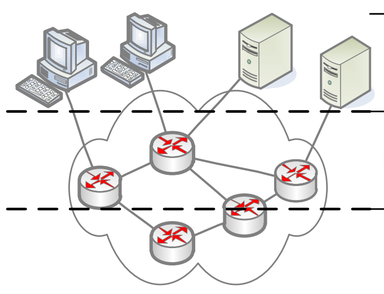
Securing the Router Infrastructure of the Internet

PIs: Tilman Wolf and Russell Tessier, University of Massachusetts Amherst
http://www.ecs.umass.edu/ece/wolf/

Vulnerabilities in Packet Processors of Modern Routers

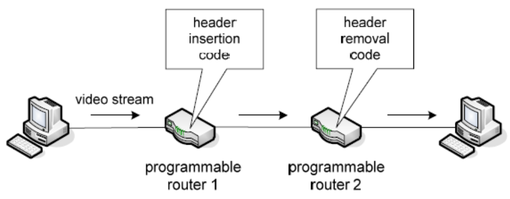
- Programmable data plane introduces **new type of attack**
  - Hacking of packet processing engine on router inside the network

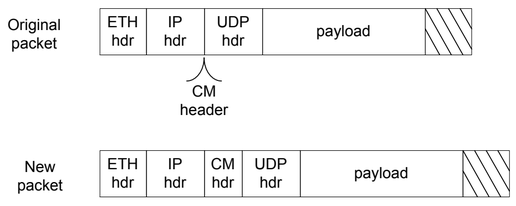


Attack target	Goal of attack	Attack examples	Defenses
End-system	Data access and modification	Hacking, phishing, espionage, etc.	Virus scanner, firewall, network intrusion detection system, etc.
	Denial-of-service	Denial-of-service attack via botnets, etc.	
Control plane	Data access and modificaiton	Malicious route announcement, DNS cache poisoning, etc.	Secure routing protocols (with cryptographic authentication), secure DNS (DNSSEC), etc.
	Denial-of-service	DNS recursion attack, etc.	
Data plane	Data access and modificaiton	Eavesdropping, man-in-the-middle attack, etc.	Secure network protocols (IPSec, TLS), etc.
	Denial-of-service	Exploit of vulnerable packet processing code	Processing monitor, etc.

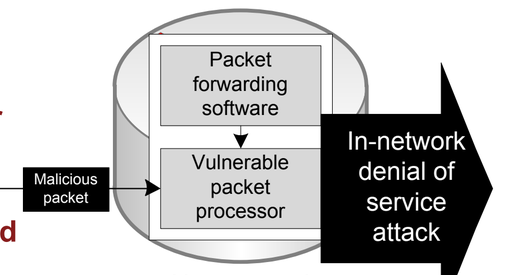
Focus of this work

- Many different potential vulnerabilities
  - We focus on **one example** to show that it is possible
  - Specific attack depends on system, software, etc.
- Requirements
  - Vulnerability must be **in packet processing code**
  - Vulnerability must be **triggered by data packet**
- Protocol processing: header insertion
  - Congestion management (CM) protocol

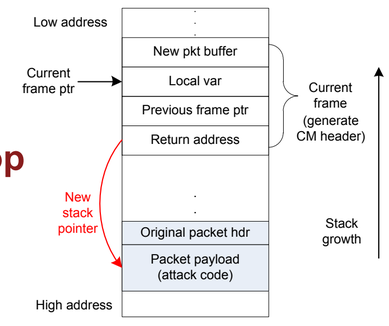


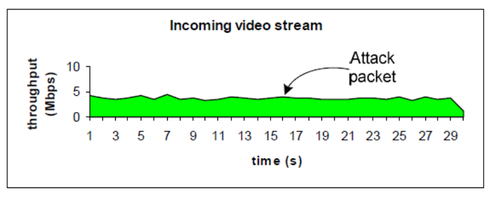


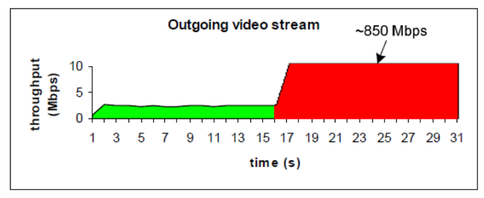
- Vulnerability can be exploited to launch attack
- **"In-network" denial of service attack**
  - Router has access to many links with high data rates
  - Potentially devastating impact
- Key questions
  - **Can such vulnerabilities occur** in packet processing code? (Yes, we show one example.)
  - **Can vulnerabilities be exploited** to launch DoS attack? (Yes for one processor type; no for another (crashed instead))



- Memory copy causes stack overwrite
  - Return address can be changed to attack code
- Attack code: **infinite transmission loop**
  - Devastating denial-of-service attack
- Prototype implementation
  - Custom network processor on NetFPGA



