

UNCLASSIFIED



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

Science and Technology for Safeguarding Australia

DST Group - Trustworthy Systems Research

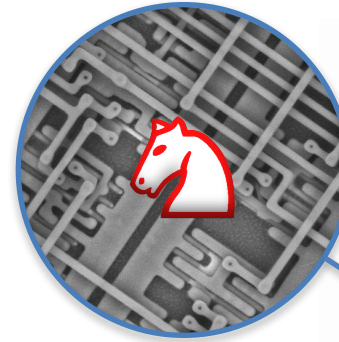
- **Organisation:**
 - Defence Science Technology Group (Australian Department of Defence)
- **Trustworthy Systems Research Group:**
 - Future Threat Estimation- Forecasting and prototyping advanced threats
 - Resilient ICT for security-critical high-assurance systems

Trustworthy Software
Resilient Software Approaches
Metrics for Trustworthy Design Tools
Trustworthiness & Assurance
Formal Verification
Resilient Architectures
Trustworthy Hardware Designs
Hardware Security Measures



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



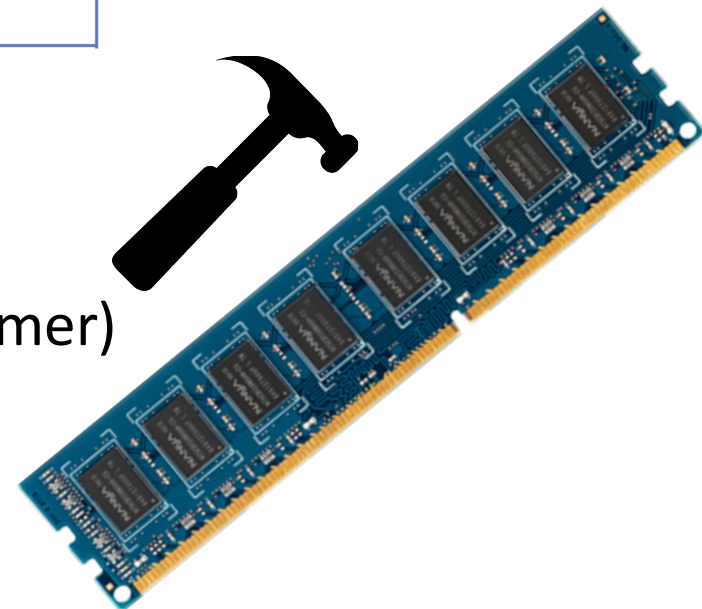
The Hardware Trojan Threat

■ Hardware Trojan Characteristics

