Australian Government
Department of Defence
Defence Science and Technology Group

Redirecting DRAM Memory Pages: Examining the Threat of System Memory Hardware Trojans

Bradley Hopkins
John Shield
Chris North

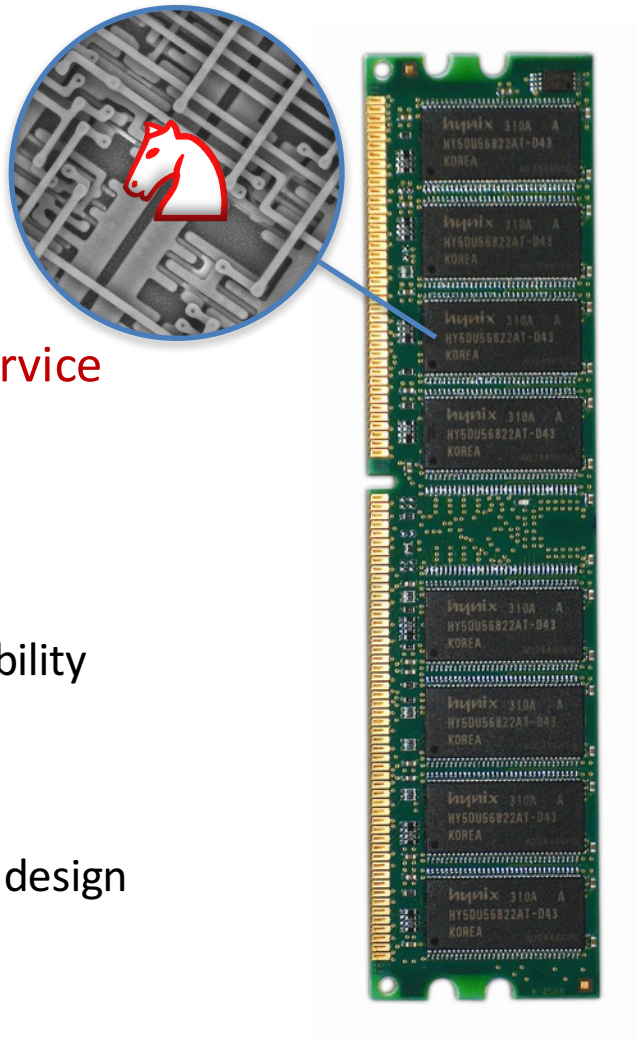
IEEE Hardware-Oriented Security and Trust (HOST)

DST Group - Trustworthy Systems Research

- **Organisation:**
  - Defence Science Technology Group (Australian Department of Defence)
- **Trustworthy Systems Research Group:**
  - Future Threat Estimation- Forecasting and prototyping advanced threats
  - Resilient ICT for security-critical high-assurance systems

Threat Forecasting

- Silicon Trojans
  - Within Integrated Circuits
  - Hard to verify post-production
- Threat
  - Leak or Modify Information, Degrade service
  - Hardware correctness assumptions
- Concern
  - Supply chain vulnerability
  - Data Confidentiality and Infrastructure Reliability
- Australia's Limitations
  - Overseas procurement
  - No significant national ITC manufacturing or design
- Informs to shape policy

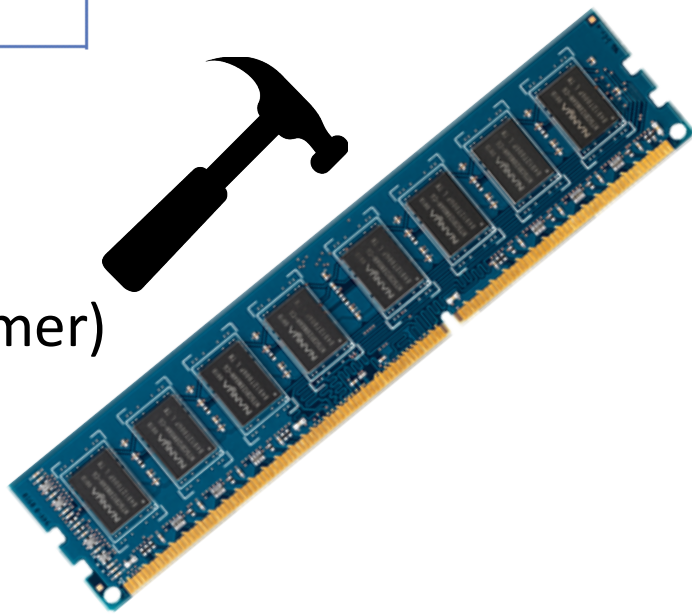


The Hardware Trojan Threat

- Hardware Trojan Characteristics

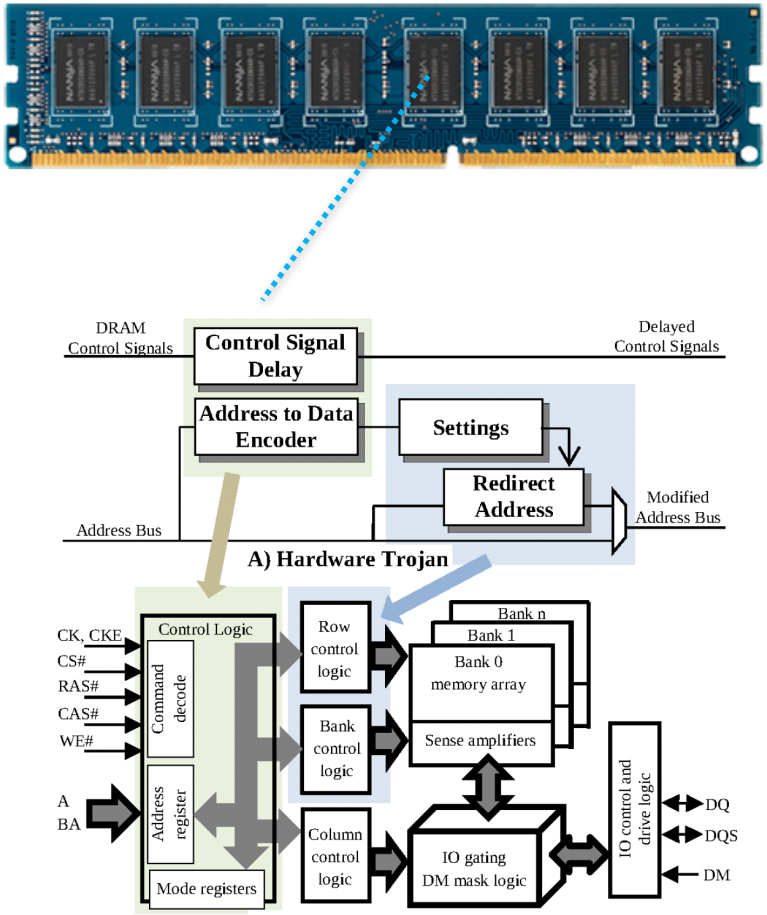
Insertion	Size
Design Phase Chip Fabrication Electronic Assembly Supply Chain	Zero Size Small Medium Large
Trigger	**Effect**
Always On Time Data Signature External Signal	Kill Switch Degradation of Service Logic Attack Leak Sensitive Information

