



Security for Internet Infrastructure

John W. Lockwood
Assistant Professor of
Computer Science and Engineering



lockwood@arl.wustl.edu
<http://www.arl.wustl.edu/~lockwood>

Research sponsor:



<http://www.globalvelocity.info/>



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



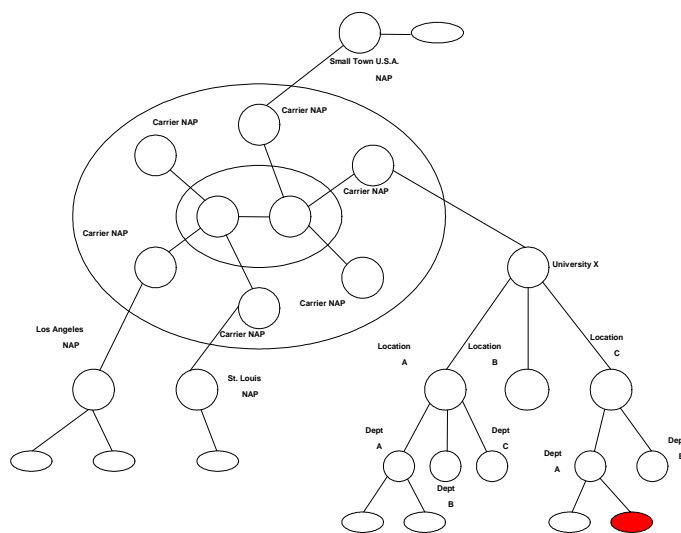


