Humboldt University

Computer Science Department
Systems Architecture Group
http://sar.informatik.hu-berlin.de

Modern SSL/TLS-Setup with Apache

Elias Rohrer, Tim Dittler, Moritz Wedel
({rohrer,dittler,wedel}@informatik.hu-berlin.de)

IT-Security Workshop 2013

[27.09.2013]

Outline

1. **Motivation**: Recent attacks on SSL/TLS
2. **Conclusions:** ECC, Forward Secrecy and Key-Pinning
3. **Project**: Conception and Demonstration
4. **Benchmarks:** Impact of TLS and ciphers
5. **Perspective**: What needs to be done...?
6. **Sources**

Humboldt Universität Informatik
Systems Architecture Group
http://sar.informatik.hu-berlin.de

Recent Attacks on SSL/TLS - 1

- **BEAST** (Browser Exploit Against SSL/TLS)
  - Exploits the Cipher Block Chaining mode (CBC) in correlation with the IV.
  - Workaround: Inserting empty fragments into the message in order to randomize the IV (by OpenSSL)
  - Fixed: TLS1.1 and 1.2

- **CRIME** (Compression Ratio Info-leak Made Easy):
  - Uses SSL/TLS Data-Compression (Deflate or gzip) to extract secrets out of HTTP-Requests
  - Turn off TLS-Compression! (Done by all newer Browsers/Webservers)

Humboldt Universität Informatik
Systems Architecture Group
http://sar.informatik.hu-berlin.de

Recent Attacks on SSL/TLS - 2

- **TIME** (Timing Info-leak Made Easy)
  - Uses HTTP-Responses and the compressed and encrypted payload's size to get information about the plaintext
  - Chosen-plaintext-attack which breaks SOP (Same Origin Policy) through injecting JavaScript in multimedia tags like *img*.
  - Support and respect 'X-Frame-Options'

- **BREACH** (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext)
  - Similar to CRIME, but using HTTP-Compression
  - Most useful to get CSRF-Token (Cross-Site-Request-Forgery)
  - Turn off HTTP-Compression? NO! But temporarily disable Django's Gzip-Compression...

Humboldt Universität Informatik
Systems Architecture Group
http://sar.informatik.hu-berlin.de

Recent Attacks on SSL/TLS - 3

- **Lucky13**
  - New attack on TLS-Data-Decryption timing-bug in CBC-Mode
  - Further development of *padding oracle attack*
  - Fixed by TLS1.1? (Closing session if decryption fails) NO!
  - Fixed by TLS1.2? (Always checks the MAC) – NO!
    - But it got AES-GCM/CCM

- **RC4 Biases in TLS**
  - Strong biases in the first 257 bytes of encryption which will allow recovery of roughly the first 200 bytes of plaintext.
  - Limiting Session ID lifetime and throttle client initiated renegotiations and connections from individual IP addresses
  - Phase out RC4 – focus on TLS 1.2 and AES-GCM

Humboldt Universität Informatik
Systems Architecture Group
http://sar.informatik.hu-berlin.de

Elliptic curve cryptography (ECC)

- Use a 2048 or 4096 Bit Key? It might be better to use ECC – the same strength with 224 Bits (and they might even be faster)

- ECDH - Elliptic Curve Diffie–Hellman-Keyagreement
- ECDSA – for digital signatures

- Usage in **Apache**: Its possible to use SSLCertificate's in parallel:

```
SSLCertificateFile "@rel_sysconfdir@/server.crt"
SSLCertificateFile "@rel_sysconfdir@/server-dsa.crt"
SSLCertificateFile "@rel_sysconfdir@/server-ecc.crt"
```


Humboldt Universität Informatik
Systems Architecture Group
http://sar.informatik.hu-berlin.de

Forward Secrecy

- Ensures that a session key deduced from a key will not be compromised if the private keys is compromised in the future.
- Uses (elliptic curve) Diffie–Hellman-Keyagreement
- In theory, Transport Layer Security (TLS) can choose appropriate ciphers since SSLv3
- OpenSSL supports perfect forward secrecy using elliptic curve Diffie–Hellman since version 1.0, with a computational overhead of approximately 15%.

