ROYAL HOLLOWAY UNIVERSITY OF LONDON

Challenges in standardising cryptography

Chris Mitchell
www.chrismitchell.net

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

1. Crypto standards – a selective history
2. Challenges
3. Ways forward
4. Some random concluding remarks

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

1. Crypto standards – a selective history
2. Challenges
3. Ways forward
4. Some random concluding remarks

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Data Encryption Standard (DES)

- Standards have played a major role in cryptographic developments for 40 years.
- In the 1970s, the US National Bureau of Standards (NBS), which later became the National Institute for Standards and Technology (NIST), requested proposals for a block cipher to become a US federal standard.
- This was implicit recognition that cryptography was becoming a vital technology for more than just the military.
- IBM made a proposal which, after modifications proposed by the NSA, became the hugely important/influential DES.
- DES, whilst now insecure in single key mode, remains in widespread use in multiple key mode.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Modes of operation and MACs

- Shortly after DES became a US federal standard, a number of parallel standards were published showing how to use DES for:
  - encrypting data to protect its confidentiality (*modes of operation*);
  - generating a *Message Authentication Code* (*MAC*), a type of checksum appended to data which guarantees its integrity and origin.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

International crypto standards

- DES was initial standardised only for US federal government use.
- However, DES soon became a US national standard (published by ANSI), and a de facto international standard for banking communications protection.
- Modes of operation and MAC standards were similarly published by ANSI and also internationally by ISO/IEC.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

ISO: from SC20 to SC27 – the modern era

- ISO/TC 97 (Information technology) established SC 20, dealing with cryptography, in the early 1980s.
- One of its earliest projects was to standardise DES, but this failed (see next slide).
- However, other work succeeded.
- When ISO/TC 97 was merged with its parallel IEC committee to become ISO/IEC JTC 1, SC 20 was reformed and expanded in scope to become SC 27, dealing with all aspects of Information security (including crypto).
- SC27 has five working groups (WGs), of which one – WG2 – looks after crypto standards.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Case study: DES and ISO

- As mentioned on the previous slide, efforts to standardise DES failed.
- In fact, the ISO DES standard was almost published, but was blocked for political reasons at the very last minute.
- Encryption (but not MACs and other crypto methods) was still a technology some governments wished to control.
- For this reason it was decided at the time that SC 27 was formed that its scope would exclude standardising encryption algorithms.
- This decision was changed in the early 2000s, and today a wide range of encryption algorithms are standardised.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

SC 27 crypto standards – range

- Today, SC 27/WG 2 has published and continues to maintain a wide range of crypto standards, including (focussing on symmetric crypto):
  - **encryption algorithms** (including block ciphers (ISO/IEC 18033-3) and stream ciphers (ISO/IEC 18033-4));
  - **modes of operation for block ciphers** (ISO/IEC 10116);
  - **MAC techniques** (ISO/IEC 9797 parts 1-3);
  - **hash functions** (IDSO/IEC 10118 parts 1-4);
  - **authenticated encryption** (ISO/IEC 19772);
  - **authentication** and **key management** protocols (ISO/IEC 9798 and ISO/IEC 11770);
  - **random bit generation** (ISO/IEC 18031);
  - **lightweight cryptography** (ISO/IEC 29192).

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

1. Crypto standards – a selective history
2. Challenges
3. Ways forward
4. Some random concluding remarks

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Maintenance and workload

- Perhaps the most serious challenge of all is merely to do with the fact that:
  - published standards need to be maintained, particularly in a fast-moving area like crypto;
  - there are now a lot of published standards;
  - there are a limited number of experts prepared to give their time …

ROYAL HOLLOWAY UNIVERSITY OF LONDON

When to standardise?

- In some cases SC 27/WG 2 has tried to standardise techniques when there are no suitable candidates.
- For example, SC 27/WG 2 started work on ISO/IEC 10118-3 (*dedicated hash-functions*) before NIST's SHA was published, when the only obvious candidates were MD4 and MD5.
- It was made clear by participating experts that these were not suitable for standardisation.
- Fortunately SHA/SHA-1 came along just at the right time.
- However, whilst there are dangers of standardising too early, there are also dangers of being too late.
- SC 27 is only now standardising key derivation techniques (ISO/IEC 11770-6) – as a result there are many slightly different techniques in use (including in SC 27 standards).

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Too many standards?

- As Andrew Tanenbaum famously said:

  The nice thing about standards is that there are so many of them to choose from.