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

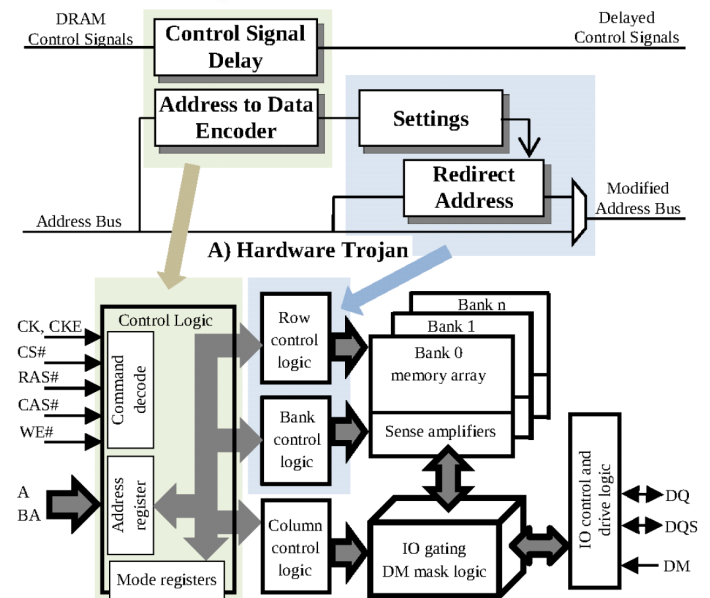
■ DRAM Memory Trojan

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



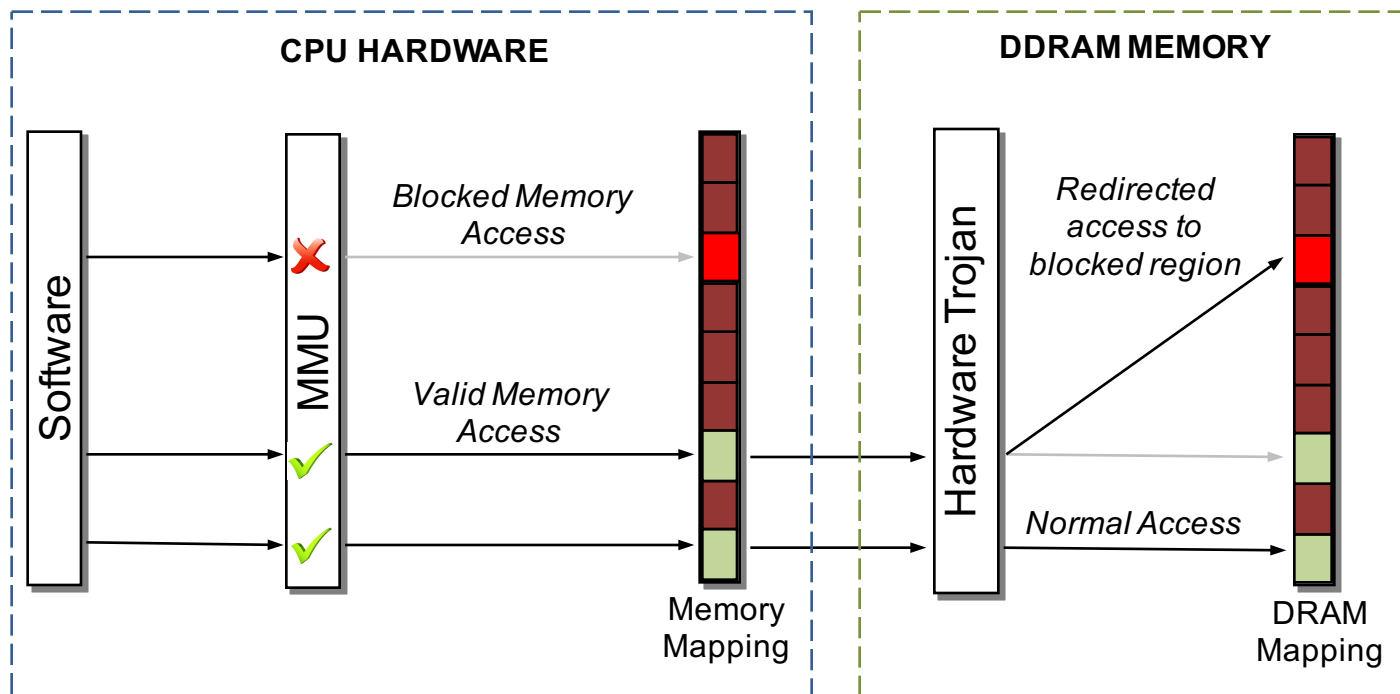
Case Study – Address Redirection Memory Trojan

- 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



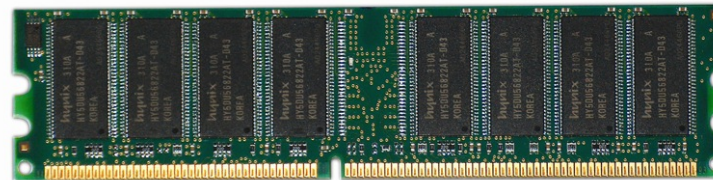
DRAM Memory Trojan – Address Redirection

■ Hardware Redirection

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

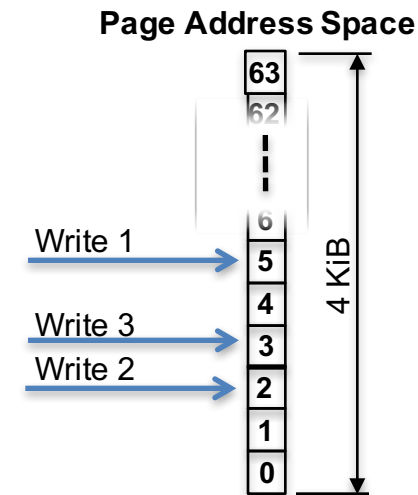
■ Software Agent

- 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	0x00000000000000020
2	0x00000000000000024
3	0x0000000000000002A

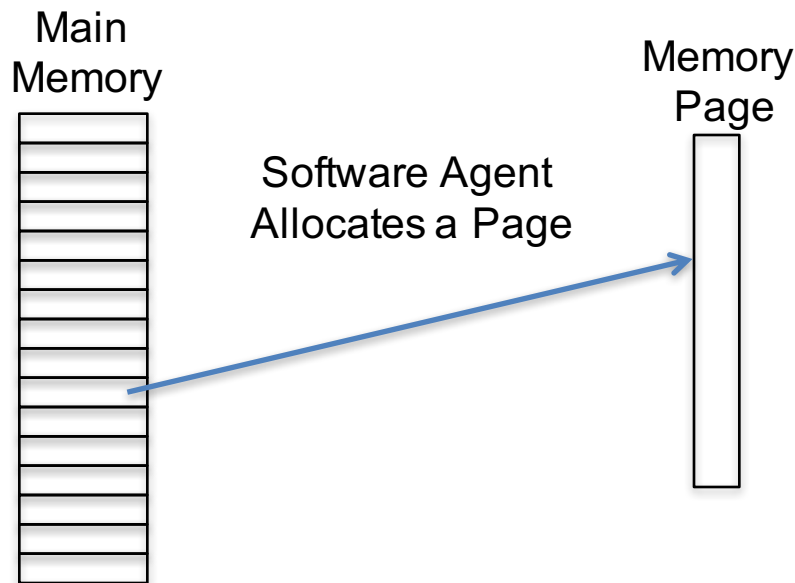
DRAM Memory Trojan - Operation

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

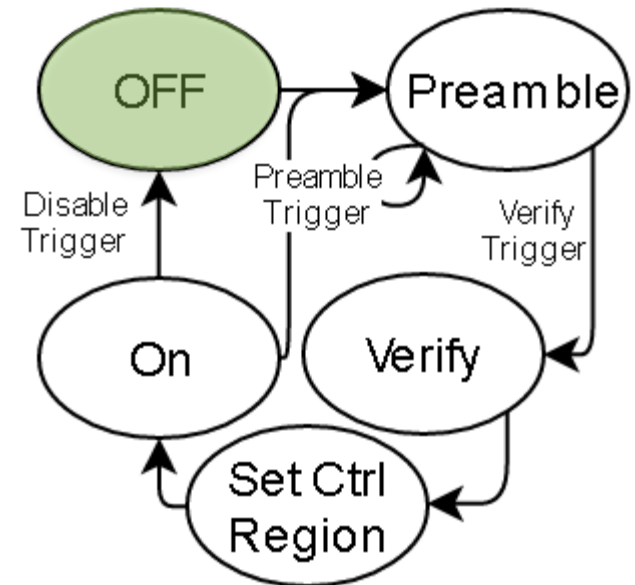


Operation – Activation Sequence (0)

