

# Automating TLS Configuration Verification

On the Back-End of the Web Application Stack



# Who Am I?

- Steven Danneman
  - @sdanndev
  - sdanneman [at] securityinnovation.com
- Security Engineer
- Security Innovation
- Seattle, WA
- Storage protocols
  - SMB, Samba Team
- Server-side



# Outline

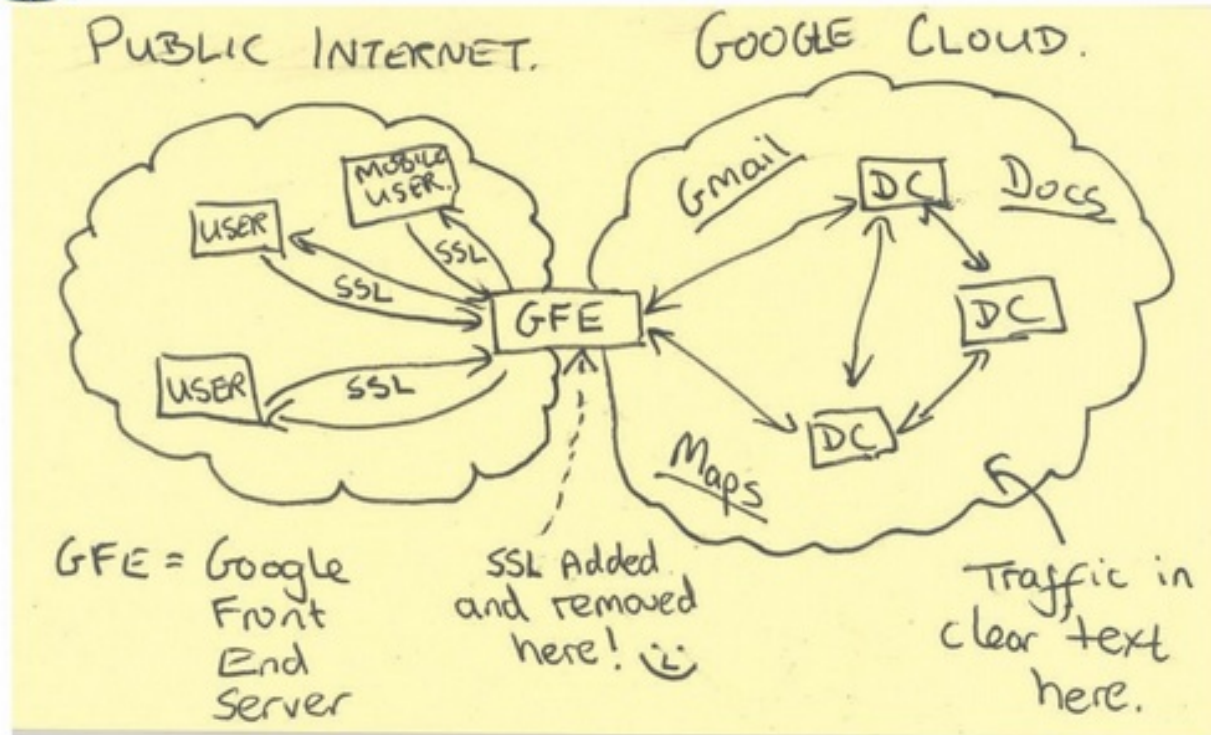
1. Motivation
2. Scope
3. Tool
4. Data
5. Conclusions

