



March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands



SSL Interception Proxies and Transitive Trust

Jeff Jarmoc
Sr. Security Researcher
Dell SecureWorks



About this talk

- History & brief overview of SSL/TLS
- Interception proxies
 - How and Why
- Risks introduced by interception
- Failure modes and impact to risk
- Tools to test
- Disclosure of vulnerable platforms
- Recommendations

Properties of Encryption

- Privacy
- Integrity
- Authenticity

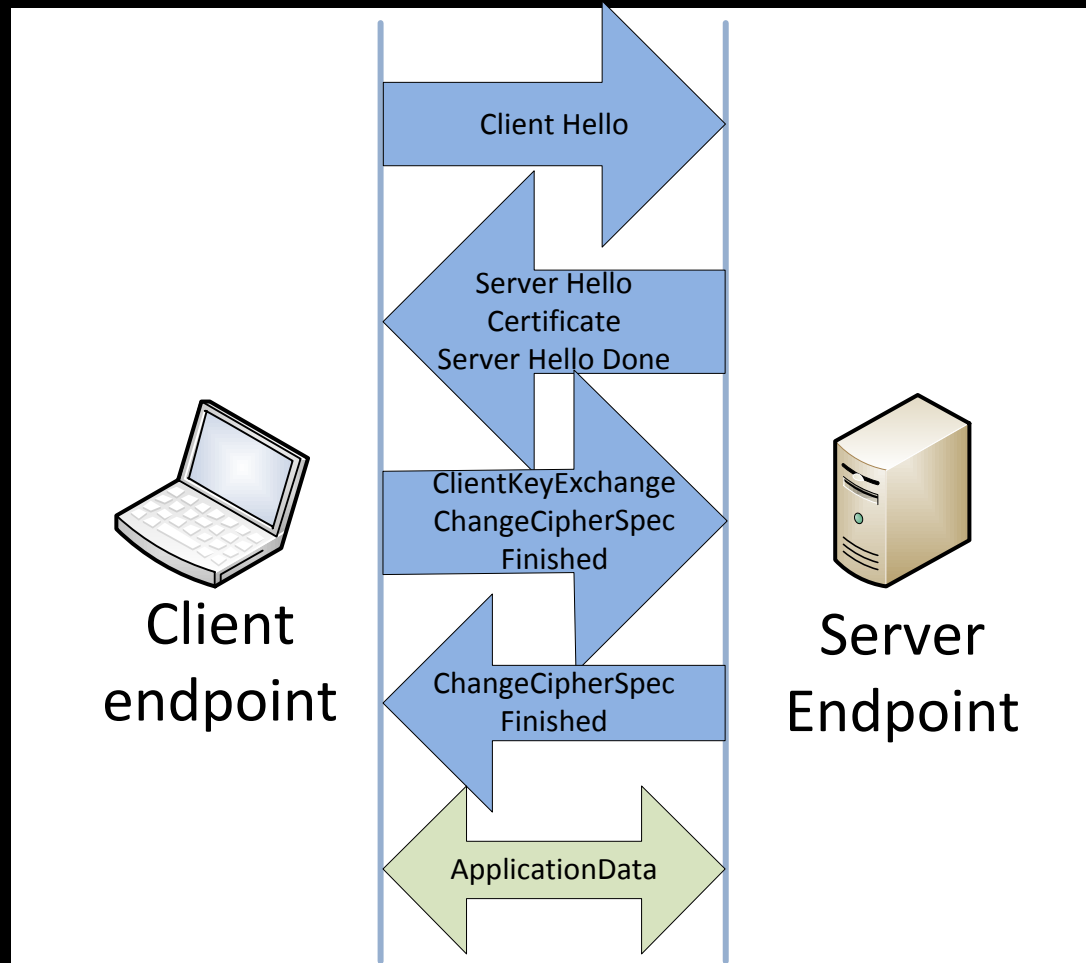


History of SSL

- SSL / TLS
 - SSL v2.0 - Netscape Draft, 1994
 - SSL v3.0 - IETF Draft, 1996
 - TLS v1.0 - RFC 2246, 1999
 - TLS v1.1 - RFC 4346, 2006
 - TLS v1.2 - RFC 5246, 2008
- Related
 - HTTP Over TLS - RFC 2818, 2000
 - X.509 and CRL - RFC 5280, 2008
 - OCSP - RFC5019, 2007



SSL Session Establishment



X.509 Certificate Validation

Responsible for validating certificate trust

- Verify certificate integrity
 - Compare signature to cert hash
- Check for expiration
 - Issue time < Current time < Expiration time
- Check Issuer
 - Trusted? Follow chain to root
- Check revocation via CRL and/or OCSP

