Course Introduction

• **What I will discuss today:**
  
  – *My experience as an “expert” witness for a few IT security cases*
  – *Technical issues*
  – *Legal issues*
  – *Lessons learned by those involved*
Agenda: Overview of Case Studies

- **Case Study #1: Tower Records**
  - **December 2002**
  - **Summary**
    - Flaw discovered in online store for Tower Records
    - Federal Trade Commission charges Tower Records with not properly securing consumer data

- **Case Study #2: Purity Wholesale Grocer**
  - **Incident: June 1998**
  - **Trial: Aug 2001**
  - **Summary**
    - Employee is accused of uploading a virus to company servers
    - 2\textsuperscript{nd} case to go to trial under 18 U.S.C. Section 1030
About the Author

- **David Rhoades**
  - PSU - B.S. Computer Engineering
  - Info Sec since 1996
  - david.rhoades@mavensecurity.com
  - Provided analysis for the FTC (case study #1)
  - Expert witness for US DOJ during case study #2.

- **Maven Security Consulting, Inc.**
  - www.MavenSecurity.com
  - info sec audits and training
  - expert testimony (obviously)
Case Study #1

Tower Records

Maven
SECURITY CONSULTING
Tower Records Incident

- **December 4, 2002**
- **A consumer identifies a security flaw in Tower Records online store.**
- **An “order status” URL can be manipulated to view other customer orders**
- **Bug finder tells the world via music forum posting**
LET'S LOOK AT PEOPLE'S TOWER RECORDS ORDERS!

I Love Everything | New Answers | Unanswered Questions | Ask A Question | iXor.com | Donate


YOU CAN SEE WHAT PEOPLE BOUGHT!


OMG GREAT TASTE

-- Jonathan Williams (x...), December 4th, 2002.
I notice this on the right-hand side of the page: *Your privacy is important to us. Tower Records is committed to safeguarding your privacy online. We will never share your personal information with anyone for any reason without your explicit permission.*

Why do so many people only order one CD? If you're paying the postage costs you might as well order a few while you're at it.

HEY! employ self-censorship and respect people's right to privacy! what's so interesting abt. looking at the orders of people you don't know anyway?  
- *michael wells (wellsmj...), December 4th, 2002.*

I like to have my *finger* on the pulse of the nation.  
- *Jonathan Williams (x...), December 4th, 2002.*
Consumer Data Revealed

- **Name**
- **Billing & Shipping Addresses**
- **Items ordered**
- **Email address**
- **Phone Numbers**

- **No credit card information was revealed!**
Legal Charges & My Involvement

• Charges are brought by FTC...not against the bug finder but against Tower Records!

• FTC charges alleged that
  – Tower Records violated their own stated privacy policy
  – Security flaw was easy to prevent
  – Tower Records did not take adequate precautions

• FTC hires me to evaluate technical details of the weakness – was Tower negligent?
Technical Details

- Each consumer received an email confirmation for their order
- Email included an order status URL to view the order
- “orderno” was unique identifier for each order
  - Simple numeric string
  - Sequentially issued from one order to the next
Trivial Attack? (Look Ma’, no foo!)

- **Bug finder was a non-technical person with no IT security experience**
  - Posted finding to music forum, not Bugtraq!
- **In the URL?!? No über elite hacking tools needed!**
  - Mad IE skillz 😊
- **Sequentially issued order numbers!**
- **Bug was found a few days after the code was put into production!!!**
Side Note / Rant: Qualys Case Study for Tower Records

- Case study was online even AFTER the incident

Leading Online Retailer Ensures Customer Information Remains Confidential With Vulnerability Assessment

Tower Records makes it a top priority to protect the confidential information of customers who order music, videos, and DVDs from the company's Web site, www.towerrecords.com. After all, customer confidence is an essential ingredient for online sales leadership. "It's crucial to protect the privacy of our customers who order online, to keep their trust and keep them coming back," says Kevin Ertell, Director of Online Operations.
What was the root cause?