# MOTIVATION

# The Network Is Hostile



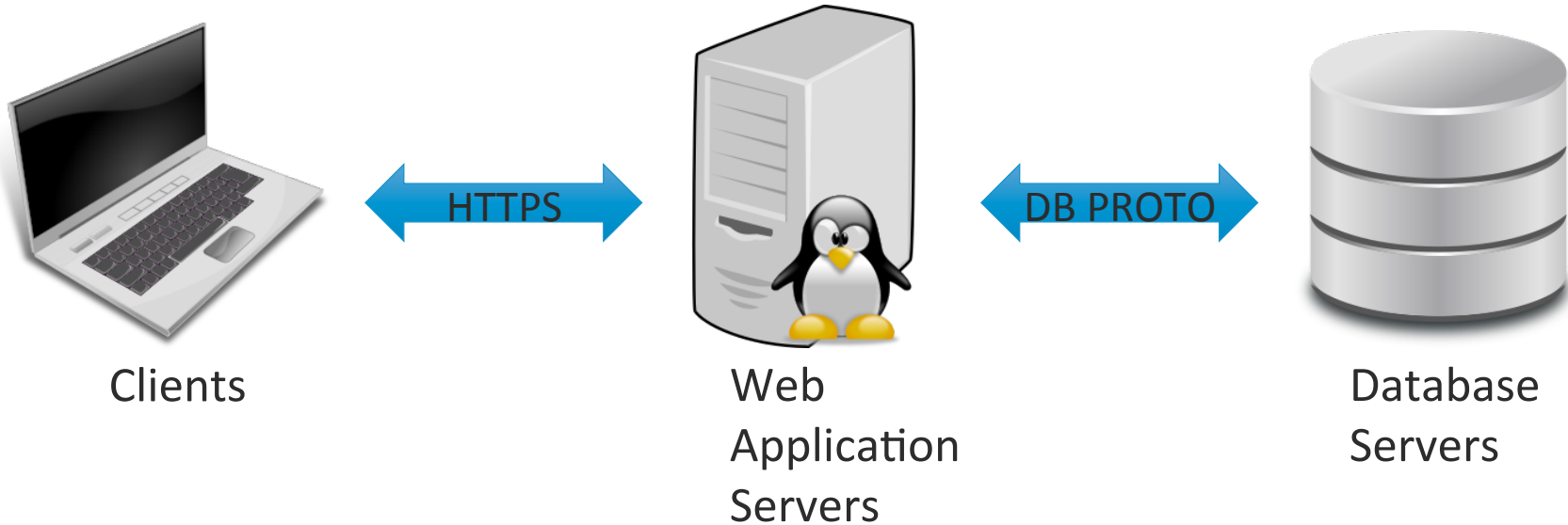
# Current Efforts - Google



TOP SECRET//SI//NOFORN

# Customer Data Is The Target

# The Simple Web Application







If You Cant  
Measure It You  
Can't Improve It.

