Australian Government
Department of Defence
Defence Science and
Technology Organisation

Hard Disk Guard Based Policy Enforcement

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

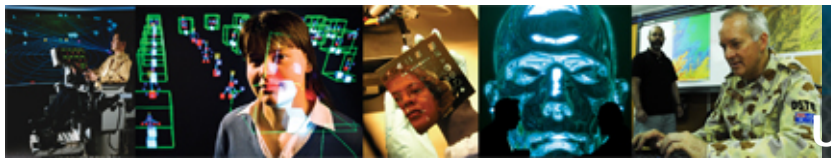
Mark.Beaumont@dsto.defence.gov.au

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

DSTO

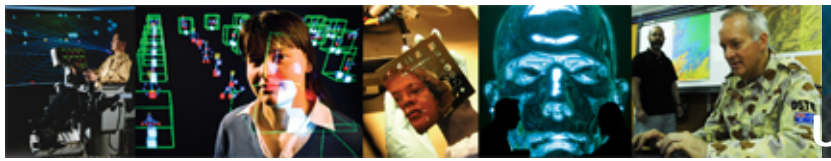
Overview

- Threat
- Solution
- Prototype Operation
- Policy Applications

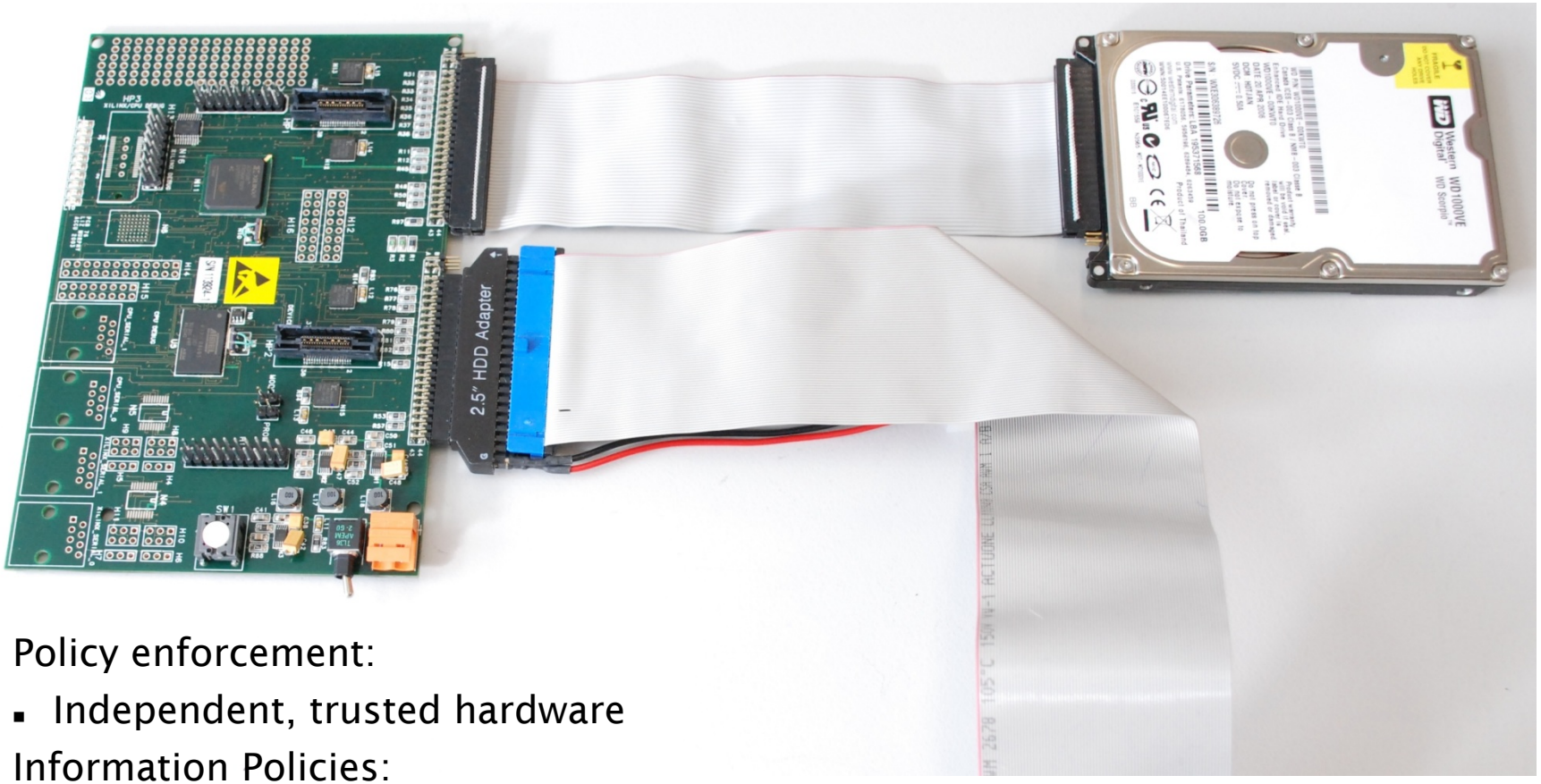


The Threat

- 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

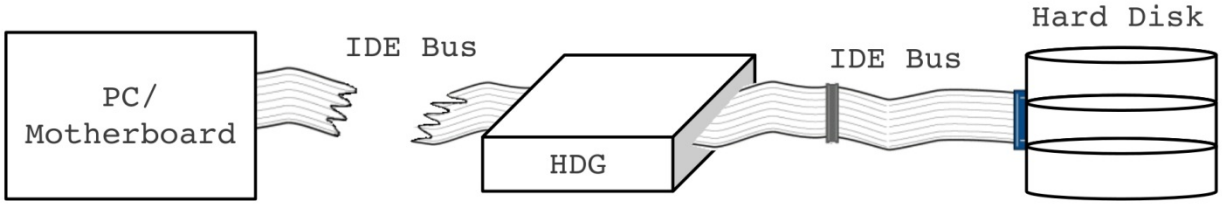


The Hard Disk Guard Prototype

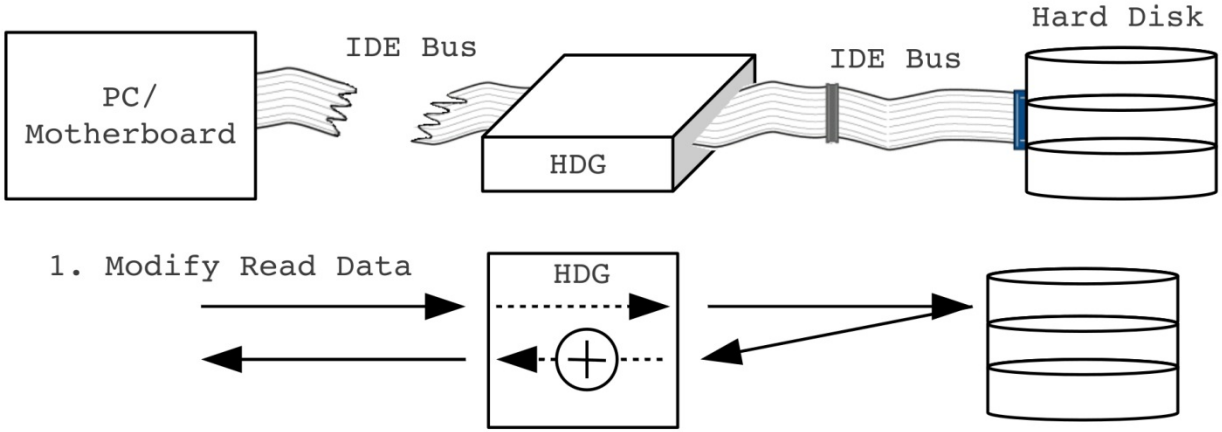


- Policy enforcement:
  - Independent, trusted hardware
- Information Policies:
  - Stored Data – access, confidentiality
  - Data Content – blacklists, virus checking

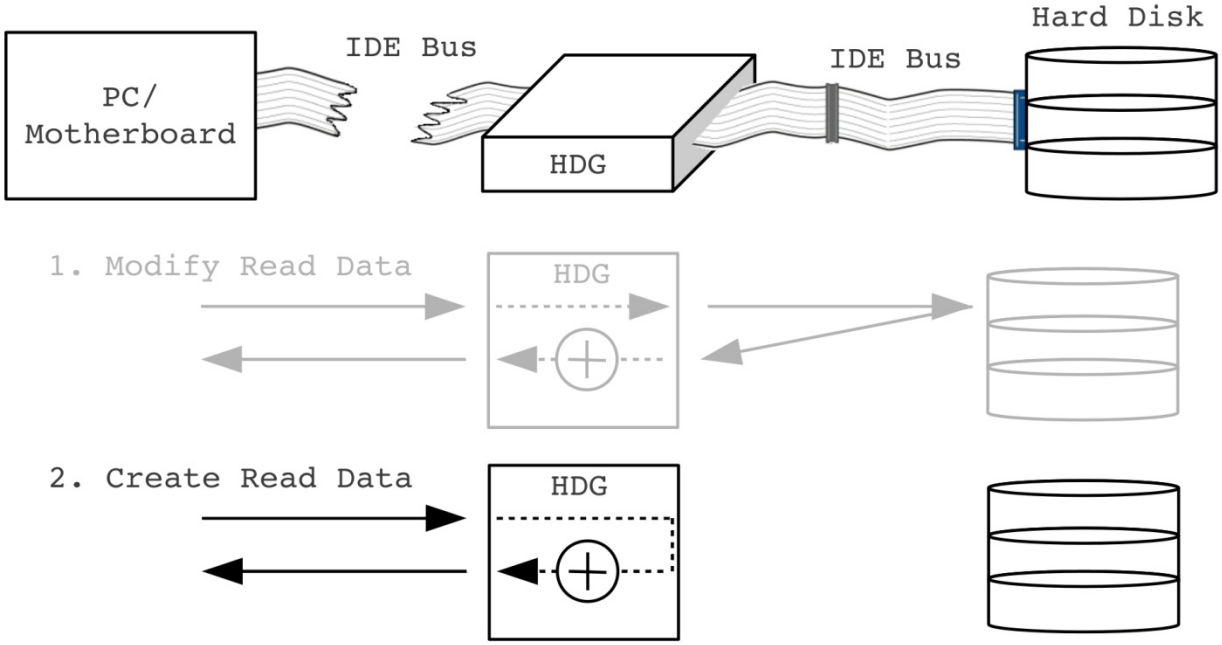
The Hard Disk Guard (HDG)



