CERT.be

M3AAWG
MESSAGING MALWARE MOBILE

BetterCrypto · org

Applied Crypto Hardening

David Durvaux

Brussels, 12th June 2014

Why better crypto?

The NSA

The only part of government that actually listens.

But of course...

- It is not only the NSA, who intercepts
- Other nations now have a blueprint (thanks to Snowden) in case they did not have the technical skills yet
- Criminals now have a blueprint,...
- Everyone has!
- So, what can we do?

Don’t give them anything for free

It’s your home, your fight!

Who (authors of bettercrypto)

Wolfgang Breyha (uni VIE),
David Durvaux (CERT.be),
Tobias Dussa (KIT-CERT),
L. Aaron Kaplan (CERT.at),
Florian Mendel (IAIK/A-Sit)
Christian Mock (coretec),
Daniel Kovacic (A-Trust),
Manuel Koschuch (FH Campus Wien),
Adi Kriegisch (VRVis),
Ramin Sabet (A-Trust),
Aaron Zauner (azet.org),
Pepi Zawodsky (maclemon.at),

And many other contributors!!

Agenda

- Introduction to BetterCrypto project
- Practical Settings
- Testing
- Conclusion

BetterCrypto

Why?

- Crypto is cryptic
- A lot of difficult concepts
- A lot of algorithms
- A lot of parameters
- …

The Idea

- Really difficult for systems administrators
  - A “cookbook” can help!
    - That’s BetterCrypo

