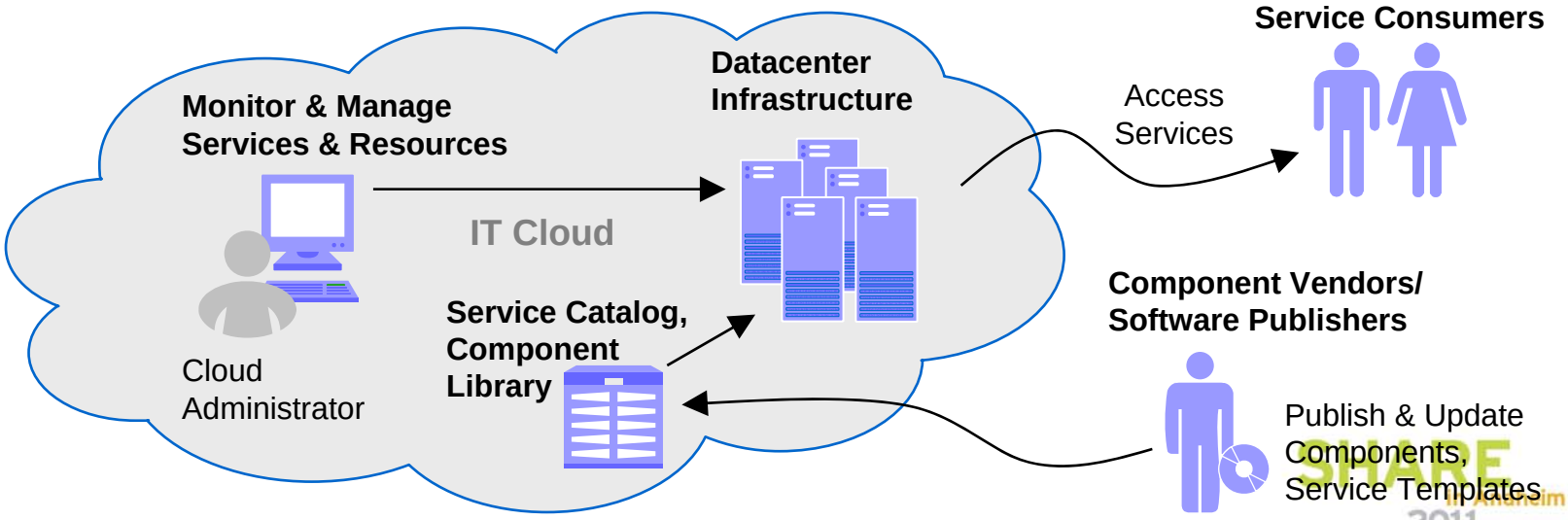
The New Hacker Playground: “The Clouds”
Session 8842