- Crypto standards are produced by many bodies:
  - national (NIST, ANSI, DIN, BSI, …), and
  - international (ISO/IEC, IEEE, IETF, ITU-T, ETSI, …).
- Too often they overlap/conflict.
- Arguably even the ISO/IEC standards contain too many choices, e.g. ISO/IEC 18033-3 contains seven different block ciphers.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Visibility/adoption of standards

- One major practical problem with ISO/IEC standards is that they are not freely available.
- Indeed they are rather expensive to buy.
- As a result they are widely ignored.
- Too often IETF RFCs, many of which are not in any sense standards, are treated as the authoritative source for crypto technology.
- This is despite the fact that the process for adopting an ISO/IEC standard is far more rigorous than that used to decide whether an RFC should be promulgated.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Reputation of standards

- The recent Snowden revelations have damaged the reputation of the crypto standards bodies.
- It seems that algorithms of dubious security were included in national (NIST) and international (ISO/IEC) standards – see next slide.
- Whilst the offending techniques have been de-standardised, this potentially damages trust long-term.
- Indeed, two lightweight block ciphers were recently submitted by the US national body (ANSI) for possible standardisation by ISO/IEC.
- Despite having desirable efficiency properties, and having been subject to widespread scrutiny, they were rejected – mainly, I suspect, because of suspicion of the US.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Case study: Dual_EC_DRBG

- Dual_EC_DRBG is a random bit generation technique.
- Following NIST, it was included in ISO/IEC 18031, along with a set of 'recommended parameters'.
- Only because of Snowden did the world suddenly realise:
  - the technique had originally been designed to allow the scheme to be broken if the parameters are chosen carefully (but only by the chooser of the parameters);
  - the 'recommended parameters' were of unknown provenance.
- As soon is this became known, SC 27/WG 2 issued a press release, and shortly afterwards a corrigendum was published removing Dual_EC_DRBG from the standard.

http://www.theguardian.com/technology/2013/dec/23/security-company-rsa-denies-insta

Security company RSA deni... | BBC - Homepage

free become a member | sign in | subscribe | search | jobs | dating | more | UK edition

theguardian
Winner of the Pulitzer prize 2014

UK world politics sport football opinion culture business lifestyle fashion environment tech travel | all sections

ome › tech

Data protection

Security company RSA denies knowingly installing NSA 'back door'

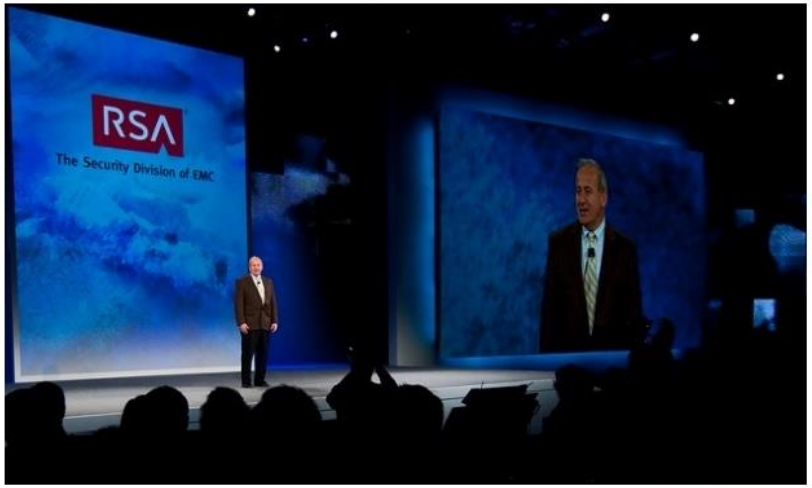
Denial follows allegations that pioneering company made NSA algorithm its default in return for payment

harles Arthur

@charlesarthur

onday 23 December
013 19.30 GMT

Shares 56 Comments 44



The chief executive of RSA, Art Coviello, speaking at a conference in 2010. Photograph: Kevin Bocek/Flickr

The security company RSA has denied that it knowingly weakened the encryption it used in its products as part of a secret contract with the US's National Security Agency.

A report from the Reuters news agency on Friday alleged that RSA arranged a $10m contract to use a mathematically weaker formula in a number of its products, which would in effect have created a "back door" for cracking encrypted

Most popular

Raheem Sterling: Manchester United launch bid to sign Liverpool wantaway

Cameron's immigration bill to include crackdown on illegal foreign workers

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Not invented here and standards

- There are many reasons why ISO/IEC standards are not always adopted.
- One is that they cost money (as discussed before).
- However, many parties seem possessed by an irrepressible desire to invent their own techniques.
- IETF is a prime example (the US influence is strong, and international standards are hence regarded as irrelevant).
- More surprisingly, ETSI, with apparently good relations with ISO, insists on designing its own algorithms in SAGE rather than joining forces with SC 27.
- Historically, the banking community have also tended to write their own standards.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Case study: MD5

- This diversification of algorithm standards can have very damaging consequences.
- As mentioned before, MD5 (a hash function) was not standardised by ISO/IEC for sound security reasons.
- However, it was published by the IETF in an RFC.
- This has led to its very widespread (and continuing) use, despite the fact it is insecure.
- Indeed there are known real-world attacks (notably the *Flame* malware) which have exploited its use.

