HTTPsig: HTTP Response Signing Using DNSSEC

Cosmin Dumitru, Alex Giurgiu, Arthur van Kleef, and Niek Timmers
{cosmin.dumitru,alex.giurgiu,arthur.vankleef,niek.timmers}@os3.nl
System and Network Engineering, University of Amsterdam

SNE

Introduction

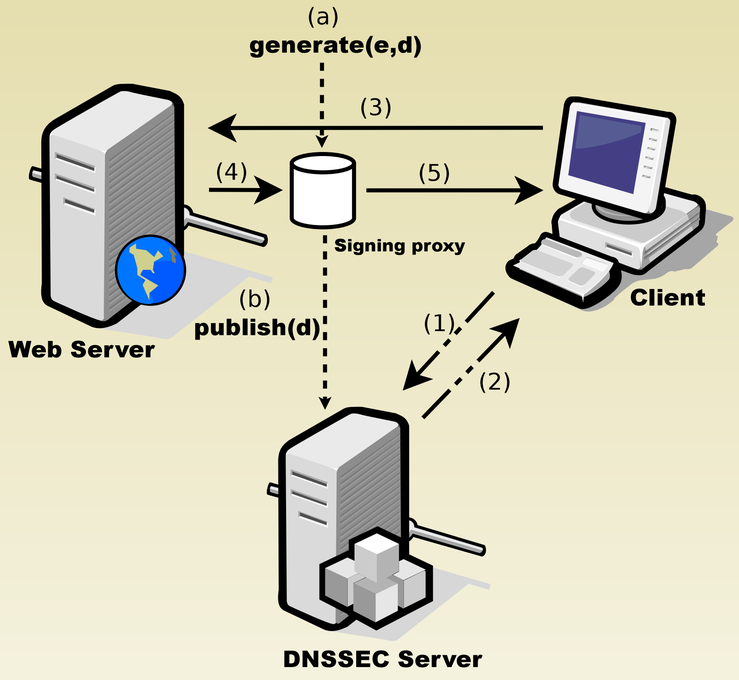
Achieving authenticity and integrity for HTTP traffic can be a subtle task on the Internet. During our project at University of Amsterdam we have designed a new approach that will achieve this. The HTTPsig project uses public key cryptography for signing HTTP responses. It relies on a DNSSEC infrastructure to store and authenticate public keys without key material stored at a third party.

Impact

- Facilitates signing of web content.
- Provides mitigation against MITM (SSL strip attack).
- Usage of DNSSEC for another purpose than just validating IP addresses.

HTTPsig

HTTPsig introduces two new additions in the HTTP client-server scenario. One is a signing proxy, a transparent layer between the web server and client. The role of the signing proxy is to perform signing on any HTTP response that traverses it. The signature is added to the header of the signed response. The second addition is a client module that receives the response and validates it using a public key retrieved via DNSSEC. The result of the validation decides the further action that needs to be taken by the client.



(a) generate key pair *(e,d)*.
(b) publish public key in DNSSEC zone.

(1) Client requests the HTTPsig public key from DNSSEC resolver.
(2) Client receives the Web Server's IP and public key *d*.
(3) Client sends HTTP request to the Web Server.
(4) Web Server sends HTTP response to the Signing Proxy.
(5) Signing Proxy uses the private key *e* to sign the HTTP response.
(6) Client checks HTTP response signature using the public key *d*.

Design

HTTPsig supports modern crypto algorithms and is designed in a modular manner supporting future algorithms. It adds four additional headers to the HTTP response:

```
HTTPsig-SigCipher: dsa,sha1

HTTPsig-PublicKey: 4e1243bd22c66e76c2ba9eddc1f91394e57f9f83

HTTPsig-Signature:
MC4CFQC2FrW/S0daiL4GlKuW4e2yrHweXwIVAN/iGS/9AHG91t4d10AdbC5mkwFU

HTTPsig-OriHeaders:
Date,Server,Last-Modified,ETag,Accept-Ranges,Content-Length
```

The headers are used to check the key validity and response integrity. Possible uses:

- Provide a boot-strap for chain-of-trust files: public keys, certificates, checksums
- Identify webservers to applications without the need of encryption

Contact

If you have any questions please feel free to email us.

`http://www.os3.nl`