PCI Express Integrity

Gord Caruk

Architect

ATI Technologies

Copyright

- Copyright – a form of intellectual property rights which differs from physical property rights:
  - ✓Copyright legislation prevents the copying of “protected content” and delays the entry of protected content into the public domain
  - ✓Most countries have established a concept of "fair use" or "fair dealing" where consumers are allowed to copy protected content for personal or private use
- Wide interpretation of “fair use”

Protecting the "Protected Content"

- "Protected content" has been copied and distributed widely via the PC platform in the past
- Concerns have been heard that "protected content" might be captured moving across PCI Express
- PCI Express has inherent characteristics which make capturing "protected content" off the interface extremely improbable

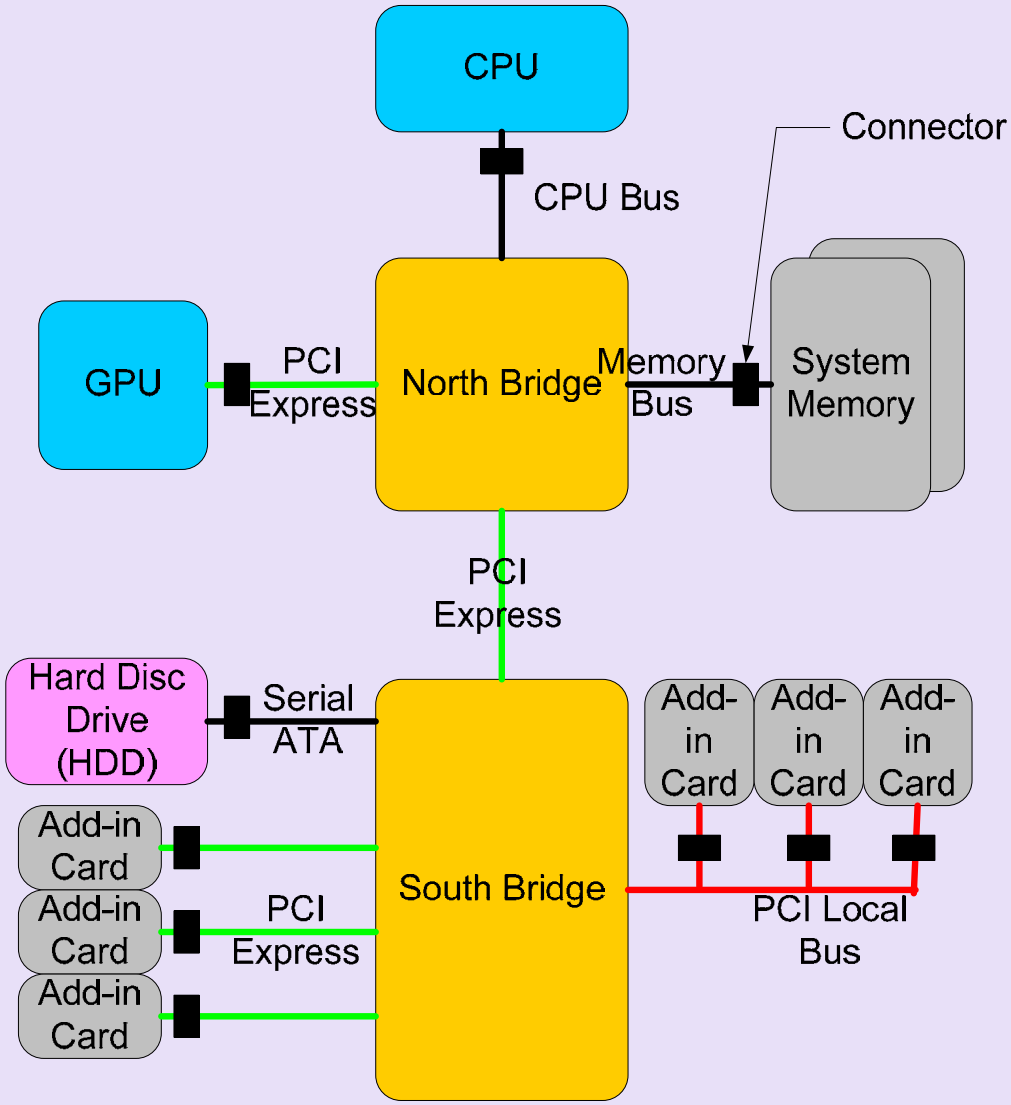
From the Dictionary

- Eavesdrop
  - ✓ To observe or listen in secret to obtain information
- Snoop
  - ✓ To look into or inquire about inquisitively, or in a meddlesome fashion. ***Idiom:*** stick one's nose into.
- Integrity
  - ✓ Ethical strength, free from defect
- Robust
  - ✓ Powerfully built, sturdy, strong

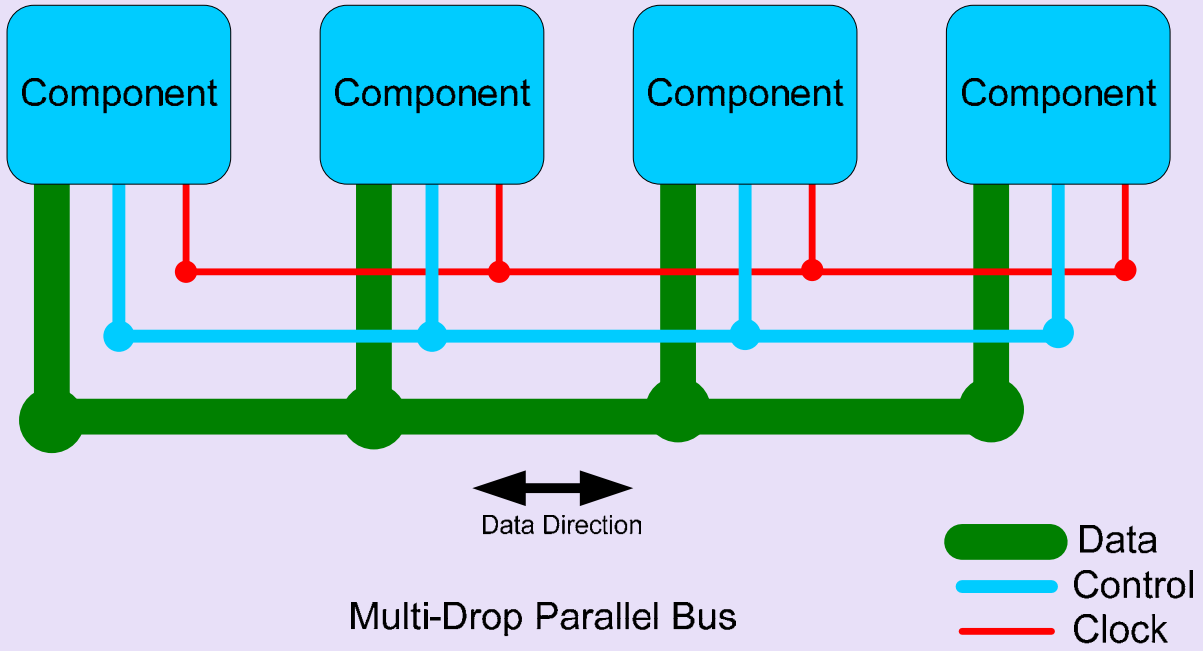
PCI Express Integrity / Robustness Features

- Point to point interconnect
- No clock
- Minimum operating speed
- 8b/10b Encode
- Randomized data
- Lane to lane skew
- Packetized transactions
- Separate completions
- PCI Express interconnect is significantly more complex than historical busses and is clearly in a different category with respect to susceptibility to illegal interception of data during transit