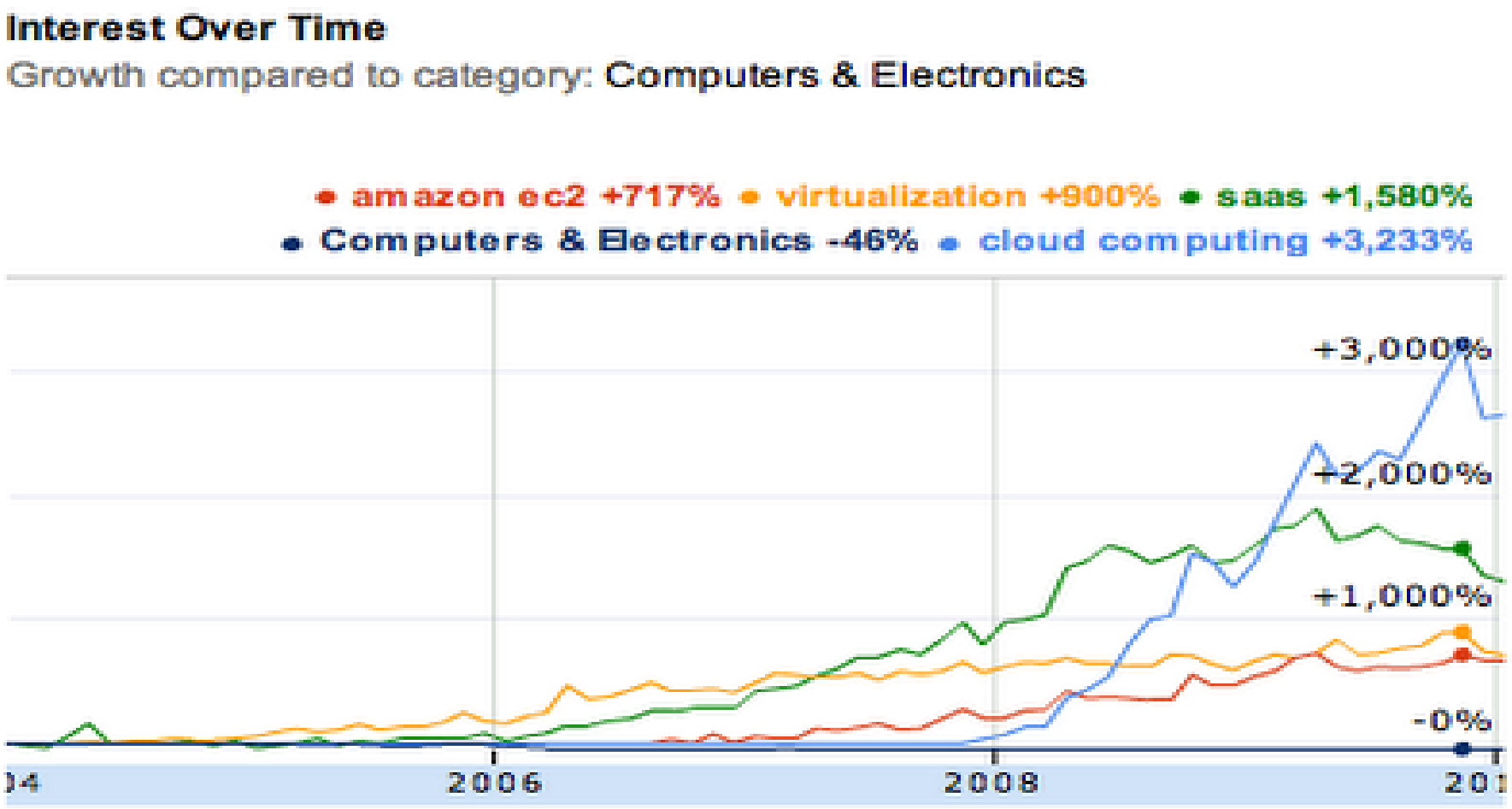
Ellis Holman
eaholma@us.ibm.com

Cloud computing or Software As A Service (SAAS) is beginning to converge on a common set of attributes

- **Automated provisioning of computing resources and services**
- **Elastic scalability**
- **Highly virtualized infrastructure**
- **Standardized set of offerings which leverage common software stacks and operational policies**



At least one study shows increasing interest in cloud computing



Trust is a huge issue in the cloud environment

- The customer's compute tasks are now executing within the cloud providers infrastructure
- The "servers" these tasks are operating on are guests under the cloud's hypervisors -- i.e. essentially fictions created by the hypervisor software.
- The hypervisor is software, so it is easily modified; and it is all-powerful with respect to the guest instances running under it -- the hypervisor can copy, modify, or delete data from within the guest at will.
- This is a new trust problem: the customer must trust that the cloud provider's hypervisors and management software are behaving appropriately and haven't been tampered with.

Risky user behavior leads to unfortunate consequences

- Recent Webroot research data about risky behavior from a survey of 1,100 users of social networks, showed that:
  - About one third of the respondents said they include at least three pieces of personally identifiable information
  - Over one third use the same password across multiple sites.
  - Two-thirds of respondents said they do not restrict any details of their personal profile from being visible through a public search engine such as Google
  - Over half are not sure who can see their profile.

