UCTrust Wireless Agenda - 2010-08-13

From: David Walker <DHWalker@ucdavis.edu>
To: UCTrust Wireless Project <UCTrustWireless@ucdavis.edu>
Subject: Today's conference call
Date: Fri, 13 Aug 2010 09:38:24 -0700

Everyone,

A quick reminder that we have a call at 11:00 today. I suggest everyone take a minue review the comparison of our alternative strategies on the wiki (https ://spaces.ais.ucla.edu/x/7oSsAQ), as well as Erik Klavon's note about eduroam and Radius's handling of contact information before the call. I've attached Erik's note for reference.

David

email message attachment, "Attached message - Including contact information in Radius transactions"

From: Erik Klavon <erikk@berkeley.edu>
To: uctrustwireless@ucdavis.edu
Subject: Including contact information in Radius transactions
Date: Thu, 5 Aug 2010 19:18:34 -0700

Hi

I volunteered to "research Radius's and eduroam's capabilities to send [a roaming user's] contact information" from the user's home institution to the visited institution.

The service definition[1] on the eduroam website states in section 5.3 that

> [i]n case of a security incident caused by an end user, the affected institution must inform its NRO [national roaming operator]. The NRO will then inform the end user's home federation through their respective NRO official contact in SA5 [the group that operates eduroam].

I can find no mention in eduroam documentation of directly including contact information in RADIUS transactions.

As for the RADIUS protocol, I haven't yet found an example of a IANA standardized attribute[2] that is specifically designated for the purpose of communicating contact information in the form of an email address. If there is no standard attribute for this purpose, we could create a new attribute (or attributes) for this purpose and start the standardization process. We will probably face challenges in adapting radius servers to work with the new attribute(s). While this sounds like a fun project, it probably wouldn't reach a useful stage for some time. We might be able to make this work for a UC roam implementation, depending on the flexibility of our RADIUS servers, but again the work involved makes this unattractive.

There are other options that don't require a specific attribute dedicated to communicating contact information. The Reply-Message attribute [RFC 2865 5.18] contains "text which MAY be displayed to the user" and "[w]hen used in an Access-Accept, it is the success message." We could agree on the convention that we populate the Reply-Message with the contact information when returning an Access-Accept response. My guess is that most home institutions would rewrite the response to include local information in this field (such as terms of service) if this information makes it back to the client via 802.1X when authentication succeeds.

Another option is to require the use of a common mailbox name as the contact address for eduroam at each participating institution. This is inspired by the mailbox names for common services, roles and functions [RFC 2142]. For example, if the common mailbox name for eduroam was eduroam-accountmaster, the email address at UCLA would be eduroam-accountmaster@ucla.edu. Suppose the user with RADIUS username mvn@ucla.edu used an unpatched OS while on the UCB wireless network. UCB can create the contact email address for this user by concatenating the common mailbox name eduroam-accountmaster, the @ sign, and the realm from the RADIUS username. Note that the eduroam service definition[1] states in section 1 that the realm is the institution's domain name.

One additional idea. We could agree to include the RADIUS username in an X header in emails sent to a contact address. Each institution could then automatically pass on the information to their users. I think this would greatly decrease the cost of delivering these notices without having to expose user email addresses directly. It also gives each institution a point of control to manage the communications going to their users.

Erik

[1] http://www.eduroam.org/downloads/docs/GN2-07-327v2-DS5_1_1-_eduroam_Service_Definition.pdf
[2] http://www.iana.org/assignments/radius-types/

A useful web page for looking up many common RADIUS attributes in the RFCs:
http://freeradius.org/rfc/attributes.html