LinkSec CipherSuites Revisited

David Johnston

david.johnston@ieee.org

dj.johnston@intel.com

What will LinkSec Offer?

- Data Privacy
- Data Source Integrity
- Replay Protection
- It will NOT offer
  - Non Repudiation
- It probably cannot offer
  - Protection of non-data packets
    - They differ between MACs
    - They don’t work encrypted

The need for Cryptographic Suites

- The need to choose a set of cryptographic methods in LinkSec has been discussed
- Can choose between many things
  - Parameters (PN length, ICV Length etc)
  - Privacy modes (CTR, CBC etc)
  - Integrity modes (HMAC-SHA1, MD5, OMAC, PMAC etc)
  - Block Functions (AES-128, DES, 3DES-EDE etc)
  - Combo Modes (CCM, OCB)

Cipher Suites are Best

- Many of the options on the previous slide interact (E.G. linking privacy with auth)
- Conservatism leads us to try and stick with modes used in their 'default' configuration.
  - Twisting modes around has in the past led to misuse and hence poor security
  - Variation of parameters can lead to poor security (e.g. variable tag sizes in CCM)
- Hardware implementation issues lead us to defining a minimal and useful default set of features
- So a cipher suite approach is an approach that allows us to work within these constraints
  - Each entry can be verified for security as a static configuration
  - The interaction between modes would be well defined for each cipher suite entry. Each mixing would have its own entry.

Basic Primitives

- Null, RC4, DES, 3DES, AES, HMAC-SHA1 etc
- Impacts:
  - HW Implementations
  - Crypto strength
  - Exportability
  - Interoperability
- AES is crypto du jour
- NULL is probably necessary
- RC4-40 has been used for exportability before but is not a good choice for engineering reasons
  - it has a heavily serial algorithm

Privacy

- FIPS standards specifies crypto modes using DES, 3DES and AES-128
  - Not a bad place to take guidance
  - Simpler FIPS related approvability for devices
  - DES deprecated for new equipment
  - Unencumbered, parallelizable modes available (E.G. CTR)
    - Good for speed

Integrity

- Auth mode based on block crypto function is a nice approach for implementers. FIPS is less useful here
  - Authentication modes still a matter of debate in NIST
  - OMAC is looking like the most likely candidate for FIPS approval
    - Not parallelizable
- Other parallelizable options are encumbered
  - E.G. PMAC
- Could use an auth specific algorithm
  - HMAC-SHA1
    - Works
    - Requires independent hardware

Combo Modes?

- There are combined confidentiality modes that use a single block cipher
  - CCM
    - Not parallelizable
    - Non encumbered
    - Used in 802.11i
  - OCB
    - Parallelizable
      - Addresses the needs of really high speed equipment
    - Encumbered
      - Must be optional if it is specified at all
    - Bigger
      - Needs AES decrypt => more gates
- These are the engineers choices
  - One cipher block implementation
  - AES a known quantity

Basic Goals for Ciphersuite Entries

- Likely to lead to FIPS 140 approvability
- Meets implementation constraints
  - Speed, cost, size etc
- Allows interoperability
- Is not trying to be ‘creative’ with the crypto

Frame Format Requirements

- Crypto has an impact on the frame format
  - Insertion of IVs
  - Appending MACs
- What should this stuff be bound to?
  - It seems a ciphersuite would be appropriate
- Might some of this be parametizable?
  - IV length? Key Length? MIC length?
  - May then have to dynamically inform a frame formatter how to behave, redefine MTU etc.
- Alternative is to only permit defined ciphersuites
  - My preferred option, parameters sound like too much complexity

The need for ciphersuites

- Privacy and Integrity methods interact
- Different mixes impact the frame format differently
- A Ciphersuites list gives a list of permitted combinations or instances of combo modes
  - Frame format effects tied to the ciphersuite entry
  - Easier to negotiate cipher suites than combinations of privacy and integrity algorithms

E.G.

- Null
- Auth only – OMAC
- Non secure (40 bit) mode
  - Why bother? NULL is insecure, an illusion of security is worse than none at all.
- AES-128 in CCM mode
  - Keylength = 128 bit
  - Frame expansion = ??
  - Great for wireless devices
- AES-128 in OCB mode
  - Keylength = 128
  - Frame expansion = ??
  - Great for very high speed devices
  - But is encumbered – Pay your $$

The provider bridge problem

- Provider bridges result in end to end connections (and SAs) between dissimilar technologies (e.g. 802.11 vs. 802.3)
- Likely to be variations in crypto needs
  - PN length, parallelizable modes etc.
- Need a global default, present on both devices to address this case.
  - Must address speed, cost needs of lower end device

Vendor Proprietary & Playpens

- Vendor Proprietary areas and playpen areas are needed for all the usual reasons
  - So include an OUI in the table
  - Include a playpen area in the 00-00-00 OUI

A Suggested Ciphersuite

OUI	Cipher #	Type	M/O	Defined in
00-00-00	0	NULL	Mandatory	x.y.z
00-00-00	1	AES-128 in CCM Mode	Mandatory	x.y.z
00-00-00	2	AES-128 in OCB Mode	Optional	x.y.z
00-00-00	3	OMAC	Mandatory	x,y,z
00-00-00	4	PMAC	Options	x.y.z
00-00-00	4-32767	*Reserved*		
00-00-00	32768-65535	*Playpen*		x,y,z
ab.cd.ef	0-65535	*Vendor Proprietary*		x,y,z

There are other ciphersuites

- That was the data confidentiality ciphersuite
- Also will need others
  - Port authentication ciphersuite
  - Key exchange ciphersuite
- These are the domain of another PAR
  - But the combination of these may lead to the need for higher level cipher suites (crypto||key exchange||device auth entries)

Mandatory/Optional Issues

- Presence of unencumbered modes with low overhead address needs of low end devices
- Presence of default modes addresses provider bridge case
- Optional modes might be mandatory for some devices for technical reasons (e.g. parallelizability)
  - Need to make sure the dividing line is clear
  - So define the dividing line. E.G. OCB mandatory above 1.1 gbps.

Negotiable Elements

- There is good reason to make some elements negotiable
  - Primarily PN length. Different priorities exist for different MAC/PHYs
  - Can do this by increasing the number of cipher suite entries
    - Eliminates the need for secondary negotiation mechanisms
    - Is one way of keeping the parameter constant during the life of an SA

Backup info – AES Modes Speed

- Fast AES block => 11 clocks per AES
  - For CCM mode => 2 AES per 128 bits
  - 1Mhz => (128*(10^6))/2*11 bps => 5.8 Mbps
  - 50MHz easy in 1.3u
    - AES-CCM good for 250Mbps serial data. Can be stretched > 2gbps
- OCB allows parallelization and has fewer AES invocations
  - 1MHz => 11.64 Mbps
  - Multi gigabit devices can be addressed
  - Less feed forward => Pipelining easier => 200Mhz+ straightforward
  - No upper limit on speed