Communicable Crypto

What can cryptographers prove?
What do people need?
How can we bridge the gap?

RWC2016

Daniel Kahn Gillmor <dkg@aclu.org>
Speech, Privacy, and Technology Project, ACLU
0EE5 BE97 9282 D80B 9F75 40F1 CCD2 ED94 D217 39E9

ACLU Goals

- Freedom of Speech
- Freedom of Association
- Equality and Justice
- Privacy

For everyone!

Our Opposition

- Censorship
- Discrimination
- Surveillance
- Chilled speech

Censorship and Surveillance

- Surveillance of content $\longrightarrow$ censoring topics
- Surveillance of metadata $\longrightarrow$ censoring people

Surveillance alone

- Information is power
- Information differentials are power differentials
  - Prediction
  - Manipulation
  - Control

Chilling effects

Surveillance plus threat = internalized censorship

Communication and growth

- Personal
- Social

For Everyone

- Who is subject to surveillance?
- Who is at risk from threats?
- Does defense alone raise suspicion?

How do we reach the most vulnerable?

- Infrastructure
- Defaults
- Clarity

Clarity is Key

- Misunderstandings are dangerous
- What does your cryptographic tool, protocol, or construct do?
- What does the user understand?

Who is the user of crypto?

- End users
- System Administrators
- Application Developers
- Library Developers
- Protocol Designers

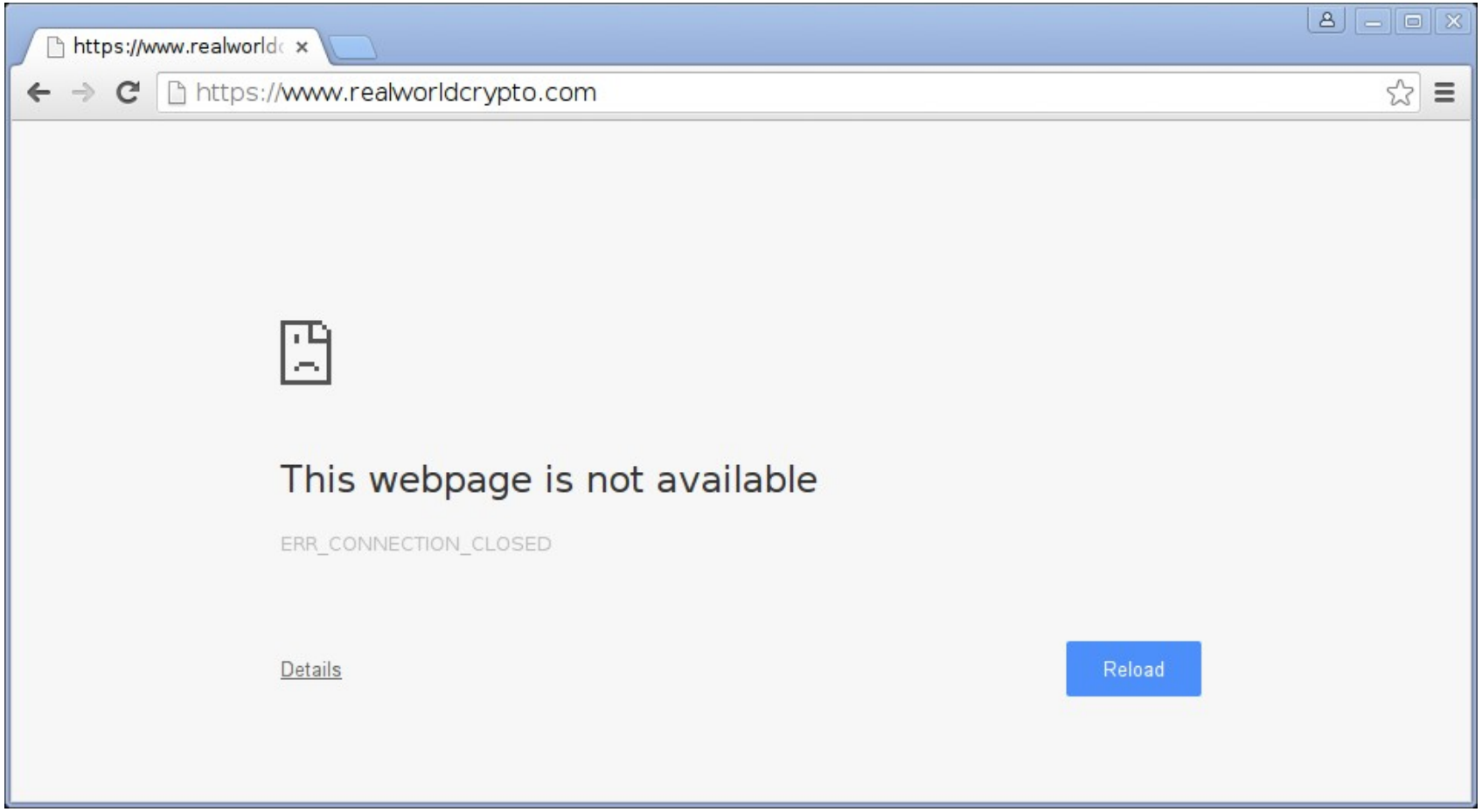
End users

- Clear/simple concepts
- Graphical indicators
- Straightforward workflows
- Defaults

