



Computing Security for RT and Embedded Systems

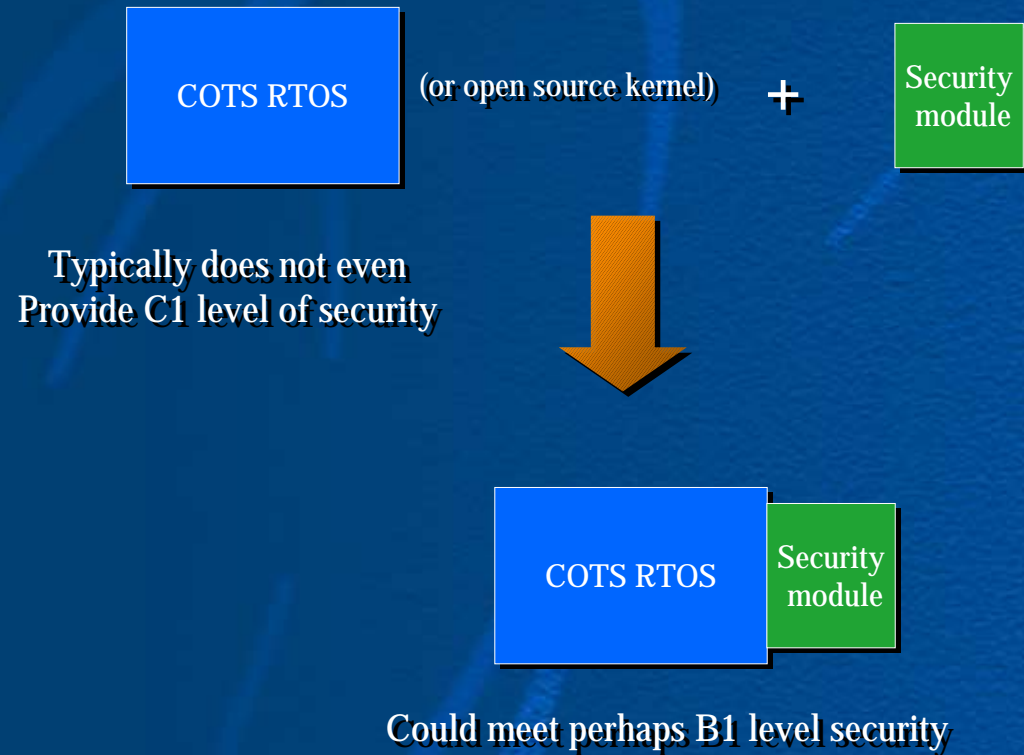
Kernel module approach

Mitch Bunnell, CTO LynuxWorks

Embedded System Security

- Protect data
- Prevent crashing
- Prevent takeover
- Fend off denial of service attacks

