MITM-ing cryptographic standards

~~Looking back on a 3 year old accident~~

~~How the f*** did we get there again?~~

Tales from a Rogue Archive

MITM-ing cryptographic standards

~~Looking back on a 3 year old accident~~
~~How the f*** did we get there again?~~

Tales from a Rogue Archive

*not sponsored by

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

MITM-ing cryptographic standards

~~Looking back on a 3 year old accident~~
~~How the f*** did we get there again?~~

Tales from a Rogue Archive

wtf bru

*not sponsored by

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
CSRC
Projects
Publications +
Topics +
News & Updates
Events
Glossary
About CSRC +
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
PREPARE

COMPUTER SECURITY RESOURCE CENTER

NIST UPDATES THE RISK MANAGEMENT FRAMEWORK (SP 800-37 REV. 2)!

NEW SEARCH INTERFACE AVAILABLE FOR CRYPTO ALGORITHM VALIDATIONS

REQUESTING LIGHTWEIGHT CRYPTO ALGORITHM NOMINATIONS

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- see our greatly-expanded **publications library**,
- explore content by **topic**,
- search our **glossary** of information security terms, and
- subscribe to **CSRC email updates**.

POPULAR LINKS

Crypto Standards & Guidelines

Publications:
Drafts / **FIPS** / **SP 800s**

Crypto Module Validation

FIPS 140-2 Modules & Vendors

Crypto Algorithm Validations

Risk Management Framework

RECENT NEWS

RMF Update: NIST Publishes SP 800-37 Rev. 2

December 20, 2018

NIST has published an update to its Risk Management Framework specification, in NIST Special Publication (SP) 800-37 Revision 2.

NIST Releases Draft SP 800-189 for Comment

December 17, 2018

Draft Special Publication 800-189, "Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation," is now available for comment. The deadline for submitting comments is February 15, 2019.

NIST Publishes NISTIR 8011 Vol. 3

NIST
Search CSRC
CSRC MENU
CSRC
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
PREPARE

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

POPULAR LINKS

- Crypto Standards & Guidelines
- Publications:
  Drafts / FIPS / SP 800s
- Crypto Module Validation
- FIPS 140-2 Modules & Vendors
- Crypto Algorithm Validations
- Risk Management Framework

NIST UPDATES THE RISK MANAGEMENT FRAMEWORK (SP 800-37 REV. 2)!

NEW SEARCH INTERFACE AVAILABLE FOR CRYPTO ALGORITHM VALIDATIONS

REQUESTING LIGHTWEIGHT CRYPTO ALGORITHM NOMINATIONS

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- see our greatly-expanded **publications library**,
- explore content by **topic**,
- search our **glossary** of information security terms, and
- subscribe to **CSRC email updates**.

RECENT NEWS

RMF Update: NIST Publishes SP 800-37 Rev. 2

December 20, 2018

NIST has published an update to its Risk Management Framework specification, in NIST Special Publication (SP) 800-37 Revision 2.

NIST Releases Draft SP 800-189 for Comment

December 17, 2018

Draft Special Publication 800-189, "Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation," is now available for comment. The deadline for submitting comments is February 15, 2019.

NIST Publishes NISTIR 8011 Vol. 3

NIST
Search CSRC
CSRC MENU
CSRC
PROJECTS

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

Cryptographic Standards and Guidelines

Project Overview

Users of the former "Crypto Toolkit" can now find that content under this project. It includes cryptographic primitives, algorithms and schemes are described in some of NIST's Federal Information Processing Standards (FIPS), Special Publications (SPs) and NIST Internal/Interagency Reports (NISTIRs).

Crypto Standards and Guidelines, by Project Area

- Block Cipher Techniques
- Digital Signatures
- Hash Functions
- Key Management
- Message Authentication Codes (MACs)
- Post-quantum Techniques
- Random Bit Generation

Implementation-related References

- Examples with Intermediate Values
- Object Identifiers (OIDs): Computer Security Objects Register
- Cryptographic Algorithm Validation Program (CAVP)

PROJECT LINKS

Overview

Publications

ADDITIONAL PAGES

Example Values
Crypto-Enabled Applications
Withdrawn Crypto Standards
Archived Crypto Projects
AES Development

CONTACTS

Dr. Lily Chen
lily.chen@nist.gov

GROUP

Cryptographic Technology

RELATED PROJECTS

NIST
Search CSRC
CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

CSRC

Publication Search

Quick Links

- Draft Pubs
- Final Pubs
- FIPS
- SPs (Special Pubs)
- NISTIRs
- ITL Bulletins
- White Papers
- Journal Articles
- Conference Papers
- Books

Search

800-

Search publication record data

(not a full text search)

Sort By

Number (highest to lowest)

Results View

Brief

Items Per Page All

Date

/ / / /

Search Results

Keywords: ✖ 800- Sorted By: ✖ Number (highest to lowest) Status: ✖ Draft ✖ Final Series: ✖ SP

Showing **170** matching records.

Series	Number	Title	Status	Release Date
SP	800-203	**2017 NIST/ITL Cybersecurity Program Annual Report** Download: SP 800-203 (DOI); Local Download	Final	7/02/2018
SP	800-202	**Quick Start Guide for Populating Mobile Test Devices** Download: SP 800-202 (DOI); Local Download; Computer Forensics Tool Testing (CFTT) Program; CFTT Federated Testing Project	Final	5/10/2018
SP	800-195	**2016 NIST/ITL Cybersecurity Program Annual Report** Download: SP 800-195 (DOI); Local Download	Final	9/28/2017
SP	800-193	**Platform Firmware Resiliency Guidelines** Download: SP 800-193 (DOI); Local Download	Final	5/04/2018
SP	800-192	**Verification and Test Methods for Access Control Policies/Models** Download: SP 800-192 (DOI); Local Download	Final	6/27/2017
SP	800-190	**Application Container Security Guide** Download: SP 800-190 (DOI); Local Download	Final	9/25/2017
SP	800-189	**Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation** Download: SP 800-189 (DRAFT) (DOI); Local Download	Draft	12/17/2018
SP	800-188	**De-Identifying Government Datasets (2nd Draft)** Download: Draft SP 800-188; Comment Template	Draft	12/15/2016
SP	800-187	**Guide to LTE Security** Download: SP 800-187 (DOI); Local Download	Final	12/21/2017
SP	800-185	**SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash** Download: SP 800-185 (DOI); Local Download; Comments Received on Draft SP 800-185	Final	12/22/2016

NIST
Search CSRC
CSRC MENU
CSRC
PROJECTS
CRYPTOGRAPHIC MODULE VALIDATION PROGRAM

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

Cryptographic Module Validation Program

Validated Modules

> ***All questions regarding the implementation and/or use of any validated cryptographic module should first be directed to the appropriate VENDOR point of contact (listed for each entry).***

SEARCH our database of validated modules.

The FIPS 140-1 and FIPS 140-2 validated modules search provides access to the official validation information of all cryptographic modules that have been tested and validated under the Cryptographic Module Validation Program as meeting requirements for FIPS PUB 140-1 and FIPS PUB 140-2. The search results list all issued validation certificates that meet the supplied search criteria and provide a link to view more detailed information about each certificate. The Certificate Detail listing provides the detailed module information including algorithm implementation references to the CAVP algorithm validation, Security Policies, original certificate images or reference to the consolidated validation lists, and vendor product links if provided.

If a validation certificate is marked as **revoked**, the module validation is no longer valid and may not be referenced to demonstrate compliance to FIPS 140-1 or FIPS 140-2.

If a validation certificate is marked as **historical**, Federal Agencies should not include these in new procurement. This does not mean that the overall FIPS-140 certificates for these modules have been revoked, rather it indicates that the certificates and the documentation posted with them are more than 5 years old and have not been updated to reflect latest guidance and/or transitions, and may not accurately reflect how the module can be used in FIPS mode. Agencies may make a risk determination on whether to continue using the modules on this list based on their own assessment of where and how the module is used.