Challenges to Stopping Worm and Virus Attacks

- 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

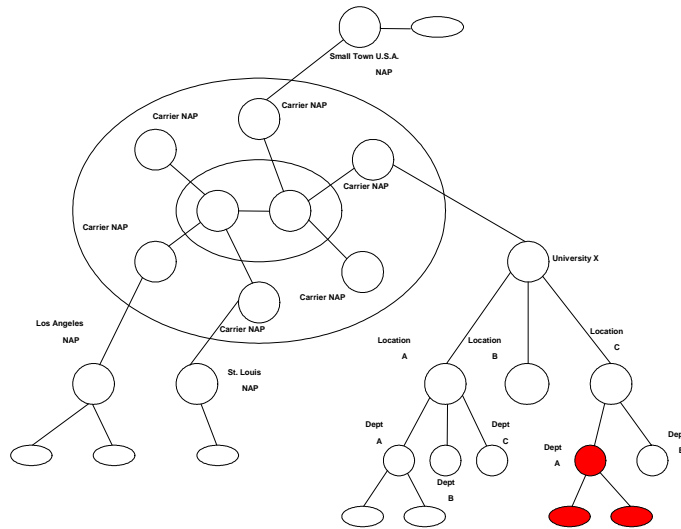


Virus/Worm/Data Spread in Unprotected Networks

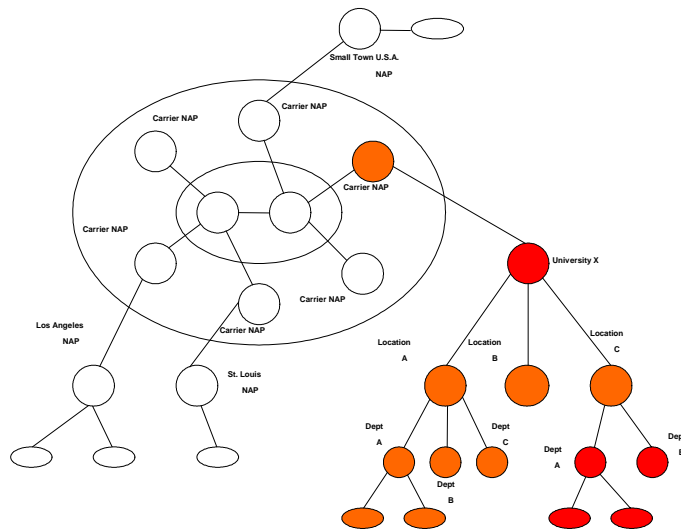




Virus/Worm/Data Spread in Unprotected Networks

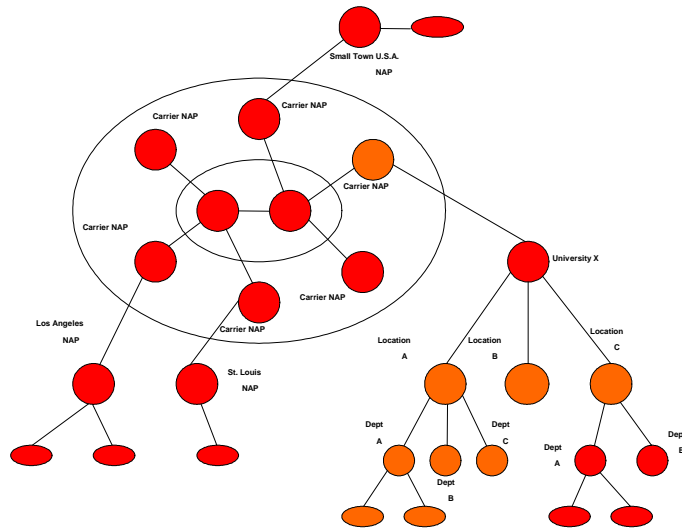


Virus/Worm/Data Spread in Unprotected Networks