That's not…

- A crypto course
- A static document

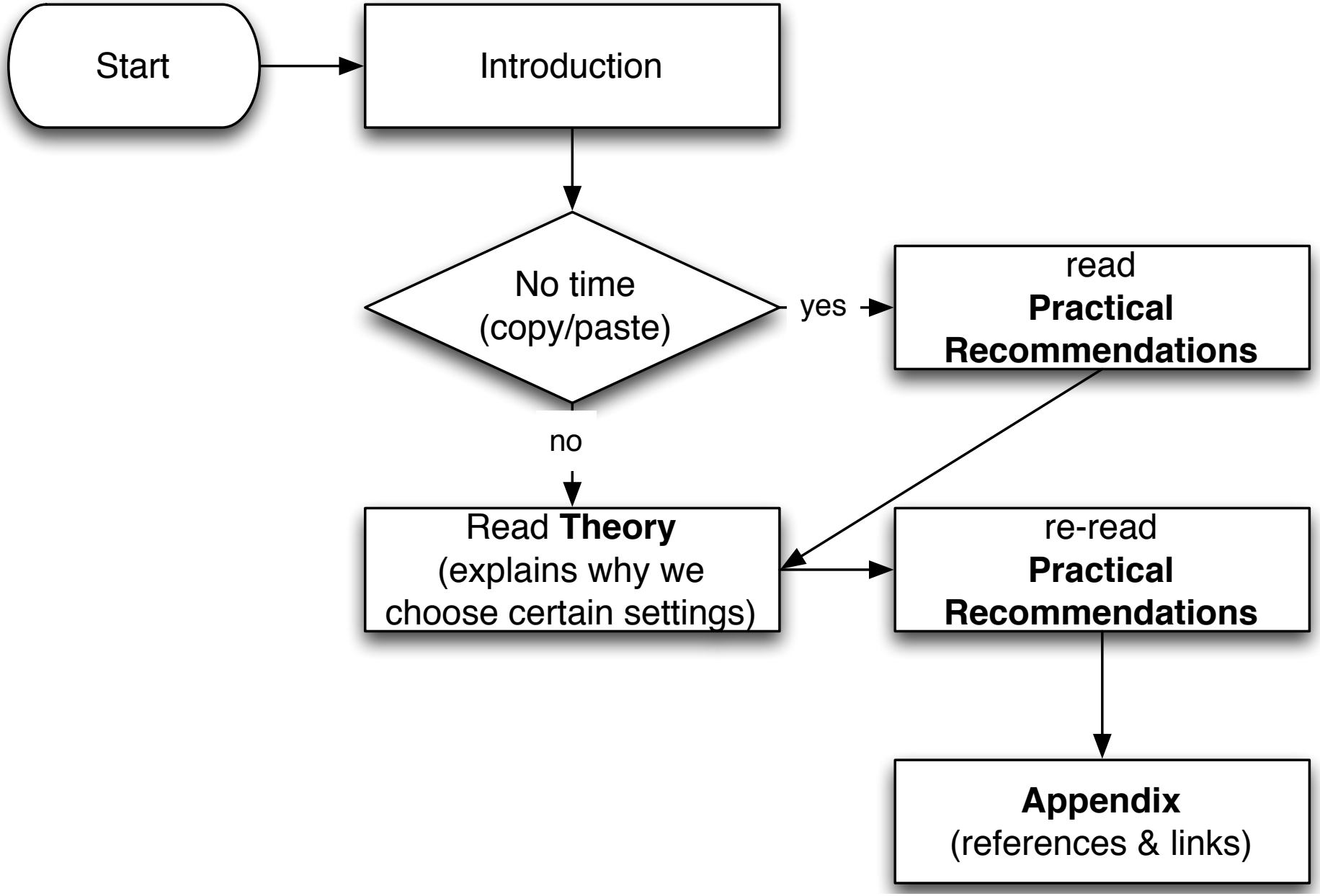
In brief

- Community effort to produce best common practices for typical servers
- Continuous effort
- From diverse areas of expertise: sysadmins, cryptologists, developers, IT security pros
- Open Source (CC-BY-SA)
- Open to comments / suggestions / improvements

2 parts

- First part = configurations
  - The most important part
  - Cover as many tools as possible
- Second part = theory
  - Explain and justify choose we made
    - Transparency

How to use the bettercrypto guide?



BetterCrypto CipherSuite

- 2 cipher suites
  - version A
    - stronger
    - fewer supported clients
  - version B
    - weaker
    - more “universal”

Some general thoughts on settings

- General
  - Disable SSL 2.0 (weak algorithms)
  - Disable SSL 3.0 (BEAST vs IE/XP)
  - Enable TLS 1.0 or preferably better
  - Disable TLS-Compression (SSL-CRIME Attack)
  - Implement HSTS (HTTP Strict Transport Security)

Cipher Suite A

- TLS 1.2
- Perfect forward secrecy / ephemeral Diffie Hellman
- Strong MACs (SHA-2) or
- GCM as Authenticated Encryption scheme

ID	OpenSSL Name	Version	KeyEx	Auth	Cipher	MAC
0xC09F	DHE-RSA-AES256-GCM-SHA384	TLSv1.2	DH	RSA	AESGCM(256)	AEAD
0xC06B	DHE-RSA-AES256-SHA256	TLSv1.2	DH	RSA	AES(256) (CBC)	SHA256
0xC030	ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH	RSA	AESGCM(256)	AEAD
0xC028	ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES(256) (CBC)	SHA384

