Network Working Group   N.D. McBurnett
Internet-Draft   Avaya Inc.
Expires: August 13, 2001   February 12, 2001

SACRED Scenarios
draft-ietf-sacred-scenarios-00

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 13, 2001.

Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

Abstract

This memo presents scenarios for securely acquiring credentials. This ID is an interim product of work-in-progress within the Securely Available Credentials (sacred)[1] working group.

Table of Contents

1. Introduction 3
2. Scenarios 4
2.1 Obtaining Root Certs 4
2.2 Home Desktop Computer 4
2.3 Work Desktop Computer 6
2.4 Public Lab / On-campus Shared Workstation 6
2.5 Public Kiosk Mobility 7
2.6 Platforms with Limited Capabilities 8
2.7 Uploading Credentials 9
2.8 Changing authentication information 9
2.9 User Self-Enrollment 9
2.10 Bulk Initialization of a Credential Server's Repository . . 9
2.11 Possible scenarios to justify time-to-live requirement . . . 9
References 10
Author's Address 10
A. Acknowledgements 11
Full Copyright Statement 12

1. Introduction

The scenarios below are intended to provoke discussion of what SACRED should and shouldn't do. It is not necessarily true that SACRED should support all of these or to what extent SACRED should support them. These scenarios should encompass most of the sorts of things that we expect SACRED to play a part in.

[These scenarios are collected mostly as-is from several individuals. From an editorial standpoint, no effort has been made to hammer them into a coherent style, pending feedback on their general utility, the preferred style, and additional input.]

2. Scenarios

2.1 Obtaining Root Certs

A new student, Carol, needs to configure her browser so it will work in the campus environment. The campus has deployed their own self-signed root certificate which is used to sign things like TLS certificates for campus web servers, SACRED server certs, etc. They have bundled this root certificate up as a SACRED credential named ExampleU-Root (possibly along with trust policies of some sort, etc.) and published the name and fingerprint of this bundle in some paper medium (her acceptance letter, the campus newspaper, or the like.)

Carol connects to the SACRED server and gets the ExampleU-Root credential. Her client calculates and displays the fingerprint, and since it matches the published fingerprint, Carol tells the client to accept the credential. She can be confident that it authentic without even needing to authenticate the SACRED server or present any credentials of her own.

Note that other mechanisms may offer an alternative to checking a fingerprint - e.g. the Password Derived Moduli (PDM) scheme could work if the server had a userid and password for the user, and the user could thus use these to authenticate the server, and accept the root credentials simple on the basis of trusting an authenticated server.

2.2 Home Desktop Computer

Scenario Overview

A university utilizing a PKI infrastructure for various applications and services on-campus is likely to find that many of its users would like to make use of the same PKI-enabled services and applications on computers located in their residence. These home computers may be owned either by the university or by the individual but are permanently located at the residence as opposed to laptop systems that may be taken home. The usage depicted in this scenario may be motivated by formal telecommuting arrangements or simply by the need to catch up on work from home in the evenings. The basic scenario should apply equally well to the commercial, health care, and higher education environments.

Assumptions

This scenario assumes that the institution has not implemented a hardware token-based PKI mobility solution

The home computer has a dial-up as opposed to a permanent network connection.

The PKI applications, whenever practical, should be functional in both on-line and off-line modes. For example, the home user signing an email message to be queued for later bulk sending and the reading of a received encrypted message may be supported off-line while composing and queuing of an encrypted message might not be supported in off-line mode.

Applications using digital signatures will require nonrepudiation.

There institution prefers that the user be identified via a single certificate / key-pair from all computers used by the individual.

The home computer system can not be directly supported by the institution's IT staff. Hardware, operating system versions, and operating system configurations will vary widely. Significant software installations or specialized configurations will be difficult to implement.

Uniqueness of Scenario

The PKI mobility support needed for this scenario is, in general, similar to the other mobility scenarios. However, it does have several unique aspects:

The home-user scenario differs from the general public workstation case in that it provides the opportunity to permanently store the user's certificate and key-pair on the workstation.

Likewise the appropriate CA certificates and even certificates for other users can be permanently stored or cached on the home workstation.

Another key difference is the need to support off-line use of the PKI credentials given the assumed dial-up network connection.

The level of hardware and software platform consistency (operating system versions and configurations) will vary widely.

Finally, the level of available technical support is significantly less for home systems than for equivalent systems managed by the IT staff at the office location.

2.3 Work Desktop Computer

This will usually involve a subset of the requirements of the Home Desktop Computer scenario.

2.4 Public Lab / On-campus Shared Workstation

Scenario Overview

Many colleges and universities operate labs full of computer systems that are available for use by the general student population. These computers are typically configured with identical hardware and an operating system build that is replicated to all of the systems in the lab. Many typical configurations provide no permanent storage of any type while others may offer individual disk space for personal files on a central server. Some scheme is generally used to ensure that the configuration of the operating system is preserved across users and that temporary files created by one user are removed before the next user logs in. Students generally sit down at the next available workstation without any clear pattern of usage.