- DRAM Memory Trojan
  - Is this really a problem?
  - DRAM disturbance errors (Row Hammer)



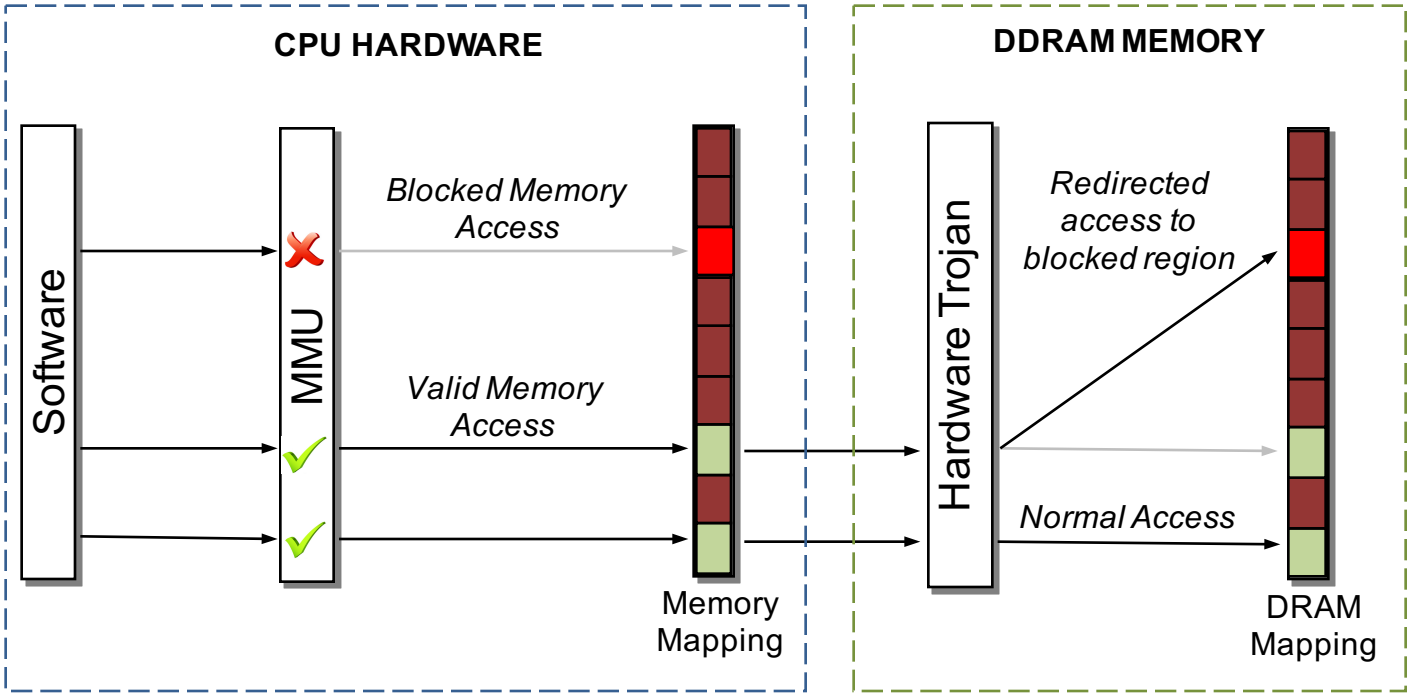
Case Study – Address Redirection Memory Trojan

- Small size
  - simple primitives that can be leveraged by an unprivileged software agent using standard memory transactions
- Maps to the technology
  - Operates in a standard system
  - No hardware or operating system changes
  - ECC/scrambling remains active
- Can be leveraged by unprivileged cooperative software for privilege elevation



Effect

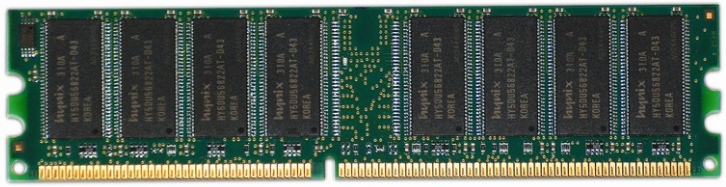
- Memory Protection is Key to Software Security
  - Privilege Levels and Data Isolation



DRAM Memory Trojan – Address Redirection

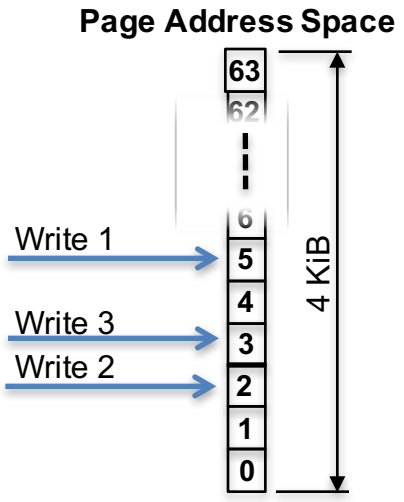
- Hardware Redirection
  - Modify Row Addresses
  - Receive Address Bus Signalling
  - Keep track of 3 addresses
    - Target Address
    - Redirect Address
    - Control Region Address

- Software Agent
  - Command and Control
    - Broadcast Control Signals
    - Page Handling
    - Coordinates between DRAM ICs
  - User Interface
    - Data Analytics
    - Data Modification



DRAM Memory Trojan Command Channel

- Address Bus Decoding
  - No data line access
- Encoding Scheme
  - Page Address in 64 parts
  - Sequential WRITES using the Non-Temporal SSE instructions
  - Encoded value ends on ROW change or READ



