IEEE 802.1 Security Interim Minutes, May 30-31 2006

Minutes taken by Allyn Romanow

Plenary Meeting, Tuesday AM July 30, 2006

Mick Seaman, general

- General Intro to the meeting:
- Mick Seaman - 802.1 WG and TG Operation
- IEEE Patent policy discussed and slides shown
- Agree to meet with rest of 802.1 at next interim mtg
- Agenda
    - 802.1AR Secure Device Identifier – want to move it along, make a schedule
    - MACsec Key Agreement protocol- want to come to something that can go in .1af draft

Mike Borza - 802.1AR, secure Device ID

- Discussion of schedule
- Want to have a Task Group ballot for July and another for Sept. Interim
- Discussion of SNMP and DevID- .1AR doesn't mandate SNMP, uses LMI
- What is the asymmetric crypto primitive?
    - Candidates:
        RSA 2048
        Ntru
        elliptic curve ECC-224
        DSA

      Requirement – for the future, thru 2010.
      Need size 2048, so RSA 2048 is the only viable alternative. Fulfills FIPS 140-2, 201 requirements.
      There are IP issues with the Elliptic Curve. We don't understand those issues, so it's not on the table here.
- Life cycle- have a target not-after date for IDevID – 2049 rollover date. Local policy can dictate whether this is enforced.

Plenary Meeting, Tuesday AM July 30, 2006

802.1af MACsec Key Agreement

Brian Weis –LKS presentation, slides

- Concern that KSP key generation method will make it difficult to get FIPS 140-2 approval.
- Proposes traditional key server method for deriving key instead of key contribution method used by KSP.
- Other aspects of LKS similar to KSP - liveness

Plenary Meeting, Wednesday AM May 31, 2006

Mick Seaman, MACsec Key agreement

KSP slides, includes changes
Optional key distribution method using a TLV

Mike Borza- continuation of .1AR

- Discuss use of LDevID
- Went through Max Pritikin's notes on draft

Mike took notes on comments to update draft

Max Pritikin – slides on Enrollment

- How you get the LDevID, a difficult problem
- Start discussion
- When 802.1AR is used, what are the communication protocols?
- Do we need enrollment? Yes.
- Mechanism in MIB for IdevID

Wrap up, Planning

- .1AR two TG ballots

Sept TG ballot- get good and definite text in the draft. Around the first of Sept. have text worth balloting, consensus and indicate scope of the doc. Schedule driven. Put in placeholders if not developed at the due date.
Also do a near hand TG- to get all the contributors who are seriously interested.

- WG ballot in Nov. if everything goes well
- Now- June 15 collect material from the meeting and integrate with Mike's draft. Just need placeholder text, want to have the territory staked out.

Discussion at July mtg.

Brian Weis presentation

Typical FIPS 140-2 Evaluation
Went over what's involved in getting FIPS-140 certification

Mick- update

Attach key contribution to key, means this key was generated after key contrib. process. When change servers, reboot, can verify the key he's distributing is based on your current state.
An integrity check. Can be viewed as a key or something attached to a key.

There's a performance win in using key distributed from server. When get previous key from same server, it's an update, and don't have to do key contrib. check because liveness ensures the new key from server is good.
It's when you change servers, need to run the contrib. check.
From 2 party, it's a 4 way handshake.
For group it's generated at one end, wrapped in keywrap
Key server monitors key contributions
Everyone gets everyone's key contribs
Authenticated the time of the key, it's after the key contrib..
Key contrib. is really a nonce.

Status- need to do re-labeling.
2 participants is 4-way handshake
Goal – Mick and Brian write text
Discuss in July meeting, no ballot
Wants to flesh out use cases
Solicit feedback re FIPS after July meeting

July meeting planning

Attendees:
Paul Congdon paul.congdon@hp.com
Mick Seaman mick_seaman@ieee.org
Allyn Romanow allyn@cisco.com
Jan Schlossberg jands@cisco.com
Keti Kilcrease kilcreas@cisco.com
Guy Hutchison hutch@marvelll.com
Dina Birrell dbirrell@cisco.com
Neil Peers npeers@advaoptical.com
Brian Weis bew@cisco.com
Yongbum Kim ybkim@broadcom.com
Charles Qi zqi@broadcom.com
Max pritikin pritikin@cisco.com
Joe Salowey jsalowey@cisco.com
Ken Grewal ken.grewal@intel.com
Men Long men.long@intel.com
Ron Tisinger tisinger@cisco.com
Shelly Cadora scadora@cisco.com
Ludwig Winkel Ludwig.winkel@siemans.com
Frank Chao fchao@cisco.com
Mark Gravel mar.gravel@hp.com
Thomas Dineen tdineern@netcom.com
Mike Borza mborza@ellipticsemi.com
Pankaj K Jha panka.kijha@intel.com