Typical Computer Architecture

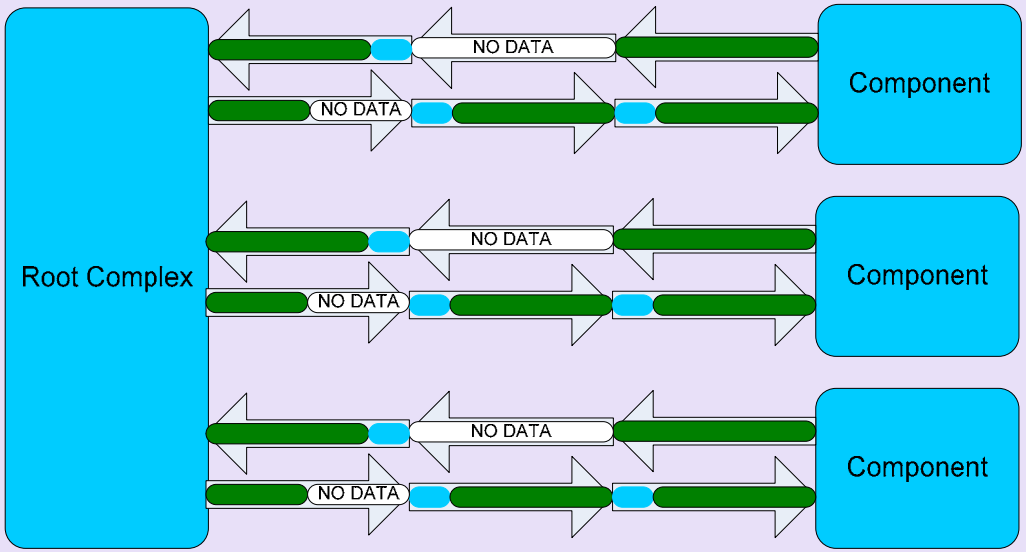


Multi-Drop Physical Topology



- Multi-point bus topology makes it possible to insert an “eavesdropping” card into an otherwise unmodified system, because the connectors are bussed together electrically

PCIe Physical Topology

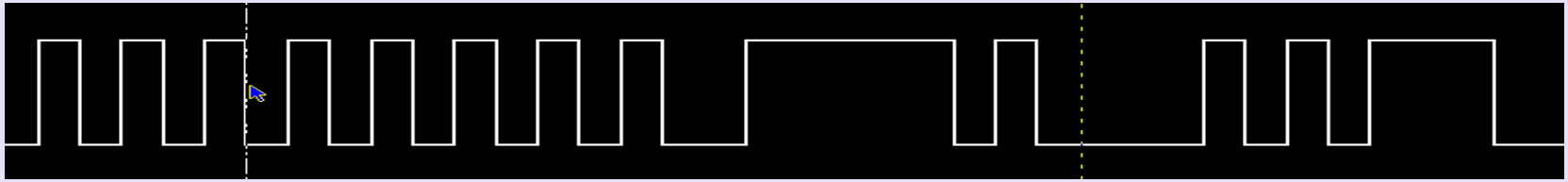


PCI Express Interconnect (x1)

- PCI Express topology is point to point. A card plugged into an adjacent slot cannot see the traffic on the interconnect.
- The presence, or absence, of a connector is an extremely poor indicator of susceptibility

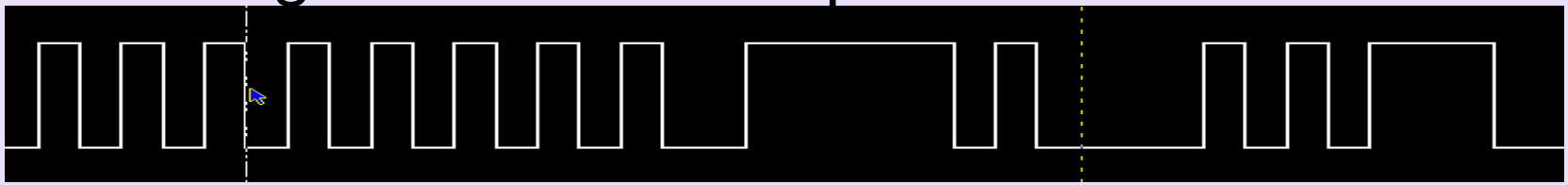
PCIe Receive Clock

- PCIe does not have an “embedded clock”
- Rather, all information needed to regenerate a clock is contained in the incoming data
  - ✓ Frequency is 2.5 / 5 GHz (400 ps / 200 ps UI)
  - ✓ Align phase of clock to the center of the single bit data changes
    - change PLL frequency to slide clock
    - pick a phase of the clock closer to center of bit change