Many people rely on virtualized email which can be compromised

- For the thousands of users that go to http://www.gmail.com the data flowing across a network is in the open
- Gmail website sends a cookie (a text file) containing your session ID to the browser.
- This file makes it possible for the website to know that you are authenticated
- This makes it possible for an attacker sniffing traffic on the network to insert an image served from http://mail.google.com and force your browser to send the cookie file, thus getting your session ID.
- Once this happens the attacker can log in to the account without the need of a password.
- Use https://www.gmail.com instead

Cross site scripting can allow personal data to be exposed

- A CSS vulnerability is caused by the failure of a site to validate user input before returning it to the client's web-browser
- The essence of cross-site scripting is that an intruder causes a legitimate web server to send a page to a victim's browser that contains malicious script or HTML of the intruder's choosing
- The malicious script runs with the privileges of a legitimate script originating from the legitimate web server

Security is sometimes forgotten in the rush to virtualize

- "We're finding security is the forgotten stepchild in the virtualization build out," says Stephen Elliott, IDC's research director for enterprise systems management software. "That's scary when you think about the number of production-level VMs." According to IDC, 75 percent of companies with 1,000 or more employees are employing virtualization today.

Isolation of virtual servers can be attacked in a number of ways

- Shared Hardware attacks
  - SMT attacks are something old and something new
- Attacking the host scheduler
- Accessing/using real hardware
  - USB port
  - Video card
  - Passing real hardware will wedge entire box
- Covert Channels
  - Internal networks
  - Resource sharing

Covert Channels can be used to pass data between machines

- Use something like memory on one machine
- Detect it on another
  - RDTSC (**Time Stamp Counter**) or any other timesource tool
  - May also want to use RDTSCP which is a serialized version of RDTSC
- Pass data in Layer 2
  - Little or no use of EBTables
  - Could use IPX or Appletalk
  - Maybe even DECnet
  - Filters in a hardware router don't exist

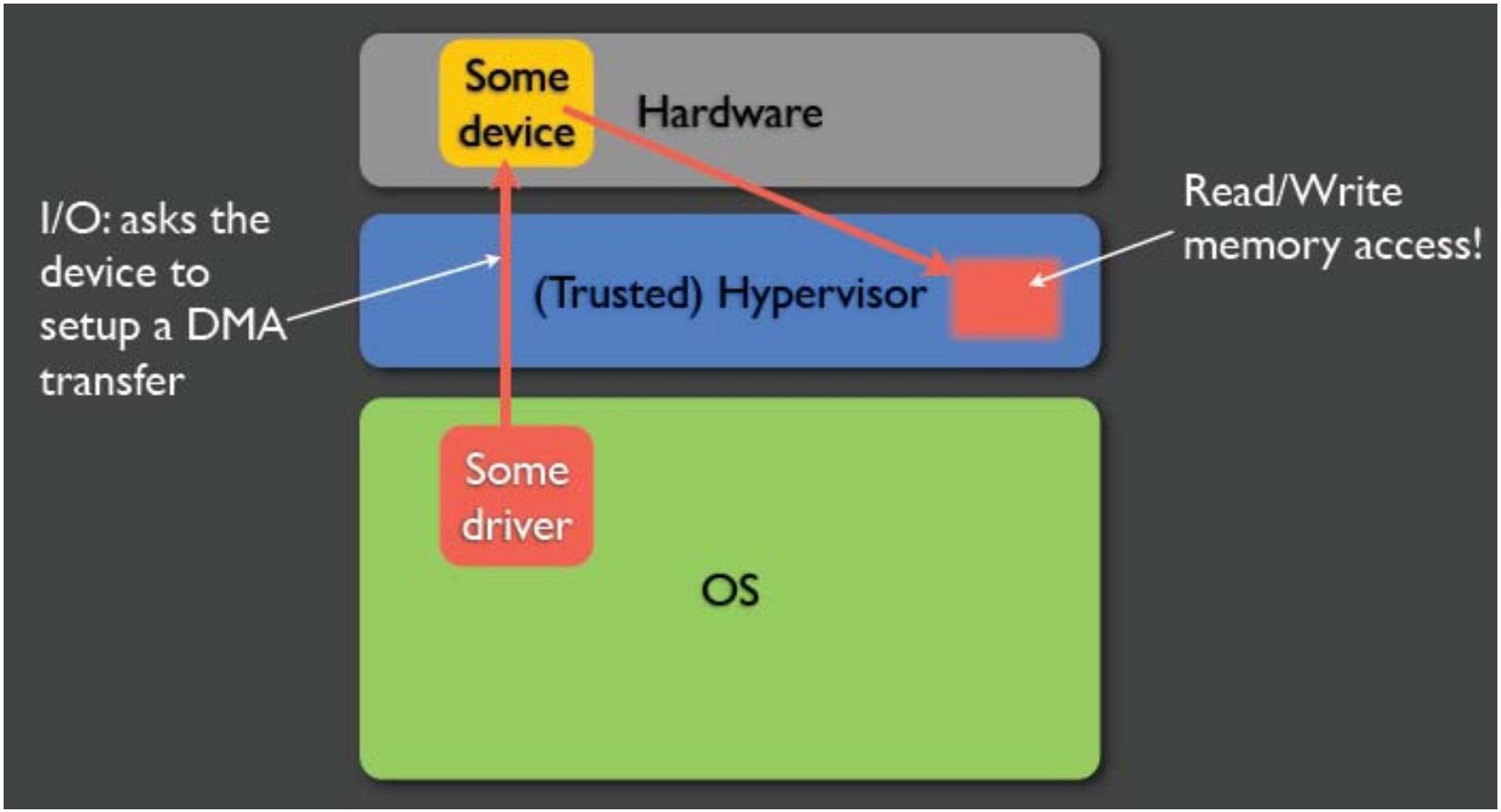
Empirical“mapping” reveals how to launch VMs so it maximizes the placement.

