(in)secure.iacr.org

Brandon Enright, Eric Rescorla, Stefan Savage,
Hovav Shacham, Scott Yilek

-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----

secure.iacr.org

secure.iacr.org

Issued by: UTN-USERFirst-Hardware

Expires: Thursday, January 7, 2010 3:59:59 PM US/Pacific

This certificate is valid

▼ Details

Subject Name	
Country	US
Other Name	95120
State/Province	CA
Locality	San Jose
Other Name	6721 Tannahill Dr
Other Name	IACR, C/O Kevin McCurley
Organization	International Association for Cryptologic Research
Organizational Unit	s1.iacr.org
Organizational Unit	Comodo InstantSSL
Common Name	secure.iacr.org
Issuer Name	
Country	US

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

=

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

×

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

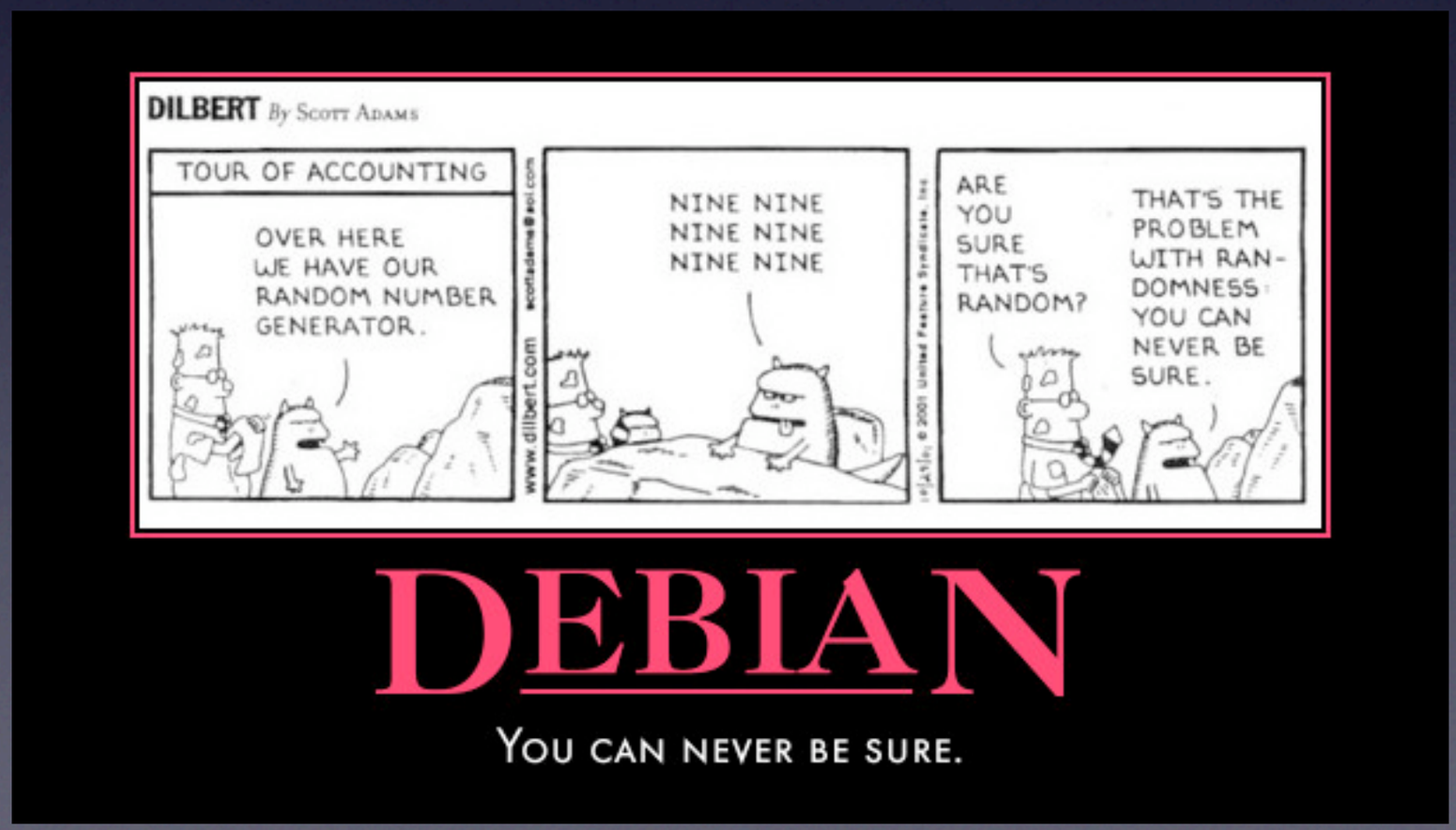
History

- Issued: 8 Jan 2008
- Replaced: 30 May 2008
- Revoked: 19 Jun 2008

- Valid until: 7 Jan 2010
- Do browsers check CRLs?

Huh?

- Generated using OpenSSL on Debian or Debian-derived Linux distribution
- 32-bit x86; process ID: xxxxx



The Debian OpenSSL bug

- Debian maintainer runs OpenSSL under Valgrind; notices uninitialized memory use:

```
MD_Update(&m,buf,j); /* purify complains */
```

- Solution: #ifdefs it out, plus more lines
- Side effect: no entropy from /dev/random.

Key generation

- Affected apps: ssh-kegen, openssl genrsa, …
- Sole entropy source: process id
  - 32k possible keys
  - (per key size, processor architecture)
- Easy to detect: build blacklist of bad keys
- For keys on blacklist, private key is known

Bug effects on SSL

- Weak server keys in certificates
  - Impersonate server
    - Decrypt recorded RSA sessions
- Weak server randomness
  - Decrypt recorded RSA_DHE sessions *
  - Timing attacks — predictable blinding

* given all server traffic

SSL cert survey

- We have been surveying SSL certs daily
  - Popular sites
    - 59k IPs, 56 days of UCSD :443 traffic
- Supplementary scans:
  - ~20k random hosts
  - ~200k Wikipedia-linked hosts

Statistics (May 17*)

	Unique certs	# bad	% bad
Overall	43,491	279	0.64%
Big CA	40,077	225	0.56%
Self-signed	619	27	4.36%

* 421 certs replaced 13–17 May

The CAs

- Key collisions:
  - We found (inter-CA) collisions
  - We believe major CAs saw colliding keys
- Alerting, revocation: as of July 15,
  - 76% of bad big-CA certs still in use
  - 66% of bad self-signed certs …

Thanks!

http://www.cs.ucsd.edu/~hovav/