Internet-Draft
Intended status: Standards Track
Expires: January 2014

M. Sporny
Digital Bazaar
July 2013

HTTP Signature Nonces

draft-sporny-http-signature-nonces-00

Abstract

This document is an extension to the HTTP Signatures specification and describes a method of adding replay resistance to HTTP messages sent over unsecure channels.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The HTTP Signatures specification provides a standard way for clients to digitally sign HTTP requests, adding origin authentication and message integrity to the HTTP protocol. Typically, HTTP Signatures are protected from replay attacks by using a low-level secure communication channel, such as those provided by Secure Sockets Layer or Transport Layer Security. There are cases where operating SSL or TLS channels are computationally or financially cost prohibitive. In these instances, this specification provides an alternate mechanism for protecting HTTP Signatures against replay attacks.

2. Signature Authentication Scheme Extensions

The "signature" authentication scheme is outlined in [HTTP SIGNATURES REFERENCE]. The section below is the extension to the Authorization Header that is required to enable HTTP Signature nonces to be used. The grammar below assumes that the "params" grammar is extended with a "client" and "nonce" field.

```
credentials := "Signature" SP params
params := keyId "," algorithm [", " headers] [", " ext] [", " clientId ", " nonce] ", " signature
clientId := "client-id" "=" ClientNumber
nonce := "nonce" "=" NonceNumber
ClientNumber := 128-bit unsigned integer represented as a base-10 string
NonceNumber := 32-bit unsigned integer represented as a base-10 string
```

2.1 Extended Signature Parameters

The following section details the extended set of signature parameters for the Authorization Header.

2.1.1 clientId

REQUIRED if "nonce" parameter is used. The client identifier is a 128-bit unsigned integer that is used to identify the specific client that is using a nonce-based signature. It is necessary because there may be multiple HTTP Signature clients behind the same IP address, using the same private key to generate signatures.

2.1.2 nonce

REQUIRED if "client-id" parameter is used. The nonce is a 32-bit unsigned integer that is used to detect replay attacks on a network. When a nonce is used in a digital signature, the next message sent by the client MUST increment the nonce value before it is used again. A ±5 minute window is used to detect replay attacks by the receiver of the message. If a nonce is re-used during the time window, the receiving party MUST respond as if a replay attack is being performed.

3. Appendix A: Test Values

The following test data uses the following RSA 2048-bit keys, which we will refer to as `keyId=Test` in the following samples:

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDCFENGw33yGihy92pDjZQhl0C3
6rPJj+CvfSC8+q28hxA161QFNUd13wuCTUcq0Qd2qsBe/2hFyc2DCJJg0h1L78+6
Z4UMR7EOcpfdUE9Hf3m/hs+FUR45uBJeDK1HSFHD8bHKD6kv8FPGfJTotc+2xjJw
oYi+1hqp1fIekaxsyQIDAQAB
-----END PUBLIC KEY-----
```

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDCFENGw33yGihy92pDjZQhl0C36rPJj+CvfSC8+q28hxA161QF
NUd13wuCTUcq0Qd2qsBe/2hFyc2DCJJg0h1L78+6Z4UMR7EOcpfdUE9Hf3m/hs+F
UR45uBJeDK1HSFHD8bHKD6kv8FPGfJTotc+2xjJwoYi+1hqp1fIekaxsyQIDAQAB
AoGBAJR8ZkCUvx5kzv+utdl7T5MnordT1TvoXXJGXK7ZZ+UuvMNUCdN2QPc4sBiA
QWvLw1cSKt5DsKZ8UETpYPy8pPYnnDEz2dDYiaew9+xEpubyeW2oH4Zx71wqBtOK
kqwrXa/pzdpiucRRjk6vE6YY7EBBs/g7uanVpGibOVAEsqH1AkEA7DkjVH28WDUg
f1nqvfn2Kj6CT7nIcE3jGJsZZ7zlZmBmHFDONMLUrXR/Zm3pR5m0tCmBqa5RK95u
412jt1dPIwJBANJT3v8pnkth48bQo/fKel6uEYyboRtA5/uHuHkZ6FQF7OUkGogc
mSJluOdc5t6hI1VsLn0QZEjQZMEOWr+wKSMCQQCC4kXJEsHAve77oP6HtG/IiEn7
kpyUXRNvFsDE0czpJJBvL/aRFUJxuRK91jhjC68sA7NsKMGg5OXb5I5Jj36xAkEA
gIT7aFOYBFwGgQAQkWNKLvySgKbAZRTeLBacpHMuQdl1DfdntvAyqpAZ0lY0RKmW
G6aFKaqQfOXKCyWoUiVknQJAXrlgySFci/2ueKlIE1QqIiLSZ8V8OlpFLRnb1pzI
7U1yQXnTAEFYM560yJlzUpOb1V4cScGd365tiSMvxLOvTA==
-----END RSA PRIVATE KEY-----
```

And all examples use this request:

```
POST /foo?param=value&pet=dog HTTP/1.1
Host: example.com
Date: Thu, 05 Jan 2012 21:31:40 GMT
Content-Type: application/json
Content-MD5: Sd/dVLAcvNLSq16eXua5uQ==
Content-Length: 18

{"hello": "world"}
```

3.1 Default Test

The string to sign would be:

```
POST /foo?param=value&pet=dog HTTP/1.1
host: example.com
date: Thu, 05 Jan 2012 21:31:40 GMT
```

The Authorization header would be:

```
Authorization: Signature keyId="Test",algorithm="rsa-sha256",client-id=1596338745637,nonce=273,signature="ATp0r26dbMIxOopqw0OfABDT7CKMIoENumuruOtarj8n/97Q3htHFYpH8yOSQk3Z5zh8UxUym6FYTb5+A0Nz3NRsXJibnYi7brE/4tx5But9kkFGzG+xpUmimN4c3TMN7OFH//+r8hBf7BT9/GmHDUVZT2JzWGLZES2xDOUuMtA="
```

3.2 All Headers Test

Parameterized to include all headers, the string to sign would be (`+ "\n"` inserted for readability):

```
1596338745637 273 + "\n"
POST /foo?param=value&pet=dog HTTP/1.1 + "\n"
host: example.com + "\n"
date: Thu, 05 Jan 2012 21:31:40 GMT + "\n"
content-type: application/json + "\n"
content-md5: Sd/dVLAcvNLSq16eXua5uQ== + "\n"
content-length: 18
```

The Authorization header would be:

```
Authorization: Signature keyId="Test",algorithm="rsa-sha256",headers="request-line host date content-type content-md5 content-length",client-id=1596338745637,nonce=273,signature="H/AaTDkJvLELy4i1RujnKlS6dm8QWiJvEpn9cKRMi49kKF+mohZ15z1r+mF+XiKS5kOOscyS83olfBtsVhYjPg2Ei3/D9D4Mvb7bFm9IaLJgYTFFuQCghrKQQFPiqJN320emjHxFowpIm1BkstnEU7lktH/XdXVBo8a6Uteiztw="
```

4. Normative References

Author's Address

Manu Sporny
Digital Bazaar
1700 Kraft Drive
Suite 2408
Blacksburg, VA 24060
US
Phone: +1 540 961 4469
EMail: msporny@digitalbazaar.com
URI: http://manu.sporny.org/