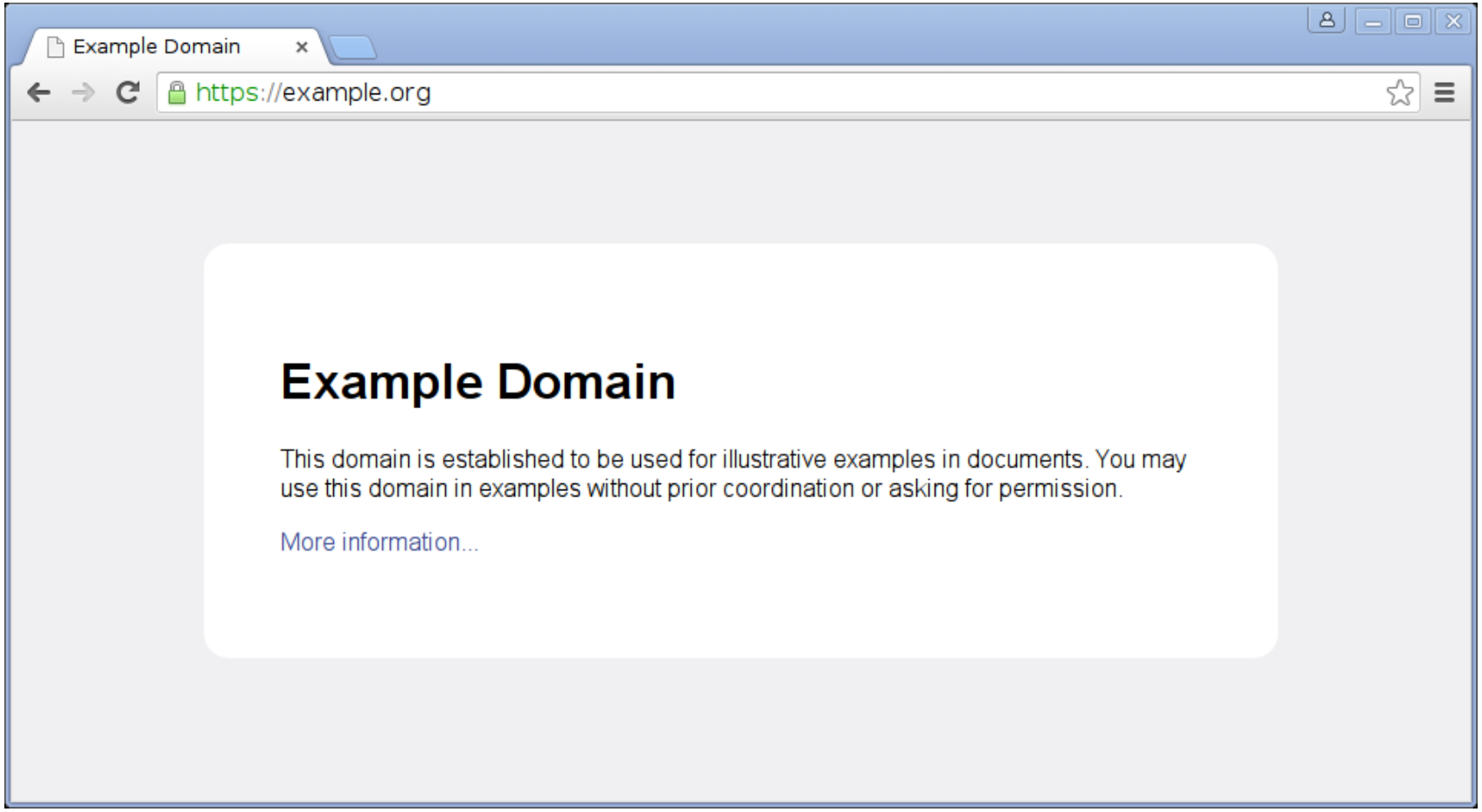
End users


RealWorldCrypto
www.realworldcrypto.com
Real World Cryptography Conference
Upcoming RWC conference:
2016
Past conferences:
2015
2014
2013
2012
The Levchin Prize:
nominations
Social media:
Overview
This annual conference aims to bring together cryptography researchers with developers implementing cryptography in real-world systems. The conference goal is to strengthen the dialogue between these two communities. Topics covered focus on uses of cryptography in real-world environments such as the Internet, the cloud, and embedded devices.
The 2016 edition of the workshop will be held in Stanford, CA on January 6-8, 2016. For further details, visit the workshop website.
The Levchin Prize

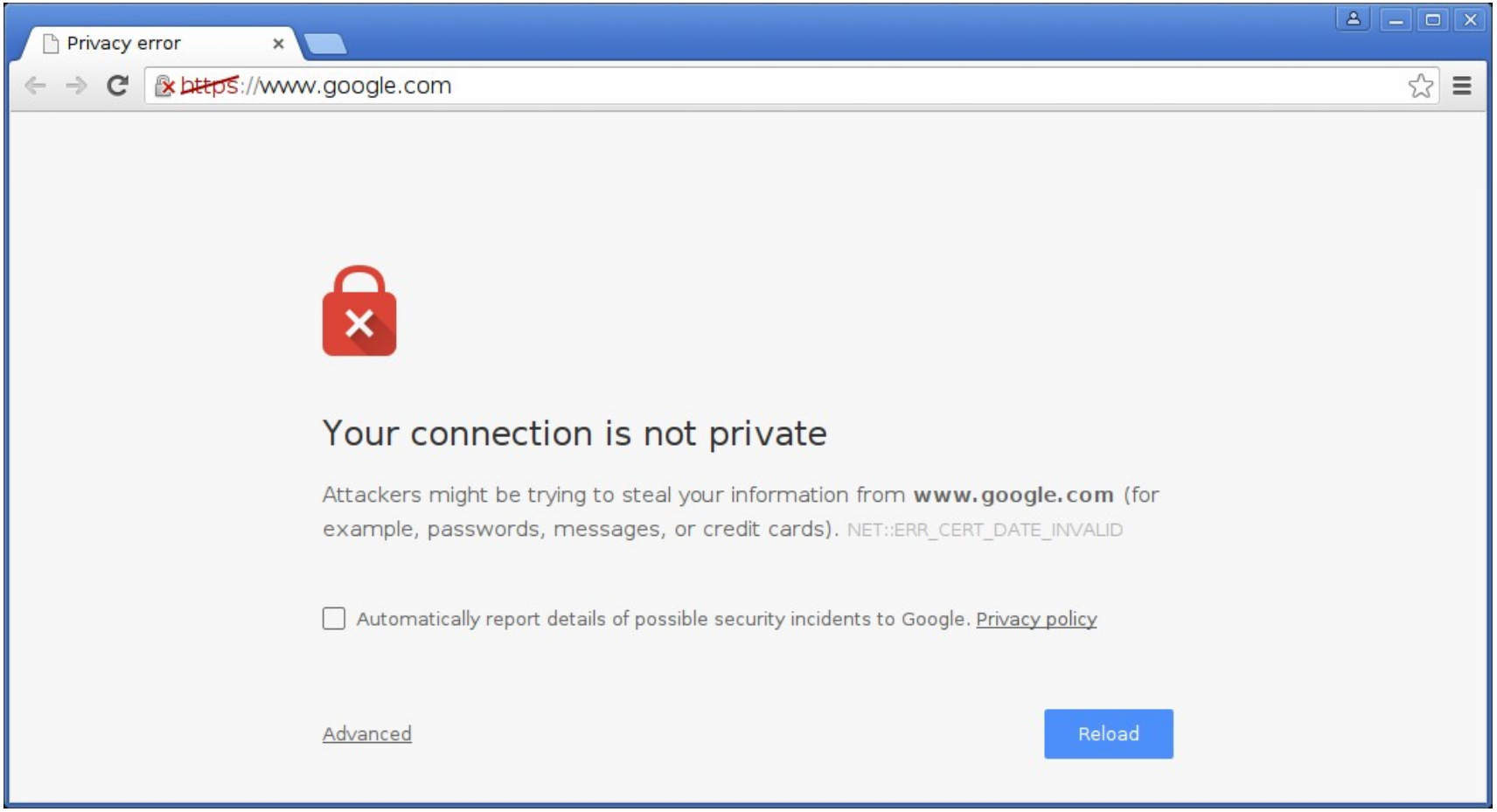
End users


https://www.realworld
https://www.realworldcrypto.com
This webpage is not available
ERR_CONNECTION_CLOSED
Details
Reload