- Set up any memory page

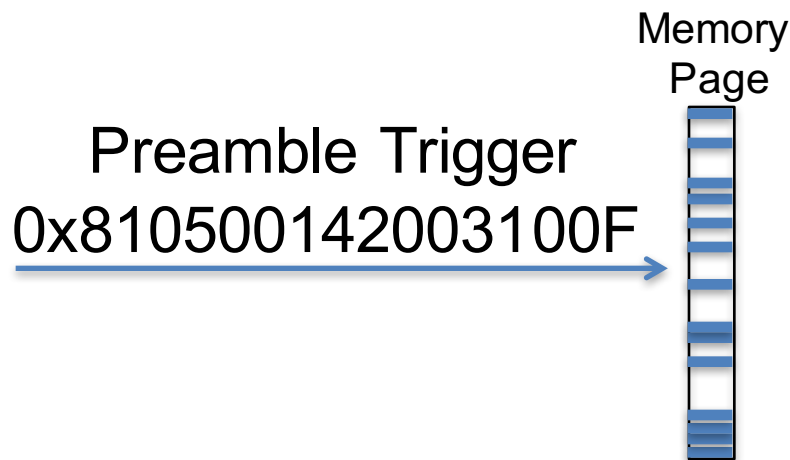


Activation Statemachine

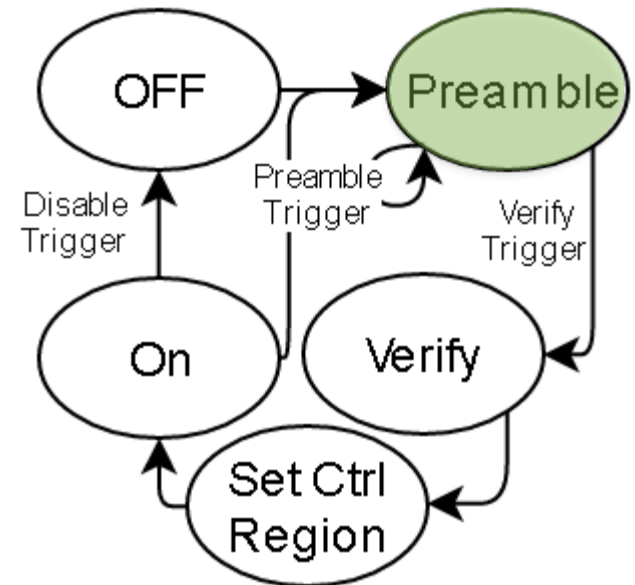


Operation – Activation Sequence (1)

- Address Bus Encoded
- 2 Unique Words of 64 bits

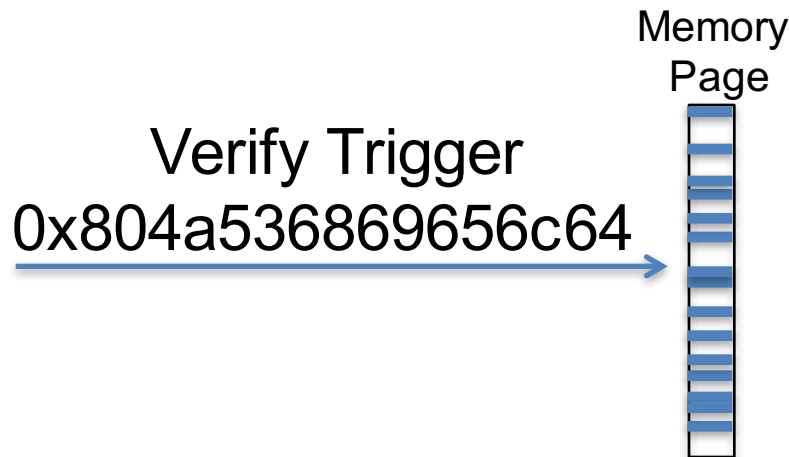


Activation State Machine

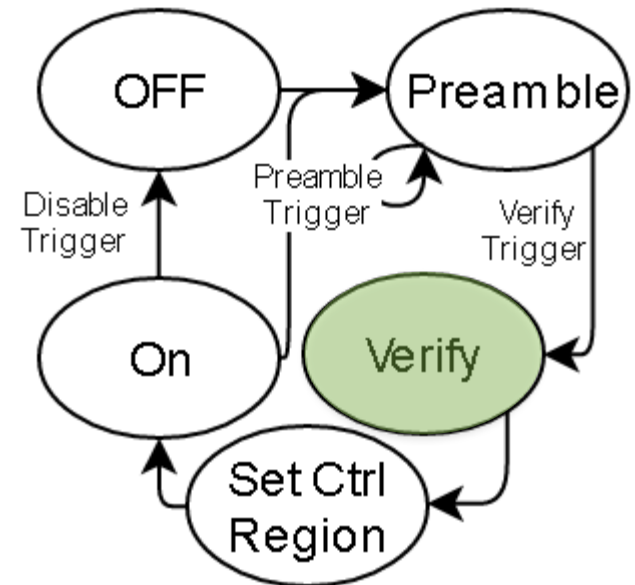


Operation – Activation Sequence (3)