Result

Typical Uses

- Privacy
 - Cipher Suite prevents sniffing
- Integrity
 - Cipher Suite prevents modification
- Authenticity
 - Certificate validation ensures identity

Malicious uses

- Privacy
 - Cipher Suite bypasses detection
- Integrity
 - Cipher Suite bypasses prevention
- Authenticity
 - Certificate validation ensures identity

Enterprise Response

- Intercept, Inspect, Filter
 - DLP
 - Web Content Filters
 - Anti-Malware Solutions
 - IDS / IPS
 - NG / DPI Firewalls
 - Endpoint Security Suites

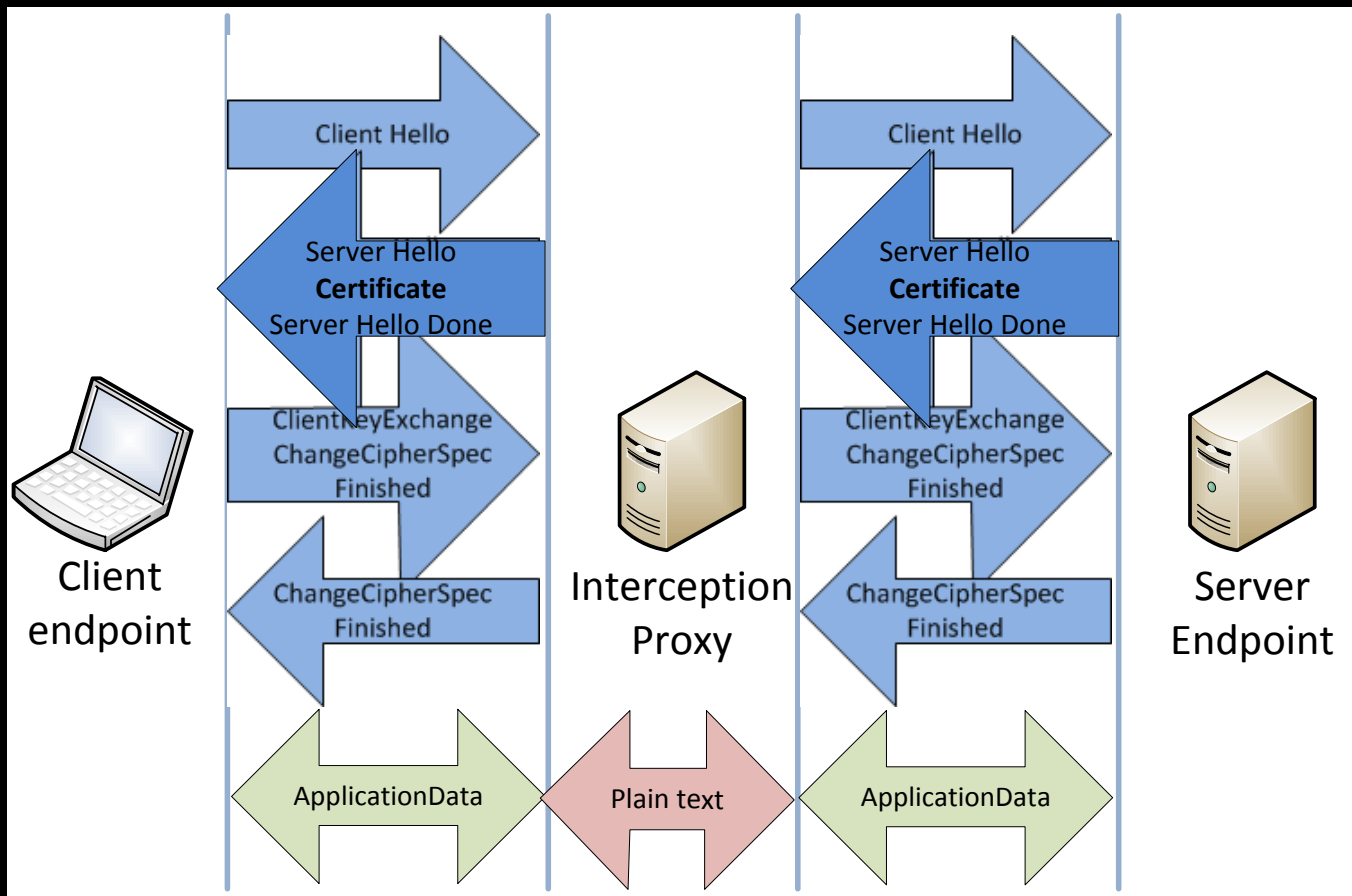


- Broadly termed 'SSL Interception Proxies'