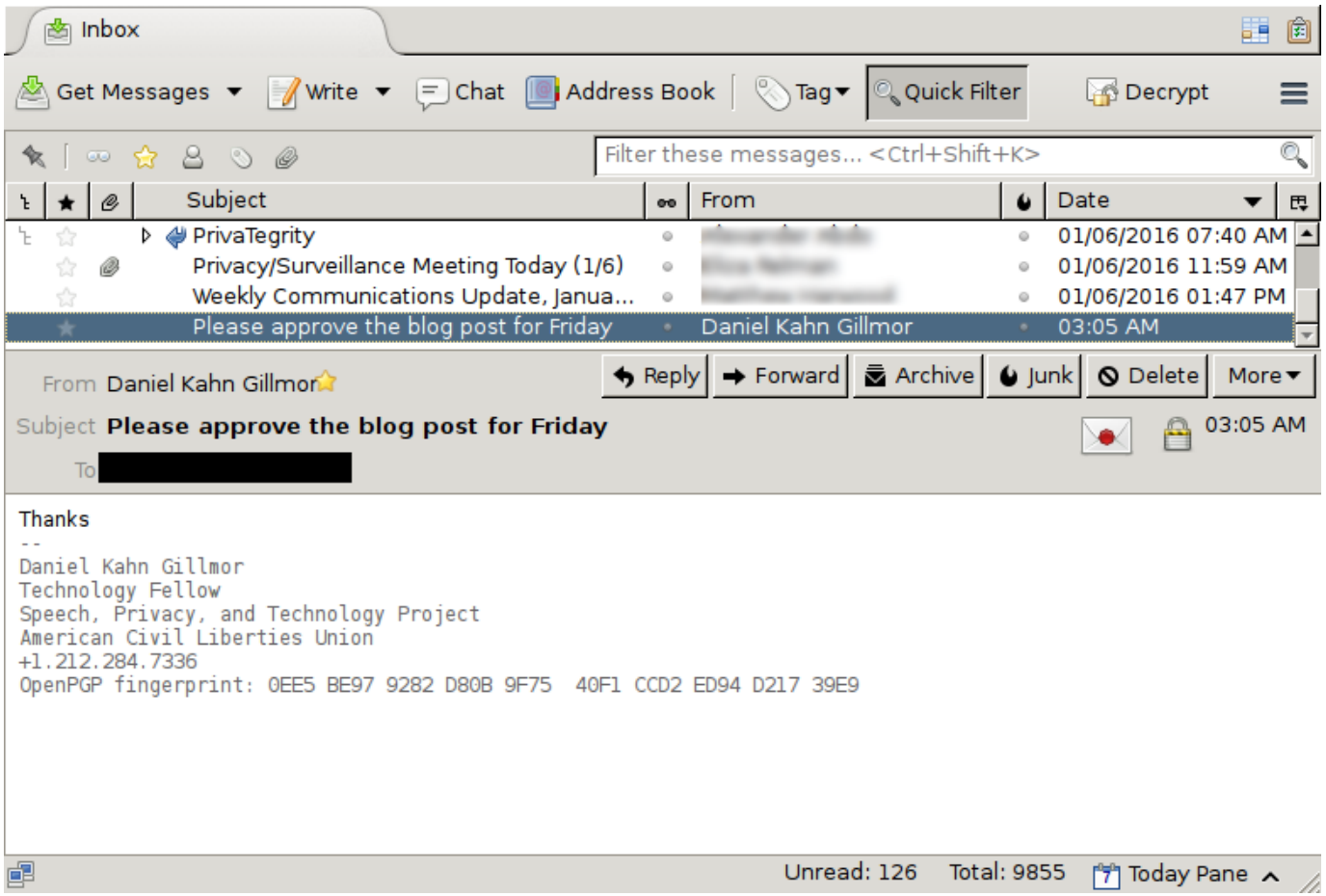
End users


Example Domain
https://example.org
Example Domain
This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission.
More information...

End users


Privacy error
https://www.google.com
Your connection is not private
Attackers might be trying to steal your information from www.google.com (for example, passwords, messages, or credit cards). NET::ERR_CERT_DATE_INVALID
Automatically report details of possible security incidents to Google. Privacy policy
Advanced
Reload

End users


Inbox
Get Messages
Write
Chat
Address Book
Tag
Quick Filter
Decrypt
Filter these messages... <Ctrl+Shift+K>
Subject
From
Date
PrivaTegrity
01/06/2016 07:40 AM
Privacy/Surveillance Meeting Today (1/6)
01/06/2016 11:59 AM
Weekly Communications Update, Janua...
01/06/2016 01:47 PM
Please approve the blog post for Friday
Daniel Kahn Gillmor
03:05 AM
From Daniel Kahn Gillmor
Reply
Forward
Archive
Junk
Delete
More
Subject Please approve the blog post for Friday
03:05 AM
To [redacted]
Thanks
--
Daniel Kahn Gillmor
Technology Fellow
Speech, Privacy, and Technology Project
American Civil Liberties Union
+1.212.284.7336
OpenPGP fingerprint: 0EE5 BE97 9282 D80B 9F75 40F1 CCD2 ED94 D217 39E9
Unread: 126
Total: 9855
Today Pane

System Administrators

- Complexity → failure
- Config files/dialogs
- Making decisions for other people
- Common patterns/tradeoffs
- Logging/alerts
- Defaults

System Administrators

mod_ssl - Apache HTTP Ser...

https://httpd.apache.org/docs/2.4/mod/mod_ssl.html

Search

Modules | Directives | FAQ | Glossary | Sitemap

Apache HTTP Server Version 2.4

Apache > HTTP Server > Documentation > Version 2.4 > Modules

Apache Module mod_ssl

Available Languages: en | fr

Description:	Strong cryptography using the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols
Status:	Extension
Module Identifier:	ssl_module
Source File:	mod_ssl.c

Summary

This module provides SSL v3 and TLS v1.x support for the Apache HTTP Server. SSL v2 is no longer supported.

This module relies on OpenSSL to provide the cryptography engine.

Further details, discussion, and examples are provided in the SSL documentation.

Environment Variables

This module can be configured to provide several items of SSL information as additional environment variables to the SSI and CGI namespace. This information is not provided by default for performance reasons. (See SSLOptions StdEnvVars, below.) The generated variables are listed in the table below. For backward compatibility the information can be made available under different names, too. Look in the Compatibility chapter for details on the compatibility variables.

Variable Name:	Value Type:	Description:
HTTPS	flag	HTTPS is being used.
SSL_PROTOCOL	string	The SSL protocol version (SSLv3, TLSv1, TLSv1.1, TLSv1.2)
SSL_SESSION_ID	string	The hex-encoded SSL session id
SSL_SESSION_RESUMED	string	Initial or Resumed SSL Session. Note: multiple requests may be served over the same (Initial or Resumed) SSL session if HTTP KeepAlive is in use
SSL_SECURE_RENEG	string	true if secure renegotiation is supported, else false
SSL_CIPHER	string	The cipher specification name
SSL_CIPHER_EXPORT	string	true if cipher is an export cipher
SSL_CIPHER_USEKEYSIZE	number	Number of cipher bits (actually used)
SSL_CIPHER_ALGKEYSIZE	number	Number of cipher bits (possible)
SSL_COMPRESS_METHOD	string	SSL compression method negotiated
SSL_VERSION_INTERFACE	string	The mod_ssl program version
SSL_VERSION_LIBRARY	string	The OpenSSL program version
SSL_CLIENT_M_VERSION	string	The version of the client certificate
SSL_CLIENT_M_SERIAL	string	The serial of the client certificate
SSL_CLIENT_S_DN	string	Subject DN in client's certificate
SSL_CLIENT_S_DN_x509	string	Component of client's Subject DN
SSL_CLIENT_SAN_Email_n	string	Client certificate's subjectAltName extension entries of type rfc822Name
SSL_CLIENT_SAN_DNS_n	string	Client certificate's subjectAltName extension entries of type dNSName

Topics
- Environment Variables
- Custom Log Formats
- Request Notes
- Expression Parser Extension
- Authorization providers for use with Require

Directives

SSLCACertificateFile
SSLCACertificatePath
SSLCADNRequestFile
SSLCADNRequestPath
SSLCARevocationCheck
SSLCARevocationFile
SSLCARevocationPath
SSLCertificateChainFile
SSLCertificateFile
SSLCertificateKeyFile
SSLCipherSuite
SSLCompression
SSLCryptoDevice
SSLEngine
SSLFIPS
SSLHonorCipherOrder
SSLInsecureRenegotiation
SSLOCSPDefaultResponder
SSLOCSPEnable
SSLOCSPOverrideResponder
SSLOCSPResponderTimeout
SSLOCSPResponseMaxAge
SSLOCSPResponseTimeSkew
SSLOCSPUseRequestNonce
SSLOpenSSLConfCmd
SSLOptions
SSLPassPhraseDialog
SSLProtocol
SSLProxyCACertificateFile
SSLProxyCACertificatePath
SSLProxyCARevocationCheck
SSLProxyCARevocationFile
SSLProxyCARevocationPath
SSLProxyCheckPeerCN
SSLProxyCheckPeerExpire
SSLProxyCheckPeerName
SSLProxyCipherSuite
SSLProxyEngine
SSLProxyMachineCertificateCh
SSLProxyMachineCertificateFile