- **Tight deadline for new code vs. approaching holiday season**
  - *Internal emails hinted at this*
  - *Code review & testing was not evident; things over looked…*
    - Prior code did validate the “shopper number” with the “order number”; so an attacker would need both
    - New code only required “order number”
      - Sequential numeric string (“pick a card, ANY card”)
Tower Records Settles FTC Charges

- FTC press release dated April 21, 2004 reveals that Tower and FTC settle the charges.
  
  - "Tower Records Settles FTC Charges"
Settlement Details

- **Tower is prohibited from misrepresenting the extent to which it maintains and protects the privacy, confidentiality, or security of personal information collected from or about consumers.**
- **Tower must establish and maintain a comprehensive information security program.**
- **Security program must be certified as meeting or exceeding the standards in the consent order by an independent professional within six months, and every other year thereafter for a period of ten years.**
- **The settlement also contains record-keeping provisions to allow the FTC to monitor compliance.**
This note is directly from the FTC press release on April 21, 2004 at http://www.ftc.gov/opa/2004/04/towerrcords.htm

- "NOTE: A consent agreement is for settlement purposes only and does not constitute an admission of a law violation. When the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions. Each violation of such an order may result in a civil penalty of up to $11,000."

Copyright 2002-2005 Maven Security Consulting Inc. All rights reserved.
Tower Records: Lessons Learned

- **Network security scanners are not enough**
- “Independent” reviews help give fresh perspective and **CYA**
- **Train your developers about security issues**
- **Policies and procedures are needed**
Case Study #2

Purity Wholesale Grocer

Maven Security Consulting
The story you are about to hear is true. The names have NOT been changed.

- **It’s 2 AM on June 18, 1998. A modem begins to ring.** The caller authenticates and begins uploading a virus to the file server. The virus is strategically located so that it will spread to the desktop systems when company employees begin to login later that morning.

- **Soon, the call ends and the modem goes silent.** A few hundred miles away at another location for the same company another modem begins to ring, and the process repeats itself.
Case Study Agenda

- **The Trial**
  - Who, what, where, when, why

- **The Law:**
  - 18 USC 1030

- **Attack Details**

- **The Evidence**

- **Technical Observations**

- **The Defense Argument**

- **Misc. Evidence**

- **The Verdict & Beyond**

- **Lessons Learned & General Advice**

- **Conclusion**
The Trial

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
CASE NO. 00-434-CR-GOLD/SIMONTON

US vs. Herbert Pierre-Louis
News Headlines After Arrest

• “Internal net saboteurs being brought to justice”
  – By Sharon Gaudin
  – Network World, 08/27/01
The Attack – Key Facts

- **June 18, 1998 (2 AM EST)**
  - virus downloaded via dial-up
  - five sites called; three sites infected; only two get damaged
  - charged with two counts (18 USC 1030)

- **Inside job**
  - privileged account used for access
  - virus placed in specific location

- **Monkey Dropper virus**
  - would damage hard drive
The Attack – Effect

- **Computers activated by morning staff**
- **Virus triggered and damages two East coast locations**
- **East coast staff warned West coast staff**
  – damage is avoided at those sites
The Attack – Damages

➢ The Attack

The Motive

Introducing 18 USC 1030

Case Details

• **Two sites are down from virus**

• **Business is stopped at all locations until cause is determined**
  – fear of further data lose

• **Business is halted for 2 days**

• **Estimated over $75,000 in lost profits (based on daily yearly average)**
The Nature of the Victim Business

- **Victim – Purity Wholesale Grocer**
  - *middle-man broker between sellers (farmers) and buyers (grocery stores)*
  - *food is perishable; lost sales opportunities cannot be recovered*
  - *Buyers and sellers will find another broker*
The Motive

The Attack

- The Motive

Introducing 18 USC 1030

Case Details

- **IS group at Purity is in flux**
  - popular manager recently left
  - switching hardware platforms
  - small IS group merging with bigger group
  - rumors of layoffs

- **Suspect was given a written reprimand 10 days prior to attack**
Introducing the Law: 18 USC 1030

The Attack

The Motive

Introducing 18 USC 1030

Case Details

• **Computer Fraud and Abuse Act of 1986 (US)**
  18 U.S.C 1030
  – **U.S. Code – Title 18 – Section 1030**
  – **Fraud and related activity in connection with computers**
  – A federal crime to knowingly send a computer virus which causes at least $5000 in damage.
Case Details