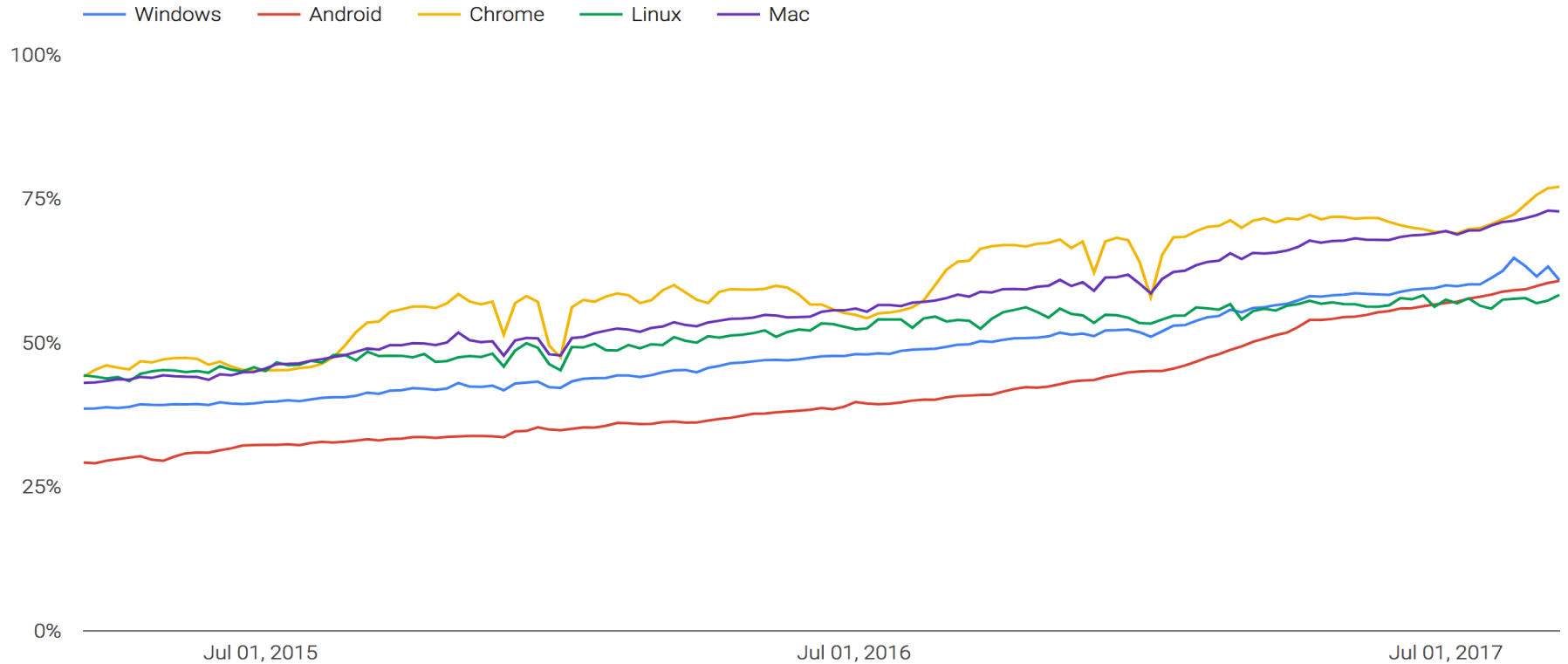
Lord Kelvin

# Proper (current) TLS Configuration

1. TLS is Enabled
2. Protocols
  - TLSv1.2
3. Cipher Strength
  - Perfect Forward Secrecy
  - $\geq$  AES 128
  - GCM
4. Certificate Chain
  - Signed by a known CA
5. Known Vulnerabilities
  - Has none

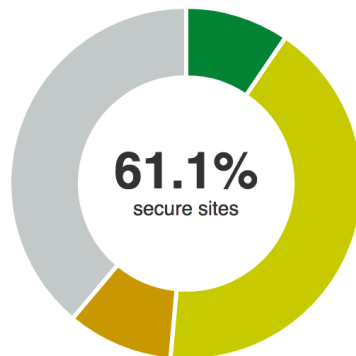
# The HTTPS Success Story

Percentage of pages loaded over HTTPS in Chrome by platform



## SSL Pulse

### SSL Security Summary

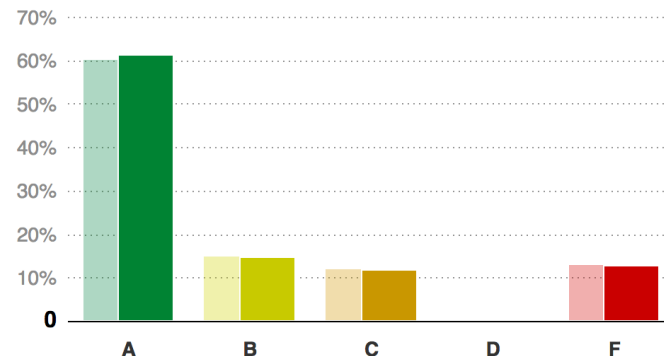


Total sites surveyed  
**139,011**  
+ 0.2 %

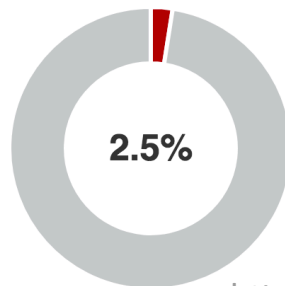
Inadequate security  
**54,039**  
- 0.9 %

Secure sites  
■ A+ ■ A ■ A-  
**84,972**  
+ 0.9 %

### SSL Labs Grade Distribution

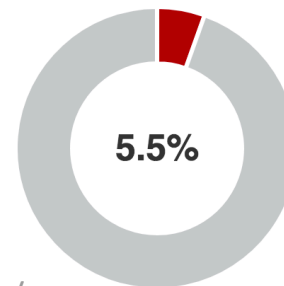


### Certificate Chain



Sites with incomplete  
certificate chain  
**3,446**  
+ 0.0 %

### Cipher Strength



Sites that support weak  
or insecure cipher suites  
**7,577**  
- 0.1 %



O-Saft

nabla-c0d3 / **sslyze**

SSL/TLS Server Test

rbsec / **ssllscan**

**COMODO SSL Analyzer**

**SSL Checker**

testssl.sh

SSL Web Server Test

**TestSSLServer**

**SSL Decoder**

DigiCert® SSL Installation Diagnostics Tool



**Symantec** CryptoReport

# Mozilla SSL Configuration Generator

- ☒ Apache
  - ☐ Nginx
  - ☐ Lighttpd
  - ☐ HAProxy
  - ☐ AWS ELB
- ☐ Modern
  - ☒ Intermediate
  - ☐ Old