It is important to note that validation certificates are issued for cryptographic *modules*. A module may *either* be an

PROJECT LINKS

Overview

News

ADDITIONAL PAGES

- **Standards**
- **IG Announcements**
  - Announcements Archive
- **Contacts**
- **Notices**
- **Validated Modules**
  - Search
- **Modules In Process**
  - Modules In Process List
  - Implementation Under Test List
- **CMVP Management Manual and FAQs**
- **Use of FIPS 140-2 Logo and Phrases**

CONTACTS

Beverly Trapnell

NIST CMVP Acting Program Manager

cmvp@nist.gov

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

Computer Security Resource Center

Due to the lapse in government funding, csrc.nist.gov and all associated online activities will be unavailable until further notice. Learn more.

Explore
Settings
Tweet
Search Twitter

briankrebs
@briankrebs

Due to a government shutdown, we're going to take away resources that might otherwise help make things more secure. Someone had to unpublish or hide this information. Well done USG! csrc.nist.gov/publications commerce.gov/news/blog/2018...

ory
RITY RESOURCE CENTER

Computer Security Resource Center

apse in government funding, csrc.nist.gov and all associated online activities will be unavailable until further n

4:36 am · 4 Jan 2019 · Twitter Web Client

223 Retweets 32 Quote Tweets 381 Likes

Chris Olive @ChrisEOlive · 4 Jan 2019
Replying to @briankrebs
When I worked at the #DoD, shutdowns meant “all non-essential functions” would shutdown. So… read into that whatever you like. I’m sure the disposition here hasn’t changed in 25 years.

2

Clint Bowling @bowlingca44 · 4 Jan 2019
Replying to @briankrebs
No wall no deal

New to Twitter?

Sign up now to get your own personalized timeline!

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

Relevant people

briankrebs
@briankrebs

Independent investigative journalist. Covers cybercrime, security, privacy. Author of 'Spam Nation,' a NYT bestseller. Former Washington Post reporter, '95-'09

Trends for you

Trending in France
Fields
47.7K Tweets

Trending in France
#BAC2022
37.9K Tweets

Trending in France
Dunkerque
1,047 Tweets

Trending in France
Cyclades
5,697 Tweets

Trending in France

Don’t miss what’s happening
People on Twitter are the first to know.

gandi.net
DOMAINS
HOSTING
SSL CERTIFICATES
Log in
Chat with us

Register a domain name

nist.rip

INCLUDED WITH EVERY DOMAIN NAME

- ✓ 2 mailboxes with 3GB storage
- ✓ Unlimited aliases and forwarding
- ✓ 1 Standard SSL certificate 1 Year to activate
- ✓ Our LiveDNS nameservers Anycast + DNSSEC

865 results

nist.rip appears to be taken. See WHOIS

nist.sh	-30% ~~€ 88.24~~	€ 61.76 1 year then € 88.24 /year	🛒
nist.st		€ 22.78 1 year then € 24.96 /year	🛒
nist.page VIEW CONDITIONS		€ 16.04 1 year then € 16.96 /year	🛒
nist.art Premium Lower Renew Price	-46% ~~€ 1,201.24~~	€ 652.21 1 year then € 51.29 /year	🛒
nist.sk		€ 22.80 1 year then € 24.96 /year	🛒
nist.tw		€ 25.00 1 year then € 24.96 /year	🛒
nist.mobi	-85% ~~€ 34.87~~	€ 5.28 1 year then € 34.87 /year	🛒
nist.tv		€ 34.20 1 year then € 34.96 /year	🛒

Shopping Cart 0

Your shopping cart is empty

Looks like you haven't added anything to your cart yet

Prices for **France**, incl. VAT in € (EUR) Change

NIST
Search CSRC
CSRC MENU
CSRC
MONITOR
CATEGORIZE
SELECT
PREPARE
AUTHORIZE
IMPLEMENT
ASSESS

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

This is an archive
(replace .gov by .rip)

- Projects
- Publications +
- Topics +
- News & Updates
- Events
- Glossary
- About CSRC +

POPULAR LINKS

Crypto Standards & Guidelines

Publications:
Drafts / FIPS / SP 800s

Crypto Module Validation

FIPS 140-2 Modules & Vendors

Crypto Algorithm Validations

Risk Management Framework

NIST UPDATES THE RISK MANAGEMENT FRAMEWORK (SP 800-37 REV. 2)!

NEW SEARCH INTERFACE AVAILABLE FOR CRYPTO ALGORITHM VALIDATIONS

REQUESTING LIGHTWEIGHT CRYPTO ALGORITHM NOMINATIONS

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- see our greatly-expanded **publications library**,
- explore content by **topic**,
- search our **glossary** of information security terms, and
- subscribe to **CSRC email updates**.

RECENT NEWS

RMF Update: NIST Publishes SP 800-37 Rev. 2

December 20, 2018

NIST has published an update to its Risk Management Framework specification, in NIST Special Publication (SP) 800-37 Revision 2.

NIST Releases Draft SP 800-189 for Comment

December 17, 2018

Draft Special Publication 800-189, "Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation," is now available for comment. The deadline for submitting comments is February 15, 2019.

NIST Publishes NISTIR 8011 Vol. 3

NIST
Search CSRC
CSRC MENU
CSRC
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
PREPARE

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

This is an archive
(replace .gov by .rip)

- Projects
- Publications +
- Topics +
- News & Updates
- Events
- Glossary
- About CSRC +

POPULAR LINKS

Crypto Standards & Guidelines

Publications:
Drafts / FIPS / SP 800s

Crypto Module Validation

FIPS 140-2 Modules & Vendors

Crypto Algorithm Validations

Risk Management Framework

NIST UPDATES THE RISK MANAGEMENT FRAMEWORK (SP 800-37 REV. 2)!

NEW SEARCH INTERFACE AVAILABLE FOR CRYPTO ALGORITHM VALIDATIONS

REQUESTING LIGHTWEIGHT CRYPTO ALGORITHM NOMINATIONS

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- see our greatly-expanded **publications library**,
- explore content by **topic**,
- search our **glossary** of information security terms, and
- subscribe to **CSRC email updates**.

RECENT NEWS

RMF Update: NIST Publishes SP 800-37 Rev. 2

December 20, 2018
NIST has published an update to its Risk Management Framework specification, in NIST Special Publication (SP) 800-37 Revision 2.

NIST Releases Draft SP 800-189 for Comment

December 17, 2018
Draft Special Publication 800-189, "Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation," is now available for comment. The deadline for submitting comments is February 15, 2019.

NIST Publishes NISTIR 8011 Vol. 3

1 2 3 4 5 6 7 8 9
Projects | CSRC - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:18
Projects | CSRC
csrc.nist.rip/projects
Guest
NIST
Search CSRC
CSRC MENU
CSRC

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

This is an archive
(replace .gov by .rip)

- Projects
- Publications +
- Topics +
- News & Updates
- Events
- Glossary
- About CSRC +

Search

Search Project Name, Acronym, Description

Sort By: Relevance (best match)

Items Per Page: 25

Topics

Match ANY: ● Match ALL: ○

Projects

Sorted By: ✖ Project Name (A-Z)

Showing **1** through **25** of **70** matching records.

1 | 2 | 3 > >>

Access Control Policy and Implementation Guides ACP&IG

Adequate security of information and information systems is a fundamental management responsibility. Nearly all applications that deal with financial, privacy, safety, or defense include some form of access (authorization) control. Access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system. In some systems, complete access is granted after s successful authentication of the user, but most...

Access Control Policy Testing ACPT

Access control systems are among the most critical security components. Faulty policies, misconfigurations, or flaws in software implementation can result in serious vulnerabilities. The specification of access control policies is often a challenging problem. Often a system's privacy and security are compromised due to the misconfiguration of access control policies instead of the failure of cryptographic primitives or protocols. This problem becomes increasingly severe as software systems...

