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.

developments

. Bernstein

n Professor,
ty of Illinois at Chicago

aar,
raphic Implementations,
che 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.

Standarc

Goals: p
integrity

nts

n

r,
is at Chicago

plementations,
siteit 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

Goals: protect cor
integrity, and avail

ago

ons,

hoven

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 confidentialit integrity, and availability.

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.

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

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 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.

out me

r of:

, used by Yahoo
ndle Internet mail;
ns, used by Facebook
blish server addresses;
che, used by OpenDNS
k up server addresses;
25519 public-key system
by Apple to protect
tored on iPhones;
ha20 secret-key cipher
by Chrome to encrypt
PS connections to Google.

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 Ste
Appelba
Osvik–de
MD5 ⇒

Yahoo
et mail;
by Facebook
r addresses;
by OpenDNS
r addresses;
lic-key system
o protect
Phones;
t-key cipher
to encrypt
tions to Google.

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–Soti
Appelbaum–Lenstr
Osvik–de Weger e
MD5 ⇒ rogue CA

ok
s;
DNS
s;
stem

er
t
oogle.

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 ⇒ rogue CA for TLS.

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 ⇒ rogue CA for TLS.

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.

2012 Flame: new MD5 attack.

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.

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.

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.

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.

d crypto is failing

protect confidentiality,
, and availability.

d crypto does a bad job
ng these goals today,
even worse job tomorrow.

ndardization process
t insist on security;
mportant warnings
yptographers;
predictable improvements
uter technology; and
e to resist attack.

MD5

2008 Stevens–Sotirov–Appelbaum–Lenstra–Molnar–Osvik–de Weger exploited MD5 ⇒ 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

Renesas
Security
by T-Sys
CC assu

s failing

nfidentiality,
lability.

oes a bad job
goals today,
e job tomorrow.

on process
security;
warnings
ers;
e improvements
ology; and
attack.

MD5

2008 Stevens–Sotirov–Appelbaum–Lenstra–Molnar–Osvik–de Weger exploited MD5 ⇒ 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 Dig

Renesas HD65145
Security Microcon
by T-Systems, cer
CC assurance leve

y,

job
y,
rrow.

ments
d

MD5

2008 Stevens–Sotirov–Appelbaum–Lenstra–Molnar–Osvik–de Weger exploited MD5 ⇒ 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 Certi

Renesas HD65145C1 “High-
Security Microcontroller”: t
by T-Systems, certified by B
CC assurance level EAL4+.

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+.

MD5

2008 Stevens–Sotirov–Appelbaum–Lenstra–Molnar–Osvik–de Weger exploited MD5 ⇒ 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+.

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.

MD5

2008 Stevens–Sotirov–Appelbaum–Lenstra–Molnar–Osvik–de Weger exploited MD5 ⇒ 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+.

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.

MD5

2008 Stevens–Sotirov–Appelbaum–Lenstra–Molnar–Osvik–de Weger exploited MD5 ⇒ 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+.

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.

evens–Sotirov–
um–Lenstra–Molnar–
e Weger exploited
rogue CA for TLS.

ame: new MD5 attack.

y 1996, a few years
e introduction of MD5,
and Dobbertin were
or MD5 to be scrapped.

crypto standardization
ed using MD5.

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: A
random–
(Didn't s
secretly

rov–
ra–Molnar–
xploited
for TLS.

MD5 attack.

few years
tion of MD5,
ertin were
be scrapped.

andardization
D5.

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
random-number g
(Didn't say: desig
secretly predictabl

–

ck.

D5,

ped.

ion

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 NS
secretly predictable to NSA.

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.)

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.)

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

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.)

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

NIST *then* standardized Dual EC.

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.)

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.

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.)

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.

Citizen Digital Certificates

HD65145C1 “High-
Microcontroller”: tested
stems, certified by BSI at
rance level EAL4+.

Chunghwa Telecom
PKI Smart Card, tested by
IT Security Laboratory,
0-2 Level 2 certificate
rom NIST and CSE.

d for two million people.
rnstein–Chang–Cheng–
eninger–Lange–van
n: 184 keys factored.

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.

Heartble

Crypto s
rewards

gital Certificates

C1 "High-
troller": tested
tified by BSI at
I EAL4+.

a Telecom
: Card, tested by
ity Laboratory,
2 certificate
and CSE.

million people.
hang–Cheng–
ange–van
s factored.

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 standardiza
rewards unnecessa

ficates

-

ested
3SI at

ted by
tory,
te

ple.
ng–

.

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 proc
rewards unnecessary comple

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.

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.

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

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.

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.

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.

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.

C

NSI draft “Dual EC”
number generator.
say: designed by NSA,
predictable to NSA.)

østeen: Dual EC is biased.
dorenko–Schoenmakers:
C is even more biased.

en standardized Dual EC.

umow–Ferguson:
ave been easy to make
C secretly predictable.

pt standard until 2014.

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.

Quantur

Attacker
a large S
RSA, DS

“Dual EC”
enerator.
ned by NSA,
e to NSA.)

ual EC is biased.
choenmakers:
nore biased.

rdized Dual EC.

rguson:
easy to make
predictable.

rd until 2014.

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 compute

Attacker equipped
a large Shor comp
RSA, DSA, ECDS

”

SA,

)

biased.

ers:

d.

al EC.

ke

e.

14.

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 break
RSA, DSA, ECDSA, ECDH,

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.

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.

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

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.

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.)

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.

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.