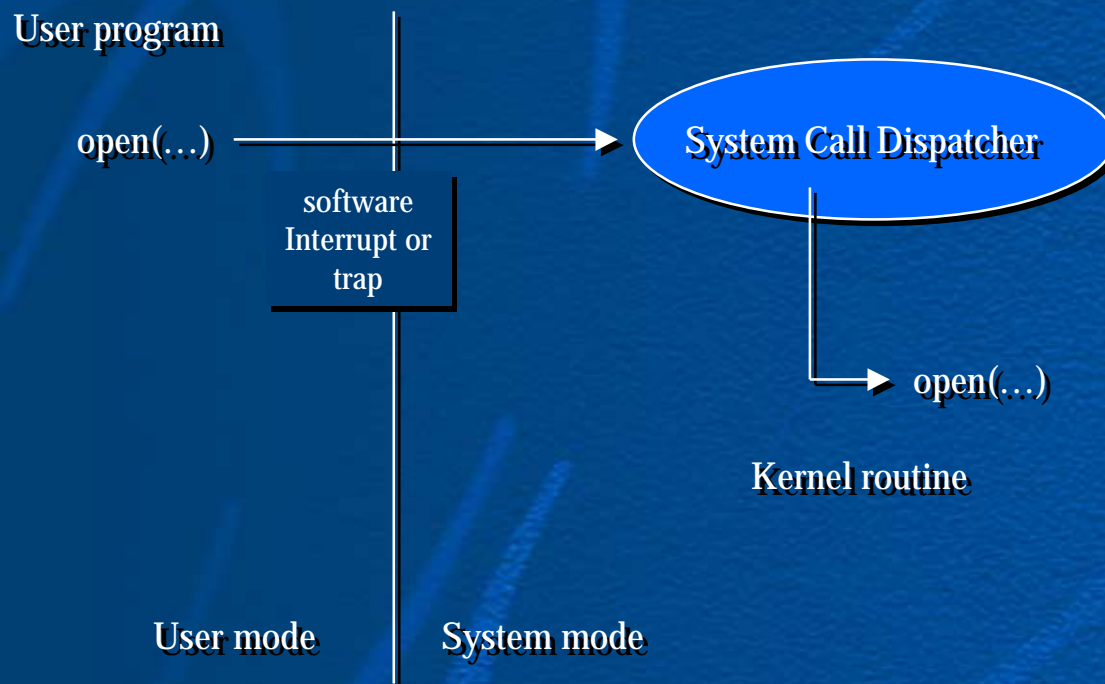
Security as a Module



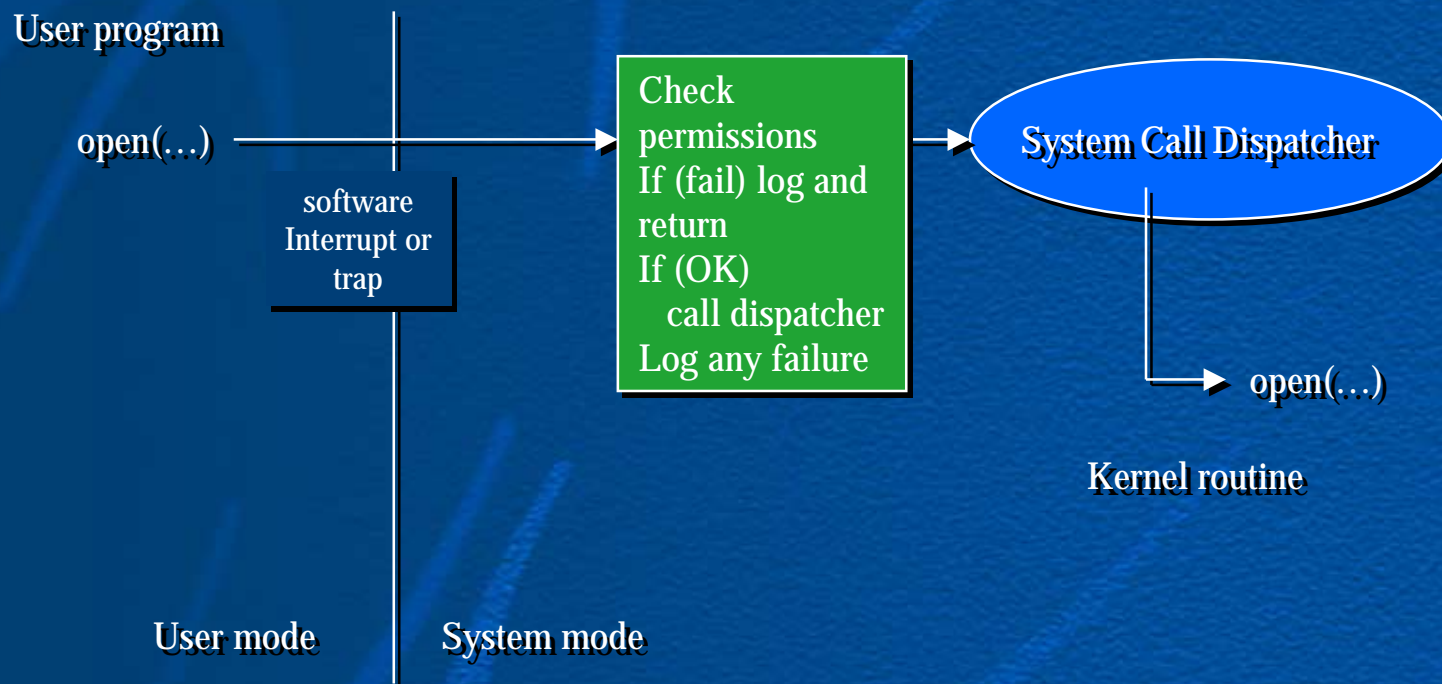
Security for Embedded Systems

- Must be a separate module
- Must be extensible
- Must be configurable (can be tailored) by user applications
- Requires an RTOS (or open source kernel) that provides memory protection