Algorithms for Intrusion Measurement AIM

The Algorithms for Intrusion Measurement (AIM) project furthers measurement science in the area of algorithms used in the field of intrusion detection. The team focuses on both new detection metrics and measurements of scalability (more formally algorithmic complexity). This analysis is applied to different phases of the detection lifecycle to include pre-emptive vulnerability analysis, initial attack detection, alert impact, alert aggregation/correlation, and compact log storage. In...

Apple macOS Security Configuration APPLE-OS

CSD's macOS security configuration team is working to develop secure system configuration baselines supporting different operational environments for Apple macOS version 10.12, "Sierra." These configuration guidelines will assist organizations with hardening macOS

1 2 3 4 5 6 7 8 9
Initial commit · plcp/nist.rip@5d01686 · GitHub - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:20
Projects | CSRC
Initial commit · plcp/nist.r
github.com/plcp/nist.rip/commit/5d01686bc811bc67a5bd12ee771baa00d5e797e6
Guest
Split
Unified
Filter changed files
.gitignore
library.html
nist.py
pdfs
.gitignore
requirements.txt
whitelist.txt

Showing **6 changed files** with **350 additions** and **0 deletions**.

```
+
+    text += '</body></html>'
+    return text
+
+
+ @app.route('/', defaults={'path': 'index.html'})
+ @app.route('/<path:path>')
+ def nist(path):
+    path = fixup_path(path)
+    path = redact_path(path)
+
+    out = from_filesystem(path)
+    if out is None:
+        pull_wayback(path)
+        out = from_filesystem(path)
+
+    if out is None:
+        return not_found(path), 404
+
+    if path.endswith('.js'):
+        mimetype = 'text/script'
+    elif path.endswith('.css'):
+        mimetype = 'text/css'
+    else:
+        mime = magic.Magic(mime=True)
+        mimetype = mime.from_buffer(out)
+
+    out = out.replace(b'csrc.nist.gov', b'csrc.nist.rip')
+    out = out.replace(b'webmaster-csrc@nist.gov', b'webmaster-csrc@nist.rip')
+    return Response(out, mimetype=mimetype)
+
+
+ if __name__ == '__main__':
+    app.run(host='0.0.0.0', port='8080')
```

1 pdfs/.gitignore

```
@@ -0,0 +1 @@
+ *.pdf
```

3 requirements.txt

1 2 3 4 5 6 7 8 9
Initial commit · plcp/nist.rip@5d01686 · GitHub - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:20
Projects | CSRC
Initial commit · plcp/nist.r
github.com/plcp/nist.rip/commit/5d01686bc811bc67a5bd12ee771baa00d5e797e6
Guest
Split
Unified
Filter changed files
.gitignore
library.html
nist.py
pdfs
.gitignore
requirements.txt
whitelist.txt

Showing **6 changed files** with **350 additions** and **0 deletions**.

```
+
+     text += '</body></html>'
+     return text
+
+
+ @app.route('/', defaults={'path': 'index.html'})
+ @app.route('/<path:path>')
+ def nist(path):
+     path = fixup_path(path)
+     path = redact_path(path)
+
+     out = from_filesystem(path)
+     if out is None:
+         pull_wayback(path)
+         out = from_filesystem(path)
+
+     if out is None:
+         return not_found(path), 404
+
+     if path.endswith('.js'):
+         mimetype = 'text/script'
+     elif path.endswith('.css'):
+         mimetype = 'text/css'
+     else:
+         mime = magic.Magic(mime=True)
+         mimetype = mime.from_buffer(out)
+
+     out = out.replace(b'csrc.nist.gov', b'csrc.nist.rip')
+     out = out.replace(b'webmaster-csrc@nist.gov', b'webmaster-csrc@nist.rip')
+     return Response(out, mimetype=mimetype)
+
+
+ if __name__ == '__main__':
+     app.run(host='0.0.0.0', port='8080')
```

1 pdfs/.gitignore

```
@@ -0,0 +1 @@
+ *.pdf
```

3 requirements.txt

NIST Special Publication 800-90A
Revision 1

Recommendation for Random Number Generation Using Deterministic Random Bit Generators

Elaine Barker
John Kelsey

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-90Ar1

COMPUTER SECURITY

National Institute of
Standards and Technology
U.S. Department of Commerce

sp800-90Arev1-final (7-16-2015) with ceiling corrections
102 / 110
100%
nist.rip
3/10
98
99
100
101
102
103

Appendix D : (Informative) References

[FIPS 140] Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001 (including Change Notices as of December 3, 2002).
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf [accessed 6/9/15].

[FIPS 180] Federal Information Processing Standard (FIPS) 180-4, *Secure Hash Standard* (*SHS*), March 2012.
http://csrc.nist.rip/publications/fips/fips180-4/fips-180-4.pdf [accessed 6/9/15].

[FIPS 197] Federal Information Processing Standard (FIPS) 197, *Advanced Encryption Standard* (*AES*), November 2001.
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [accessed 6/9/15].

[FIPS 198] Federal Information Processing Standard (FIPS) 198-1, *The Keyed-Hash Message Authentication Code* (*HMAC*), July 2008.
http://csrc.nist.rip/publications/fips/fips198_-1/FIPS-198-1_final.pdf [accessed 6/9/15].

[SP 800-38A] National Institute of Standards and Technology Special Publication (SP) 800-38A, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, December 2001.
http://csrc.nist.rip/publications/nistpubs/800-38a/sp800-38a.pdf [accessed 6/9/15].

[SP 800-38D] National Institute of Standards and Technology Special Publication (SP) 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, November 2007.
http://csrc.nist.rip/publications/nistpubs/800-38D/SP-800-38D.pdf [accessed 6/9/15].

[SP 800-57] NIST Special Publication (SP) 800-57 Part 1 Revision 3, *Recommendation for Key Management—Part 1*: General, July 2012.
http://csrc.nist.rip/publications/nistpubs/800-57/sp800_-57_part1_rev3_general.pdf [accessed 6/9/15].

[SP 800-67] NIST Special Publication (SP) 800-67 Revision 1, *Recommendation for the Triple Data Encryption Algorithm* (*TDEA*) *Block Cipher*, January 2012.
http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf [accessed 6/9/15].

[SP 800-90B] NIST Special Publication (SP) 800-90B (Draft), *Recommendation for the Entropy Sources Used for Random Bit Generation*, August 2012 [re-released September 2013].
http://csrc.nist.rip/publications/drafts/800-90/draft-sp800-90b.pdf [accessed 6/9/15].

[SP 800-90C] NIST Special Publication (SP) 800-90C (Draft), *Recommendation for Random Bit Generator (RBG) Constructions*, August 2012 [re-released September 2013].

sp800-90Arev1-final (7-16-2015) with ceiling corrections
3 / 110
100%
3
4
5
6
7
mailto:rbg_comments@nist.rip

however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-90A Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-90A Rev. 1, 109 pages (June 2015)
CODEN: NSPUE2

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-90Ar1

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments may be provided to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: rbg_comments@nist.rip

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

1 2 3 4 5 6 7 8 9
Don't corrupt original files · plcp/nist.rip@c8bebdc · GitHub - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:43
Projects | CSRC
Don't corrupt original file
github.com/plcp/nist.rip/commit/c8bebdc50536e850393d0a5e4c3fb66c9ffb37e2
Guest
Product
Team
Enterprise
Explore
Marketplace
Pricing
Search
Sign in
Sign up
plcp / nist.rip
Public
Notifications
Fork 0
Star 0
Code
Issues 1
Pull requests
Actions
Projects
Wiki
Security
Insights

Don't corrupt original files

Browse files

master

plcp committed on 15 Jan 2019

1 parent 655a019 commit c8bebdc50536e850393d0a5e4c3fb66c9ffb37e2

Showing **1 changed file** with **3 additions** and **0 deletions**.

Split
Unified

3 nist.py

```
@@ -337,6 +337,9 @@ def nist(path):
        mime = magic.Magic(mime=True)
        mimetype = mime.from_buffer(out[:2**20])

+    if 'application' in mimetype or path.endswith(library_extensions):
+        return Response(out, mimetype=mimetype)
+
    out = out.replace(bytes(_old_url, 'utf8'), bytes(_base_url, 'utf8'))
    out = out.replace(b'webmaster-csrc@nist.gov', b'webmaster-csrc@nist.rip')

```

0 comments on commit c8bebdc

Please sign in to comment.

