Understanding Encryption Services Using Wireshark

Sunday June 16th 2013

Larry Greenblatt
Jedi Knight  |  InterNetwork Defense
About me

**Musician:**
Gung Ho! - Lead Guitar / Vocals / Songwriter
– *Philly's #1 Cyber Punk Band since 1980*
– *Produced by Otto Capobianco*

**Martial Artist:**
Black Sash Taiji
3rd Degree Black Belt JLFS

**Hobbies (my day job):**
Network nerd (& InfoSec geek) 1984
Consultant / Instructor / Author
CISM, CISSP, CEH, ECSA, Security+
Co-Founder of InterNetwork Defense
Just How Long Have I Been a Network Dweeb?
Guidelines from my Mother

Always suspect of anyone:
- “That's what they want you to think”
- “That's how they get you”
- “They get you coming and going”

Can tell you the Greek origin of any word
Guidelines from my band

You know you could mess somebody up wit dat!
Guidelines from Robert Anton Wilson

“*You Can't Speak Matter of Factually About Anything You Can't Measure*”

“You should view the world as a conspiracy run by a very closely-knit group of nearly omnipotent people, and you should think of those people as yourself and your friends.”

Robert Anton Wilson
1932–2007
What is a Hacker?

RFC-2828

"someone who figures things out and makes something cool happen"
with Bob & Alice

A Consumers Guide to:

1) Confidentiality
2) Authentication
3) Integrity
4) Non-Repudiation

By Employing:

Symmetric, Asymmetric and Hashing Algorithms
It is said that “Packets Do Not Lie”
The Intelligent Consumer

welcome to the crypto-Mart

Aisle 1
Symmetric Algorithms (Shared Secret)

RC4
AES
Twofish
Blowfish
DES & 3DES
E0

Aisle 2
Asymmetric Algorithms (Public/Private)

Diffie-Hellman
RSA
ECC
El Gamal

Aisle 3
Hashing Algorithms (Message Digests)

MD5
SHA1, SHA2 & SHA3
Skein
Whirlpool
<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</td>
<td>40</td>
</tr>
<tr>
<td>TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)</td>
<td>40</td>
</tr>
<tr>
<td>TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)</td>
<td>40</td>
</tr>
<tr>
<td>TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)</td>
<td>40</td>
</tr>
<tr>
<td>TLS_RSA_WITH_RC4_128_MD5 (0x0004)</td>
<td>40</td>
</tr>
</tbody>
</table>

Compression Methods Length: 1
- Compression Methods (1 method)

Extensions Length: 54
- Extension: renegotiation_info
- Extension: server_name
- Extension: status_request
- Extension: elliptic_curves

**Extension: ec_point_formats**

<table>
<thead>
<tr>
<th>Offset</th>
<th>Value 1</th>
<th>Value 2</th>
<th>Value 3</th>
<th>Value 4</th>
<th>Value 5</th>
<th>Value 6</th>
<th>Value 7</th>
<th>Value 8</th>
<th>Value 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0090</td>
<td>c0 09 c0 0a 00 32 00 38 00 13 00 04 01 00 00 36</td>
<td>.........2.8.........</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00a0</td>
<td>ff 01 00 01 00 00 00 00 14 00 12 00 00 0f 73 73</td>
<td>.................</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00b0</td>
<td>6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 00 05 00</td>
<td>l.gstatic.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00c0</td>
<td>05 01 00 00 00 00 00 0a 00 06 00 04 00 17 00 18</td>
<td>.................</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00d0</td>
<td>00 0b 00 02 01 00</td>
<td>.........</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Part 1

Symmetric Encryption

• Bob wants to share a secret with Alice
  - First they must both secretly agree on a shared key. How?
Symmetric Encryption

- **Strengths**
  - Fast

- **Challenges**
  - Key Agreement
  - Scalability
    - $N(N-1)/2$

- **Security Services:**
  - Confidentiality
  - Limited* authenticity

*Alice knows it is Bob, but she can’t prove it!
Part 2

Asymmetric Encryption

• Alice creates a related key pair
  – She keeps one to herself (private key will sign)
  – Gives the other to anyone who wants it (public)

• Public key:
  – ID card
  – PKI: Validates x.500 name
Asymmetric Encryption

- **Advantages over symmetric**
  - Key Distribution
  - Scalability (2N)
  - Provides Non-Repudiation

- **Disadvantages**
  - Much slower
  - Requires Trusted 3\textsuperscript{rd} Party
    - PKI Hierarchy
    - OpenPGP Web of Trust
Certificate (id-at-commonName=mail.google.com, id-at-organizationName=)