System Administrators

mod_ssl - Apache HTTP Ser...

https://httpd.apache.org/docs/2.4/mod/mod_ssl.html

SSL_CLIENT_SAN_Email_n	string	Client certificate's subjectAltName extension entries of type rfc822Name
SSL_CLIENT_SAN_DNS_n	string	Client certificate's subjectAltName extension entries of type dNSName
SSL_CLIENT_SAN_OTHER_msUPN_n	string	Client certificate's subjectAltName extension entries of type otherName, Microsoft User Principal Name form (OID 1.3.6.1.4.1.311.20.2.3)
SSL_CLIENT_I_DN	string	Issuer DN of client's certificate
SSL_CLIENT_I_DN_x509	string	Component of client's Issuer DN
SSL_CLIENT_V_START	string	Validity of client's certificate (start time)
SSL_CLIENT_V_END	string	Validity of client's certificate (end time)
SSL_CLIENT_V_REMAIN	string	Number of days until client's certificate expires
SSL_CLIENT_A_SIG	string	Algorithm used for the signature of client's certificate
SSL_CLIENT_A_KEY	string	Algorithm used for the public key of client's certificate
SSL_CLIENT_CERT	string	PEM-encoded client certificate
SSL_CLIENT_CERT_CHAIN_n	string	PEM-encoded certificates in client certificate chain
SSL_CLIENT_CERT_RFC4523_CEA	string	Serial number and issuer of the certificate. The format matches that of the CertificateExactAssertion in RFC4523
SSL_CLIENT_VERIFY	string	NONE, SUCCESS, GENEROUS or FAILED:reason
SSL_SERVER_M_VERSION	string	The version of the server certificate
SSL_SERVER_M_SERIAL	string	The serial of the server certificate
SSL_SERVER_S_DN	string	Subject DN in server's certificate
SSL_SERVER_SAN_Email_n	string	Server certificate's subjectAltName extension entries of type rfc822Name
SSL_SERVER_SAN_DNS_n	string	Server certificate's subjectAltName extension entries of type dNSName
SSL_SERVER_SAN_OTHER_dnsSRV_n	string	Server certificate's subjectAltName extension entries of type otherName, SRVName form (OID 1.3.6.1.5.5.7.8.7, RFC 4985)
SSL_SERVER_S_DN_x509	string	Component of server's Subject DN
SSL_SERVER_I_DN	string	Issuer DN of server's certificate
SSL_SERVER_I_DN_x509	string	Component of server's Issuer DN
SSL_SERVER_V_START	string	Validity of server's certificate (start time)
SSL_SERVER_V_END	string	Validity of server's certificate (end time)
SSL_SERVER_A_SIG	string	Algorithm used for the signature of server's certificate
SSL_SERVER_A_KEY	string	Algorithm used for the public key of server's certificate
SSL_SERVER_CERT	string	PEM-encoded server certificate
SSL_SRP_USER	string	SRP username
SSL_SRP_USERINFO	string	SRP user info
SSL_TLS_SNI	string	Contents of the SNI TLS extension (if supplied with ClientHello)

x509 specifies a component of an X.509 DN; one of C,ST,L,O,OU,CN,T,I,G,S,D,UID,Email. In Apache 2.1 and later, x509 may also include a numeric _n suffix. If the DN in question contains multiple attributes of the same name, this suffix is used as a zero-based index to select a particular attribute. For example, where the server certificate subject DN included two OU attributes, SSL_SERVER_S_DN_OU_0 and SSL_SERVER_S_DN_OU_1 could be used to reference each. A variable name without a _n suffix is equivalent to that name with a _0 suffix; the first (or only) attribute. When the environment table is populated using the StdEnvVars option of the SSLOptions directive, the first (or only) attribute of any DN is added only under a non-suffixed name; i.e. no _0 suffixed entries are added.

The format of the *_DN variables has changed in Apache HTTPD 2.3.11. See the LegacyDNStringFormat option for SSLOptions for details.

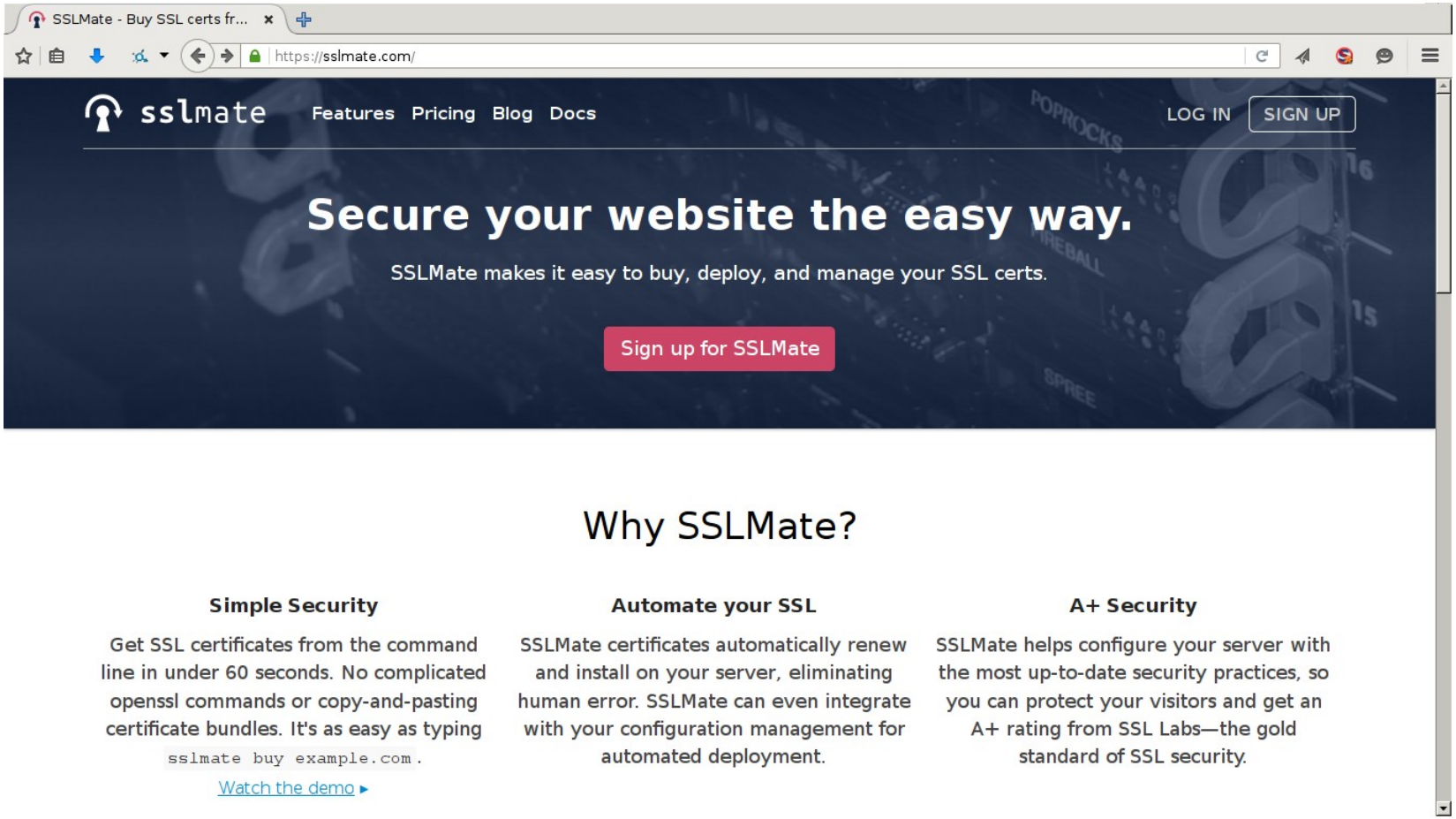
SSL_CLIENT_V_REMAIN is only available in version 2.1 and later.