Regenerating Clock

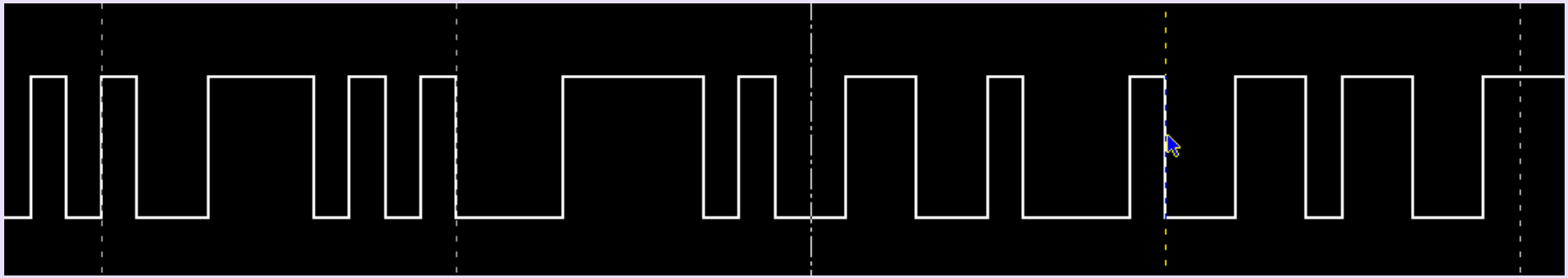
- PCIe receive clock is generated by:
  - ✓ "watching" the data signal switching every 400 ps
  - ✓ locking an oscillator to the minimum period of the data changes
  - ✓ aligning the oscillator's rising edges to occur at the mid-point of the symbol bit
  - ✓ doing this at 2.5 / 5 GHz
- This operation is technically extremely difficult. Generating this clock is the most difficult of the challenges associated with recovering the data moving over the PCI Express interconnect.



Minimum Operating Speed

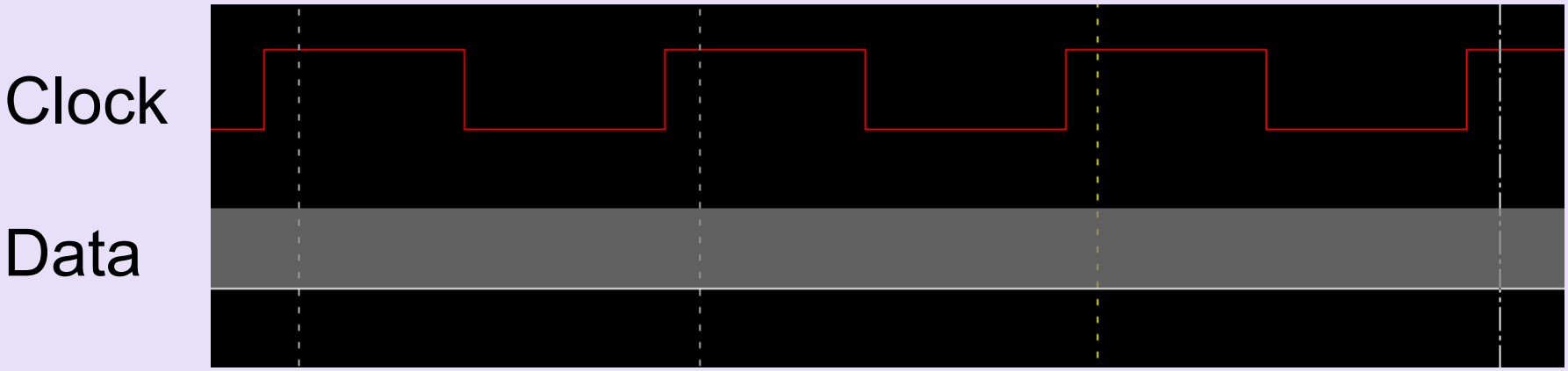
- Multi-point busses have:
  - ✓ Relatively low maximum operating frequencies
  - ✓ Can be slowed down to very low frequencies
- PCI Express:
  - ✓ Has a very narrow range of operating frequency
  - ✓ Cannot be slowed down to make snooping easier
  - ✓ Is intolerant of line discontinuities. PCIe will likely fail if tapping in via an eavesdropping device.
  - ✓ Further exacerbated by PCIe 2.0's 5GT/s data rate
- Eavesdropping device is swamped by high data rate