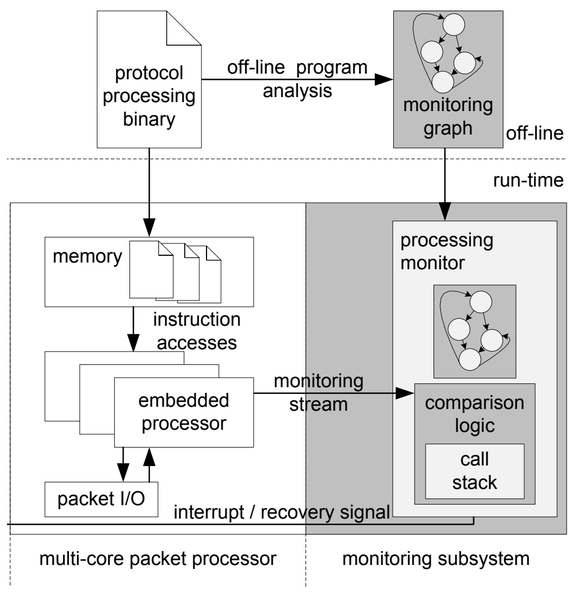




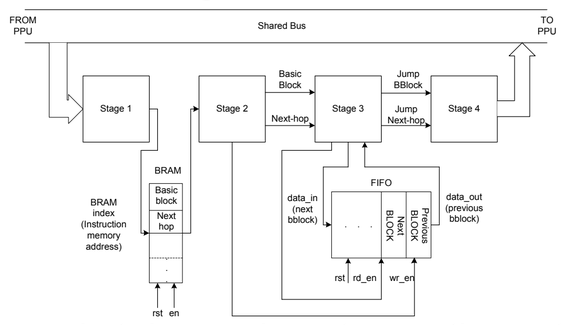
(b) Benign traffic and single attack packet on custom network processor

Embedded Hardware Monitor for Detecting Attacks

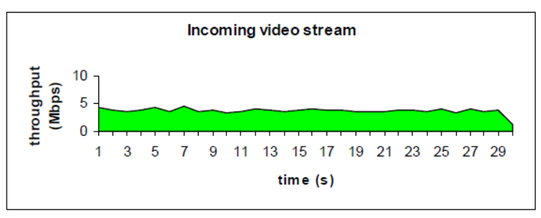
- Processing monitor tracks operation of single processor core
  - **Verifies that execution on processor occurs "as intended"**
- Functionality
  - Offline: **analysis of packet processing application**
    - "Monitoring graph" is model of application (10% size of binary)
  - Online: **verification of executed instructions**
    - Each instruction needs to match monitoring graph
  - **Invalid instruction: attack detected**
    - Trigger interrupt/recovery

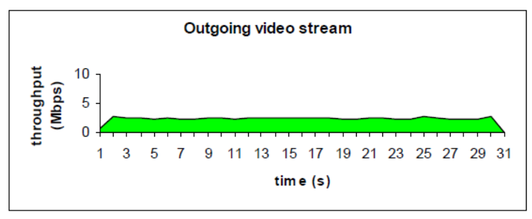


- NetFPGA implementation
  - **Single core, 4-way multithreading**
  - Pipelined monitoring based on **instruction address pattern**

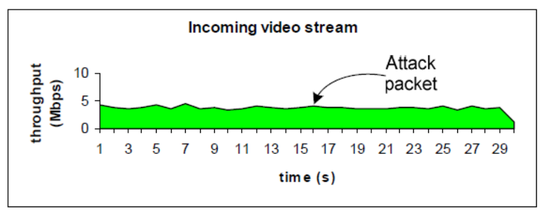


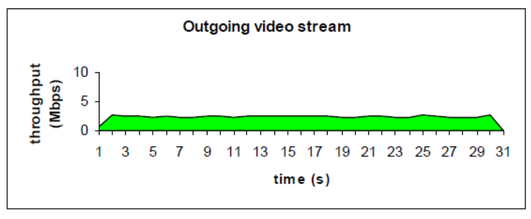
- Attack packet dropped, router continues to operate





(a) Benign network traffic





(b) Benign traffic and single attack packet

- Small amount of **extra logic and memory**

	Single Processor	Single core w/ Instr. level monitor
Slice LUTs	15,025	15,112
BRAM (RAMB16s)	124	130
detection time	NA	5 cycles
speed (MHz)	62.5	62.5
throughput(avg in Mbps)	67.2	64.1

Ongoing Research

- Hardware monitor operation
  - Current system based on non-deterministic finite automaton (NFA)
  - Developing deterministic finite automaton (DFA)
    - Higher performance, simpler monitor implementation
    - Requires pre-processing of monitoring graph
- Multicore system implementation
  - Four-core implementation on Altera FPGA system
  - Sharing of monitoring among cores to reduce overhead
- Secure download of monitoring graph
  - Important practical problem

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27–29th 2012
National Harbor, MD

UMASS AMHERST