The Attack

The Motive

Introducing 18 USC 1030

Case Details

- **2nd case in nation brought under 18 U.S.C 1030**

- **Victim offline from business for several days**

- **Losses estimated over $75,000 (including lost profits)**

Copyright 2002-2005 Maven Security Consulting Inc. All rights reserved.
Court Logistics

The Attack

The Motive

Introducing 18 USC 1030

➢ Case Details

- **Where**
  - *Southern District of Florida in Miami*

- **Judge**
  - *US District Judge Alan S. Gold*

- **When**
  - *Trial: Aug 28-30, and Sept 4-5, 2001*
Court Cases – Who’s Who

The Attack

The Motive

Introducing 18 USC 1030

Case Details

• **Prosecution**
  – United States Government
  – Assistant U.S. Attorneys Richard Boscovich and Kirk Ogrosky.
  – Expert witness: David Rhoades, Maven Security Consulting Inc.

• **Defense**
  – Defense attorney: Manuel Casabielle
  – Defendant: Herbert Pierre-Louis from Broward County FL
    • computer hardware technician for victim

• **Victim**
  – Purity Wholesale Grocers
  – Boca Raton-based company
  – $1.5 billion in annual sales
  – 6th largest privately held company in Florida.
Expert Witness Credentials

- Prosecution had a *plethora* expert witnesses
  - Phone company *(phone records)*
  - Anti-Virus *(the virus used)*
  - FBI *(work PC forensics)*
  - David Rhoades *(attack scripts; general dial-up security)*
- Defense relied on “trojan horse attack script” used to remote control the attack via defendant’s PC
- i.e. The Magic Bullet Theory
Credentials – David Rhoades (Why me?)

- **Information security & “hacking” subject matter expert**
  - speaker at international conferences
  - can explain security concepts to layman

- **Active consultant providing ethical hacking service**
  - requires creating “attack scripts”

- **Attack scripting knowledge was the key**
The Evidence
Target Machines – Procomm Servers

- **Procomm Servers**

- **Expert Witness Preparations**

- **Attack Details**

- **Call Log Evidence**

---

- **File server for local network**
  - *Custom software was essential for business on file servers*
    - C:\NEWPBS\NEWPBS.EXE
  - *A malicious payload there could potentially infect many desktops*
    - Desktops pull from file servers
  - *The server would not be infected, just clients*
    - The waiter with the poisoned bread
Procomm Features – User Accounts

- **Normal users**
  - upload to set location (*virus would have no impact*)
  - many people had normal access
  - open mode: anyone with phone number could create normal user

- **SYSOP users**
  - upload anywhere
  - only two SYSOP accounts
  - limited sharing of those accounts
Procomm Features – Last Caller

- **SYSOP user was needed to place virus effectively**

- **“Last Caller” screen on server**
  - Server console showed account name, date, and time of last user login.

- **Normal user calls early AM typical**
  - normal users had scripted their access for off hours

- **SYSOP calls early AM were not typical: might raise suspicions**

- **SYSOP attack would need a follow-up call with normal user to change “Last Caller” (hide attack)**
Expert Witness Preparations – What I did to prepare

• **Examined phone bill & Procomm logs**
• **Correlated phone bill entries with Procomm logs**
• **Duplicated the environment**
  – Got copy of exact Procomm version in use by victim
  – Used same OS as victim
  – Got Procomm startup config script used by victim
  – Tested various call scenarios to determine the resulting log entries
Attack Details

Five Purity Procomm servers were called early AM on June 18, 1998
- SLC (UT), Tacoma (WA), Hopkins (NY), Minneapolis (MN), & Buffalo (NY)
  - Two sites failed during the call – uploading files was not possible
    - SLC (UT) & Minn. (MN)
  - Three sites had virus uploaded
    - i.e. infected sites
  - Two sites damaged
The Main Evidence – Call Logs

- **Two sets of logs available**
  - One from each Procomm server
  - Defendant’s home phone bills
Each infected site (three) had two types of phone calls:

- **Primary calls**
  - SYSOP user accounts used
  - uploaded virus
  - shown on defendant’s home phone bill

- **Secondary calls**
  - IMMEDIATELY after each primary call
  - normal user accounts used
  - very brief call (login then logout)
  - purpose? “Last Caller” console
  - Not shown on defendant’s phone bill !?!
### 3 Tacama Washington Site (Items #4 and #6 from Defendant’s Phone Bill)

<table>
<thead>
<tr>
<th>Line #</th>
<th>DATE</th>
<th>TIME (PT)</th>
<th>TIME (ET)</th>
<th>ACTIVITY</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>06/17/98</td>
<td>9:24:53 PM</td>
<td>12:24:53 AM</td>
<td>IMPACT logged in.</td>
<td>Authorized vendor calls in</td>
</tr>
<tr>
<td>2</td>
<td>06/17/98</td>
<td>9:26:19 PM</td>
<td>12:26:19 AM</td>
<td>IMPACT uploaded C:\NEWPBS\DOWNLOAD\IMP.DAT successfully.</td>
<td>uploads data file into only directory allowed</td>
</tr>
<tr>
<td>3</td>
<td>06/17/98</td>
<td>11:38:41 AM</td>
<td>2:38:41 AM</td>
<td>IMPACT logged out.</td>
<td>session ends - session duration 0:01:41</td>
</tr>
<tr>
<td>4</td>
<td>06/17/98</td>
<td>12:34:41 AM</td>
<td>3:34:41 AM</td>
<td>HOST online.</td>
<td>time interval until next login 0:53:37</td>
</tr>
<tr>
<td>5</td>
<td>06/17/98</td>
<td>10:20:11 PM</td>
<td>1:20:11 AM</td>
<td>PURITY logged in.</td>
<td>SYSOP user logs in (call #4 from suspect's phone bill)</td>
</tr>
<tr>
<td>6</td>
<td>06/17/98</td>
<td>10:20:18 PM</td>
<td>1:20:18 AM</td>
<td>PURITY Changed directory to c:\newpbs.</td>
<td>changes to NEWPBS directory</td>
</tr>
<tr>
<td>7</td>
<td>06/17/98</td>
<td>10:21:05 PM</td>
<td>1:21:05 AM</td>
<td>PURITY uploaded c:\newpbs**\B000000000000000 successfully.</td>
<td>attempts to upload but fails due to unknown reason (could be line noise or misc. computer glitch)</td>
</tr>
<tr>
<td>8</td>
<td>06/17/98</td>
<td>10:21:16 PM</td>
<td>1:21:16 AM</td>
<td>PURITY logged out.</td>
<td>session ends – session duration 0:01:05</td>
</tr>
<tr>
<td>9</td>
<td>06/17/98</td>
<td>10:21:16 PM</td>
<td>1:21:16 AM</td>
<td>HOST online.</td>
<td>time interval until next login 0:01:26</td>
</tr>
<tr>
<td>10</td>
<td>06/17/98</td>
<td>10:22:42 PM</td>
<td>1:22:42 AM</td>
<td>QKING First logon - added to user file.</td>
<td>new account created (this is Secondary Call # B)</td>
</tr>
<tr>
<td>11</td>
<td>06/17/98</td>
<td>10:21:16 PM</td>
<td>1:21:16 AM</td>
<td>QKING logged in.</td>
<td>session ends – session duration 0:00:12</td>
</tr>
<tr>
<td>12</td>
<td>06/17/98</td>
<td>10:22:55 PM</td>
<td>1:22:55 AM</td>
<td>QKING logged out.</td>
<td>time interval until next login 0:07:27</td>
</tr>
<tr>
<td>13</td>
<td>06/17/98</td>
<td>1:30:21 PM</td>
<td>4:30:21 AM</td>
<td>SUPPORT logged in.</td>
<td>SYSOP user logs in (call #6 from suspect's phone bill)</td>
</tr>
<tr>
<td>14</td>
<td>06/17/98</td>
<td>1:30:27 PM</td>
<td>4:30:27 AM</td>
<td>SUPPORT Changed directory to c:\newpbs.</td>
<td>changes to NEWPBS directory</td>
</tr>
<tr>
<td>15</td>
<td>06/17/98</td>
<td>1:30:55 PM</td>
<td>4:30:55 AM</td>
<td>SUPPORT uploaded c\newpbs\NEWPBS. EXE successfully.</td>
<td>uploads file successfully</td>
</tr>
<tr>
<td>16</td>
<td>06/17/98</td>
<td>1:31:10 AM</td>
<td>4:31:10 AM</td>
<td>SUPPORT logged out.</td>
<td>session ends – session duration 0:00:49</td>
</tr>
<tr>
<td>17</td>
<td>06/17/98</td>
<td>1:31:10 AM</td>
<td>4:31:10 AM</td>
<td>HOST online.</td>
<td>time interval until next login 0:00:35</td>
</tr>
<tr>
<td>18</td>
<td>06/17/98</td>
<td>1:31:45 AM</td>
<td>4:31:45 AM</td>
<td>QK First logon - added to user file.</td>
<td>new account created (Secondary Call #D)</td>
</tr>
<tr>
<td>19</td>
<td>06/17/98</td>
<td>1:31:45 AM</td>
<td>4:31:45 AM</td>
<td>QK logged in.</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>06/17/98</td>
<td>1:31:50 AM</td>
<td>4:31:50 AM</td>
<td>QK logged out.</td>
<td>Session ends – session duration 0:00:05</td>
</tr>
</tbody>
</table>