- Enumerating public servers using external probes and translating responsive public IPs to internal IPs (via DNS queries within the cloud)
- Another created by launching a number of cloud instances of varying types and surveying the resulting IP address assigned
- By manipulating how they request for new VMs using legitimate calls, it was possible to engineer a 40-percent chance of securing VM resources on the physical server hosting an identified target
- Time-shared caches allow an attacker to measure when other instances are experiencing computational load
- While the attacker does not directly learn exactly which keys are pressed, the attained resolution suffices to conduct the password-recovery attacks on SSH sessions

Windows desktop software could let an attacker break out of the VM environment

- Lets an attacker create or alter executable files on the Windows host OS -- but only
- If VMware's Shared Folders feature is enabled
  - At least one folder on the underlying host system is configured to share files with the VM
- Workarounds for the bug include disabling Shared Folders altogether, or configuring it to read-only access to the host folder

Malicious driver code can target the hypervisor via DMA



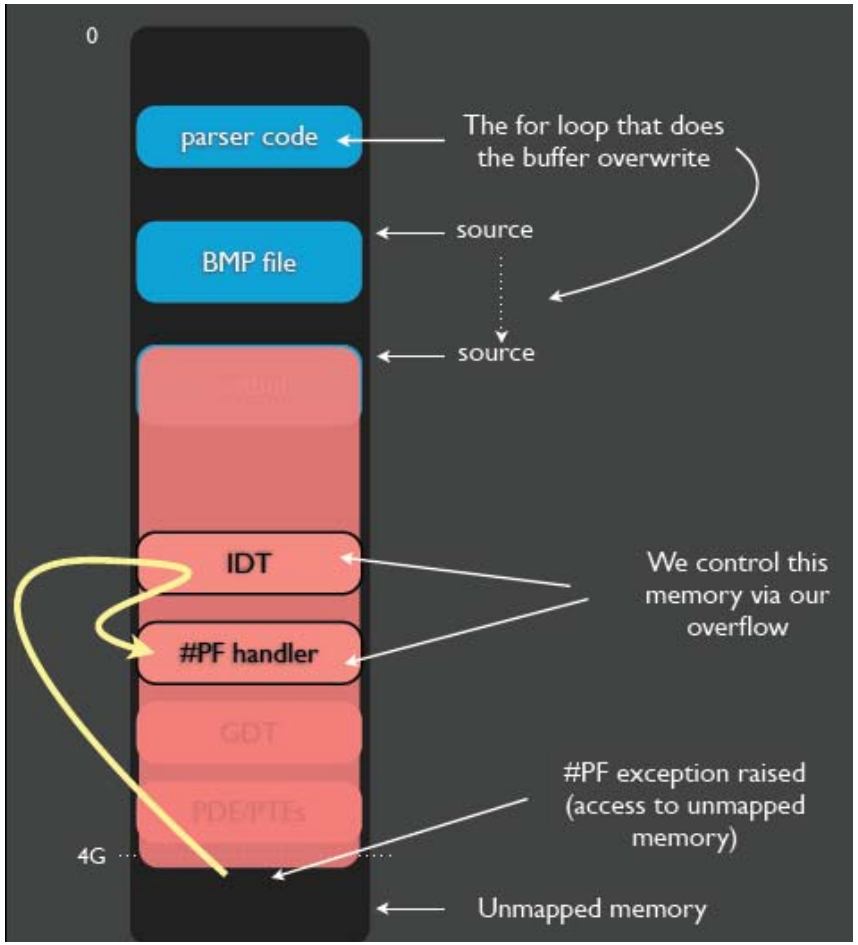
Hypervisors can be compromised by DMA

- Taking control over hypervisor's code by DMA.
- If there is a programming error in the hypervisor code (e.g. a buffer overflow in a hypercall), it could allow to overwrite hypervisor's code and install the backdoors as well.
  - If the said error was reachable by an unprivileged domain, it could allow for direct elevation to ring0 from domU.
- Hypervisors that are designed to be the only all powerful entities in the system (and thus are able to control administrative operations), e.g. Hyper-V[15], are attractive targets for placing a backdoor as well.

Related attacks

- Loic Duflot (2006) - jump to SMM and then to kernel from there (against OpenBSD securelevel)
- Now prevented by most BIOSes (thanks to the D_LCK bit set)
- Sun Bing (2007) - exploit TOP_SWAP feature of some Intel chipsets to load malicious code before the BIOS locks the SMM and get your code into SMM
  - But this requires reboot

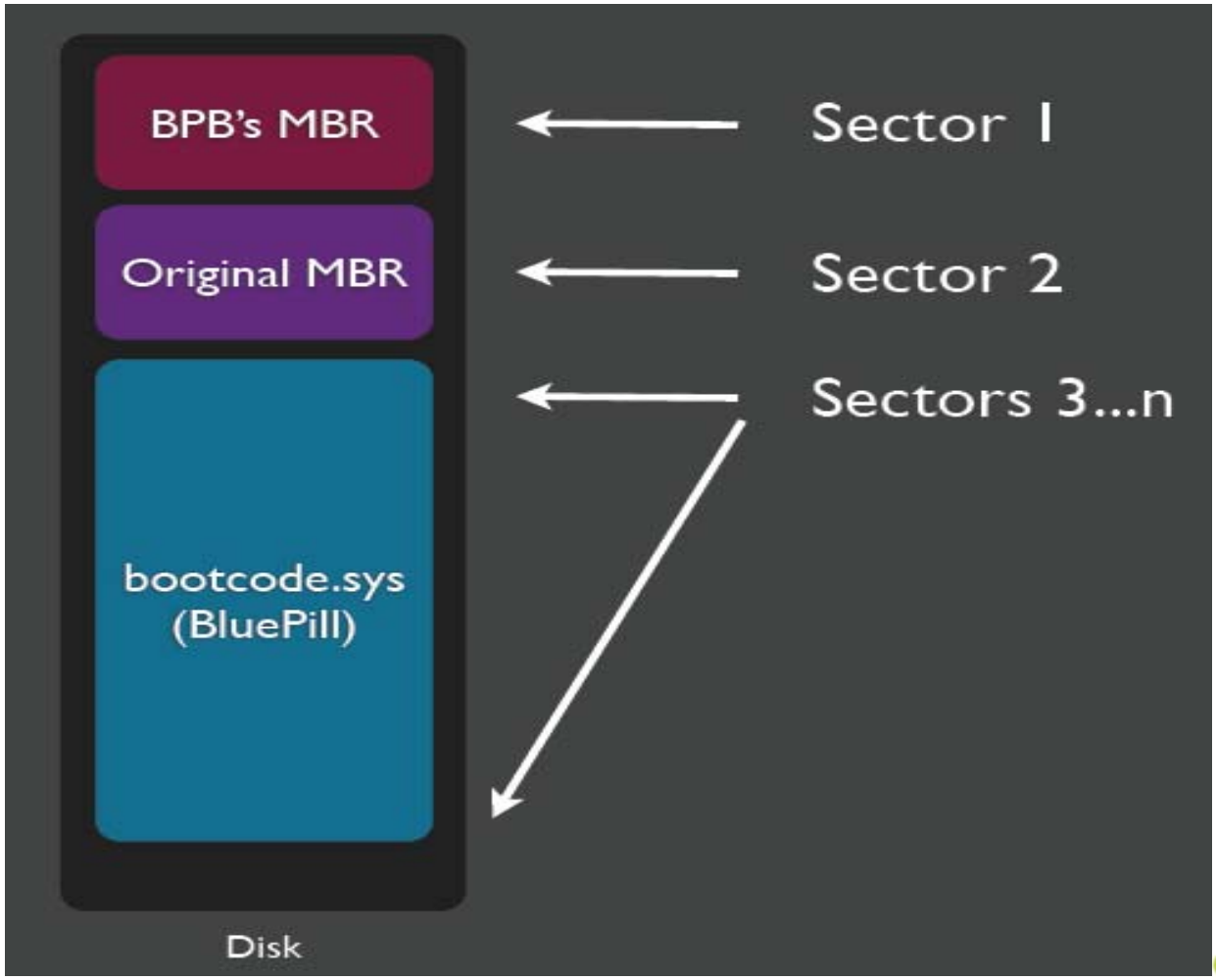
Infecting the BIOS, difficult, not impossible