Randomized, Encoded Data

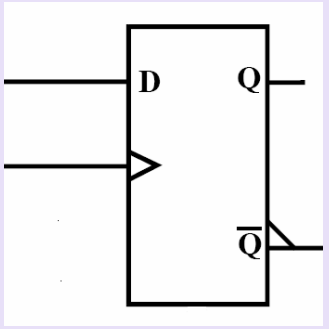


- 8b/10b encoding of scrambled data hides the actual value
- Direct visibility of the data is not possible
- Eavesdropping device must determine symbol alignment, decode the symbol, unscramble to determine that byte of data (very difficult)

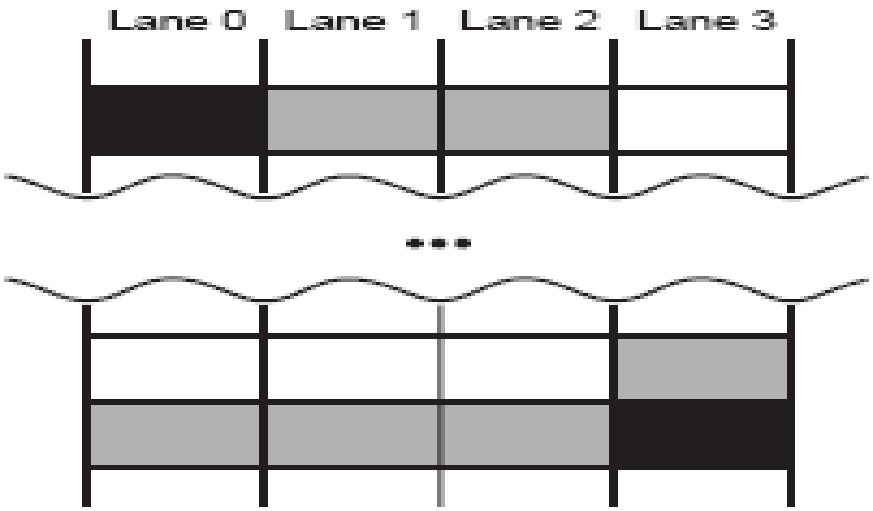
Same Data on a Parallel Bus



- Data on a parallel bus is easily captured
- Value easily determined



Lane Skew



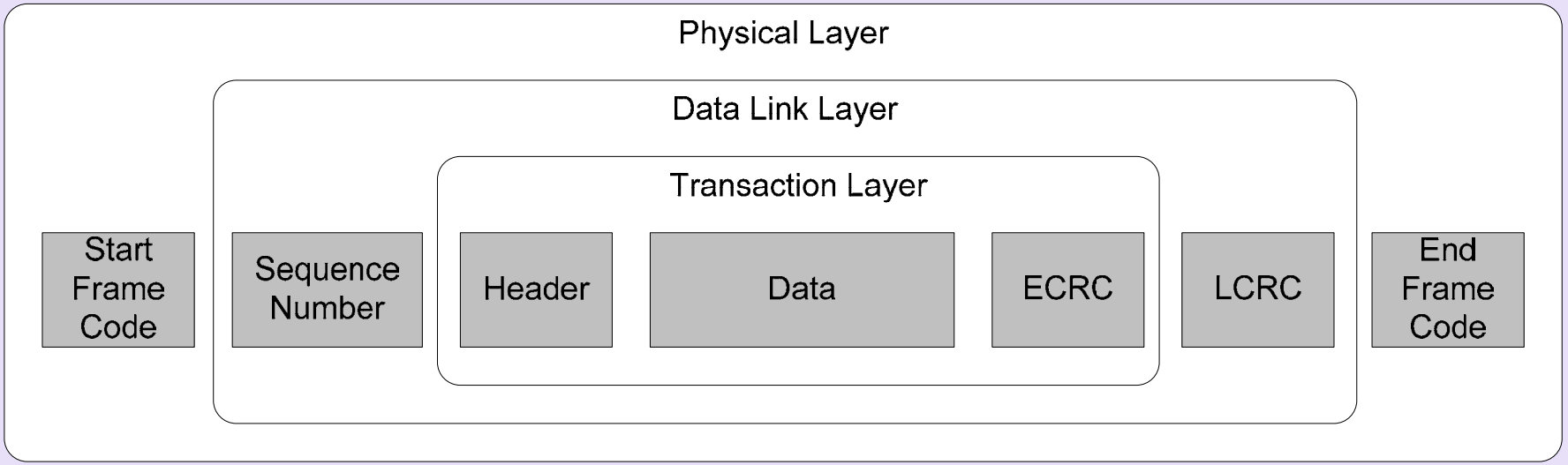
STP/END Framing Symbols- Physical Layer