Address to Data Encoding

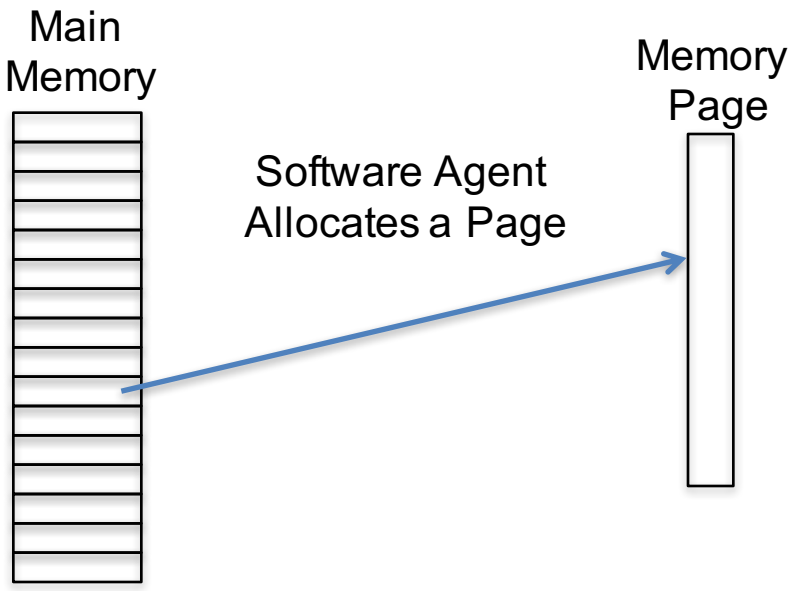
Write	Encoded Value
1	0x0000000000000020
2	0x0000000000000024
3	0x000000000000002A

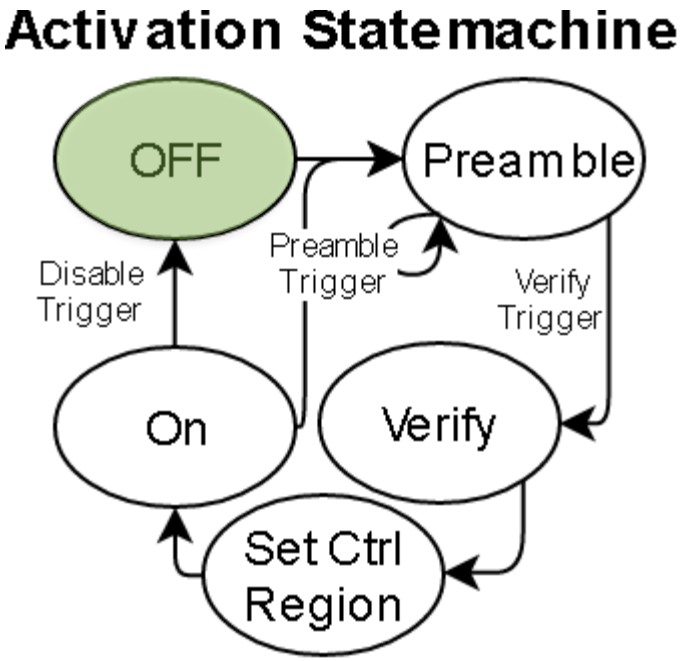
DRAM Memory Trojan - Operation

- Software agent performs command and control
- 3 Main Steps
  - 1) Activation Sequence
  - 2) Page Discovery
  - 3) Redirection

Operation – Activation Sequence (0)

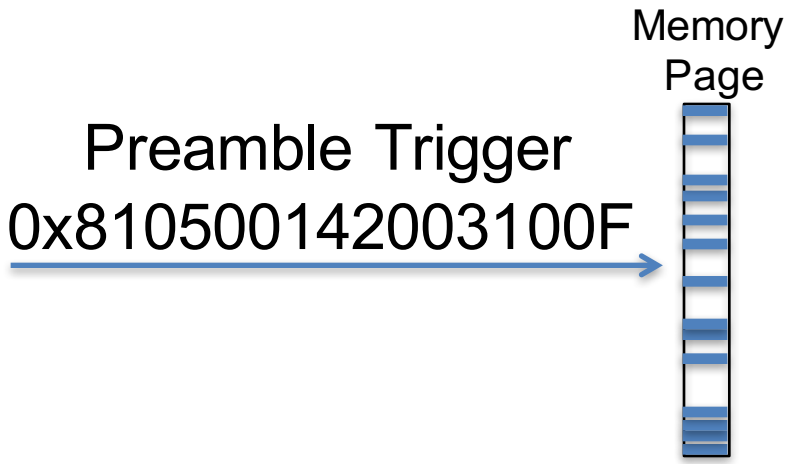
- Set up any memory page

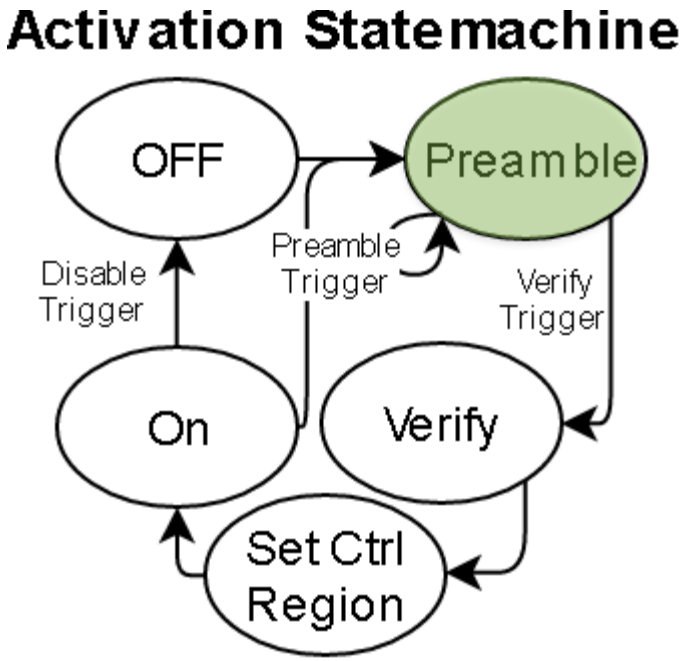




Operation – Activation Sequence (1)

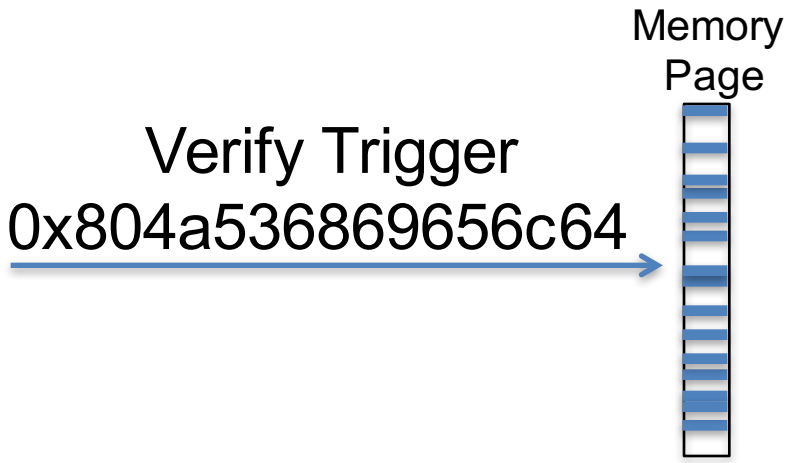
- Address Bus Encoded
- 2 Unique Words of 64 bits

