genua

SSL TLS
Erweiterte Einführung

Deutscher Perl Workshop 2015

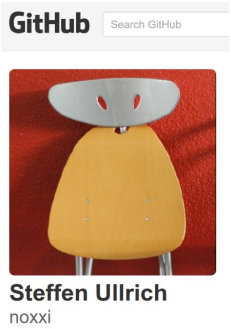
Steffen Ullrich

Slides: http://noxxi.de/talks.html

about:me

genua

- Perl seit 1997
- genua mbH seit 2001 https://genua.de
  - Application Level Firewalls
  - Forschung IT-Sicherheit
- Maintainer IO::Socket::SSL seit 2006
  - Non-Blocking I/O
  - Sichere Defaults
  - SSL-Interception



genua

- Ziel des Vortrages
  - Überblick zu SSL/TLS
  - nicht zu technisch
  - Grundprinzipien
  - Ecken und Kanten, etablierte Lösungen bzw. Workarounds
  - typische Missverständnisse klären

Motivation

HTTPS Everywhere

Lavabit

Was ist SSL/TLS?

genua

- Verschlüsselung des Datentransports
  - Ende-zu-Ende
  - Client-Server Szenarien
- Netscape:
  1994 SSL1.0 – 1995 SSL2.0 – 1996 SSL3.0
- Standardisierung:
  1999 TLS 1.0 (SSL3.1) - RFC2246
  2006 TLS 1.1 (SSL3.2) - RFC4346
  2008 TLS 1.2 (SSL3.3) - RFC5246
  ???? TLS 1.3

http://en.wikipedia.org/wiki/Transport_Layer_Security

Was bietet TLS?

genua

- Verschlüsselung:
  - Schutz vor Mithören und Manipulation
  - Symmetrische Cryptographie
- Identifikation:
  - Erkennung von Man-In-The-Middle
  - Schutz vor DNS-Spoofing
  - Public-Key-Cryptographie, Zertifikate, Signaturen
  - Hauptquelle der Probleme
  - 75% dieses Vortrags

Was bietet TLS nicht?

genua

- schützt nur Transport zwischen Client und Server, nicht Ablage von Daten
- keine Aussagen über Vertrauenswürdigkeit oder Sicherheit der Gegenstelle
- kein Schutz vor CSRF, XSS, SQL-Injection...
- auch Malware ist über TLS transportierbar
- schützt nicht vor Tracking, Anzeigen...

Anwendungen

genua

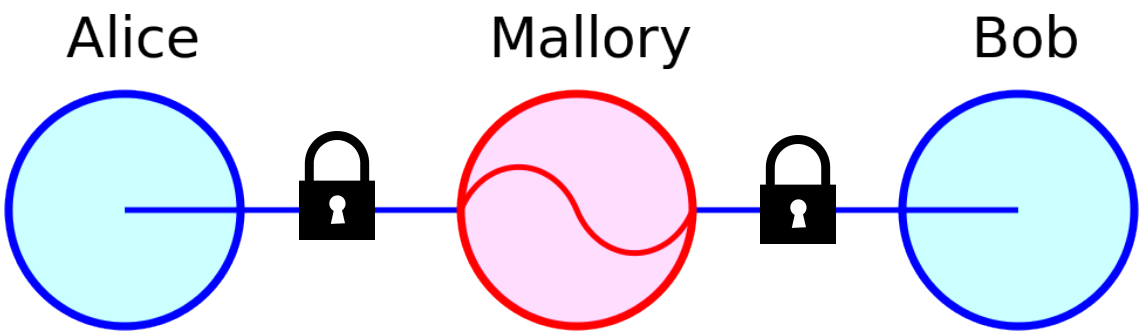
- HTTPS
- Mail: SMTP, IMAP, POP3
- FTPS (nicht sftp), VoIP(SIP), VPN, LDAP, stunnel...
- implizites TLS („SSL“):
  direkt nach Verbindungsaufnahme
- explizites TLS („TLS“):
  über spezielle Anweisungen im plain Text
  (STARTTLS, STLS, AUTH TLS...)

Identifikation - wozu

genua

- Sicherstellen, dass Gegenstelle die gewünschte ist.
- Fehlerhafte Identifikation ermöglicht Man-In-The-Middle und damit transparentes Mithören und Manipulation der verschlüsselten Daten.