Key-Pinning

- Certificates are usually validated by checking the signature hierarchy

- Pinning is the process of associating a host with their expected *X509* certificate or public key. Once a certificate or public key is known for a host, the certificate or public key is associated or 'pinned' to the host.
  - “Trust pinned certificates only?”

- Two IETF-Drafts:
  - Public Key Pinning Extension for HTTP (HPKP)
  - Trust Assertions for Certificate Keys (TACK)

Humboldt Universität Informatik
Systems Architecture Group
http://sar.informatik.hu-berlin.de

Conclusions

- TLS1.1/1.2 isn't supported by most browsers - but this is the only solution!

- Until then: Use latest versions of server software and browsers, use strong cipher suites and prevent yourself from using RC4
  - Use Diffie-Hellman ciphers to obtain (perfect) forward secrecy (Prefer ECDHE over DHE)

- Watch out for Key-Pinning becoming stable

Humboldt Universität Informatik
Systems Architecture Group
http://sar.informatik.hu-berlin.de

wasupTLS

- **Goal**: provide an Apache2 configuration for websites with sensible data
  - It must work *today* and not exclude any users (Instead users with unsafe browsers should be warned.)

- The project consists of three parts which should be used together:
  - Apache2 config file
  - Server-side script to export TLS information
  - Client-side script to warn users with unsafe browsers

- Fork at https://github.com/t2d/wasuptls

Humboldt Universität Informatik
Systems Architecture Group
http://sar.informatik.hu-berlin.de

wasupTLS: Decisions

- Based on stable software (Debian wheezy, OpenSSL 1.0.1e and Apache 2.4)
- Export TLS information via SSI
- BEAST is considered to be mitigated client-side, Priority is Forward Secrecy -> no RC4
- Prefer ECDHE over DHE
- HTTP Strict Transport Security
- No Key-Pinning as it isn't stable at the moment.

Humboldt Universität Informatik
Systems Architecture Group
http://sar.informatik.hu-berlin.de

wasupTLS: Apache Config

- SSLProtocol -ALL +SSLv3 +TLSv1 +TLSv1.1 +TLSv1.2

- SSLCipherSuite ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:ECDH+3DES:DH+3DES:RSA+AES:RSA+3DES:!ADH:!AECDH:!MD5:!DSS:!aNULL

- SSLHonorCipherOrder on
- SSLCompression off

- Header append Strict-Transport-Security "max-age=15768000 ; includeSubDomains"
- Header always append X-Frame-Options "sameorigin"

Humboldt Universität Informatik
Systems Architecture Group
http://sar.informatik.hu-berlin.de