The same basic technical solutions used to operate public labs are often also used in general environments where several people share a single workstation. This is often found in locations with shift work such as medical facilities and service bureaus that provide services to multiple time zones.

Assumptions

This scenario assumes that the institution has not implemented a hardware token-based PKI mobility solution.

The computer systems are permanently networked with LAN connections.

The configuration of the computer system is centrally maintained and customizations are relatively easy to implement. For example it would be easy to load enterprise root certificates, LDAP server configurations, specialized software, and any other needed components of the PKI infrastructure on to the workstations.

Applications using digital signatures will require nonrepudiation in some of the anticipated environments. Examples of this might include homework submission in a public lab environment or medical records in a health care environment.

The institution prefers that the user be identified via a single certificate / key-pair from all computers used by the individual.

Many anticipated implementations of this scenario will not implement any user authentication at the desktop operating system level. Instead, user authentication will occur at during the startup of networked applications such as email, web-based services, etc. Login at the desktop level may be with generic user names that are more targeted at matching printouts to machines than identifying users.

Users, with almost ridiculous frequency, will walk away from a system forgetting to first logout from running authenticated applications.

Uniqueness of Scenario

The PKI mobility support needed for this scenario is, in general, similar to the other mobility scenarios. However, it does have several unique aspects:

Unlike situations with personal workstations, there is no permanent storage available to hold user key pairs and certificates.

Appropriate CA certificates and custom software are easily added and maintained for these types of shared systems.

The workstations are installed in public locations and users will frequently forget to close applications before permanently walking away from the workstation.

2.5 Public Kiosk Mobility

Overview

This scenario describes the needs of the traveler or the shopper. This person is traveling light (no computer) or is burdened with everything but a computer. It recognizes the increasing availability of internet access points in public spaces, such as libraries, airports, shopping malls, and "cyber cafes".

The Need

In our increasingly mobile society, the chances of needing information when away from the normal computing place are great. One may need to look up a telephone number. Have you tried to find a phone book at a public phone lately? It may become necessary to use a data device to find the next place to rush to. Mapquest to the rescue. With the proliferation of wireless devices (electronic leashes), others have the ability to create a need for quick access to electronic information. A pager can generate a need to check

the email inbasket or address book. A cell phone can drive you to your database to answer a pressing question.

The ability to quickly access sensitive or protected information or services from publicly available devices will only become more necessary as we become more and more "connected".

The Device

The access device is more a function of the best discount or marketing effort than of design. Any number of Intel based hardware platforms will be encountered. Macintosh is encountered from time to time. Linux has been spotted in a couple of local internet coffee shops.

Since these devices are open to the public I/O ports are not likely to be. In order to protect the device and it's immediate network environment, most devices will be in some sort of protective container. Access to serial, parallel, USB, firewire, SCSI, or PCMCIA connections will not be possible. Likewise floppy, zip, or cd drives. Therefore, any software "token" must be obtained from the network itself.

The Concerns

1. Getting the "token". Since it will be necessary to obtain the token (key, certificate, credential) from across the network. How can it be protected during transit?

2. Where did you get it? One of the primary controls in the Public Key Infrastructure is protection of the private key. Placing the key on a host that is accessible from a public network means that there is an inherent exposure from that network. The access controls and other security measures on the host machine are an area of concern.

3. How did you get it? When you obtained the token from the server, how did it know that you are you? Authentication becomes critical.

4. What happens to the token when you leave? You've checked your mail, downloaded a recipe from that super-secure recipe server, found out how to get to the adult beverage store for the... uh... accessories... for the meal, and you're off! Is your token? Or is it still sitting there on the public kiosk waiting for those youngsters coming out of the music store to notice and cruise the information highway on your ticket?

2.6 Platforms with Limited Capabilities

Cell Phones, PDAs, Appliances, etc.

2.7 Uploading Credentials

2.8 Changing authentication information

2.9 User Self-Enrollment

2.10 Bulk Initialization of a Credential Server's Repository

2.11 Possible scenarios to justify time-to-live requirement

[Under what circumstances should the protocol or SACRED credential format get involved in time-to-live criteria? Does it imply that the client software and host are trusted to enforce the restriction, even though it is not part of the underlying certificates or whatever in a way that can be validated by the party that relies on the credential?]

References

[1] <http://www.ietf.org/html.charters/sacred-charter.html>

[2] <http://www.educause.edu/hepki/>

[3] <http://bcn.boulder.co.us/~neal/ietf/>

Author's Address

Neal D. McBurnett
Avaya Inc.
1300 W 120th Ave.
Westminster, CO 80234
US

Phone: +1 303-538-4852
EMail: nealmcb@avaya.com
URI: http://bcn.boulder.co.us/~neal/

Appendix A. Acknowledgements

The editor gratefully acknowledges the contributions of Jim Jokl, Kevin Unrue and Internet2's HEPKI-TAG[2] (Higher Education PKI Technical Advisory Group).

The XML source[3] for this document is available and can be formatted into text or html via xml2rfc or via the web thanks to the folks at http://xml.resource.org/.

Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC editor function is currently provided by the Internet Society.