- Address Bus Encoded
- 2 Unique Words of 64 bits

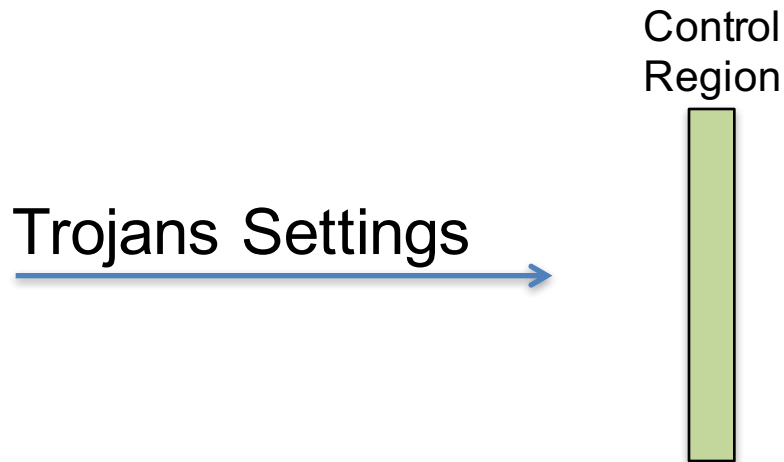


Activation State Machine

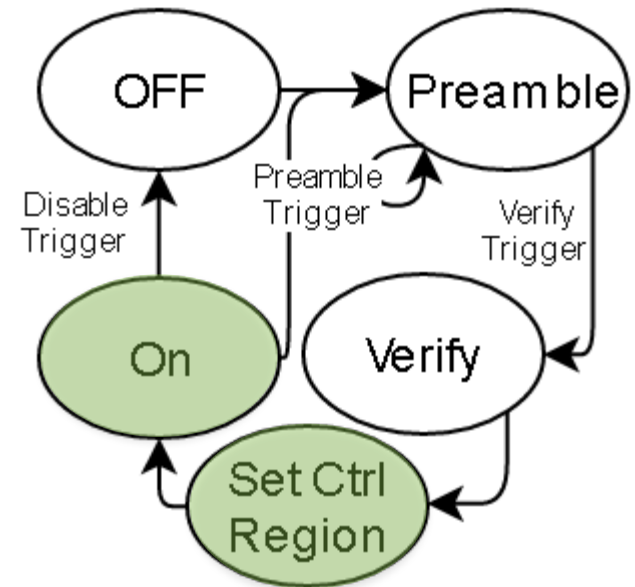


Operation – Activation Sequence (4)

