use Validated Algorithms and Cryptographic Modules, Control of Keying Material, Compromises, Accountability and Auditing)

SECTION 6: OTHER ISSUES

6.1 Required Security Strength

6.2 Interoperability

6.3 When Algorithms are No Longer Approved

6.4 Registration Authorities (RAs)

6.5 Cross Certification

* NIST Cryptographic Toolkit (http://csrc.nist.gov/groups/ST/toolkit/):

Block Ciphers

Block Cipher Modes

Digital Signatures

Entity Authentication

Implementation Guideline

Key Management

Key Derivation Functions

Message Authentication

Random Number Generation

Secure Hashing

Algorithms

* NISTIR 7977 NIST Cryptographic Standards and Guidelines Development Process (http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf).

Irena