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
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 → censoring topics
- Surveillance of metadata → 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

Real World Cryptography Conference

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
End users

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

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
System Administrators

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

![Image of mod_ssl - Apache HTTP Server](https://httpd.apache.org/docs/2.4/mod/mod_ssl.html)

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL_CLIENT_S_DN</td>
<td>Client certificate's subject DN extension string</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN</td>
<td>Issuer DN of client's certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_6509</td>
<td>Component of issuer DN</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_FMT</td>
<td>Algorithm used for the signature of client certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_FMT_6509</td>
<td>Algorithm used for the signature of client certificate (with time)</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP</td>
<td>Regular expression with client chain certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_6509</td>
<td>Validity of client certificate (with time)</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Number of days until client certificate expires</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP</td>
<td>Algorithm used for the signature of client certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Algorithm used for the public key of client certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP</td>
<td>Fingerprinted client certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Fingerprinted client certificate in client certificate chain</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Serial number and issuer of the certificate. The format matches that of the CertificateRequestName in RFC4512</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP</td>
<td>MORE, PREVIOUS, LOCAL, or TRUSTED review</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP</td>
<td>Version of the server certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP</td>
<td>Serial of the server certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Subject DN in server certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Server certificate's subjectDNName extension entry of type 4512Name</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Server certificate's subjectDNName extension entries of type 4512Name</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Server certificate's subjectDNName extension entries of type 4512Name, SRPName from (OID 1.3.6.1.5.5.7.87, SRP 4060)</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Component of server's Subject DN</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Issuer DN of server's certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Component of issuer's DN</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Validity of server certificate (with time)</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Algorithm used for the signature of server's certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Algorithm used for the public key of server's certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Fingerprinted server certificate</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>DH or RSA signature key</td>
</tr>
<tr>
<td>SSL_CLIENT_I_DN_REGEXP_6509</td>
<td>Contents of the SHA1 extension (if supplied with ClientHello)</td>
</tr>
</tbody>
</table>

**SSL** specifies a component of an X.509 DN, one of 1.2.5.21.1,1.3.6.1.5.5.7.87,1.3.6.1.5.5.7.88,2.17 or 1.3.6.1.5.5.7.88.2.17. In Apache 2.1 and later, **SSL** may also include a numeric _a_ suffix. If the DN in question contains multiple attributes of the same name, the suffix is used as a sub-named entry to select a particular attribute. For example, when the server certificate subject DN included two OU attributes, the `SSL_CLIENT_I_DN_REGEXP_6509` and `SSL_CLIENT_I_DN_REGEXP_6509` could be used to reference them. Available names without a _a_ suffix are equivalent to that name with a _a_ suffix (the first one is used). Attributes. When the environment variable is populated using the `SSL*ECERT` option of the `SSL*`_ecert_ option, the first or only attribute of any 2ND is added only under a non-suffixed name (i.e., no _a_ suffixed entries are added). The format of the _a_ value is new in Apache 2.3.11. See the `SSL*ECERT`_value_ of `SSL*ECERT`_option_ for details. `SSL_CLIENT_I_DN_REGEXP` is only available in version 2.1 and later. A number of additional environment variables can also be used in SSL/proxy expressions, or in custom key formats.

![Image of ACLU logo](https://www.american civliberties union.org)

**Communicable Crypto**
System Administrators

Why SSLMate?

**Simple Security**
Get SSL certificates from the command line in under 60 seconds. No complicated openssl commands or copy-and-pasting certificate bundles. It's as easy as typing `sslmate buy example.com`.

**Automate your SSL**
SSLMate certificates automatically renew and install on your server, eliminating human error. SSLMate can even integrate with your configuration management for automated deployment.

**A+ Security**
SSLMate helps configure your server with the most up-to-date security practices, so you can protect your visitors and get an A+ rating from SSL Labs—the gold standard of SSL security.
System Administrators

Let’s Encrypt
System Administrators

Let’s Encrypt

caddy@mattman:~$ nano Cad_

Communicable Crypto 23
System Administrators

Let’s Encrypt

Communicable Crypto
Application Developers

- Complexity is expensive
- Library API
- Error handling
- Maintenance and Lifecycle
- Make failure findable
- Defaults
Communicable Crypto
Application Developers

ZMap is an open-source network scanner that enables researchers to easily perform Internet-wide network studies. With a single machine and a well provisioned network uplink, ZMap is capable of performing a complete scan of the IPv4 address space in under 5 minutes, approaching the theoretical limit of ten gigabit Ethernet.

ZMap can be used to study protocol adoption over time, monitor service availability, and help us better understand large systems distributed across the Internet.

Check out our Getting Started Guide, read our Research Paper, or
Application Developers

The Update Framework (TUF)
Like the S in HTTPS, a plug and play library for securing a software updater

A Framework for Securing Software Update Systems

The Update Framework (TUF) helps developers secure their new or existing software update systems. Software update systems are vulnerable to many known attacks, including those that can result in clients being compromised or crashed. TUF helps solve this problem by providing a flexible security framework that can be added to software updaters.
Application Developers

Debian Code Search

Search all 130 GiB of source code within Debian:

[Search Box]

See the FAQ for supported keywords

© 2012-2014 Debian Code Search - Contact / Send Feedback

POWERED BY Rackspace

Communicable Crypto
Library Developers

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

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 on top of miTLS, and hence protocol scenarios written in FlexTLS can benefit from robust libraries for messaging and cryptography. FlexTLS can be used to evaluate and communicate the impact of new protocol vulnerabilities.

FlexTLS was used to identify recent attacks on TLS implementations, such as SKIPL and FREAK, as well as to program the first proof-of-concept for Logjam. It is also being used to experiment with proposed designs of the upcoming version 1.3 of TLS. Our goal is to create a modular architecture of FlexTLS where protocol analysts and practitioners can easily test TLS implementations and share protocol designs, attacks or proofs.
Library Developers

getdns is a modern asynchronous DNS API. It implements DNS entry points from a design developed and vetted by application developers, in an API specification originally edited by Paul Hoffman. With the development of this API, we intend to offer application developers a modernized and flexible way to access DNS security (DNSSEC) and other powerful new DNS features; a particular hope is to inspire application developers towards implementing them in their applications.
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

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 (aleksey.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