Flame Exploited Long-Known Flaw in MD5 Certificate Algorithm

Posted 2012-06-13 Print

Flame attackers' ability to forge a valid certificate for Windows Update should be a warning to companies to stop using the MD5 algorithm to issue security certificates.

By: Robert Lemos

A known weakness in the MD5 hash function gave the group behind the Flame malware an opportunity to forge a valid certificate for Microsoft's Windows Update service.

Yet while security researchers have known about the weakness for more than a decade, nearly every company today continues to use the MD5 hash function to secure its systems, one security vendor reports.

Certificate-management firm Venafi scanned 450 companies in the Global 2000 and found that every single one had MD5 certificates associated with their networks. In total, 17.4 percent of the certificates used to sign servers, code and VPN access still used the MD5 algorithm, the company found.

The continued use of the broken cryptographic hash algorithm puts the companies at risk, as cyber-criminals are expected to quickly adopt attacks against the MD5, now that Flame has demonstrated the possibilities, says Jeff Hudson, CEO of Venafi.

"We are going to all our customers and saying, you have to get MD5 off the network," Hudson says. "It's critically important, because ... the backdoor is wide open."

Microsoft issued an emergency patch on June 3 to invalidate the fake certificate,

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Intellectual property issues

- Some standards bodies prohibit standardisation of patent-protected schemes.
- ISO/IEC, however, allows this, as long as fair and non-discriminatory terms are agreed by the IP owner.
- Enforcing this relies on the standards committee learning whether algorithms are protected.
- As a side issue, it is interesting to note that apparently minor crypto-related features of the 3G mobile standards which were patent-protected during the standards-writing process have meant that 'late' entrants to the mobile phone market (e.g. Apple) have had to make huge payments to the IP owners.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Commercial issues

- Many of the experts attending the standards committees are employees of companies with commercial interests in what is/is not standardised.
- As a result, the schemes that are standardised are sometimes influenced by commercial preferences.
- This is perfectly legitimate – if you attend, you get a say – but it may not always be desirable in a global sense …
- Academics can play an important role in challenging what look like poor decisions, as they are often unencumbered by commercial considerations.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Case study revisited: DES and ISO

- As mentioned earlier in this talk, efforts to make DES an international standard in the 1980s foundered under US government pressure.
- However, triple DES is now part of ISO/IEC 18033-3.
- It remains primarily for commercial reasons – it is significantly weaker than the key length would lead a user to expect.
- However, because it is in wide use, de-standardising it would cause major commercial problems.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Political issues

- Similarly, governments, who often fund standards committee attendees, may wish to promote technologies which favour individual nation states.
- One reason is that if technologies are standardised then it is acceptable to list them in requirements specifications under WTO rules.
- This can lead to nations trying to get national standards made international – this can, in turn, exacerbate the excess of standards problem.
- Let alone issues like Dual_EC_DRBG …

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Language issues

- Cryptographic algorithm standards are intended to describe:
  - how to implement algorithms;
  - in what circumstances they should be used;
  - how parameters/options should be chosen.
- They are not textbooks – in particular, they are not concerned with *why* particular aspects of a scheme are designed the way they are.
- After all, a software developer or protocol designer does not need to know such information – if they want it they can read a textbook or take a crypto course!
- Standards should be as simple and as easy to use as possible.
- This is an area academics writing standards often really struggle with, as they instinctively want to explain and thereby risk making standards unnecessarily long and complex.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Legacy issues

- Legacy is one of the bugbears of security.
- This holds for standards development. In some cases SC 27/WG 2 has had to retain undesirable options in standards because they are in use and, if used appropriately, they remain secure.
- Such options are flagged as deprecated for new applications.
- Of course, there are obvious hazards in leaving such options in standards.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Case study: MAC padding

- When computing a CBC-MAC (using a block cipher to compute a MAC), the last block of data needs to be 'padded'.
- Historically this was done using a string of all zeros.
- This is secure if the message length is known to the recipient by independent means – otherwise it is insecure.
- Thus this padding method should only be used with great care and its use is deprecated.
- However it is still in ISO/IEC 9797-1 because of the huge legacy of applications.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Poor implementation

- Although this is not necessarily the fault of the standards, there are many examples of implementations being found not to follow standards correctly.
- This is perhaps not so much a problem for algorithm standards, but is certainly an issue for random number generation (as needed for crypto keys).
- May also be a problem for some aspects of key management and authentication.
- This is perhaps a cultural issue amongst the developer community.
- Also we need to make standards as clear and precise as possible and not burdened with unnecessary detail.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Dealing with issues in standards

- If a security weakness is found in a standardised algorithm, protocol or procedure, this needs to be fixed (e.g. remove algorithm or amend advice on use).
- Historically, SC 27/WG 2 has been receptive to news of problems and reasonably quick to act.
- However, acting has typically meant simply amending the standard and not telling the world.
- This needs to change (and changes are afoot).