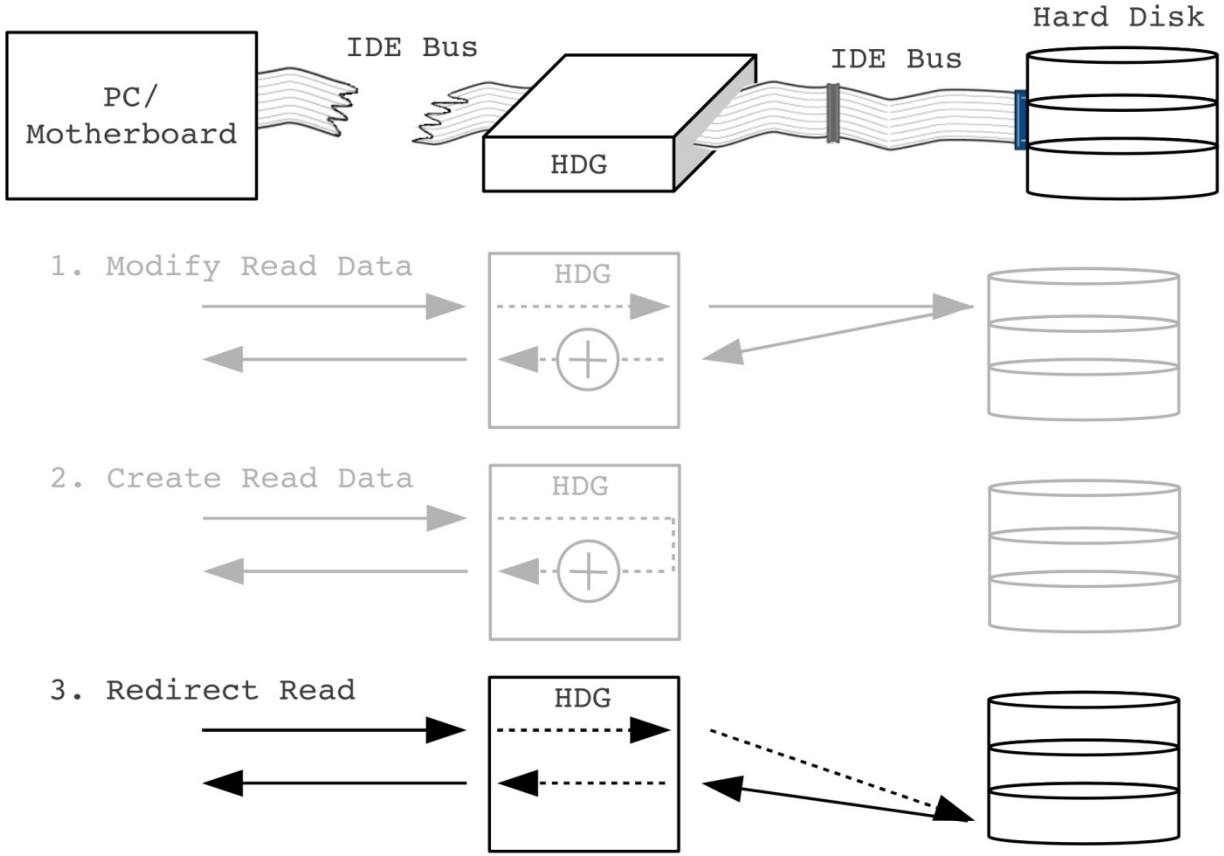
The Hard Disk Guard (HDG)

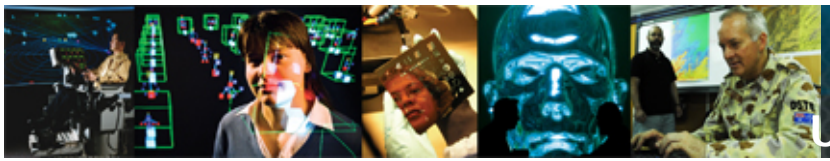


The Hard Disk Guard (HDG)