  Aktives MITM in lokalen Netzen recht einfach.



http://commons.wikimedia.org/wiki/File:Man_in_the_middle_attack.svg#/media/File:Man_in_the_middle_attack.svg

Identifikation
Zertifikate

genua

X.509 Zertifikat

Issuer:
C=GB, ST=Greater Manchester, L=Salford,
O=COMODO CA Limited,
CN=PositiveSSL CA 2

Validity
Not Before: May 30 00:00:00 2014 GMT
Not After : Aug 27 23:59:59 2016 GMT

Subject:
OU=Domain Control Validated,
OU=PositiveSSL Wildcard,
CN=*.genua.de

....
X509v3 Subject Alternative Name:
DNS:*.genua.de, DNS:genua.de

Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus: 00:ae:86:....

Nur Eigentümer des Zertifikats hat passenden Private Key.

Identifikation
Zertifikat und Trustchain

genua

Certificate Hierarchy

- AddTrust External CA Root
  - PositiveSSL CA 2
    - *.genua.de

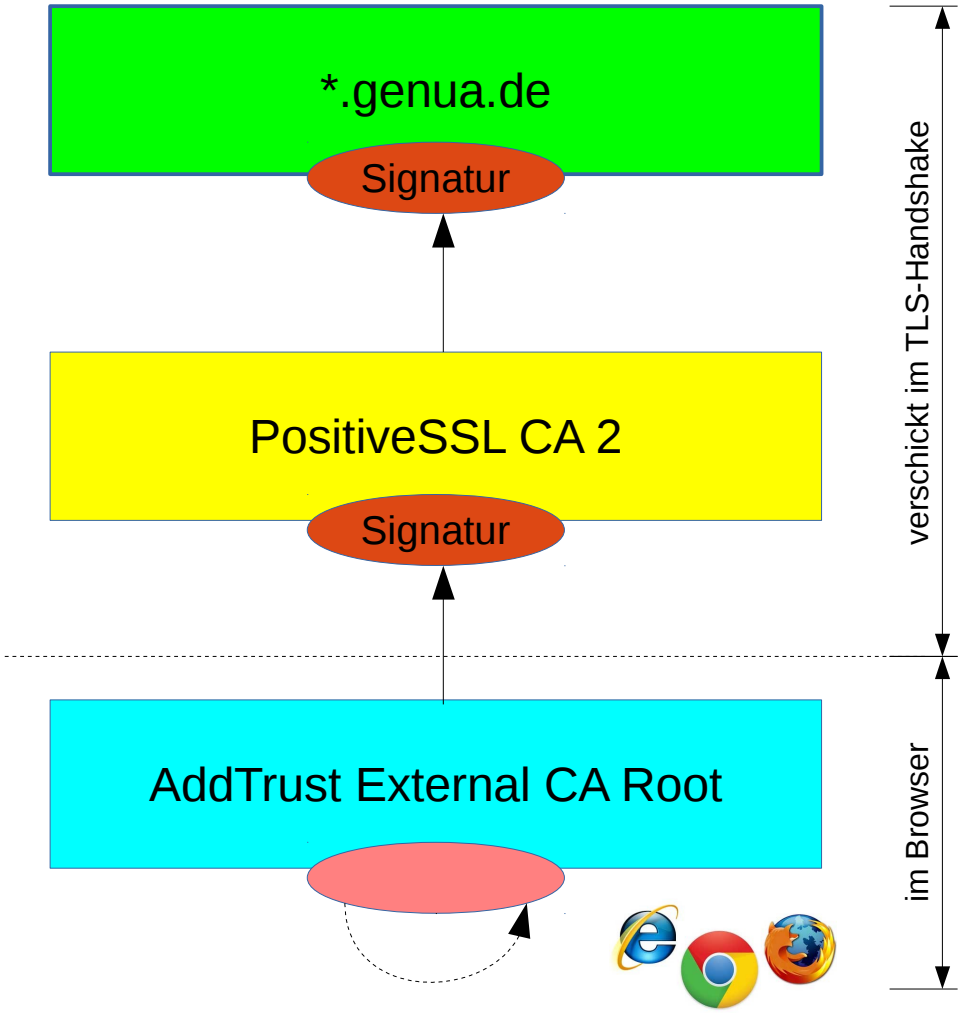
Certificate Fields

- *.genua.de
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before
      - Not After
    - Subject