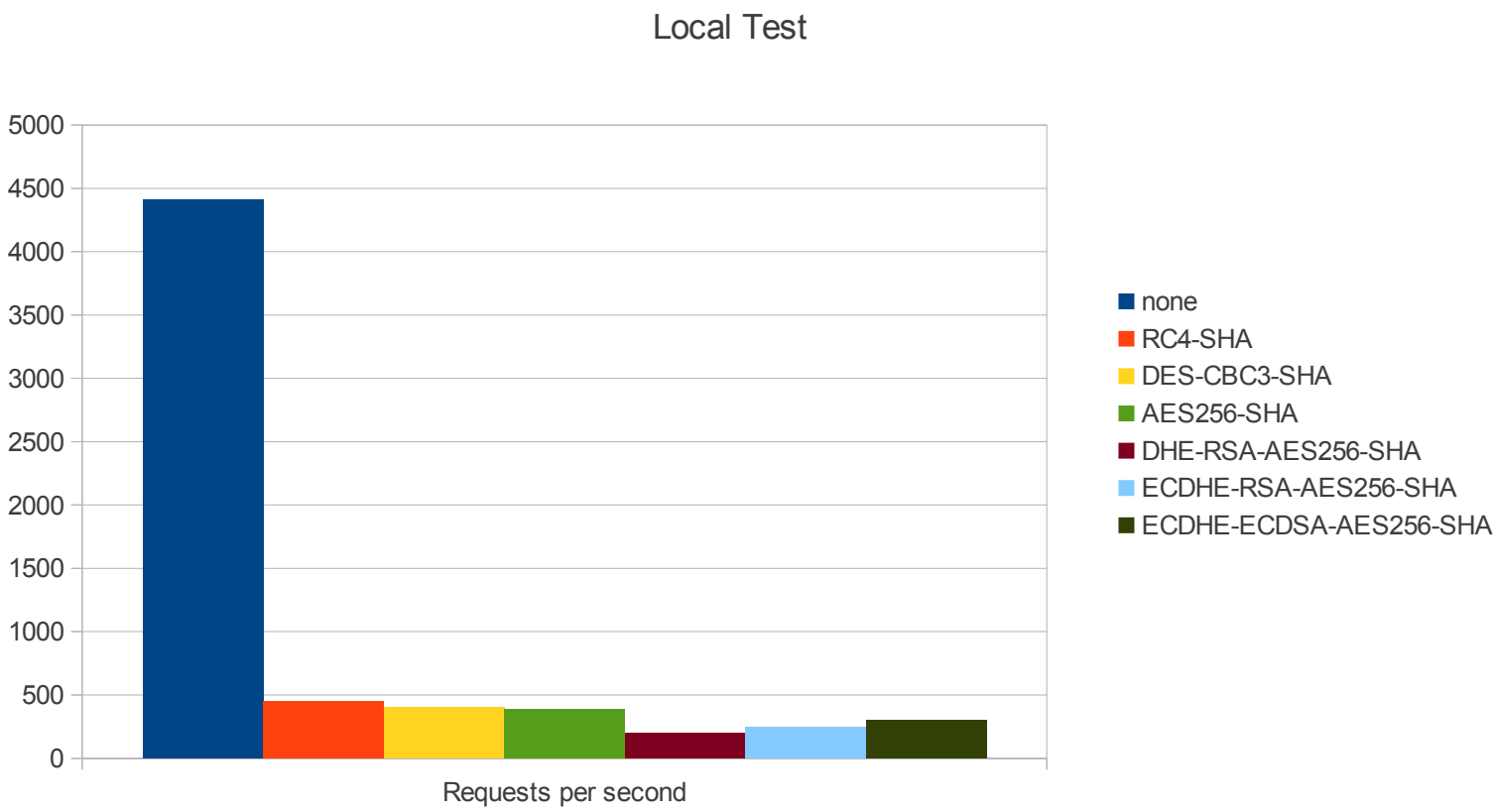
wasupTLS: JavaScript

- Tests if cipher suite is using
  - Forward Secrecy
  - No SSLv3
  - No RC4
  - No 3DES
- If not, we warn the user with a popup containing information about her_his vulnerability.

