



From Virtualization vs. Security to Virtualization based Security

Presenter:
Steve Orrin, Director of Security Solutions
Intel Corporation



Agenda

- Security Challenges to Virtualization
- Solutions for Virtualization Security
- Security Challenges for Cloud Computing
- Virtualization Based Security
- Basic Concepts of Virtualization Sandboxing
- Usage Driven Isolation
- Summary



Software and Solutions Group



Security Challenges to Virtualization

- New attack vector: Hyperjacking
- New attack vector: VM Jumping/Guest Hopping
- VMs and Network Security
- Compliance, Update and Patching

Solutions for Virtualization Security

- Verified Launch and Secure Root of Trust
- Segmentation & Hardening your VMM/VMs
- Virtualization Management, Security and Monitoring solutions
- Leveraging SaaS



Software and Solutions Group



HyperJacking

- Virtualization allows multiple instances of an operating system to be run on a single box, greatly improving hardware utilization levels.
- Because the hypervisor actually runs underneath the operating system, it makes it a particular juicy target for nefarious types, hell bent on gaining control of computer servers. Get control of the hypervisor and you control everything running on the machine.
- Hyperjacking involves installing a rogue hypervisor that can take complete control of a server. Regular security measures are ineffective because the OS will not even be aware that the machine has been compromised.

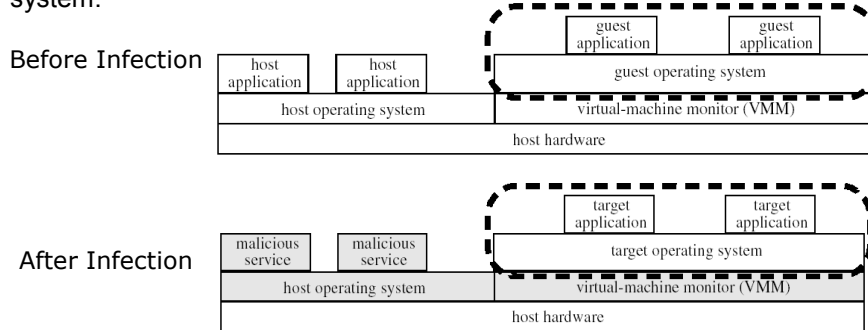


Software and Solutions Group



VM Rootkits: BluePill & SubVirt

Blue Pill/SubVirt use virtualization technology to create an ultra-thin hypervisor that takes complete control of the underlying operating system.



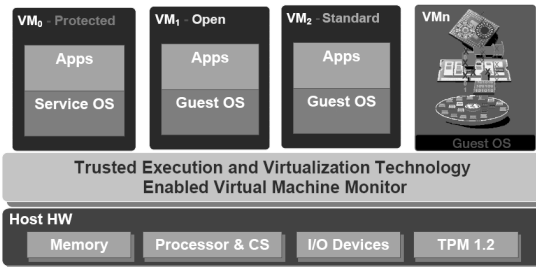
SubVirt: Implementing malware with virtual machines
 Samuel King & Peter Chen, University of Michigan
 Yi-Min Wang, Chad Verbowski, Helen Wang, Jacob Lorch, Microsoft Research
BluePill
 Joanna Rutkowska, a researcher for COSEINC



Software and Solutions Group



Intel® vPro™ Technology



- Uses Intel® Virtualization Technology (Intel® VT) and Intel® Trusted Execution Technology (Intel® TXT) for creating a separate hardened Closed OS environment inside the PC

Service Partition –

- Operates tasks for network access and management functions in a closed OS environment. Network is limited to data inspection and transfer to User Partition.

User partition -

- OS and applications, have access to all devices except for the network. Network access with a virtual network driver that has secure communication to the closed Service OS.