Each attacked site had a one-two punch of Primary call (upload virus) IMMEDIATELY followed by Secondary call (to change last logon screen)
<table>
<thead>
<tr>
<th>Line #</th>
<th>DATE</th>
<th>TIME (CT)</th>
<th>TIME (ET)</th>
<th>ACTIVITY</th>
<th>Comments</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6/17/1998</td>
<td>7:39 PM</td>
<td>8:39:50 PM</td>
<td>HOST online.</td>
<td>last caller (vendor with normal activity) that day logged out - time interval until next call</td>
<td>4:54:20</td>
</tr>
<tr>
<td>2</td>
<td>6/18/1998</td>
<td>12:34 AM</td>
<td>1:34:10 AM</td>
<td>SUPPORT First logon - added to user file.</td>
<td>Attempt at SYSOP access fails because the SUPPORT user was not defined at this site prior to this call. Although the caller created an account called &quot;SUPPORT&quot; it would not have SYSOP privileges, and thus would not be able to upload the virus to the proper location. This is secondary call #E</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>6/18/1998</td>
<td>12:34 AM</td>
<td>1:34:10 AM</td>
<td>SUPPORT logged in.</td>
<td></td>
<td>0:00:18</td>
</tr>
<tr>
<td>4</td>
<td>6/18/1998</td>
<td>12:34 AM</td>
<td>1:34:28 AM</td>
<td>SUPPORT logged out.</td>
<td>session ends - session duration</td>
<td>0:00:38</td>
</tr>
<tr>
<td>5</td>
<td>6/18/1998</td>
<td>12:34 AM</td>
<td>1:34:28 AM</td>
<td>HOST online.</td>
<td>time interval until next login</td>
<td>0:00:09</td>
</tr>
<tr>
<td>6</td>
<td>6/18/1998</td>
<td>12:35 AM</td>
<td>1:35:06 AM</td>
<td>PURITY logged in.</td>
<td>SYSOP user logs in (call #6 from phone bill)</td>
<td>0:00:09</td>
</tr>
<tr>
<td>7</td>
<td>6/18/1998</td>
<td>12:35 AM</td>
<td>1:35:15 AM</td>
<td>PURITY Error changing to c:\newpbs !</td>
<td>requested directory does not exist - the error message shown to the user is not very obvious (see analysis below with table)</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>6/18/1998</td>
<td>12:35 AM</td>
<td>1:35:41 AM</td>
<td>PURITY uploaded c:\program files\procomm plus\aspect\HOST\NEWPBS.EXE successfully.</td>
<td>Without changing directories, any uploads by a SYSOP will (by Procomm's standard defaults) will be uploaded into the directory shown. In other words, the caller simply hit upload and did not have to specify a target directory.</td>
<td>0:00:26</td>
</tr>
<tr>
<td>9</td>
<td>6/18/1998</td>
<td>12:35 AM</td>
<td>1:35:58 AM</td>
<td>PURITY logged out.</td>
<td>session ends - session duration</td>
<td>0:00:52</td>
</tr>
<tr>
<td>10</td>
<td>6/18/1998</td>
<td>12:35 AM</td>
<td>1:35:58 AM</td>
<td>HOST online.</td>
<td>time interval until next login</td>
<td>0:01:13</td>
</tr>
<tr>
<td>11</td>
<td>6/18/1998</td>
<td>12:37 AM</td>
<td>1:37:11 AM</td>
<td>QK failed to enter name.</td>
<td>Secondary call #F (attempted) Cover-up/Follow-up call - QK account existed prior to login and this caller failed to enter the password 4 times and was automatically disconnected session ends -- session duration</td>
<td>0:00:02</td>
</tr>
<tr>
<td>Line #</td>
<td>DATE</td>
<td>TIME (CT)</td>
<td>TIME (ET)</td>
<td>ACTIVITY</td>
<td>Comments</td>
<td>Timing (HH:MM:SS)</td>
</tr>
<tr>
<td>-------</td>
<td>-----------</td>
<td>-------------------</td>
<td>------------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>12</td>
<td>6/18/1998</td>
<td>12:37 AM</td>
<td>1:37:13 AM</td>
<td>HOST online.</td>
<td>time interval until next login</td>
<td>0:00:42</td>
</tr>
<tr>
<td>14</td>
<td>6/18/1998</td>
<td>12:37 AM</td>
<td>1:37:55 AM</td>
<td>QKING logged in.</td>
<td>session ends - session duration</td>
<td>0:00:04</td>
</tr>
<tr>
<td>17</td>
<td>6/18/1998</td>
<td>3:13 AM</td>
<td>4:13:57 AM</td>
<td>JADE logged in.</td>
<td>vendor dials in and performs normal activity (not shown in this table for brevity)</td>
<td></td>
</tr>
</tbody>
</table>

