Hard Disk Guard Based Policy Enforcement

Mark Beaumont
(Bradley Hopkins, Chris North & Ken Yiu)
Defence Science and Technology Organisation (DSTO)
Edinburgh, South Australia, Australia

Mark.Beaumont@dsto.defence.gov.au

IEEE International Symposium on Policies for Distributed Systems and Networks
6-8 June 2011, Pisa, Italy
Overview

- Threat
- Solution
- Prototype Operation
- Policy Applications
The Threat

- Information System policy enforcement
  - Software
    - Access control - files system permissions
    - Networking - authentication protocols,
  - Hardware
    - Processor modes, MMU
- Do you trust your software?...hardware?...policy?
- Threats
  - Malicious software
  - Hardware Trojans
The Hard Disk Guard Prototype

- Policy enforcement:
  - Independent, trusted hardware
- Information Policies:
  - Stored Data – access, confidentiality
  - Data Content – blacklists, virus checking
The Hard Disk Guard (HDG)
The Hard Disk Guard (HDG)

1. Modify Read Data
The Hard Disk Guard (HDG)

1. Modify Read Data

2. Create Read Data
The Hard Disk Guard (HDG)

1. Modify Read Data
2. Create Read Data
3. Redirect Read
The Hard Disk Guard (HDG)

1. Modify Read Data

2. Create Read Data

3. Redirect Read

4. HDG Read Data
Remote Management:
- In-band over ATA bus
- Update policies and configuration
- Can be secured
Administration

Web Page cached to hard disk

HDG

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

...<h2>HDG Configuration</h2>

<p>update:p1: {"SIMPLE POLICY UPDATE"}</p>
<p>update:p2: {"SIMPLE POLICY UPDATE NO. 2"}</p>
<p>update:c1: {"CONFIGURATION COMMAND"}</p>
<p>update:c2: {"CONFIGURATION COMMAND"}</p>

<h2>END HDG Configuration</h2>

...
HDG in Action

Linux OS only sees 120GB WD hard disk
active:1
disk:WD1200JB

500GB PATA Hard disk

120GB virtual disk {personal, untrusted}

320GB virtual disk {enterprise, SOE}
Linux OS only sees 120GB WD hard disk

active:1
disk:WD1200JB

# echo "switch domain" > temp

active:1
disk:WD1200JB

500GB PATA Hard disk

120GB virtual disk {personal, untrusted}

320GB virtual disk {enterprise, SOE}

unused
UNCLASSIFIED

HDG in Action

Linux OS only sees 120GB WD hard disk

HDG
active:1
disk:WD1200JB

500GB PATA Hard disk
120GB virtual disk {personal, untrusted}
320GB virtual disk {enterprise, SOE}

# echo "switch domain" > temp

HDG
active:1
disk:WD1200JB

unused

Reboot PC

Windows OS only sees 320GB WD hard disk

HDG
{add offset}
active:2
disk:WD3200BEVE

unused
Distributed Policy Enforcement

Distribute Policies:
- software patches
- access control
- storage quotas
Example Policy Enforcement
Example Policy Enforcement

HDG

System Policy
master:ro
temp:rw

Dirty Sector Table
{826190 → 23639810,
629766 → 23491863,
329651 → 22900172,
...}

320GB Hard disk

Master Image

Temporary Storage

OS sees 120GB hard disk
Conclusions

- Cannot trust commodity software or hardware.
- Simple retrofittable components
- Trusted computing elements required
- Ongoing research into using COTS hardware without requisite trust.
Questions?