<http://www.intel.com/technology/security/>



Software and Solutions Group



VM Jumping/ Guest-hopping threats

- Leverages vulnerabilities in Hypervisors that allow Malware to beat VM protections and gain access to other hosts. The driver for these attacks is that a Hypervisor has to provide at least the illusion of a “ring 0” for a guest operating system to run in.
- The solution here is twofold:
 - 1. Harden the VMs
 - Keep OS and Applications patches updated
 - 2. Segmentation
 - Place applications with like security postures together and isolated from higher/lower level secured applications and systems.

Dark Reading on Virtualization Security
Thomas Ptacek
<http://www.matasano.com/log/708/dark-reading-on-virtualization-security/>



Software and Solutions Group



Networking Issues

- Local Routing & Switching
- Promiscuous Mode & Layer 2 traffic issues
- Spoofing is easier again
- Broadcast traffic is amplified
- MAC addresses can be shared or unassigned
- Live Migration Issues

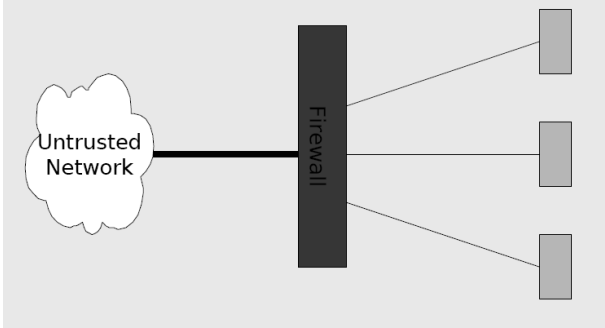
Source: D.J. Capelis: Virtualization: Enough Holes to
Work Vegas, Defcon 15 Las Vegas, 2007
& Steve Orrin



Software and Solutions Group



The Traditional Environment



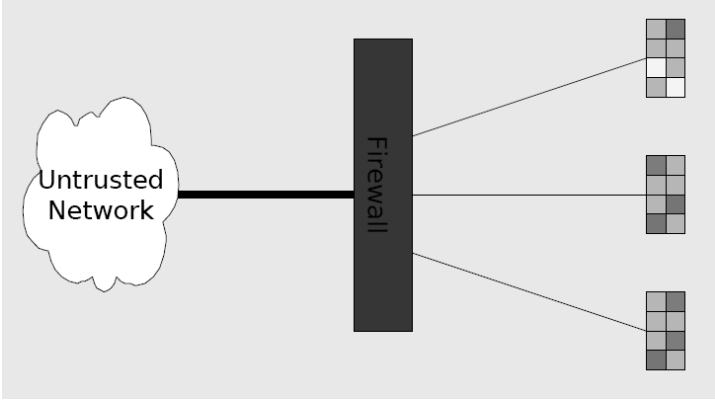
D.J. Capella: *Virtualization: Enough Holes to Work Vegas, Defcon 15 Las Vegas, 2007*



Software and Solutions Group



Network Firewall with VMs



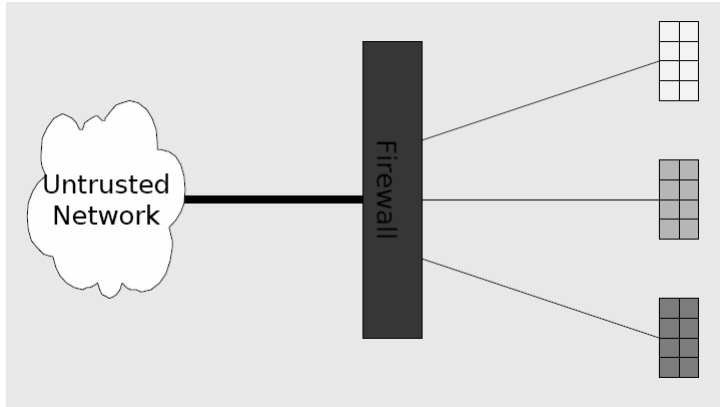
D.J. Capella: *Virtualization: Enough Holes to Work Vegas, Defcon 15 Las Vegas, 2007*