A number of additional environment variables can also be used in SSLRequire expressions, or in custom log formats:

```
HTTP_USER_AGENT     PATH_INFO      AUTH_TYPE
HTTP_REFERER        QUERY_STRING   SERVER_SOFTWARE
```

SSLProxyMachineCertificateCh
SSLProxyMachineCertificateFil
SSLProxyMachineCertificatePat
SSLProxyProtocol
SSLProxyVerify
SSLProxyVerifyDepth
SSLRandomSeed
SSLRenegBufferSize
SSLRequire
SSLRequireSSL
SSLSessionCache
SSLSessionCacheTimeout
SSLSessionTicketKeyFile
SSLSessionTickets
SSLSRPUnknownUserSeed
SSLSRPVerifierFile
SSLStaplingCache
SSLStaplingErrorCacheTimeout
SSLStaplingFakeTryLater
SSLStaplingForceURL
SSLStaplingResponderTimeout
SSLStaplingResponseMaxAge
SSLStaplingResponseTimeSkew
SSLStaplingReturnResponderEr
SSLStaplingStandardCacheTime
SSLStrictSNIVHostCheck
SSLUserName
SSLUseStapling
SSLVerifyClient
SSLVerifyDepth
- Comments

System Administrators



System Administrators

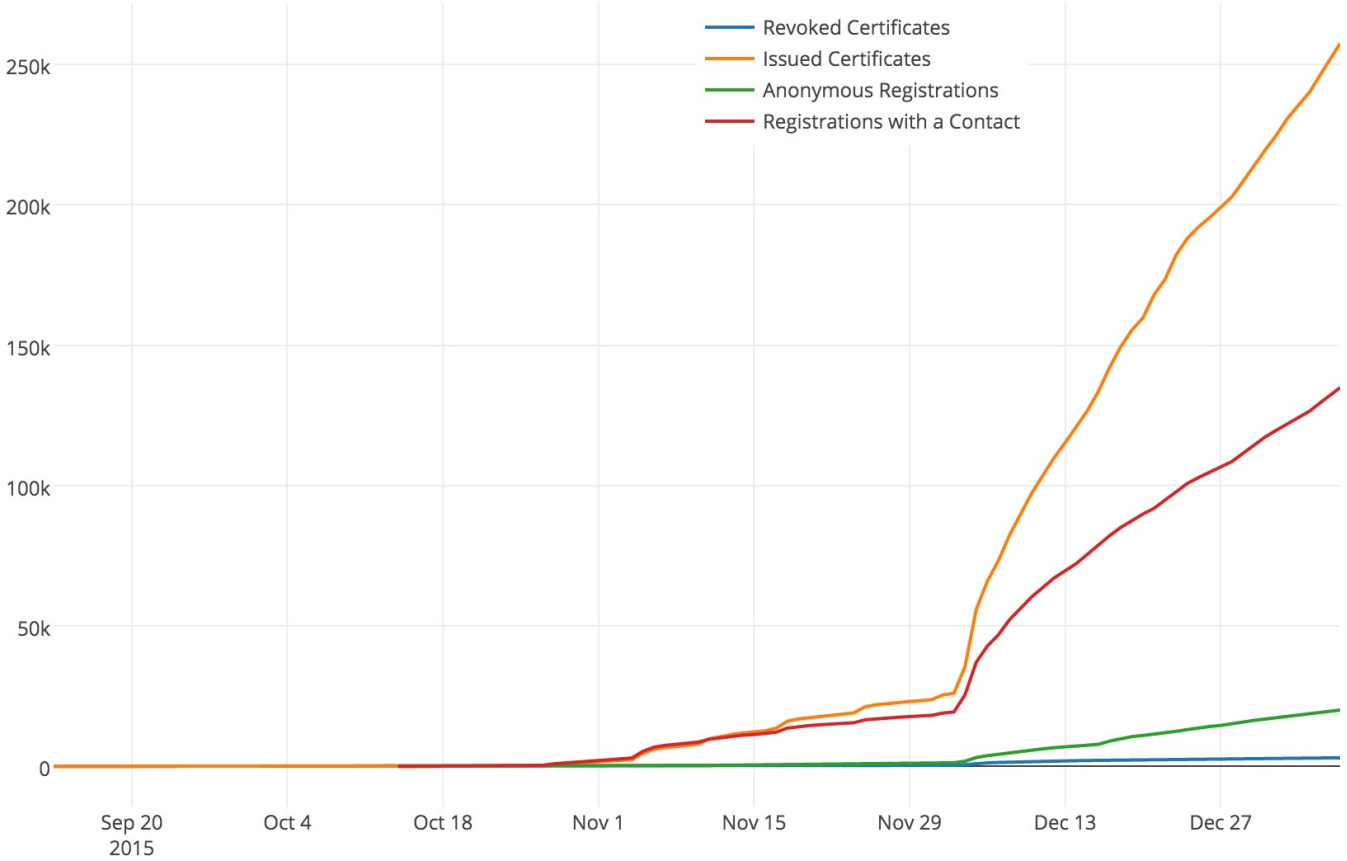
Let's Encrypt

System Administrators

Let's Encrypt

```
caddy@mattman:~$ nano Cad_
```

System Administrators



Application Developers

- Complexity is expensive
- Library API
- Error handling
- Maintenance and Lifecycle
- Make failure findable
- Defaults

