IEEE 802.1 Minutes, January 2007

Opening Remarks, Monday AM, January 22, 2007

Meeting logistics – Tony Jeffree

Discussion about affiliation disclosure – Tony Jeffree

- Everyone must disclose who is materially supporting their attendance
- There was significant discussion about the ramifications and nuances of this requirement
- The chairman will insure everyone discloses an entity – writing down "I refuse to disclose" will constitute failure to disclose, which implies loss of voting membership

Discussion of IEEE patent policy – Tony Jeffree

- Tony showed the required two slides and insured everyone in the room was aware of IEEE patent policy
- A call for patents was asked – no one disclosed any patents

Discussion of moving Link Aggregation from P802.3 to P802.1 – Bob Grow

- This will be a P802.3 effort whose purpose is to simply remove the existing standard from P802.3 and put it in P802.1
- After this effort has been completed revisions can occur
- There are timing issues to make this occur with P802.3 revision to insure a link aggregation standard is available

Discussion of this week's meeting agenda – Mick Seaman

- Sorted out what will be discussed this week

Security Task Group, Monday, January 22, 2007

P802.1ar Discussion – Mike Borza

Is a protocol needed in P802.1ar?

- The consensus is any protocol should be in P802.1af not in P802.1ar
- There may be timing and logistical issues with coordinating with P802.1af
- "The standard will define a service interface that all compliant implementations must provide and a reference to P802.1af as an example of a protocol that leverages DevID."

Security Task Group, Monday PM, January 22, 2007

RSA and ECC in 802.1AR – Max Pritikin (given by David McGrew)

- This presentation is on the web site
- The performance increase in ECC is not compelling for P802.1ar versus AES
- NIST specifications show 112 bits as secure through 2030 and 128 bits as secure indefinitely
- Is a key that is good till 2030 okay?
- Performance – key generation
  - ECC is faster but DOCSIS has shown that use of RSA is not insurmountable
  - This is a definite advantage for ECC but there are ways to make RSA work

- Performance – crypto operations
  - Signing – ECC requires fewer resources
  - Verification – RSA requires fewer resources
  - P802.1ar has to perform the signing operation only infrequently; it is the identity management infrastructure that will need to scale to the number of devices in the network
- Discussion about key generation at device manufacture time
  - For inexpensive device this process must be fast and not require much overhead otherwise the manufacture cost increases
  - There may be a different view between the manufactures that are in an "inexpensive device" versus a larger system
  - Do not want a server "you trust" on the manufacture line
  - Do not introduce delay on the manufacture line – do not increase the cost of the device
  - This is a big strength of ECC
- Gate Counts
  - Again this is a debate between big devices versus small devices
- TCG uses RSA for compatibility
  - Need a bit more interaction with TCG on this issue
- PKIX and ECC
  - In progress – continued discussions on list and via draft submissions
  - Would use of ECC imply a dependency on incomplete standards?
  - We should have an official discussion with IETF WG to understand what they are considering
- Transport Costs
  - RSA keys are larger
  - Might cause trouble with large UDP packets, etc
- Comments or discussion
  - There needs to be a good discussion about ECC/RSA issue
  - 128 bits is the barest minimum
  - Regarding keys not meeting NIST 2030 date does not imply that the device will fail in 2030
  - The 2030 date could be a problem for consumer electronic devices because they have a very long time span (40 years)
  - Consumer electronic devices would prefer the indefinite time
  - What we are discussing is "what is the minimum?"
    - This will create an interoperability problem
    - Verification versus generation – your devices generations the small key size but must be able to verify a larger key
- So where does this leave us?
  - This discussion was more around key length not ECC and RSA
  - What is the consensus between 112 and 128 bits?
    - What is the probability of the 2030 date being accelerated?
      - This date will probably stand unless there is some large break through

Right now we have text that says 2048 bit RSA so a way forward is waiting for comments

We may have folks criticizing this decision so we need to have a solid basis for what the committee deciding

A way forward may be to require 2048 generation and 3072 verification

Is there an organization that standardizes or requires ECC?

Straw Poll

Is it worth while to investigate 2048 bit signing and 3072 verification?

Many for and no against

Some one needs to investigate this and report back

Should we continue specifying RSA with a possible unknown of the key size?

Paul will look for organizations that have standardize ECC

Discussion about whether it is best to have a mandatory and optional crypto

We had this discussion at the last meeting so we need to make a decision

Not all the necessary people are in the room to make the decision

What is the impact on the document?