Server Version

OpenSSL Version

HSTS Enabled ☒

apache 2.2.15 | intermediate profile | OpenSSL 1.0.1e | [link](#)

Oldest compatible clients: Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3, Java 7

```
<VirtualHost *:443>
...
SSLEngine on
SSLCertificateFile      /path/to/signed_certificate
SSLCertificateChainFile /path/to/intermediate_certificate
SSLCertificateKeyFile   /path/to/private/key

# Uncomment the following directive when using client certificate authentication
#SSLCACertificateFile   /path/to/ca_certs_for_client_authentication

# HSTS (mod_headers is required) (15768000 seconds = 6 months)
Header always set Strict-Transport-Security "max-age=15768000"
...
</VirtualHost>

# intermediate configuration, tweak to your needs
SSLProtocol              all -SSLv2 -SSLv3
SSLCipherSuite            ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:
SSLHonorCipherOrder      on
```

<https://mozilla.github.io/server-side-tls/ssl-config-generator/>

# SCOPE



# Most Popular Databases

| Rank     |          |          | DBMS                   | Database Model    | Score    |          |          |
|----------|----------|----------|------------------------|-------------------|----------|----------|----------|
| Apr 2017 | Mar 2017 | Apr 2016 |                        |                   | Apr 2017 | Mar 2017 | Apr 2016 |
| 1.       | 1.       | 1.       | Oracle +               | Relational DBMS   | 1402.00  | +2.50    | -65.54   |
| 2.       | 2.       | 2.       | MySQL +                | Relational DBMS   | 1364.62  | -11.46   | -5.49    |
| 3.       | 3.       | 3.       | Microsoft SQL Server + | Relational DBMS   | 1204.77  | -2.72    | +69.72   |
| 4.       | 4.       | ↑ 5.     | PostgreSQL +           | Relational DBMS   | 361.77   | +4.14    | +58.05   |
| 5.       | 5.       | ↓ 4.     | MongoDB +              | Document store    | 325.43   | -1.51    | +12.98   |
| 6.       | 6.       | 6.       | DB2 +                  | Relational DBMS   | 186.66   | +1.74    | +2.57    |
| 7.       | 7.       | 7.       | Microsoft Access       | Relational DBMS   | 128.18   | -4.76    | -3.79    |
| 8.       | 8.       | 8.       | Cassandra +            | Wide column store | 126.18   | -3.01    | -3.49    |
| 9.       | ↑ 10.    | 9.       | Redis +                | Key-value store   | 114.36   | +1.35    | +3.12    |
| 10.      | ↓ 9.     | 10.      | SQLite                 | Relational DBMS   | 113.80   | -2.39    | +5.83    |



TOTAL RESULTS

4,457,222

TOTAL RESULTS

510,365

TOTAL RESULTS

51,998



# Why Are These On The Internet?

# My Guess

- Bad configuration
- Remote administration
- Mix of self-hosted and cloud resources
- Two-tier architecture
  - Thick client makes direct DB calls
  - Javascript sends JSON directly to NoSQL

# Regardless

- There are a LOT of them
- LAN / Internal WAN are not safer
- We need encryption everywhere

