Towards Truly Ubiquitous and Opportunistic Trust Infrastructures:

Position for Next Generation Cybersecurity Infrastructure Workshop

Stephen Nightingale (night@nist.gov), Scott Rose, Doug Montgomery

NIST, High Assurance Domains Project

October 1, 2014

Introduction

On review of the calling notice for the Next Generation Cybersecurity Infrastructure workshop, we note that Federated Identities [1] are a component of current solutions. Often, these identities rely on secure network communications to provide trustworthy authentication. Authentication mechanisms for existing frameworks such as Shibboleth (http://shibboleth.net), which uses SAML [2], standardized in 2005, incorporate a wide eco-system of specific authentication methods like: passwords, certificates, smart cards, Kerberos tickets, X.509 certificates, and secure remote passwords. With the recent development of DANE [3] – the DNS based Authentication of Named Entities, secured by DNSSEC [4], a potential basis for a truly ubiquitous and opportunistic, single rooted trust infrastructure is emerging. Its inclusion as an authentication mechanism for federated identities is worthy of consideration. A summary of our current and proposed work in the High Assurance Domains project at NIST is given below.

What We Are Doing

The basis of our effort is the development of authentication protocols that use public keys distributed through the DNS, secured by DNSSEC, a mechanism generically termed DANE (the DNS based Authentication of Named Entities). This is an authentication mechanism that may replace or augment the X.509 Certificate Authority infrastructure, which requires a certificate issued by some authority, at some cost and with some time lag. This certificate has to be explicitly acquired, and installed in the application (such as a web server). Under DANE, the keys are installed as resource records in the Domain Name System (DNS).

Our current focus is the research and development of a ubiquitous secure email infrastructure, implicitly through DANE and explicitly through OpenPGP [5][6] and S/MIME [7]. The public keys for these secure email protocols would be stored in the DNS (in newly specified resource records) and associated with an end user's email address. The model can be extended to include other network applications: instant
messaging, HTTPS, etc. A collaborator is also developing a code-signing [8] application where the code-signing party’s public key will be retrievable from the DNS, analogous to the OpenPGP application.

The HAD secure email project at NIST is supporting the development of these initiatives by developing and deploying test infrastructure, accessible through the HAD-Pilot web site [8]. We have a series of protocol test systems for email transmission security and email content security. Email server-to-server security is facilitated with SPF/DKIM/DMARC [9][10][11], DANE and TLS [12] protocols, and is a greater concern of email providers. Email content security is facilitated by S/MIME with X.509, and OpenPGP protocols, and is a greater concern for email users. Test systems are under development for OpenPGP and SMIMEA.

References


[6] Using DANE to Associate OpenPGP Public Keys with Email Addresses, draft-ietf-dane-openpgpkey-00.


[9] rfc4408 Sender Policy Framework (SPF) for Authorizing Use of Domains in Email.

