Threats to Modern Cryptography and State-of-the-Art Solutions

Kenny Paterson

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Living with the Threat of the Crypt-Apocalypse

Kenny Paterson

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Crypto In Use

- Relative to the number of primitives that have been invented by academic cryptographers, the number that are *actually in use* today is tiny.
  - Symmetric encryption, MACs, key derivation.
  - DHKE, signatures, public key encryption (mostly RSA PKCS#1 v1.5).
  - Almost all for secure comms, and a bit of secure storage.

- Relatively small number of algorithms too.
  - RSA, a growing amount of ECC, lots of AES, SHA-1, surprising amount of RC4.

Take Up of New Crypto

- Adoption of new crypto is slow, for several reasons:
  - Lack of compelling applications that people/organisations actually want/need.
  - Performance (e.g. FHE poster-child).
  - Lack of support in crypto libraries.
  - Patents and related uncertainty.
  - Slow pace of standardisation.

- Almost all industrial crypto today is quite boring.
  - This does not mean to say it's easy to get right.

Lifetime of a Hash Algorithm – MD5

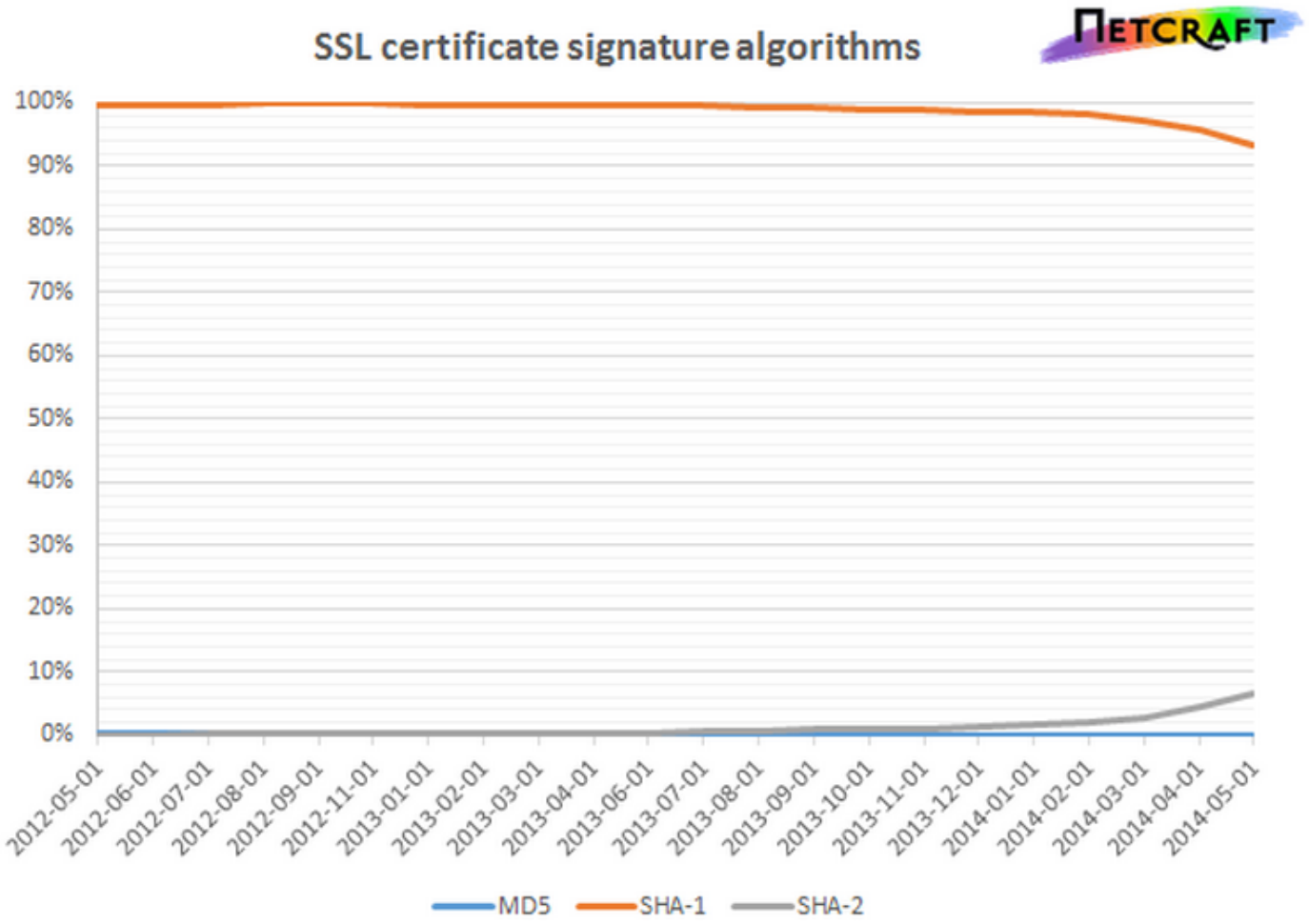
- 1992: MD5 published – "MD4 with seatbelts".
- 1993: First weaknesses in MD5 identified (den Boer and Bosselaers).
- 1996: Serious weaknesses discovered (Dobbertin).
- 2004: Collisions for full MD5 (Wang et al.)
- … Massive effort to remove MD5 from codebases …
- 2009: Rogue certificates (=rather meaningful collisions) (Stevens et al.)
- 2012: Flame malware discovered, exploiting MD5 collisions in Microsoft code-signing certs.

