UCTrust Metadata Listing IdP Network Addresses

UCTrust Metadata To List IdP Network Addresses

In order to use Shibboleth-based authentication for access to wireless networks, certain IP addresses of the guest's home institution's Identity Provider (IdP) system must be accessible before the authentication event. This document describes an extension to the UCTrust Metadata for this.

Ensuring the Validity and Correctness of UCTrust Security Information describes UCTrust's management of federation-wide information, the authenticity of which must be verifiable by software processes. Currently, one file, UCTrust-AAP.xml, is contained in the metadata to provide each campus's certifications for level of assurance.

The Proposal

Add a second file,

`IdPAddresses.txt`

, to the UCTrust metadata to list the IP addresses each IdP requires to be accessible. This text file would have multiple lines, each line specifying one IP subnet that must be accessible in CIDR Notation. Comment lines beginning with "#" are also allowed and will be used to indicate the UC location associated with a following list of address lines. For example,

```
# [IdPAddresses].txt 2010-07-06-01
\#
# This file lists the IP addresses that must be accessible on the network to end-users in order to utilize
# Shibboleth [IdPs] within UCTrust.
\#
# UC Berkeley
128.32.177.0/24
128.32.203.0/24
# UC Davis
128.120.211.128/25
128.120.210.233/32
2001:DB8::/48
# UC Irvine
...
```

Processing Requirements

- Wireless providers should retrieve and process this file at least nightly in order to avoid service outages for people visiting their campuses.
- Identity providers should avoid service outages for their traveling community members by phasing updates to compensate for wireless provders' time lags for processing updates. Whenever possible, new addresses should be added at least a week before they will be required to allow for processing by UCTrust's metadata initiators and certifiers. Old addresses should not be removed until after they are no longer required.