1 2 3 4 5 6 7 8 9
Projects | CSRC - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:43
Projects | CSRC
csrc.nist.rip/projects
Guest
NIST
Search CSRC
CSRC MENU
https://csrc.nist.rip/library

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

CSRC

This is an archive
(replace .gov by .rip)

Projects

Publications +

Topics +

News & Updates

Events

Glossary

About CSRC +

Search

Search Project Name, Acronym, Description

Sort By: Relevance (best match)

Items Per Page: 25

Topics

Match ANY: ● Match ALL: ○

Projects

Sorted By: ✖ Project Name (A-Z)

Showing **1** through **25** of **70** matching records.

1 | 2 | 3 > >>

Access Control Policy and Implementation Guides ACP&IG

Adequate security of information and information systems is a fundamental management responsibility. Nearly all applications that deal with financial, privacy, safety, or defense include some form of access (authorization) control. Access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system. In some systems, complete access is granted after s successful authentication of the user, but most...

Access Control Policy Testing ACPT

Access control systems are among the most critical security components. Faulty policies, misconfigurations, or flaws in software implementation can result in serious vulnerabilities. The specification of access control policies is often a challenging problem. Often a system's privacy and security are compromised due to the misconfiguration of access control policies instead of the failure of cryptographic primitives or protocols. This problem becomes increasingly severe as software systems...

Algorithms for Intrusion Measurement AIM

The Algorithms for Intrusion Measurement (AIM) project furthers measurement science in the area of algorithms used in the field of intrusion detection. The team focuses on both new detection metrics and measurements of scalability (more formally algorithmic complexity). This analysis is applied to different phases of the detection lifecycle to include pre-emptive vulnerability analysis, initial attack detection, alert impact, alert aggregation/correlation, and compact log storage. In...

Apple macOS Security Configuration APPLE-OS

CSD's macOS security configuration team is working to develop secure system configuration baselines supporting different operational environments for Apple macOS version 10.12, "Sierra." These configuration guidelines will assist organizations with hardening macOS

1 2 3 4 5 6 7 8 9
NIST Computer Security Resource Center | Library - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:43
Projects | CSRC
NIST Computer Security R
csrc.nist.rip/library
Guest

```
Files available¹ to download: Filter                                                                [guide]
                                                                                                     [back]
       * NIST IR 7046.pdf
       * alt-SP800-171r1.pdf
       * NIST IR 6390 Randomness Testing of the Advanced Encryption Standard Candidate Algorithms, 1999-09.pdf
       * NIST SP 500-299 Draft Cloud Computing Security Reference Architecture, 2013-05-15.pdf
       * NIST SP 800-079-2 Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI), 2015-07-30 (Final).pdf
       * alt-NIST SP 800-88_Guidelines for Media Sanitization.pdf
       * NIST IR 7358 Program Review for Information Security Management Assistance (PRISMA), 2007-01.pdf
       * NIST SP 800-063v1.0.2 Electronic Authentication Guideline, 2006-04.pdf
       * cr-mfa-nist-sp1800-17.pdf
       * NIST SP 800-034r1 Contingency Planning Guide for Federal Information Systems, 2010-05.pdf
       * NIST SP 800-040r3 Guide to Enterprise Patch Management Technologies, 2013-07-22 (Final).pdf
       * NIST IR 7085.pdf
       * alt-IR8204-draft.pdf
       * NIST IR 7442.pdf
       * NIST SP 800-084 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, 2006-09-21 (Final).pdf
       * NIST SB 2009-02 Using PIV Credentials In Physical Access Control Systems (PACS).pdf
       * NIST IR 7551.pdf
       * NIST SB 2008-07 Guidelines On Implementing A Secure Sockets Layer (SSL) Virtual Private Network (VPN).pdf
       * NIST SP 800-070r2 National Checklist Program for IT Products; Guidelines for Checklist Users and Developers, 2011-02.pdf
       * NIST SP 800-051r1 Guide to Using Vulnerability Naming Schemes, 2011-02-25 (Final).pdf
       * NIST SP 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, 2017-08-07 (Final).pdf
       * alt-SP800-64r2.pdf
       * NIST IR 7697 Common Platform Enumeration; Dictionary Specification 2.3, 2011-08.pdf
       * NIST SP 800-038E Recommendation for Block Cipher Modes of Operation; the XTS-AES Mode for Confidentiality on Storage Devices, 2010-01-18 (Final).pdf
       * alt-SP800-55-rev1.pdf
       * NIST IR 7874.pdf
       * NIST SP 500-269 Web Application Scanner Functional Specification 1.0, 2007.pdf
       * NIST SB 1998-02 InfoSec and the World Wide Web (WWW).txt
       * NIST SP 800-059 Guideline for Identifying an Information System as a National Security System, 2003-08-20 (Final).pdf
       * NIST IR 7628 Guidelines for Smart Grid Cyber Security; Volume 02, 2010-08.pdf
       * fs-itam-nist-sp1800-5c.pdf
       * NIST SP 800-164 Guidelines on Hardware-Rooted Security in Mobile Devices, 2012-10-31 (Draft).pdf
       * NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing, 2011-12-09 (Final).pdf
       * NIST SP 800-054 Border Gateway Protocol Security, 2007-07.pdf
       * fs-pam-nist-sp1800-18-draft.pdf
       * NIST SB 2003-10 Information Technology Security Awareness, Training, Education, and Certification.pdf
       * NIST SB 2002-12 Security of Public Web Servers.pdf
       * NIST IR 7815 Access Control for Suspicious Activity Report (SAR) Systems, 2011-11-18.pdf
       * fs-itam-nist-sp1800-5a-draft.pdf
       * NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices, 2007-11.pdf
       * alt-SP800-183.pdf
       * alt-SP800-57part2.pdf
       * hit-wip-nist-sp1800-8b.pdf
       * NIST IR 7657 A Report on the Privilege (Access) Management Workshop, 2010-03.pdf
       * NIST SP 800-132 Recommendation for Password-Based Key Derivation; Part 1; Storage Applications, 2010-12-22 (Final).pdf
       * NIST SP 800-079-1 Guidelines for the Accreditation of PIV Card Issuers, 2008-06.pdf
       * NIST SP 800-121r1 Guide to Bluetooth Security, 2012-06-12.pdf
       * alt-SP800-182-2015AnnualReport.pdf
       * NIST SP 800-116.pdf
       * NIST SB 1998-02 Information Security and the World Wide Web (WWW).txt
       * NIST SP 800-046r1 Guide to Enterprise Telework and Remote Access Security, 2009-06.pdf
       * NIST IR 7665.pdf
```

NIST Computer Security Resource Center | Library - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:44
Projects | CSRC
NIST Computer Security R
csrc.nist.rip/library
Guest

```
* NTRU-Prime-Round2.zip
* 140sp483.pdf
* NIST.IR.8136.pdf
* 140crt961.pdf
* 140sp2180.pdf
* itlbul2010-07.pdf
* Lake-and-Locker-April2018.pdf
* 140sp1898.pdf
* program_SHA3_workshop_aug2014.pdf
* 140sp3738.pdf
* 140sp128.pdf
* NIST.SP.800-140.pdf
* Sandi_opening.pdf
* CMT20verbose.pdf
* 140sp2869.pdf
* werner_ness_gnd_derived_credentials_fips201-2_2015.pdf
* DavidT-ISPAB-Sept2006.pdf
* 2012_agenda-ispab-october-meeting.pdf
* RMAC.pdf
* 140sp3509.pdf
* may30_future-privacy-health-it_gbuchelt.pdf
* ckms_workshop_summary2012_final.pdf
* fips180-2.pdf
* ECDSA_Prime.pdf
* 3_software-assurance_pblack.pdf
* Chenok.pdf
* 140sp1308.pdf
* TinyJAMBU-Statements.pdf
* 140-1comments.pdf
* 03-06-Ahmed.pdf
* 140crt877.pdf
* qsg_select_management-perspective.pdf
* FERC-comments.pdf
* ISPAB_CDC-Social-Media_JNall.pdf
* fr000215.pdf
* 140crt495.pdf
* physecpaper05.pdf
* 140sp2485.pdf
* 140sp1730.pdf
* PIV-Gupta.pdf
* may30_road-confidence-samate_pblack.pdf
* 140sp3676.pdf
* 20101219_RBAC2_Final_Report.pdf
* isap-spec-round2.pdf
* ransomware_guidance.pdf
* fissea_2013_peer_choice_winner_poster.pdf
* 140sp3438.pdf
* CMT11verbose.pdf

-- 18321 files displayed --

Files sourced from archive.org and fismapedia.org. Download everything here.
```