Field Value

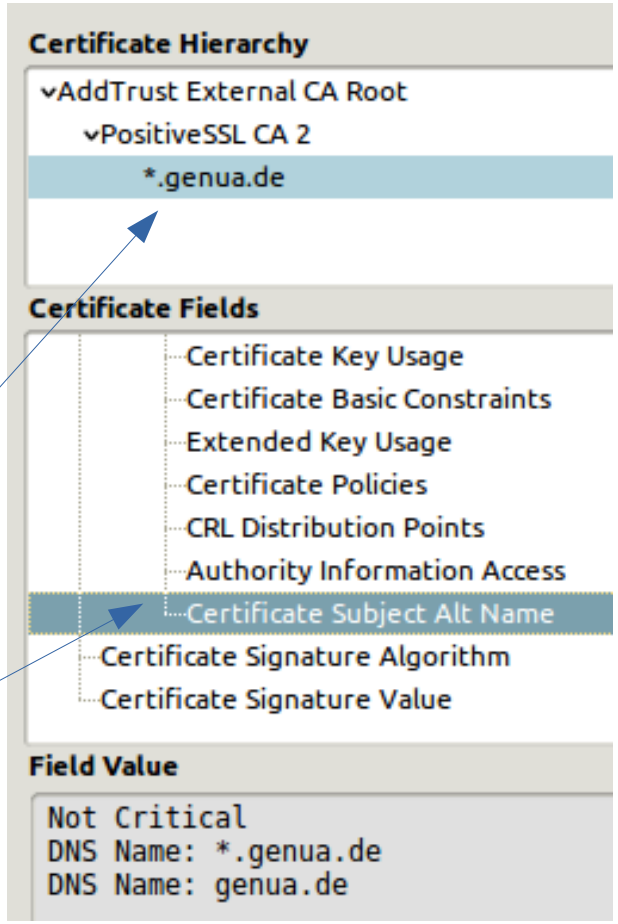
```
CN = PositiveSSL CA 2
O = COMODO CA Limited
L = Salford
ST = Greater Manchester
C = GB
```

abgeleitetes Vertrauen



eingebautes Vertrauen

Identifikation
Verifikation Subject



Gewünschtes Ziel muß mit Subject übereinstimmen.

Identifikation
Verifikationsfehler

genua

https://foobar.maulwuff.de/ | Certificate Error: Navigatio...

There is a problem with this website's security certificate.

The security certificate presented by this website has expired or is not yet valid.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this

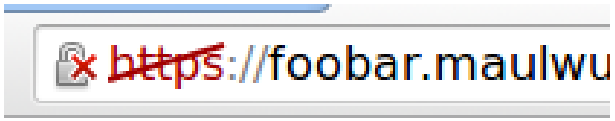
Click here to close this webpage.

Continue to this website (not recommended).

More information

- If you arrived at this page by clicking a link, check the website addres sure that it is the address you were expecting.
- When going to a website with an address such as https://example.cor the address, https://www.example.com.

For more information, see "Certificate Errors" in Internet Explorer Help.



Your connection is not private

Attackers might be trying to steal your information from **foobar.maulwuff.de** (for example, passwords, messages, or credit cards).

Hide advanced

Back to safety

This server could not prove that it is **foobar.maulwuff.de**; its security certificate is from **www.maulwuff.de**. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to foobar.maulwuff.de (unsafe)

NET::ERR_CERT_COMMON_NAME_INVALID

Technical Details

foobar.maulwuff.de uses an invalid security certificate.

The certificate is only valid for the following names:
www.maulwuff.de, maulwuff.de

(Error code: ssl_error_bad_cert_domain)

Identifikation oft nicht verstanden

genua

Trust not trusted certificates and skip hostname verification

0

I have a server witch is running a https web server. When i enter it with my browser i get errors that the domain does not match (because i use IP of the server) and the cerificate is not trusted. Now i need to send GET requests to that server using apache httpclient 4.2.1. I found a piece of code online that helps me:

```
    httpClient = new DefaultHttpClient(a, b);
    SSLSocketFactory sslSocketFactory = new SSLSocketFactory(
            new TrustStrategy() {
                @Override
                public boolean isTrusted(X509Certificate[] arg0, String arg1) throws
                    return true;
                }
            }, SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER);
    httpClient.getConnectionManager().getSchemeRegistry().register(new Scheme("https
```

SSL Vulnerability in ******** VU#582497

0

Recently received a warning letter that my application security threatened.

```
---------- Forwarded message ----------
  From: CERT Coordination Center <cert@cert.org>
  Subject: SSL Vulnerability in ********* VU#582497
  Cc: cert@cert.org
```

```
    private static class NullHostnameVerifier implements HostnameVerifier {
        public boolean verify(String hostname, SSLSession session) {
            return true;
        }
    }
```

Can anyone suggest on this issue. What is my fault?