CiperSuite B

- TLS 1.2, TLS 1.1, TLS 1.0
- Allowing SHA-1

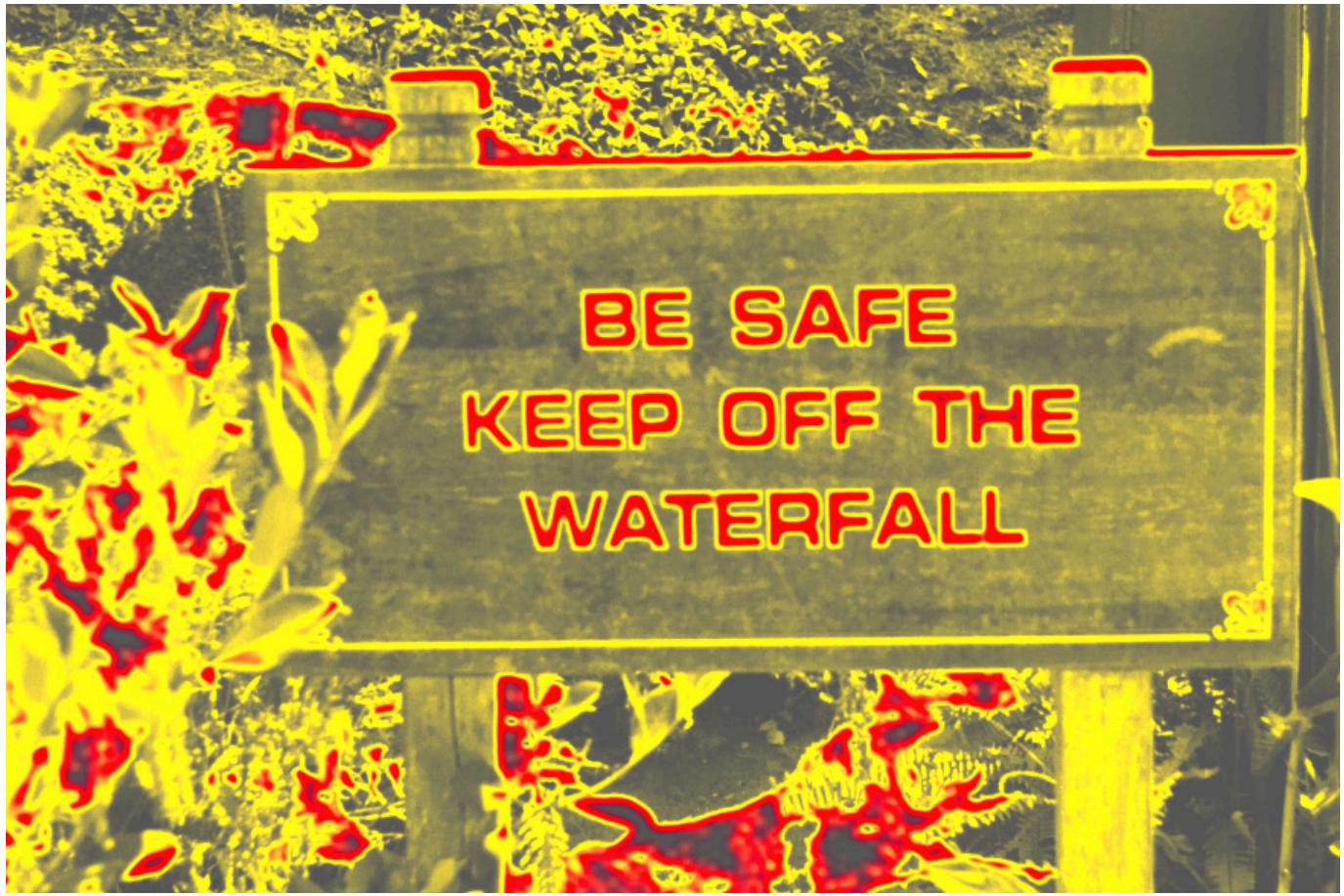
Cipher Suite B

ID	OpenSSL Name	Version	KeyEx	Auth	Cipher	MAC
0x009F	DHE-RSA-AES256-GCM-SHA384	TLSv1.2	DH	RSA	AESGCM(256)	AEAD
0x006B	DHE-RSA-AES256-SHA256	TLSv1.2	DH	RSA	AES(256)	SHA256
0xC030	ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH	RSA	AESGCM(256)	AEAD
0xC028	ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES(256)	SHA384
0x009E	DHE-RSA-AES128-GCM-SHA256	TLSv1.2	DH	RSA	AESGCM(128)	AEAD
0x0067	DHE-RSA-AES128-SHA256	TLSv1.2	DH	RSA	AES(128)	SHA256
0xC02F	ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	ECDH	RSA	AESGCM(128)	AEAD
0xC027	ECDHE-RSA-AES128-SHA256	TLSv1.2	ECDH	RSA	AES(128)	SHA256
0x0088	DHE-RSA-CAMELLIA256-SHA	SSLv3	DH	RSA	Camellia(256)	SHA1
0x0039	DHE-RSA-AES256-SHA	SSLv3	DH	RSA	AES(256)	SHA1
0xC014	ECDHE-RSA-AES256-SHA	SSLv3	ECDH	RSA	AES(256)	SHA1
0x0045	DHE-RSA-CAMELLIA128-SHA	SSLv3	DH	RSA	Camellia(128)	SHA1
0x0033	DHE-RSA-AES128-SHA	SSLv3	DH	RSA	AES(128)	SHA1
0xC013	ECDHE-RSA-AES128-SHA	SSLv3	ECDH	RSA	AES(128)	SHA1
0x0084	CAMELLIA256-SHA	SSLv3	RSA	RSA	Camellia(256)	SHA1
0x0035	AES256-SHA	SSLv3	RSA	RSA	AES(256)	SHA1
0x0041	CAMELLIA128-SHA	SSLv3	RSA	RSA	Camellia(128)	SHA1
0x002F	AES128-SHA	SSLv3	RSA	RSA	AES(128)	SHA1

Compatibility (B suite)