It is not a lot of work to change the document

Should we defer this discussion and focus on other issues so we can progress the document

There does not appear to be any consensus on this issue

There appears to a be a consensus that the standard provides interoperability across all devices – do not create an option that allows the for interoperability problems

Proposal on the floor to leave the document as is and work on other items

This will allow comments and we will deal with them as they are balloted

What is the cost in gates to verify RSA?

This would help determine the cost on consumer devices

The implementation for verification and signing are about the same

Comment disposition P802.1ar – Mike Borza

Review of the technical comments and accept the editorial changes

The ballot comment disposition is the official repository of how the comments were dealt with

Security Task Group, Tuesday AM, January 23, 2007

Review of P802.1af – Mick Seaman

Should get a task group ballot after the March meeting

Discussion about separate security interim in May

Paul will see about Sacramento

Consider a 3 day and figure on leaving after lunch on the third day

Week of May 7 looks good

Go through the various parts of the draft indicating what was done and what needs to be accomplished soon

Goal was to get all the clauses in place

Need to get wake on LAN and wake on LAN packet format

- There was a difference of opinion concerning what packet format was needed
- Worked on introduction and the scope clause
  - The scope should describe in detail in section 1.2 what is where in the document
  - New managed object clause for KaY
- How many different conformance clauses will be needed?
  - Is it a protocol conformance?
  - What system level conformance will be demanded?
  - The goal would be complete interoperability
  - This takes us into the EAP method issues
    - Currently, do not know which EAP method will be used
  - Need to get to KaY standing on its own, which will improve the performance clause
  - Need to be able to say if you previously did 802.1x then you currently should conform
    - This will break if a specific EAP method is required
    - If backwards compatibility is a goal then the selection of EAP methods will be constrained
    - Previous discussions wanted to restrict the EAP methods to a small set
    - There are several EAP methods that will be standard track in the future
    - TLS should be a standard track soon
  - Discussion about how to choose and proceed with regards to EAP type
    - One way forward is put out a draft that requires TLS
    - Can there be different levels of conformance so previous implementations are not disenfranchised?
    - TLS is probably the best option available today
    - There are a number of emerging technologies that would supersede TLS
    - TLS has a high overhead, which can cause problems for some devices that need
    - Most implementations begin with OpenSSL, which has high overhead
    - It would be an onerous requirement to require TLS if it is not linked to P802.1ar
    - Trial – we require EAP authentication methods and recommend TLS
      - There is a difficulty in requiring something in another standard so saying if P802.1ar then must use TLS in P802.1af
      - There should be some type of linkage
      - You could say if you do TLS then you must do it the way P802.1ar specifies
      - There must be a minimum mechanism to perform mutual authentication – this may be pre-shared keys
      - EAP TLS does provide the ability to put a box on the network and being able to find the box and authentication
    - Summary
      - Mick will put this into the conformance clause so everyone has the opportunity to sort thorough it
- KaY Options
  - Pre-shared keys

- They do not belong in MKA
- Think of MKA as a blob and the KaY simply provides the keys from the PAE or from the pre-share
  - This simplifies the MIB layout
  - Would make pre-shared keys mandatory
    - This is not a burdensome requirement
    - Some discussion that pre-shared is not necessary
    - Maybe specify an interface for pre-shared keys
    - The example of pass phrase to key in wireless network is a problem
      - The results of how the key is represented and how the key is put into the device must result in the same key
    - The MIB would take a string and convert it into a key in a standard way
- Summary
  - Pre-shared keys will be optional but if implemented then the MIB will take a string and create a key with a specified key
  - Further discussion – the object should be a text string that represents a raw key. Then the vendor can use what ever method to generate the key but they must provide the raw key in a string representation that is put into the device via a MIB object
  - <Find data on pre-shared keys and the current state of the standards and practices>

Wake on LAN

- Clause 7.1.4
  - Should reflect how networks are used today to create a guest/authenticated VLAN until they are authenticated
  - Show how the security, KaY integrates with the bridge, to show how communications works and make sure it does
  - Must realize that most networks do not have VLANs – most small networks do not have VLANs so this standard is a bit beyond the typical implementation. Hence, 7.1.4 provides a filtering of frames to provide the security by frame filtering rather than VLAN tagging
  - Review of figure 7.5
    - Shows how the filtering of frames would work between authenticated and unauthenticated sides of a network
    - Want the management protocols flowing so the network can be maintained
    - The rule is any frames that will be selectively relayed will be quickly recognizable quickly, which implies a well known address
  - Review of figure 7.14
    - Multi-access LAN with MAC Sec
    - See also figure 7-12 to understand the context of figure 7-14
    - Generalize model of the multi-access LAN is shown in figure 7-13

