IEEE 802.1 Minutes, January 2004

Interim Meeting, Monday AM, January 12, 2004

Notes taken by Michael Wright and Allyn Romanow, allyn@cisco.com

Summary of LinkSec

802.1X

Short discussion of disposition of comments. Will incorporate ballot changes and recirculate, while sponsor ballot pool is being formed.

802.1AE

Went through the comments on Task Group Ballot. Decided not to have another ballot before the next meeting, to clean up the document based on discussions and comments, and ballot after the Plenary meeting.

802.1af

Started to lay out the pieces – presentations by Jim Burns and John Hollbrecht
Invite contributions of use cases for key management and authentication
Invite contributions for key management methods, as discussed in John Viega's slides
Invite contributions on central partitioning of the KEYsec work

Agenda – Tony Jeffree

- Administrative stuff
  - Officers
  - Website
- Voting membership rules
- 802.1 WG and TG operation
- Patent Policy
  - The two required slides were shown to the committee attendees and the chair made sure everyone in the room was aware of the policy
- May Interim
  - May be in Barcelona in May, Norm may help

Task Group Agenda – Mick Seaman and Dolors Sala

- Need more and better comments
- Maybe make the ballot working group so if folks don't respond then lose voting privileges.
- Need work on increasing the PDU size
  - How big will the .1ad extension be and also how big will the MACSEC extension be
  - Need to get this done now so the various standards that are depended are not held up.
  - Next step is get ready for a joint session in March so we need to get ready

MACSEC – Dolors Sala

- Need better ballot responses here and contributions!!!

Disposition of comments 802.1ad – Allyn Romanow

- See the disposition document for the official disposition of comments
- Several comments were extensive enough to create a new draft on the server
- Discussion of SA and Group SA definitions and use
- Mick did a presentation of his view of Group SA and SA

Interim Meeting, Monday AM, January 12, 2004

Ballot Disposition of 802.1ae – Allyn Romanow

See the disposition document for the official disposition of comments
Discussion of section 7 – use of the terms uni-directional and directional and how these terms are used in the document and what are their meanings.
Discussion about the definition and use of SAID
Discussion about cipher suites – which to use, how to specify without stopping value add
Selecting a mandatory algorithm should be to increase interoperability
But need to understand there are markets that will require their particular cipher suites.
ICV coverage discussion
Number of comments about what should be covered and what should not be covered

Interim Meeting, Tuesday AM, January 13, 2004

Review of new Clause 6 of 802.1ae/D2-1 – Mick Seaman

Review of Clause 6 so folks know what to look for and what its purpose is
Not much to see if things said here has been said in other places in the document
This clause should stand on its own that is read separately
Look at threats posed by abuses of the MAC Service
MAC Service refers both to the ISS and services provided to LLC client
Place holder 6.4 for status and point to point parameters – this is discussed in other places in the document
6.5 is a discussion of security threats, which has been revised
    Add delayed or out of order frames to list of threats
    It would be out of scope to try to enumerate exploits that this standard will not solve. There is a short list at the end of Clause 6.5 that lists some of these types of things that this standard will not solve.
6.7 MACSec guarantees
    List of what it will guarantee and a list of what it can guarantee
    Explanation of what is meant by bounded time – for example what is the time it would take an attacker to figure out key.
    List of what it does not do
6.8 Security services
    This section needs text from others. Please contribute
    Need some policy to localize attacks
6.9 Quality of service maintenance
    Can attack the operation of particular MACs
    Limit the use of MAC control frames to setup connections then after connection setup use MACSec facilities to setup QOS
    List of QOS was taken from earlier work
Discussion of priority issues, how to maintain priority, etc

Disposition of ballot comments 802.1x Rev/D8 – Tony Jeffree

Will put the ballot changes and do another recirculation. This will not delay much because during this time the sponsor ballot pool has to be formed.
There is a fix to the state machines that Jim Burns found supplicant backend state machine. Issue eapFail could be set in the request state – the state machines fail if this occurs.
Issues with the EAP signaling for mutual authentication
The discussion moved from simple signal to a discussion of what is the policy
Make sure the information being discovered in EAP are passed to 802.1x
Leave things as is for now. If this issue gets a better fix then it can be handled at sponsor ballot
MIB and state machine bug will be fixed and then a recirculation ballot will be run.