1 2 3 4 5 6 7 8 9
NIST Computer Security Resource Center | Library - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:46
Projects | CSRC
NIST Computer Security R
csrc.nist.rip/library
Guest

```
Files available[1] to download: bluetooth                                                                                     [guide]
                                                                                                                              [back]
      * NIST SP 800-121r1 Guide to Bluetooth Security, 2012-06-12.pdf
      * NIST SB 2008-11 Bluetooth Security; Protecting Wireless Networks And Devices.pdf
      * NIST SP 800-121r2 Guide to Bluetooth Security, 2017-05-08 (Final).pdf
      * NIST SP 800-121 Guide to Bluetooth Security, 2008-09.pdf

      -- 4 files displayed --


Files sourced from archive.org and fismapedia.org. Download everything here.
```

1 2 3 4 5 6 7 8 9
NIST Computer Security Resource Center | Library - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:48
Projects | CSRC
NIST Computer Security R
csrc.nist.rip/library
Guest

Files available[1] to download: Filter

[collapse guide]
[back]

```
+ ANNUAL REPORTS

* [IR 7111]+4 - Computer Security Division 2003 Annual Report
* [IR 7219]+4 - Computer Security Division 2004 Annual Report
* [IR 7285]+4 - Computer Security Division 2005 Annual Report
* [IR 7399]+3 - Computer Security Division 2006 Annual Report
* [IR 7442]+3 - Computer Security Division 2007 Annual Report
* [IR 7536]+3 - Computer Security Division 2008 Annual Report
* [IR 7653]+3 - Computer Security Division 2009 Annual Report
* [IR 7751]+4 - Computer Security Division 2010 Annual Report
* [IR 7816]+3 - Computer Security Division 2011 Annual Report
* [SP 800-165]+1 - Computer Security Division 2012 Annual Report
* [SP 800-170]+1 - Computer Security Division 2013 Annual Report
* [SP 800-176]+1 - Computer Security Division 2014 Annual Report
* [SP 800-182]+1 - Computer Security Division 2015 Annual Report
* [SP 800-195]+1 - NIST-ITL Cybersecurity Program Annual Report
* [SP 800-203]+1 - NIST-ITL Cybersecurity Program Annual Report

+ AUDIT & ACCOUNTABILITY

* [August 2003]+3 - IT Security Metrics
* [August 2005]+9 - Implementation Of FIPS 201, Personal Identity Verification (PIV) Of Federal Employees And Contractors
* [FIPS 140]+246 - Security Requirements for Cryptographic Modules
* [FIPS 191]+1 - Guideline for The Analysis of Local Area Network Security
* [FIPS 198]+7 - The Keyed-Hash Message Authentication Code (HMAC)
* [FIPS 199]+7 - Standards for Security Categorization of Federal Information and Information Systems
* [FIPS 200]+2 - Minimum Security Requirements for Federal Information and Information Systems
* [February 2000]+ - Guideline for Implementing Cryptography in the Federal Government - ITL Bulletin
· * es-idam-sp1800-2a.pdf
· * es-idam-sp1800-2b.pdf
· * NIST SP 1800-2.pdf
· * es-idam-sp1800-2c.pdf
· * es-idam-sp1800-2.pdf
· * es-idam-nist-sp1800-2b-draft.pdf
· * es-idam-nist-sp1800-2a-draft.pdf
· * es-idam-nist-sp1800-2c-draft.pdf
· * es-idam-nist-sp1800-2-draft.pdf
· * es-idam-sp1800-2.zip
· * es-idam-nist-sp1800-2-draft.zip
· * NIST.SP.1800-2.pdf
* [January 2002]+6 - Guidelines on Firewalls and Firewall Policy - ITL Security Bulletin
* [January 2006]+3 - Testing And Validation Of Personal Identity Verification (PIV) Components And Subsystems For Conformance To Federal Information Processing Standard 201
* [January 2007]+4 - Security Controls For Information Systems: Revised Guidelines Issued By NIST - ITL Security Bulletin
* [June 2003]+33 - ASSET: Security Assessment Tool For Federal Agencies
* [March 2004]+12 - Federal Information Processing Standard (FIPS) 199, Standards For Security Categorization Of Federal Information And Information Systems - ITL Bulletin
* [March 2006]+19 - Minimum Security Requirements For Federal Information And Information Systems: Federal Information Processing Standard (FIPS) 200 Approved By The Secretary Of Commerce - ITL Security Bulletin
* [May 2005] - Recommended Security Controls For Federal Information Systems: Guidance For Selecting Cost-Effective Controls Using A Risk-Based Process - ITL Bulletin
* [IR 6981]+2 - Policy Expression and Enforcement for Handheld Devices
* [IR 7275]+13 - Specification for the Extensible Configuration Checklist Description Format (XCCDF)
* [IR 7284]+2 - Personal Identity Verification Card Management Report
* [IR 7316]+3 - Assessment of Access Control Systems
```

1 2 3 4 5 6 7 8 9
Border Gateway Protocol Security - Google Scholar - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:50
Projects | CSRC
NIST Computer Security R
Border Gateway Protocol
scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Border+Gateway+Protocol+Security&btnG=
Guest
Google Scholar
SIGN IN
Articles
My profile
My library

Border Gateway Protocol Security

About 51,600 results (**0.10** sec)

Any time
Since 2022
Since 2021
Since 2018
Custom range...
Sort by relevance
Sort by date
Any type
Review articles
□ include patents
☑ include citations
Create alert

[PDF] **Border gateway protocol security** — [PDF] nist.rip

R Kuhn, K Sriram, D Montgomery - NIST Special Publication, 2007 - csrc.nist.rip

Although not well known among everyday users, the **Border Gateway Protocol** (BGP) is one of the critical infrastructure **protocols** for the Internet. BGP is a routing **protocol**, whose …

☆ Save 99 Cite Cited by 31 Related articles All 11 versions

Enhancing **border gateway protocol security** using public blockchain — [PDF] mdpi.com

L Mastilak, M Galinski, P Helebrandt, I Kotuliak, M Ries - Sensors, 2020 - mdpi.com

… on routing based on **Border Gateway Protocol** (BGP). Routers … , as with many other routing **protocols**. However, this trust … to increase the **security** of BGP routing **protocol**, most based …

☆ Save 99 Cite Cited by 6 Related articles All 10 versions

Securing the **border gateway protocol**: A status update — [PDF] springer.com

ST Kent - … on Communications and Multimedia **Security**, 2003 - Springer

… is exchanged between ASes using the **Border Gateway Protocol** (BGP) [1], … **secure** means of verifying the authorization of BGP control traffic. In April 1997, we began work on the **security** …

☆ Save 99 Cite Cited by 53 Related articles All 16 versions

Secure border gateway protocol (S-BGP) — [PDF] msstate.edu

S Kent, C Lynn, K Seo - IEEE Journal on Selected areas in …, 2000 - ieeexplore.ieee.org

… Routing information is exchanged between ASes in **Border Gateway Protocol** (… **security** architecture described in this paper. In this section we describe the problem—how the **protocol** …