# TOOL



O-Saft

nabla-c0d3 / **sslyze**

SSL/TLS Server Test

rbsec / **ssllscan**

**COMODO SSL Analyzer**

**SSL Checker**

testssl.sh

SSL Web Server Test

**TestSSLServer**

**SSL Decoder**

DigiCert® SSL Installation Diagnostics Tool



**Symantec**.CryptoReport





O-Saft

nabla-c0d3 / sslyze

SSL/TLS Server Test

rbsec / sslscan

**COMODO SSL Analyzer**

**SSL Checker**

testssl.sh

SSL Web Server Test

**TestSSLServer**

**SSL Decoder**

DigiCert® SSL Installation Diagnostics Tool



**Symantec CryptoReport**



SECURITY INNOVATION



Qualys. SSL Labs

O-Saft

nabla-c0d3 / sslyze

SSL/TLS Server Test

rbsec / sslscan

SSL Checker

**testssl.sh**

Analyzer

Test

TestSSLServer

SSL Decoder

DigiCert® SSL Installation Diagnostics Tool



Symantec. CryptoReport



**Pinboard**

@Pinboard

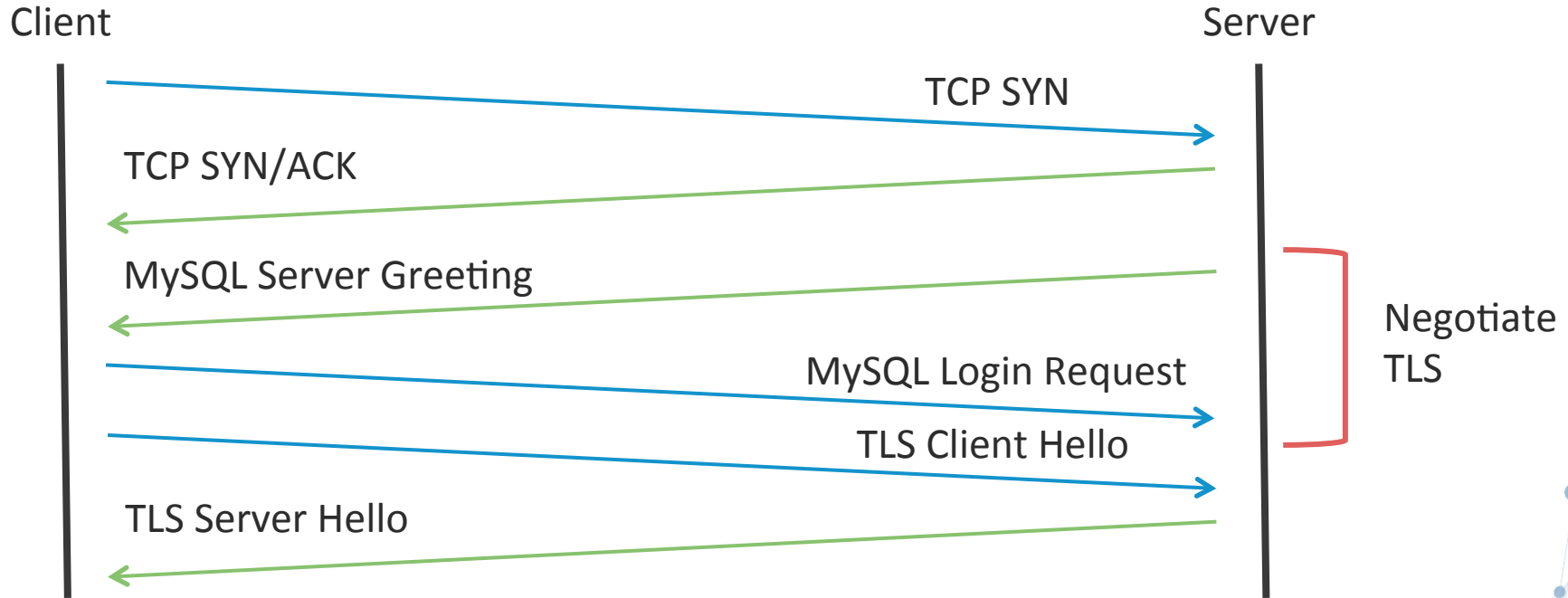
Follow



The Programmers' Credo: we do these things not because they are easy, but because we thought they were going to be easy

1:15 PM - 5 Aug 2016

# STARTTLS - MySQL



# testssl.sh 2.9.5 – Released 9/18/2017

```
$ ./testssl.sh --openssl ./bin/  
openssl.Linux.x86_64.static --starttls  
mysql <hostname>:3306
```

```
$ ./testssl.sh --openssl ./bin/  
openssl.Linux.x86_64.static --starttls  
postgres <hostname>:5432
```

```
$ ./testssl.sh --openssl ./bin/  
openssl.Linux.x86_64.static  
<hostname>:27017
```



