

Xen Security



Steven Hand

XenSource, Inc.

Overview



- Why now?
- Why Xen?
- Xen: Security Enhanced
 - XenSE open community effort
 - Current technical work areas
 - Non-issues
- Summary and questions

The need for security



- One of the major problems for home, enterprise and government users:
 - Malware alone cost businesses an estimated \$200bn worldwide in 2004
 - Many fear an increase in concerted attacks (cyber-terrorism, e-extortion, commercial warfare, ...)
 - Hidden costs in inefficient business practices
- Open-source an emerging requirement:
 - Independent vetting of software
 - Governments keen to avoid vendor lock-in

Solution Requirements



- Standard model built around:
 - a small 'separation kernel',
 - mandatory access control, and
 - a set of validated security policies
- Experience has shown also need:
 - *User Experience*
 - Incremental benefit,
 - High performance, and
 - Convenience
 - *Quality of Service*
 - Predictable partitioning and performance
 - Defense against DOS attacks

Xen and Trusted Computing



- Xen has the potential to become *the* trusted computing solution:
 - Open source
 - Small size (~40K lines of code in 2.0, hopefully reducing to ~20K lines in 3.0)
 - Easy to add isolated security services
 - High performance implementation
 - Runs existing application software
 - SRT scheduling and hard resource partitioning gives performance predictability

Xen: Security Enhanced



- XenSE is about building a trusted computing platform around Xen
- Open community effort:
 - All design and implementation done in public domain (mailing lists, source repositories)
 - Buy-in from government (NSA, GCHQ, EU), industry (IBM, HP, Intel, AMD) and academia
 - Lots to do (targeting 4.0 timescale)
- Meeting earlier this week to kick-off...

XenSE Work Areas



- Mandatory access control
 - Add MAC to Xen subjects / objects
 - IBM sHype patch great start
- TPM support
 - Trusted/secure boot
 - TPM virtualization
- Minimizing the TCB
- Devices and device security
- User-interface issues

XenSE: Minimizing the TCB

- Current (2.0/3.0) TCB is too large:
 - Xen, Dom0 kernel, Dom0 root, Network...
 - Great for convenience but bad for security
- Minimizing the TCB involves:
 - Reviewing the Domain «-» Xen interface
 - Adding fine-grained access control
 - Refactoring Domain0:
 - Decomposing functions into isolated components
 - Involves support for 'lightweight domains'
 - Integration with trusted boot + attestation

XenSE: Device Security



- *Availability* a key part of security
- Currently device drivers (and devices) major cause of instability in OSes
- Device security requires:
 - Full implementation of safe hardware interface (w/ IOMMU or other h/w support)
 - Scheduler support for multiple DD domains
 - Restartability, reconfigurability, attestation
 - (possibly) support for secure I/O path

XenSE: User-Interfaces



- Major unaddressed TC issue
 - User convenience *vs* security
- Mostly desktop/notebook concerns:
 - Trusted display (labeled or multihead wm)
 - Trusted HID (incl. attested console access)
- Tensions regarding performance:
 - e.g. how much can be done in server?
 - Initially looking at multi-layer X11 support
- 3D and beyond will be driven by h/w support

XenSE: Non-Issues



- Aiming for agile open design process and “code rules” implementation
- NOT currently focusing on:
 - Standardization,
 - Policy development,
 - Digital Rights Management,
 - Formal methods, or
 - Evaluation – although will endeavor to make XenSE “evaluable”.

XenSE: Summary



- Community effort to build a (the first?) successful trusted computing platform
- Aiming to support wide range of uses:
 - Firewall/IDS domains
 - Virtual Private Machines (VPMs)
 - Conventional MLS systems
- Huge potential market for products
- Want input from as many people, organizations and interests as possible.