SSL / TLS Interception Proxies

- Man In The Middle
- Negotiate two sessions
 - Act as Client on Server Side
 - Act as Server on Client Side
 - Generate new server key pair on client side
- Disrupt Authenticity to Effect Privacy/Integrity
- End-to-end session becomes two point-to-point sessions

SSL / TLS Interception Proxies



Disrupt Authenticity to Effect Privacy/Integrity

Establishing endpoint trust

- Private CA
 - Must be added as trust root to all endpoints
 - Can pose a logistical challenge
- Public SubCA
 - Delegated public root authority
 - These are sometimes available
 - Trustwave disclosed this, reversed course
 - GeoTrust previously advertise it as GeoRoot
 - Signing Key exposure risks are significant

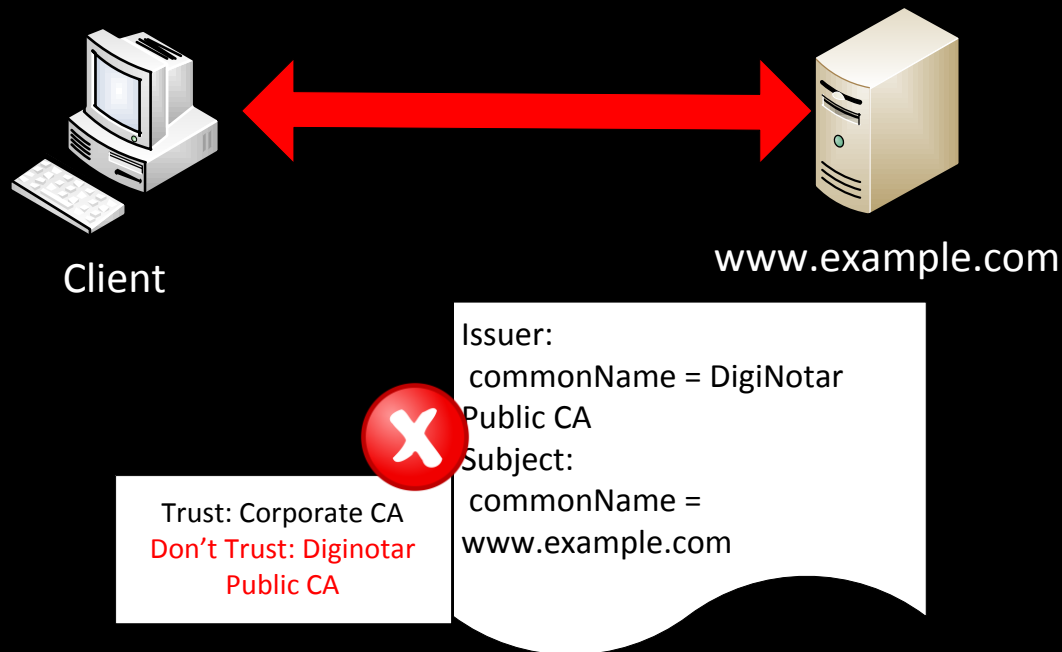


Unintended side effects

- Two separate cipher-suite negotiations
 - May use weaker crypto than endpoints support
- Proxy becomes high-value target
 - Access to clear-text sessions
 - Contains Private Keys
- Legalities – disclosure, user expectations
- **Transitive Trust**
 - Client cannot independently verify server identity
 - Client relies on Proxy's validation of server-side certificate