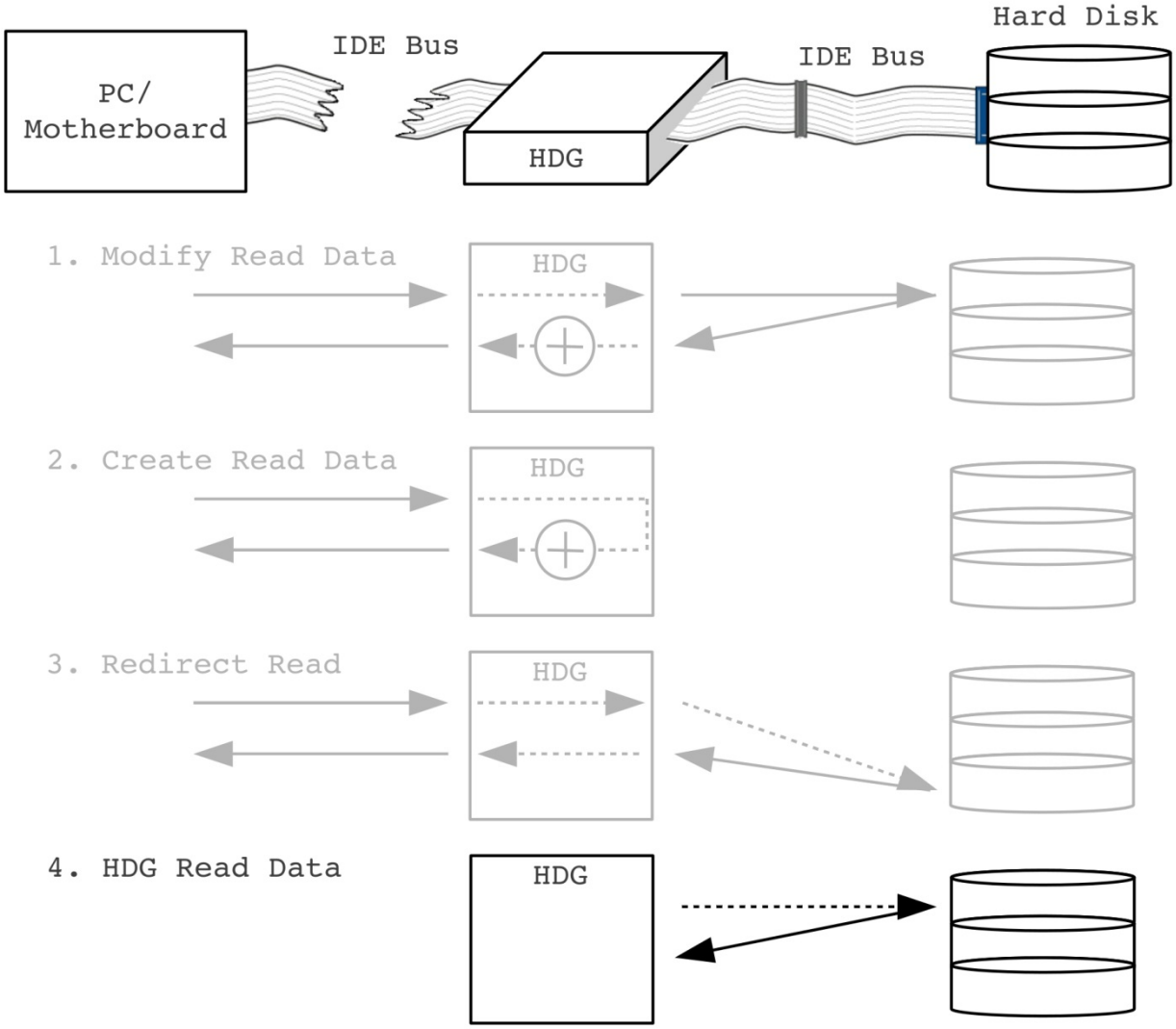
The Hard Disk Guard (HDG)



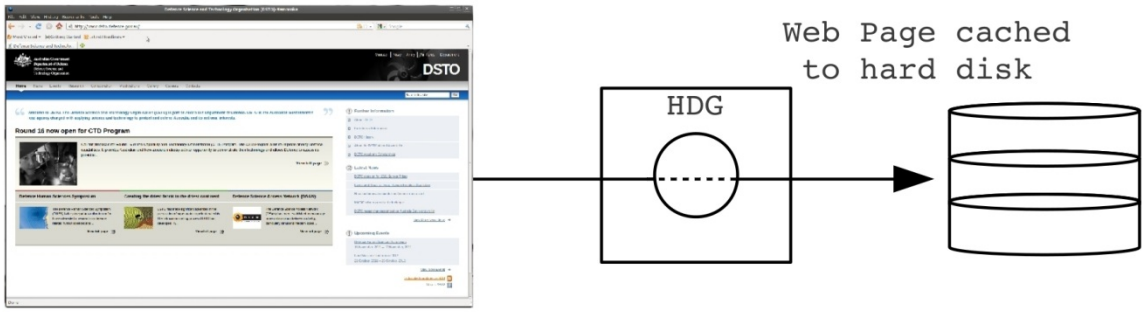


DSTO

The Hard Disk Guard (HDG)