### 5.1 Additional Details about Error Message

When a user fails to change (switch) upload directories, the error message returned is a single line of text that says, "Error change to c:\no-such-directory\!" This single line message is then followed by 10 lines of normal text that shows the command options available to the user, such as <U> for upload and <G> for Goodbye. The difference is very subtle, especially at 1:30 AM.

See the samples below.
Technical Observations – Complex Behavior

- Complex behavior
  - (Tacoma) error made by caller; virus upload not successful
  - (Hopkins) error from prev. site is repeated but then corrected during the call
  - (Tacoma) called 2nd time to fix the mistake made during 1st call
**Success message**

Current directory is c:\program files\procomm plus\aspect\HOST

Change to what directory? c:\newpbs

Changed directory to c:\newpbs.

<F>iles  <U>pload  <D>ownload

<H>elp  <T>ime  <C>hat

<R>ead mail  <L>eave mail  Fax  <B>ack

<G>oodbye

<S>witch directory

<A>bort (SHUT DOWN HOST)

Your Choice?

---

**Failure message**

Current directory is c:\program files\procomm plus\aspect\HOST

Change to what directory? c:\newpbs

Error changing to c:\newpbs!

<F>iles  <U>pload  <D>ownload

<H>elp  <T>ime  <C>hat

<R>ead mail  <L>eave mail  Fax  <B>ack

<G>oodbye

<S>witch directory

<A>bort (SHUT DOWN HOST)

Your Choice?
Phone Bill for Primary Calls (Rounds to Min)

Primary Call Timing from Suspect's Phone Bill

<table>
<thead>
<tr>
<th>Phone Bill Item #</th>
<th>Time (min)</th>
<th>Call Duration (min)</th>
<th>Interval Timing (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

Legend:
- Blue: Call Duration (min)
- Purple: Interval Timing (min)
Technical Observations

Phone Bill Missing Calls

Theories for Missing Phone Bills
Procomm Server Logs for Secondary Calls (Rounds to Sec)
Technical Observations – Non-Uniform Timing

