RSA and ECC in 802.1AR

Max Pritikin
(Channeled by David McGrew)

Key sizes

- The questions around RSA vs ECC are not related to the relative security of these algorithms.
- NIST specifications show 112 bits as secure through 2030, and 128 bits as secure indefinitely
  - "Recommendation for Key Management – Part 1: General", NIST Special Publication 800-57, August, 2005. http://csrc.nist.gov/CryptoToolkit/kms/SP800-57Part1August2005.pdf
- Slightly larger key sizes recommend by European Network of Excellence in Cryptology (ECRYPT)
  - "Yearly Report on Algorithms and Keysizes",ʌEuropean Network of Excellence in Cryptology (ECRYPT), Information Society Technologies,ʌD.SPA.10ʌ(2004).ʌ http://www.ecrypt.eu.org/documents/D.SPA.10-1.1.pdf

NIST recommended Key lifetime

Table 4: Recommended algorithms and minimum key sizes

Algorithm security lifetimes	Symmetric key algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
Through 2010 (min. of 80 bits of strength)	2TDEA[22] 3TDEA AES-128 AES-192 AES-256	Min.: $L = 1024$; $N = 160$	Min.: $k=1024$	Min.: $f=160$
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: $L = 2048$ $N = 224$	Min.: $k=2048$	Min.: $f=224$
Beyond 2030 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: $L = 3072$ $N = 256$	Min.: $k=3072$	Min.: $f=256$

NIST recommended Key size

Table 4: Recommended algorithms and minimum key sizes

Algorithm security lifetimes	Symmetric key algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
Through 2010 (min. of 80 bits of strength)	2TDEA[22] 3TDEA AES-128 AES-192 AES-256	Min.: $L = 1024$; $N = 160$	Min.: k=1024	Min.: f=160
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: $L = 2048$ $N = 224$	Min.: k=2048	Min.: f=224
Beyond 2030 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: $L = 3072$ $N = 256$	Min.: k=3072	Min.: f=256

ECRYPT security levels

Table 7.1: Minimum symmetric key-size in bits for various attackers.

Attacker	Budget	Hardware	Min security
"Hacker"	0	PC	51
	< $400	PC(s)/FPGA	56
	0	"Malware"	59
Small organization	$10k	PC(s)/FPGA	62
Medium organization	$300k	FPGA/ASIC	66
Large organization	$10M	FPGA/ASIC	76
Intelligence agency	$300M	ASIC	81

ECRYPT key size equivalences

Table 7.2: Key-size Equivalence.

Security (bits)	RSA	DLOG		EC
		field size	subfield	
48	480	480	96	96
56	640	640	112	112
64	816	816	128	128
80	1248	1248	160	160
112	2432	2432	224	224
128	3248	3248	256	256
160	5312	5312	320	320
192	7936	7936	384	384
256	15424	15424	512	512

802.1AR thoughts

- Specify keysize recommendations in number of symmetric key bits
  - I think 112bits
  - 128bits? (e.g. beyond 2030?)
- "For the purposes of use the DevID never expires." (section 6.2.2)
  - We've indicated it is the peer application leveraging the DevID that determines if the NIST etc lifetimes are acceptable. Should we directly reference the lifetimes?
  - Is it realistic to provide better than this with current technologies?
- A 128bit LDevID based on a 112bit IDevID is secure beyond 2030

Performance (key generation)

- Key Generation
  - ECC is faster but DOCSIS has shown that use of RSA is not insurmountable
    - In fact this argues that RSA is acceptable all around as it is successfully used in various deployments today
    - Batching and hardware assist used with RSA

Performance (crypto operations)

- Signing
  - ECC requires fewer resources
- Verification
  - RSA requires fewer resources
- A supporting 802.1AR 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.

Gate counts

- ASIC RSA implementation in 0.35um, RSA-1024
  radix-4: gate count: 132K, performance 237Kb/s
  radix-16: gate count: 155K, performance 377Kb/s

  "Two Fast RSA Implementations Using High-Radix Montgomery Algorithm"
  Soner Yeşil, A. Neslin İsmailoğlu, Y. Çağatay Tekmen, Murat Aşkar
  http://www.bilten.metu.edu.tr/Web_2002_v1/tr/yayinlar/RSA.PPT

- FPGA and ASIC implementation of ECC in 0.35um for ECC in GF(2^163):

  ASIC gate count: 46 K gates, performance: 53Kb/s
  http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/9966/32022/01489020.pdf

- These citation suggests that the advantages that ECC has over RSA is something like "twice as fast or half the circuit size" (How much advantage would 50k fewer gates be?)

Thanks to Ming Zhang

TCG uses RSA for compatibility

- (What happened to the liaison?)
- "The TPM contains a 2048-bit RSA key pair called the endorsement key (EK)."

  https://www.trustedcomputinggroup.org/specs/TPM/Main_Part1_Rev94.zip

- "Version 3 of the X.509 certificate structure can be leveraged to dovetail TCG credentials into existing PKI tools and services. TCG credential profiles do not utilize all aspects of X.509 defined fields and some fields are overloaded with TCG specific interpretations."

  https://www.trustedcomputinggroup.org/specs/IWG/Credential_Profiles_V1_R0.981-2.pdf

TCG

- “TCG standardizes the RSA5 algorithm for use in TPM modules. Its recent release into the public domain combined with its long track record makes it a good candidate for TCG. The RSA key generation engine is use to create signing keys and storage keys. TCG requires a TPM to support RSA keys up to a 2048-bit modulus, and mandates that certain keys (the SRK and AIKs, for example) must have at least a 2048-bit modulus.

  https://www.trustedcomputinggroup.org/groups/TCG_1_0_Architecture_Overview.pdf

PKIX and ECC

In progress

- Continued discussions on list and via draft submissions
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-ecc-pkalgs-03.txt
  - (expired draft) http://tools.ietf.org/wg/pkix/draft-ietf-pkix-sha2-dsa-ecdsa/draft-ietf-pkix-sha2-dsa-ecdsa-00.txt
  - Algorithm Identifiers in Subject Public Key Info under active discussion

Would use of ECC imply a dependency on incomplete standards?

Transport Costs

- RSA keys are larger
  - RSA keys & signatures ~ 256 bytes
  - ECC keys & signatures ~ 32 bytes
- *Might* cause trouble with large UDP packets etc.