Application Developers

CVE - Search Results

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=certificate

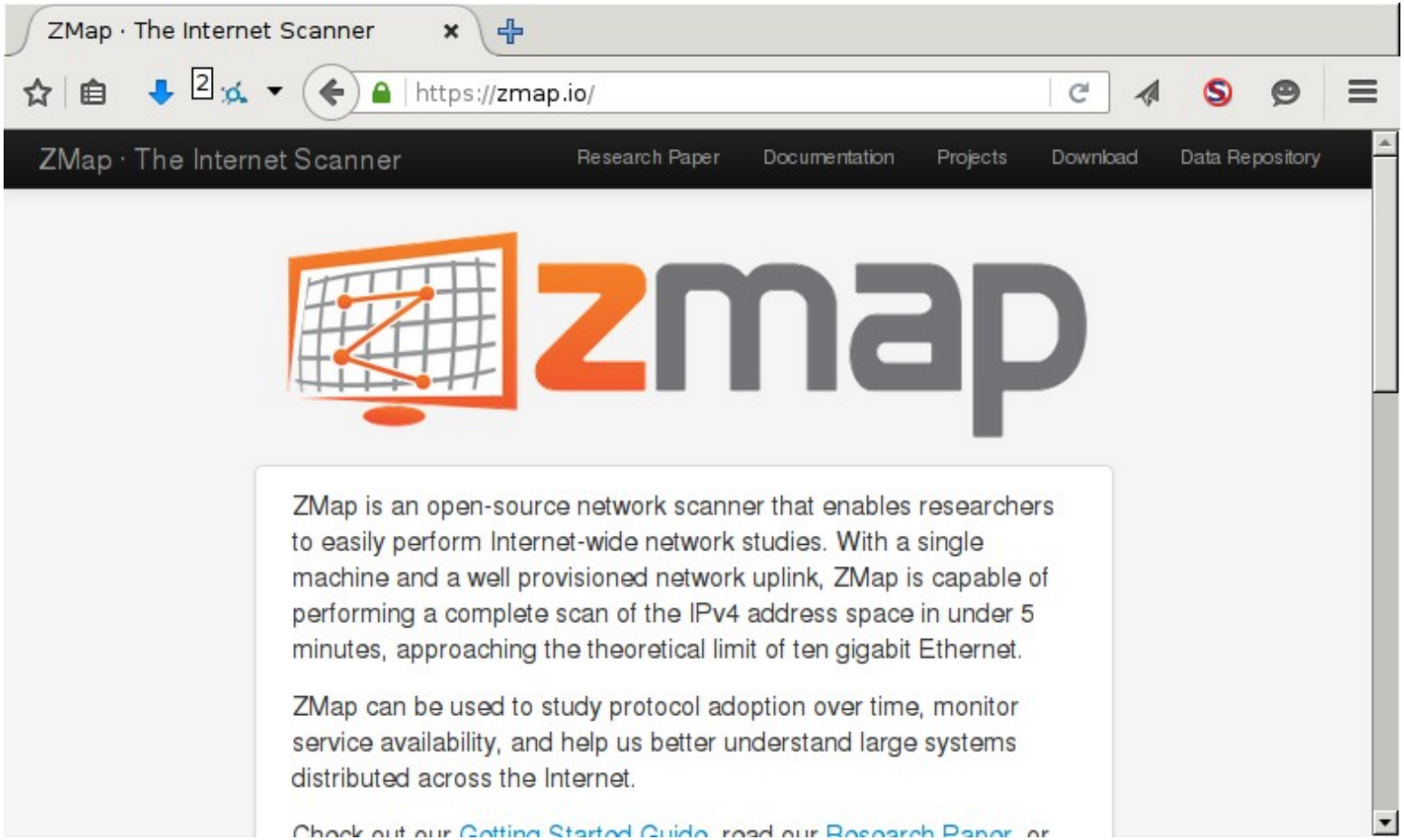
Terminology
Documents
FAQs
CVE List
CVE-ID Syntax Change
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID
CVE In Use
CVE-Compatible Products
NVD for CVE Fix Information
CVSS for Scoring CVE-IDs
CVE Numbering Authorities (CNAs)
News & Events
Calendar
Free Newsletter
Community
CVE Editorial Board
Sponsor
Contact Us
Search the Site
Site Map

There are **2048** CVE entries that match your search.

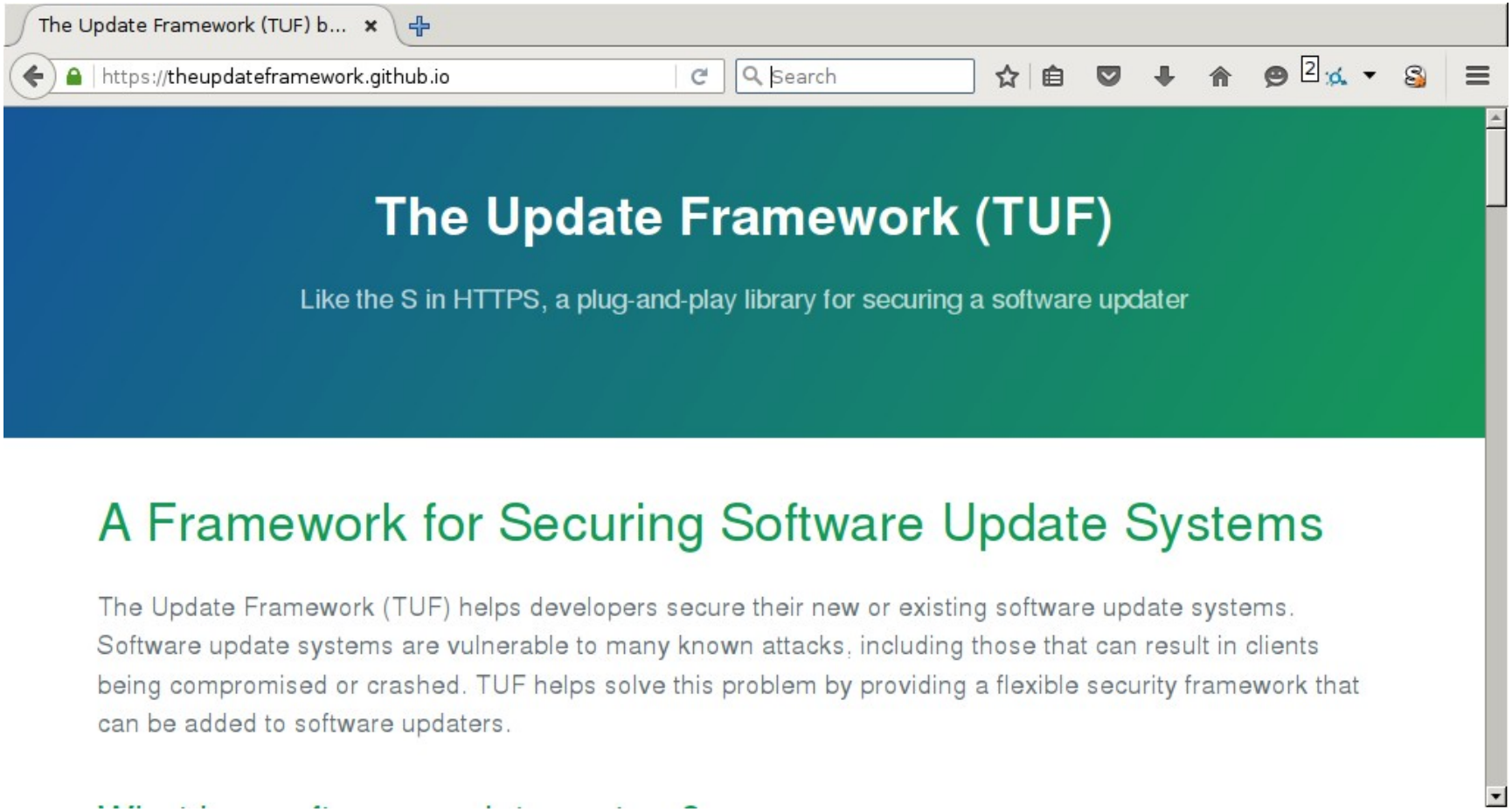
Name	Description
CVE-2015-7298	ownCloud Desktop Client before 2.0.1, when compiled with a Qt release after 5.3.x, does not call QNetworkReply::ignoreSslErrors with the list of errors to be ignored, which makes it easier for remote attackers to conduct man-in-the-middle (MITM) attacks by leveraging a server using a self-signed certificate. NOTE: this vulnerability exists because of a partial CVE-2015-4456 regression.
CVE-2015-7061	The ASN.1 decoder in Apple OS X before 10.11.2, tvOS before 9.1, and watchOS before 2.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted certificate, a different vulnerability than CVE-2015-7059 and CVE-2015-7060.
CVE-2015-7060	The ASN.1 decoder in Apple OS X before 10.11.2, tvOS before 9.1, and watchOS before 2.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted certificate, a different vulnerability than CVE-2015-7059 and CVE-2015-7061.
CVE-2015-7059	The ASN.1 decoder in Apple OS X before 10.11.2, tvOS before 9.1, and watchOS before 2.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted certificate, a different vulnerability than CVE-2015-7060 and CVE-2015-7061.
CVE-2015-6999	The OCSP client in Apple iOS before 9.1 does not check for certificate expiry, which allows remote attackers to spoof a valid certificate by leveraging access to a revoked certificate.
CVE-2015-6997	The X.509 certificate-trust implementation in Apple iOS before 9.1 does not recognize that the kSecRevocationRequirePositiveResponse flag implies a revocation-checking requirement, which makes it easier for man-in-the-middle attackers to spoof endpoints by leveraging access to a revoked certificate.
CVE-2015-6932	VMware vCenter Server 5.5 before u3 and 6.0 before u1 does not verify X.509 certificates from TLS LDAP servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2015-6357	The rule-update feature in Cisco FireSIGHT Management Center (MC) 5.2 through 5.4.0.1 does not verify the X.509 certificate of the support.sourcefire.com SSL server, which allows man-in-the-middle attackers to spoof this server and provide an invalid package, and consequently execute arbitrary code, via a crafted certificate, aka Bug ID CSCuw06444.
CVE-2015-6303	The Cisco Spark application 2015-07-04 for mobile operating systems does not properly verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate, aka Bug IDs CSCut36742 and CSCut36844.
CVE-2015-6298	The admin web interface in Cisco AsyncOS 8.x before 8.0.8-113, 8.1.x and 8.5.x before 8.5.3-051, 8.6.x and 8.7.x before 8.7.0-171-LD, and 8.8.x before 8.8.0-085 on Web Security Appliance (WSA) devices allows remote authenticated users to obtain root privileges via crafted certificate-generation arguments, aka Bug ID CSCus83445.
CVE-2015-6276	Cisco TelePresence IX5000 8.0.3 stores a private key associated with an X.509 certificate under the web root with insufficient access control, which allows remote attackers to obtain cleartext versions of HTTPS traffic or spoof devices via a direct request to the certificate directory, aka Bug ID CSCuu63501.
CVE-2015-6251	Double free vulnerability in GnuTLS before 3.3.17 and 3.4.x before 3.4.4 allows remote attackers to cause a denial of service via a long DistinguishedName (DN) entry in a certificate

