Debian, OpenSSL, and SSL certificates

Brandon Enright, Eric Rescorla,
Stefan Savage, Hovav Shacham
(UC San Diego; RTFM, Inc.)

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.
- 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

SSL cert survey

- We have been surveying SSL certs daily
  - Popular sites
  - 59k IPs, 56 days of UCSD :443 traffic
  - Supplementary ~200k random hosts
  - Why SSL?
    - more polite than SSH
    - SSL keys go to CAs — more visibility

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%

Underestimating …

- Disclosure: May 13
- Our first survey: May 17
- 421 certs reissued during period:
  - Some due to normal expiration
  - But some were revoked/reissued
- We're working on analyzing these

Key collisions

- Key collision:
  - Two users end up with same key
    - Many instances expected — birthday bound
- We found key collisions.
- We found a VeriSign–Thawte key collision
- Did major CAs register same key twice?

Alerting and revocation

- CAs could check all issued certificates, alert users, revoke weak keys
- We do not see evidence of this!
- As of July 15:
  - 76% of bad big-CA certs still in use
  - 66% of bad self-signed certs …

Questions?

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