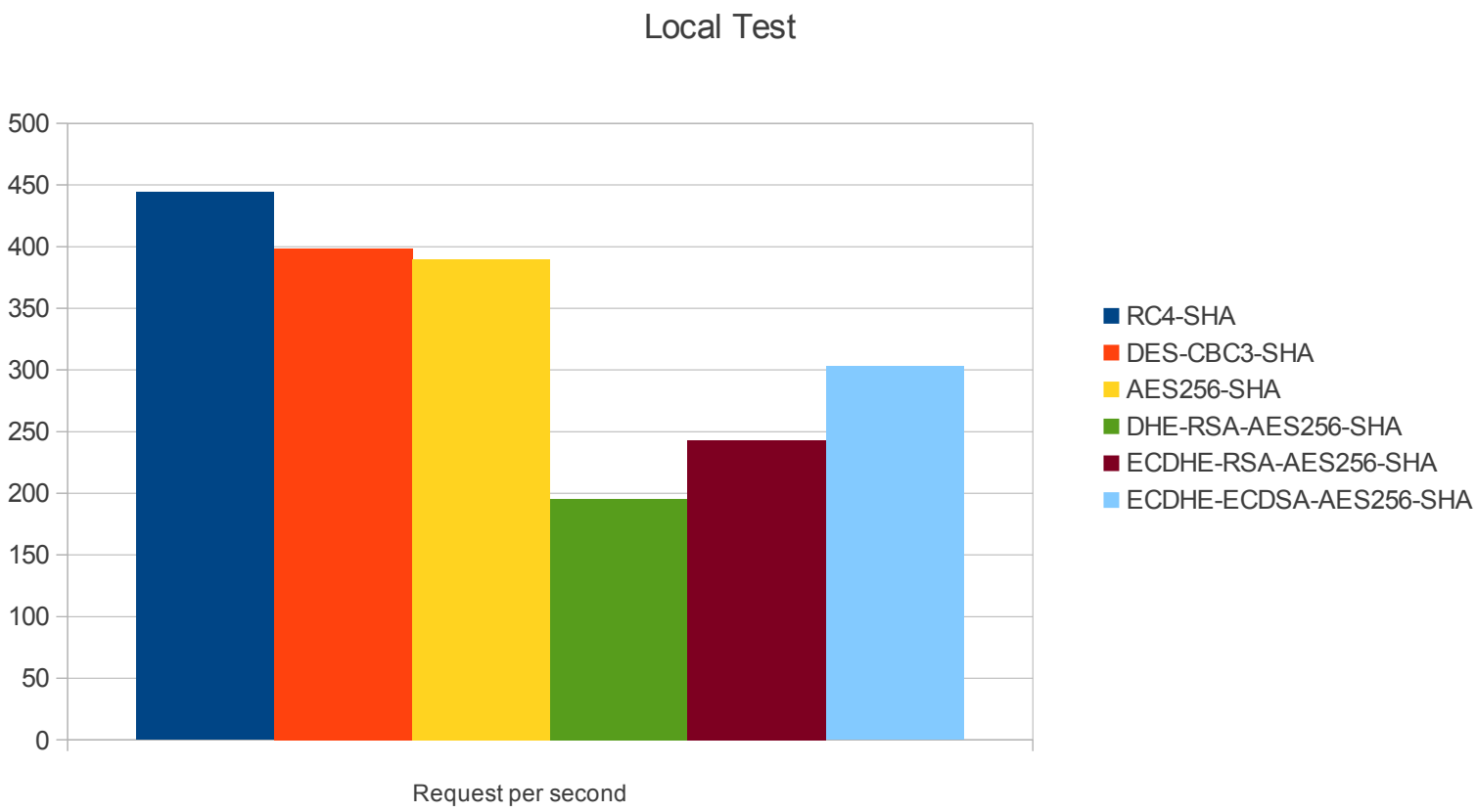
- DEMO

Humboldt Universität Informatik
Systems Architecture Group
http://sar.informatik.hu-berlin.de

Benchmark - 1


Local Test
5000
4500
4000
3500
3000
2500
2000
1500
1000
500
0
Requests per second
none
RC4-SHA
DES-CBC3-SHA
AES256-SHA
DHE-RSA-AES256-SHA
ECDHE-RSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA

Benchmark - 2


Local Test
500
450
400
350
300
250
200
150
100
50
0
Request per second
RC4-SHA
DES-CBC3-SHA
AES256-SHA
DHE-RSA-AES256-SHA
ECDHE-RSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA

Benchmark - 3

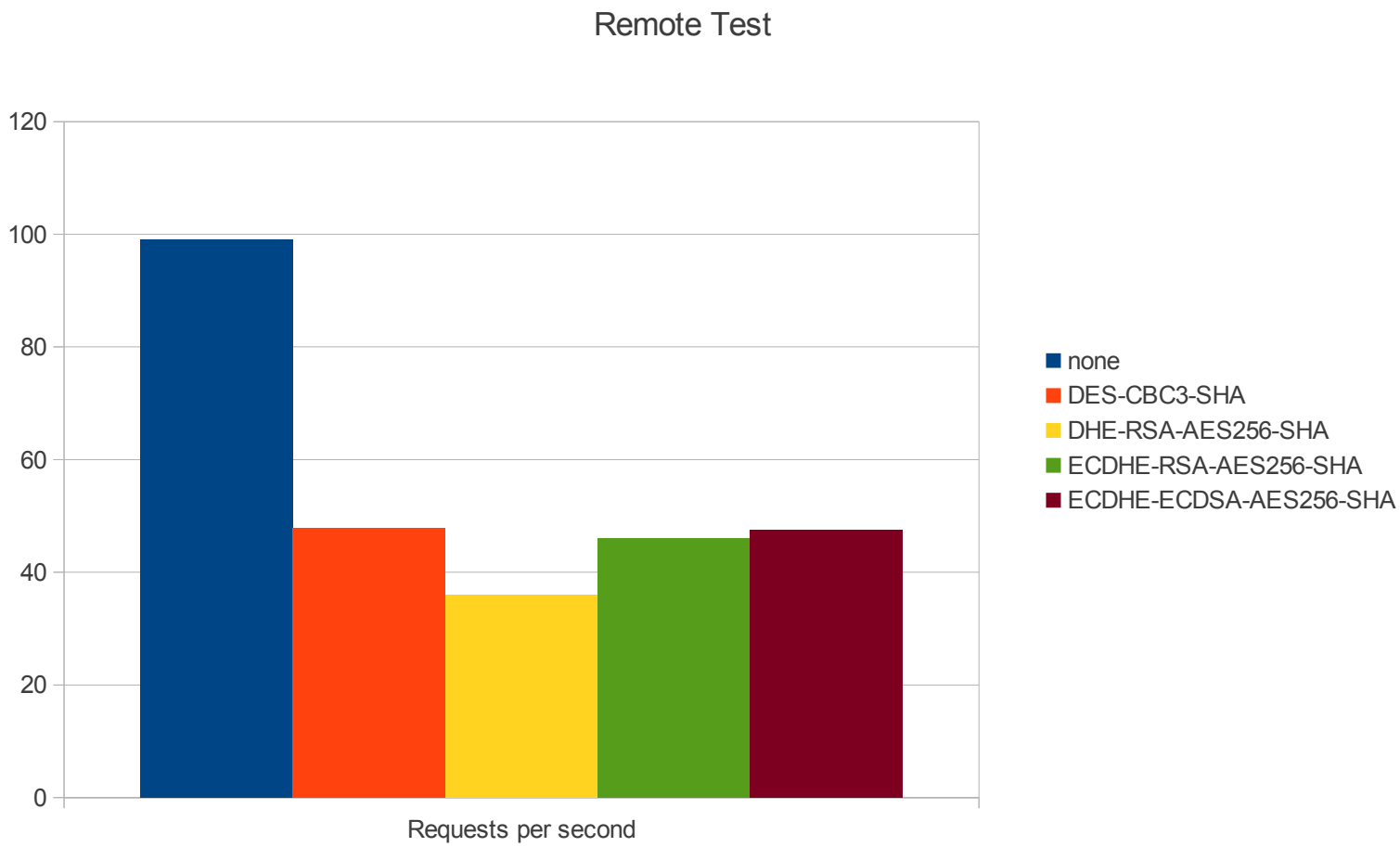
Filter: ip.addr == 83.223.73.60 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
557	12.193268	141.20.	83.223.	TCP	74	37543 > https [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=31293509 TSecr=0 WS=128
559	12.196213	83.223.	141.20.	TCP	74	https > 37543 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=154689132 TSe
560	12.196227	141.20.	83.223.	TCP	66	37543 > https [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=31293510 TSecr=154689132
561	12.196326	141.20.	83.223.	TLSv1.1	291	Client Hello
562	12.199376	83.223.	141.20.	TCP	66	https > 37543 [ACK] Seq=1 Ack=226 Win=15552 Len=0 TSval=154689133 TSecr=31293510
563	12.206597	83.223.	141.20.	TLSv1.1	1514	Server Hello
564	12.206632	83.223.	141.20.	TCP	825	[TCP Previous segment lost] [TCP segment of a reassembled PDU]
565	12.206640	83.223.	141.20.	TCP	1514	[TCP Out-Of-Order] [TCP segment of a reassembled PDU]
566	12.206650	141.20.	83.223.	TCP	66	37543 > https [ACK] Seq=226 Ack=1449 Win=17536 Len=0 TSval=31293513 TSecr=154689134