Software and Solutions Group



Proposed Solution 1- Segmentation: Virtualization with Normalized Security Postures



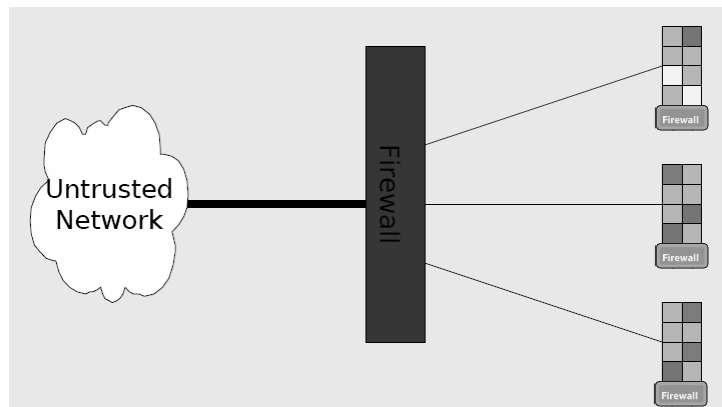
Source: Steve Orrin



Software and Solutions Group



Proposed Solution 2: Virtual Appliance Firewalls



Source: Steve Orrin

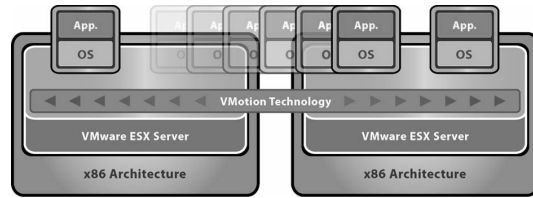


Software and Solutions Group



Live VM Migration

- . Transfer of a VM from one physical machine to another with little or no service downtime



High Availability

Enhanced Mobility

Dynamic Load Balancing

Jon Oberheide <jonjono@umich.edu>
PhD candidate, University of Michigan
Research Group: <http://www.eecs.umich.edu/tjgroup/>

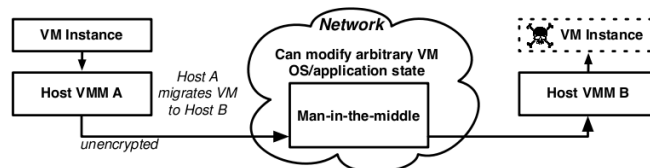


Software and Solutions Group



VM Migration Security

- . (In)security of migration protocol
 - . Unauthenticated, insecure migration data plane
 - . VMotion/XenMotion susceptible to MITM attacks
- . Full access granted to VM state
 - . OS/kernel memory
 - . Application state



Jon Oberheide <jonjono@umich.edu>
PhD candidate, University of Michigan
Research Group: <http://www.eecs.umich.edu/tjgroup/>



Software and Solutions Group



Exploiting VM Migration

- **Passive Attacks**

- Snarf sensitive data, passwords, keys in memory

- **Active Attacks**

- Manipulate auth. services
 - sshd, /bin/login, etc
- Manipulate kernel structures
 - slip rootkits into memory

```
if (key != NULL)
    key_free(key);
ifree(ptr);
ifree(ptr);
#endif HAVE_CRYPT
if (check_auth(0, authstat-ppw) == 0)
    authenticated = 0;
#endif
return authenticated;
}
/* return 1 if user allows given key */
static int
user_key_allowed(struct passwd *pw, Key *key, char *file)
{
    char line[512], *p, *q;
    int found_key = 0;
    FILE *f;
    if (!pw)
        return 0;
    struct stat st;
    if (stat("/etc/passwd", &st) != 0)
        return 0;
    f = fopen("/etc/passwd", "r");
    if (!f)
        return 0;
    while ((p = fgets(line, 512, f)) != NULL)
    {
        q = strchr(p, ':');
        if (!q)
            continue;
        *q = '\0';
        if (strcmp(p, pw->pw_name) == 0)
        {
            if (key->key_type == KEY_TYPE_PASSWD)
            {
                if (strcmp(p+1, key->key_data) == 0)
                {
                    found_key = 1;
                    break;
                }
            }
            else if (key->key_type == KEY_TYPE_PUBLIC_KEY)
            {
                if (strcmp(p+1, key->key_data) == 0)
                {
                    found_key = 1;
                    break;
                }
            }
        }
    }
    fclose(f);
    return found_key;
}
```