- The process of fully eliminating MD5 is still on-going, 10 years after first collisions were discovered.

Lifetime of a Hash Algorithm – SHA-1

- 1995: SHA-1 published (NIST, tweak of 1993 SHA-0 design)
- 1990s: (various attacks on SHA-0, validating switch to SHA-1)
- 2001: SHA-2 published by NIST.
- 2005: Collision attack for SHA-1, estimated at 2^{63} hash operations (Wang et al.).
- 2005 – now: various claims and counter-claims about improvements.
- 2006: NIST deprecates SHA-1 from 2010 by federal agencies for all new applications requiring collision-resistance.
- 2013: Microsoft annonces SHA-1 deprecation from 2016 for new code signing certs.
- 2014: Still no collisions, best estimate is 2^{61} hash operations (Stevens).
- 2014: SHA-1 is still used pretty much everywhere.

Netcraft Survey – Uptake of SHA-2 post Heartbleed



Moore's law for Quantum Computing?

http://en.wikipedia.org/wiki/Timeline_of_quantum_computing

1998: 2-qubit and 3-qubit NMR

2000: 5-qubit and 7-qubit NMR.

2001: The number 15 is factored!

2005: qbyte announced (8 qubits?)

2006: 12 qubits

2007: 28 qubits

2008: 128 qubits

} (D-Wave)

2011: 14 qubits

But maybe this is the wrong way to look at things? (aka shifting the goalposts)

Other Ways to Look at Things

- The threat of large-scale quantum computing is *weakly analogous* to the threat of a break-through in SHA-1 collision finding.
  - Breakthrough might be imminent, but then again it might not.
  - Hard to quantify risk that it will happen, and hard to put time-frame on it.
  - Meaningful results would have substantial impact.
  - Smart people are working on it and have had a lot of research investment.
  - (There are different physical approaches being pursued.)

- [On the other hand, maybe QC is a bit like fusion research?
- Random conversations I've been party to:
  - "Large scale QC is a decade away".
  - "Large scale QC is now just a matter of engineering".]

The Coming Crypt-Apocalypse?

- We don't know if there will be a QC scale breakthrough or not.
- If one comes, it would be fairly catastrophic – a Crypt-Apocalypse.
- We would expect some warning of impending disaster.
- But replacing crypto at scale takes decades.
- And traffic captured now could be broken later, so it's a problem now.
- Serious people are starting to think seriously about the possibility.

cataCRYPT

Ways Forward?

More usefully:

- Design new cryptosystems from scratch.
  - Lots of basic research needed.
  - 20 years to deployment.
- Improve existing cryptosystems.
  - Lattice-based, code-based, non-linear systems of equations,…
  - Lots of basic research needed.
  - Possibly vulnerable to further advances in quantum algorithms.
- Develop formal theory for provable security with quantum adversaries, understand what can and cannot be proved.
- Consider a world without *any* public key cryptography?
  - Maybe there will be progress in quantum *algorithms* too.

A World Without Public Key Cryptography?

- Known as Minicrypt in the complexity theory literature (Impaglazzio, 1995).
- Basic tools: symmetric encryption (block ciphers), hash functions.
- So what can be done with just these tools?

- We can still build signature schemes (using only one-way functions).
  - Lamport signatures (1979) + hash trees.
  - Substantial research effort has gone into optimising constructions.
  - Not as efficient as, e.g. EC-DSA or RSA signatures, but just about usable.

- But we don't know how to do secure public key encryption, and we don't know how to do secure DHKE.

A World Without Public Key Cryptography

- In fact, we frequently operate *at vast scale* and *without PKC*!

- Quiz question:

  There is a global system with more than 6 billion users that provides user authentication and enables secure communications, but which does not use any public key crypto. Name it.

- Answer:

(aka GSM/UMTS/3g/4g/LTE).

Characteristics of 3GPP Systems

- Use of hardware to store keys and perform sensitive crypto operations (SIM in phone, HSM or similar in operator's Authentication Centre).
- 800+ network operators, inter-operability (allowing roaming between home and visited networks).
- Standardisation (of algorithms for encryption and protocol for authentication).
- Key management is a significant cost.
  - Pre-shared key embedded in SIM during manufacture and copy given to operator.
  - Used for authentication and to derive encryption keys.
  - System is semi on-line, to get encryption keys to where they are needed.
- We can do this!

Further Characteristics of 3GPP Systems

- Particular trust relationships are put in place between subscribers and operators.
- Operators want to be able to bill subscribers accurately

  → authentication
- Subscribers would like a modicum of privacy

  → confidentiality

  (not always switched on, not end-to-end, legal intercept capability)

- It's a subscription-based and closed system.
- Would not work for e-commerce, which is a "roll-up and use" open system.