How to disable “defaultHostnameVerifier” property in SpringXD

0

1

I have a requirement to connect to a https URL from my processor module when a message is put on a Q (suppose q name here is: readFromQ) and then just log the response from the url GET call. I am using http-client processor for making a GET call to the url here. My stream looks like below :

stream create --name hitSSL --definition "jms --destination=readFromQ | http-client --url='"https://remoteHost:remotePort/trafficcontrol/'" --httpMethod=GET | log"

Now the problem is that this URL presents spring-xd with a certificate that does not match with the hostname I am trying to hit. The certificate is named something like abc.mycompany.com, whereas the URL's hostname is remoteHost.

Spring XD throws : **java.security.cert.CertificateException: No name matching remoteHost found**.

My cacerts does have the abc.mycompany.com certificate added.

I need to know if there is a way I can disable SpringXD from verifying hostname with CN while establishing SSL connection. Is there a way to disable the java property **javax.net.ssl.HttpsURLConnection.setDefaultHostnameVerifier**

MITM durch fehlerhafte Verifikation Zertifikate

genua

CWE-297: Improper Validation of Certificate with Host Mismatch

Improper Validation of Certificate with Host Mismatch

Weakness ID: 297 *(Weakness Variant)* **Status:** Incomplete

Description

Description Summary

The software communicates with a host that provides a certificate, but the software does not properly ensure that the certificate is actually associated with that host.

CVE-2014-5075 MitM Vulnerability in the Smack XMPP Library for Java

Georg Lukas, rt-solutions.de, 2014-08-05

Smack is an Open Source XMPP (Jabber) client library for instant messaging and presence written in Java. Smack prior to version 4.0.2 is vulnerable to TLS Man-in-the-Middle attacks, as it fails to check if the server certificate matches the hostname of the connection.

Murray McAllister 2013-12-17 20:14:42 EST **Description**

```
It was found that PyWBEM, a Python library for making CIM (Common Information
Model) operations over HTTP using the WBEM CIM-XML protocol, failed to verify the
URI matches the Subject of the certificate. This could allow a man-in-the-middle
attacker to spoof an SSL server if they had a certificate that was valid for any
domain name.
```

Vulnerability Details : CVE-2011-1429

Mutt does not verify that the smtps server hostname matches the domain name of the subject of an X.509 certificate, which allows man-in-the-middle attackers to spoof an SSL SMTP server via an arbitrary certificate, a different vulnerability than CVE-2009-3766.

Publish Date : 2011-03-16 Last Update Date : 2011-09-21

CVE-2011-0633

The libwww−perl (LWP) module Net::HTTPS did not fully validate SSL certificates by default prior to version 6.00. Multiple Perl modules (such as WWW::Mechanize and LWP::UserAgent) do not enable full validation of SSL certificates when using libwww-perl, leaving software that uses them vulnerable to man-in-the-middle attacks. This issue was addressed by changing the default behavior of libwww-perl to enable full validation of SSL certificates.

Ubuntu Security Notice USN-2292-1

Authored by Ubuntu | Site security.ubuntu.com Posted Jul 17, 2014

Ubuntu Security Notice 2292-1 - It was discovered that the LWP::Protocol::https perl module incorrectly disabled peer certificate verification completely when only hostname verification was requested to be disabled. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could possibly be exploited in certain scenarios to alter or compromise confidential information in applications that used the LWP::Protocol::https module.