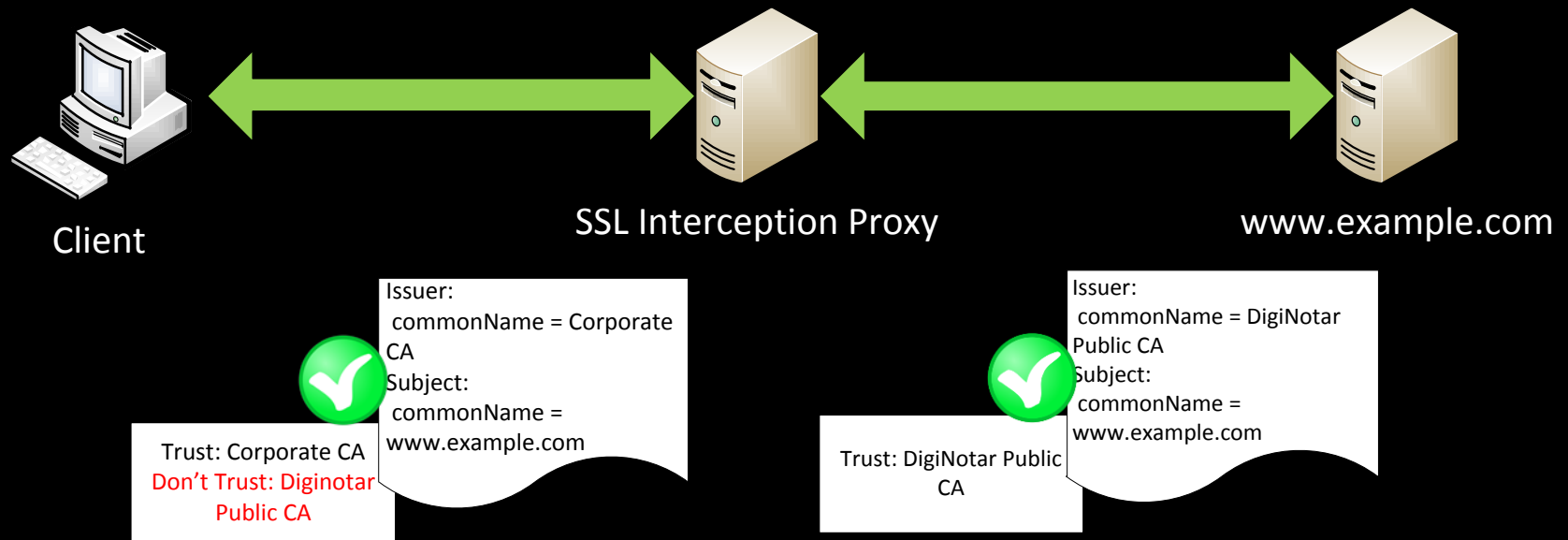
Untrusted Root

- Client does not trust server certificate's CA



Transitive Root Trust

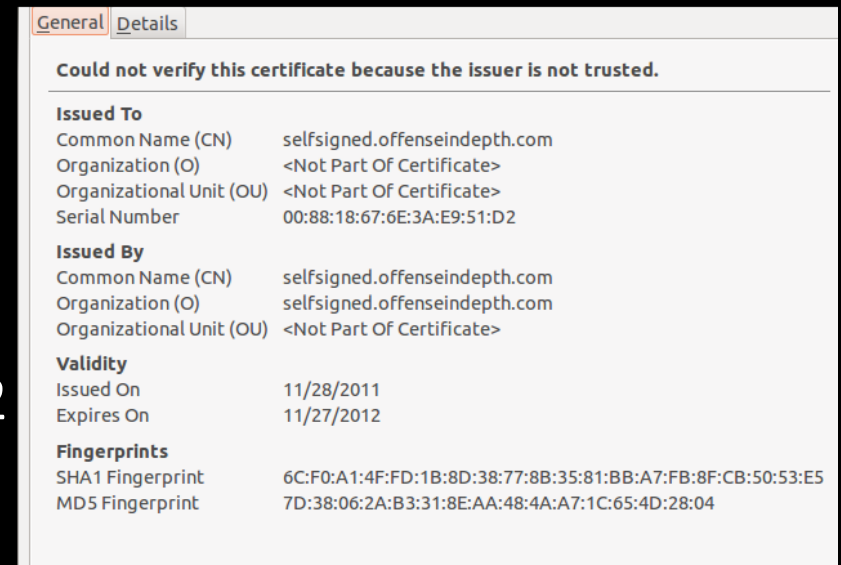
- Proxy trusts Server Certificate's CA
- Client trusts Proxy Certificate's CA



- Therefore, Client trusts Server Certificate's CA

Transitive Trust – X.509

- X.509 Validation flaws can also be transitive
 - Self-signed certificates
 - Expired certificates
 - Revoked certificates
 - Basic constraints
 - Moxie Marlinspike, 2002
 - Null prefix injection
 - Moxie Marlinspike, 2009
 - Dan Kaminsky, 2009



General Details

Could not verify this certificate because the issuer is not trusted.

Issued To

Common Name (CN)	selfsigned.offenseindepth.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	00:88:18:67:6E:3A:E9:51:D2

Issued By

Common Name (CN)	selfsigned.offenseindepth.com
Organization (O)	selfsigned.offenseindepth.com
Organizational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	11/28/2011
Expires On	11/27/2012

