Meeting notes from 802.23/Dallas/November 9/10/11, 2010
I don't expect to generate anything more in the way of minutes
-Geoff
==========
802.23 was called to order at approximately 9:00 AM on Tuesday, November 9, 2010
Venue: Hyatt Dallas @ Reunion, Kessler Board Room

Attending
Geoff Thompson, Chair / Interdigital
George Bumiller/RIM

Call for Patents
Geoff Thompson noted that he is aware of Nortel patents and takes the action item to solicit an LoA from Nortel
(Ref: New article encountered on the web regarding Nortel filing a patent infringement suit against Vonage. The posting is dated 9/2010 but the case may actually be from 2007. However that is not material to our concern which is only that Nortel has patents.)

The meeting schedule for the week was reviewed
We will not meet on Wed AM to enable attendance at the 802.11 Midweek Plenary
We will move to .16 on Wed PM for Presentation from Mat Sherman/Home Security Office

The first item of business undertaken was a review of Green Book edits and new material since the last meeting. The chair presented GB Version 0.3

(Karen Randall arrives 10:00)

Upon review of the Green Book draft presented by Thompson (esp slides 10-13) it was agreed to by all that we have to include "Unauthorized Access" in our standard.

Slide 14 accepted

Slide 17 requires that we add a discussion and explanation of what ESInet is.

NENA i3 (mat'l as shown in these slides) was accepted as normative requirements for our standard. Participants are encouraged to provide parallel requirements from other countries/markets.

Slide 19 agreed, Further it is expected that SNMP will be needed generally to load and manage the MIB that contains the location information.

Finished going through Green Book and gave copies of current state to attendees

Started going through ECRIT unauthorized access draft (01)

Started examining permutations of 2 levels of unauthorized access

Break for lunch Tuesday, 12:10 to 1:30

Pick back up at 1:40 (in terms of attendance we lost George, and gained Terry Cobb and Kathyrn Bennett)

Cases to UNAUTHORIZED SERVICE to consider

EUT-1 Open Access LAN Owns VoIP Service

EUT-2 Open Access LAN No VoIP Service/No default VoIP

EUT-3 Open Access LAN Default VoIp Service

EUT-4 Controlled Access LAN Owns VoIP Service
Has access

EUT-5 Controlled Access LAN Owns VoIP Service
Has no normal access

EUT-6 Controlled Access LAN No VoIP Service/No default VoIP
Has access

EUT-7 Controlled Access LAN No VoIP Service/No default VoIP
Has no normal access

EUT-8 Controlled Access LAN Default VoIp Service
Has access

EUT-9 Controlled Access LAN Default VoIp Service
Has no normal access

EUT-1 Fully authorized case
EUT-2 No functionality
EUT-3 Fully authorized case
EUT-4 Fully authorized case
EUT-5 This is the case that has the security risk.
The security risk is that a non-conformant VoIP Service Provider could allow full use of the access network by acting as a proxy.
That would allow misuse of the reserverd channel in the access network.
PROPOSAL: That we not allow this case.
If you come through the ES channel of the access network you must use the default VoIP provider !
(Paul Nikolich attended the meeting for awhile)
EUT-6 No functionality

EUT-7 No functionality
EUT-8 Fully authorized case as far as L1/l2 are concerned
EUT-9 This is the focal case of interest where 802.23 added capabilities make unauthorized access work.

(Chair AI, Feed this back to ECRIT) continue on with review of IETF draft

RE: the text:
==========
Note: At the time of writing there is no regulation in place that
demands the functionality described in this memo. SDOs have started
their work on this subject in a proactive fashion in the anticipation
that national regulation will demand it for a subset of network
environments.
==========
We believe that the above statement may NOT BE TRUE in the case where VoIP service and access service are offered in a bundled package.
(Chair AI, Feed this back to ECRIT)

Nikolich and then Cobb leave at about 2:50 PM

We don't understand the statement:
"The end host uses a Location Configuration Protocol (LCP) to retrieve location information."
as we expect the Location Configuration retrieval to be a local operation (??) thus any protocol spec would be internal and out of scope for IETF.

(During the meeting on Wed, Terri Brooks helped us figure this out. The EUT talks to the LoST server directly. Per the entire paragraph.)