Disposition of ballot comments 802.1ae D1 – Allyn Romanow

Comment 71 – Jim Burns

Key agreement requirements
Gathered all of the Key agreement in the document and put in one place so we can understand it better
Discussion of signaling key and packet number exhaustion
Is this a generic interface or will there be a specific parameters?
The generic interface will be made more specific as we settle on the exact requirements of the cipher suite
These parameters will probably feed into the state machines
When do the LMI indications fire?
What is the definition of "almost exhausted"?
How much time should be given for renewal?

From KaY to SecY

Responses
What cipher suite SecY should be using
If null cipher suite if all the neighbors are SecY then can put SecTag on otherwise the SecTag is determine by management entity

LMI has signal that goes to the local box

What cipher suite is running on the SecY?
May be local services that want to bind to the cipher suite
Example – downloading policies from some policy server
Discussion about how to insure that services using this interface are authenticated to some level
Indication of authorization level
Discussion about where must the authentication knowledge must reside or what the authentication level of a device implies. You can not manage the network from the AAA server because it is not possible for the AAA server to have such knowledge

Assumption the KaY makes on the MACSec

Different Ethertype for MACSec frames

KaY runs outside of MACSec for independency to defend against DOS attacks
Detect location of DOS attacks
Range of things we can do to mitigate DOS attacks
Discovery
Connections between peer stations, what potential connections are available
Will not have a port up indication but will need mechanism to run KaY on the new connection
Need OperStatus to indicate there is a new connection so it can be known that the CA configuration has changed
If there is a change in the trust relationship then the LAN should bounce. This prevents attacks by some entity joining the LAN secretly.
Authentication
Not much effect on SecY it assumes authentication was completed
Authorization
Authorization levels – need more details
Host and infrastructure levels
MAC Service Maintenance
Some commit protocol
Don't cause an asymmetry in the connection
Need a fast commit protocol so startup is fast
Key Maintenance
Up to KaY to maintain the CA

KaY must not require one entity to communicate through the one it is trying to authenticate. There can not be any asymmetries.

Interim Meeting, Tuesday PM, January 13, 2004

Disposition of ballot comments 802.1ae D1 – Allyn Romanow
Comment 79 – Paul Congdon
Short discussion
Review of Section 9.3.1 – Allyn Romanow
SecTag is covered by ICV but not encrypted

802.1af, KEYsec Discussion
Lightweight Key Exchange and Authentication – John Viega
http://www.ieee802.org/1/files/public/docs2004/Authentication_and_Key_Exchange.pdf
There have been implementation difficulties with good crypto solutions
Requirements
Require mutual entity authentication, temporal consistency, i.e., replay protection
Web servers are the primary application that require one-way authentication
Entity authentication is implicit in message integrity. It is implicit that the entity sending the message is authenticated.
What can go wrong?

- One entity can pretend to be another
- Single entity authentication is rarely adequate and can lead to spectacular failures
- Password authentication is particularly suspect, but we will want to support it

Key management – secrecy necessary for authentication. Keys are necessary, and a source of big risk.

- A number of decisions about keys need to be made. There are many ways people think they are getting authentication, but they really are not.
- Provide secure means for initial key setup if possible, if it the first step needs to be insecure, it must be secure after that

Usability by the end-user is the most important requirement.

- Defense in depth, multi-factor, multiple methods, configurability, a range of solutions to meet various needs.

Efficiency – Public key crypto is expensive.

- Use it for doing things you can't do with symmetric keys. Use public key to start, and then switch to symmetric.
- How terse is the protocol? This is relevant in some environments, e.g., phones

Level of security assurance

- Traditional approach – lack of attacks, extensive review, no guarantees
- Model checking – model protocol as a state machine, use model checker to prove wither protocol is resistant to know attacks. Model checkers have significant limitations. The number of possible states to check is too large.
- Provable secure protocol – prove that the protocol is secure. If you find an attack on this protocol, then you have also found an attack on a well-vetted algorithm.
- Need a concrete security model and some review.