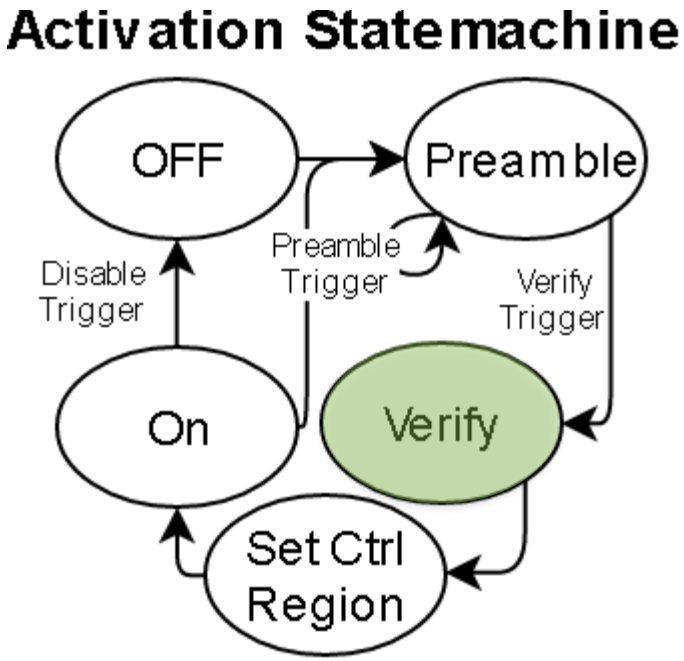




Operation – Activation Sequence (3)

- Address Bus Encoded
- 2 Unique Words of 64 bits

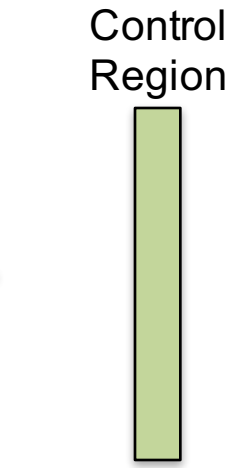


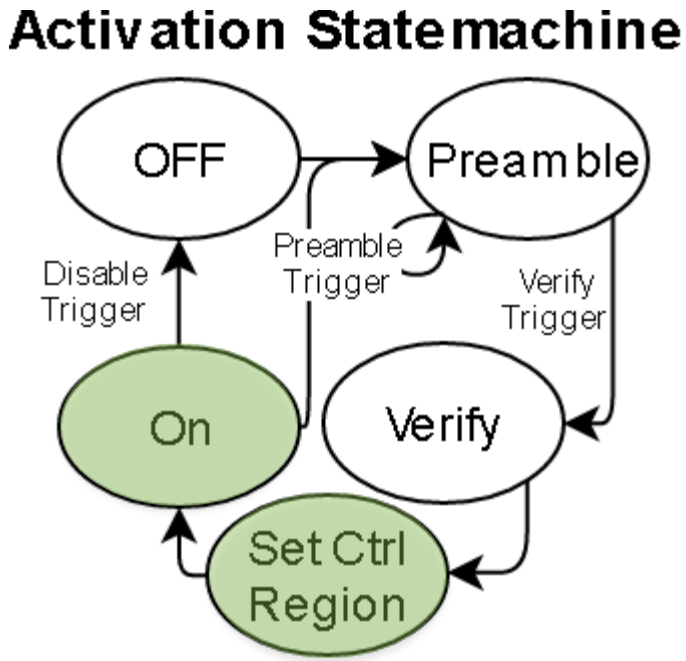


Operation – Activation Sequence (4)

- Memory Page becomes Control Region
  - Settings written with address bus encoding

