Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 14, 2017

J. Peterson
Neustar

March 13, 2017

Short-Lived Certificates for Secure Telephone Identity
draft-peterson-stir-certificates-shortlived-00.txt

Abstract

When certificates are used as credentials to attest the assignment of ownership of telephone numbers, some mechanism is required to provide certificate freshness. This document specifies short-lived certificates as a means of guaranteeing certificate freshness, in particular relying on the Automated Certificate Management Environment (ACME) to allow signers to acquire certifcates as needed.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 14, 2017.

Table of Contents

1. Introduction

The STIR problem statement [RFC7340] discusses many attacks on the telephone network that are enabled by impersonation, including various forms of robocalling, voicemail hacking, and swatting. One of the most important components of a system to prevent impersonation is the implementation of credentials which identify the parties who control telephone numbers. The STIR certificates [I-D.ietf-stir-certificates] specification describes a credential system based on [X.509] version 3 certificates in accordance with [RFC5280] for that purpose. Those credentials can then be used by STIR authentication services [I-D.ietf-stir-rfc4474bis] to sign PASSporT objects [I-D.ietf-stir-passport] carried in a SIP [RFC3261] request.

The STIR certificates document specifies an extension to X.509 that defines a Telephony Number (TN) Authorization List that may be included by certificate authorities in certificates. This extension provides additional information that relying parties can use when validating transactions with the certificate. When a SIP request, for example, arrives at a terminating administrative domain, the calling number attested by the SIP request can be compared to the TN Authorization List of the certificate that signed the request to determine if the caller is authorized to use that calling number in SIP.

No specific recommendation is made in the STIR certificates document for a means of determining the freshness of certificates with a TN Authorization List. This document explores how short-lived certificates could be used as a means of preserving that freshness.

Short-lived certificates also have a number of other desirable properties that fulfill important operational requirements for network operators. The use of the Automated Certificate Management Environment (ACME) [I-D.ietf-acme-acme] to manage these short-lived certificates is the focus of the architecture specified here. The interaction of STIR with ACME has already been explored in [I-D.peterson-acme-telephone].

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Short-lived certificates for STIR

While there is no easy definition of what constitutes a "short-lived" certificate, the term typically refers to certificates that are valid only for days or even hours, as opposed to the months or years common in traditional public key infrastructures. When the private keying material associated with a certificate that has an expiry of months or years is compromised by an adversary, the issuing authority must revoke the certificate, which requires relying parties to review certificate revocation lists or to access real-time status information with protocols such as OCSP. Short-lived certificates offer an alternative where, if compromised, certificates will shortly expire anyway, and rather than revoking and reissuing the certificate in response to a crisis, certificates routinely roll-over and cannot be cached for a long term by relying parties, minimizing their value to attackers.

One of the additional benefits of using short-lived certificates is that they do not require relying parties to perform any certificate freshness check. The trade-off is that the signer must acquire new certificates frequently, so the cost of round-trip times to the certificate authority is paid on the signer's side rather than the verifier's side; however, in environments where many parties may rely on a single certificate, or at least where a single certificate will be used to sign many transactions during its short lifetime, the overall architecture will incur less processing delay.

In the STIR context, the TN Authorization List defined in [I-D.ietf-stir-certificates] adds a new wrinkle to the behavior of short-lived certificates. Because a subject may have authority over multiple telephone numbers, a certificate issued to that subject could attest the authority over all, some, or just one of those telephone numbers. If an authentication service wanted to acquire a

new certificate on a per-call basis, for example, they could acquire a certificate that can only sign for the calling party number of the call in question. At the other end of the spectrum, a large service provider could acquire a certificate valid for millions of numbers, but expire the certificate after a very short duration - say one hour - to reduce the risk that the certificate would be compromised.

This inherent flexibility in the architecture permits authentication services to implement very narrow policies for certificate usage. A large service provider who wanted to avoid revealing which phone numbers they controlled, for example, could provide no information in the certificate that signs a call other than just the single telephone number that corresponds to the calling party's number. How frequently the service provider feels that they need to expire that certificate and acquire a new one is entirely a matter of policy to them. This makes it much harder for entities monitoring signatures over calls to guess who owns which numbers, and provides a much more complicated threat surface for attackers trying to compromise the service.

In order to reduce the burden on verification services, an authentication service could also piggyback a short-lived certificate onto the signed SIP request, so that no network lookup and consequent round-trip delay would be required on the terminating side to acquire the new certificate. [I-D.ietf-stir-rfc4474bis] already provides a way of pointing to a certificate in a MIME body associated with the SIP request. Future work could specify other means of carrying certificates within SIP requests via a header rather than a body, to optimize for intermediaries adding and extracting these certificates.

4. Certificate Acquisition with ACME

One of the primary burdens of short-lived certificates is building an operational system that allows signers to acquire new certificates and put them to immediate use. ACME [I-D.ietf-acme-acme] is designed for exactly this purpose. After a client registers with an ACME server, and the authority of the client for the names in question is established (through means such as [I-D.peterson-acme-telephone]), the client can at any time apply for a certificate to be issued by sending an appropriate JSON request to the server. That request will contain a CSR [RFC2986] indicating the intended scope of authority as well the validity interval of the certificate in question. Ultimately, this will enable the client to download the certificate from a certificate URL designated by the server.

[TBD: What needs to fixed for the TN Authorization List extension, including both TN and SPC cases>]

5. IANA Considerations

This document contains no actions for the IANA.