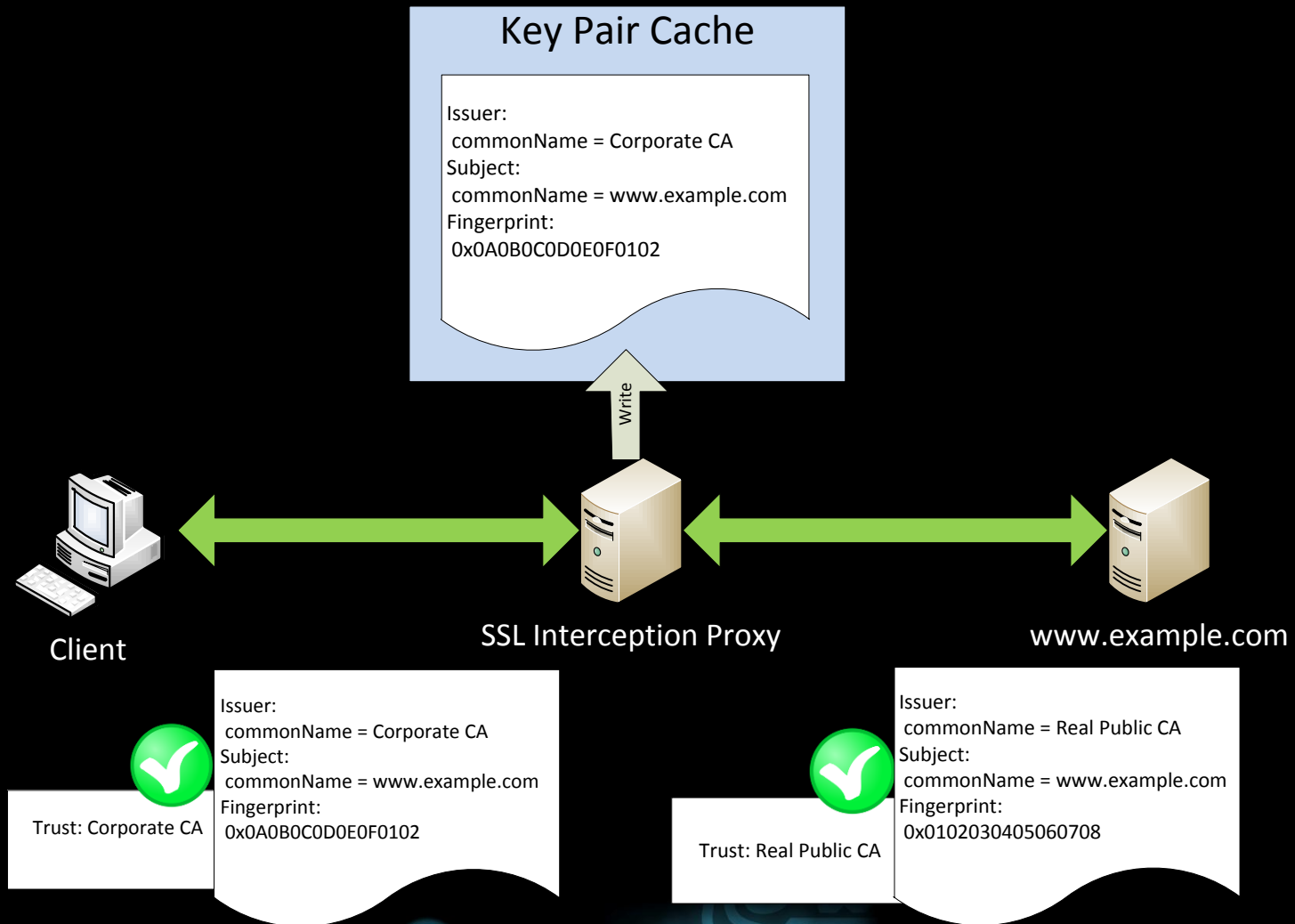
Fingerprints

SHA1 Fingerprint	6C:F0:A1:4F:FD:1B:8D:38:77:8B:35:81:BB:A7:FB:8F:CB:50:53:E5
MD5 Fingerprint	7D:38:06:2A:B3:31:8E:AA:48:4A:A7:1C:65:4D:28:04