Handshake Simulation

Bing Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Chrome 31 / Win 7	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Firefox 10.0.12 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Firefox 17.0.7 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Firefox 21 / Fedora 19	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Firefox 24 / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Googlebot Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 6 / XP No FS [1] No SNI [2]			Fail[3]
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 8 / XP No FS [1] No SNI [2]			Fail[3]
IE 8-10 / Win 7	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 11 / Win 7	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 11 / Win 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Java 6u45 No SNI [2]			Fail[3]
Java 7u25			Fail[3]
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
OpenSSL 1.0.1e	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Opera 17 / Win 7	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Safari 6 / iOS 6.0.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Safari 6.0.4 / OS X 10.8.4	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Safari 7 / OS X 10.9	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Tor 17.0.9 / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Yahoo Slurp Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256

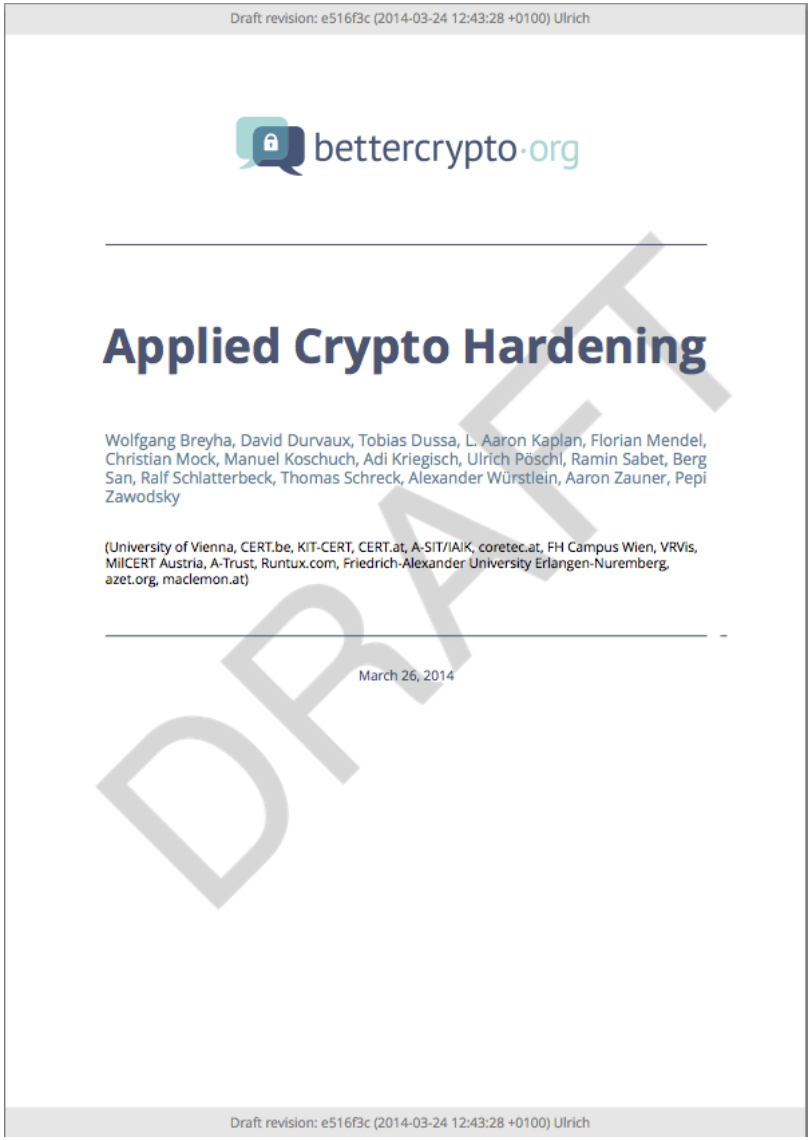


Practical Settings

Tools covered

- Web servers
- SSH
- Mail Servers
- VPNP
- GP/GPG
- IPMI/ILO
- Instant Messaging
- RDBMS
- Proxy
- Kerberos
- …

Let's have a look



Draft revision: e516f3c (2014-03-24 12:43:28 +0100) Ulrich

bettercrypto.org

Applied Crypto Hardening

Wolfgang Breyha, David Durvaux, Tobias Dussa, L. Aaron Kaplan, Florian Mendel, Christian Mock, Manuel Koschuch, Adi Kriegisch, Ulrich Pöschl, Ramin Sabet, Berg San, Ralf Schlatterbeck, Thomas Schreck, Alexander Würstlein, Aaron Zauner, Pepi Zawodsky