- This is to allow an unsecured entity to bootstrap into the secure network
- This is the biggest thing in the draft even though it is a small amount of text but it is a non-trivial issue
- This text relies upon knowledge of how the bridge operates to setup a network and to setup security
- Add a clarification to 7-14 that it is a specific representation of 7-13
- To make the WoL practical we will have to pick one
- Is this bi-directional or uni-directional?
  - Currently, it is uni-directional
  - To extend to bi-directional we would have understand all the incoming frames and their respective security threats so we can understand the potential threat vectors coming from an unsecured network into a secured network
- There are the cases where stations on the shared LAN do not care about MACSec and those stations that want MACSec but must bootstrap and exist on a real shared media

Clause 13 MIB

- Is the introduction correct?
  - The text was taken from P802.1AE
  - Needs a review to make sure it is correct
  - The general purpose objects of P802.1AE should also exist in P802.1af
- What security considerations should be in the MIB?
  - What approach to take to put this together?
    - There appears to be two ways to approach so input is needed to sort out the correct way to go
  - A lot of the material is available from P802.1AE
  - Underlying principles
    - A key can be written but not read
    - Some LAN protocols allow sniffing a packet and the key to decrypt can be determined
    - The MIB could reveal some things but the desire is to reveal only locally
  - An approach
    - Here is a set of objects and determine the security consideration from there
  - Discussion of approach
    - It is the access of the objects that creates the security
    - From top down look at the object and understand the scope of their affect
    - A risk assessment of the objects would be a useful approach
    - There are some tools in the IETF that may provides these capabilities
    - How the keys are distributed Master/Session and localization of keys

Is SNMP a good way to distribute keys?
There are a limited number ways to distribute keys
Is there a classification of the exposures that exist with the MIBs?
    This implies looking at the operational requirements
    There are probably only a half dozen categories
Does SNMP version 3 have a local view?
    Not really
    Need separate security policies
    SNMPv3 looks at authenticated or not authenticated
    It is out of context of the protocol but it can be done with mechanism such as IP address filtering
There can be a initialization state and then write is removed so the administration can create a key but once the user has "used" the key the administrator can not modify the key again
SNMPv3 can use 3DES and AES the original standard called out DES
This means we need to strengthen the SNMPv3 requirement in both P802.1af and P802.1ar
The only way to do key distribution is using EAP TLS
RFC 3826 is SNMPv3 with AES

Security Task Group, Tuesday PM, January 23, 2007

P802.1ar comment resolution – Mike Borza

Continued from yesterday the review of ballot comments
The official disposition of comments is kept by the editor and is available on the P802.1 web site

Mike is no longer able to continue as editor – Mick Seaman

We want to thank Mike for his work
Discussion about how and who can replace Mike
    It is essential to have an editor
    The editor must understand and defend the document
        This is a must to get through sponsor ballot

Back to comment resolution – Mike Seaman

Discussion about how to capture the authentication mechanism
    P802.1af is the most logical place but then there is a discussion within the context of P802.1af about what it will require
    So P802.1ar will point to P802.1af as providing an authentication mechanism to be used by default when P802.1ar identifiers are available
Discussion about requiring a mechanism that identifies a remote as being an P802.1ar device
    Is there a reason to identify a certificate as a P802.1ar?
        No
        Maybe a non-critical extension could be used
Discussion about authorization
    Are we going to start worrying about authorization after the authentication?
    Questions about this being in scope not only for P802.1ar but P802.1x, etc
    This may help but it is probably out of scope

Discussion about a standard reference for keying and key insertion

There are no standards that specify how to do key insertion into a device

Discussion about notAfter time

The IDevId should use infinity and LDevId can set the value to a specific time and P802.1ar must enforce the notAfter time

Discussion about clause 7.5.4 Random number generator

Attendees:

NAME	SURNAME	Affiliation
Osama	Aboul-Magid	Nortel Networks
Florin	Balus	Alcatel-Lucent
Vinay	Bannai	Adtran
Hugh	Barrass	Cisco
Alan K	Bartky	Broadcom
Davide	Bergamasco	Cisco
Jan	Bialkowski	Infinera, Inc
Rob	Boatright	Harman Pro
Jean-Michel	Bonnamy	France-Telecom
Mike	Borza	Elliptic Semiconductor
Paul	Bottorff	Nortel Inc
Rudolf	Brandner	Siemens Networks GMBH & co KG
Robert	Brunner	Ericsson
Frank	Chao	Cisco Systems, Inc
Jaihyung	Cho	ETRI
Paul	Congdon	Hewlett Packard
Diego	Crupnicoff	Mellanox
William	Dai	Broadcom
Wael	Diab	Broadcom
Thomas	Dineen	Self
Linda	Dunbar	Futurewei Technologies
Hesham	Elbakoury	Nortel
David	Elie-Dit-Cosaque	Alcatel-Lucent
Don	Fedyk	Nortel
Felix Feifei	Feng	Samsung
Norm	Finn	Cisco Systems
Howard	Frazier	Broadcom
John	Fuller	Gibson Guitar
Geoffrey	Garner	Samsung
Anoop	Ghanwani	Brocade
Franz	Goetz	Siemens
Mark	Gravel	Pro Curve Networking by HP
Eric	Gray	Ericsson
Ken	Grewal	Intel
Robert M.	Grow	Intel
Craig	Gunther	Harman Pro
Mitch	Gusat	IBM Research
Steve	Haddock	Extreme Networks
Chuck	Harrison	None
Brian	Hassink	Hatteras Networks
Myron	Hattig	Intel
Asif	Hazarika	Fujitsu
Guy	Hutchison	NOT CONFIRMED

Raj	Jain	Washington University in Saint Louis
David	James	Self
Tony	Jeffree	Self, Cisco, Broadcom, Hewlett Packard
Michael	Johas Teener	Broadcom
Keti	Kilcrease	Cisco Systems
Tae-eun	Kim	Extreme Networks
Yongbum	Kim	Broadcom
Mike	Ko	IBM
Raghu	Kondapalli	Marvell
Kwok	Kong	IDT
Bruce	Kwan	Broadcom Corp
Kari	Laihonen	Teliasonera
David	Law	3Com Europe Ltd
Yannick	Le Goff	France Telecom
John	Lemon	Adtran
Gael	Mace	Thomson
Dan	Maltbie	Woven Systems, Inc
David	Martin	Nortel Networks
David	McGrew	Cisco
Menucher	Menuchery	Marvell Semiconductors
John	Messenger	Adva Optical Networking Ltd
Dinesh	Mohan	Nortel
Pedro	Nunes	Siemens Networks
Don	O'Connor	Fujitsu Network Communications
Karen	O'Donoghue	NSWCDD (US Navy)
Hiroshi	Ohta	NTT
David	Olsen	Harman Pro
Shlomo	Ovadia	Entropic Communications
Tim	Ozugur	Alcatel-Lucent
Rong	Pan	Cisco Systems
Glenn	Parsons	Nortel
Mark	Pearson	Hewlett-Packard
Neil	Peers	Adva Optical Networking Ltd
Joe	Pelissier	McData
Karen	Randall	Randall Consullting
Dwayne	Reeves	Fujitsu Network Communications
Guenter	Roeck	Teak Technologies
Josef	Roese	Deutsche Telecom
Allyn	Romanow	Cisco Systems
Dan	Romascanu	Avaya
Jessy V	Rouyer	Alcatel-Lucent
Eric	Ryu	Samsung
Ali	Sajassi	Cisco
Joseph	Salowey	Cisco
Panagiotis	Saltsidis	Ericsson
Mick	Seaman	Mick Seaman
Koichiro	Seto	Hitachi Cable
Himanshu	Shah	Ciena Corp
Ravi	Shendy	Emulex
Gopi	Sirineni	Marvell
Nurit	Sprecher	Seabridge Networks
Kevin B	Stanton	Intel
Bob	Sultan	Huawei Technologies
Richard	Sun	Dallas Semiconductor
Muneyoshi	Suzuki	NTT
Attila	Tacacs	Ericsson
Francois	Tallet	Cisco

Bert	Tanaka	Woven Systems
John	Terry	Brocade Communications
Pat	Thaler	Broadcom
Geoff	Thompson	Nortel/GCSI
Oliver	Thorp	Fujitsu
Fred	Tuck	NOT CONFIRMED
Maarten	Vissers	Alcatel-Lucent
Dennis	Volpano	Cranite Systems
Manoj	Wadekar	Intel
Brian	Weis	Cisco
Bert	Wijnen	Alcatel-Lucent
Peter	Willis	BT
Michael D.	Wright	Senforce Technologies
Yongji	Wu	Huawei Technologies Co Ltd
Zong Liang	Wu	Entropic Communications Inc
Ming	Zhang	Cisco Systems