CVE-2012-5784 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Apache Axis 1.4 and earlier, as used in PayPal Payments Pro, PayPal Mass Pay, PayPal Transactional Information SOAP, the Java Message Service implementation in Apache ActiveMQ, and other products, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

FortiClient Android and iOS multiple vulnerabilities

Risk	2 Low
Date	Feb 25 2015
Impact	MitM condition and potential credential harvesting

FortiClient Android and iOS are affected by two vulnerabilities:

1. Android and iOS FortiClient do not check the validity of server certificates.
   An attacker may perform a man-in-the-middle attack between the FortiClient and the following services:
   - A remote FortiGate with SSL VPN service running by default on port 443
   - A remote FortiGate with Endpoint control running by default on port 8010

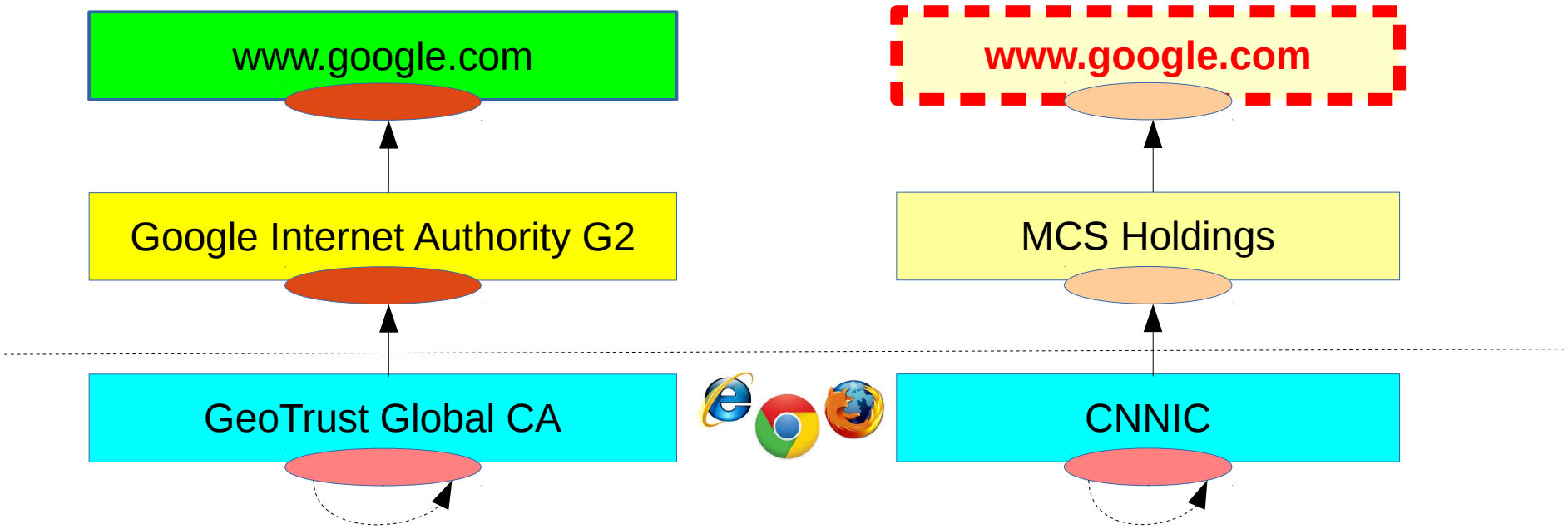
The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software

Vulnerability Note VU#582497

Multiple Android applications fail to properly validate SSL certificates

Original Release date: 03 Sep 2014 | Last revised: 08 Dez 2014

100+ Root-CA
alle gleichberechtigt



CNNIC hatte gefälschten SSL-Zertifikate für Google-Domains beglaubigt und legt laut Google wenig Transparenz beim Signieren von Zwischen-Zertifizierungsstellen an den Tag.

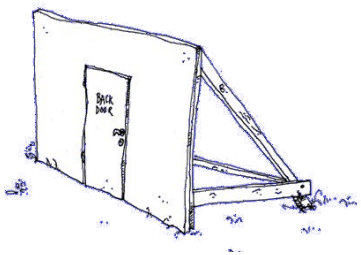
Google will die Root-Zertifikate der chinesischen Zertifizierungsstelle China Internet Network Information Center (CNNIC) aus allen Google-Programmen wie Chrome verbannen. Google

100+ Root-CA
es reicht wenn eine kaputt ist

genua

06.09.2011 15:02

DigiNotar-Hack: Kritische Infrastruktur war unzureichend geschützt



Die kritische Infrastruktur bei der kompromittierten Zertifizierungsstelle DigiNotar war unzureichend geschützt. Das geht aus dem Zwischenbericht (PDF) des Sicherheitsunternehmens Fox-IT hervor. Demnach standen die CA-Server zwar in einer sicheren Umgebung, waren jedoch über das Management-LAN erreichbar. Dadurch konnte sich der Angreifer wohl von außen zu den