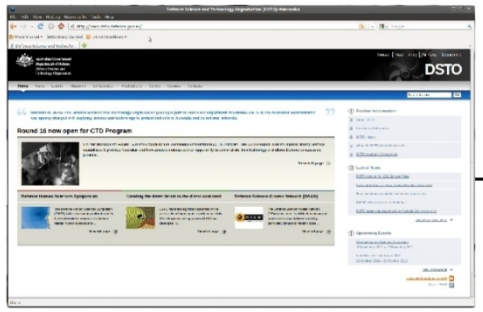


Administration



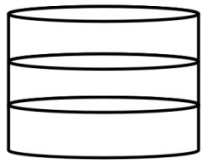
- Remote Management:
  - In-band over ATA bus
  - Update policies and configuration
  - Can be secured

Administration



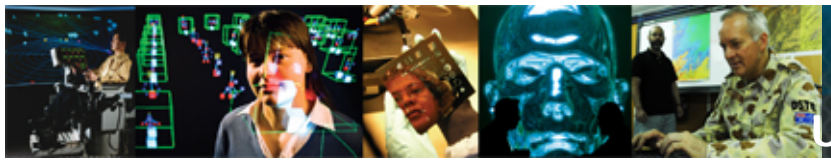
Web Page cached to hard disk

HDG

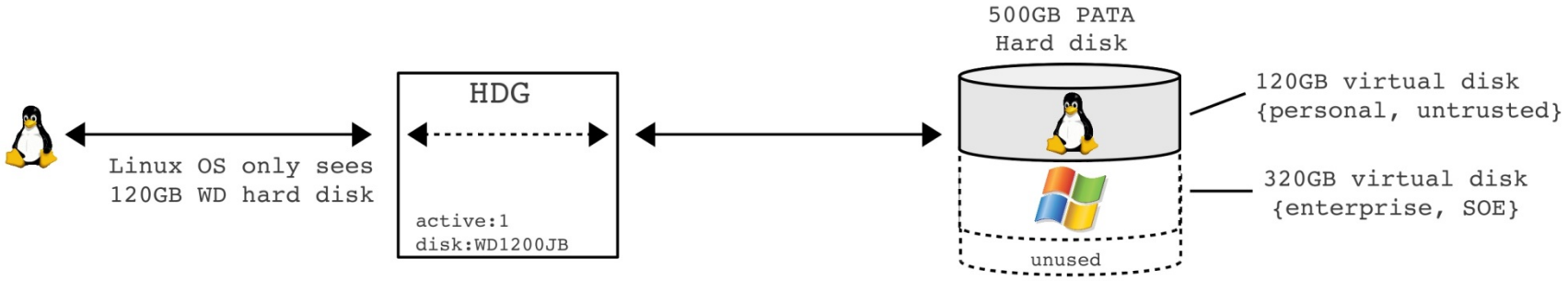


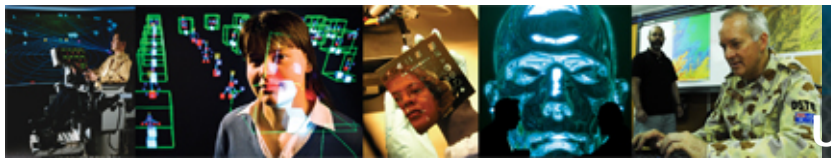
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Stric
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd

...

