Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 3, 2011

R. Barnes
BBN Technologies
P. Saint-Andre
Cisco Systems, Inc.
July 2, 2010

High Assurance Re-Direction (HARD) Problem Statement
draft-barnes-hard-problem-00

Abstract

This document describes several security challenges involved with the increasingly common practice of third-party hosting of applications, in particular the inability to know with a high level of assurance that the hosting provider is authorized to offer an application on behalf of an organization or individual.

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 January 3, 2011.

Table of Contents

1. Introduction

Internet applications such as websites, email services, and instant messaging (IM) services are increasingly offered by third-party hosting providers (e.g., "apps.example.net"). However, an organization that contracts with such a hosting provider typically wants its applications to be associated with its DNS domain name (e.g., "example.com") instead of the hosting provider's name. This introduces a problem that we call "High Assurance Re-Direction" (HARD): how can a user or peer of the application securely know that the hosting provider is authorized to offer that application on behalf of the organization?

This is indeed a HARD problem, to which no good solutions currently exist. To help technologists find such solutions, this document describes the problem and suggests some possible paths to solutions.

2. Security Challenges of Hosted Applications

Let us assume that a company called Example.com wishes to offload responsibility for its corporate instant messaging service ("im.example.com") to a hosting provider called Apps.Example.Net using the Extensible Messaging and Presence Protocol [XMPP]. The company sets up DNS service location records [DNS-SRV] that point im.example.com at apps.example.net:

```
_xmpp-client._tcp.im.example.com. 90 IN SRV 0 0 5222 apps.example.net
_xmpp-server._tcp.im.example.com. 90 IN SRV 0 0 5269 apps.example.net
```

When a user juliet@example.com attempts to log in to the IM service at im.example.com, her client discovers apps.example.net and resolves that name to an IP address and port. However, Juliet wants to be sure that the connection is encrypted using Transport Layer Security [TLS] so her client checks the certificate offered by the XMPP service at the resolved IP address and port.

Her client expects the server identity in the certificate to be "im.example.com" (or perhaps "*.example.com"). But what if the identity is, instead, "apps.example.net" or "*.example.net"? Now her client will need to prompt Juliet to accept this certificate mismatch either temporarily or permanently. Because such security warnings are unnerving to end users, the owners of the company would prefer that the IM service offer a certificate with an identity of "im.example.com". Unfortunately, the IM server software used by the hosting provider probably needs runtime access to the private key associated with the certificate. This makes both the security personnel at Example.com and the lawyers at Apps.Hosting.Net

uncomfortable. There are several possible solutions (see for instance [XMPP-DNA]:

- o Terminate the hosting agreement. However, this is unpalatable to the company (IM is not their core competence) and the hosting provider (less revenue).
- o Deploy DNS security extensions [DNSSEC] so that users can be sure that the redirect has not been tampered with. However, DNSSEC is not yet widely deployed, so the Example.com admins discover that this option is not available.
- o Deploy the IM service using attribute certificates (ACs) instead of public key certificates (PKCs). However, the hosting provider's software does not support ACs and there are no tools available that would enable Example.com to generate such ACs.

The same problem exists in a number of other technologies, including the Hypertext Transport Protocol [HTTP], the Internet Message Access Protocol [IMAP], the Location-to-Service Translation Protocol [LOST], and the discovery of Location Information Servers [LIS].

3. Security Considerations

This entire memo is about security.

4. IANA Considerations

This document has no actions for the IANA.

5. Informative References

[DNS-SRV] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[DNSSEC] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[HTTP] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[IMAP] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, March 2003.

[LIS] Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)", draft-ietf-geopriv-lis-discovery-15 (work in progress), March 2010.

[LOST] Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", RFC 5222, August 2008.

[TLS] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[XMPP] Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 3920, October 2004.

[XMPP-DNA] Lindberg, J. and S. Farrell, "Domain Name Assertions", draft-ietf-xmpp-dna-00 (work in progress), January 2010.

Authors' Addresses

Richard Barnes
BBN Technologies
9861 Broken Land Parkway
Columbia, MD 21046
USA

Phone: +1 410 290 6169
Email: rbarnes@bbn.com

Peter Saint-Andre
Cisco Systems, Inc.
1899 Wyknoop Street, Suite 600
Denver, CO 80202
USA

Phone: +1-303-308-3282
Email: psaintan@cisco.com