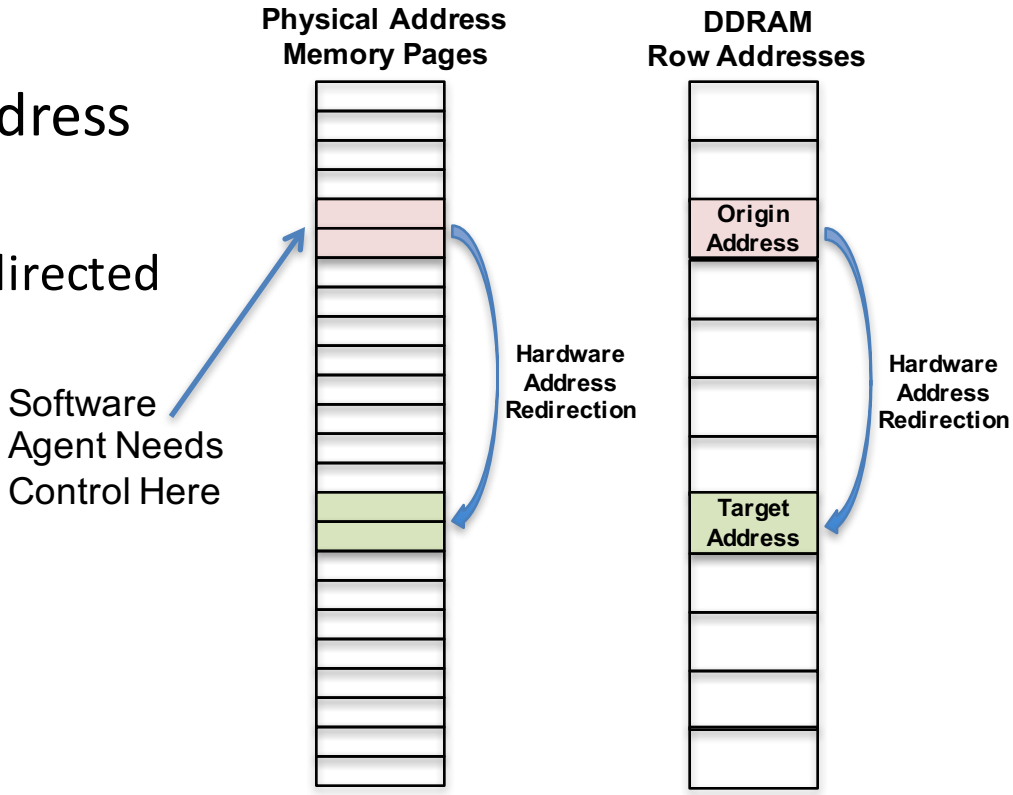
Trojans Settings





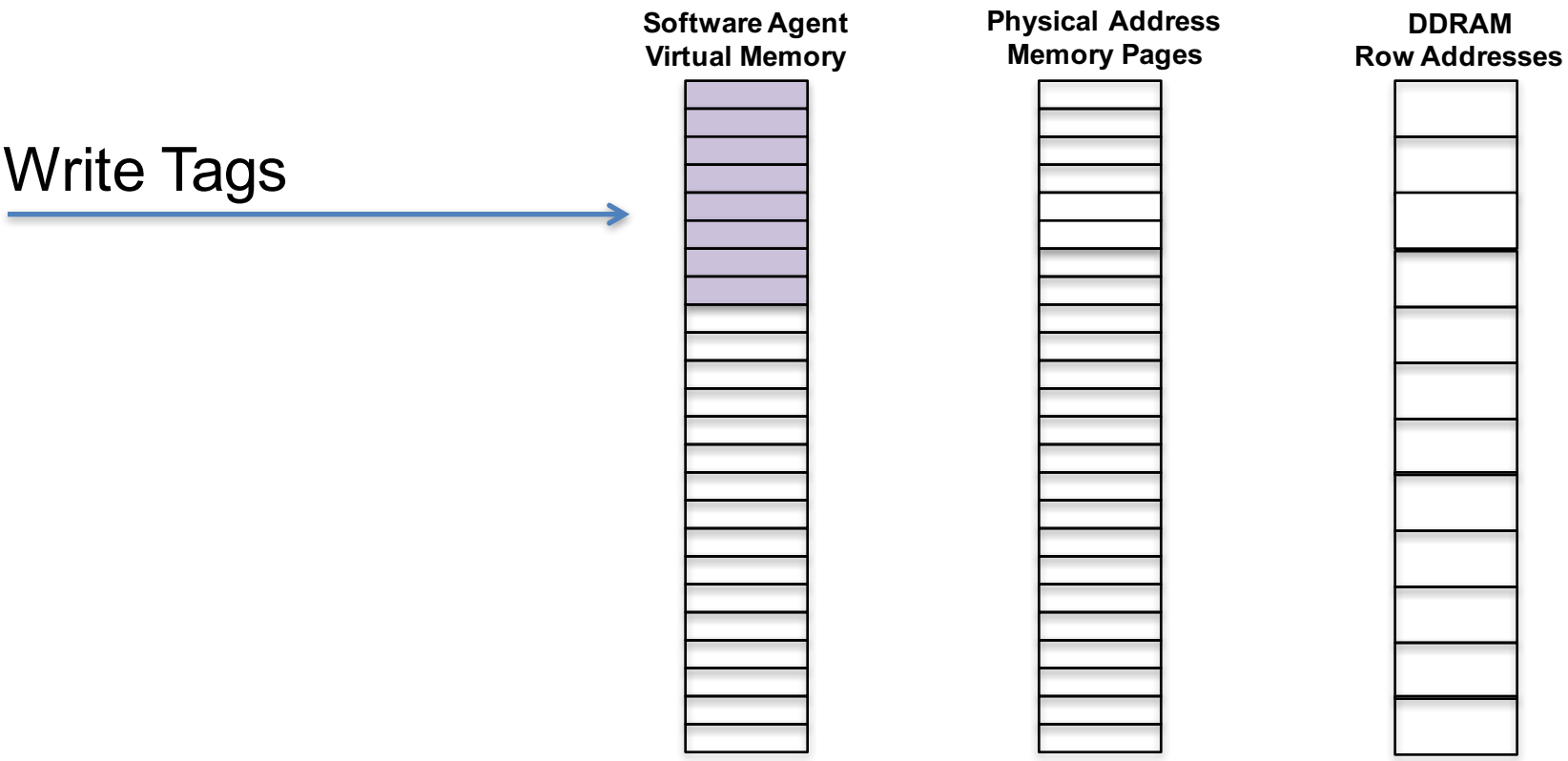
Operation – Page Discovery (0)

- Redirection Sizing
  - Hardware 8KiB Redirection
  - Pages 4KiB each
- Control Need for Origin Address
  - Alternative is errors
  - Memory other programs redirected
- Discover pages to use



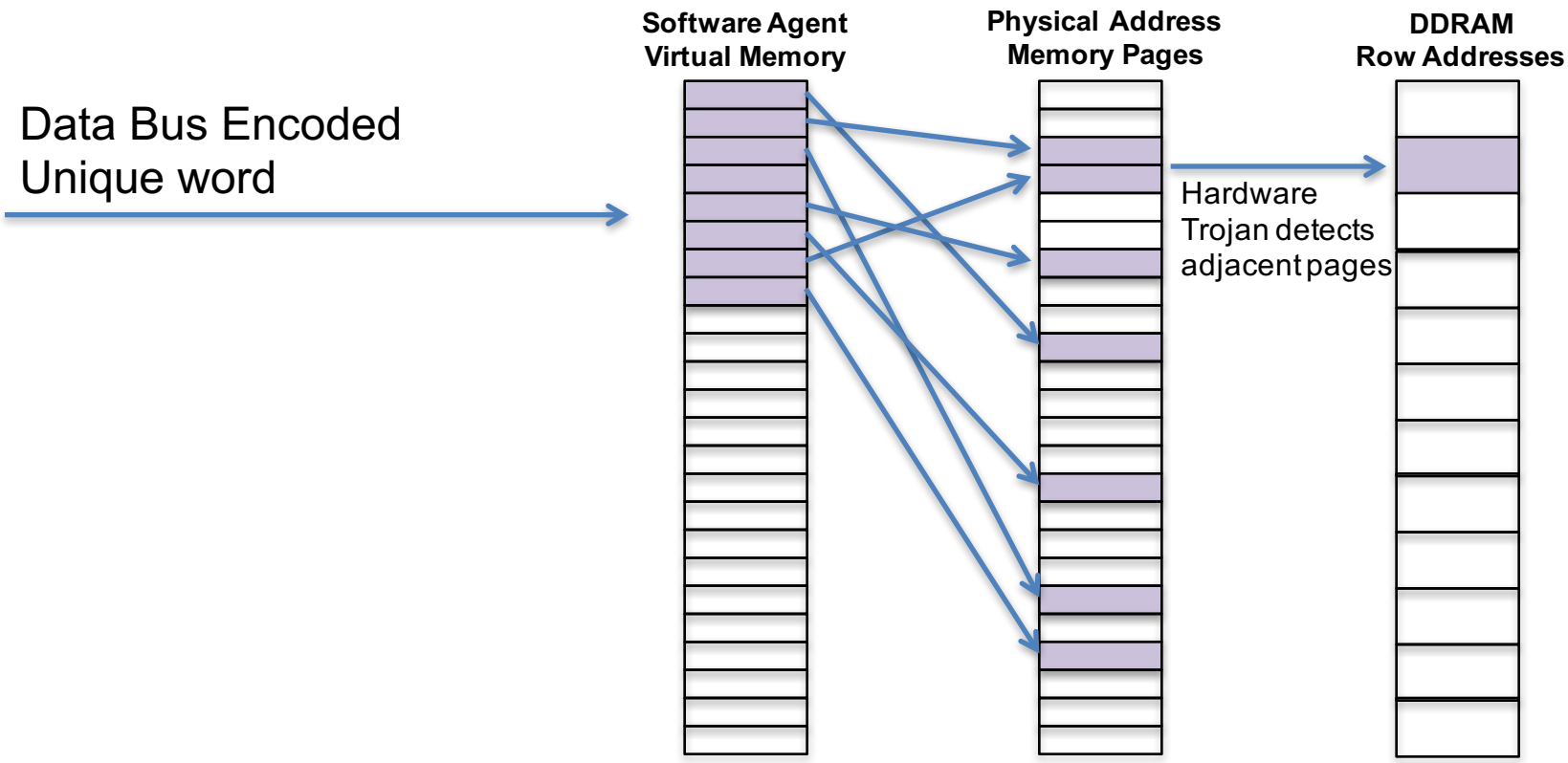
Operation – Page Discovery (1)