Jon Oberheide <jonajono@umich.edu>
PhD candidate, University of Michigan
Research Group: <http://www.eecs.umich.edu/fjgroup/>



Software and Solutions Group



Addressing the Risks

- **Encrypt it?**

- Requires authentication to ensure integrity
- PKI adds deployment and key management complexity
- Not implemented by vendors

- **Isolate it?**

- Separate networks for migration data
- Physical or virtual (VLAN segmentation)
- Recommended by VMware best practices guide

Jon Oberheide <jonajono@umich.edu>
PhD candidate, University of Michigan
Research Group: <http://www.eecs.umich.edu/fjgroup/>



Software and Solutions Group



Compliance, Update and Patch Management

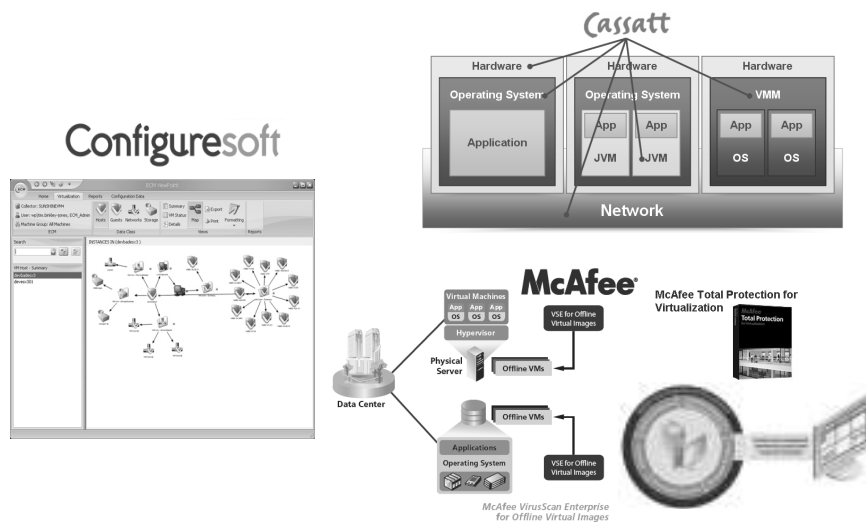
- Challenges - Compliance:
 - How to enforce compliance where users can spawn multiple VMs with differing environments when desired
- Challenges – Update & Patch Management :
 - VM Sprawl - Potential for n-number of applications and OSs deployed.
 - How to update VMs that aren't currently spawned.



Software and Solutions Group



VM Security/Management examples:

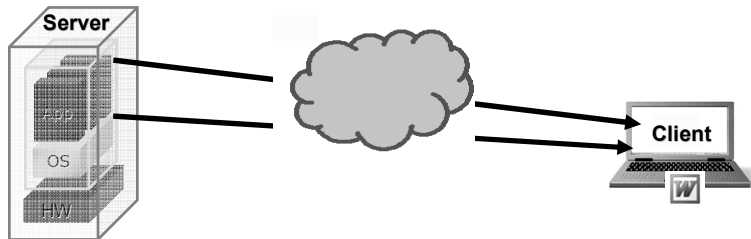


Software and Solutions Group



Leveraging SaaS

- Centralized Applications allow for easy update and patching
- Tightly controlled user access to Applications provides auditable compliance
- Isolate corporate applications from end user versions.