Mechanism: Interception of all System Calls



Mechanism: Interception of all System Calls

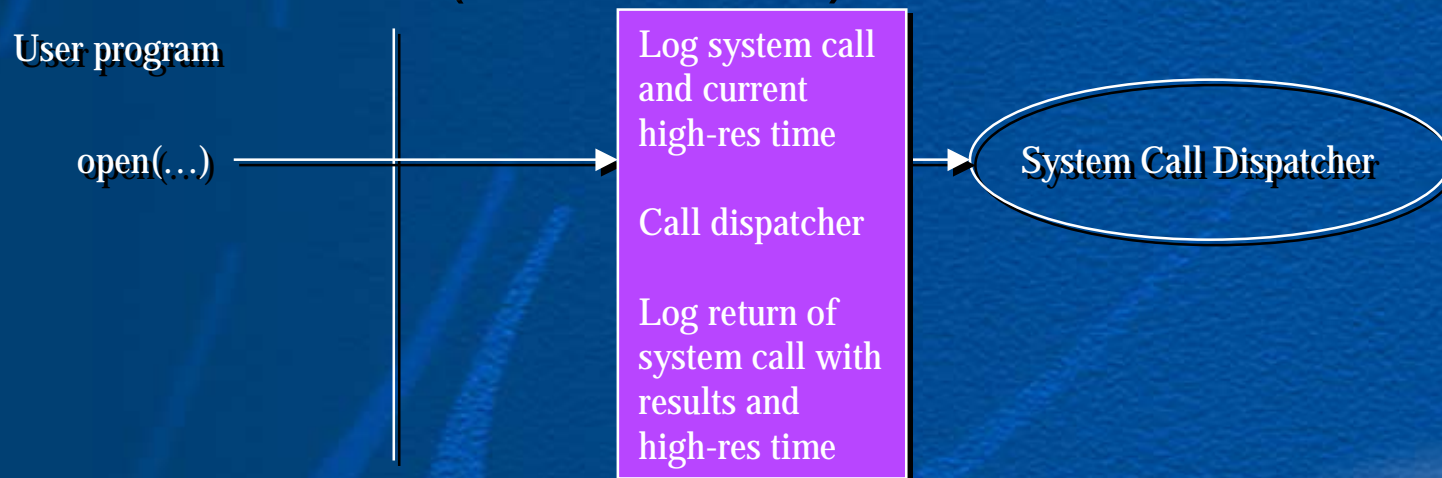


Proposed APIs

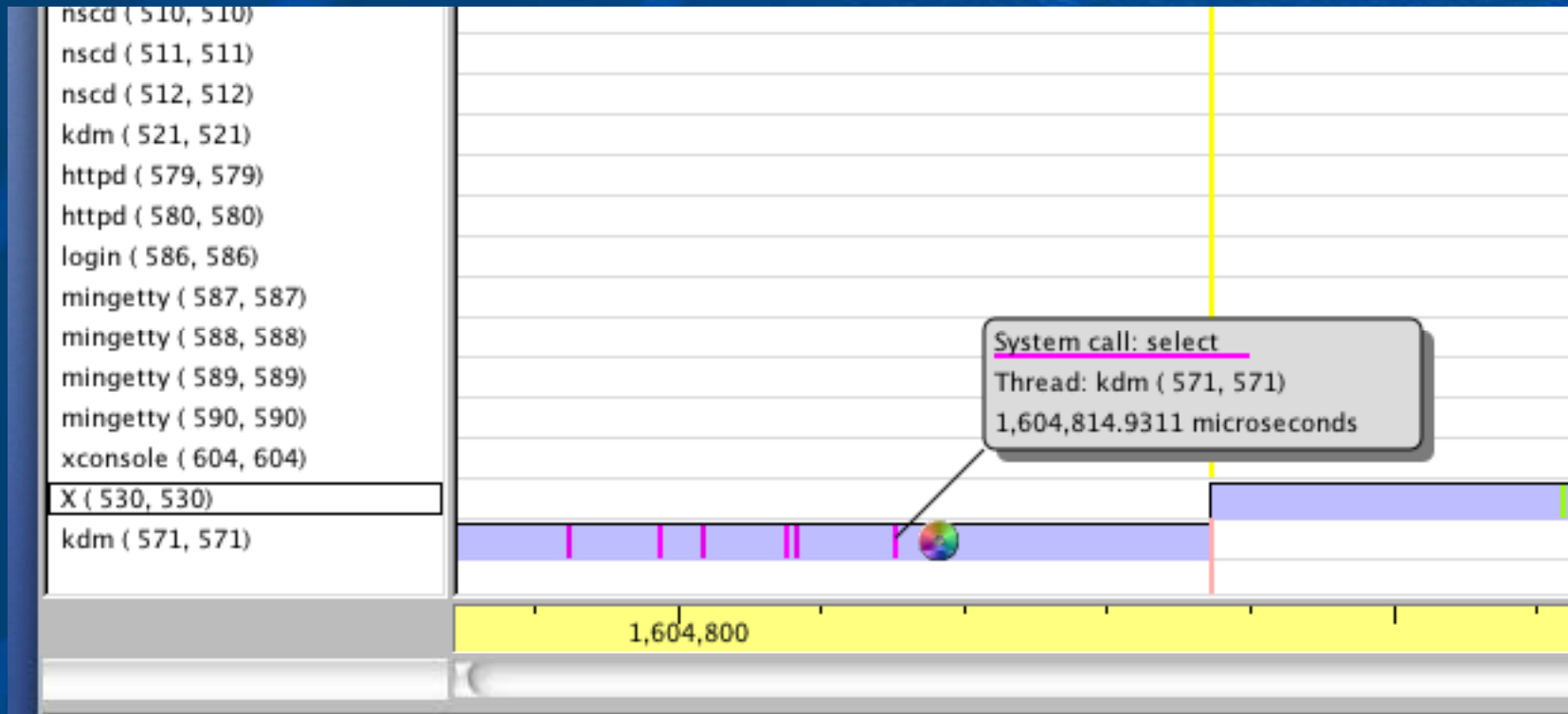
- Kernel API
 - Call to get list of all system calls and their prototypes (same for traps)
 - Call to intercept system call and trap dispatch
- Security Module API
 - Calls to tailor the security module