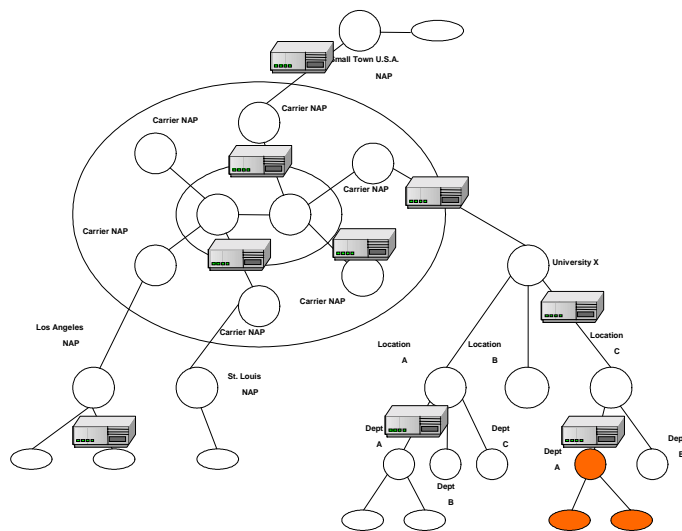




Virus/Worm/Data Spread in Unprotected Networks



Virus/Worm/Data Containment in Protected Networks

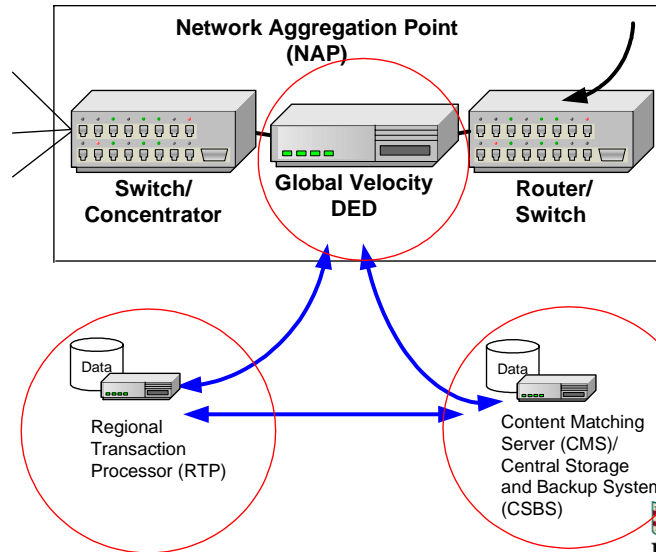


Content Scanning and Protection Device





Complete Protection System

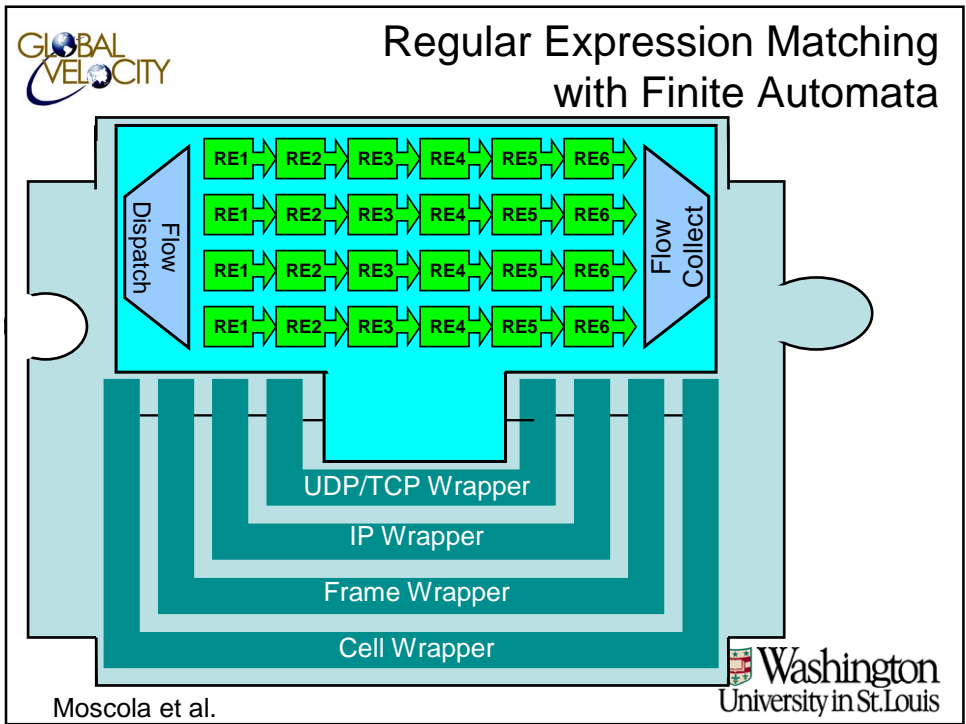
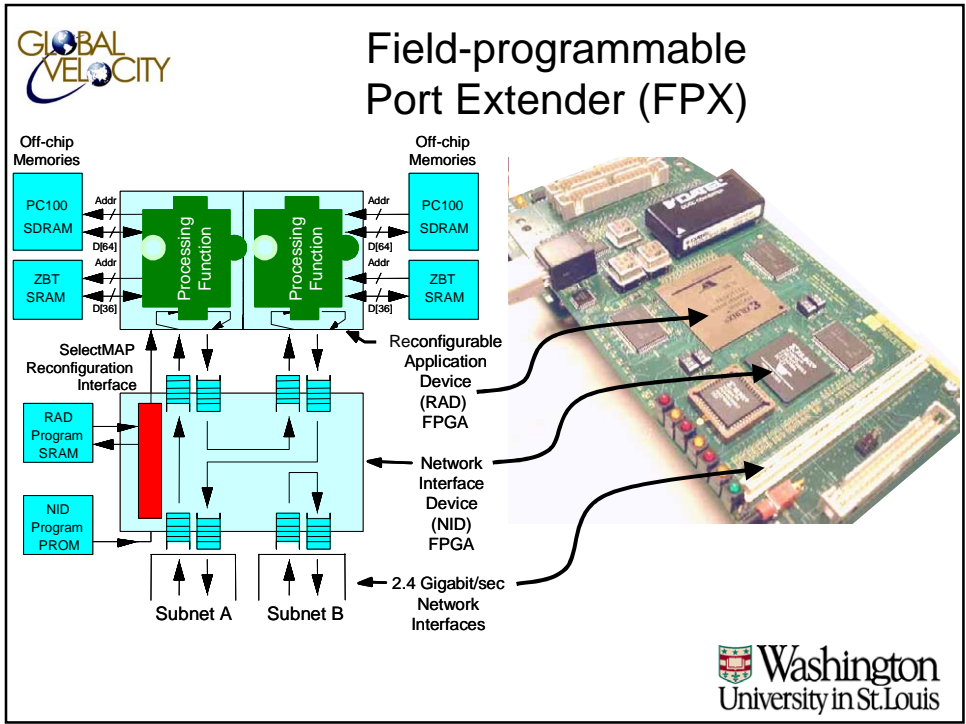