- Tag memory pages



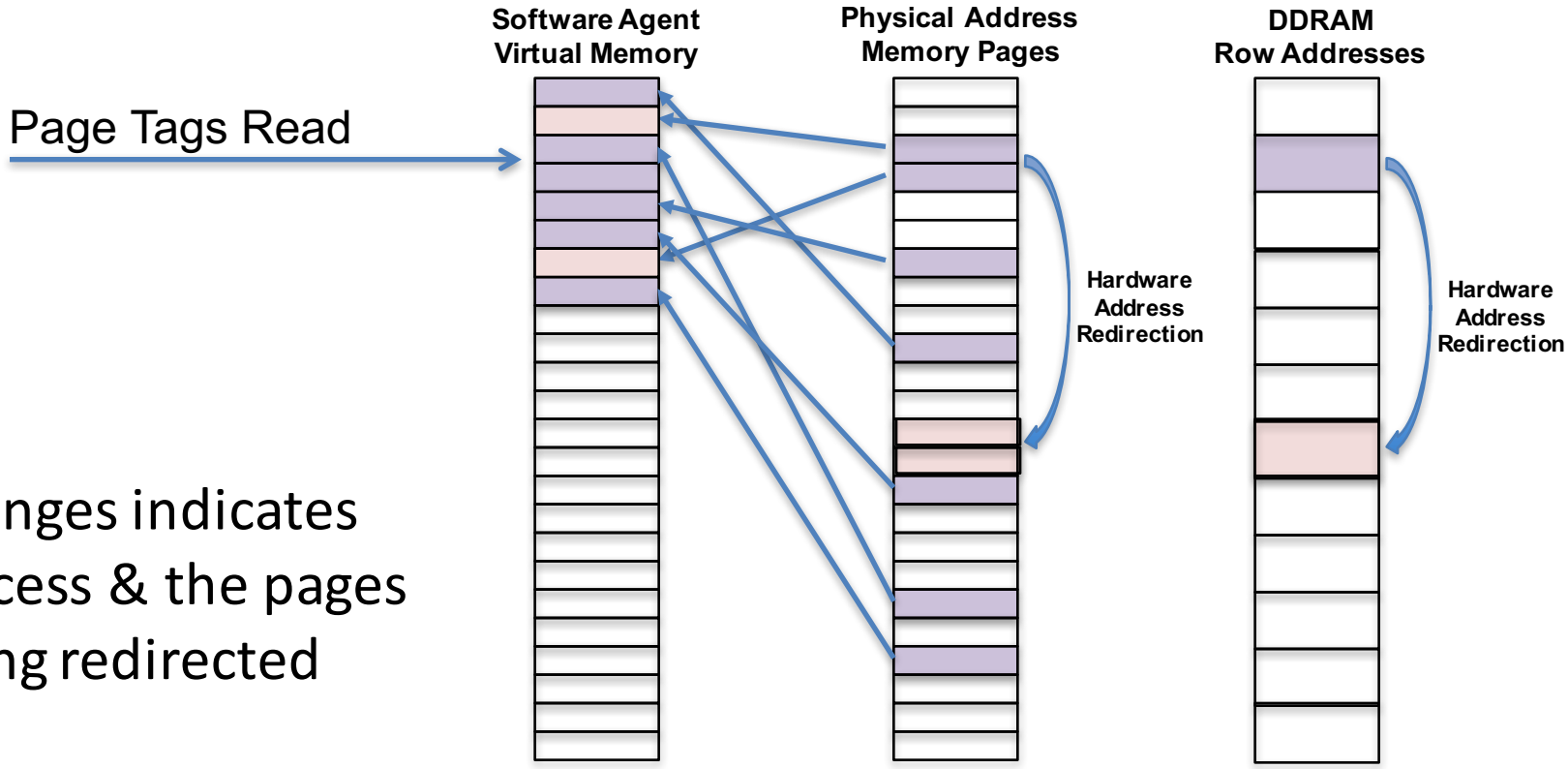
Operation – Page Discovery (2)

- Signal Hardware Trojan on each page



Operation – Page Discovery (3)

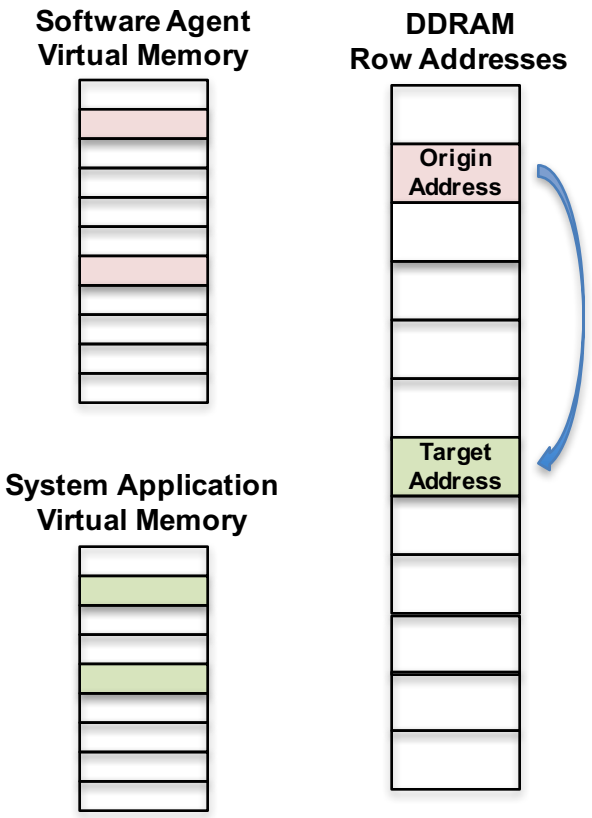
- Tell trojan to redirect
- Request Data