# testssl.sh 2.9.5 – Custom OpenSSL

```
$ wget https://testssl.sh/openssl-1.0.2k-dev-chacha.pm.ipv6.Linux+FreeBSD.tar.gz
$ tar -xvf openssl-1.0.2k-dev-chacha.pm.ipv6.Linux+FreeBSD.tar.gz
x bin/openssl.Linux.x86_64.static
$
```

<https://blog.securityinnovation.com>

A record via supplied IP "192.168.56.101"  
rDNS (192.168.56.101): --  
Service set: STARTTLS via POSTGRES

#### Testing protocols via sockets

SSLv2 not offered (OK)  
SSLv3 not offered (OK)  
TLS 1 offered  
TLS 1.1 offered  
TLS 1.2 offered (OK)  
SPDY/NPN (SPDY is an HTTP protocol and thus not tested here)  
HTTP2/ALPN (HTTP/2 is a HTTP protocol and thus not tested here)

#### Testing ~standard cipher categories

|                                            |                  |
|--------------------------------------------|------------------|
| NULL ciphers (no encryption)               | not offered (OK) |
| Anonymous NULL Ciphers (no authentication) | not offered (OK) |
| Export ciphers (w/o ADH+NULL)              | not offered (OK) |
| LOW: 64 Bit + DES encryption (w/o export)  | not offered (OK) |
| Weak 128 Bit ciphers (SEED, IDEA, RC[2,4]) | offered (NOT ok) |
| Triple DES Ciphers (Medium)                | offered          |
| High encryption (AES+Camellia, no AEAD)    | offered (OK)     |
| Strong encryption (AEAD ciphers)           | offered (OK)     |

#### Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4

PFS is offered (OK)

ECDHE-RSA-AES256-GCM-SHA384  
ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA  
DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-SHA256  
DHE-RSA-AES256-SHA DHE-RSA-CAMELLIA256-SHA  
ECDHE-RSA-AES128-GCM-SHA256  
ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA  
DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-SHA256  
DHE-RSA-AES128-SHA DHE-RSA-SEED-SHA  
DHE-RSA-CAMELLIA128-SHA

Elliptic curves offered: prime256v1

# DATA



# MySQL Editions

## Community

- Packaged for your favorite Linux distro
- yaSSL library

## Source Code

- Self-compile
- Self-initialize
- OpenSSL library

## Enterprise

- Distributed directly from Oracle for paid customers
- OpenSSL library

## Location:

Local Server

## Configuration:

Default Install

Key: BLOCKER

SHIPPABLE

SECURE

| Server                                | MySQL              | MySQL                     | PostgreSQL                  | MongoDB           |
|---------------------------------------|--------------------|---------------------------|-----------------------------|-------------------|
| Version                               | 5.7.18             | 5.7.18                    | 9.5.7                       | 3.4.6             |
| TLS Library                           | yaSSL              | OpenSSL                   | OpenSSL                     | OpenSSL           |
| Protocol                              |                    |                           |                             |                   |
| SSLv3                                 | Yes                | No                        | No                          | No                |
| TLSv1.0                               | Yes                | Yes                       | Yes                         | Yes               |
| TLSv1.1                               | Yes                | Yes                       | Yes                         | Yes               |
| TLSv1.2                               | No                 | Yes                       | Yes                         | Yes               |
| Require TLS                           | No                 | No                        | No                          | Configurable      |
| Ciphers                               |                    |                           |                             |                   |
| DES                                   | Yes                | No                        | No                          | No                |
| RC4                                   | Yes                | No                        | Yes                         | No                |
| Triple DES                            | Yes                | Yes                       | Yes                         | No                |
| Strongest                             | DHE-RSA-AES256-SHA | DHE-RSA-AES256-GCM-SHA384 | ECDHE-RSA-AES256-GCM-SHA384 | AES256-GCM-SHA384 |
| PFS                                   | Yes                | Yes                       | Yes                         | No                |
| Server Order                          | Yes                | No                        | Yes                         | No                |
| Vulnerabilities                       |                    |                           |                             |                   |
| Secure Renegotiation                  | No^                | Yes                       | Yes                         | Yes               |
| Secure Client-Initiated Renegotiation | No                 | Yes                       | Yes                         | Yes               |
| TLS_FALLBACK_SCSV                     | No                 | Yes                       | Yes                         | ?                 |
| SWEET32                               | No                 | No                        | No                          | Yes               |
| BEAST                                 | No                 | No                        | No                          | No                |
| LUCKY13                               | No                 | No                        | No                          | No                |