Content Scanning Technology



- 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







Selecting the Search Strings

Address: http://192.168.50.50/view_property.php

Select	Edit	Delete	Id	Search String	Description	Author	Value
<input type="checkbox"/>	EDIT	DELETE	17	IHEX(6c744e5076)	Clear and Present Danger	9	3.00
<input type="checkbox"/>	EDIT	DELETE	6	ViRuS	An Email Virus	15	5.00
<input type="checkbox"/>	EDIT	DELETE	13	Copyright.* WashU	WashU Copyright	12	1.00
<input type="checkbox"/>	EDIT	DELETE	128	(L l)(A a)(D d)(E e)(N n)	Terrorist Last Name	5	100.00
<input type="checkbox"/>	EDIT	DELETE	127	(O o)sama	Terrorist First Name	5	5.00
<input type="checkbox"/>	EDIT	DELETE	112	Patient (Confidential Record)	Confidential Information	17	5.00
<input type="checkbox"/>	EDIT	DELETE	113	Medical (Information Record)	Medical Record	17	5.00
<input type="checkbox"/>	EDIT	DELETE	114	Do Not (Distribute Release)	Confidential Information	17	5.00
<input type="checkbox"/>	EDIT	DELETE	129	IHEX(1B688E6D)	Internet Worm	19	6.00
<input type="checkbox"/>	EDIT	DELETE	130	NASA (C c) (onfidential ONFIDENTIAL)	Confidential Information	20	5.00
<input type="checkbox"/>	EDIT	DELETE	133	IHEX(683063423739)	SoBigF Internet Worm (MIME64)	16	11.00



Edit Search strings

Address: http://192.168.50.50/aed_property.php?key=133&op=1

SYSTEM OVERVIEW PROGRAM DED MANAGE ACCOUNTS ONLINE SUPPORT

Manage DED Library

Manage DED Library

Click "ADD" to generate a new entry.

search_string: IHEX(683063423739)

description: SoBigF Internet Worm (MIME64)

Author: 16

Value: 11.00

Update Entry



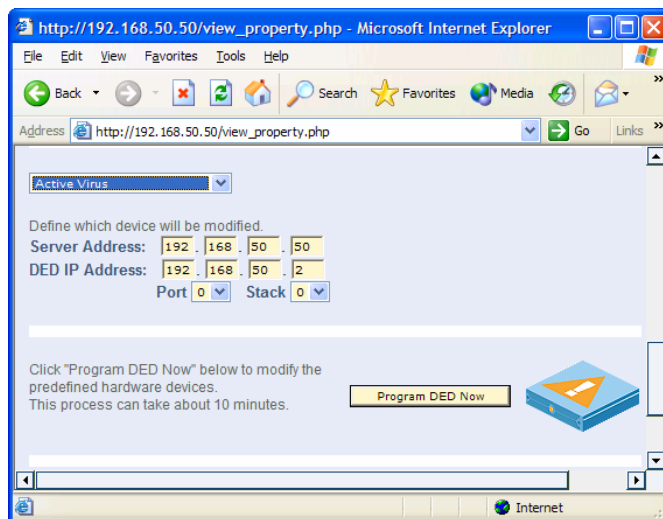


Data Scanning Technologies

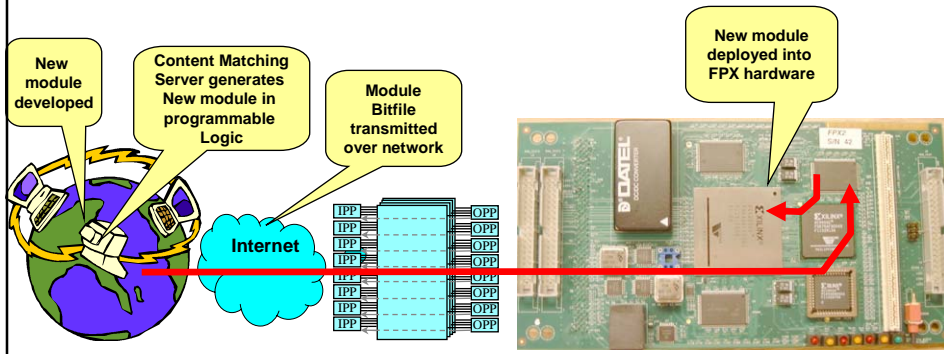
- Protocol Processing
 - Layered Protocol Wrappers
 - Process Cells/frames/packets/flows in hardware
- Regular Expression Matching
 - Deterministic Finite Automata (DFA)
 - Dynamically programmed into FPGA logic
- Fixed String Matching
 - Bloom Filters
 - Dynamically programmed into BlockRAMs