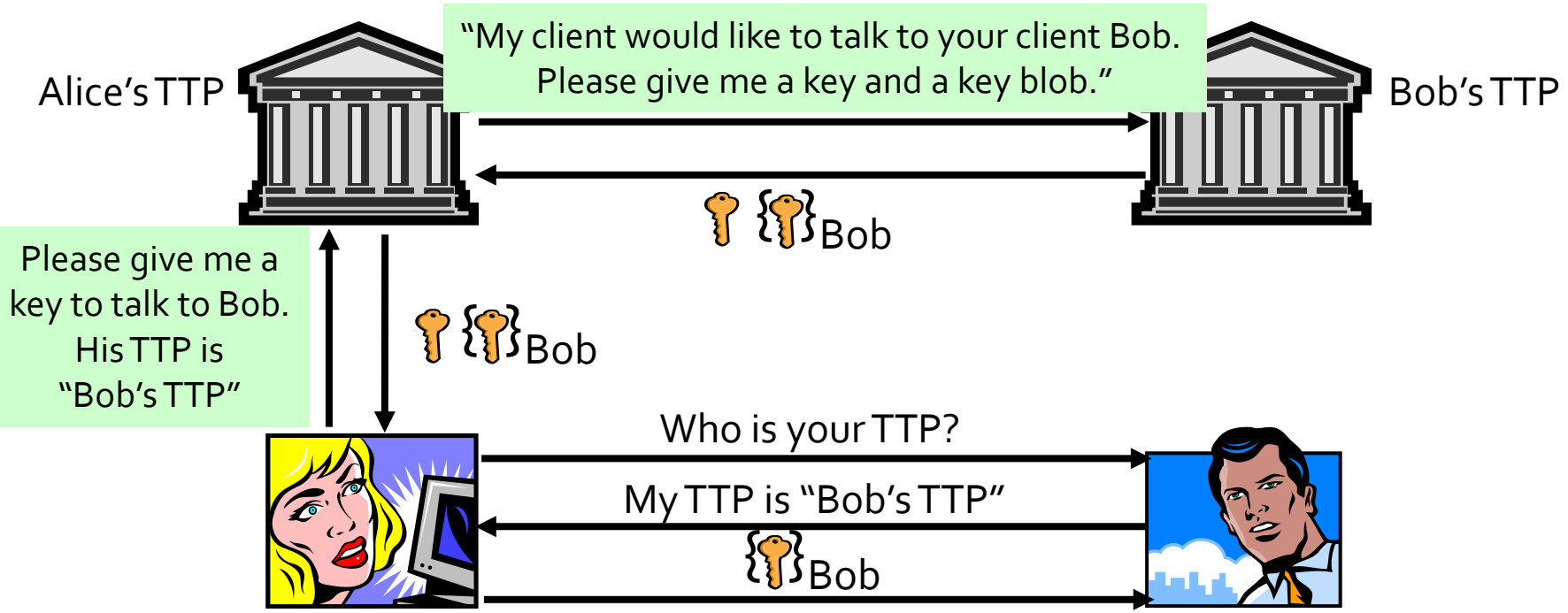
Open Systems without PKC?

- Challenge is to replace PKC in *open* systems.
- Prototypical application: e-commerce, protected by SSL/TLS.
- Characteristics and requirements:
  - No pre-arranged trust relationships or keys.
  - Customers (and credit card providers) want privacy against eavesdroppers.
  - Customers want to be able to verify identity of servers.

- Security Meta-Theorem:

Any cryptographic problem can be solved by the introduction of sufficiently many trusted third parties.

Applying the Meta-Theorem come the Crypt-Apocalypse



- Low-tech 4-party protocol to establish keys for authentication and secure communications.
- Can even integrate fairly smoothly with existing SSL/TLS PSK protocol flow.
- Deployment would messy, expensive, hard, disruptive, but eminently *possible* given enough motivation.

Applying the Meta-Theorem come the Crypt-Apocalypse

- Proposed "solution" has problems…
- Client (Alice) needs trust relationship with TTP (who pays?).
- Built-in key escrow facility.
  - Apply the Security Meta-Theorem again…
  - Users contract with multiple TTPs and use secret-sharing techniques.
  - Still weaker than truly escrow-free solutions based on PKC.
- Proposed solution is also more "on-line" than existing PKC-based system.
  - But reality is that existing system becomes on-line as soon as practical, scalable revocation mechanisms are considered.
  - OCSP!
- Solution has obvious privacy issues.
  - But then so has SSL/TLS!
  - Research question: can these be addressed using only symmetric techniques?

Concluding Remarks

- The Crypt-Apocalypse might be coming… or it might not.
- It deserves serious consideration either way.
- Post-quantum Public Key Crypto is one sensible response.
- Thinking about redesign of Trust and Key Management Infrastructures is another response.

- Questions/Comments?