

# Bloom Filters for String Matching



Michael Attyg, Sarang Dharmapurikar, and John W. Lockwood: <http://www.arl.wustl.edu/projects/fpx/reconfig.htm>

## The Problem

How do you efficiently scan for and filter tens of thousands of strings to:

- Filter latest virus / worm
- Protect sensitive information
- Alert network administrator of security threat
- How do you quickly change search criteria?
- Virus/Worm applications are a rapidly evolving threat
- Quick reaction times are absolutely necessary!

## Who Cares about String Matching?

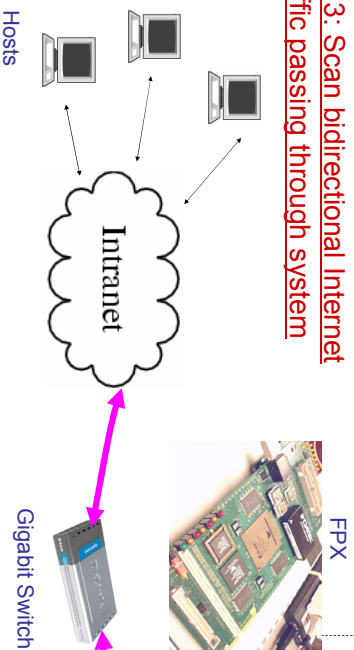
- Network Administrators
- Organizations that use the Internet
- Governments with classified secrets
- Corporations with proprietary information



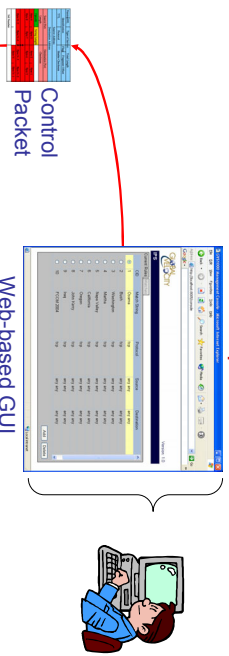
## The Solution

- A device has been developed at Washington University that:
- Scans for and blocks Internet traffic containing offending signatures
- Begins searching for over 10,000 variable length strings within milliseconds of coming online
- Generates alert messages to notify a network administrator
- Utilizes technology that is compatible with local and wide-area networks (Internet Protocol)

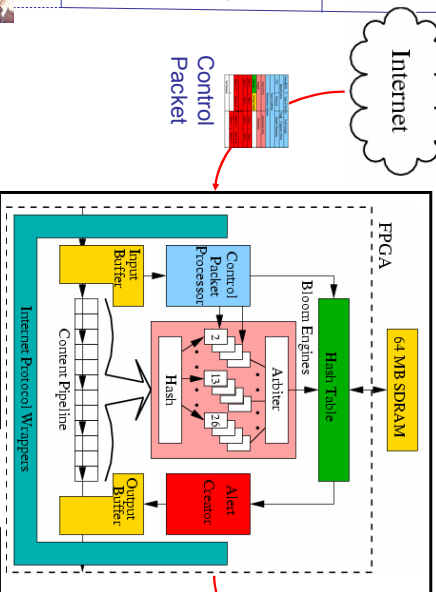
## Step 3: Scan bidirectional Internet traffic passing through system



## Step 1: Program signatures into hardware via UDP control packets



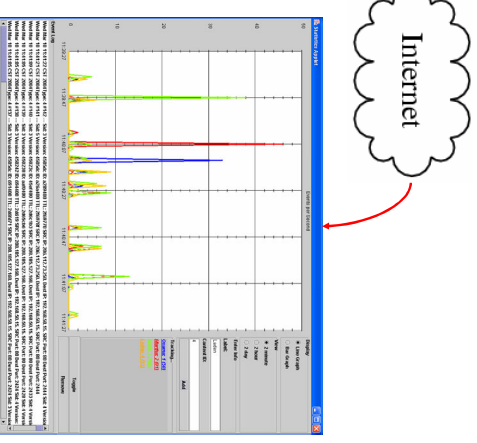
## Step 2: Program Bloom filters and hash table to detect signatures



## Operation Summary

1. Signatures converted to UDP control packets
2. Control packets sent to the hardware system
  - Bloom Filters and Hash Table programmed
3. Scanning of Internet traffic begins immediately
4. String matches generate alert messages
  - Software controller processes alerts

## Step 4: Act on alert messages



Alerts sent to end users & network administrators  
String matches per second displayed

## Commercialization

Global Velocity, located in St. Louis MO, has an exclusive license to the high-speed network content scanning technology. They are actively commercializing the technology. Markets include governmental agencies, universities, and corporations for network infrastructure protection and intelligence applications.  
<http://www.globalvelocity.info/>

