The Cryptographic Year in Review

Prof. Bart Preneel
COSIC
KU Leuven, Belgium
Bart.Preneel(at)esat.kuleuven.be

24 October 2012

The Cryptographic Year in Review

http://www.ecrypt.eu.org

2012

Outline

- crypto algorithms
  - symmetric encryption
  - hash functions
  - public key crypto
  - padding attacks
- PKI
- hacks

CRYPTOGRAPHY ≠ SECURITY

crypto is only a tiny piece of the security puzzle
  - but an important one
most systems break elsewhere
  - incorrect requirements or specifications
  - implementation errors
  - application level
  - social engineering (layer 8)

AES update

- Rijndael algorithm designed in Belgium
- minor theoretical weaknesses in 2010/2011
- 2012: no news is good news
- 2255 implementations validated by NIST

- fast implementation: cycle per byte
  - bitsliced 7.60
  - 2010 Intel Westmere 1.27
  - 2011 Intel Sandy Bridge 0.64
  - 2011 AMD Bulldozer 1.30
  - 2012 Intel Ivy Bridge 0.64

GSM/DECT

- easy to break
  - tools are available to get traffic and key

Satellite telephones

- GMR-1 and GMR-2 broken
- used by Thuraya and military

intercepting phone conversations is illegal

Hash functions

protect short hash value rather than long text

collision resistance
preimage resistance
2nd preimage resistance
2004 Hash function crisis: the complexity of collision attacks

- MD4
- MD5
- SHA-0
- SHA-1
- Brute force

Brute force: 4 million PCs or US$ 100K hardware (1 year)

SHA-3: 224, 256, 384, and 512-bit message digests (similar to SHA-2)

NIST AHS competition (SHA-3)
- Call: 02/11/07
- Deadline (64): 31/10/08
- Round 1 (51): 09/12/08
- Round 2 (14): 24/7/09
- Final (5): 10/12/10
- Selection: 02/10/12

Alternatives to SHA-1
- RIPEMD-160 [BSI/KU Leuven 96]
  - still unbroken but output length too short for long term security
- SHA-2 [NIST/NSA 02]
  - seems to withstand attacks
  - some reservations
The Cryptographic Year in Review
Bart Preneel

Finalists

Software performance - eBash [Bernstein-Lange11]

Hardware: post-place & route results for ASIC 130nm [Guo-Huang-Nazhandali-Schaumont'10]

Keccak

Performance of hash functions - Bernstein (cycles/byte) Intel Core 2 Quad Q9550; 4 x 2833MHz (2008)

Public key crypto

"new" factorization record in January 2010: 768 bits

- should have been done in 2010
- still lots of 512-bit keys around

increased "acceptance" of ECC
- example NSA Suite B in USA
- Certicom challenge: ECC2K-130: 1 year with 60 KEuro (a large effort is underway)
- limited commercial deployment outside government
Key lengths for confidentiality
http://www.ecrypt.eu.org

<table>
<thead>
<tr>
<th>duration</th>
<th>symmetric</th>
<th>RSA</th>
<th>ECC</th>
</tr>
</thead>
<tbody>
<tr>
<td>days/hours</td>
<td>50</td>
<td>512</td>
<td>100</td>
</tr>
<tr>
<td>3-4 years</td>
<td>73</td>
<td>1024</td>
<td>146</td>
</tr>
<tr>
<td>10-20 years</td>
<td>103</td>
<td>2048</td>
<td>206</td>
</tr>
<tr>
<td>30-50 years</td>
<td>141</td>
<td>4096</td>
<td>282</td>
</tr>
</tbody>
</table>

Assumptions: no quantum computers; no breakthroughs; limited budget

Quantum computers?
exponential parallelism \( n \) coupled quantum bits
\( 2^n \) degrees of freedom!

Shor 1994: perfect for factoring
but: can a quantum computer be built?

If a large quantum computer can be built...
all schemes based on factoring (such as RSA) will be insecure
same for discrete log (\( \mathbb{Z}_p, \text{ECC} \))
symmetric key sizes: \( x^2 \)
hash sizes: unchanged!

alternatives: postquantum crypto
– McEliece, NTRU,…
– so far it seems very hard to match performance of current systems while keeping the security level against conventional attacks

Problematic public keys (1/3)

\[ \text{11.7 million openly accessible public keys (TLS/PGP)} \]
\[ \text{6.4 million distinct RSA moduli rest: ElGamal/DSA (50/50) and 1 ECDSA} \]

- 1.1% of RSA keys occur in >1 certificate
- easy to factor: 0.2% of RSA keys
  - 12,000 keys!
  - 40% have valid certs
- 5.6% of TLS hosts share public keys
- 5.2% default manufacturer keys
  - 0.34% have by accident the same key
- 12 million openly accessible public keys (5.8 TLS/6.2 SSH)
  - 23 million hosts (12.6/10.2)
  - 1%: 512-bit RSA keys

Problematic public keys (2/3)

- low entropy during key generation
- RSA keys easy to factor, because they form pairs like: \( n = p \cdot q \) and \( n' = p' \cdot q' \) so \( \gcd(n,n')=q \)
- DSA keys: reuse of randomness during signing or weak key generation
  - why ???
  - embedded systems
  - routers, server management cards, network security devices
  - key generation at first boot