Interoperability – discussion of drawbacks of 802.1x, RADIUS, Kerberos, IKE

Other requirements –

- Multi-party – multipoint. We have ignored the shared key solutions
- Support for password reset.
- Protection against bad random number generators

Possible directions, John's suggestions

- Assumptions – mutual authentication, usability a priority, key exchange is necessary to form the secure connection, ignore multi-party and key servers for now
- Discussion of some features of symmetric and public key protocols

Initial thoughts- authentication alone is not adequate, must end up with a secure channel

- Shared secrets and password necessary
- Allow devices to cache credentials, long-term shared secrets stored in devices
- Lightweight shared secrets are the workhorses
- Support one-time setup for passwords – in an annex put recommendations for passwords.
- Provide forward secrecy
- Need a simple framework, avoid legacy that made IPsec difficult to adopt, i.e., IKE interoperation
- Start with public key based authentication, put new device on network, want to prove it came from the vendor you bought it from

Comment Mick – we could make new protocols or use a RADIUS server.

How not to take 3 years to do this part.

Comment Bob M.– What are we going to do for the keying mechanism?

There are people who want to write an EAP method.

Mick- wants one soup-to-nuts solution

John- what he would retain from IKE is the key management.

We should not use pre-existing structures that do too much for our relatively reduced purposes.

Mick would like to have use cases to talk about in detail at the next meeting.

The uses are extremely varied. Examples are edge and infrastructure.

Solicit contributions for a discussion of use cases

Contributions for methods, as per John's slides.

Contributions on central partitioning of the problem

Mick's thoughts on RADIUS and IKE.

Two different infrastructures in the world Radius, and IKE.

Some might view IKE that simply replace IP with MAC and your are done

Not so because of PKI

IKE looks good. Can easily be changed to accommodate our needs. However, all the attractive uses require PKI. Suggs we'll be using RADIUS.

PAR is in relation to 802.1X. Mick thinks of it as controlled and uncontrolled ports. Do we still want to use EAP? We should provide on set of options to use EAP.

Where are we? Known – could start a document which contains Jim's ballot comment – the requirements issue for LMI. Discussion about what methods and what qualification will be placed on them.

Frame size for 802.1AE – Allyn Romanow

GCM will not increase the size of the data

CVC will increase the size of the data

If optional cipher suites then have to account for the block size increase by various cipher suites

Discussion about how the encryption and block alignment works

The ICV should be at least twenty bytes

The nonce is the SOA and Packet Number

Use of the term EtherTypes – Mick Seaman

Need to define the term

Two places 802.3 or 802 O&A

Suggest that 802.3 define and a maintenance item for 802 O&A to point to the 802.3 document

Need a short term fix in 802.1AB to point to 802.3 for the definitions

Interim Meeting, Wednesday AM, January 14, 2004

Rules for signing the sign-up sheet – Tony Jeffree

Disposition of comments 802.1ab/D7 – Bill Lane

See the disposition of comments document for the official disposition of comments

172 comments
Couple of issues with handling undefined or improper use of TLVs

Interim Meeting, Wednesday PM, January 14, 2004

Ballot Disposition IEEE 802.1ad/D2 – Mick Seaman

Lots of discussion about how to carry customer priority from C-VLAN to S-VLAN when the two are in separate physical boxes connected by a MAC that can not carry priority – 802.3

802.1af KEYsec Discussion- Jim Burns – Architecture for .1af
http://www.ieee802.org/1/files/public/docs2004/802_1af_initial_block_diagram.pdf

Diagram shows a high level overview
Discovery phase – discover a connection
Then pass into authentication component, AAA component, EAP method

Results in a master key
Can succeed or fail at both authentication and at authorization time
After discovery, someone has to be the initiator and the responder. 1af does this.

The commit causes the enable session
Authentication cache is for the first time only, then go to the connection cache.
Master key stays in the authentication cache.