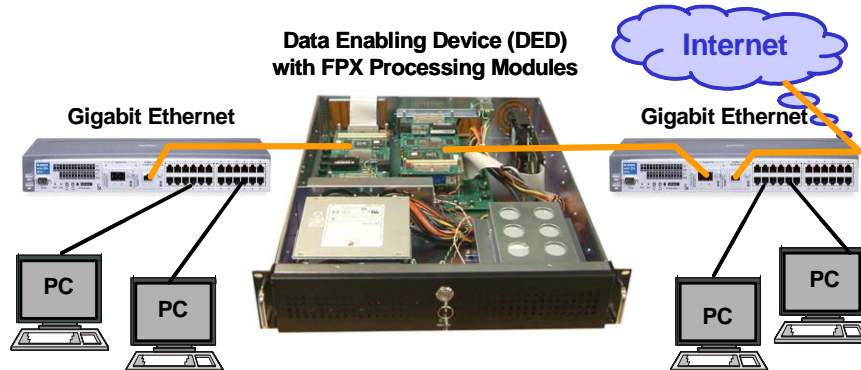
Program the Hardware



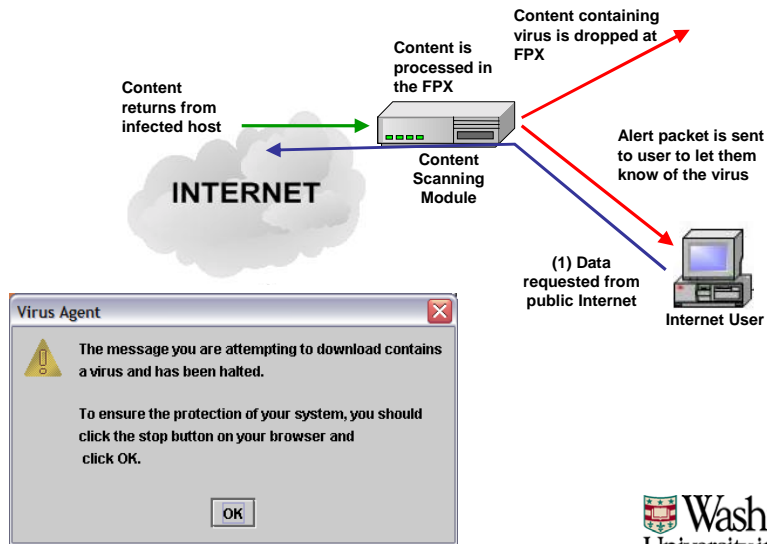
Remotely reprogramming hardware over the network



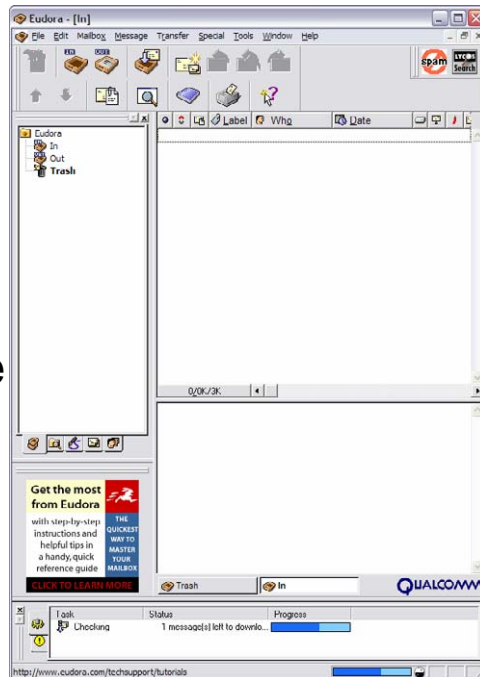
Network Configuration with Gigabit Ethernet



Active Virus Protection



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)