## Location:

Local Server

## Configuration:

Hardened

Key: BLOCKER

SHIPPABLE

SECURE

| Server                                | MySQL              | MySQL                     | PostgreSQL                | MongoDB           |
|---------------------------------------|--------------------|---------------------------|---------------------------|-------------------|
| Version                               | 5.7.18             | 5.7.18                    | 9.5.7                     | 3.4.6             |
| TLS Library                           | yaSSL              | OpenSSL                   | OpenSSL                   | OpenSSL           |
| Protocol                              |                    |                           |                           |                   |
| SSLv3                                 | No                 | No                        | No                        | No                |
| TLSv1.0                               | No                 | No                        | No                        | No                |
| TLSv1.1                               | Yes                | No                        | No                        | No                |
| TLSv1.2                               | No                 | Yes                       | Yes                       | Yes               |
| Require TLS                           | Yes                | Yes                       | Yes                       | Yes               |
| Ciphers                               |                    |                           |                           |                   |
| DES                                   | No                 | No                        | No                        | No                |
| RC4                                   | No                 | No                        | No                        | No                |
| Triple DES                            | No                 | No                        | No                        | No                |
| Strongest                             | DHE-RSA-AES256-SHA | DHE-RSA-AES256-GCM-SHA384 | DHE-RSA-AES256-GCM-SHA384 | AES256-GCM-SHA384 |
| PFS                                   | Yes                | Yes                       | Yes                       | No                |
| Server Order                          | Yes                | Yes                       | Yes                       | No                |
| Vulnerabilities                       |                    |                           |                           |                   |
| Secure Renegotiation                  | No^                | Yes                       | Yes                       | Yes               |
| Secure Client-Initiated Renegotiation | No                 | Yes                       | Yes                       | Yes               |
| TLS_FALLBACK_SCSV                     | No                 | Yes                       | Yes                       | Yes               |
| SWEET32                               | Yes                | Yes                       | Yes                       | Yes               |
| BEAST                                 | Yes                | Yes                       | Yes                       | Yes               |
| LUCKY13                               | No                 | Yes                       | Yes                       | No                |

# To The Cloud!

**Location:**  
The Cloud

**Configuration:**  
Default

**Key:** BLOCKER

SHIPPABLE

SECURE

| Server                                | MySQL                   | MySQL              | MySQL                | MySQL                   |
|---------------------------------------|-------------------------|--------------------|----------------------|-------------------------|
| Provider                              | Cloud 1                 | Cloud 2            | Cloud 3              | Cloud 4                 |
| TLS Library                           | OpenSSL                 | yaSSL              | OpenSSL              | OpenSSL                 |
| Protocol                              |                         |                    |                      |                         |
| SSLv3                                 | Yes                     | Yes                | No                   | No                      |
| TLSv1.0                               | Yes                     | Yes                | Yes                  | Yes                     |
| TLSv1.1                               | No                      | Yes                | Yes                  | Yes                     |
| TLSv1.2                               | Yes                     | No                 | Yes                  | Yes                     |
| Require TLS                           | No                      | No                 | No                   | Yes                     |
| Ciphers                               |                         |                    |                      |                         |
| DES                                   | Yes                     | Yes                | No                   | No                      |
| RC4                                   | Yes                     | Yes                | No                   | No                      |
| Triple DES                            | Yes                     | Yes                | Yes                  | Yes                     |
| Strongest                             | ECDHE-RSA-AES256-SHA384 | DHE-RSA-AES256-SHA | ECDHE-RSA-AES256-SHA | ECDHE-RSA-AES256-SHA384 |
| PFS                                   | Yes                     | Yes                | Yes                  | Yes                     |
| Server Order                          | No                      | Yes                | No                   | Yes                     |
| Vulnerabilities                       |                         |                    |                      |                         |
| Secure Client-Initiated Renegotiation | Yes                     | No                 | No                   | No                      |
| SWEET32                               | No                      | No                 | No                   | No                      |
| BEAST                                 | No                      | No                 | No                   | No                      |
| LUCKY13                               | No                      | No                 | No                   | No                      |
| POODLE                                | Yes                     | No                 | No                   | No                      |
| LOGJAM                                | Yes                     | No                 | No                   | No                      |