- signedCertificate
  - version: v3 (2)
  - serialNumber: 0x2b9f7ee5ca25a62514204782753a9bb9
- signature (shaWithRSAEncryption)
- issuer: rdnSequence (0)
- validity
- subject: rdnSequence (0)
  - rdnSequence: 5 items (id-at-commonName=mail.google.com, id-at-organizationName=)
- subjectPublicKeyInfo
  - algorithm (rsaEncryption)
    - Padding: 0
    - subjectPublicKey: 30818902818100af39159868e492fe4f4ff1bbff0d2eb0f
- extensions: 4 items
  - algorithmIdentifier (shaWithRSAEncryption)
Certificate (id-at-commonName=mail.google.com, id-at-organizationName=)
  signedCertificate
    version: v3 (2)
    serialNumber : 0x2b9f7ee5ca25a62514204782753a9bb9
  signature (shaWithRSAEncryption)
  issuer: rdnSequence (0)
  validity
  subject: rdnSequence (0)
    rdnSequence: 5 items (id-at-commonName=mail.google.com, id-at-organizationName=)
  subjectPublicKeyInfo
    algorithm (rsaEncryption)
      Padding: 0
      subjectPublicKey: 30818902818100af39159868e492fe4f4ff1bbff0d2eb0f
  extensions: 4 items
    algorithmIdentifier (shaWithRSAEncryption)
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>2127</td>
<td>0.005072</td>
<td>173.194.43.30</td>
<td>192.168.1.14</td>
<td>TLSv1</td>
<td>1484</td>
<td>Server H</td>
</tr>
</tbody>
</table>

Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)
Length: 77
Version: TLS 1.0 (0x0301)

Random
Session ID Length: 32
Session ID: adf7fc0895c40eacdc257aa8f5093536cd2556b95ed61

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Compression Method: null (0)
Extensions Length: 5

Extension: renegotiation_info
Where & What to Encrypt?

- **Application** (S/MIME, OpenPGP, SSH)
- **Presentation** (TrueCrypt, PKZip)
- **Transport** (SSL/TLS)
- **Network** (IPSec)
- **Link layer** (watch out! router support)
Encrypting eMail

1) Session Key
   encrypts email

2) Add Session key to mail

3) Alice's Public Key
   encrypts Session Key

Hello Alice,
I love you, I love you, I love you.
Please marry me, Bob.
Decrypting eMail

Hello Alice,
I love you I love you I love you.

Please marry me,
Bob

5) Session Key decrypts message

4) Alice’s Private Key decrypts the Session Key
Part 3

Hashing Algorithms

Understand Integrity checks with:

a) Message Digests
b) Message Authentication Codes
c) Digital Signatures
Authenticating the Hash

- **Message Digest**
  - Not-Authenticated

- **Message Authentication Code (MAC)**
  - Authenticated Symmetrically
  - Authentication only (*message can be repudiated*)

- **Digital Signatures**
  - Authenticated Asymmetrically
    - Authentication
    - Non-Repudiation
Message Authentication Codes

- Message digest is salted with symmetric key
  - Hash provides integrity
  - Symmetric key provides authenticity

Important! - Does not provide non-repudiation
  - Bob Claims “Alice sent the message”
Message Authentication Codes

Hello Alice,
I love you.
Yours Truly,
Bob

MD5

128 bit MAC
dddd77bbac3025a0afbb8e43706800

128 bit MAC
dddd77bbac3025a0afbb8e43706800

If Bob’s MAC ≠ Alice’s MAC, then document has changed or did not come from Bob

Bob

Alice
Signing a message

Bob’s Private

Hello Alice,
I love you.
Yours Truly,
Bob

128 bit checksum
(Message Digest)
dkdthttbhacdbh2233a3fbba1e45700800

Digital Signature
(Encrypted Message Digest)
Validating the Signature

Hello Alice,
I love you.
Yours Truly, Bob

Digital Signature
(Encrypted Message Digest)

Bob’s Public

Message Digest
07af87c19afcf059205a034646c3

Message Digest
07af87c11cfd5059120da54646c3

HASH

Alice

If Alice’s Digest = Bob’s Digest
then:
1) Document likely not changed – (integrity)
2) Came from Bob – (authentication)
3) Bob cannot deny sending - (non-repudiation)
signedCertificate
- version: v3 (2)
- serialNumber: 0x2b9f7ee5ca25a62514204782753a9bb9
  - signature (shaWithRSAEncryption)
  - issuer: rdnSequence (0)
    - rdnSequence: 3 items (id-at-commonName=Thawte SGC CA)
  - validity
  - subject: rdnSequence (0)
    - rdnSequence: 5 items (id-at-commonName=mail.google.com)
  - subjectPublicKeyInfo
    - algorithm (rsaEncryption)
“Captain, the Federation's x.500 based hierarchical trust model of PKI is very logical. Perhaps we can trust the public Certificate Authorities.”

