Report of the Security Working Group

FreeBSD DevSummit

EuroBSDCon 2013

Agenda

/dev/random	Mark Murray (in absentia)
Package signing	Baptiste Daroussin
Mitigation	Sofian Brabez
VuXML / portaudit	Dag-Erling Smørgrav

/dev/random

- Fixed some known entropy harvesting bugs
- Pluggable random generator framework
  - Yarrow, RDRAND, Padlock, block, panic, various dummies; Fortuna in 11
  - Backtracking: RDRAND and Padlock will be disconnected and fed into Yarrow / Fortuna
- Collect more entropy early in the boot process
  - Pawel's device attach timing patch; statistical tests show we get at least 4 bits per device, even on VMs
  - Have the installer dump entropy
  - Early harvesting ensures clone divergence

Package signing

- Short-term solution for 10:
  - Package builders submit hashes to signing service
  - Fingerprints ship with base, one file per key (/etc/pkg/fingerprints/{trusted,revoked})
  - Key distribution and revocation handled by freebsd-update
- Status:
  - pkg is ready
  - Signing server is missing
  - Need to generate and commit keys

Mitigation

- Included in 10, but off by default:
  - stackgap randomization adds a random amount of empty space at the top of the stack
  - mmap randomization inserts a random gap between consecutive mappings
- Stack protection can now be enabled by default (but hasn't yet) after libc changes
- ldbase randomization discussed, but not implemented

VuXML / portaudit

- VuXML shortcomings:
  - Auditing based on string matching, which is unreliable
  - Many errors in VuXML (very common: > instead of >=)
  - Auditing tools do not verify base system version
  - The kernel patch level does not necessarily reflect the userland patch level
- Start including CPE information in ports, stored as annotations in pkgng packages
  - Common Platform Enumeration: NIST standard for uniquely identifying software packages
  - Specification includes matching algorithm, reference implementation available
  - NIST publish CPE matching rules for every CVE
- Install a script in /libexec that prints the userland patch level