Internet Worm and Virus Protection with Extensible Networks

John W. Lockwood: lockwood@arl.wustl.edu, and the ARL Reconfigurable Networking Hardware Group: http://www.arl.wustl.edu/arl/projects/fpx/reconfig.htm

The Problem

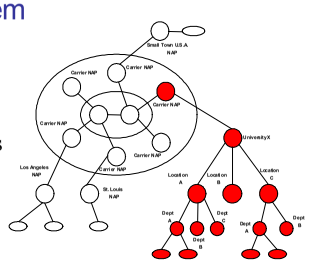
Computer virus infections are spreading

- New virus spread quickly though email, web, and peer-to-peer tools

Confidential Data is leaking through networks

- Government secrets, personal data, and corporate information are stolen

Internet infrastructure is at risk



Who Cares ?

Who cares about computer virus infections ?

- People that own a business with a network
- Organizations that use the Internet

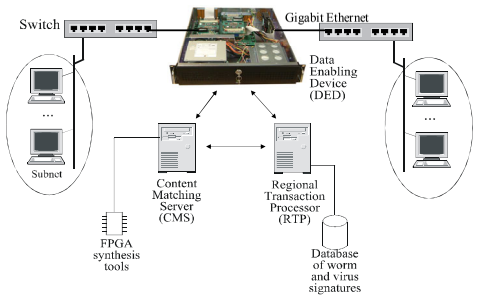
Who cares about confidential data leaks ?

- Governments with classified secrets
- Corporations with proprietary information

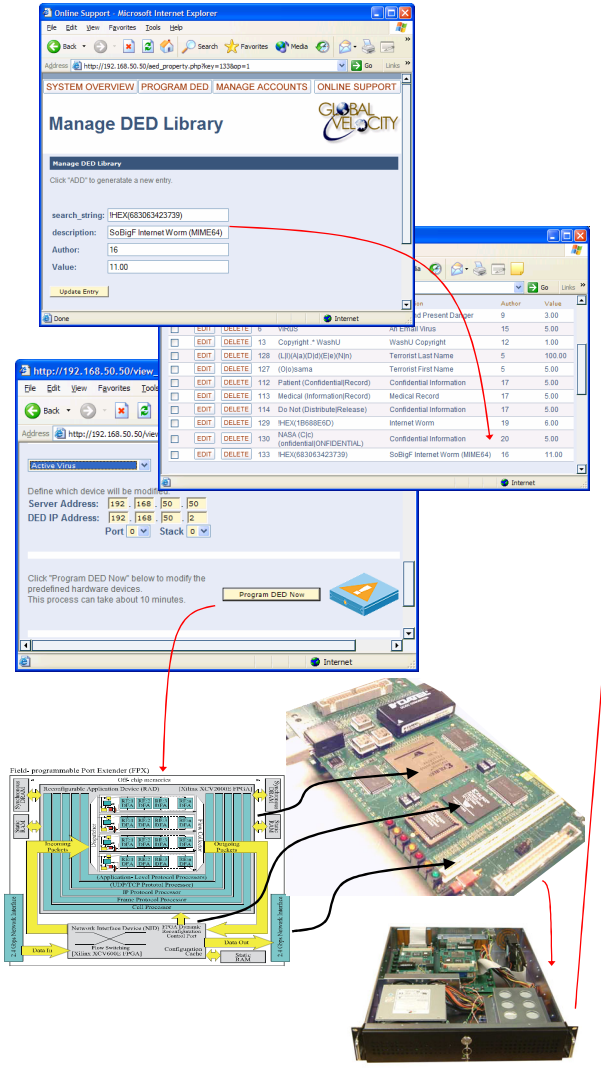
How can networks be made safe ?

A device has been developed at Washington University that:

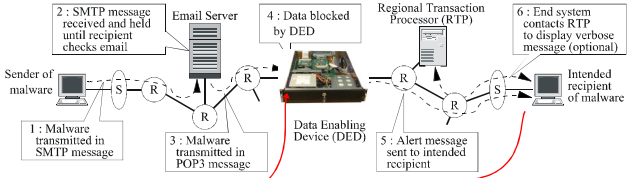
- Identifies & acts on content in Internet packets at high speed (Gigabits/second) without delay (real-time)
- Scans and blocks network traffic using reconfigurable hardware at speeds up to 100x faster than could be done in software
- Utilizes technology is compatible with Local and wide-area networks (Internet Protocol)



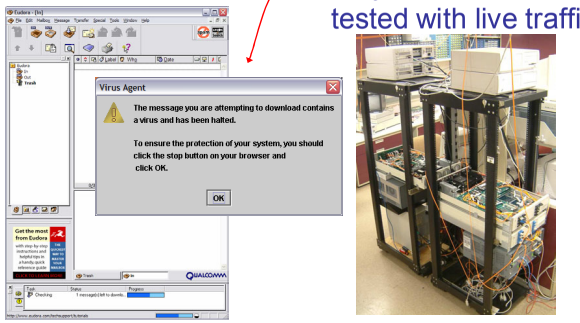
How it works: An automated design flow builds FPGA hardware that is dynamically deployed to scan and block malicious network content



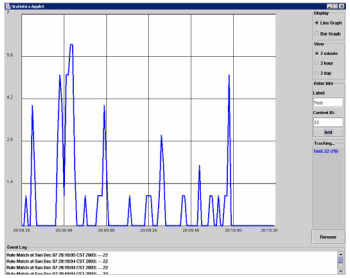
Technology has Many Applications



System has been tested with live traffic



Alerts sent to end users & network administrators



Intelligent gateways are easily deployed

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/