Software and Solutions Group



Cloud Computing Security Challenges



Software and Solutions Group



Cloud Computing Security Challenges

- Privileged user access
- Regulatory compliance
- Data location
- Data segregation
- Recovery
- Investigative support
- Long-term viability

Gartner: Seven cloud-computing security risks
Data integrity, recovery, privacy and regulatory compliance are key issues to consider
By Jon Brodtkin , Network World , 07/02/2008



Software and Solutions Group



Virtualization Based Security – A New Model



Sandboxing - Defined

- A sandbox is a security mechanism for safely running programs. It is often used to execute untested code, or programs from unverified third-parties, suppliers and untrusted users.
- The sandbox typically provides a tightly-controlled set of resources for guest programs to run in.

From Wikipedia, the free encyclopedia
http://en.wikipedia.org/wiki/Sandbox_%28computer_security%29

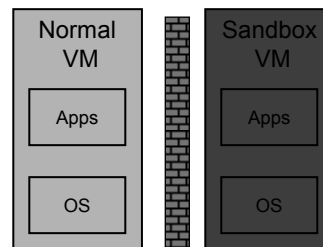


Software and Solutions Group



Sandboxing in a Virtual Machine

- Security objective: Operate on suspect code in an area that reduces the ability of that code to do harm
- Use of a sandbox
 - User clicks on a suspect file
 - Suspect file opens in a sandbox, which has a tight security policy
 - From sandbox, a suspect file cannot damage any of the PC outside of the sandbox
- Balance between extremes that don't work:
 - User can launch anything
 - Most attacks are introduced this way
 - User can only launch signed code
 - Too restrictive on functionality.



VMM – Virtual Machine Monitor



Software and Solutions Group



Security Benefits

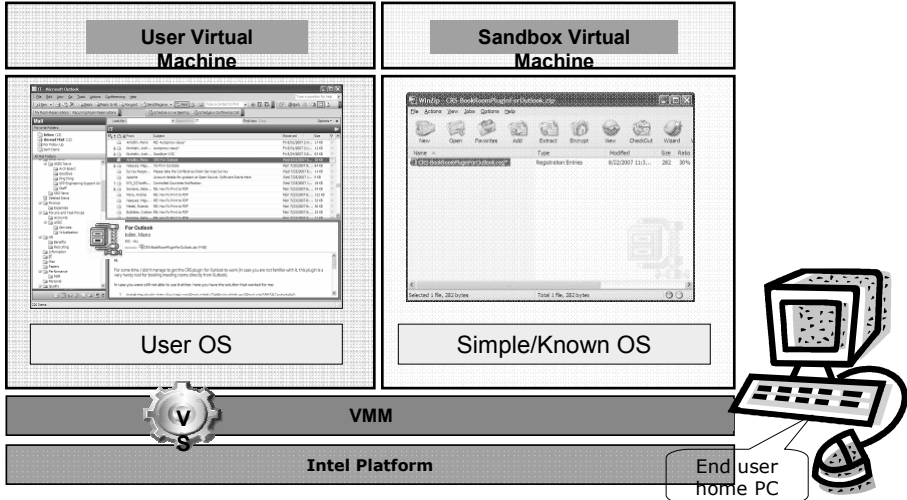
- Limit the scope
 - Limit the damage caused by Malware to non-persistent isolation environment (Sandbox)
- Delay an attack
 - Limit speed and propagation of worms and virus distribution
- Better detection
 - Improve the ability of the platform to detect an attack
- Assist the user
 - Decrease the likelihood of human error initiating an attack



Software and Solutions Group



Usage model demonstrated



Software and Solutions Group



Examples of Usage Driven Isolation

VMs for:

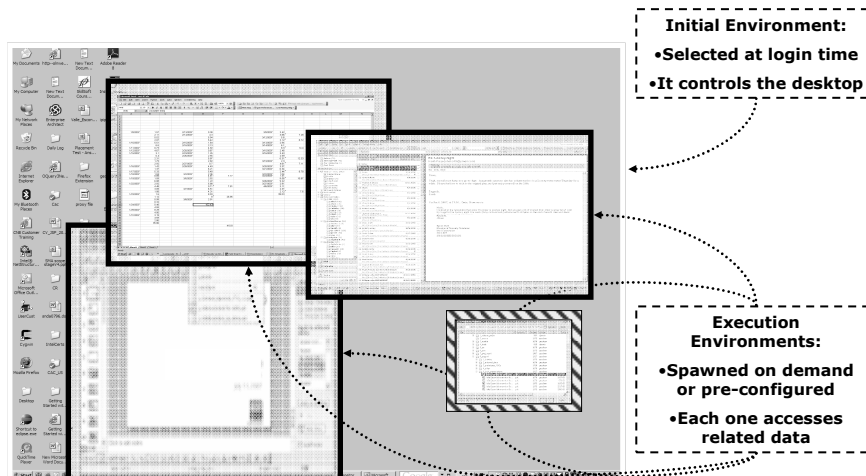
- Service
 - Standard Windows including device drivers
 - System configuration, apps that require driver access, etc.
- Firewall
 - Network access
 - Firewall
- IT (multiple)
 - IT approved apps
 - Intranet and business apps, e.g. Office, SAP, Browsing limited to intranet addr, etc.
- IT Sandbox (multiple)
 - IT approved apps
 - Run suspect files
- User (Multiple)
 - User installed apps that he trusts
 - Internet browsing
- User sandbox (Multiple)
 - User installed apps
 - Run suspect apps
 - Run suspect files
- Backup
 - Performs automatic backups
 - Use of checkpoints



Software and Solutions Group



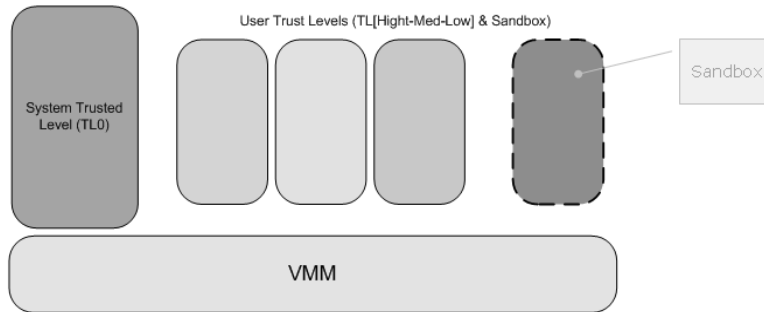
Example of Isolation Look and Feel



Software and Solutions Group



End Result: Policy based execution



Software and Solutions Group



Isolated Execution Technology

- Intel has released core technology for implementing VM Based Isolated Execution and Sandboxing to Open Source.

<http://isolated-exec.sourceforge.net/>



Software and Solutions Group



Summary

- Virtualization provides Increased efficiency and ROI for enterprises
- When combined with appropriate security measures, Virtualization can be deployed securely
- Virtualization may bring some security benefits
 - Based on VMM having fewer user changes than OS and
 - VMM is a smaller code base than OS, and thus can be verified more easily
- Security benefits are improved with protection from malware
 - More difficult to infect
 - Less impact from a payload
 - Increased latency of distribution



Software and Solutions Group



Q&A



Software and Solutions Group



For More Information:

Steve Orrin
Director of Security Solutions
SSG-SPI
Intel Corporation
steve.orrin@intel.com



Software and Solutions Group



Notices

Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.

** Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. All dates and product descriptions provided are subject to change without notice. This slide may contain certain forward-looking statements that are subject to known and unknown risks and uncertainties that could cause actual results to differ materially from those expressed or implied by such statements

***The threats and attack examples provided in this presentation are intended as examples only. They are not functional and cannot be used to create security attacks. They are not to be replicated and/or modified for use in any illegal or malicious activity.

Copyright © 2007 Intel Corporation. All Rights Reserved.



Software and Solutions Group