“But Spock, I have never met Thawte or Verisign. I feel I can trust my friends. Call it a hunch, I trust OpenPGP more.”
PKI Hierarchical Trust Model
Certificate (id-at-commonName=mail.google.com,id-at-organ)
- signedCertificate
  - version: v3 (2)
    - serialNumber: 0xb9f7ee5ca25a62514204782753a9bb9
  - signature (shaWithRSAEncryption)
- issuer: rdnSequence (0)
  - rdnSequence: 3 items (id-at-commonName=Thawte SGC CA)
  - validity
- subject: rdnSequence (0)
  - rdnSequence: 5 items (id-at-commonName=mail.google.com)
- subjectPublicKeyInfo

Frame (558 bytes) Reassembled TCP (1848 bytes)
Why Trust a CA?

RFC-3280 (updated in 4630)

- **Top tier**
  - Internet Policy Registration Authority (IPRA)
    - *Internet PCA Registration Authority (MIT),?*

- **Second tier**
  - Policy Certification Authorities (PCAs)
    - *UNINETT, DFN-PCA, SURFnetPCA*

- **Third tier**
  - Certification Authorities (CAs)
    - *VeriSign, Duetsche Telekom, Thawte, etc.*
Internet PCA Registration Authority

Root Key

Note: The IPRA Certificate has been re-issued. The public key remains the same, but the expiration date has been advanced through 9/15/99.

NOTE: It is not known whether or not the Safekeyper box is Y2K compliant or whether or not we will be able to issue a certificate that expires (or is issued) beyond the year 2000!

I am pleased to inform you that we have (finally) created the Internet Society sponsored "Internet PCA Registration Authority" (IPRA). I have enclosed a uuencoded file that contains its self-signed certificate, as well as a version where it is "exploded" (courtesy of the trivial program which is part of the TIS/PEM distribution) and finally a more human readable version.

In addition to being available on this Web Page we will shortly be submitting an Internet Informational RFC which will contain it.

The IPRA will be operated under the authority of the Internet Society by MIT for a period of time after which physical control will be turned over to Internet Society staff (or other designated party as determined by the Society).

The IPRA Private Key is protected via a Certificate Signature Unit. Click here to read more about this technology.

~Jeff Schiller

You can get the IPRA Certificate in a form downloadable into Netscape version 2.0 (or greater) here: http://bs.mit.edu/ipra.ca.
Internet PCA Registration Authority

HTTP 404 Not Found - Microsoft Internet Explorer

The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:

- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- Open the bs.mit.edu home page, and then look for links to the information you want.
- Click the Back button to try another link.
- Click Search to look for information on the Internet.

HTTP 404 - File not found
Internet Explorer
Certificate Revocation

Compromised Private Keys

- Certificate Revocation Lists (CRL)
- Online Certificate Status Protocol (OCSP)
- Problems:
  - Client checking may be disabled
  - Browsers configured to fail soft
  - Upstream servers may block CRL
  - Compromised CA certificates
  - Algorithms cracked
  - More...
extensions: 4 items

- Extension (id-ce-basicConstraints)
  - Extension Id: 2.5.29.19 (id-ce-basicConstraints)
  - critical: True
  - BasicConstraintsSyntax

- Extension (id-ce-cRLDistributionPoints)
  - Extension Id: 2.5.29.31 (id-ce-cRLDistributionPoints)
  - CRLDistPointsSyntax: 1 item
    - DistributionPoint
      - distributionPoint: fullName (0)
      - fullName: 1 item
        - GeneralName: uniformResourceIdentifier (6)
          - uniformResourceIdentifier: http://crl.thawte.com/ThawteSGCCA.crl

- Extension (id-ce-extKeyUsage)
  - Extension Id: 2.5.29.37 (id-ce-extKeyUsage)

Frame (558 bytes) Reassembled TCP (1848 bytes)
Certificate (id-at-commonName@mail.google.com, id-at-organizationName=Google Inc,)
signedCertificate
  version: v3 (2)
  serialNumber: 0x2b9f7e5ca25a62514204782753a9bb9
  signature (shaWithRSAEncryption)
  issuer: rdnSequence (0)
  validity
  subject: rdnSequence (0)
  subjectPublicKeyInfo
  extensions: 4 items
    Extension (id-ce-basicConstraints)
    Extension (id-ce-cRLDistributionPoints)
    Extension (id-ce-extKeyUsage)
    Extension (id-pe-authorityInfoAccessSyntax)
      Extension Id: 1.3.6.1.5.5.7.1.1 (id-pe-authorityInfoAccessSyntax)
      AuthorityInfoAccessSyntax: 2 items
        AccessDescription
          accessMethod: 1.3.6.1.5.5.7.48.1 (id-pkix.48.1)

  accessLocation: 6
  uniformResourceIdentifier: http://ocsp.thawte.com
Online Certificate Status Protocol