Backdoors can be placed in machines running the Xen hypervisor

- **An attacker can gain backdoor control over the host by overwriting Xen code and data structures**
- **Not a single byte in dom0 domain is modified**
- **The detection of such a backdoor is difficult if conducted from within dom0**
- **Modification of device drivers and core kernel code to conveniently conduct DMA to arbitrary physical address**
- **This allows for control over the hypervisor.**
- **Two backdoors have been implemented:**
  - **One resides in the hypervisor code**
  - **The other resides in a hidden domain with artificially elevated privileges**

Blue Pill Boot = MBR infector + Blue Pill loader + Blue Pill that supports nested virtualization



High consumption of resources can lead to denial of service

- ***Label1:***
- ***add $1, $2, $3***
- ***br Label1***

- High-ILP program executes without stalls
- Repeatedly access register file at high rate
- Create repeated hot spots at register file
- Heat-up time short (1.2ms), cooling time long (12ms)
- Degrades CPU utilization to 10%, but is it due to hogging fetch bandwidth or due to heat?

This type of resource hog can render a system nearly inoperative

- Resource sharing prevalent in current systems
- Malicious users can exploit the sharing
- DOS attacks maliciously hog shared resource
- Can render the system practically inoperative
- For example:
  - Fork bomb
  - TCP *syn* flood
- Can be detrimental to businesses and organizations

Distributed denial of service attacks can also be used

- Not particularly sophisticated and appears to be more of a nuisance than a threat to security
  - It uses a variety of well-known distributed denial of service (DDoS) attacks that try to overwhelm Web sites with useless requests and make them unavailable for legitimate users
- Botnet code behind some attacks do not use typical antivirus evasion techniques and does not appear to have been written by a professional malware writer

VMWare has some networking issues which make a hacker's job easier

- Bypass the host firewall
  - Pick any IP address set that you want, not shared by the rest of the network
  - VM bypasses firewall by default in bridged mode, no traffic goes to host firewall
- Promiscuous Mode
  - All network traffic of all virtual machines visable
- MAC Impersonation
- Easier to spoof
  - Some mechanisms to prevent, but are turned off by default

A Content Mangement (CMS) product allows anyone in your organization to update your Web site using some simple HTML forms

- Updates can do it from anywhere via the Web.
- No need to have access to FTP as there are no files to upload
- Need to add a story to the front of your site? Just enter a password and type away
  - But what if a hacker were to do this?
  - A malicious, untrue news release posted on your site for just an hour, and which found its way onto the internet rumor mill, could halve a company's stock price
  - And the harder you work to publicize your denial of the story, the more people get alerted to the fact that you've been hacked
  - So the hacker wins twice

SQL Inject attack involves solving a puzzle that is a cross between Hangman and 20 Questions