07.02.2012 16:15

Trustwave verkaufte Man-in-the-Middle-Zertifikat

Der Zertifikatsherausgeber Trustwave hat einer Firma ein Zertifkat verkauft, mit dem sich diese gültige Zertifikate für beliebige Server ausstellen konnte. Damit war es ihr dann möglich auch den verschlüsselten Datenverkehr ihrer Mitarbeiter etwa mit Diensten wie denen von Google oder Hotmail zu überwachen. Mittlerweile habe man das CA-Zertifikat jedoch widerrufen und werde das zukünftig auch nicht mehr tun, gelobt der Zertifikatsherausgeber.

04.01.2013 12:32

Fatale Panne bei Zertifikatsherausgeber Türktrust

Der türkische Zertifikatsherausgeber Türktrust hat einen fatalen Fehler begangen: Er hat zwei SSL-Zertifikate ausgestellt, die sich wiederum selbst zum Ausstellen von Zertifikaten für beliebige Domains eignen. Mit einem der sogenannten SubCA-Zertifikate wurde ein SSL-Zertifikat für *.google.com ausgestellt, welches auch zum Einsatz kam. Laut Türktrust handelt es sich bei dem Vorfall um eine Verkettung unglücklicher Umstände, Hinweise auf einen Missbrauch gebe es nicht.

On Wednesday, July 2, we became aware of unauthorized digital certificates for several Google domains. The certificates were issued by the National Informatics Centre (NIC) of India, which holds several intermediate CA certificates trusted by the Indian Controller of Certifying Authorities (India CCA).

The India CCA certificates are included in the Microsoft Root Store and thus are trusted by the vast majority of programs running on Windows, including Internet Explorer and Chrome. Firefox is not affected because it uses

Identifikation: Revocation

genua

https://revoked.grc.com

Security Certificate
Revocation Awareness Test

If you can see this (and apparently you can), you are using a **revocation UNaware** web browser!

The SSL/TLS security certificate for this special website has been deliberately revoked. Since you **are** seeing this page, we know that this web browser is allowing a site with a **known invalid certificate** to display its pages. This is likely not the behavior you would choose.

Here's what we know:

- **The Firefox browser** currently leads the industry in certificate revocation checking security. It incorporates its own mature internal technology and Firefox checks for revocation by default (thus protecting all users). And it does this on every operating system platform.
- **Google's Chrome browser** is the least certificate-secure browser on the Internet. It puts speed before security, so *it is the only browser on the Internet* to disable certificate checking by default.
- **Internet Explorer** uses Windows' built-in revocation checking which is also enabled by default.
- **The mobile Android platform** currently offers **no** certificate revocation checking of its own, so Android apps (including all users of Google's Chrome browser) are vulnerable to malicious certificate abuse. The only way to use Android securely today is with Firefox, which brings along its own certificate security.
- **iOS is only a bit better than the Android disaster.** It only checks for revocation of extended validation (EV) certificates and trusts everything else. On iOS, Safari and the LastPass Tab browser get this benefit. But incredibly, Chrome on iOS doesn't pay attention to any certificate revocation.

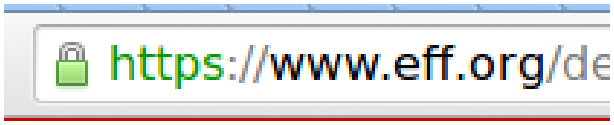
This "revoked.grc.com" test was born from the revelation of the worrisome "Heartbleed" vulnerability that had existed in plain sight for two years without public awareness in the industry standard open source OpenSSL security suite. However, this special site is about more than that:

kurze Expiration = Revocation des armen Mannes

Perl: $socket->ocsp_resolver->resolve_blocking();

Identifikation:
Wie kann man Zertifikate bekommen

genua



- Kaufen von einer der 100+ CAs
  - Unterschiedliche Preise, Konditionen.
  - Von 0,-*
  - Host-Zertifikate, Wildcards, Multi-Domain...
  - Validierung Besitz der Domain über spezielle E-Mail o.ä. - „domain validated certificate“ (DV)

Bogus SSL certificate for Windows Live could allow man-in-the-middle hacks

The race is on to kill trust in a live.fi credential issued without authorization.