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

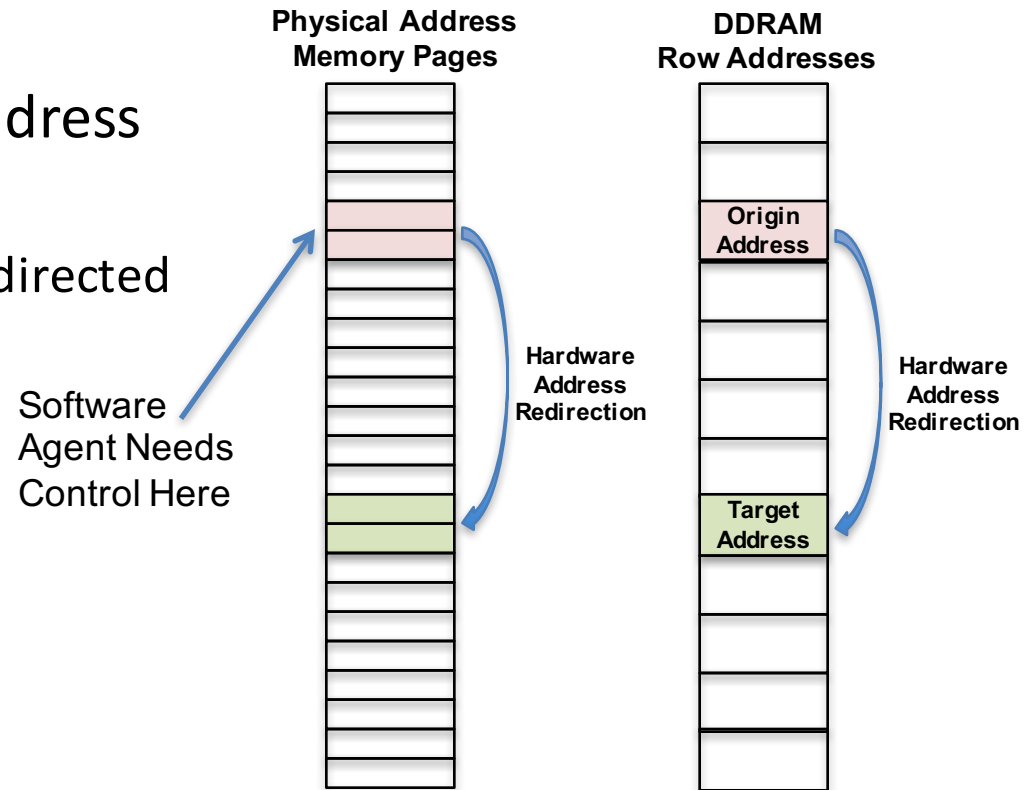


Activation Statemachine



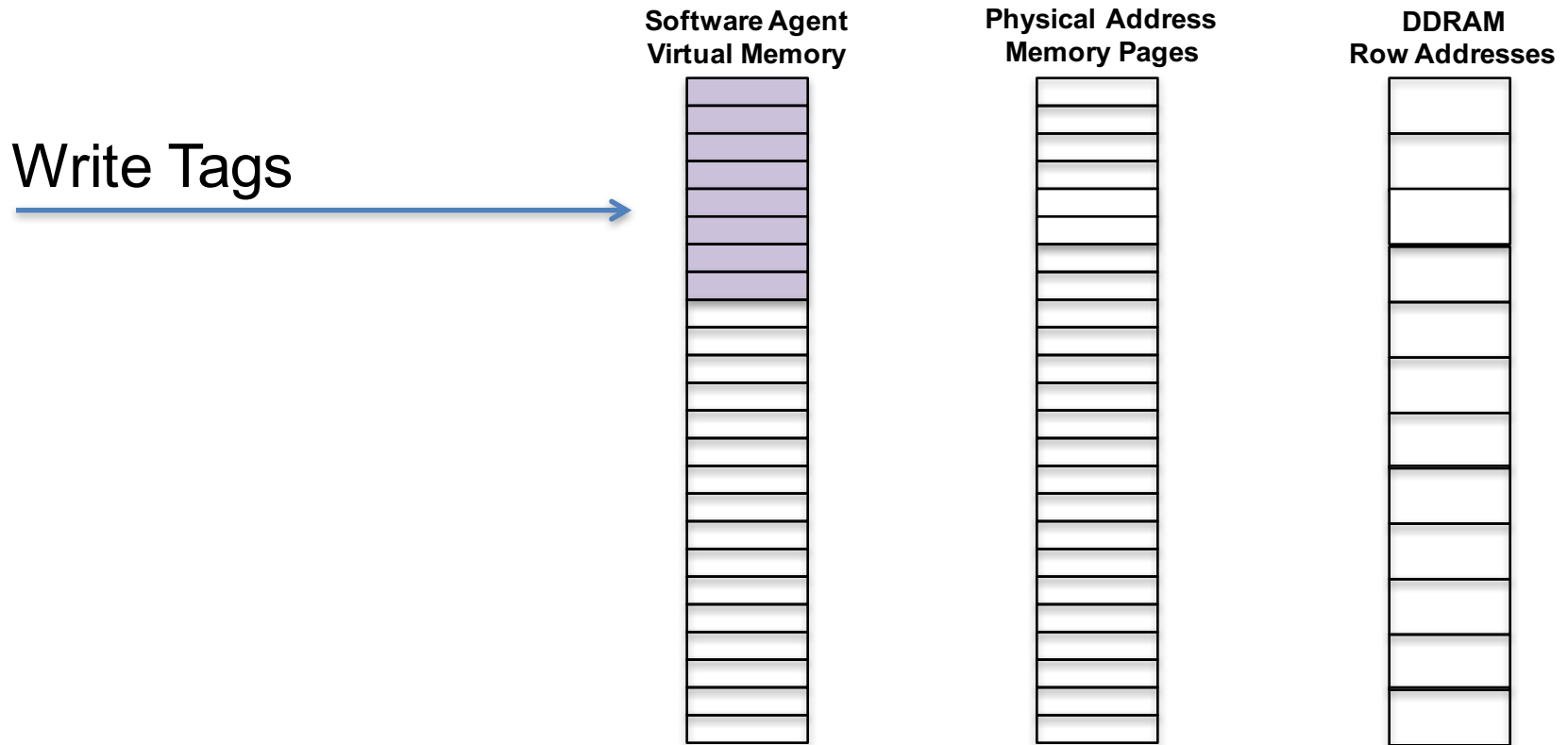
Operation – Page Discovery (0)