- tbsRequest
  - requestList: 1 item
    - Request
      - reqCert
        - hashAlgorithm (SHA-1)
          - Algorithm Id: 1.3.14.3.2.26 (SHA-1)
          - issuerNameHash: 1e9209aa713c794bca1e931a0a61ad3fd0ba6
          - issuerKeyHash: 3b349a709173b28a1b0cf4e937cdb370329e18
          - serialNumber: 0x2b9f7ee5ca25a62514204782753a9bb9
        - requestExtensions: 1 item
<table>
<thead>
<tr>
<th>Issued To</th>
<th>Issued By</th>
<th>Expiration</th>
<th>Friendly Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail.google.com</td>
<td>UTN-USERFirst-Hardw...</td>
<td>3/14/2014</td>
<td>Fraudulent</td>
</tr>
<tr>
<td>login.live.com</td>
<td>UTN-USERFirst-Hardw...</td>
<td>3/14/2014</td>
<td>Fraudulent</td>
</tr>
<tr>
<td>login.skype.com</td>
<td>UTN-USERFirst-Hardw...</td>
<td>3/14/2014</td>
<td>Fraudulent</td>
</tr>
<tr>
<td>login.yahoo.com</td>
<td>UTN-USERFirst-Hardw...</td>
<td>3/14/2014</td>
<td>Fraudulent</td>
</tr>
<tr>
<td>login.yahoo.com</td>
<td>UTN-USERFirst-Hardw...</td>
<td>3/14/2014</td>
<td>Fraudulent</td>
</tr>
<tr>
<td>login.yahoo.com</td>
<td>UTN-USERFirst-Hardw...</td>
<td>3/14/2014</td>
<td>Fraudulent</td>
</tr>
<tr>
<td>Microsoft Corporation</td>
<td>VeriSign Commercial S...</td>
<td>1/31/2002</td>
<td>Fraudulent, NOT...</td>
</tr>
<tr>
<td>Microsoft Corporation</td>
<td>VeriSign Commercial S...</td>
<td>1/30/2002</td>
<td>Fraudulent, NOT...</td>
</tr>
</tbody>
</table>

Certificate intended purposes

Server Authentication, Client Authentication
Detecting Certificate Authority compromises and web browser collusion

Posted March 22nd, 2011 by ioerror in ssl tls ca tor certificates torbrowser

Thanks to Ian Gallagher, Seth Schoen, Jesse Bums, Chris Palmer, and other anonymous birds for their invaluable feedback on this writeup.

The Tor Project has long understood that the certification authority (CA) model of trust on the internet is susceptible to various methods of compromise. Without strong anonymity, the ability to perform targeted attacks with the blessing of a CA key is serious. In the past, I’ve worked on attacks relating to SSL/TLS trust models and for quite some time, I’ve hunted for evidence of non-academic CA compromise in the wild.

I’ve also looked for special kinds of cooperation between CAs and browsers. Proof of collusion will give us facts. It will also give us a real understanding of the faith placed in the strength of the underlying systems.

Does certificate revocation really work? No, it does not. How much faith does a vendor actually put into revocation, when verifiable evidence of malice is detected or known? Not much, and that’s the subject of this writing.

Last week, a smoking gun came into sight: A Certification Authority appeared to be compromised in some capacity, and the attacker issued themselves valid HTTPS
Where Are We Going?

Life on the Planet Earth, through the instrumentality of the human nervous system, has begun to migrate from the Womb Planet, to escape from gene pools, to establish colonies in high orbit, from whence it can more accessibly contact and communicate with Life in the Galaxy.

Men and women who know from whence they come and where they are going, who share a vision beyond the local-mundane will emerge from the larval gene-pools and as cyber (pilot) individuals, who learn quickly, work effectively, grow naturally, socialize lovingly and evolve gracefully. It is probably true that species coast along on serene stupidity until faced with an evolutionary challenge; at which point individuals leave the primitive collectives and become very smarter very faster. (Timothy Leary -1976)
Top 10 voted Bruce Schneier Facts

When Bruce Schneier observes a quantum particle, it remains in the same state until he has finished observing it.

17646 votes

Bruce Schneier knows Alice and Bob's shared secret.

6579 votes

Vs lbh nfxrq Oehpr Fpuarvre gb qrpelcg guvf, ur'q pehfu lbhe fxhyy jvgu uvf ynhtu.

2048 votes

Most people use passwords. Some people use passphrases. Bruce Schneier uses an epic passpoem, detailing the life and works of seven mythical Norse heroes.

1975 votes

Bruce Schneier's secure handshake is so strong, you won't be able to exchange keys with anyone else for days.

1925 votes

Bruce Schneier once decrypted a box of AlphaBits.
Thank You!

- Improvise
- Adapt
- Overcome