- Changes indicates success & the pages being redirected

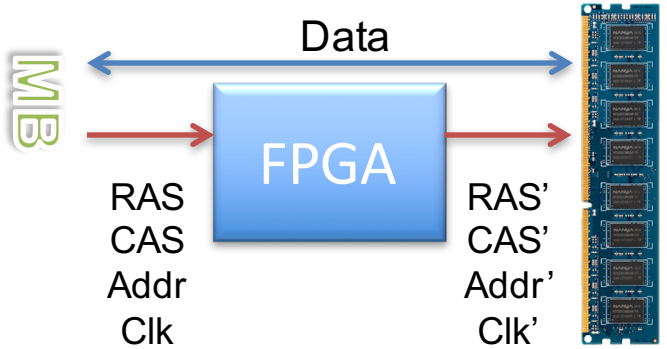
Operation – Redirection

- Redirection from Origin Address
  - Set by Page Discovery
- Redirected to Target Address
  - Settable in the Control Region
- DRAM Trojan redirects only within its own chip
  - Page Discovery for each DRAM

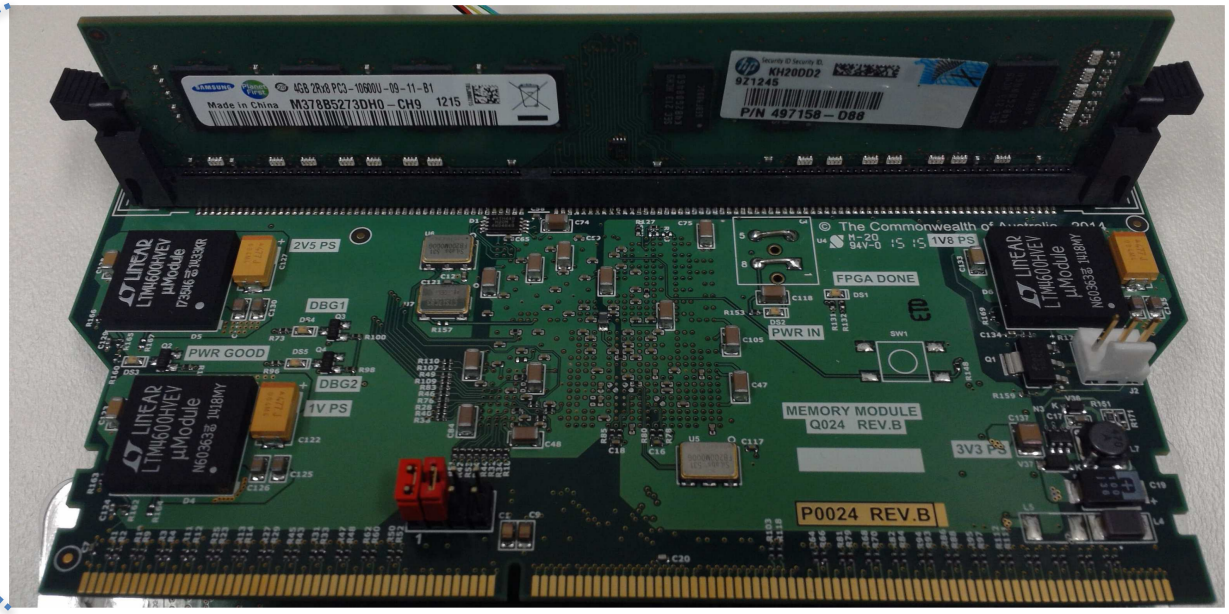


Prototype Demonstrator

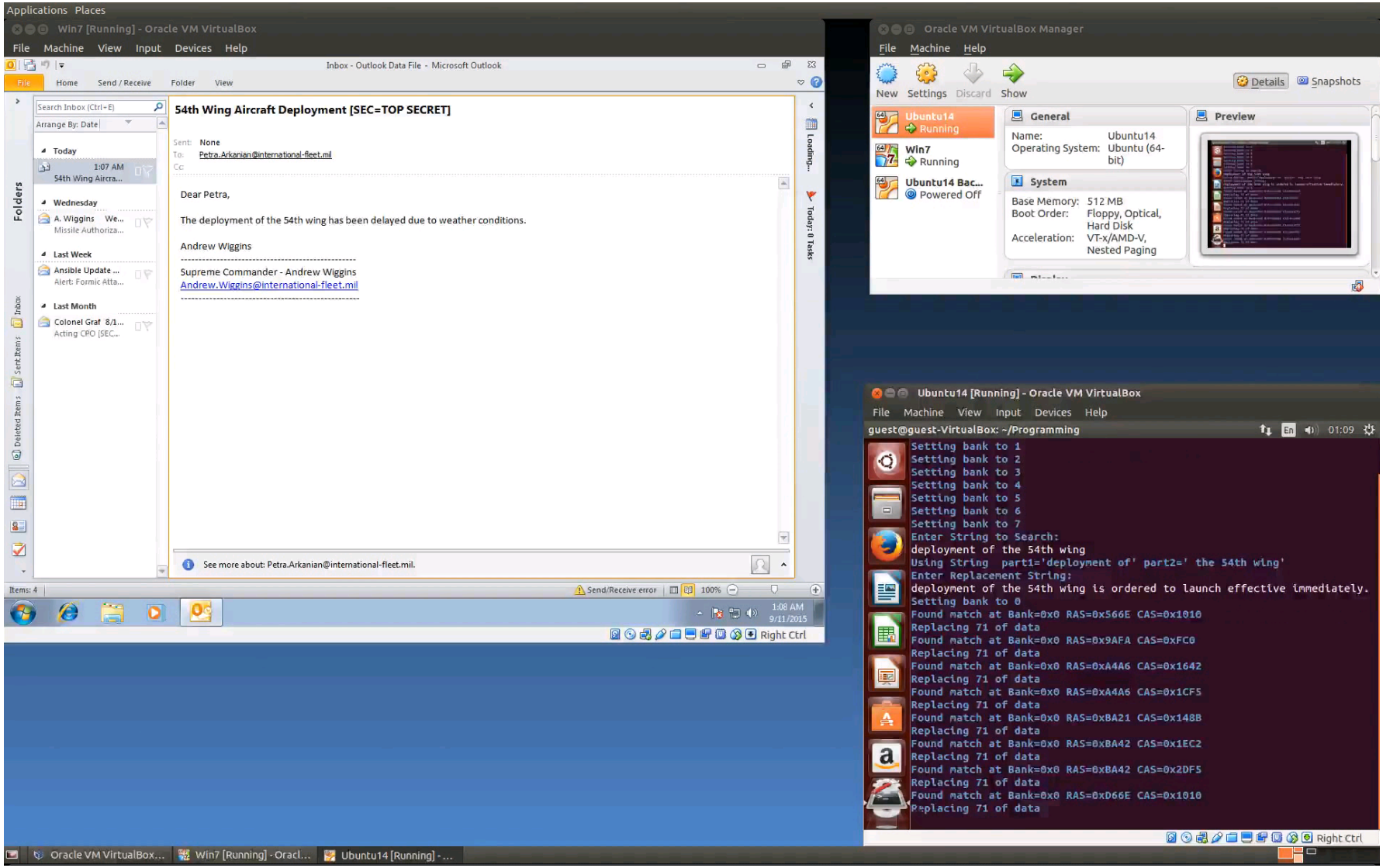
- DDR3 Memory Interposer Card
  - Developing an emulation platform is difficult
  - Derating of bus speeds (DDR800)
  - Derating CAS latency