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



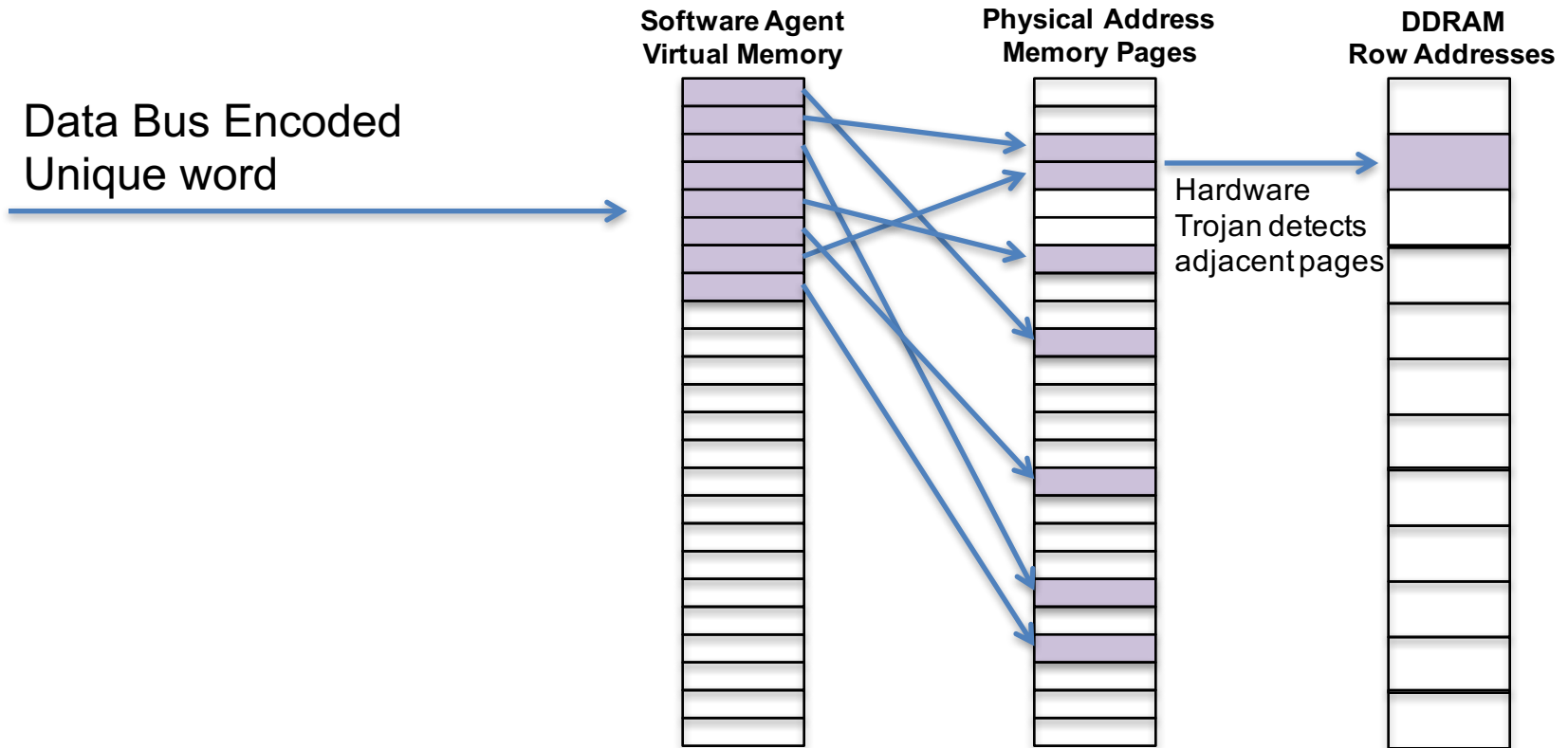
Operation – Page Discovery (1)

- Tag memory pages



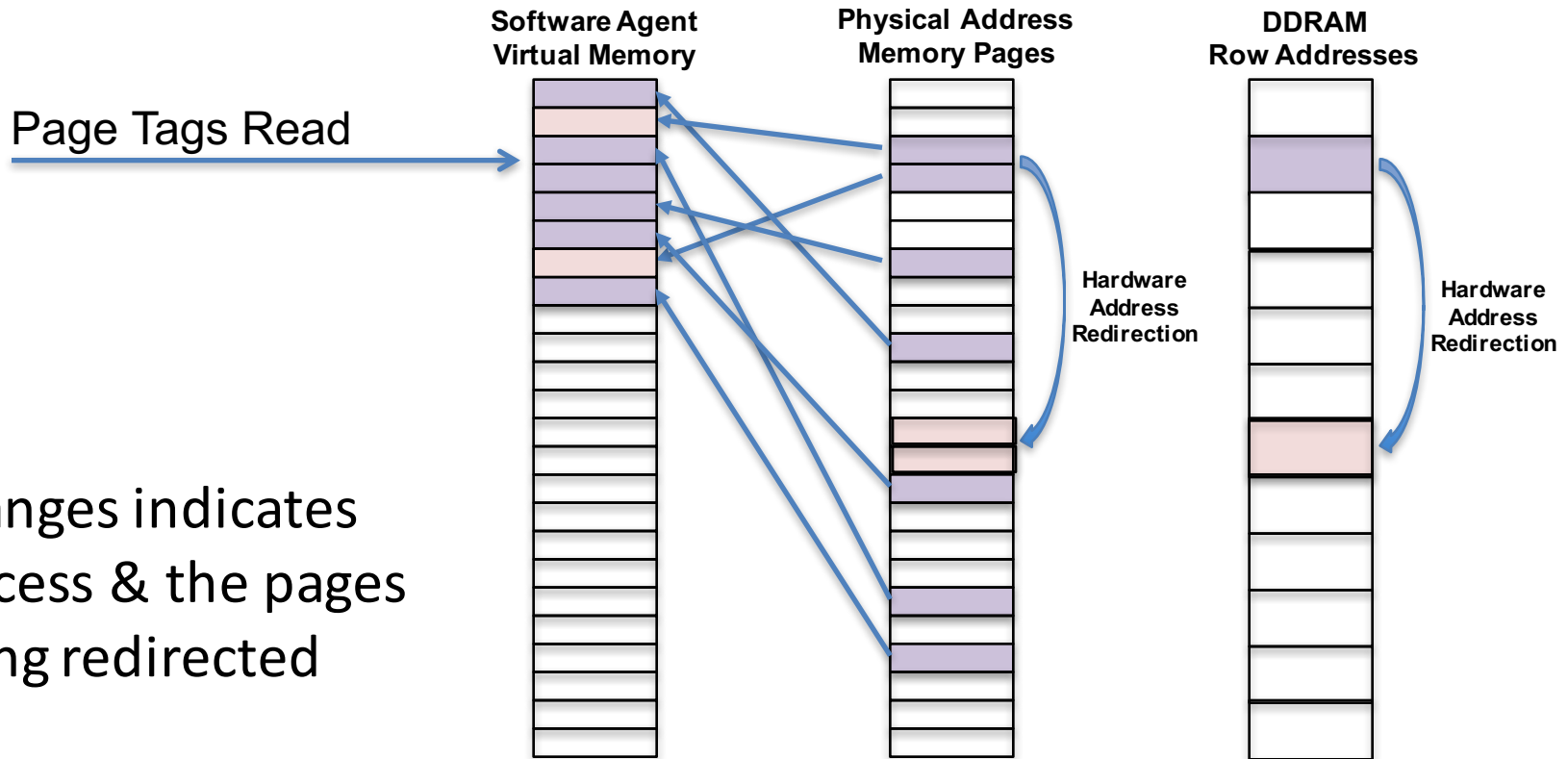
Operation – Page Discovery (2)