(University of Vienna, CERT.be, KIT-CERT, CERT.at, A-SIT/IAIK, coretec.at, FH Campus Wien, VRVis, MilCERT Austria, A-Trust, Runtux.com, Friedrich-Alexander University Erlangen-Nuremberg, azet.org, maclemon.at)

March 26, 2014

DRAFT

Draft revision: e516f3c (2014-03-24 12:43:28 +0100) Ulrich

Mail Encryption

- GPG / PGP – end to end protection
  - Use public / private crypto to protect your emails
  - Chain of trust
  - Independent of the mail client / transport layer
  - Can be used to verify author and/or protect content
- STARTTLS for SMTP – in transit

Mail Server

- SMTP make use of opportunistic TLS
- 3 modes for mailservers
  - Mail Submission Agent (MSA)
  - Receiving Mail Transmission Agent (MX)
  - Sending Mail Transmission Agent (SMTP client)

Mail Server

- Correct DNS configuration without CNAMEs
- Enable encryption
- NO self-signed certificates

SMTP client mode

- Hostname used as HELO must match the PTR RR
- Setup a client certificate
- Common name or alternate subject name must match the PTR RR
- Don‘t touch cipher suite

MSA

- Listen on port 587
- Enforce SMTP AUTH
- No SMTP AUTH on unencrypted connections
- (use recommended cipher suites)

Postfix: MX & SMTP client

- In main.cf
  - Enable opportunistic TLS

```
# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
# use 0 for Postfix >= 2.9, and 1 for earlier versions
smtpd_tls_loglevel = 0
# enable opportunistic TLS support in the SMTP server and client
smtpd_tls_security_level = may
smtp_tls_security_level = may
smtp_tls_loglevel = 1
# if you have authentication enabled, only offer it after STARTTLS
smtpd_tls_auth_only = yes
tls_ssl_options = NO_COMPRESSION
```

Postfix: MSA

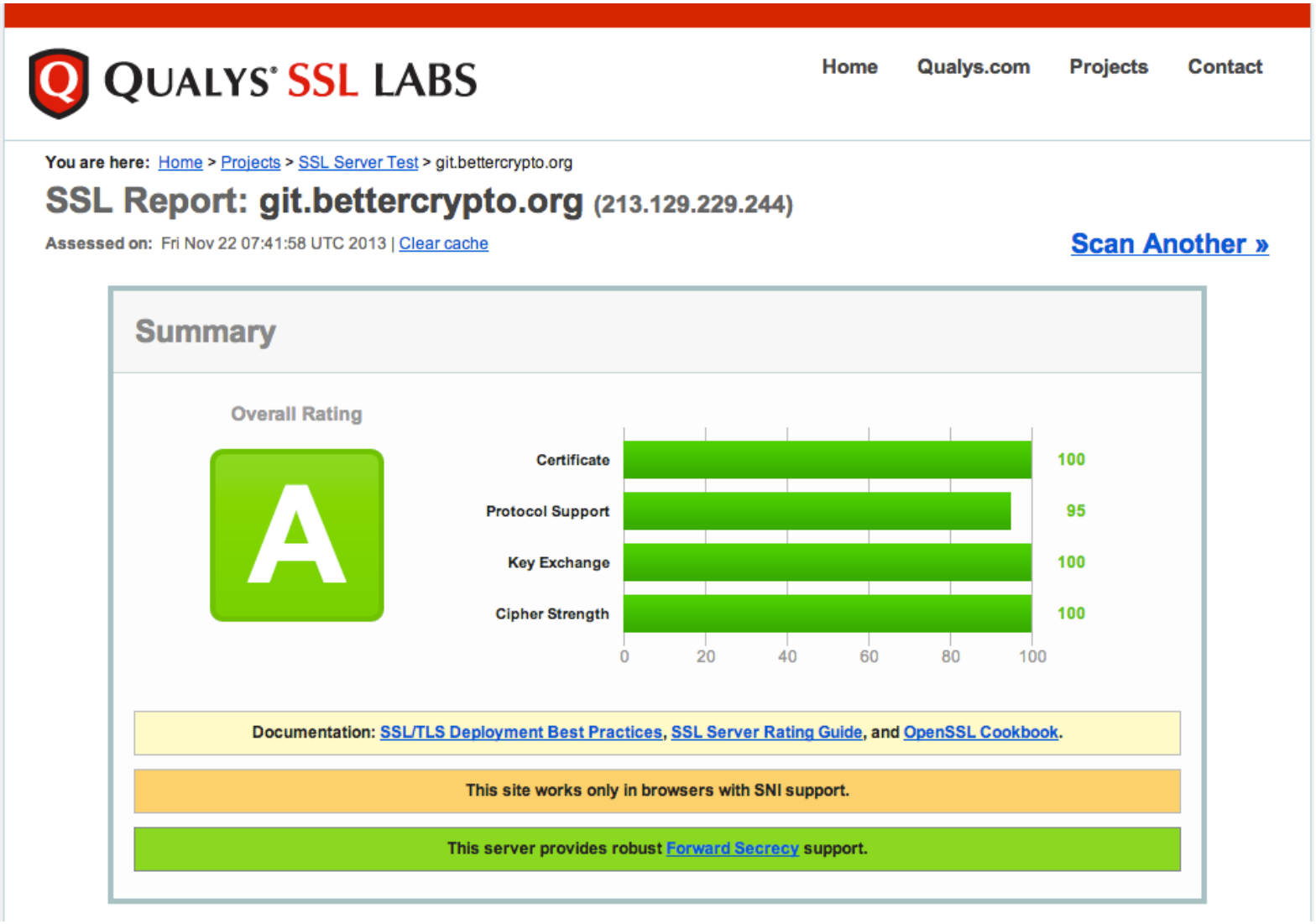
- Define ciper suite:

```
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3
smtpd_tls_mandatory_ciphers=high
tls_high_cipherlist=EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:\
  \EECDH+aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL\
  \:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256\
  \-SHA:CAMELLIA128-SHA:AES128-SHA
```

