

Using VProbes for Intrusion Detection

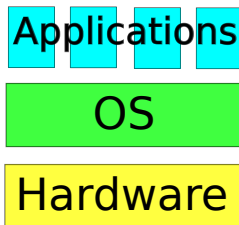
Alex Dehnert

VMware Intern, Summer 2011
Massachusetts Institute of Technology, S.B. 2012

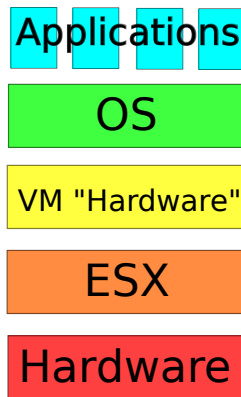
Thursday, September 15, 2011

Virtualization

Traditional



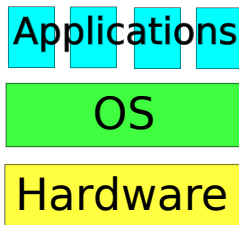
Virtualized



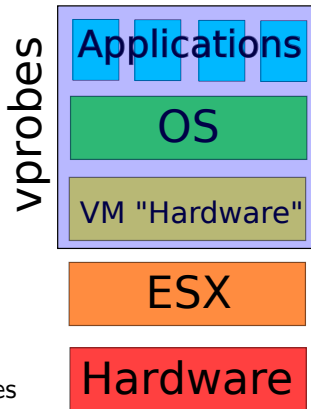
- ▶ Consolidation
- ▶ Security
- ▶ Unique virtualization features

Virtualization

Traditional

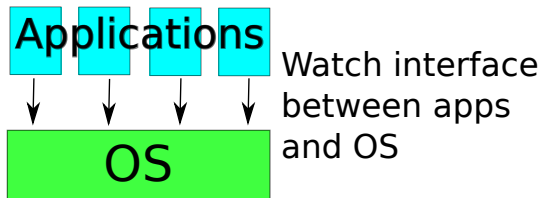


Virtualized



- ▶ Consolidation
- ▶ Security
- ▶ Unique virtualization features
 - ▶ vprobes

vprobes IDS



- ▶ Use vprobes to watch application/OS communication
- ▶ Build a profile of normal behavior
- ▶ Alert when abnormal behavior occurs

Cost of Intrusions

- \$114 billion** Total global cost of cybercrime annually, as estimated by Symantec
- \$75 billion** 2011 spending on IT security for US companies, according to the Ponemon Institute
- \$170 million** Cost to Sony of the recent PlayStation Network hack, including shutting down PSN, network security improvements, etc.

Sources: The Fiscal Times, Huffington Post