☆ Save 99 Cite Cited by 1025 Related articles All 27 versions

Securing the **border gateway** routing **protocol** — [PDF] dtic.mil

BR Smith… - … of GLOBECOM'96. 1996 …, 1996 - ieeexplore.ieee.org

… intra-domain **protocols** and several sets … **protocols** currently defined are the **Border Gateway Protocol** (BGP) [20] and the Inter-Domain Routing **Protocol** (IDRP) [19,7]; these two **protocols** …

☆ Save 99 Cite Cited by 194 Related articles All 13 versions

A survey of **security** techniques for the **border gateway protocol** (BGP) — [PDF] academia.edu

MO Nicholes, B Mukherjee - IEEE communications surveys & …, 2009 - ieeexplore.ieee.org

… the interface between domains run a **protocol** called **Border Gateway Protocol** (BGP). Figure 1 … a survey of **security** techniques that are useful for the BGP control **protocol** used between …

☆ Save 99 Cite Cited by 52 Related articles All 8 versions

[PDF] Securing the **border gateway protocol** — [PDF] wxcafe.net

ST Kent - The Internet **Protocol** Journal, 2003 - wxcafe.net

… ensure that all of our **protocols** and associated applications provide **security**. In this issue we

https://csrc.nist.rip/library/NIST SP 800-054 Border Gateway Protocol Security, 2007-07-17 (Final).pdf vide **security** for this …

Length-preserving encryption with HCTR2 - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:53
Projects | CSRC
NIST Computer Security R
Border Gateway Protocol
Length-preserving encryp
eprint.iacr.org/2021/1441.pdf
Guest
Length-preserving encryption with HCTR2
29 / 31
100%
nist.rip
1/1
25
26
27
28
29

INDOCRYPT 2007. Ed. by K. Srinathan, C. Pandu Rangan, and Moti Yung. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 252–267. ISBN: 978-3-540-77026-8. DOI: 10.1007/978-3-540-77026-8_19.

[Mon85] Peter L. Montgomery. "Modular Multiplication Without Trial Division". In: *Mathematics of Computation* 44 (1985), pp. 519–521. ISSN: 0025–5718. DOI: https://doi.org/10.1090/S0025-5718-1985-0777282-X. URL: https://www.ams.org/journals/mcom/1985-44-170/S0025-5718-1985-0777282-X/S0025-5718-1985-0777282-X.pdf.

[MV04] David McGrew and John Viega. *The Galois/Counter Mode of Operation (GCM)*. Submission to NIST Modes of Operation Process. 2004. URL: https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf.

[Nan08] Mridul Nandi. *Improving upon HCTR and matching attacks for Hash-Counter-Hash approach*. Cryptology ePrint Archive, Report 2008/090. 2008. URL: https://ia.cr/2008/090.

[Nan21] Mridul Nandi. Private communication. 2021-09.

[Pat09] Jacques Patarin. "The "Coefficients H" Technique". In: *Selected Areas in Cryptography*. Ed. by Roberto Maria Avanzi, Liam Keliher, and Francesco Sica. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 328–345. ISBN: 978-3-642-04159-4. DOI: 10.1007/978-3-642-04159-4_21. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.702.3488.

[Pat91] Jacques Patarin. "Pseudorandom permutations based on the D.E.S. scheme". In: *EUROCODE '90*. Ed. by Gérard Cohen and Pascale Charpin. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, pp. 193–204. ISBN: 978-3-540-47546-0. DOI: 10.1007/3-540-54303-1_131.

[Sar07] Palash Sarkar. "Improving Upon the TET Mode of Operation". In: *Information Security and Cryptology—ICISC 2007: 10th International Conference, Seoul, Korea, November 29–30, 2007. Proceedings*. Ed. by Kil-Hyun Nam and Gwangsoo Rhee. Berlin, Heidelberg:

15. Dutta, A., Nandi, M.: Tweakable HCTR: A BBB Secure Tweakable Enciphering Scheme. In: Chakraborty, D., Iwata, T. (eds.) Progress in Cryptology – INDOCRYPT 2018. pp. 47–69. Springer International Publishing, Cham (2018)

16. Fleischmann, E., Forler, C., Lucks, S.: McOE: A Family of Almost Foolproof On-Line Authenticated Encryption Schemes. In: Canteaut, A. (ed.) Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers. Lecture Notes in Computer Science, vol. 7549, pp. 196–215. Springer (2012). https://doi.org/10.1007/978-3-642-34047-5_12, `https://doi.org/10.1007/978-3-642-34047-5_12`

17. Jean, J., Nikolic, I., Peyrin, T.: Tweaks and Keys for Block Ciphers: The TWEAKEY Framework. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II. Lecture Notes in Computer Science, vol. 8874, pp. 274–288. Springer (2014). https://doi.org/10.1007/978-3-662-45608-8_15, `https://doi.org/10.1007/978-3-662-45608-8_15`

18. Jean, J., Nikolić, I., Peyrin, T., Seurin, Y.: Submission to CAESAR : Deoxys v1.41 (October 2016), `http://competitions.cr.yp.to/round3/deoxysv141.pdf`

19. Lipmaa, H., Rogaway, P., Wagner, D.: Comments to NIST concerning AES modes of operations: CTR-mode encryption. In: National Institute of Standards and Technologies. Citeseer (2000)

20. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. In: Advances in Cryptology-Crypto 2002, Proceedings. vol. 2442, pp. 31–46 (2002)

21. McGrew, D., Viega, J.: The Galois/counter mode of operation (GCM). submission to NIST Modes of Operation Process **20** (2004), `https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-revised-spec.pdf`

22. Patarin, J.: The "Coefficients H" Technique, p. 328–345. Springer-Verlag, Berlin, Heidelberg (2009), `https://doi.org/10.1007/978-3-642-04159-4_21`

23. Peyrin, T., Seurin, Y.: Counter-in-tweak: authenticated encryption modes for tweakable block ciphers. In: Annual International Cryptology Conference. pp. 33–63. Springer (2016)

24. Purnal, A., Andreeva, E., Roy, A., Vizár, D.: What the Fork: Implementation Aspects of a Forkcipher. In: NIST Lightweight Cryptography Workshop 2019 (2019)

25. Rogaway, P.: Authenticated-Encryption with Associated-Data. In: Proceedings of the 9th ACM conference on Computer and communications security. pp. 98–107 (2002)

26. Rogaway, P.: Evaluation of some blockcipher modes of operation. Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan (2011), `https://crossbowerbt.github.io/docs/crypto/rogaway_modes.pdf`

27. Rogaway, P., Bellare, M., Black, J.: OCB: A block-cipher mode of operation for efficient authenticated encryption. ACM Transactions on Information and System Security (TISSEC) **6**(3), 365–403 (2003)

28. Rogaway, P., Krovetz, T.: The Software Performance of Authenticated-Encryption Modes. FSE. LNCS **6733**, 306–327 (Springer (2011))

29. Rogaway, P., Shrimpton, T.: A Provable-Security Treatment of the Key-Wrap Problem. Advances in Cryptology-EUROCRYPT 2006 pp. 373–390 (2006)

30. Vanhoef, M., Piessens, F.: Key reinstallation attacks: Forcing nonce reuse in WPA2. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. pp. 1313–1328. ACM (2017)

31. Whiting, D., Housley, R., Ferguson, N.: Counter with CBC-MAC (CCM). submission to NIST Modes of Operation Process (2003), `https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm.pdf`

Acknowledgements

This work was supported by CyberSecurity Research Flanders with reference number VR20192203. This work was supported in part by the Research Council KU Leuven C1 on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract num-

Draft NIST SP 800-216, Recommendations for Federal Vulnerability Disclosure Guidelines - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:55
Projects | CSRC
NIST Computer Security
Border Gateway Protoc
Length-preserving enc
1154.pdf
Draft NIST SP 800-216,
Paste it §
Sentry ONE 2021 MAY-
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-216-draft.pdf
Guest
Draft NIST SP 800-216, Recommendations for Federal Vulnerability Disclosure Guidelines
35 / 39
100%
nist.rip
1/1
31
32
33
34
35