- EV-Zertifikate
  - Green bar !!!

  - Bessere Überprüfung des Owners (so wie früher).
  - Nur einige CA können EV ausstellen, im Browser verankert welche.
  - Revocation wird gecheckt, fail hard.

Identifikation – FAQ 1

genua

- Kann man eigene CA sein, die von allen Browsern akzeptiert wird?
  Ja, sofern man das entsprechende Knowhow hat und die notwendige Sicherheit bieten kann. Anforderungen werden höher, was die Browser akzeptieren.
- Kann man eine Zwischen-CA kaufen um Zertifikate für viele Domains auszustellen?
  Prinzipiell schon, nur sind auch die die Anforderungen hoch, da das Missbrauchspotential hoch ist. Aber z.B. Google hat es und Cloudflare wohl auch. MCS Holdings hingegen wohl nicht mehr.

Identifikation – FAQ 2

genua

- Kann man eine eigene private CA betreiben?
  Ja, nur muss diese in alle Browser, die ihr vertrauen sollen. In größeren Firmen ist das recht typisch.
- Kann die eigene CA auch EV ausstellen?
  Nein, welche CA EV ausstellen können ist fest in den Browsern hinterlegt.
- Warum nicht einfach self-signed benutzen?
  Wenn es nur einige wenige Clients gibt, ist das eine brauchbare Option. Aber man muss auf sicherem Weg allen Nutzern Bescheid geben, welches Zertifikat korrekt ist. Vorinstallierte Root-CAs lösen genau dieses Problem des Initialvertrauens.

Identifikation – FAQ 3

genua

- Wie kann ich sicherstellen, dass kein anderer Zertifikate für meine Domain ausstellt?
  - Identitätsmissbrauch verhindern
  - Zertifikats-/Publickeypinning preloaded oder mit HPKP (Chrome 38, Firefox 35)
- Öffentliche Zertifikate für localhost, mDNS (*.local) oder interne Toplevel-Domains:
  Diese Hostnamen sind keiner einzelnen Person/Firma zuzuordnen. Daher werden keine öffentliche CA's dafür (mehr) Zertifikate ausstellen.

Identifikation – FAQ 4

genua

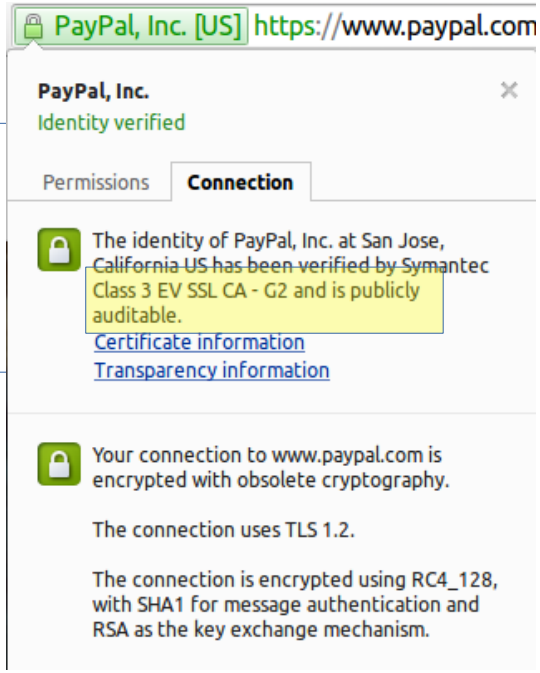
- Braucht man ein Zertifikat nur für ein https-Redirect zu einer anderen Seite?
  Ja, das Redirect findet erst innerhalb des HTTP-Protokolls statt, welches bei HTTPS erst nach erfolgreicher Validierung des Zertifikats benutzt wird.
- Geht ein Redirect über DNS CNAME?
  Nein, in diesem Falle gibt es einen Namenskonflikt, da der Hostname in der URL nicht dem des Zertifikats entspricht.

genua

Das ist doch alles kaputt !!

Wir müssen wohl erstmal damit leben und es könnte schlimmer sein. Kleine Hoffnungsstreifen sind die Aufdeckung von Missbrauch durch Certificate Transparency und Pinning.