Search Master Copy of CVE
Download CVE
View CVE
CVE-ID Syntax Change
CVE-ID Syntax Compliance
CVE-ID Syntax Guidance
CVE-ID Syntax Test Data
About CVE Identifiers
Data Sources/Product Coverage
Editorial Policies
CVE Editor's Commentary
Reference Key/Maps
Search Tips
Updates & RSS Feeds
Request a CVE Identifier
ITEMS OF INTEREST
Terminology
Common Vulnerability Scoring System (CVSS)
Common Vulnerability Reporting Framework (CVRF)
National Vulnerability Database (NVD)

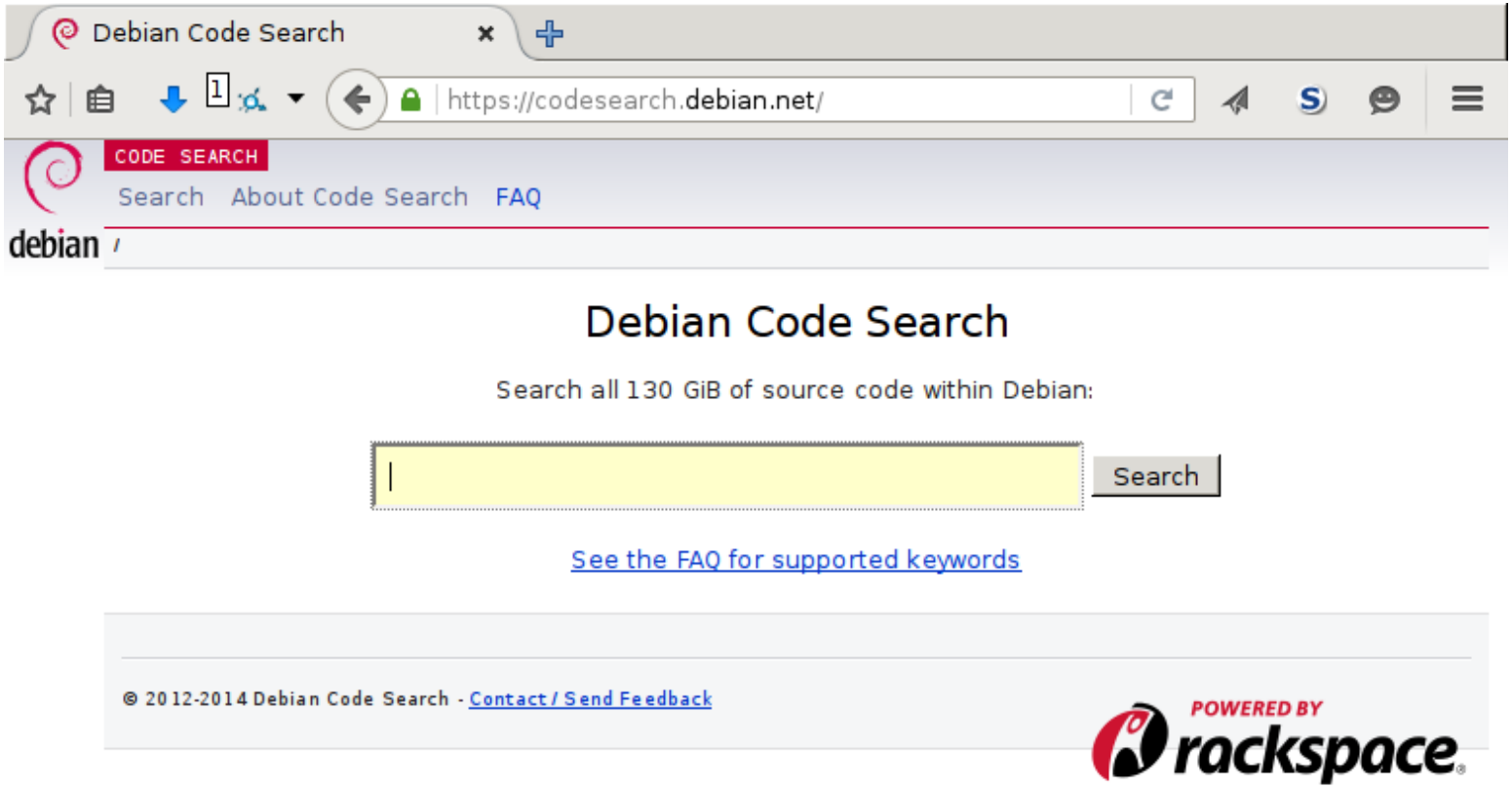
Application Developers



Application Developers



Application Developers



Library Developers

- What features should they expose?
- API lifecycle management
- Test vectors
- Formal verification
- Defaults

Library Developers

0-RTT TLS:

```
TLS_connect(ctx, params);

TLS_send(ctx, sz, data);

-----------

TLS_connect_with_replayable_data

     (ctx, params, sz, data);

TLS_send_replayable(ctx, sz, data);
```

Library Developers

miTLS - A verified reference im...