<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 POLICY & CONFIGURATION



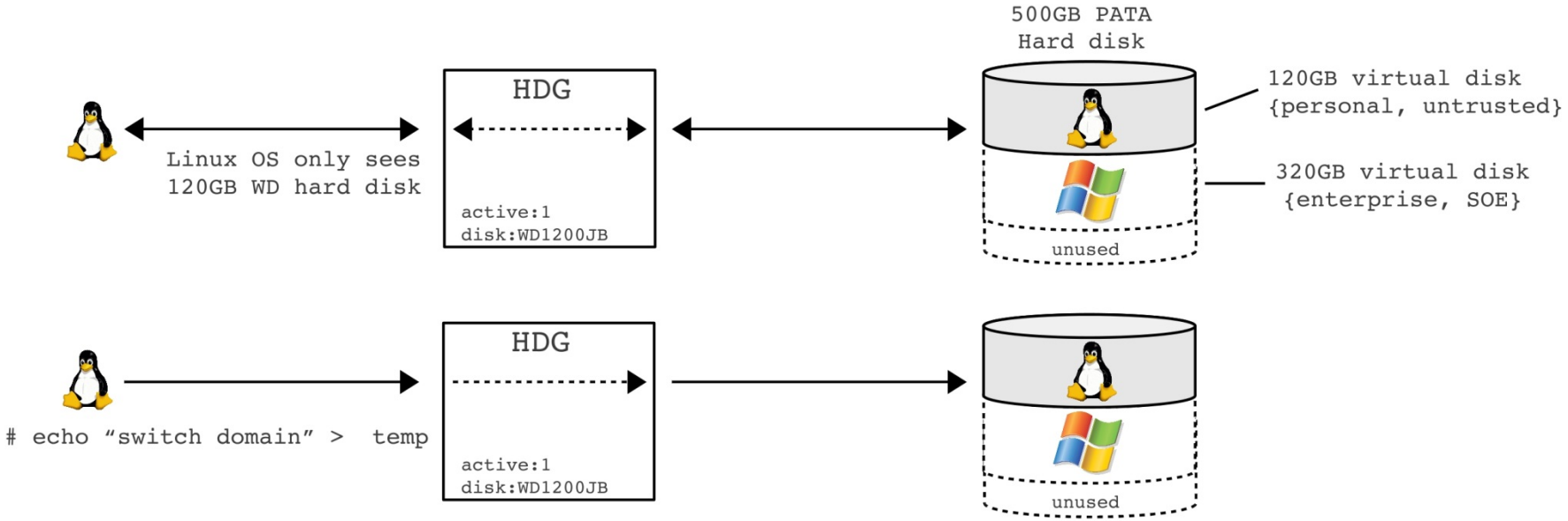
HDG in Action



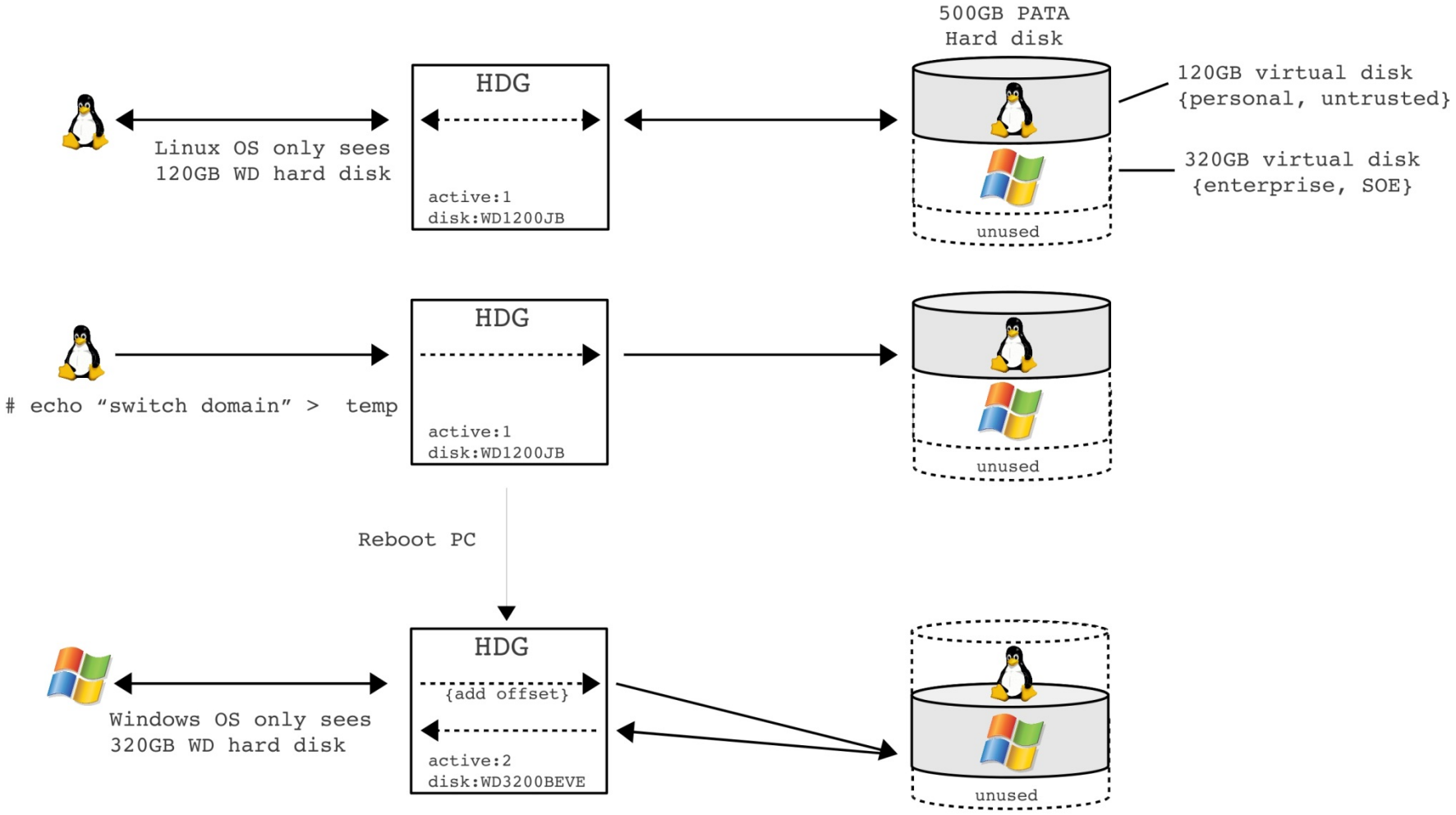


DSTO

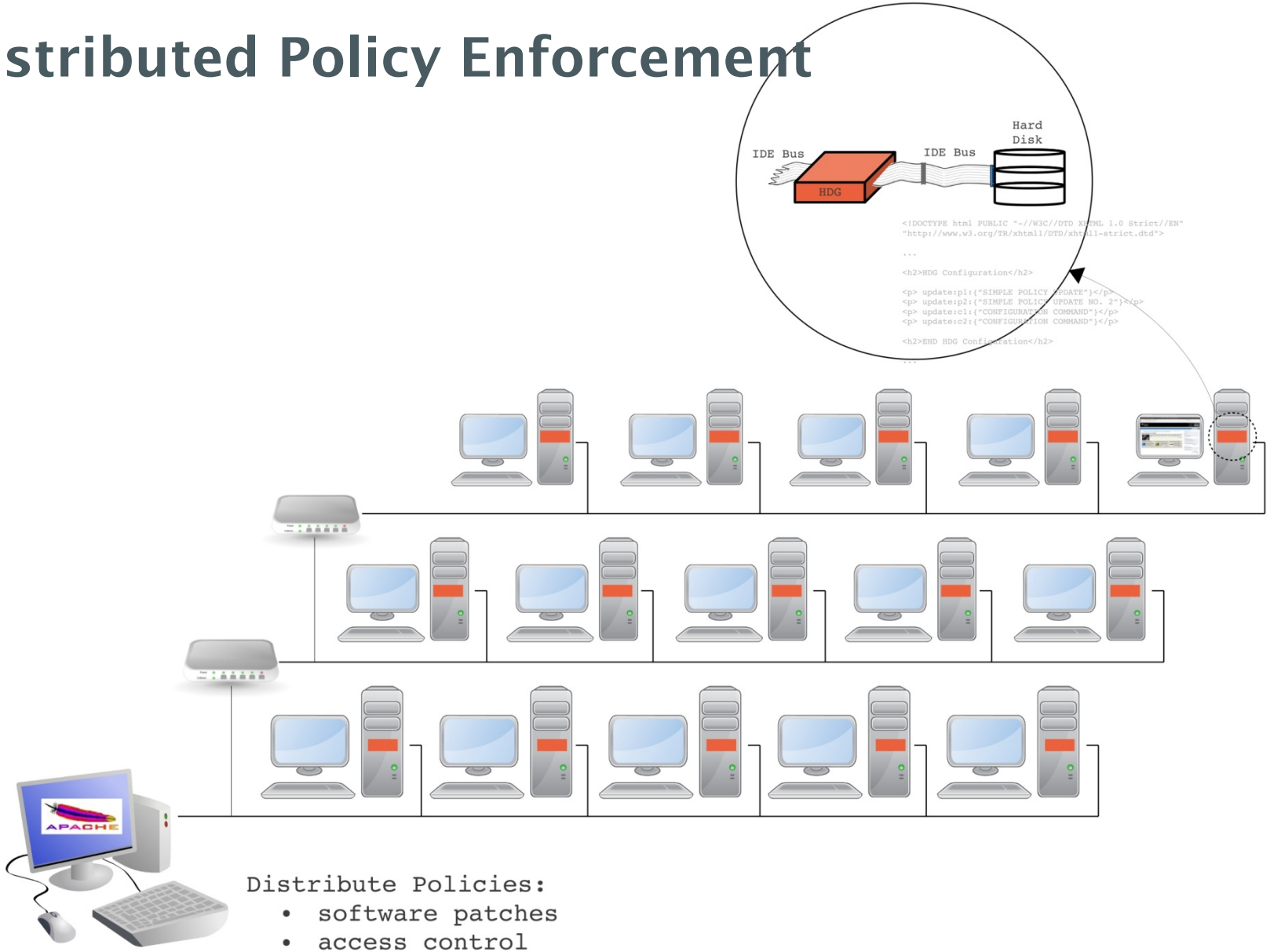
