

lec 25

Victory Lap

One more Security Story

XZ Utils (2024) compression software

- attacker spent 3 years gaining trust
 - created situation where open source maintainer was overworked, then "volunteered"
- release tarball != git sources
- several distros patch SSHD to link system → XZ
- when activated, overrides SSHD decrypt function to give backdoor access

Security takeaways

- any system with bugs is likely vulnerable
 - and all systems have bugs
- any system with humans is likely vulnerable
- any system with complex security policies is vulnerable
 - so are systems with simple policies
- difficult to detect a breach (WD purchase order)
- difficult to recover from a breach
- trust is everything

OS Recap

- Kernel/user mode distinction
 - untrusted user code can invoke kernel
- Virtual CPUs (processes, threads)
 - synchronization mechanisms
 - scheduler policy
- Virtual memory
 - address translation, page tables
 - demand paging, copy on write; eviction policy
- virtual storage (file systems)
 - underlying device characteristics
 - FS data structures; transactions
 - disk scheduling

OS Future

- how can we make OSes more reliable?
- UW study has shown ~ 50% of severe Linux bugs could be prevented by better lang.
- Rust Ownership
 - memory safety
 - thread safety