- **Timing changes from call to call**
  - timing for routine tasks
    - login then change to proper upload directory
  - duration of primary calls
  - duration of secondary calls
  - duration between calls

Phone Bill Missing Calls

Theories for Missing Phone Bills
Technical Observations – Unpredictable Primary Call Length

- **Primary & Secondary calls were coordinated**
- **But duration of Primary calls had unknowns**
  - upload speed is variable; connection speed & line noise
- **How could they be remotely coordinated?**
Phone Bill Missing Calls

Technical Observations

- **Phone Bill Missing Calls**

Theories for Missing Phone Bills

- **There were 14 calls total according to Procomm logs**
  - Primary: upload of virus
  - Secondary: login then logout
- **Six of them were on defendant’s phone bill**
  - All Primary calls
  - All were 1 minute or longer
- **Secondary calls**
  - not billed
  - under 18 seconds
Theories for Missing Phone Bills

- **Why were “secondary” calls not on defendant’s phone bill?**
- **Theories**
  - *calling card or 10-10 #*
    - Counter argument: Why not all?
  - *too short to be billed*
    - Phone company billing expert testimony disproves this
- **One theory never tested**
  - flagged and billed later
  - *phone bills after the incident were not seized*
The Defense Argument – Attack Script

- Defense argued for attack script planted on home PC

- Defendant had Procomm w/ RapidRemote activated
  - accessed home PC from work for testing purposes
  - short cut on work PC for home PC access (user name and password)

- Anyone at work could have planted attack script
# The Defense Argument – Magic Script Theory Debunked

<table>
<thead>
<tr>
<th>Defense Assertion</th>
<th>Reality Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary calls were scripted (i.e. Attack Script)</td>
<td>Procomm actions can be scripted; but timing and behavior of calls were dynamic &amp; intelligent</td>
</tr>
<tr>
<td>Attack script was planted on defendant’s home PC</td>
<td>Co-workers did not recall every seeing shortcut for home PC at work.</td>
</tr>
<tr>
<td>Automatically trigger the night of the incident</td>
<td>OK</td>
</tr>
<tr>
<td>Real attacker made Secondary calls to ensure virus upload (Primary calls) were successful</td>
<td>Secondary call (Normal user) could not remotely determine success of Primary (SYSOP) call Calls were synchronized; non-predictable timing – margin for error small;</td>
</tr>
</tbody>
</table>
Evidence – Other Facts

The Defense Argument

- Evidence – Other Facts

The Verdict (Sept 2001)

- **FBI forensics on defendant’s work PC**

- **Defendant deleted 110 files days before the virus was uploaded.**
  - Preparing to leave job?

- **Anti-virus software on work PC detected the Monkey Dropper virus on floppy disks**
  - Twice: seven days before, and then two days before the attack.
Defendant Behavior (After the Attack)

- Defendant never returned to work after the attack
- First calling in with car problems
- Then calling in sick
- Finally, faxing in his resignation.

The Defense Argument

- Evidence – Other Facts

The Verdict (Sept 2001)
Defendant Behavior - Strange quote during FBI interview

The Defense Argument

Evidence – Other Facts

The Verdict (Sept 2001)

- Prior to his arrest the defendant was interviewed in his home by two FBI agents
- When presented with the phone bill & Procomm server logs which showed the virus was uploaded from his home phone line...
  - The FBI said “It looks like you did it”
  - The defendant agreed and said, “If I did it I guess I will have to pay the piper.”

Copyright 2002-2005 Maven Security Consulting Inc. All rights reserved.
The Verdict – Guilty (Sept 2001)

- **Trial lasted 6 days**

- **Jury took only 6 hours to deliberate**

- **Defendant is found guilty on both counts**
  - The two locations where virus was triggered and caused damages.
News Headlines After Guilty Verdict

- "Computer Saboteur Found Guilty"
  - Sharon Gaudin,
  - Network World, 09/07/01

- "Jury Convicts Herbert Pierre-Louis of Sending Computer Virus to Destroy Purity Wholesale Grocers Inc's Computer Systems"
The Reversal (March 2002)

http://pub.bna.com/eclr/00434.htm
Motion for Judgment of Acquittal

- **Defendant raises two issues:**

- 1) **Did damage really equal $5000?**

- 2) **Does “lost profits” based on a “daily average” calculation prove required amount ($5000) beyond a reasonable doubt?**
The Law Revisited – Damage?