 - Mechanism for extending the security module

Proof of Concept

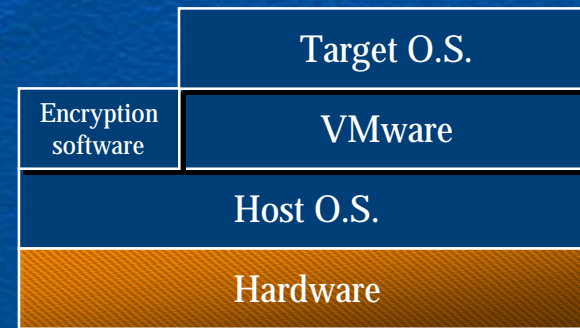
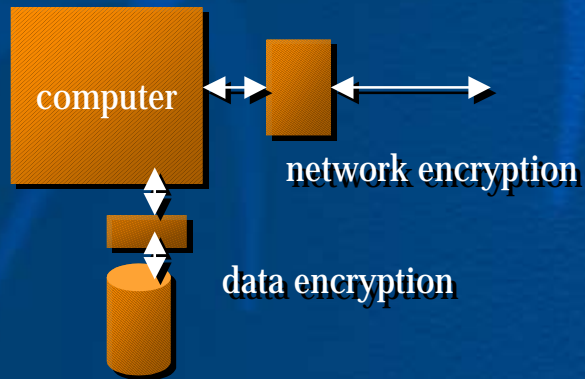
Created a kernel trace module of LynxOS and Linux that Intercepts all traps into the kernel (and more)



Proof of Concept



Storage and Network Security: the NetTop approach



NetTop emulates this

with this

Storage and Network Security: a lighter approach

