

Signatur-Algorithmen einer Zertifikatskette anzeigen

Da mit SHA1 signierte Zertifikate inzwischen als unsicher eingestuft werden, habe ich nach einer einfachen Möglichkeit gesucht, wie ich herausfinden kann, welche meiner Zertifikate davon betroffen sind.

Es reicht allerdings nicht, nur das Serverzertifikat auszutauschen. Es sollte auch die Zertifikatskette (Certificate chain) untersucht werden, da ggf. auch das Zwischen- und CA-Zertifikat ausgetauscht werden muss. Wobei das CA-Zertifikat natürlich nur von der CA, bzw. dem Herausgeber selbst (Geotrust, Thawte, etc) ausgetauscht werden kann.

Aufgerufen wird das Script so (kann dann z.B. in einer Schleife mit euren verschiedenen Servern/Ports gefüttert werden):

```
# ./check-ssl-chain.sh www.heise.de:443
Signature Algorithm: sha256WithRSAEncryption
  Subject: C=DE, ST=Niedersachsen, L=Hannover, O=Heise Zeitschriften Verlag GmbH und Co KG
Signature Algorithm: sha256WithRSAEncryption

Signature Algorithm: sha256WithRSAEncryption
  Subject: C=US, O=thawte, Inc., CN=thawte SHA256 SSL CA
Signature Algorithm: sha256WithRSAEncryption
```

oder:

```
# ./check-ssl-chain.sh google.com:443
Signature Algorithm: sha1WithRSAEncryption
  Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=google.com
Signature Algorithm: sha1WithRSAEncryption

Signature Algorithm: sha1WithRSAEncryption
  Subject: C=US, O=Google Inc, CN=Google Internet Authority G2
Signature Algorithm: sha1WithRSAEncryption

Signature Algorithm: sha1WithRSAEncryption
  Subject: C=US, O=GeoTrust Inc., CN=GeoTrust Global CA
Signature Algorithm: sha1WithRSAEncryption
```

Das Beispiel 1 (Heise) zeigt, dass der Admin fleissig war und die Zertifikate schon gegen SHA256-signierte ausgetauscht hat. Google hingegen setzt noch mit SHA1 signierte Zertifikate ein.

Hier noch das Script:

```
#!/bin/sh

HOST=$1
TMP=`mktemp -d`

echo QUIT | openssl s_client -showcerts -connect $HOST 2>/dev/null | sed -ne
'/BEGIN CERT/,/END CERT/p' | awk -v TMP="$TMP" '/BEGIN/{n++;}{print >TMP"/out" n ".crt" }'

for i in `ls $TMP/out*`; do
  openssl x509 -in $i -noout -text | egrep "Signature Algorithm|Subject:"
  echo
done

rm -rf $TMP
```