RE: ZBP Considerations

>From a Layer1/2 point of view it would seem that this model gets a ZBP caller (1) an IP address under normal operation and (2) gets a ZBP caller as far as the router. Whether or not to provide router service to get to 911 is a router decision. Layer1/2 has done its job without regard to the users ZBP status

If, on the other hand the network (for example) deauthenticated a users 802.1X credentials (e.g. no credit left) then the user would be fully locked out of the normal L1/2 facility and would have to use the ES channel reserved for unauthenticated users.

Dr. Seung-Moon Ryu of the PicoCast Forum in Korea joined us.

Adjourn for the day at 5:00 PM

GOT attended Mat Sherman's presentation in 802.16

802.23 Reconvened on Wednesday at 1:30 PM

Attending were:
    Geoff Thompson/InterDigital
    Karen Randall/Randall Consulting
    Seung-Moon Ryu/PicoCast Forum
    Terri Brooks/True Position

Terri introduced herself and the rest of the group introduced themselves to her.

We reviewed the Tuesday PM work and Terri helped us understand some of it.

The group continued the review of the IETF Unauthorized Access draft

The following text strikes us as strange:
    The end host has no obligation to determine location information.
(Does this mean information that is different from any location information information that it may "retrieve" as opposed to "determine" (determine would be an independent process in this context.) ??
      It may attach location information if it has location available (e.g., from a GPS receiver).

We should map the contents of a SIP INVITE packet GOT Homework item.
(We thought the EUT was supposed to have Loc info cached.)
Is it that the distinction is "host" vs. "EUT", i.e. terminal vs. host
If that is so, then an Access Point would be an example of "host"
    (This needs to be researched and our understanding cleared up)

Apparently L3 can get location information from any L2 entity (i.e. us) via HTTP (per RFC5985 A.4)

At this point the latest version of the ECRIT Framework was retrieved
    draft-ietf-ecrit-framework-12.txt
Reading and understanding this is a homework item

This finished most of the meeting time for the day.
Since we were losing at least one attendee, we discussed plans for an interim.
We decided by consensus to have an interim meeting.

The available venues were considered.
We decided by consensus to meet with 802.11/15, etc in LA on Tues/Wed/Thurs Jan 18/19/20

Adjourn until Thurs. 9:00 AM

The meeting was convened on Thurs 9:15 AM
Attending were:
    Geoff Thompson/InterDigital
    Terri Brooks/True Position
    George Bumiller/RIM

Reviewing Framework still

Pertinent text:
6.3. Who adds location, endpoint or proxy

   The IETF emergency call architecture prefers endpoints to learn their location and supply it on the call.

(That is the job we have taken on, i.e. supplying information to the upper layers from L1/L2 of the EUT.)

AND

6.5. End system location configuration

   Unless a user agent has access to provisioned or locally measured location information, it must obtain it from the access network.

(This text assumes that an "access network" is a Layer 3 network and that it has servers to come up with this sort of information. Our assumption would be (RATHER) a Layer1/2 network. As a result, location would be provided at the upper layer interface of the control plane of the EUT. Further, there MIGHT be communication between Layer1/2 entities via a Layer 2 protocol such as LLDP.)

Sect 6.6 points out that L2 location has an advantage that it can't be spoofed by IP tunneling. We need to investigate and try to make sure that it also can't be spoofed by L2 tunnels/VLANs

RE: 6.7
It would be our goal to duck that problem by merely restricting ourselves to PIDF-LO
    (Review RFC 4119 to make sure that this is a reasonable approach.) (See 6.12)

(Terri leaves @ 11:30)

RE: 6.9, Multiple locations
Since ANY location that we provide from L2 is likely to have competiing information from the L3 mechanisms, we have to assume that we will ALWAYS be dealing with the multiple location problem thus RFCs 5491 and 5222 are homework items.

Completes review of Sect. 6

Adjourn at 11:50 AM (Thompson & Bumiller)

Next meeting in LA in Jan
The Chair committed to
    Send these notes to attendees
    Edit notes down into minutes and post to reflector & repository
    Send a LoA request to Michelle Lee
    Comb the notes for action items
    Develop response/questions/proposals to ECRIT with respect to the documents reviewed,
    especially the Unauthorized Access and Framework drafts