Crypto developments

Daniel J. Bernstein

Research Professor,
University of Illinois at Chicago

Hoogleraar,
Cryptographic Implementations,
Technische Universiteit Eindhoven

A bit about me

Designer of:

- `qmail`, used by Yahoo
  to handle Internet mail;
- `tinydns`, used by Facebook
  to publish server addresses;
- `dnscache`, used by OpenDNS
  to look up server addresses;
- Curve25519 public-key system
  used by Apple to protect
  files stored on iPhones;
- ChaCha20 secret-key cipher
  used by Chrome to encrypt
  HTTPS connections to Google.

Standard crypto is failing

Goals: protect confidentiality, integrity, and availability.

Standard crypto is failing

Goals: protect confidentiality, integrity, and availability.

Standard crypto does a bad job of meeting these goals today, and an even worse job tomorrow.

Standard crypto is failing

Goals: protect confidentiality,
integrity, and availability.

Standard crypto does a bad job
of meeting these goals today,
and an even worse job tomorrow.

The standardization process
does not insist on security;
ignores important warnings
from cryptographers;
ignores predictable improvements
in computer technology; and
is unable to resist attack.

MD5

2008 Stevens–Sotirov–Appelbaum–Lenstra–Molnar–Osvik–de Weger exploited MD5 $\Rightarrow$ rogue CA for TLS.

MD5

2008 Stevens–Sotirov–Appelbaum–Lenstra–Molnar–Osvik–de Weger exploited MD5 $\Rightarrow$ rogue CA for TLS.

2012 Flame: new MD5 attack.

MD5

2008 Stevens–Sotirov–Appelbaum–Lenstra–Molnar–Osvik–de Weger exploited MD5 $\Rightarrow$ rogue CA for TLS.

2012 Flame: new MD5 attack.

Fact: By 1996, a few years after the introduction of MD5, Preneel and Dobbertin were calling for MD5 to be scrapped.

MD5

2008 Stevens–Sotirov–Appelbaum–Lenstra–Molnar–Osvik–de Weger exploited MD5 $\Rightarrow$ rogue CA for TLS.

2012 Flame: new MD5 attack.

Fact: By 1996, a few years after the introduction of MD5, Preneel and Dobbertin were calling for MD5 to be scrapped.

Internet crypto standardization continued using MD5.

Taiwan Citizen Digital Certificates

Renesas HD65145C1 "High-Security Microcontroller": tested by T-Systems, certified by BSI at CC assurance level EAL4+.

Taiwan Citizen Digital Certificates

Renesas HD65145C1 "High-Security Microcontroller": tested by T-Systems, certified by BSI at CC assurance level EAL4+.

Used in Chunghwa Telecom HICOS PKI Smart Card, tested by DOMUS IT Security Laboratory, FIPS 140-2 Level 2 certificate jointly from NIST and CSE.

Taiwan Citizen Digital Certificates

Renesas HD65145C1 "High-Security Microcontroller": tested by T-Systems, certified by BSI at CC assurance level EAL4+.

Used in Chunghwa Telecom HICOS PKI Smart Card, tested by DOMUS IT Security Laboratory, FIPS 140-2 Level 2 certificate jointly from NIST and CSE.

Deployed for two million people.

Taiwan Citizen Digital Certificates

Renesas HD65145C1 "High-Security Microcontroller": tested by T-Systems, certified by BSI at CC assurance level EAL4+.

Used in Chunghwa Telecom HICOS PKI Smart Card, tested by DOMUS IT Security Laboratory, FIPS 140-2 Level 2 certificate jointly from NIST and CSE.

Deployed for two million people. 2013 Bernstein–Chang–Cheng–Chou–Heninger–Lange–van Someren: 184 keys factored.

Dual EC

2004: ANSI draft "Dual EC" random-number generator.
(Didn't say: designed by NSA, secretly predictable to NSA.)

Dual EC

2004: ANSI draft "Dual EC" random-number generator. (Didn't say: designed by NSA, secretly predictable to NSA.)

2006 Gjøsteen: Dual EC is biased.
2006 Sidorenko–Schoenmakers: Dual EC is even more biased.

Dual EC

2004: ANSI draft "Dual EC" random-number generator. (Didn't say: designed by NSA, secretly predictable to NSA.)

2006 Gjøsteen: Dual EC is biased.
2006 Sidorenko–Schoenmakers: Dual EC is even more biased.

NIST *then* standardized Dual EC.

Dual EC

2004: ANSI draft "Dual EC" random-number generator. (Didn't say: designed by NSA, secretly predictable to NSA.)

2006 Gjøsteen: Dual EC is biased.
2006 Sidorenko–Schoenmakers: Dual EC is even more biased.

NIST *then* standardized Dual EC.

2007 Shumow–Ferguson: would have been easy to make Dual EC secretly predictable.

Dual EC

2004: ANSI draft "Dual EC" random-number generator. (Didn't say: designed by NSA, secretly predictable to NSA.)

2006 Gjøsteen: Dual EC is biased.
2006 Sidorenko–Schoenmakers: Dual EC is even more biased.

NIST *then* standardized Dual EC.

2007 Shumow–Ferguson: would have been easy to make Dual EC secretly predictable.

NIST kept standard until 2014.

Heartbleed

Crypto standardization process rewards unnecessary complexity.

Heartbleed

Crypto standardization process rewards unnecessary complexity.

Exception: small platforms.
But modern crypto platforms are complicated software devices.

Heartbleed

Crypto standardization process rewards unnecessary complexity.

Exception: small platforms.
But modern crypto platforms are complicated software devices.

Complex crypto is practically impossible to get right and audit.
Many security holes: Heartbleed, goto fail, new SChannel bug, etc.

Heartbleed

Crypto standardization process rewards unnecessary complexity.

Exception: small platforms.
But modern crypto platforms are complicated software devices.

Complex crypto is practically impossible to get right and audit.
Many security holes: Heartbleed, goto fail, new SChannel bug, etc.

Crypto is front line, performance-constrained.
Hard to isolate and monitor.

Quantum computers

Attacker equipped with
a large Shor computer breaks
RSA, DSA, ECDSA, ECDH, etc.

Quantum computers

Attacker equipped with
a large Shor computer breaks
RSA, DSA, ECDSA, ECDH, etc.

Retroactively decrypts intercepted ciphertexts, **whether or not they have "perfect forward secrecy".**

Quantum computers

Attacker equipped with
a large Shor computer breaks
RSA, DSA, ECDSA, ECDH, etc.

Retroactively decrypts intercepted ciphertexts, **whether or not they have "perfect forward secrecy".**

No evidence that attackers
have a Shor computer today.
(D-Wave computer seems to be
quantum but isn't Shor.)

Quantum computers

Attacker equipped with
a large Shor computer breaks
RSA, DSA, ECDSA, ECDH, etc.

Retroactively decrypts intercepted ciphertexts, **whether or not they have "perfect forward secrecy".**

No evidence that attackers
have a Shor computer today.
(D-Wave computer seems to be
quantum but isn't Shor.)
My probability assessment:
Medium probability by 2025.
High probability by 2030.