Protecting Confidential Data on Personal Computers with Storage Capsules

Kevin Borders, Eric Vander Weele, Billy Lau, and Atul Prakash
Problem: Malicious Software

- Computing becomes pervasive, so is malware
  - Over 23 million computers cleansed in 2008 [1]

- Consequences are severe:
  - Financial loss
  - Identity theft
  - Fraud

Scenario

- Tasks that require confidentiality protection
  - Perform financial analysis of credit card expenditure
  - Writing journal containing controversial political beliefs
  - Writing business proposal
<table>
<thead>
<tr>
<th>Account Number</th>
<th>Login Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234-5678-9012-3456</td>
<td>KBorders01</td>
<td>secret</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/6/2009</td>
<td>CLICK-TO-PAY PAYMENT, THANK YOU</td>
</tr>
<tr>
<td>4/9/2009</td>
<td>$0.00 LATE PAYMENT - FEE NOT CHARGED</td>
</tr>
<tr>
<td>3/12/2009</td>
<td>$208.56 DTE ENERGY PAYMENT DETROIT MI</td>
</tr>
<tr>
<td>3/14/2009</td>
<td>$25.62 SPEEDWAY 05399 583 MICHIGAN CITY IN</td>
</tr>
<tr>
<td>3/14/2009</td>
<td>$25.74 CAFE BA-BA REEBA CHICAGO IL</td>
</tr>
<tr>
<td>3/15/2009</td>
<td>$43.63 VZWRLLS*APOCC VISN 800-922-0204 CA</td>
</tr>
<tr>
<td>3/17/2009</td>
<td>$21.54 JEWEL-OSCO 3443 CHICAGO IL</td>
</tr>
<tr>
<td>3/19/2009</td>
<td>$17.15 SPEEDWAY 07786 855 PAW PAW MI</td>
</tr>
<tr>
<td>3/22/2009</td>
<td>$18.73 KROGER #689 YPSILANTI MI</td>
</tr>
<tr>
<td>3/22/2009</td>
<td>$140.69 SAMS CLUB YPSILANTI MI</td>
</tr>
<tr>
<td>3/24/2009</td>
<td>$26.93 YPSILANTI FUEL STOP Q17 YPSILANTI MI</td>
</tr>
<tr>
<td>3/26/2009</td>
<td>$11.26 KROGER #605 ANN ARBOR MI</td>
</tr>
<tr>
<td>4/4/2009</td>
<td>$28.39 KROGER #689 YPSILANTI MI</td>
</tr>
<tr>
<td>4/5/2009</td>
<td>$27.11 MEIJER INC#227 Q01 WHITE LAKE MI</td>
</tr>
</tbody>
</table>
IS THIS SAFE ENOUGH?
Goals

Provide confidentiality for local sensitive files against malicious software
Related Work: Trusted Boot

- Not 100% safe
- Need to verify all software prior to installation
  - Hard
- Verify documents
  - Even harder!!
Related Work: Strict Inter-Process Flow Control

- Mandatory Access Control with strict control flow policy = Limited Usability
- Air gap greatly limits utility
Contribution - Storage Capsules

- A system that can securely access confidential information from a compromised commodity OS
Approach

- Allow normal OS and standard applications to access sensitive data
- Two modes of operation:

<table>
<thead>
<tr>
<th>Normal Mode</th>
<th>Secure Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>• No restrictions</td>
<td>• Prevent network output</td>
</tr>
<tr>
<td>• Perform non-sensitive operations</td>
<td>• Edit sensitive documents</td>
</tr>
<tr>
<td>• No storage protection</td>
<td>• Encrypt changes to Storage Capsules</td>
</tr>
</tbody>
</table>
From the User’s Perspective

1. Open Container
2. Edit Document
3. Close Container

Similar to TrueCrypt, but contents safe when open
Capsule Architecture

- **Capsule VM**
  - **Capsule Server**
  - **Standard OS**
  - **Virtual Drivers**

- **Primary VM**
  - **Capsule Viewer**
  - **Standard Programs**
  - **Primary OS**
  - **Virtual Drivers**

- **Capsule VMM Module**
  - **VMM OS**
  - **Physical Device Drivers**

- **VMM**
  - **Hardware**

- **Green** = Trusted Computing Base
- **Red** = Not Trusted
Threat Model

- **We trust:**
  - The user,
  - The capsule VM, and
  - The VMM

- **Do not trust:**
  - The primary OS
  - Applications

- **Covert Channels**
  - Channels within the primary VM are blocked
  - Channels in Capsule VM, VMM, and hardware may not be blocked
Opening a Storage Capsule

1. Open Store

2. Open Store

Viewer

Server

VMM Module
Opening a Storage Capsule

1. Open Store

2. Open Store

3. Escape

3b. Warning!

Viewer → Server → VMM Module
Opening a Storage Capsule

1. Open Store
2. Open Store
3. Escape
4. Disable Output/Save Snapshot
3b. Warning!
Opening a Storage Capsule

1. Open Store
2. Open Store
3. Escape
4. Disable Output/Save Snapshot
5. Enter Decryption Password

3b. Warning!
Accessing a Storage Capsule
Closing a Storage Capsule

1. Close Store Escape Sequence
Closing a Storage Capsule

1. Close Store Escape Sequence

2. Revert Snapshot/Enable Output
Covert Channels Illustrated
Attacks - Covert Channels

• Primary OS and Capsule could be manipulated, but we:
  ▫ Fix the file store size
  ▫ Re-encrypt the store before every export
  ▫ The user controls transition timing with a secure key escape sequence

• External Devices – store data on floppy, CD-ROM, USB, SCSI, etc.
  ▫ Device output is disabled in secure mode
Attacks - Covert Channels (pt. 2)

- **VMM** – manipulate memory utilization and layout, store information in virtual network
  - VMM does not over-commit memory and uses fixed layout
  - Restart the virtual network during transition to normal mode
- **Hardware** – store data in CPU or disk cache
  - Restoration code adds noise to CPU, full reset would completely clear CPU
  - Would need to clear all disk caches or move all files to block disk covert channels
Attacks - Secure Mode Forgery

- Malware could fake secure mode UI
- To be safe, users are only required to:
  - Remember that they are supposed to enter a key escape sequence (like ctrl+alt+del) to enter secure mode
  - Heed warnings
Performance - Transitions

To Secure Mode

To Normal Mode
Disk Performance - Secure Mode

- For Apache build:
  - Storage Capsules 38% slower than native system
  - Only 5.1% slower than running TrueCrypt in VM
Limitations

• Changes made outside Capsules in secure mode are lost
  ▫ Background computations
• Network connections are lost in secure mode
  ▫ Downloads, services, etc.
• Short-lived sessions are impractical due to transition time
Conclusion

• Introduced Storage Capsules, a new mechanism for securing files on personal computers
  ▫ Similar to existing file encryption software
  ▫ Provide better protection and usability
  ▫ Works in the face of a compromised OS

• Covert channel analysis
  ▫ Explores covert channels on many layers
Questions