567	12.206660	141.20.	83.223.	TCP	78	[TCP Dup ACK 566#1] 37543 > https [ACK] Seq=226 Ack=1449 Win=17536 Len=0 TSval=31293513 TSecr
568	12.206676	141.20.	83.223.	TCP	66	37543 > https [ACK] Seq=226 Ack=3656 Win=20480 Len=0 TSval=31293513 TSecr=154689134
569	12.210152	141.20.	83.223.	TLSv1.1	216	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
570	12.214656	83.223.	141.20.	TLSv1.1	348	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
571	12.215198	141.20.	83.223.	TLSv1.1	231	Application Data
572	12.220789	83.223.	141.20.	TLSv1.1	732	Application Data, Application Data
573	12.221945	141.20.	83.223.	TCP	66	37543 > https [FIN, ACK] Seq=541 Ack=4604 Win=26240 Len=0 TSval=31293516 TSecr=154689138
574	12.224897	83.223.	141.20.	TCP	66	https > 37543 [FIN, ACK] Seq=4604 Ack=542 Win=17696 Len=0 TSval=154689139 TSecr=31293516
575	12.224953	141.20.	83.223.	TCP	66	37543 > https [ACK] Seq=542 Ack=4605 Win=26240 Len=0 TSval=31293517 TSecr=154689139