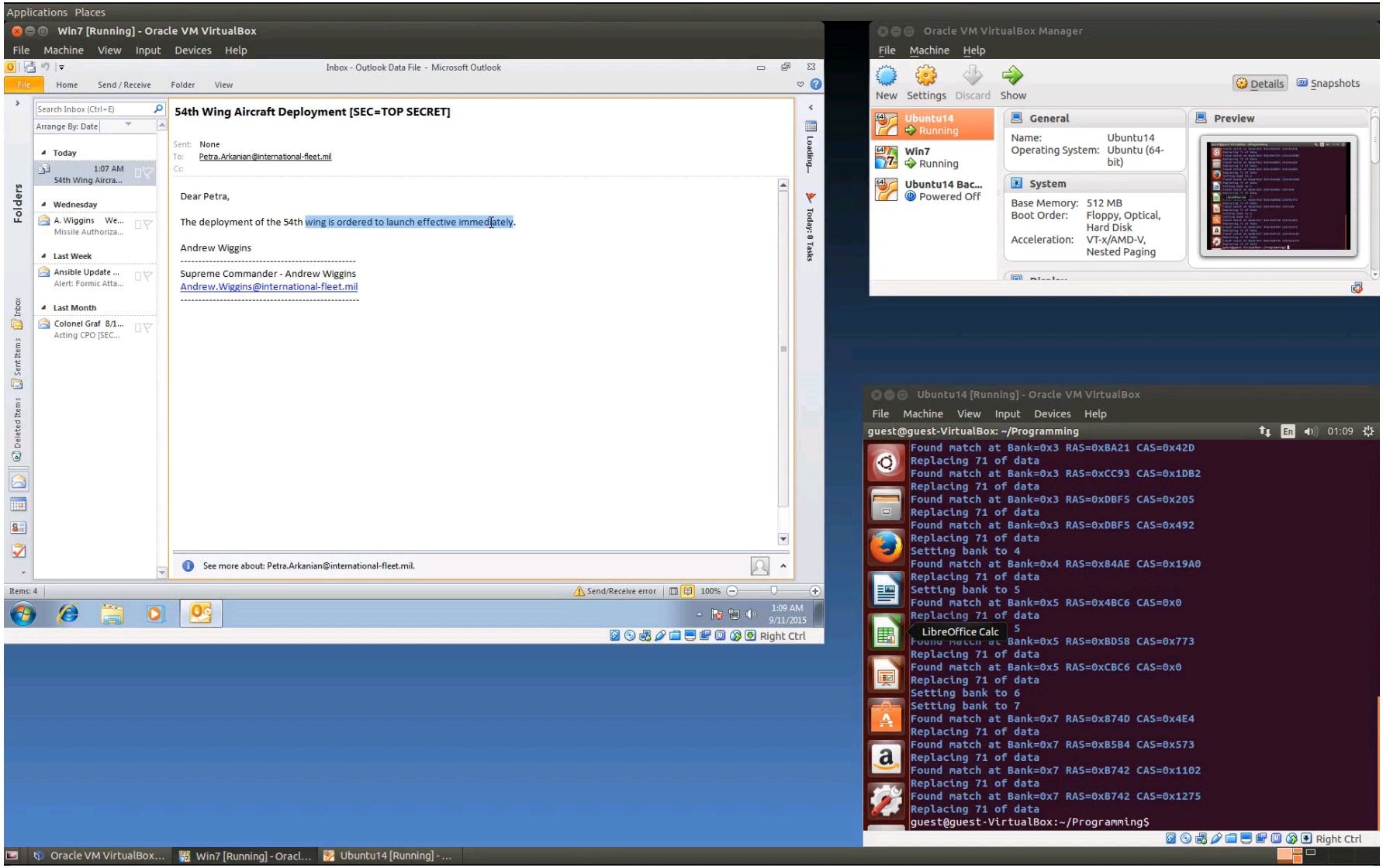
- Trojan architecture in FPGA(Xilinx Kintex-7) rather than silicon
  - Implementation over a full DIMM
  - Logically equivalent to that embedded into individual DRAM ICs.



Use Case: Cloud Computing(1)



Use Case: Cloud Computing(2)



Design Insights

- Simple, small hardware primitives can be leveraged to great effect
- Contextual Layout Information
  - Overcoming Virtualisation
  - Multiple DIMM coordination needed
- Command and Control
  - Many options exist – Ours uses addressing signaling only
  - Characterization of channel needed
- Co-operative Software Agents
  - Reduces hardware complexity
  - Provides analytics on data and layout
  - Unprivileged

Mitigation Strategies

- Increase complexity requirements
  - must assume memory contents, address traffic and access times can be observed (or modified)
- Disrupt contextual and layout information
  - Memory encryption/scrambling
  - Authenticated memory
- Disrupt Command and Control
  - Oblivious Memory
- The cost – size, performance …
- Hardware support for trustworthy systems?