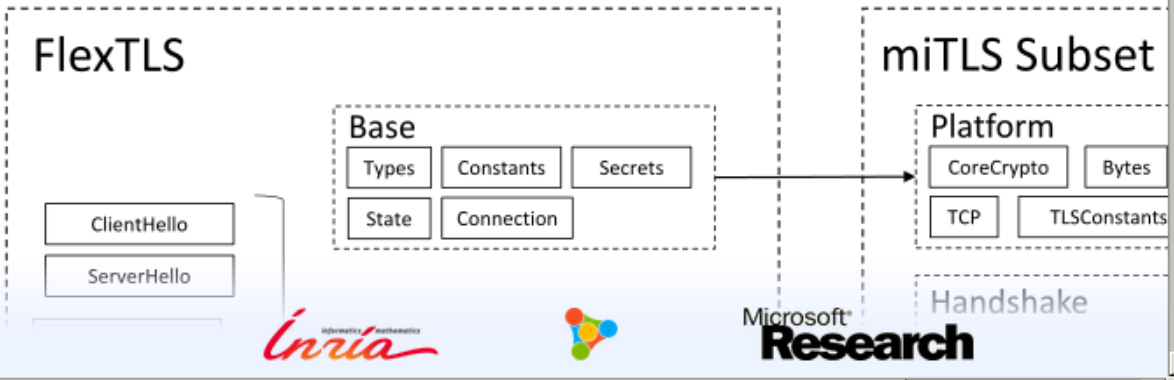
http://www.mitls.org/pages/flextls

miTLS | Publications | Attacks | Code | FlexTLS

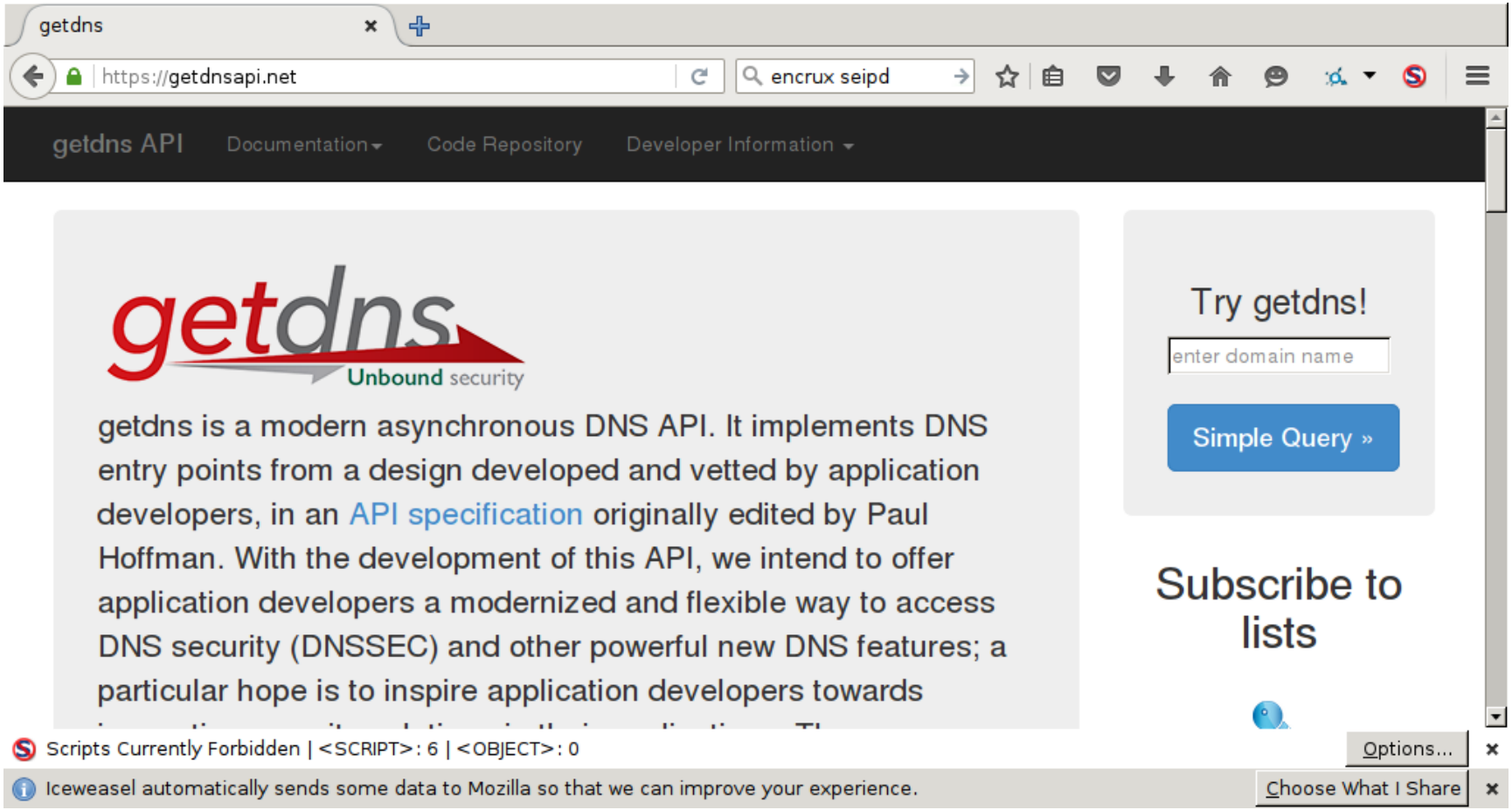
FlexTLS: A Tool for Testing TLS Implementations

FlexTLS is a tool for rapidly prototyping and testing implementations of the Transport Layer Security (TLS) protocol. FlexTLS is built implementation of TLS, and hence protocol scenarios written in FlexTLS can benefit from robust libraries for messaging and cryptogr scripts in FlexTLS can be used to evaluate and communicate the impact of new protocol vulnerabilities.

FlexTLS was used to discover recent attacks on TLS implementations, such as **SKIP and FREAK**, as well as to program the first pro FREAK and **Logjam**. It is also being used to experiment with proposed designs of the upcoming version 1.3 of TLS. Our goal is to cre where protocol analysts and practitioners can easily test TLS implementations and share protocol designs, attacks or proofs. Her modular architecture of FlexTLS:



Library Developers



Protocol Designers

- How do primitives fit together?
- What properties do they provide?
- Sidechannels
- Deployment/interop/upgrade/deprecation
- Defaults

Protocol Designers

- TLS mac-then-encrypt
  - Replace with AEAD
- OpenPGP SEIPD degradation
  - Deprecate SED (+ design chunkable encryption mechanism)
- DNS privacy

Protocol Designers

IRTF Crypto Forum Research Gr...

https://irtf.org/cfrg

encrux seipd

IRTF Research Groups People Other

Crypto Forum Research Group CFRG

Charter

The Crypto Forum Research Group (CFRG) is a general forum for discussing and reviewing uses of cryptographic mechanisms, both for network security in general and for the IETF in particular.

The CFRG serves as a bridge between theory and practice, bringing new cryptographic techniques to the Internet community and promoting an understanding of the use and applicability of these mechanisms via Informational RFCs (in the tradition of, e.g., RFC 1321 (MD5) and RFC 2104 (HMAC). Our goal is to provide a forum for discussing and analyzing general cryptographic aspects of security protocols, and to offer guidance on the

CHAIRS

The CFRG is chaired by Kenny Paterson (kenny.paterson@rhul.ac.uk) and Alexey Melnikov (alexey.melnikov@isode.com).

MAILING LIST

Cryptographers are not...

- UI/UX people
- Configuration specialists
- Application developers
- API wizards
- Protocol designers

Most Cryptographers are not yet...

- UI/UX people
- Configuration specialists
- Software engineers
- API developers
- Protocol designers

Collaboration

- Practice explaining what guarantees your constructs can offer
- Listen to user needs
- Sometimes the best solution doesn't involve new crypto
- Without crypto, we lose on surveillance, censorship, discrimination, and privacy