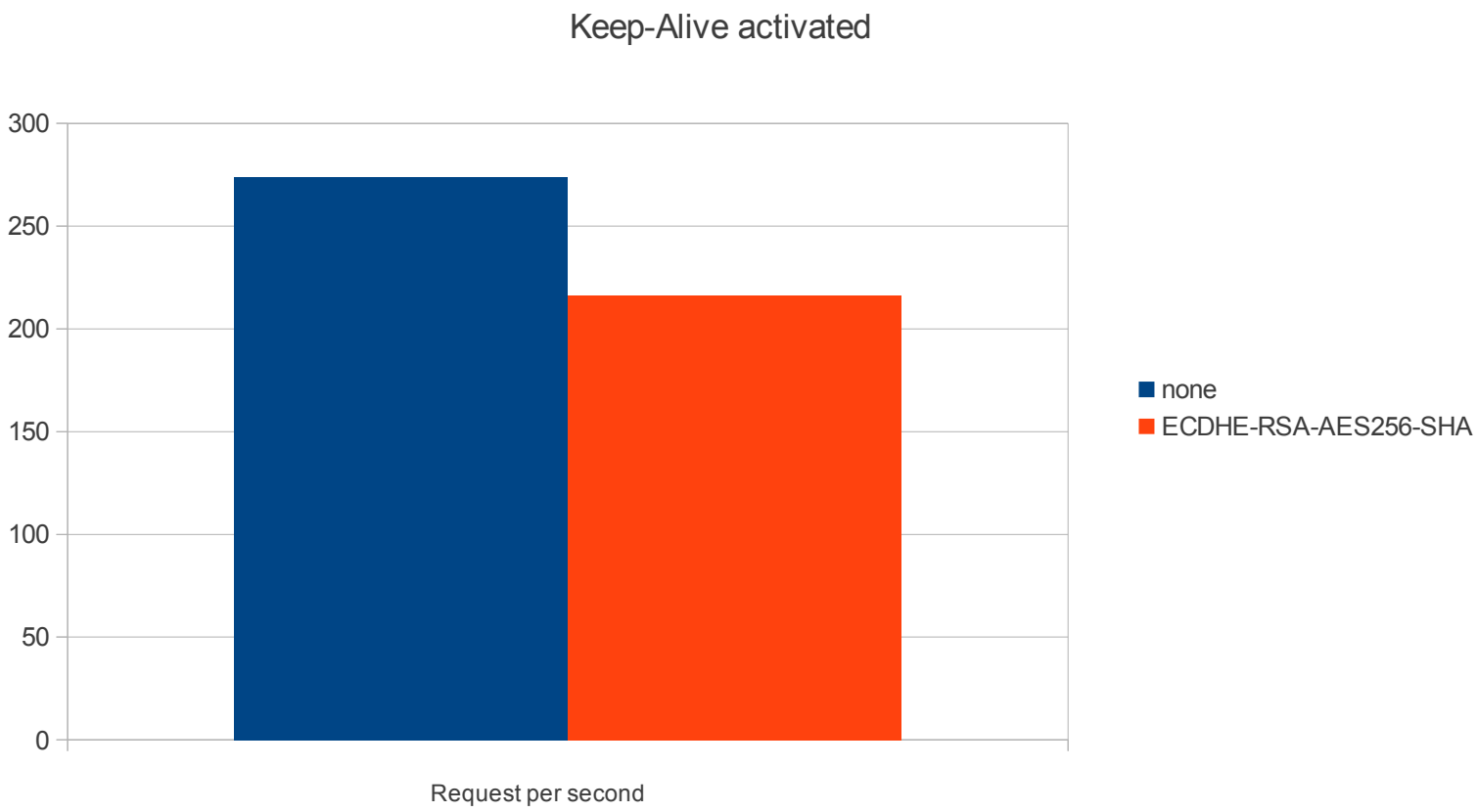
HTTP: 10 packets/request

HTTPS: 18 packets/request

Benchmark - 4


Remote Test
120
100
80
60
40
20
0
Requests per second
none
DES-CBC3-SHA
DHE-RSA-AES256-SHA
ECDHE-RSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA

Benchmark - 5


Keep-Alive activated
300
250
200
150
100
50
0
Request per second
none
ECDHE-RSA-AES256-SHA

Perspective...

- What needs to be done...?
  - Key-Pinning
  - Push upgrade process to TLS1.2
  - Get rid of RC4

  - Tune sites for TLS
  - “Gmail switched to using HTTPS for everything by default […] we had to deploy no additional machines and no special hardware.”

    https://www.imperialviolet.org/2010/06/25/overclocking-ssl.html

- Watch SPDY/HTTP2
  - Reduced amount of roundtrips

Humboldt Universität Informatik
Systems Architecture Group
http://sar.informatik.hu-berlin.de

Sources

- https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.3.pdf
- http://www.heise.de/security/artikel/Forward-Secrecy-testen-und-einrichten-1932806.html
- http://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/
- https://github.com/ioerror/duraconf
- https://www.imperialviolet.org/2010/06/25/overclocking-ssl.html
- https://httpd.apache.org/docs/2.4/mod/mod_ssl.html
- https://isecpartners.com/media/106031/ssl_attacks_survey.pdf