- Signal Hardware Trojan on each page



Operation – Page Discovery (3)

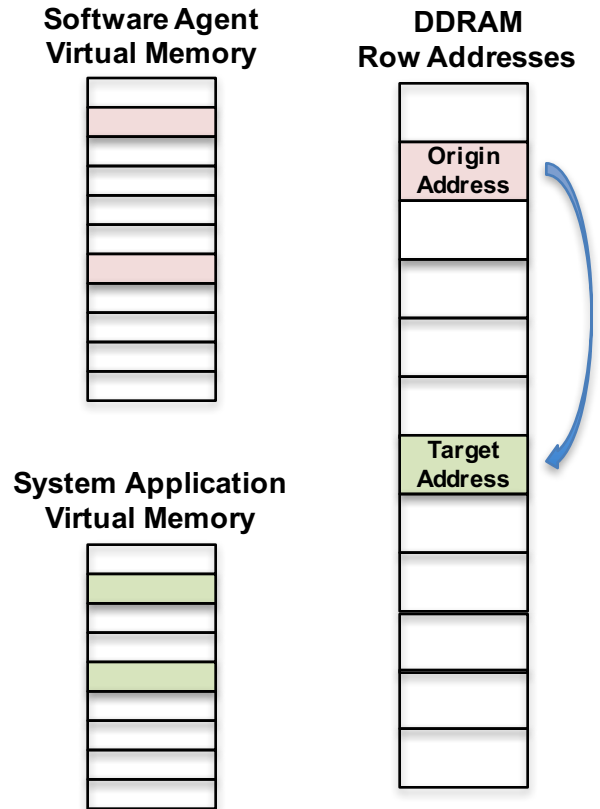
- Tell trojan to redirect
- Request Data



- Changes indicates success & the pages being redirected

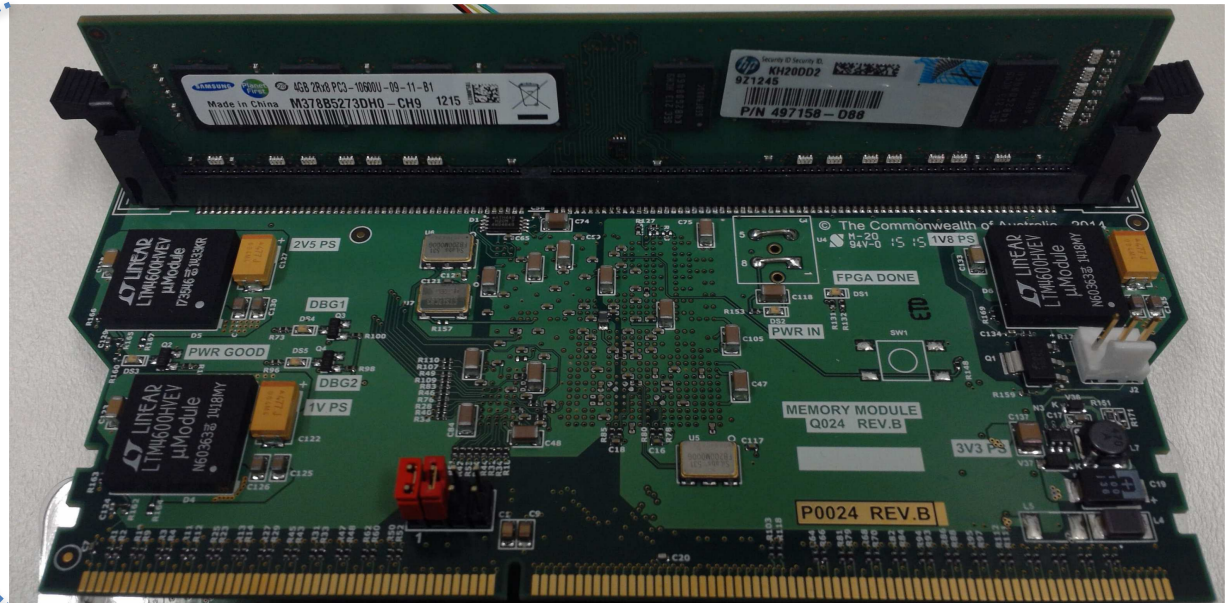
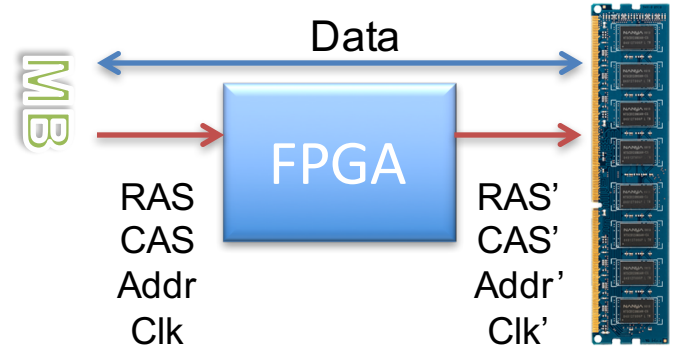
Operation – Redirection