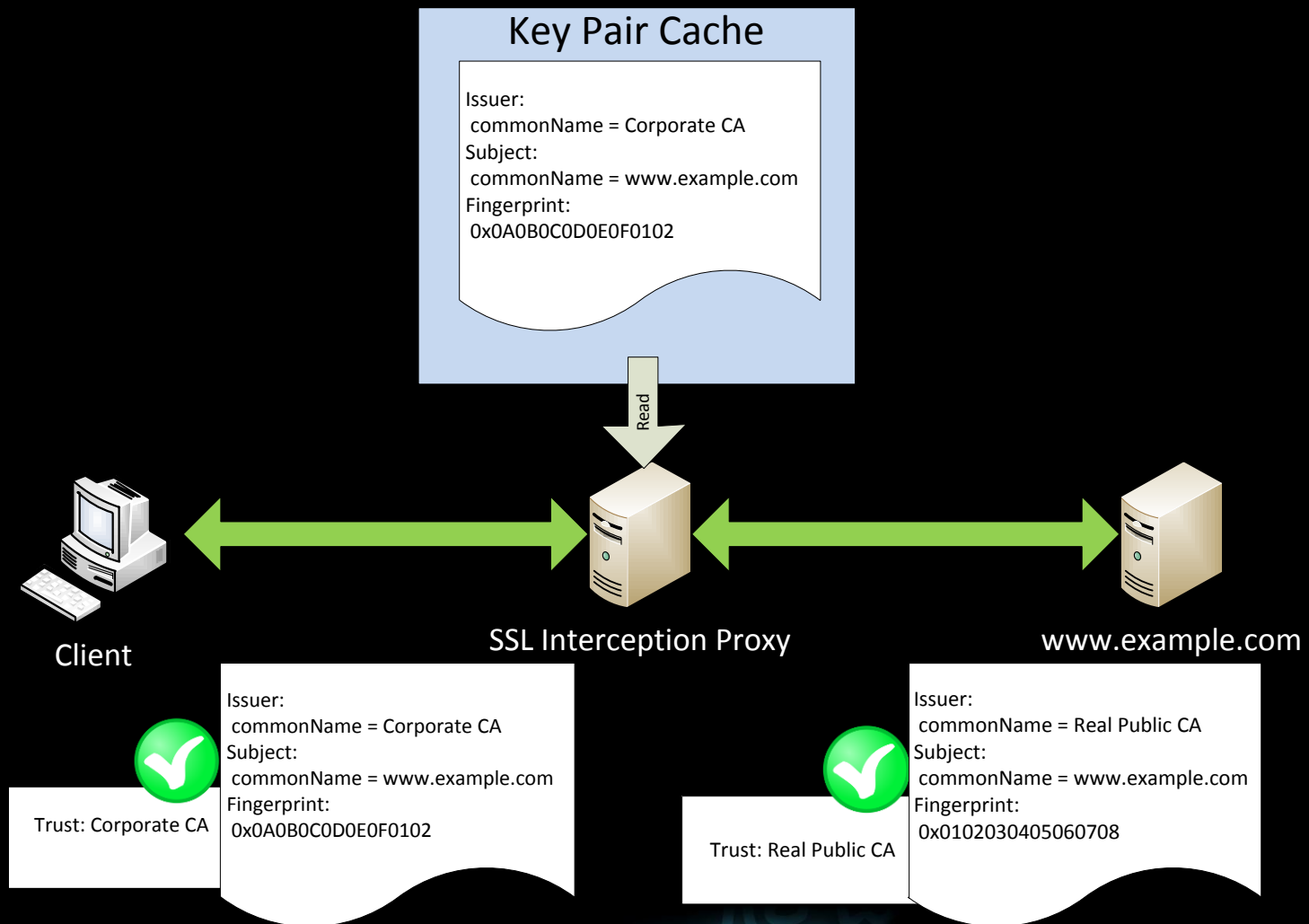
Key pair caching

- Dynamically generating SSL key pairs is computationally expensive
- Network-based interception proxies handle large numbers of connections
- Caching generated key pairs helps performance
- How cached key pairs are indexed is important

