Containment of Internet Worms and Computer Viruses with Content Filters

Washington University
Fall 2003

http://www.arl.wustl.edu/arl/projects/fpx/cse535/

Copyright 2003, John W Lockwood
Lockwood@arl.wustl.edu

Virus/Worm/Data Spread in Unprotected Networks
Virus/Worm/Data Spread in Unprotected Networks
Virus/Worm/Data Spread in Unprotected Networks
Mitigation of Worm Threat

- **Prevention**
  - Need better software engineering practices
  - Socio-economic conditions currently ensure homogeneous set of software

- **Treatment**
  - Disinfection tools (Norton, McAfee)
  - System Update in Windows
  - Security update can take DAYS to code

- **Containment**
  - Approach of this system.

---

Possible Technologies for Containment

- **Possible Technologies**
  - Firewalls
  - Content filters
  - Blacklist

- **Ad-hoc Containment methods**
  - used manually to contain Code Red
  - Block inbound access to port 80
  - Blacklisting of infected computers
  - Content filtering of data with Code Red signatures

---

From: Internet Quarantine: Requirements for Containing Self-Propagating Code
By: David Moore, Colleen Shannon, Geoffrey M. Voelker, Stefan Savage, IEEE INFOCOM 2003
Containment can Work

- Detection is easier than Prevention
  - Containment system does not need to understand how the worm itself works

- Containment can be deployed incrementally
  - Does not require universal deployment

- Effectiveness Depends on
  - Time to Detect and React
  - Strategy used to ID and contain pathogen
  - Breadth and placement of system deployment

Idealized Deployment

(a) Address Blacklisting

(b) Content Filtering
Required Reaction Time for Address Blacklisting and Content Filtering

(a) Address Blacklisting

(b) Content Filtering

Containment System

Internet

Network Intrusion Prevention
Virus/Worm/Data Containment in Protected Networks

Content Scanning and Protection Device
Virus/Worm/Data Containment in Protected Networks

Network Configuration

Ethernet switch with ATM uplink

Data Enabling Device (DED) with FPX Processing Modules

Internet
Content Scanning Technology

- Fiber optic Line Cards
  - Gigabit Ethernet
  - ATM (IP over AAL5)

- Reconfigurable Hardware
  - Uses Field Programmable Port Extender (FPX) Platform
  - Protocols processed in hardware
  - Custom Finite State Machine (FSMs) scan packets
  - Reconfigurable over the network

- Chassis / Motherboard
  - Allows Modules to Stack

Complete Protection System

Network Aggregation Point

Switch/Concentrator
Content Scanner
Router/Switch

Data
Transaction Processor
Content Matching Server

Data
Hardware Generation Interface

Add expression to database

Expressions that are programmed into the hardware

Applications for the circuit

Specify where to send log/alert messages

Specify which device to reprogram

One-step process to run CAD tools that build circuit and program FPGA

Edit Search strings

Manage DED Library

Click "ADD" to generate a new entry.

search_string: HEX(630363423739)
description: SoBigF Internet Worm (MME54)
Author: 16
Value: 11.00

Manage DED library
Programming the DED

Configuration of Content Scanning Module

UDP/TCP Wrapper
IP Wrapper
Frame Wrapper
Cell Wrapper
Implementation of Content Scanner on Field programmable Port Extender (FPX)

Remotely reprogram hardware over network
Active Virus Protection

Content returns from infected host

INTERNET

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

Active Virus Example

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
Modular Design Flow

Front End: Specify Regular Expression (Web, PHP)

Back End (1): Extract Search terms from SQL database

Back End (2): Generate Finite State Machines in VHDL

Synthesize Logic to gates & flops (Synplicity Pro)

Set Boundary I/O & Routing Constraints (DHP)

Place and Route with constraints (Xilinx)

Generate bitstream (Xilinx)

Install and deploy modules over Internet to remote scanners (NCHARGE)

In-System Data Scanning on FPX Platform

New, 2 Million-gate Packet Scanner: (9 Minutes)

Content Filter Containment = F( Reaction Time, Probe Rate)

Graph From: Internet Quarantine: Requirements for Containing Self-Propagating Code. By: David Moore, Colleen Shannon, Geoffrey M. Voelker, Stefan Savage. IEEE INFOCOM 2003