Sequence Number/LCRC- Data Link Layer

TLP - Transaction Layer

- TLP striped across lanes
- Lanes can be skewed by multiple symbol times
- Eavesdropping device must perform the difficult and burdensome task of realigning multi-lane data and reassemble packets

Packetized Transactions



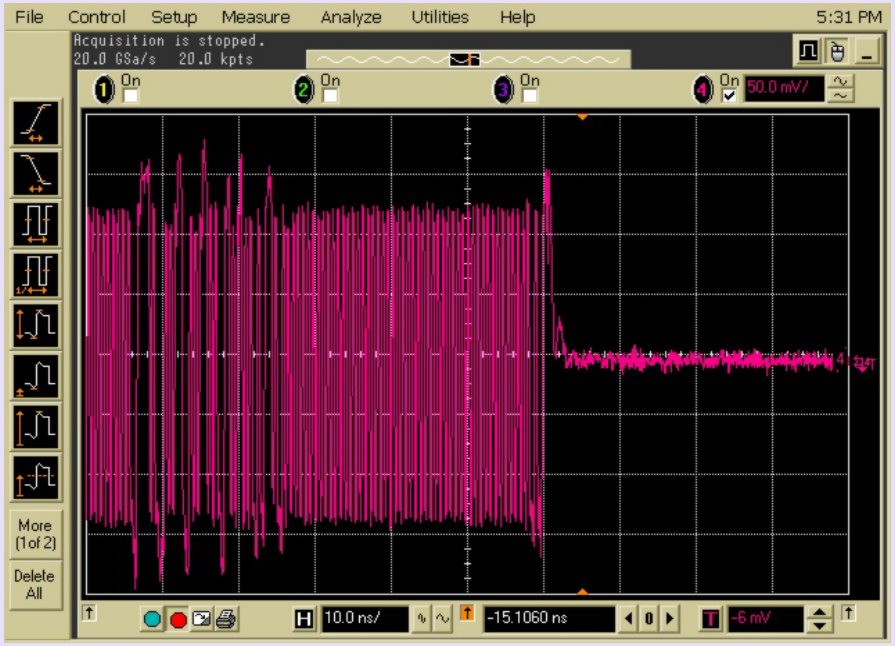
- Layers of packet abstraction
- Packetized transactions are inherently more difficult to "read"
- Eavesdropping device must strip off portions of packet and parse the rest to extract data