- The SQL Injection attack allows external users to read details from the database. In a well designed system this will only include data that is available to the public anyway. In a poorly designed system this may allow external users to discover other users' passwords.
- **Here is an example of guessing a password**
- **Find out if Jake's password includes the letter "w".** Enter xxx as user name and enter the following string as the password:

```
' OR EXISTS(SELECT * FROM users WHERE name='jake' AND password LIKE '%w%') AND ''='
```

- **Find out if Jake's password has "w" as the third letter.** Enter xxx as user name and enter the following string as the password:

```
' OR EXISTS(SELECT * FROM users WHERE name='jake' AND password LIKE '__w%') AND ''='
```

SQL Injection, allows a malicious individual to execute arbitrary SQL code on your server

- The page might be a basic HTML form that contains a textbox called CustomerNumber and a submit button
- When the form is submitted, the following SQL query is executed:

```
SELECT *
FROM Orders
WHERE CustomerNumber = CustomerNumber
```

- The results of this query are then displayed on the results page

The results can be quite devastating

- Imagine that someone comes along and enters the following data in the CustomerNumber field: “14; DROP TABLE Orders”
- This would cause the following query to execute:

```
SELECT *
FROM Orders
WHERE CustomerNumber = 14; DROP TABLE Orders
```

- Obviously, this is not a good thing!

Some simple actions can prevent problems

- Implement parameter checking on all applications
  - For example, if you're asking someone to enter a customer number, make sure the input is numeric before executing the query
  - You may wish to go a step further and perform additional checks to ensure the customer number is the proper length, valid, etc
- Limit the permissions of the account that executes SQL queries
- The rule of least privilege applies
  - If the account used to execute the query doesn't have permission to drop tables, the table dropping will not succeed!
- Use stored procedures (or similar techniques) to prevent users from directly interacting with SQL code

Off-line storage extends the flexibility of Web applications, it also opens up an entirely new type of vulnerability for users

- Gears is a browser plug-in that allows Web applications to work off-line
  - With the user's permission, the plug-in installs a copy of SQLite, a lightweight relational database, on the local machine, which applications can use to store their data
- Just as malicious hackers have harvested data from server-side databases using techniques such as SQL injection, so too could they target these client-side databases, using similar methods
- In contrast, someone wishing to fish through the database supplied by a social-networking service could simply download an identical copy of the database from that service, which would reveal the database structure

Proposed HTML 5 standards, uses JavaScript library functions to access the client-side database

- Most obvious technique would be XSS (Cross-Site Scripting), in which the surreptitious query code is embedded into a link to the legitimate sites
- Browsers can be sent to a malicious copycat site by the use of DNS hijacking, for instance. Or, if the attacker could write to the local file system, say through a browser vulnerability, then the local name resolution file (such as the hosts file on Windows) could be amended with false addresses
- A scan of local databases used for Gmail and Google Voice services turned up items such as the e-mail headers for Gmail and contact information in the Google Voice database

By default some online storage systems assign public folders with a public file that is shared

- Simple code can be used to enumerate users:

```
#!/usr/bin/env python
import httplib
f = open("dropbox_accts.txt", "w")
for num in range(1440000, 1450000):
request_string = "/u/{0}/Top%20Secret.txt".format(num) conn =
   httplib.HTTPConnection("dl.dropbox.com")
   conn.request("GET", request_string) req =
   conn.getresponse() if req.status == 200:
print(req.status)
f.write("{0}\n".format(num))
```

If there is a return on Top Secret.txt, it records the number in to a file called dropbox_accts.txt

This will revel a great deal of user information

- Obviously you should **NOT** put sensitive data on a public folder, but still people do so
- After sifting through the data it is possible to determine the name of the individual who owns the account
- From this activity it is possible to obtain an email address associated with the login of the account
- If the email address was obtained then that would lead to the login (email), account number, and the person's real name