6. Privacy Considerations

Short-lived certificates provide attractive privacy properties when compared to real-time status query protocols like OCSP, which require relying parties to perform a network dip that can reveal a great deal about the source and destination of communications. For STIR, these problems are compounded by the presence of the TN Authorization List extension to certificates. Short-lived certificates can minimize the data that needs to appear in the TN Authorization List, and consequently reduce the amount of information about the caller leaked by certificate usage to an amount equal to what is leaked by the call signaling itself.

[More TBD]

7. Security Considerations

This document is entirely about security. For further information on certificate security and practices, see [RFC5280], in particular its Security Considerations.

8. Acknowledgments

Stephen Farrell provided key input to the discussions leading to this document.

9. References

9.1. Normative References

[ATIS-0300251]
ATIS Recommendation 0300251, "Codes for Identification of Service Providers for Information Exchange", 2007.

[DSS] National Institute of Standards and Technology, U.S. Department of Commerce | NIST FIPS PUB 186-4, "Digital Signature Standard, version 4", 2013.

[I-D.ietf-acme-acme]
Barnes, R., Hoffman-Andrews, J., and J. Kasten, "Automatic Certificate Management Environment (ACME)", draft-ietf-acme-acme-05 (work in progress), February 2017.

[I-D.ietf-stir-certificates]
Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", draft-ietf-stir-certificates-11 (work in progress), October 2016.

[I-D.ietf-stir-passport]
Wendt, C. and J. Peterson, "Personal Assertion Token (PASSporT)", draft-ietf-stir-passport-11 (work in progress), February 2017.

[I-D.ietf-stir-rfc4474bis]
Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-stir-rfc4474bis-16 (work in progress), February 2017.

[I-D.peterson-acme-telephone]
Peterson, J. and R. Barnes, "ACME Identifiers and Challenges for Telephone Numbers", draft-peterson-acme-telephone-00 (work in progress), October 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2392] Levinson, E., "Content-ID and Message-ID Uniform Resource Locators", RFC 2392, DOI 10.17487/RFC2392, August 1998, <http://www.rfc-editor.org/info/rfc2392>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <http://www.rfc-editor.org/info/rfc2818>.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, DOI 10.17487/RFC2986, November 2000, <http://www.rfc-editor.org/info/rfc2986>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, DOI 10.17487/RFC3447, February 2003, <http://www.rfc-editor.org/info/rfc3447>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4055, DOI 10.17487/RFC4055, June 2005, <http://www.rfc-editor.org/info/rfc4055>.

[RFC5019] Deacon, A. and R. Hurst, "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments", RFC 5019, DOI 10.17487/RFC5019, September 2007, <http://www.rfc-editor.org/info/rfc5019>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <http://www.rfc-editor.org/info/rfc5912>.

[RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, DOI 10.17487/RFC5958, August 2010, <http://www.rfc-editor.org/info/rfc5958>.

[RFC6818] Yee, P., "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 6818, DOI 10.17487/RFC6818, January 2013, <http://www.rfc-editor.org/info/rfc6818>.

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, DOI 10.17487/RFC6960, June 2013, <http://www.rfc-editor.org/info/rfc6960>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <http://www.rfc-editor.org/info/rfc7030>.

[RFC7093] Turner, S., Kent, S., and J. Manger, "Additional Methods for Generating Key Identifiers Values", RFC 7093, DOI 10.17487/RFC7093, December 2013, <http://www.rfc-editor.org/info/rfc7093>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <http://www.rfc-editor.org/info/rfc7230>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <http://www.rfc-editor.org/info/rfc7519>.

[X.509] ITU-T Recommendation X.509 (10/2012) | ISO/IEC 9594-8, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", 2012.

[X.680] ITU-T Recommendation X.680 (08/2015) | ISO/IEC 8824-1, "Information Technology - Abstract Syntax Notation One: Specification of basic notation".

[X.681] ITU-T Recommendation X.681 (08/2015) | ISO/IEC 8824-2, "Information Technology - Abstract Syntax Notation One: Information Object Specification".

[X.682] ITU-T Recommendation X.682 (08/2015) | ISO/IEC 8824-2, "Information Technology - Abstract Syntax Notation One: Constraint Specification".

[X.683] ITU-T Recommendation X.683 (08/2015) | ISO/IEC 8824-3, "Information Technology - Abstract Syntax Notation One: Parameterization of ASN.1 Specifications".

9.2. Informative References

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, <http://www.rfc-editor.org/info/rfc2046>.

[RFC3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, DOI 10.17487/RFC3647, November 2003, <http://www.rfc-editor.org/info/rfc3647>.

[RFC5055] Freeman, T., Housley, R., Malpani, A., Cooper, D., and W. Polk, "Server-Based Certificate Validation Protocol (SCVP)", RFC 5055, DOI 10.17487/RFC5055, December 2007, <http://www.rfc-editor.org/info/rfc5055>.

[RFC6961] Pettersen, Y., "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension", RFC 6961, DOI 10.17487/RFC6961, June 2013, <http://www.rfc-editor.org/info/rfc6961>.

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <http://www.rfc-editor.org/info/rfc7340>.

[RFC7375] Peterson, J., "Secure Telephone Identity Threat Model", RFC 7375, DOI 10.17487/RFC7375, October 2014, <http://www.rfc-editor.org/info/rfc7375>.

[X.520] ITU-T Recommendation X.520 (10/2012) | ISO/IEC 9594-6, "Information technology - Open Systems Interconnection - The Directory: Selected Attribute Types", 2012.

Author's Address

Jon Peterson
Neustar, Inc.

Email: jon.peterson@neustar.biz