John Vollbrecht- 802.1af Directions
Slides http://www.ieee802.org/1/linksec/meetings/Jan04.html
Issues: There are 3 parts of .1af

1. Discovery –find who it is you're going to authenticate to
2. Authentication – an EAP method, get session key
3. Enable – execute the authorization, do the key exchange

Backends may be on either or both sides of the communication. Each circle could have a rule or policy
Requirements for Discovery

Discovery only for finding who want to authenticate to.
Why not use LLDP discovery?
How do discovery? – a variety of ways are possible.
If multiple EAP methods, when would one be selected?
. Requirements for discovery – find out what could connect to –wireless, Ethernet, etc.
Discovery is inherently insecure
Can use authentication to check on what find out in discovery
John Viega – keep discovery minimal- who can talk to and what the function is
Mick Seaman- alternatively, do more discovery to discover what you don't want to connect to. Keep discovery running all the time. Can get deep fast, a slippery slope.
A number of other protocols have worked on discovery, we should look at them.
What want to support, like roaming, impacts the characteristics of discovery.

Requirements – authentication

Assume EAP-style interface. Expect to use EAP methods

Interface from .1X to EAP, if there were another thing that could meet this interface, we would use it as well.
Want to define a minimal mandatory method, with a couple of additional approved methods.
Keying material – keying hierarchy model being worked on in IETF. We should use it. Can reuse keying material

Requirements- enable
Enable starts and stops the session
Some form of 4-way handshake
What do you start? The connection, a firewall, something else…
In .1AE, if nature of authentication changes, the port goes down
The port is brought down if anything trusted changes, or the authentication changes.
If authorization changes, protocol comes down and back up

Requirements- general
Architectural elements talk to the backend
Most likely be RADIUS, but could be something else
Consider SAML, used by WEB access and Global Grid Forum
SA required between all elements talking to each other. Assertions of attributes with proof of origin

Applications to investigate include:
.11 connection and reconnection
EAP key hierarchy
GGF
.1X
Oasis and WEB services – service authorization
Other?

Roaming in IEEE, may be doing something similar
Discovery – PANA and PPOE in IETF, how are they doing discovery?
Instances of use – profiles
We should have a couple of profiles, eg., automating network bring up
Make options very few
Mick presentation - CAs, SAs – clarification and some ideas
Rather than spelling out all potential options, have only point to multipoint SA, with point to point as a special case, rather than having two types of SAs – group and point to point
In maintaining a group, maintain separate states at the receiver
SOA is really the label for the temporal sequence of SAs

Interim Meeting, Thursday AM, January 15, 2004

Today's Agenda – Mick Seaman
Review Connection Management PAR review so it can be forward to exec
There will be a dropped precedence presentation today
Need to give 802.3 a heads up on frame size modifications for LinkSec and Provider Bridges

Ballot Disposition IEEE 802.1ad/D2 – Mick Seaman

See the disposition of comments document for the official disposition of omments
Consensus that provider should be able to detect loop in customer network and then be able to inform customer even before the customer know the problem xists.
Wording – review clause 5.1
The current clause 16.8 allows OEM loop detection or pointers to other standards that do loop detection. If you do not agree speak up.
Check with folks in the room if the current wording catches the spirit of loop detection. Consensus is any problems are language in the clause and everyone is agreed that loop detection is a good thing.
Dropped Precedence

Subject in general – Mick has tried to work out putting both explicit and implicit dropped precedence in the document. Conclusion, simply putting a set of parameters into the document would not work because of the ramifications to the whole. It looks like it is getting out of scope of the document – there is a section of industry that wants/needs this but how to accomplish it is the problem. Implicit - It is possible to get unexpected miss-ordering in the network this means management and service ramifications. That is a lot of stuff to sort out. Explicit – this is a service interface change. The editors understanding of the PAR was no service interface changes. Mick needs some direction that there may need a new PAR to do this.

Discussion – EISS does not have to be modified if it was the ISS then there would be a problem. There have been changes to the interface EISS already. Paul Bottorff – dropped precedence is an essential feature that must be included. What does the PAR say? The editor will not put it in without a vote from the committee. No new parameters without vote. This may not be a problem but need direction from the committee. There is probably a lot of support but it is more work than was previously thought. Need other folks to form some agreement about how the best way to solve this. The rule is do it right the first time and make sure everyone agrees it is the right way. The editor wants more than a comment of editor go fix the world – Mick wants the details sorted out from the beginning. We agree we want the effect but there is not consensus about how to do it. Discussion if explicit then the EISS has to change if implicit then no changes to EISS. The discussion is the editor wants other folks to step up now not later.