Separate Completions

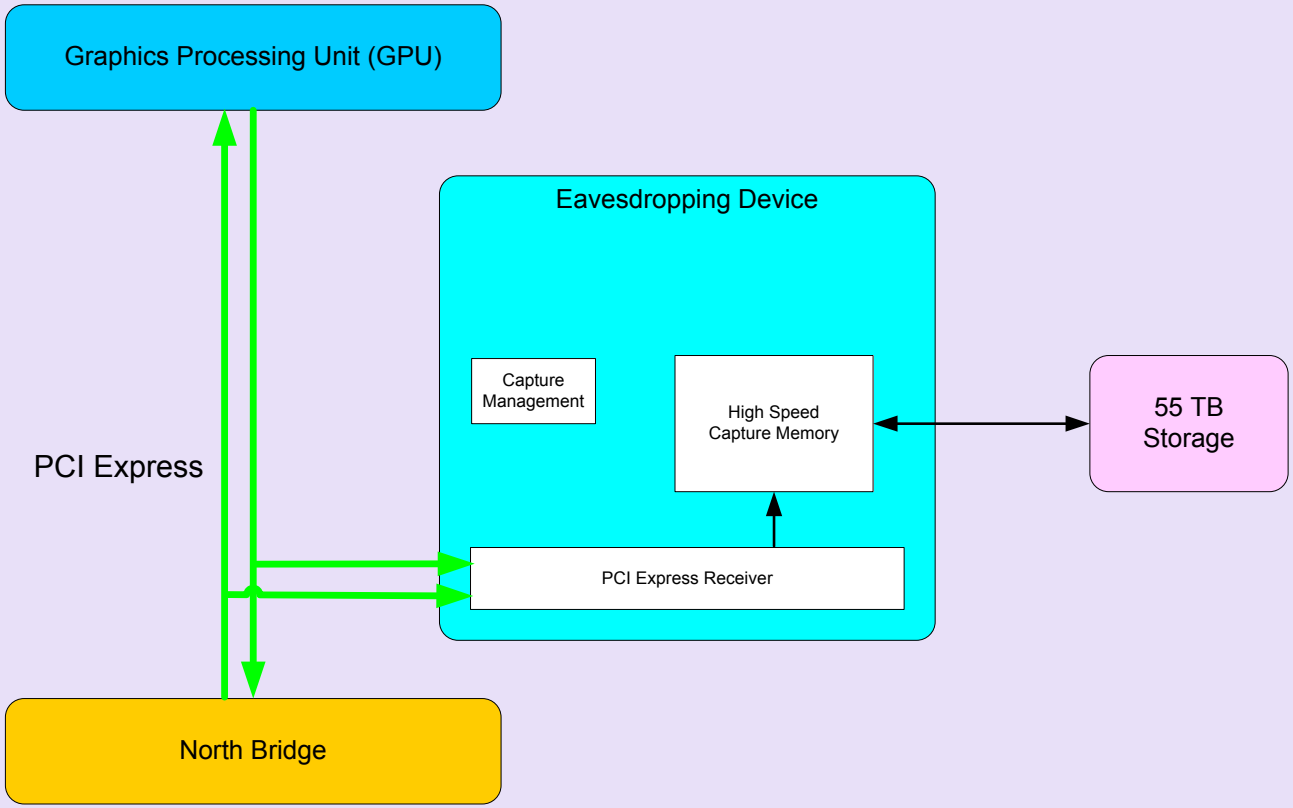
- Read requests are abstracted from their completions
- Completions can be out of order
- Eavesdropping device must re-associate the read data with the read request to make sense of completions

Power Management

- PCIe signals stop to save power
- Eavesdropping device must track these occurrences, and re-train as quickly as the communicating devices



Speculative Eavesdropping Device



- Capture at full speed rate
- Must not interfere electrically or the system will fail
- There is no professional tool that delivers this