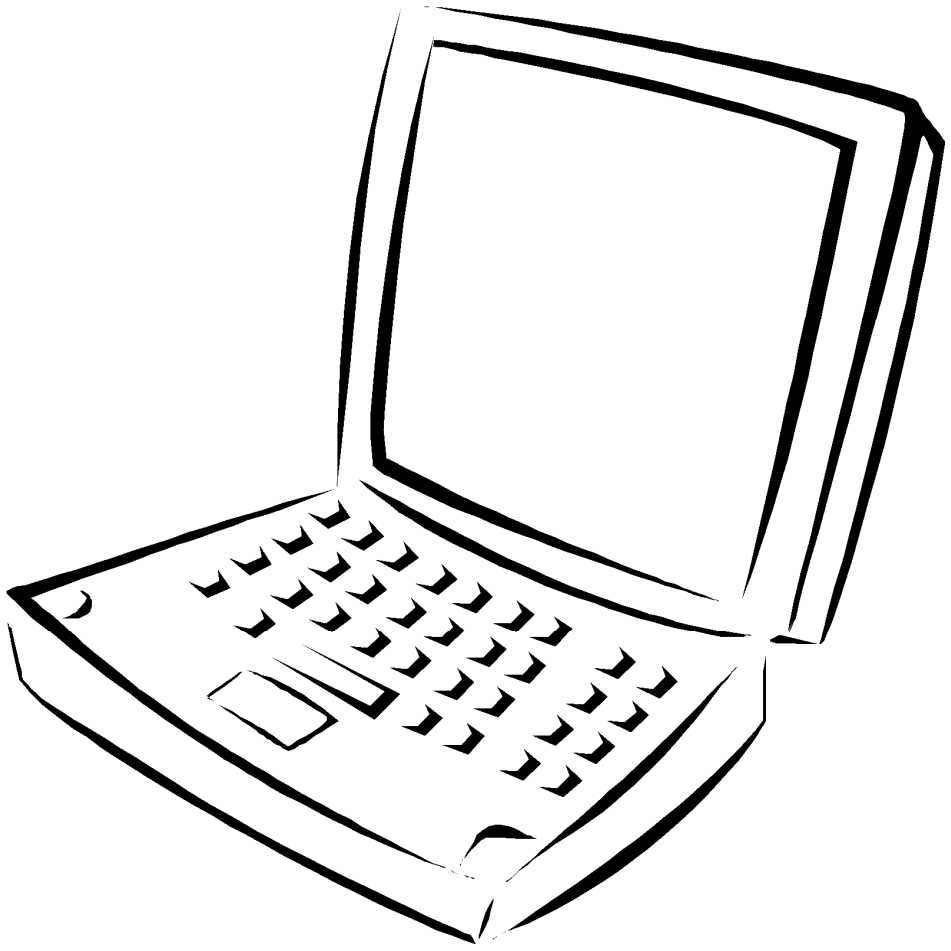
Good collaboration tools may not be so secure

- The Google Docs site indicates they use the same privacy policy as the one located at the primary Google site in addition to some other stipulations.
- Basically there is very little expectation of tight controls to the files put onto the site; security is pretty much left up to the site users.
- And that amount of security is pretty limited, considering Google Docs indicates that the files you entrust to them may be “read, copied, used and redistributed by people you know or, again if you choose, by people you do not know.
- Information you disclose using the chat function of Google Docs may be read, copied, used and redistributed by people participating in the chat.”
- Google Docs gives a nonchalant warning to “Use care when including sensitive personal information in documents you share or in chat sessions, such as social security numbers, financial account information, home addresses or phone numbers.”
- It was good to see Google Docs indicates that you may “permanently delete” files from their systems, but then in the next sentence states that “**Because of the way we maintain this service, residual copies of your files and other information associated with your account may remain on our servers for three weeks.”**

Summary

- Cloud computing offers some unique security challenges
- Old techniques have been given new life in the cloud
- Cloud computing relies on a virtualized environment which has some vulnerabilities
  - Internal DoS attacks can cause loss of service to legitimate user
- Inadvertent exposure of user data in shared areas of cloud storage services can be a problem
- Hardware too can be compromised by sophisticated attacks

QUESTIONS?



Sources

- **WMWare Hacking** by D.J Capelis
- **Heat Stroke: Power-Density-Based Denial of Service in SMT** by Jahangir Hasan, Ankit Jalote, T. N. Vijaykumar and Carla Brodley
- **Cross-Site Scripting Vulnerabilities** by Jason Rafail, CERT® Coordination Center
- **Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds** by Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage
- **Subverting the Xen Hypervisor** Rafal Wojtczuk

Sources

- **Web app storage open to attack** by Joab Jackson
- **Privacy and Cloud Computing Challenges** by Rebecca Herold