Geneva, Switzerland). Available at https://www.iso.org/standard/69725.html

[NIST TBF] National Institute of Standards and Technology (2021) *The Bugs Framework (BF)*. Available at https://samate.nist.gov/BF/Home/Approach.html

[NIST VULN] National Institute of Standards and Technology (2021) *Vulnerability Data Ontology*. Available at https://github.com/usnistgov/vulntology

[NISTIR 8138] Booth H, Turner C (2016) Vulnerability Description Ontology. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8138 Draft. Available at https://csrc.nist.rip/publications/drafts/nistir-8138/nistir_8138_draft.pdf

[NISTIR 8246] Byers R, Waltermire D, Turner C (2020) Collaborative Vulnerability Metadata Acceptance Process (CVMAP) for CVE Numbering Authorities (CNAs) and Authorized Data Publishers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8246. https://doi.org/10.6028/NIST.IR.8246

[NVD] National Institute of Standards and Technology (2021) *National Vulnerability Database*. Available at https://nvd.nist.gov/

[OMB M-20-32] Office of Management and Budget (2020) Improving Vulnerability Identification, Management, and Remediation. (The White House, Washington, DC), OMB Memorandum M-20-32, September 2, 2020. Available at https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf

1 2 3 4 5 6 7 8 9
Sentry ONE 2021 MAY- Codename - Sittard - CSPN Security Target - Chromium
mlterm
fr(bepo_afnor) Wed Jul 06, 21:57
Projects | CSRC
NIST Computer Security
Border Gateway Protoc
Length-preserving enc
1154.pdf
Draft NIST SP 800-216,
Paste it §
Sentry ONE 2021 MAY-
https://www.ssi.gouv.fr/uploads/2022/05/anssi-cible-cspn-2022_07en.pdf
Guest
Sentry ONE 2021 MAY- Codename - Sittard - CSPN Security Target
1 / 15
100%
nist.rip
1/1
1
2
3
4

Sentry ONE CSPN Security Target

1. Product identification

Publishing organization	DataLocker Inc.
Link to the organization	www.datalocker.com
Trade name of the product	Sentry ONE
Article (SKU)	SONEXXX
Version number evaluated	Device software 6.3, chipset firmware 3.05
Category of product	Secure storage

2. Description of product

2A.General description

The main use of the secure USB flash drive Sentry ONE is to automatically hardware encrypt and mandatory password protect any stored user data on the USB storage device to allow storage and/or transport.

Concerning the product reference (SONEXXX), XXX denotes storage capacity option.

As a matter of further user assurance the product is certified to FIPS 140-2 level 3, see the Security Policy #2753 for details.[1]

[1] https://csrc.nist.rip/groups/STM/cmvp/documents/140-1/140sp/140sp2753.pdf

nist.rip
New message
Inbox 9999+
Drafts
Sent
Starred 35
MORE
Archive
Spam 9999+
Trash
All mail 9999+
FOLDERS
Add folder
LABELS
Add label
All
Read
Unread
1.77 GB / 18.00 GB
5.0.2.4

[redacted]

[3] csrc.nist.gov link broken

From cso@bluecyren.com
To webmaster-csrc
December 28th, 2021

```
This link is not working:
https://csrc.nist.rip/groups/SMA/fisma/Risk-Management-Framework/select/inde
x.html


Kind Regards,


[redacted], CISSP-ISSEP, CISM, CGEIT
A Computerworld Premier 100 Leader

Cell: 407-575-5781
Web: www.BlueCyren.com
Email:  cso@BlueCyren.com

      <https://www.linkedin.com/in/[redacted]/>

CONFIDENTIALITY NOTICE: The contents of this email message and any
attachments are intended solely for the addressee(s) and may contain
confidential and/or privileged information and may be legally protected from
disclosure. If you are not the intended recipient of this message or their
agent, or if this message has been addressed to you in error, please
immediately alert the sender by reply email and then delete this message and
any attachments. If you are not the intended recipient, you are hereby
notified that any use, dissemination, copying, or storage of this message or
its attachments is strictly prohibited.
```

47.24 KB 1 file attached

nist.rip
New message
Inbox 9999+
Drafts
Sent
Starred 35
MORE
Archive
Spam 9999+
Trash
All mail 9999+
FOLDERS
Add folder
LABELS
Add label
All
Read
Unread
1.77 GB / 18.00 GB
5.0.2.4
Reset
100 %
14:09

[redacted]

[6] AES conference 2 - feedback summary report missing

From [redacted]@inesctec.pt>

To webmaster-csrc

March 16th, 2021

Hello, while trying to access the document the following document: https://csrc.nist.rip/encryption/aes/round1/conf2/feedback-summary.pdf
which is mentioned in the following webpage: https://csrc.nist.rip/encryption/aes/round1/conf2/aes2conf.htm
as: "NIST received feedback from the AES2 attendees, regarding their thoughts on the candidate algorithms."

I'm redirected to a webpage: "Unable to pull this media from the archive, send us your copy here!"

Could you please restore the mentioned document, feedback-summary.pdf, or send me a copy of it?

Thanks.
Best regards,
[redacted]

From [redacted]

To [redacted] webmaster-csrc

March 16th, 2021

Hello,

You're getting this message because we do not have this file archived, unfortunately.

I've looked a bit around, maybe these files may be of interest for you:

1. https://csrc.nist.rip/encryption/aes/round2/comments/AESround2comments-1.zip
2. https://csrc.nist.rip/encryption/aes/round2/comments/AESround2comments-2.zip

There is a primitive index of all the files we have here:

[8] Remove existing DellEMC.com links

nist.rip
New message
Inbox 9999+
Drafts
Sent
Starred 35
MORE
Archive
Spam 9999+
Trash
All mail 9999+
FOLDERS
Add folder
LABELS
Add label
All
Read
Unread
1.77 GB / 18.00 GB
5.0.2.4
100 %
14:10

From DellEMC SEO <dellemcseo@eclerx.com> July 11th, 2019

To webmaster-csrc, [redacted] DellEMC SEO

Hello,

My name is Suraj Torane and I work for eClerx supporting Dell for SEO. I'm in the process of updating DellEMC com links, and came across one on your site. On behalf of Dell I would like to request the removal of the below link from your webpage as we find it irrelevant in regards to our products and services.

The page that include the URL with DellEMC.com is listed below. We request you to please remove them.

1. **Page:** https://csrc.nist.rip/groups/STM/cavp/documents/shs/shaval.html
   Existing URL: http://www.emc.com/
2. **Page:** https://csrc.nist.rip/groups/STM/cavp/documents/dss/dsanewval.html
   Existing URL: http://www.emc.com/
3. **Page:** https://csrc.nist.rip/groups/STM/cavp/documents/dss/rsahistoricalval.html
   Existing URL: http://www.emc.com/

Thank you for your support in advance.

Regards,

[redacted]

eClerx Services Limited [www.eClerx.com]

This email is being sent for and on behalf of eClerx Services Limited (eClerx) or a subsidiary of the firm. eClerx is committed to managing personal data securely and responsibly. Please see our Privacy Notice at https://eclerx.com/privacy-policy/. This email and any attachments are confidential. If you are not the intended recipient, dissemination or copying of this email is prohibited. If you have received this in error, please notify the sender by email and then delete the email completely from your system.

eClerx is a leader in innovative business process management, change management, data-driven insights, and advanced analytics powered by subject matter experts and smart automation. Click Here to Learn more.

nist.rip
New message
Inbox 9999+
Drafts
Sent
Starred 35
MORE
Archive
Spam 9999+
Trash
All mail 9999+
FOLDERS
Add folder
LABELS
Add label
All
Read
Unread
1.77 GB / 18.00 GB
5.0.2.4

[redacted]

[3] FW: Possible to delete https://csrc.nist.rip/groups/ST/QPL/docs/QPL_[redacted].pdf

From [redacted]@nist.gov>

To webmaster-csrc

February 9th, 2021

Hello,

I realized that my email yesterday went to webmaster-csrc@nist.gov and not webmaster-csrc@nist.rip, so I am also sending to "@nist.rip" in hopes that the page can be deleted soon. Please let me know and see the message below if you need a link to [redacted]'s bio for the referring page.