HDG in Action



HDG in Action



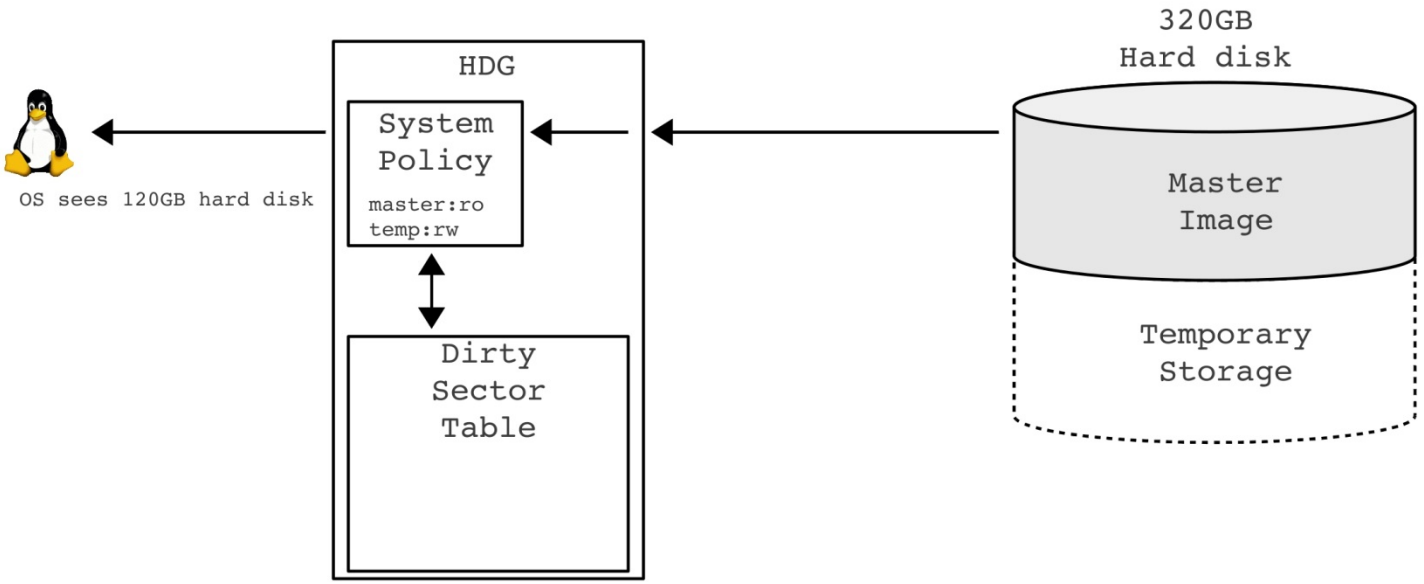
Distributed Policy Enforcement



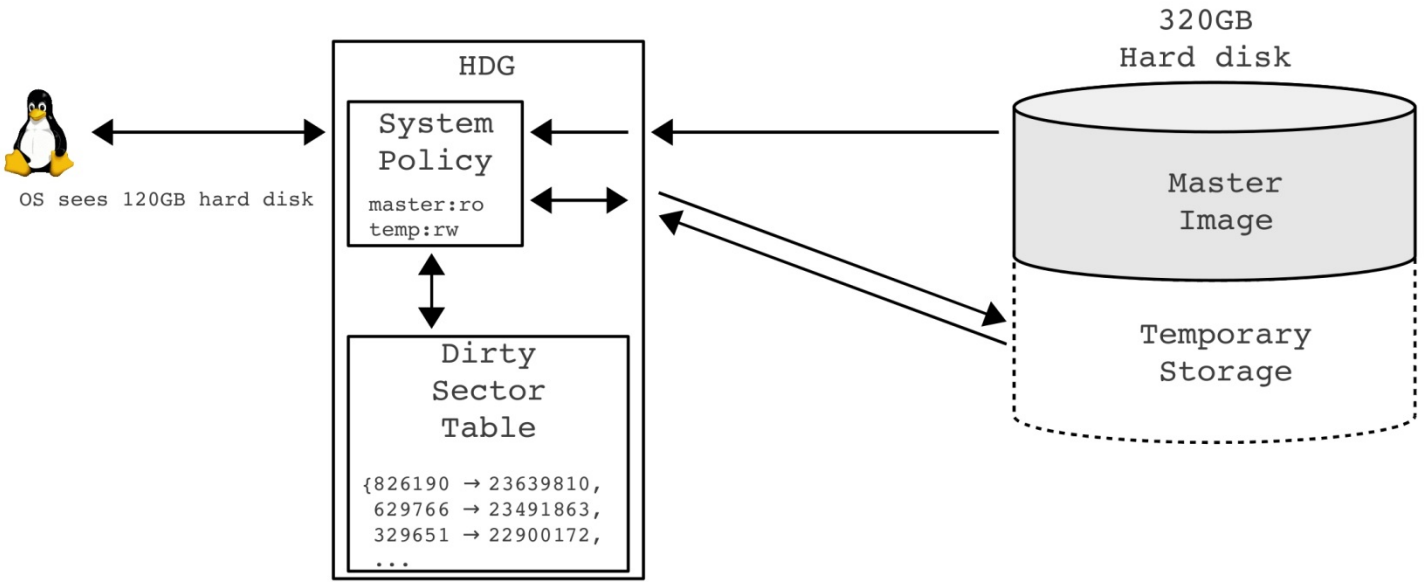
Distribute Policies:

- software patches
- access control
- storage quotas

Example Policy Enforcement

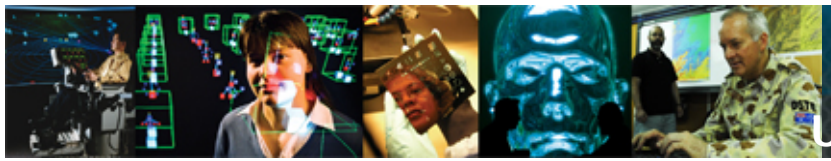
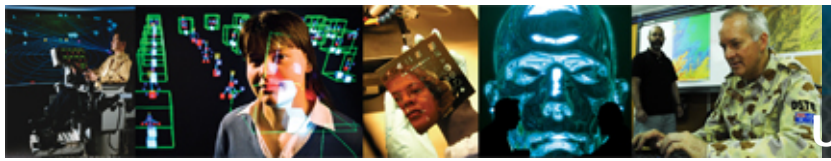


Example Policy Enforcement



Conclusions

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



Questions?