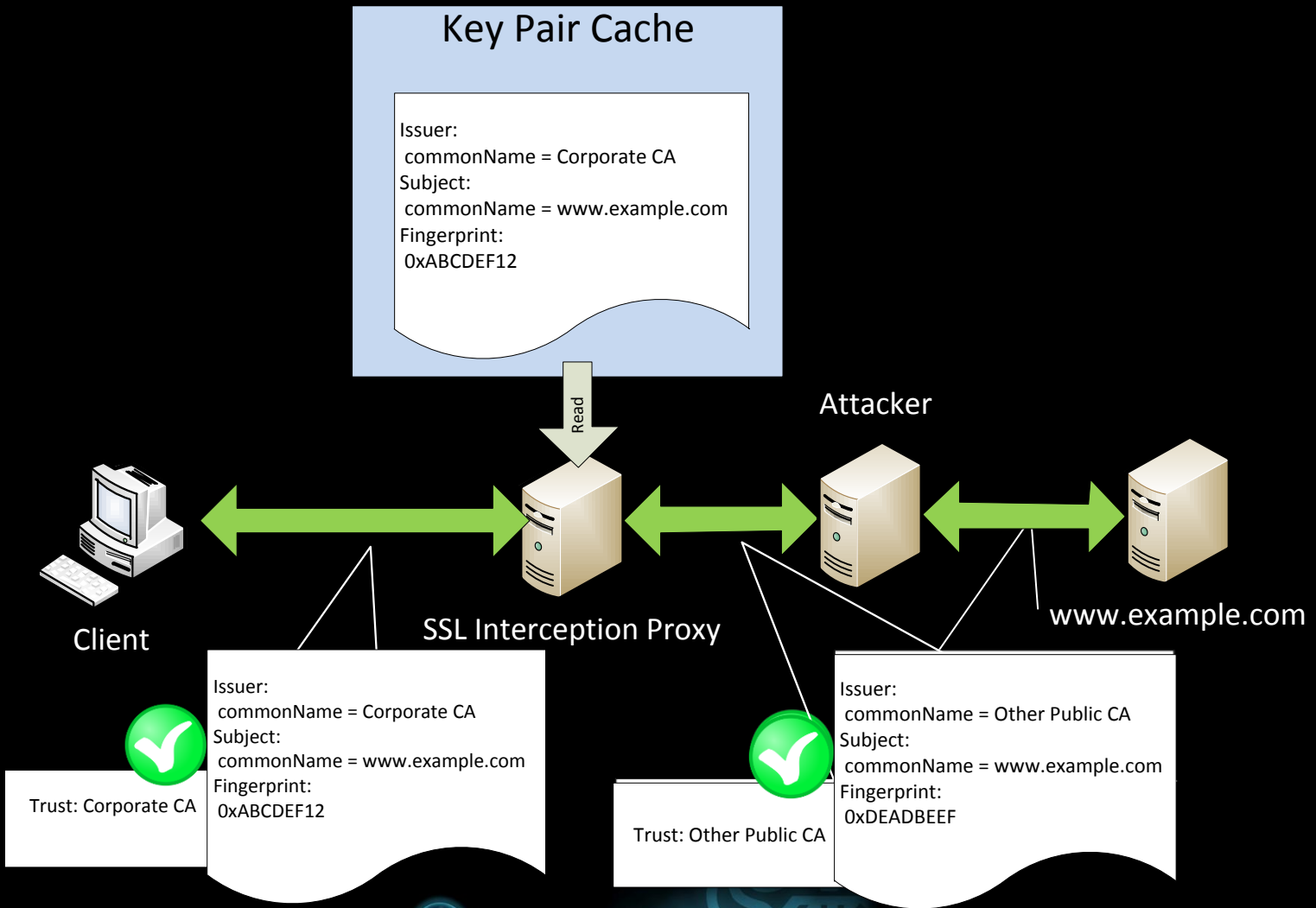
Key pair caching – First visit



Key pair caching – later visits



Key pair caching – attack

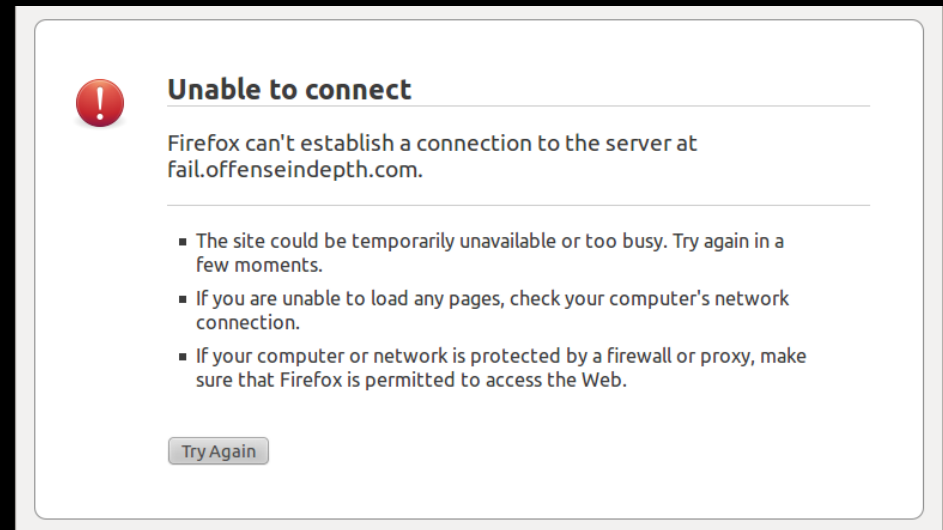


Failure Modes

- If a certificate is invalid, how do we proceed?
- No RFC specification for MITM interception
- Three common approaches
 - Fail Closed
 - Friendly Error
 - Passthrough
- Each has trade offs.

Failure Modes – Fail Closed

- Terminate both sessions immediately.
 - Security++;
- No reason given
 - User_Experience--;
- Out of band agents
 - Provide info
 - Deployment burden



Failure Modes – Friendly Error

- Terminate server side session immediately
- Provide friendly message on client side session
 - In context of requested site
 - Include content from the certificate?
 - Malformed certificate as web attack vector
 - XSS in context of requested page via invalid cert?
 - Allow user override?
 - CSRF to disable validation?