Thanks,

[redacted]

From: [redacted]@nist.gov>
Sent: Monday, February 8, 2021 1:05 PM
To: webmaster-csrc <webmaster-csrc@nist.gov>
Cc: [redacted]. (Fed) <[redacted]@nist.gov>
Subject: Possible to delete https://csrc.nist.rip/groups/ST/QPL/docs/QPL_[redacted]BIO.pdf

Hi,

As the webmaster for my group, I have been asked to see if this page:
https://csrc.nist.rip/groups/ST/QPL/docs/QPL_[redacted]BIO.pdf
can be deleted. The bio is out-of-date and [redacted] has requested that it be removed. If a link to Mr. [redacted]'s bio is required, please use this: https://www.nist.gov/people/[redacted]

Please let me know when this page has been deleted.

Thanks,

[redacted]

Standards Coordination Office
National Institute of Standards and Technology
202-604-8435 (cell)

An official website of the United States government Here's how you know

NIST

Search CSRC

CSRC MENU

CSRC

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

Projects

Publications +

Topics +

News & Updates

Events

Glossary

About CSRC +

POPULAR LINKS

Crypto Module Validation Program & Validated Modules Search

NIST Cybersecurity Framework

NIST Risk Management Framework
SP 800-53 Controls Site

Post-Quantum Cryptography

Publications / Drafts / SP 800s

Stakeholder Engagement / International Resources

NEW: NIST SP 800-53 CONTROLS PUBLIC COMMENT SITE

COMMENT ON DRAFT PUBLICATIONS

NIST'S "CYBERSECURITY INSIGHTS" BLOG

Recent updates:

- NIST updates ***Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*** guidance in NIST SP 800-161r1, which also helps fulfill NIST's responsibilities under E.O. 14028. (May 5, 2022)
- Our new **Cybersecurity and Privacy Reference Tool (CPRT)** offers a consistent format for accessing the reference data of NIST cybersecurity and privacy standards, guidelines, and frameworks. Datasets from nine NIST frameworks and other publications are available and can be searched, browsed, and exported (JSON and XLSX). (May 4, 2022)
- Learn about NIST's resources for:
  - ***Cybersecurity Supply Chain Risk Management***
  - ***DevSecOps***
  - ***Measurements for Information Security***
  - ***Operational Technology (OT) Security***
  - ***Ransomware Protection and Response***
  - ***Secure Software Development Framework (SSDF)***
  - ***Vulnerability Disclosure Guidance***

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- see our greatly-expanded **publications library**,
- explore content by **topic**,
- search our **glossary** of information security terms, and
- subscribe to **CSRC email updates**.

An official website of the United States government Here's how you know

Official websites use .gov
A **.gov** website belongs to an official government organization in the United States.

Secure .gov websites use HTTPS
A **lock** (🔒) or **https://** means you've safely connected to the .gov website. Share sensitive information only on official, secure websites.

NIST
Search CSRC
CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NEW: NIST SP 800-53 CONTROLS PUBLIC COMMENT SITE

COMMENT ON DRAFT PUBLICATIONS

NIST'S "CYBERSECURITY INSIGHTS" BLOG

Recent updates:

- NIST updates ***Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*** guidance in NIST SP 800-161r1, which also helps fulfill NIST's responsibilities under E.O. 14028. (May 5, 2022)
- Our new **Cybersecurity and Privacy Reference Tool (CPRT)** offers a consistent format for accessing the reference data of NIST cybersecurity and privacy standards, guidelines, and frameworks. Datasets from nine NIST frameworks and other publications are available and can be searched, browsed, and exported (JSON and XLSX). (May 4, 2022)
- Learn about NIST's resources for:
  - ***Cybersecurity Supply Chain Risk Management***
  - ***DevSecOps***
  - ***Measurements for Information Security***
  - ***Operational Technology (OT) Security***
  - ***Ransomware Protection and Response***
  - ***Secure Software Development Framework (SSDF)***
  - ***Vulnerability Disclosure Guidance***

POPULAR LINKS

Crypto Module Validation Program
& **Validated Modules Search**

NIST Cybersecurity Framework

NIST Risk Management Framework
SP 800-53 Controls Site

Post-Quantum Cryptography

Publications / **Drafts** / **SP 800s**

Stakeholder Engagement / **International Resources**

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

An unofficial archive of your favorite United States government website Here's how you know
NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
CSRC
This is an archive
(replace .gov by .rip)
Projects
Publications +
Topics +
News & Updates
Events
Glossary
About CSRC +
POPULAR LINKS
Crypto Module Validation Program
& Validated Modules Search
NIST Cybersecurity Framework
NIST Risk Management Framework
SP 800-53 Controls Site
Post-Quantum Cryptography
Publications / Drafts / SP 800s
Stakeholder Engagement /
International Resources
NEW: NIST SP 800-53 CONTROLS PUBLIC COMMENT SITE
COMMENT ON DRAFT PUBLICATIONS
NIST'S "CYBERSECURITY INSIGHTS" BLOG

Recent updates:

- Learn about NIST's resources for:
  - *Cybersecurity Supply Chain Risk Management*
  - *DevSecOps*
  - *Measurements for Information Security*
  - *Operational Technology (OT) Security*
  - *Ransomware Protection and Response*
  - *Secure Software Development Framework (SSDF)*
  - *Vulnerability Disclosure Guidance*

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- see our greatly-expanded **publications library**,
- explore content by **topic**,
- search our **glossary** of information security terms, and
- subscribe to **CSRC email updates**.

An unofficial archive of your favorite United States government website Here's how you know

Official websites do not use .rip
We are an unofficial archive, replace **.rip** by **.gov** in the URL to access the official website. Access our document index here.

Secure websites use HTTPS
A **lock** (🔒) or **https://** means you've safely connected to our website. Please do not share sensitive information with us.

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

This is an archive
(replace .gov by .rip)

NEW: NIST SP 800-53 CONTROLS PUBLIC COMMENT SITE

COMMENT ON DRAFT PUBLICATIONS

NIST'S "CYBERSECURITY INSIGHTS" BLOG

POPULAR LINKS

- Crypto Module Validation Program & Validated Modules Search
- NIST Cybersecurity Framework
- NIST Risk Management Framework SP 800-53 Controls Site
- Post-Quantum Cryptography
- Publications / Drafts / SP 800s
- Stakeholder Engagement / International Resources

Recent updates:

- Learn about NIST's resources for:
  - *Cybersecurity Supply Chain Risk Management*
  - *DevSecOps*
  - *Measurements for Information Security*
  - *Operational Technology (OT) Security*
  - *Ransomware Protection and Response*
  - *Secure Software Development Framework (SSDF)*
  - *Vulnerability Disclosure Guidance*

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related projects, publications, news and events. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- see our greatly-expanded publications library,

fini
it's ~~something~~

An unofficial archive of your favorite United States government website Here's how you know

Official websites do not use .rip
We are an unofficial archive, replace **.rip** by **.gov** in the URL to access the official website. Access our document index **here**.

Secure websites use HTTPS
A **lock** (🔒) or **https://** means you've safely connected to our website. Please do not share sensitive information with us.

NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

CSRC
This is an archive
ace .gov by .rip)

- Projects
- Publications
- Topics
- News & Updates
- Events
- Glossary
- About CSRC

S "CYBERSECURITY INSIGHTS" BLOG

POPULAR LINKS

Crypto Module Validation Program & Validated Modules Search

NIST Cybersecurity Framework

NIST Risk Management Framework SP 800-53 Controls Site

Post-Quantum Cryptography

Publications / Drafts / SP 800s

Stakeholder Engagement / International Resources

- *Measurements for Information Security*
- *Operational Technology (OT) Security*
- *Ransomware Protection and Response*
- *Secure Software Development Framework (SSDF)*
- *Vulnerability Disclosure Guidance*

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- see our greatly-expanded **publications library**,