**Location:**  
The Cloud

**Configuration:**  
Meta Settings

**Key:** BLOCKER

SHIPPABLE

SECURE

| Server                       | MySQL         | MySQL           | MySQL         | MySQL           |
|------------------------------|---------------|-----------------|---------------|-----------------|
| Host                         | Cloud 1       | Cloud 2         | Cloud 3       | Cloud 4         |
| TLS Library                  | OpenSSL       | yaSSL           | OpenSSL       | OpenSSL         |
| Default Configuration        |               |                 |               |                 |
| TLS Available                | Yes           | Yes             | Yes           | Yes             |
| TLS Enabled                  | Yes           | No              | Yes           | Yes             |
| TLS Required                 | No            | No              | No            | Yes             |
| Public IP Connection Allowed | No            | TCP             | No            | TCP             |
| Certificate Created          | Yes           | No              | Yes           | Yes             |
| Overall TLS Strength         | Low           | Low             | Medium        | Strong          |
| Certificate                  |               |                 |               |                 |
| Signature Algorithm          | SHA1 with RSA | SHA256 with RSA | SHA1 with RSA | SHA256 with RSA |
| Server key size              | RSA 2048 bits | RSA 2048 bits   | RSA 2048 bits | RSA 2048 bits   |
| Self Signed                  | No            | No              | No            | No              |
| CA                           | Internal      | Internal        | Internal      | Public          |
| Configuration Options        |               |                 |               |                 |
| TLS Configurable             | No            | Yes             | Somewhat      | Somewhat        |
| Avoidable Issues             |               |                 |               |                 |
| Recompiled With OpenSSL      | Yes           | No              | Yes           | Yes             |
| Severe Known Vulnerabilities | Yes           | No              | No            | No              |

# CONCLUSIONS

# The Good



# PostgreSQL



**I CAN BE  
CONFIGURED  
SECURE**

# The Cloud

- Autogenerated signed certificate

# The Cloud

If you trusted Cloud Provider 4, you probably would have gotten a MySQL server configured **more** securely than you would have done yourself.

# The Bad

# The Cloud

If you trusted Cloud Provider 1, you probably would have gotten a MySQL server configured **less** securely than you would have done yourself.

# The Cloud

- 2/4: Poor default TLS configuration
- 2/4: Autogenerated certs have medium security
- 3/4: No way to modify TLS configuration to fix detected issues
  - 1/4: No ability to change anything
- 3/4: Do not require TLS, client's choice

# On-Premises Database

- Poor default TLS configuration
- Bugs only just exposed through testing
  - MySQL (yaSSL) cipher negotiation
  - MongoDB server order
- Only newest versions (~2 years) have strong TLS support

# MySQL Community Edition

- Cannot be configured for maximum security
  - No TLSv1.2
  - TLS Downgrade Attacks
- Mitigation
  - Compile from source with OpenSSL
  - Use local transports only
    - Unix domain sockets / shared memory



# The Ugly

# Internet Survey

- I was going to do some mass scans of Internet connected hosts to tabulate real world TLS practices...
- But, since older versions, MySQL Community Edition, and some cloud providers can't be configured secure, I think we already know the results.

# Hope



Now You Can  
Measure It And  
You Can  
Improve It.

# Thank You



★ Dirk Wetter (@drwetter)

\* Creator of testssl.sh

# Thank You!

[www.securityinnovation.com](http://www.securityinnovation.com)



@sdanndev  
sdanneman@securityinnovation.com

# APPENDIX

# Future Work

- Test if non-TLS DB protocol is enabled
- Test proper client TLS configuration
- Test proper DB cluster TLS configuration
- Survey the Internet: see improvement over time



# Bugs

- MySQL: TLS cipher negotiation incorrectly matches on last byte only (yaSSL)
- OpenSSL: s\_client mysql won't connect to server with an odd number of chars in version string