Failure Modes – Passthrough

- Most common for name and expiry failures
- Continue server side session
- Client-side Certificate uses identical data
 - Relies on client-side validation routines
 - Downstream interception or unusual user-agents can combine to cause unexpected behaviors
 - Generally preserves user-experience / warnings
 - But without visibility into the original cert
 - Users often make poor choices

Testing for common issues

<https://sslltest.offenseindepth.com>

- Visit from a client behind proxy
 - Table lists vulnerabilities
 - CSS includes from host for each vuln
 - Host certs are invalid to demonstrate vuln
 - If vulnerable, CSS loads and flags vulnerability
- Shows request headers
- Certificate warnings
 - In passthrough failure mode decision will affect results.

Client visiting directly

SSL Test - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SSL Test

offenseindepth.com https://ssltest.offenseindepth.com

Test	Result
Mismatched CN	NOT VULNERABLE
Unknown CA	NOT VULNERABLE
Self Signed	NOT VULNERABLE
Expired	NOT VULNERABLE
Basic Constraints	NOT VULNERABLE
Revoked	NOT VULNERABLE
Null Char (Must Trust CA)	NOT VULNERABLE

[Null cert CA](#)

Host: ssltest.offenseindepth.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:10.0.2) Gecko/20100101 Firefox/10.0.2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Cache-Control: max-age=0

Same client via proxy

Test	Result
Mismatched CN	NOT VULNERABLE
Unknown CA	VULNERABLE
Self Signed	VULNERABLE
Expired	NOT VULNERABLE
Basic Constraints	VULNERABLE
Revoked	VULNERABLE
Null Char (Must Trust CA)	NOT VULNERABLE

[Null cert CA](#)

Connection: keep-alive
Host: ssltest.offenseindepth.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:10.0.2) Gecko/20100101 Firefox/10.0.2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: __utma=73784140.234610485.1308884376.1308884376.1308884376.1
X-IMForwards: 20
Via: 1.1 [REDACTED]



Cisco IronPort Web Security Appliance

- Self-Signed Certificates Accepted
 - No CVE, Cisco Bug ID 77544 for mitigations
- Unknown CA Roots Accepted
 - No CVE, Cisco Bug ID 77544 for mitigations

Invalid Certificate Handling:	Certificate Error	Drop	Decrypt	Monitor
		Select all	Select all	Select all
	Expired			✓
	Mismatched Hostname			✓
	Unrecognized Root Authority			✓
	All other error types			✓
<i>No end-user notification will be provided for dropped HTTPS connections. Use this setting with caution. If the connection is not dropped, an equivalent certificate will be generated.</i>				

Cisco IronPort Web Security Appliance

- Lack of CRL or OCSP checking
 - CVE-2012-1316 – Cisco Bug ID 71969
- Basic Constraints not validated
 - CVE-2012-1326
- Keypair Cache weaknesses
 - CVE-2012-0334 – Cisco Bug ID 78906

Cisco IronPort Web Security Appliance

- All findings apply to version 7.1.3-014
- Patches forthcoming
 - V7.5 - 07/2012
 - V7.7 - 07/2012
- No UI for managing trust roots
 - Patches addressed recent revocations
 - Passthrough Failure Mode
 - Problems in combination with certain downstream validators



Astaro Security Gateway

- Lack of CRL or OCSP checking
 - Firmware 8.300 Pattern 23977
- Sophos / Astaro Security Team Response
 - Design Decision
 - CRL / OCSP is broken in general
 - Monitoring ongoing developments for future response

Astaro Security Gateway

- Friendly Error failure mode
- Includes support for managing trust roots
- Includes support for managing certificate blacklists
- Updates to both pushed frequently

No known issues

- Checkpoint Security Gateway R75.20
- Microsoft Forefront TMG 2010 SP2
- Include support for managing trust roots
- Fail Closed in all tested scenarios



Recommendations - Implementers

- Patch regularly
- Test proxies prior to deployment
- Consider security and user-experience
- Inform end users of interception
- Be aware of trust roots, be ready to adapt
- Harden hosts running proxies, monitor closely
- Consider failure modes
- Realize that interception has consequences

Recommendations - Developers

- Allow administrators to manage trust roots
 - Blacklist specific certs, etc.
- Use secure default settings
 - Administrators should accept risks of less secure settings if necessary
- Test systems under attack scenarios
- Be wary of aiding attacks against authenticity
- Consider update and patch deployments
- Secure private keys



March 14-16, 2012

NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands



PLEASE COMPLETE THE SPEAKER FEEDBACK SURVEYS.

THIS WILL HELP SPEAKERS TO IMPROVE AND FOR BLACK HAT TO MAKE BETTER DECISIONS REGARDING CONTENT AND PRESENTERS FOR FUTURE EVENTS.

Questions?



SSL Interception Proxies and Transitive Trust

Jeff Jarmoc
Sr. Security Researcher
Dell SecureWorks