- Define damage?
- "any impairment to the integrity or availability of data, a program, a system, or information that causes loss aggregating at least $5,000 in value during any one-year period to one or more individuals."
The Law Revisited – Loss?

• **What constitutes “loss”?**
  – *cost of repairs*…
    • travel, etc
    • hardware/software
    • staff salaries
    • lost profits due to down time?
  – *Profits? The key question.*
  – *Without considering lost profits, the $5000 min. could not be reached*
Ambiguity & Lenity

• **No definition of loss was provided by the statute at that time**

• **Meaning of loss was ambiguous**
  – absence of a clear and definite legislative directive

• **Rule of Lenity**
  – ambiguity be resolved in favor of defendant
Acquittal Granted

- Ambiguity of “loss” leads to rule of lenity
  - Loss cannot include “lost profits”

- Therefore, $5000 in damages cannot be shown
  - 1st issue raised in acquittal, 2nd issue may have also been successful

- Judgment of Acquittal is granted; charges dismissed
  - March 22, 2002
  - Alan S. Gold
  - US District Judge
News Headlines After Acquittal

- "Miami Judge Drops Hacker Conviction"
  - From: InfoSec News
  - Date: Wed Apr 03 2002

- "Computer saboteur escapes conviction"
  - By John Leyden
  - Posted: 03/04/2002

- "Judge says hacker's damage too trivial for federal crime"
  - By Steven Bonisteel, Newsbytes.
  - April 04, 2002
Lessons Learned & General Advice
Lessons Learned for Management

- **Have an incident response plan**
- **Learn who to contact in law enforcement**
  - Get to know your law enforcement contact
- **Reduce “disgruntle-inducing” environment**
- **Virus scanner on critical servers**
- **Record caller ID for dial-up access**
  - Because that can never be spoofed ;-) 
- **Centralized virus results for desktops**
- **Incident procedures should include contacting other locations ASAP**
  - East coast can warn the west coast (e.g. Don’t open email message called “I love you!”)
Lessons Learned for Prosecution

• *Get the “call records” from the phone company ASAP*

• *Grab phone bills at least one month prior and three months after date of incident*  
  – delayed billing

• *Confiscate the home PC*
Lessons Learned for Defense

• Line of questioning during the trial was not helpful to their case

• Several points worked against defense

• Detailed call records may have help them (maybe)
Conclusion
The Law Revised!

- **18 U.S.C. §1030 was revised on Oct 26, 2001**
  - Too late to apply to this case

- **“consequential damages”**
  - “loss” is to include “any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.”
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 8, 1998 (approx.)</td>
<td>Defendant reprimanded at work</td>
</tr>
<tr>
<td>June 18, 1998 (2 AM)</td>
<td>Viruses uploaded to work servers from defendant's home phone line</td>
</tr>
<tr>
<td>June 2000</td>
<td>Defendant arrested</td>
</tr>
<tr>
<td>August 2001</td>
<td>Trial (guilty verdict from jury for both counts)</td>
</tr>
<tr>
<td>October 26, 2001</td>
<td>18 USC 1030 is revised to include lost profits as damage</td>
</tr>
<tr>
<td>March 22, 2002</td>
<td>Acquittal granted / charges dismissed</td>
</tr>
<tr>
<td>November 26, 2002</td>
<td>Appeal by prosecution fails</td>
</tr>
</tbody>
</table>
References & Resources

• **Order Granting Judgment of Acquittal**

• **18 U.S.C 1030**

• **Find Law Web Site**
Questions? – Author Contact Info

• **Thank you**
• **Fill out session evals**

• **Download these slides from**

• **Author’s contact info:**
  – David Rhoades
  – david.rhoades@mavensecurity.com

• **Security assessments, training, etc…**
  – Web app security assessments since 1996
  – VoIP security design & audit
Thank You

Honor + Knowledge = Security

Slides online at www.MavenSecurity.com under Resources

auditing web apps since 1996