This latest attack was reportedly caught by a user running the Google Chrome browser in Iran who noticed a warning produced by the "public key pinning" feature which Google introduced in May of this year. Basically, Google hard-coded the fingerprints for its own sites' encryption keys into Chrome, and told the browser to simply ignore contrary information from certificate authorities. That meant that even if an attacker got a hold of a fake certificate for a Google site —as this attacker did—newer versions of the Chrome browser would not be fooled.



Identifikation und SMTP

genua

- explizites TLS mit „opportunistischer“ Verschlüsselung
- Aktives MITM wird nicht als Problem gesehen, da dieses ja bereits STARTTLS filtern könnte.
- oft keine sinnvolle Verifikation der Zertifikate, diverse Heuristiken
- Selbst bei korrekter Identifikation kein Schutz gegen DNS-Spoofing, da MX gespoofed sein kann.

Verschlüsselung

genua

- Deutlich übersichtlicher, da primär Mathematik und nicht Vertrauensprobleme:
  - alle paar Jahr stärkere Verfahren einsetzen (Algorithmen, Keylängen...)
  - schwache Ciphern abschalten: LOW, EXPORT, RC4...
  - starke schnelle Cipher benutzen: GCM
  - Perfect Forward Secrecy: kein nachträgliches Entschlüsseln möglich (ECDHE- ..., DHE-...)
  - Client bestimmt, welche Ciphern verfügbar. Server wählt aus.

Bits: Längen von Schlüsseln und Signaturen

genua

- Länge nicht zwingend effektive Länge, abhängig vom Verfahren

Vergleich der Verschlüsselungsstärken[4][5]

Sicherheitsniveau	RSA/DH (NIST)	RSA/DH (ECRYPT)	ECDH
80	1024	1248	160
112	2048	2432	224
128	3072	3248	256
192	7680	7936	384
256	15360	15424	512[6]

http://de.wikipedia.org/wiki/Elliptic_Curve_Cryptography

- Sicherheitsniveau langfristig abschätzbar, sofern nicht unerwartete qualitative Durchbrüche in Mathematik oder Computertechnik.

Bits laut Empfehlung BSI

genua

- bis 2021+:
  2000bit RSA, SHA-2, 2000bit DH, 250bit ECDH
  (EC)DHE + AES 128/256 + GCM/CBC + SHA256/384

- Ablösen von Verfahren
  bis 2013: RC4
  bis 2014: TLS 1.0
  bis 2015: SHA-1 in Signaturen
  bis 2018: SHA-1 als HMAC

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Performance

genua

- Hauptproblem initialer Handshake:
  - 1xRTT TCP + 2xRTT TLS-Handshake
  - Reduzierung TCP-Handshake durch HTTP Keep-Alive
  - Reduzierung TLS-Handshake durch Session-Resumption (1xRTT)
  - evtl. Reduzierung TLS-Handshake durch minimale Zertifikatsketten (TCP Slow Start)
- unterschiedliche Performance von Ciphern
  - AES/AES-GCM teilweise hardwareunterstützt. Evtl. sehr langsam, wenn ohne Hardware (Java GCM).
  - ChaCha20 gut in Software

SNI – Server Name Indication

genua

- mehrere Domains auf gleicher IP
  - HTTP: Host-Header
  - TLS 1.0+: Server Name Indication
    Liefern des passenden Zertifikates bevor man den Host-Header sehen kann.
- unterstützt von allen modernen Browsern (aber nicht IE8/XP) und vielen, aber nicht allen Programmiersprachen bzw. Bibliotheken.
- Nicht unterstützt von Java6-, Python 2.7.8-, Android Apache HTTPClient, ...

Design- und Implementationsprobleme

genua

Designprobleme

2009: insecure Renegotiation
2011: BEAST (CBC)
2012: CRIME (compression)
2013: BREACH (compression)
2013: RC4
2014: POODLE (CBC+SSL3.0)

Poodle Gothic Redux by Amanda Wray

Implementierungsprobleme

2002 MSIE ignoriert CA:false
2011 iOS ignoriert CA:false
2014 Heartbleed: OpenSSL
2014 goto fail (MITM): Secure Transport
2014 remote code execution: SChannel
2014 MITM: GnuTLS
2014 FREAK: OpenSSL, Secure Transport, SChannel, Mono, IBM JSSE..

Noch Fragen?

TLS funktioniert in der Theorie, hat aber in der Praxis viele Probleme, die die Sicherheit gefährden.

Oh, schau mal die süßen Kätzchen.