Operating System Security Research

David Lie
Department of Electrical and Computer Engineering
University of Toronto

Why do we need computer security?

- We depend on computers for a lot of things:
  - Banking/Finance
  - Communication (e-mail, IM, VOIP)
  - Electronic Voting
  - Health Records
  - Filing your taxes
  - …

- Computers were never designed with security in mind:
  - So what can we do? Start over again from scratch?

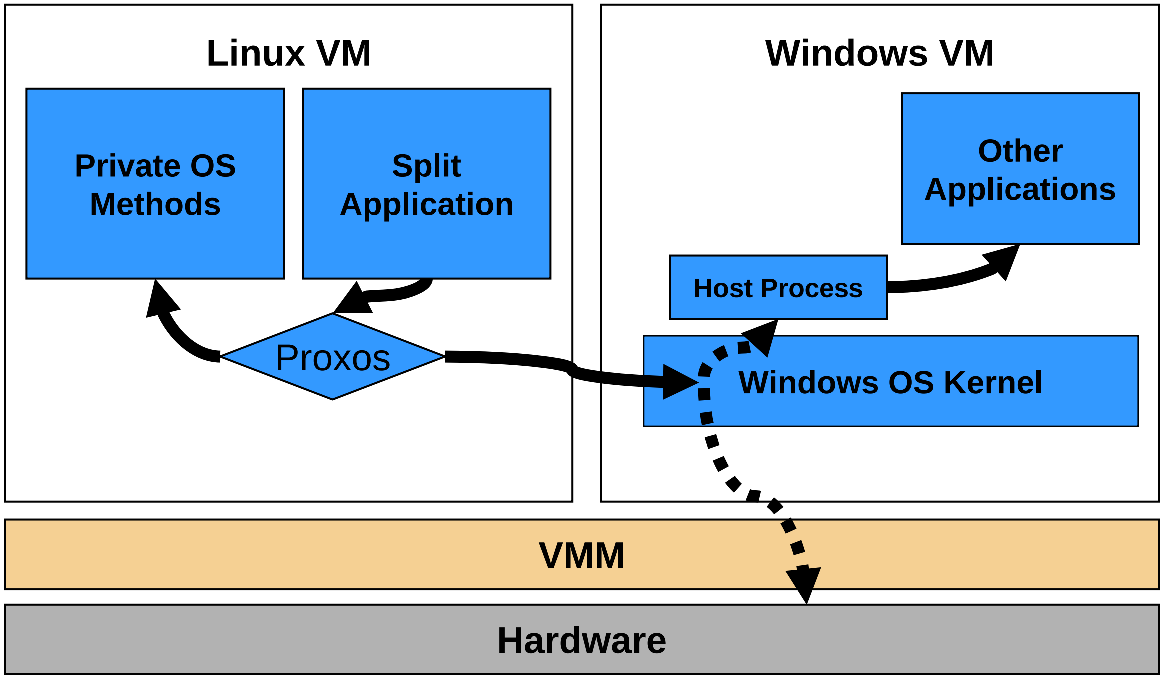
Find ways to make today’s systems secure!

Why work on existing systems?

- Too hard to move to new systems:
  - Moving all your software to a new system is expensive/time consuming.

- Solving systems now means:
  - Exciting ideas getting deployed right away
  - New commercial ideas (companies)
  - $$$
  - Saving people from a lot of grief

Proxos: Composing Operating Systems



- Virtual Machine Monitor (VMM) can run more than one OS simultaneously
  - Pick the best parts of each OS
  - Linux security with Windows ease of use

Hardware Root of Trust

- Modern operating systems are huge and bloated:
  – Too much code to make it all secure

- Lots of interest now in making hardware the new root of trust
  – Have software trust the hardware directly, by pass the OS for protection of data, cryptographic keys, user interaction
  – Initiatives like Lagrande (Intel), Presidio (AMD), TCG (Trusted Computing Group)

- Project
  – Making devices that applications can use without trusting the OS
  – Means the OS can be hacked, but your data is protected!

Courses

- ECE468: 4th year course in computer security
  - Introduction to the basics of security
  - Buffer overflows and exploits, mitigation
  - Basic Cryptography
  - SSL and Web security
  - Network security

- ECE1776: Graduate Security course covering topics in
  - Introduction to current research computer security
  - Structured as a seminar/reading course + project.