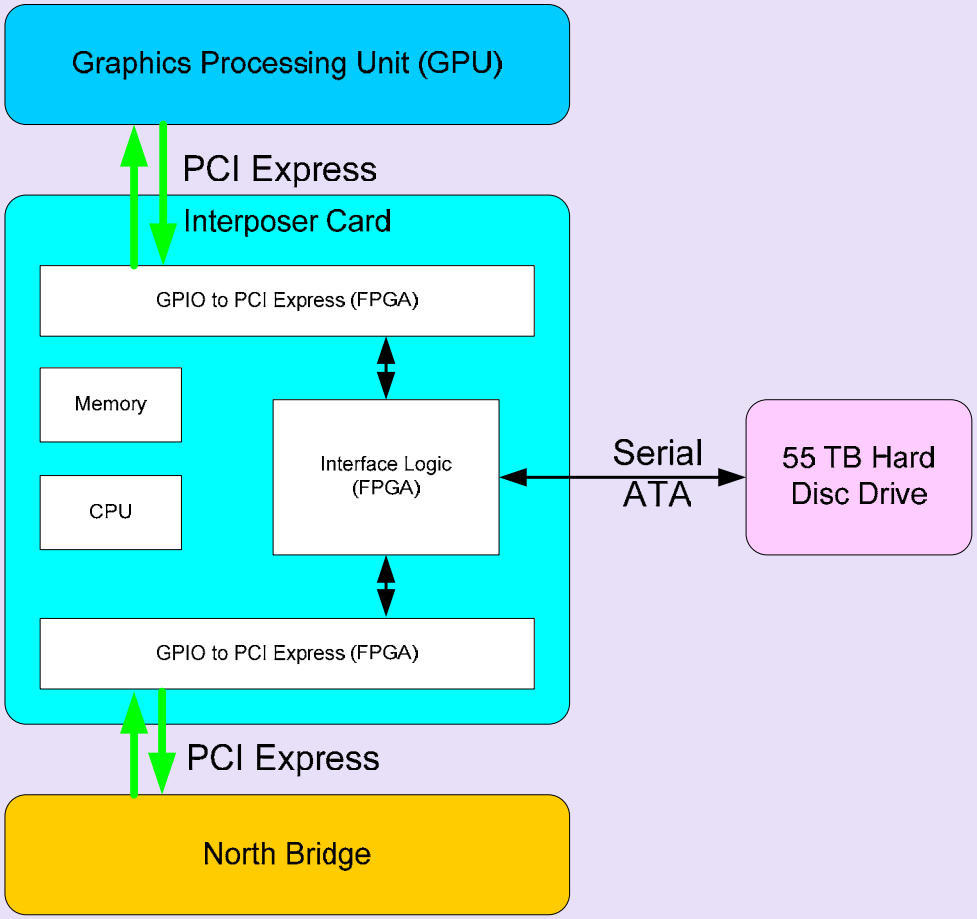
GPU Programming Model

- GPU is an extremely complicated processor
- GPU's programming interface is complex, unique, proprietary and non-public
- Data carried via PCI Express is proprietary and out or order
- Visual images are only part of the source material
- In addition to the extremely difficult task of capturing PCI Express transactions, an eavesdropping device must:
  - ✓ interpret captured PCIe data according to the GPU programming model,
  - ✓ capture the audio stream,
  - ✓ merge and synchronize it with the visual stream

Trusted Communication Channel

- Trusted Configuration Space
- Proprietary device authentication
- Allows software to distinguish between trusted and non-trusted devices and communication channels

Speculative Interposer Device



- Interposer must perform the practically impossible task of emulating the GPU and channel
- Practically impossible to capture content from the bus
- Few things in this life are impossible, but some things are very improbable

Conclusion

- The PCI Express interconnect is inherently robust, and that no additional features are required to prevent it from being snooped by the average user.
- It may be remotely possible that a malicious expert user with sufficient expertise, access to expensive tools and many man years of effort to eventually find a way to illegally snoop data in transit, but this scenario is deemed to be highly unlikely given its extreme technical challenges and infeasibility.
- To presume that communication across PCIe is straightforward and, therefore, vulnerable to the capture of protected content, is misinformed.

Thank you for attending the
PCI-SIG Developers Conference 2006.

For more information please go to
www.pcisig.com