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Case study: Encoding data fields

- A few years ago, it became clear that almost all the authentication and key management protocol standards had a specification problem.
- Many of the protocol messages are specified as being made up of the concatenation of various fields, input to a crypto-primitive.
- However, 'concatenation' was not really specified.
- It could be interpreted to mean simply taking two bit strings and joining them together to make a longer bit string.
- In some cases such an implementation could give rise to security issues.
- It was therefore necessary to amend the standard to make it clear that concatenation implied an encoding method which was uniquely and unambiguously decodable. We created and published six corrigenda to fix this problem, all within 12 months.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Case study: Encrypt-then-MAC

- ISO/IEC 19772 is concerned with authenticated encryption.
- One of the six mechanisms in the standard is 'generic encrypt-then-MAC', i.e. allowing encryption then MAC computation using arbitrary algorithms.
- It was recently pointed out that the standard as specified is insecure, since it does not mandate the inclusion of the IV used for the encryption within the scope of the MAC.
- A (quite complex) corrigendum was written and published within 12 months.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

1. Crypto standards – a selective history
2. Challenges
3. Ways forward
4. Some random concluding remarks

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Involvement of academia

- The development of novel cryptographic techniques and their assessment and cryptanalysis is primarily down to academia (at least for non-government use).
- This means academic expertise is vital to the standardisation process in SC 27/WG 2 (and elsewhere).
- Involvement at the UK level costs nothing – I chair the UK committee providing input to standards development, and you can choose which work you want to provide input to – **just contact me if you're interested**!
- Participation in international meetings as a UK delegate is also possible, but travel costs are not usually covered.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Links to external bodies/CERTs

- On the relatively rare occasions we find defects in standards we need to be more active in promulgating these issues.
- Historically we have simply amended the standard concerned, and felt this was enough.
- However, this neglects the users who may have implemented the standard, and who are unaware of the changes.
- Only now is SC 27/WG 2 developing procedures to let the wider world know as and when issues (such as Dual_EC_DRBG) are identified.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Moving faster

- Sometimes standards development can take far too long.
- It is possible to go from start to finish with an ISO/IEC standard in 2-3 years (I've done it) – however it often takes more like 5!
- Greater involvement by experts is key to getting the job done in a timely way (and this includes those editing new standards).

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Benefits of involvement

- Many academics are wary of being involved in standardisation as the payback is not easily defined (specifically, no publications and no grant money).
- However, as someone with nearly 30 years of involvement in standardisation, there are many potential benefits, including:
  - writing a standard often makes you think about things you might not otherwise worry about, and this can lead to new research;
  - standards development can lead to fruitful interactions with industry experts, and hence to joint research projects and/or consultancy (money in your pocket!);
  - above all else, there is huge satisfaction in making academic work accessible and usable by the wider world – who knows, it may even lead to an impact statement for REF.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

1. Crypto standards – a selective history
2. Challenges
3. Ways forward
4. Some random concluding remarks

ROYAL HOLLOWAY UNIVERSITY OF LONDON

What is it about crypto …?

- Over the years I can recall many occasions where it seems that development engineers and protocol designers have assumed they know better than cryptographers.
- For example, they may design their own crypto algorithm or ignore vital parts of a security protocol because they don't understand them (and hence deem them unnecessary).
- What is it about crypto that makes the man in the street assume they know as much as an expert?
- After all, most of us don't do our own surgery, or ask someone we meet in the pub to represent us in court …
- I don't know the answer, but it is a hugely serious problem!

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Bridging the gap

- The main message of this talk (if you haven't noticed already) is an appeal to everyone to think about getting involved in crypto standards development.
- Standards represent a vitally important bridge between theory and practice.
- Standards are our chance to write in simple terms what *should* happen, and isn't that what we try to discover as academics?

ROYAL HOLLOWAY UNIVERSITY OF LONDON

The future

- Despite all the challenges I have described, SC 27 has a pretty good track record … *so far*!
- Very few standardised schemes have needed to be significantly modified or removed, despite a standards portfolio going back 30 years.
- However, for this to remain true requires that the crypto community, in academia and industry, participates in and contributes to the standards process.