RSA versus DSA
Ron was wrong, Whit is right or vice versa?
Problematic public keys (3/3)

ethical problem: how to report this?

details:

Reaction attack (aka padding attack)

let's modify the ciphertext

Reaction attack (attempt 1)
sorry, you message is malformed

Reaction attack (attempt 2)
modify ciphertext in a different way

Reaction attack (attempt 3)
fast forward
Reaction attack (attempt 1001)

Meet me tonight at 20:00 at the Grande Place

Great! Now I know the plaintext

Eve

ok

Alice

ok

Bob

“Efficient padding oracle attacks on cryptographic hardware” (PKCS#11 devices)

[Bardou 12] most attacks take less than 100 milliseconds

<table>
<thead>
<tr>
<th>Device</th>
<th>PKCS#1v1.5 token</th>
<th>PKCS#1v1.5 session</th>
<th>CBC pad token</th>
<th>CBC pad session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aladdin eTokenPro</td>
<td>OK</td>
<td>OK</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Feitian ePass 2000</td>
<td>OK</td>
<td>OK</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Feitian ePass 3003</td>
<td>OK</td>
<td>OK</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Gemalto Cyberflex</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>RSA Securid 800</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Safenet iKey 2032</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>SATA dKey</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Siemens CardOS</td>
<td>(93 sec)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

2008 Rogue CA attack

[Sotirov-Stevens-Appelbaum-Lenstra-Molnar-Osvik-de Weger ‘08]

request user cert: by special collision this results in a fake CA cert (need to predict serial number + validity period)

impact: rogue CA that can issue certs that are trusted by all browsers

6 CAs have issued certificates signed with MD5 in 2008:
- Rapid SSL
- Free SSL (free trial certificates offered by RapidSSL)
- TC TrustCenter AG
- RSA Data Security
- Verisign.co.jp

Outline

- crypto algorithms
  - symmetric encryption
  - hash functions
  - public key crypto
  - padding attacks
- PKI
- hacks

Analogies

the biology analogy
the car analogy

cars have brakes so they can go fast

hidden assumption: you never drive downhill

Solution:
- don’t send error messages (bad engineering practice)
- KEM/DEM schemes and symmetric authenticated encryption

Reaction attacks: well known

[Bleichenbacher 98] PKCS #1v1.5 – 1 million chosen ciphertexts (in practice 200,000)
[Klima-Pokorny-Rosa 03] 40% improvement
[Bardou–Focardi–Kawamoto-Simionato-Steel-Tsay 12] – reduced to about 10,000 chosen ciphertexts
[Manger 01] OAEP PKCS #1v2 – a few 1000 chosen ciphertexts
[Bellare-Kohno-Namprempre 02] SSH
[Vaudenay 02] SSL, IPsec, WTLS...
[Canvel-Hiltgen-Vaudenay-Vuagnoux 03]: SSL/TLS

Solution:
- PKCS #1v2
- OAEP
Flame (successor of Stuxnet/Duqu)
- discovered in May 2012 by Cert in Iran
- targeted cyber espionage in Middle Eastern countries
- vectors: LAN, USB, Bluetooth
- record audio, screenshots, keyboard activity and network traffic (including Skype)
- kill command to wipe out its traces (used on June 8 2012)
- advanced MD5 collision attack built-in to create fake certificate for Microsoft Enforced Licensing Intermediate PCA (Windows Update)
  - similar to but independent from rogue CA attack

Malicious certificates
- Aug’11 Diginotar: target Iranian opposition
- May ’12 Flame
  - June ’12: Microsoft no longer supports RSA keys shorter than 1024 bits (except if signed before 1/1/2010)
  - NIST’s deadline is 31/12/2013
- Sept. ’12: Adobe problem

Hacks
- Privacy
  - Aug ‘12: US Federal Trade Commission orders web giant to pay $22.5m for violating privacy of rival Apple’s Safari browser users
  - Politicians and laws talks about cookies, but web companies have found many other cool ways to keep tracking users
- Java
  - Aug’12: Super-critical 0-day exploits 2 bugs
- Browsers
  - Sept ’12: new 0-day on Internet Explorer

Does Big Data Means Big Hacks?
psychology: humans are very bad at managing and evaluating risks in complex systems
economics: information security risks are typically systemic with large market failures in part due to negative externalities (e.g. software, e-commerce)
  - not so different from other areas: the larger the scale, the larger the risk (too big to fail)

Secure Computation
- PKI
- banking
- credit card
- Google
- eBay
- ...
- multi-party computation
  - "you can trust it because you don’t have to"

Summary
- AES is not broken but SHA-1 will be soon
- SHA-3 has been selected
- key generation remains problematic
- need to develop post quantum crypto
- multiparty computation becomes practical
- upgrading and fixing remains problematic
- old attacks keep coming back and new attacks get better

2012 was an exciting year for cryptanalysts
The end

Thank you for your attention

8 nov ‘12 ICC Ghent

29-30 nov ‘12
www.foryoureyesonly.be

4-8 March’13 www.secappdev.org

4-7 June’13 COSIC course
www.cosic.be