- Configure MSA SMTP:

```
submission inet n - - - - smtpd
  -o smtpd_tls_security_level=encrypt
  -o tls_preempt_cipherlist=yes
```

Tools: ssllabs



ssllabs (2)

Configuration

Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 4096 bits (p: 512, g: 1, Ys: 512) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 4096 bits (p: 512, g: 1, Ys: 512) FS	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 4096 bits (p: 512, g: 1, Ys: 512) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 4096 bits (p: 512, g: 1, Ys: 512) FS	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256

Handshake Simulation

Bing Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Chrome 31 / Win 7	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Firefox 10.0.12 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Firefox 17.0.7 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Firefox 21 / Fedora 19	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Firefox 24 / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Googlebot Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 6 / XP No FS [1] No SNI [2]			Fail[3]
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 8 / XP No FS [1] No SNI [2]			Fail[3]
IE 8-10 / Win 7	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 11 / Win 7	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 11 / Win 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Java 6u45 No SNI [2]			Fail[3]
Java 7u25			Fail[3]
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
OpenSSL 1.0.1e	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Opera 17 / Win 7	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Safari 6 / iOS 6.0.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Safari 6.0.4 / OS X 10.8.4	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Safari 7 / OS X 10.9	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Tor 17.0.9 / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Yahoo Slurp Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256

The Conclusion.

The Feavour works up towards Madness, and will ſcarcely endure to be touch'd. And what hope is there of Health when the *Patient* ſtrikes in with the Diſeaſe, and flies in the Face of the *Remedy*? Can Religion retrive us? Yes, when we don't deſpiſe it. But while our *Notions* are naught, our *Lives* will hardly be otherwiſe. What can the *Aſſiſtance* of the Church ſignify to thoſe *who* are more

Conclusion

Future ideas

- Configuration Generator (online)
- Other tools
- Other protocols

Current state as of 2014/05/31

- ✓ Solid basis with Variant (A) and (B)
- ✓ Public draft was widely presented at the CCC, RIPE meeting, IETF Strint workshop, Linuxdays, ..., M3AAWG
- Section „cipher suites“ still a bit messy, needs more work
- Need to convert to HTML

How to participate

- We need: cryptologists, sysadmins, hackers
- Read the document, find bugs
- Subscribe to the mailing list
- Understand the cipher strings Variant (A) and (B) before proposing some changes
- If you add content to a subsection, make a sample config with variant (B)
- Git repo is world-readable
- We need:
  - Add content to an subsection from the TODO list
    → send us diffs
  - **Reviewers!**

Thank you!

- BetterCrypto.org
- https://git.bettercrypto.org/ach-master.git
- http://lists.cert.at/cgi-bin/mailman/listinfo/ach

- Contact
  - david@autopsit.org — @ddurvaux