The best way forward is a small group of folks put together a draft solution. The solution must be complete so we understand the consequences of the changes.

This can not degenerate into a vote, change, vote, change it has to be consensus or this effort will never close.

Need to discuss getting a group together and what could be accomplished before the next meeting.

Need to go do our homework and determine what changes will be made and what are the consequences of those changes. The work is figure out what it takes to do each or both and can it be specified in the standard.

Who wants to be in the group? How will the group work? Done by email and at the next session
It is hard to get closure with email
Paul B, Norm, Steve, and a couple of others will be in the group

Metro Ethernet Connectivity Management Presentation – Norm Finn

Summarize what has been going on in ITU
Prove feasibility for the PAR
MEF is the coordination element for ITU and IEEE

Interim Meeting, Thursday PM, January 15, 2004

Metro Ethernet Connectivity Management Presentation Continued – Norm Finn
http://www.ieee802.org/1/files/public/docs2004/provider-con-mgt-slides-1.pdf

Connectivity Fault Management 802.1ag PAR V1.2 review – Mick Seaman

It is not a goal to do rapid restoration in this work
We have agreement so Tony will send it off to comply with the thirty day rule

How to proceed with Provider Bridge and how to resolve a couple of comments – Mick Seaman

Current state of the ballot
Last count 10 approves 6 disapproves 9 abstain – 62% approval
There will be a new revision of the comment disposition document
Mick would like to facilitate discussion about the points raised by the comment
Need to understand the consequences of the comments and the full extents of the changes to support the comment
Email exchanges will not get closure
Next meeting hope to have more idea how to bag the comment together to get them resolve and to setup break-out activities so issues can be resolved or to produce material that supports the current state of affairs
Lot of work at next meeting that will be hard to overlap – can have separate activities and get consensus
How to organize things for the March meeting to get the most work completed in the time allowed
Given the degree of consensus it would be useful putting more time on getting a draft together
Stick with four days – reduce the number of ballots at the same time
Some of the subgroup meetings will have overlap during the March meeting
How many rooms will be needed? One room for main session and two additional rooms of modest size to have two breakout sessions for the end of the week
Comments on AD – comments that help address what is in progress not necessarily in general comments that is help the situation or the consequences
They should fall into the current major sessions
What breakout sessions would there be? Dropped Precedence at least
Comment 42 Muneyoshi Suzuki
There are lot of other things that depend on this – OAM work and MACSec
Test out that the proposed resolution is okay

Comment – the architecture is not consistent with .1d and .1Q
The comment will be reject in principle however Mick will clarify the text with .1ac to make the interface look like EISS
MACSec is lined up with this model but may effect key agreement

There will be a pre-meeting 9 – 11 am at the March meeting
Next thing with AB – confirmation ballot and resolve in the March meeting
Will do the ballot disposition as a separate activity
Tony may add task group ballots to the list of ballots that you must respond to in order to maintain voting status – this will get some folks paying attention and getting the work processed
Agenda item for next March to do Real Time Ethernet

Attendees:
Brian Arnold
Paul Bottorff
Jim Burns
Dirceu Cavendish
Paul Congdon
Sharam Davari
Arjan de Heer
Craig Easley
George Eaton
Anush Elangovan
Hesham Elbakoury
Norm Finn
David Frattura
Gerard Goubert
Steve Haddock
Onn Haran
David Harrington
Kunio Hato
Marc Holness
Tony Jeffree
Manu Kaycee
Yongbum Kim
Bill Lane
Loren Larsen
Yannick Le Goff
Marcus Leech
Dennis Lou
Bill McIntosh
John Messenger
Dinesh Mohan
Bob Moskowitz
Satoshi Obara
Don O'Connor

Karen O'Donoghue
Don Pannell
Glenn Parsons
Karen Randall
Allyn Romanow
Dan Romascanu
Jessy V Rouyer
Ali Sajassi
Dolors Sala
Sam Sambasivan
Mick Seaman
Koichiro Seto
Yoshihiro Suzuki
Michel Thorsen
John Viega
Preeti Vinayakray-Jani
John Vollbrecht
Karl Weber
Bert Wijnen
Ludwig Winkel
Michael D. Wright
Mi Jeong Yang