- 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)

The screenshot displays a virtual machine environment. The host is Windows 7, running Oracle VM VirtualBox. An Outlook window is open, showing an email titled "54th Wing Aircraft Deployment [SEC=TOP SECRET]" from Andrew Wiggins to Petra.Arkonian@international-fleet.mil. The email content states: "Dear Petra, The deployment of the 54th wing has been delayed due to weather conditions. Andrew Wiggins Supreme Commander - Andrew Wiggins Andrew.Wiggins@international-fleet.mil".

The virtual machine manager shows three VMs: Ubuntu14 (Running), Win7 (Running), and Ubuntu14 Bac... (Powered Off). The details for the running Ubuntu14 VM are shown, including its name, operating system (Ubuntu (64-bit)), base memory (512 MB), boot order (Floppy, Optical, Hard Disk), and acceleration (VT-x/AMD-V, Nested Paging).

The Ubuntu 14 terminal window shows the following output:

```
Setting bank to 1
Setting bank to 2
Setting bank to 3
Setting bank to 4
Setting bank to 5
Setting bank to 6
Setting bank to 7
Enter String to Search:
deployment of the 54th wing
Using String part1='deployment of' part2=' the 54th wing'
Enter Replacement String:
deployment of the 54th wing is ordered to launch effective immediately.
Setting bank to 0
Found match at Bank=0x0 RAS=0x566E CAS=0x1010
Replacing 71 of data
Found match at Bank=0x0 RAS=0x9AFA CAS=0xPFC0
Replacing 71 of data
Found match at Bank=0x0 RAS=0xA4A6 CAS=0x1642
Replacing 71 of data
Found match at Bank=0x0 RAS=0xA4A6 CAS=0x1CF5
Replacing 71 of data
Found match at Bank=0x0 RAS=0xBA21 CAS=0x148B
Replacing 71 of data
Found match at Bank=0x0 RAS=0xBA42 CAS=0x1EC2
Replacing 71 of data
Found match at Bank=0x0 RAS=0xBA42 CAS=0x2DF5
Replacing 71 of data
Found match at Bank=0x0 RAS=0xD66E CAS=0x1010
Replacing 71 of data
```

Use Case: Cloud Computing(2)

The screenshot displays the Oracle VM VirtualBox Manager interface. On the left, a Windows 7 virtual machine is running, showing a Microsoft Outlook window with an email titled "54th Wing Aircraft Deployment [SEC=TOP SECRET]". The email content includes:

Sent: None
To: Petra.Arkanian@international-fleet.mil
Cc:
Date: 1:07 AM

Dear Petra,
The deployment of the 54th wing is ordered to launch effective immediately.
Andrew Wiggins
Supreme Commander - Andrew Wiggins
Andrew.Wiggins@international-fleet.mil

On the right, the Oracle VM VirtualBox Manager window shows the configuration for an Ubuntu 14 virtual machine. The "General" tab is selected, showing the name "Ubuntu14" and operating system "Ubuntu (64-bit)". The "System" tab shows the base memory as 512 MB and boot order as Floppy, Optical, Hard Disk. The "Acceleration" tab shows VT-x/AMD-V and Nested Paging are enabled. A "Preview" window shows a terminal window with a command prompt.

Below the VirtualBox Manager, the Ubuntu 14 virtual machine is running, showing a terminal window with the following output:

```
guest@guest-VirtualBox: ~/Programming
Found match at Bank=0x3 RAS=0xBA21 CAS=0x42D
Replacing 71 of data
Found match at Bank=0x3 RAS=0xCC93 CAS=0x1DB2
Replacing 71 of data
Found match at Bank=0x3 RAS=0xDBF5 CAS=0x205
Replacing 71 of data
Found match at Bank=0x3 RAS=0xDBF5 CAS=0x492
Replacing 71 of data
Setting bank to 4
Found match at Bank=0x4 RAS=0x84AE CAS=0x19A0
Replacing 71 of data
Setting bank to 5
Found match at Bank=0x5 RAS=0x4BC6 CAS=0x0
Replacing 71 of data
Found match at Bank=0x5 RAS=0xBD58 CAS=0x773
Replacing 71 of data
Found match at Bank=0x5 RAS=0xCBC6 CAS=0x0
Replacing 71 of data
Setting bank to 6
Setting bank to 7
Found match at Bank=0x7 RAS=0x874D CAS=0x4E4
Replacing 71 of data
Found match at Bank=0x7 RAS=0x85B4 CAS=0x573
Replacing 71 of data
Found match at Bank=0x7 RAS=0xB742 CAS=0x1102
Replacing 71 of data
Found match at Bank=0x7 RAS=0xB742 CAS=0x1275
Replacing 71 of data
guest@guest-VirtualBox: ~/Programming$
```



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?



