The Need for Internet Security

- Internet Worms and Virus Attacks
  - Annoyance to users
  - Costly to businesses (lost productivity)
  - Security threat to government (compromised data)

- Recent Attacks
  - Nimda, Code Red, Slammer
  - MSBlast
    - Infected over 350,000 hosts in Aug. 16, 2003
  - SoBigF
    - Infected 1 million users in first 24 hours
    - Infected > 200 million in the first week
    - Caused an estimated $1 billion in damages to repair.

- Detectable by a Signature in Content
  - Pattern of bytes
  - Regular Expression
  - Morphable pattern
Challenges to Stopping Worm and Virus Attacks

- End-systems difficult to maintain
  - Operating systems become outdated
  - Users introduce new machines on network

- Internet contains several types of traffic
  - Web, file transfers, telnet
  - Data may appear anywhere in the packet

- Networks process High Speed Data
  - Multi Gigabit/second data transmission rates now commonplace in campus, corporate, and backbone networks
  - Peer-to-Peer protocols dominate current and future traffic
  - Need Real-time gathering
    - No latency can be tolerated

Virus/Worm/Data Spread in Unprotected Networks
Virus/Worm/Data Spread in Unprotected Networks
Virus/Worm/Data Spread in Unprotected Networks

Virus/Worm/Data Containment in Protected Networks

Content Scanning and Protection Device
Complete Protection System

Network Aggregation Point (NAP)

Switch/Concentrator

Global Velocity DED

Router/Switch

Data

Regional Transaction Processor (RTP)

Data

Content Matching Server (CMS)/Central Storage and Backup System (CSBS)

Content Scanning Technology

- Fiber optic Line Cards
  - Gigabit Ethernet
  - ATM OC-3 to OC-48

- Reconfigurable Hardware
  - Uses Field Programmable Port Extender (FPX) Platform
  - Protocol processing and content scanning performed in hardware
  - Reconfigurable over the network

- Chassis/Motherboard
  - Allows Modules to Stack
Field-programmable Port Extender (FPX)

Regular Expression Matching with Finite Automata

Moscola et al.
Selecting the Search Strings

Edit Search strings

Manage DED Library

Click "ADD" to generate a new entry.

search_string: HEK@6303432739

description: 5-Digis Internet Worm (MINE54)

Author: 16

Value: 11.00
Data Scanning Technologies

- Protocol Processing
  - Layered Protocol Wrappers
  - Process Cells/frames/packets/flows in hardware

- Regular Expression Matching
  - Deterministic Finite Automata (DFA)
  - Dynamically programmed into FPGA logic

- Fixed String Matching
  - Bloom Filters
  - Dynamically programmed into BlockRAMs

Program the Hardware
Remotely reprogramming hardware over the network

New module developed

Content Matching Server generates
New module in programmable Logic

Module Bitfile transmitted over network

New module deployed into FPX hardware

Network Configuration with Gigabit Ethernet

Data Enabling Device (DED) with FPX Processing Modules
Active Virus Protection

Content returns from infected host

Content is processed in the FPX

Content containing virus is dropped at FPX

Alert packet is sent to user to let them know of the virus

(1) Data requested from public Internet

Internet User

Virus Agent

The message you are attempting to download contains a virus and has been halted.

To ensure the protection of your system, you should click the Stop button on your browser and click OK.

OK

Active Virus Example
Other Applications

- Protect Confidential Information with a corporate network
- Secure Classified documents
- Guard against liability for copyright infringement
- Lock medical documents for Health Insurance Portability and Accountability Act (HIPAA)