Motivation for this class

- Internet hosts are often attacked
  - Internet worms and computer viruses spread quickly
    - SoBigF worm affected > 350,000 hosts by Aug 16, 2003
  - SPAM is Rampant
    - Over 50% of all email traffic

- Networks are Fast
  - Gigabit Network adapters widely available
    - PCI-based Gigabit NIC cards sold for under $40 from Best Buy
  - Backbone networks operate at multi-Gigabit/second rates
    - OC48 = 2.4 Gigabits/second and faster

- Solution: Need Hardware-accelerated
  - Firewall on a Chip
  - Network Intrusion Detection
  - Network Intrusion Prevention
Providing Network Security in Hardware

- Make it suitable for network-wide deployment
  - Fast (Gigabit+ throughput)
  - Small (Single-chip solution)

- Have it implement baseline functionality
  - Scan Internet headers and payload

- Enable it to perform additional features
  - Extensible modules in reconfigurable hardware

- Let it be easy to use
  - Provide web-based control and configuration menus

Solution Platform

- Field-programmable Port Extender (FPX) platform
- Dynamically reconfigurable hardware
- Reconfigurable hardware implements all header, payload, and traffic flow processing
Configuration to process real traffic

- Fiber-optic Uplink
- Fast Ethernet Switch
- Protected Host(s)
- Content-Aware, Firewall
- Internet
- Wide Area Network Router / Switch
- FPX running SOPC firewall

Internet Protocol (IP) Packet Header

- Specifies Source & Destination Address
- Transfers up to 64kB of data

<table>
<thead>
<tr>
<th>ver</th>
<th>IHL</th>
<th>service type</th>
<th>total length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>identification</td>
<td>flags fragment offset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ttl</td>
<td>protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>source address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>options</td>
<td>padding</td>
<td></td>
</tr>
</tbody>
</table>
Sample Internet Packet Header

- Source Address = 128.252.5.5 (dotted.decimal)
- Destination Address = 141.142.2.2 (dotted.decimal)
- Source Port = 4096 (decimal)
- Destination Port = 80 (decimal)
- Protocol = TCP (6)

```
103  72  71  40  39  8  7  0
Src IP (hex) = 80FC0505
Dest IP (hex) = 8D8E0202
Src Port = 1000
Dest Port = 0050
Proto = 06
```

Sample Header Matching Rule

- Packet “matches” if following conditions met:
  - Source Address = 128.252.0.0 / 16
  - Destination Address = 141.142.0.0 / 16
  - Source Port = Don’t Care
  - Destination Port = 80
  - Protocol = TCP (6)

```
Src IP value = 80FC0000
Dest IP (hex) = 8D8E0000
Src Port = 0000
Dest Port = 50
Proto = 06
```

```
Src IP (hex) = FFFF0000
Dest IP (hex) = FFFF0000
Src Port = 0000
Dest Port = FFFF
Proto = FF
```

Value:
- 1 = care
- 0 = don’t care

Mask:
- 1 = care
- 0 = don’t care
Matching w/Ternary Content Addressable Memory (TCAM)

- CAM MASK [1]
- CAM VALUE [1]
- CAM MASK [2]
- CAM VALUE [2]
- CAM MASK [3]
- CAM VALUE [3]
- CAM MASK [N]
- CAM VALUE [N]

Flow ID [1]
- 16 bits

Flow ID [2]
- 16 bits

Flow ID [3]
- 16 bits

Flow ID [N]
- 16 bits

Flow List

Priority Encoder

Mask Matchers

Value Comparators

Payload

Match Bits

Source Address

Destination Address

Protocol

Bits in IP Header

Sample Keywords in packet payloads

- **General SPAM**
  - "(A|a)(M|m)(A|a)(Z|z)(l|i)(N|n)(G|g)"
  - "CALL NOW"
  - "(L|l)imited (T|t)ime (O|o)ffer"

- **Save Money SPAM**
  - "(C|c)onsolidate"
  - "(F|f)(U|u)(F|f)(U|u)(N|n)(D|d)"

- **Fast Money SPAM**
  - "MAKE MONEY FAST"
  - "(W|w)ork from home"

- **Chains and Forwards**
  - "Read this"
  - "FWD"

- **Jokes**
  - "(J|j)oke"
  - "walks into bar"

- **Work List**
  - "(H|h)omework"
  - "(M|m)achine (P|p)roblem"
  - "(C|c)(S|s)536"
  - "Lockwood"
  - "Washington University"

- **Personal List**
  - "(M|m)om"
  - "(D|d)ad"
  - "(C|c)all (H|h)ome"

- **Urgent**
  - "(U|u)(R|r)(G|g)(E|e)(N|n)(T|t)"
  - "Emergency"
FPgrep Module

Increased Throughput via Parallelism
Content Matching Module

Regular Expression (RE) Matching Circuit

Data Input 32 → 32 Data Output

Content Match Vector

Architecture of a System-On-Chip Firewall

Xilinx XCV2000E FPGA
Payload Scanner
TCAM Filter
Extensible Module(s)
Flow Buffer
Flow ID
Payload Match Bits
Interfaces to Off-Chip Memories
SDRAM 2 Controller
SDRAM 1 Controller
Free List Manager
SRAM 1 Controller
Queue Manager
Packet Scheduler

Layered Internet Protocol Wrappers

(Implemented in CS 536, Fall 2002)
**SOC-Firewall FPGA Layout**

- Layered Protocol Wrappers
- Per-flow Queuing
- Memory Controller

**Field programmable Port Extender (FPX)**

- Off-chip Memories
- RAD Program SRAM
- NID Program PROM
- SelectMAP Reconfiguration Interface
- Reconfigurable Application Device (RAD) FPGA
- Network Interface Device (NID) FPGA

Subnet A, Subnet B

2.4 Gigabit/sec Network Interfaces
Sample Waveform of Packet through Hardware

Input and Output Packets

- Shows input packets
- Shows output packets
- Displays packets as HTML tables with color coded header fields
Process to Build Custom Firewalls

Hardware Developer

Uploads extensible Plug-in modules

Module Collector

Module Library

Selects modules for custom firewall

SOPC Generator

Customized SoC Bitfile

Module Parameters

Network Administrator

Web-based Integration Tool

Select extensible components to integrate into SOC Firewall:

- Content Base Image Filter
  - Replace nothing
  - tbr: 9, slice: 10
  - SRAM = 0, SDRAM = 1

- Bloom Filter
  - Replace queue
  - bkr: 11, slice: 9
  - SRAM = 1, SDRAM = 0

- Self-Scheduled Fair Queuing
  - Replace queue
  - bkr: 9, slice: 9
  - SRAM = 0, SDRAM = 1

- Deep Classifier
  - Replace cam
  - bkr: 12, slice: 30
  - SRAM = 1, SDRAM = 0

- Control Packet Security
  - Replace nothing
  - bkr: 15, slice: 1
  - SRAM = 1, SDRAM = 0

- Block RAM Utilization
- Slice Utilization
- SRAM Utilization (of available 2)
- SDRAM Utilization (of available 3)
- nothing

Submit: Please
Reconfigure hardware over network

New module developed

Content Matching Server generates
New module in
programmable
Logic

Module Bitfile
transmitted
over network

Internet

New module
deployed into
FPX hardware

Module

Bitfile

transmitted

over network