

# Insecure Networks

John W. Lockwood

[lockwood@arl.wustl.edu](mailto:lockwood@arl.wustl.edu)

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

With slides from members of the  
Reconfigurable Networking Group

<http://www.arl.wustl.edu/arl/projects/fpx/reconfig.htm>

Presentation for:  
Society of Women Engineers,  
St. Louis, MO

November 9, 2004

John W. Lockwood



## Protect your innocent computer

- Install Anti-Virus software
  - McAfee, Symantec
- Use Firewalls
  - Provides some protection
- Read usage agreements carefully
  - Avoid using software with broad agreements
- Install security updates
  - Automatic updates are good
- Use caution with email attachments
  - Text-only is good
- Watch for unusual activity
  - Slow, unresponsive machines are suspect
- Vary use of passwords
  - Don't let one compromised account others

John W. Lockwood



# Avoid the Phishing scam

- Email received pretending to be from CitiBank

From: "Citi" <antifraud\_deptmnt.ref.num269841054@citibank.com>

To: csf@cse.wustl.edu

Subject: IMPORTANT ACCOUNT NOTICE FROM CITIBANK

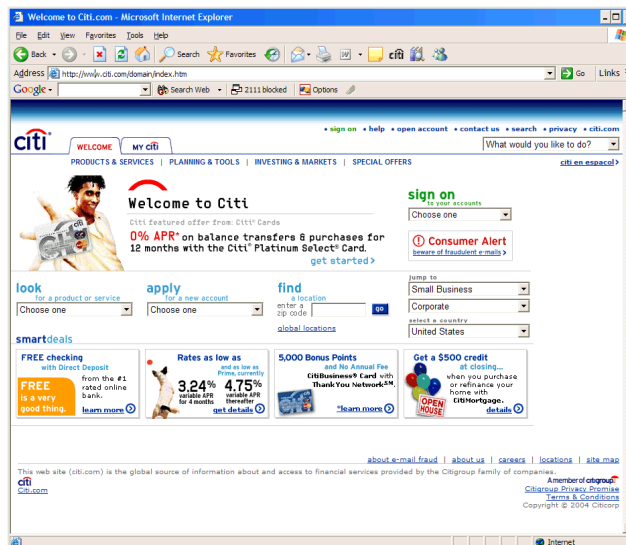
Date: Mon, 08 Nov 2004 23:47:21 +0300



John W. Lockwood



# Is this really the Citibank homepage?

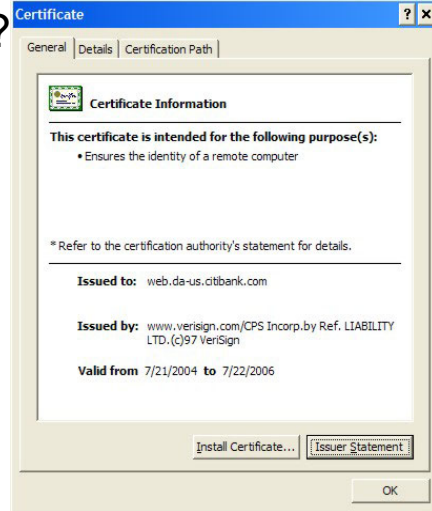


John W. Lockwood



# What does this certificate mean?

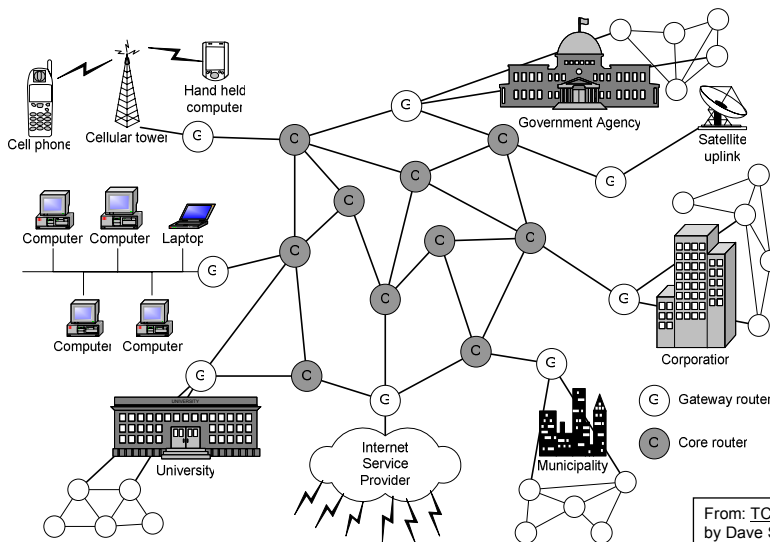
- Is this certificate valid?
- Does the certificate identify CitiBank?
- Should you trust this webpage and submit personal information?



John W. Lockwood



# Protect the Internet



John W. Lockwood



## Worms can exploit security

- Someone writes an Internet worm or computer virus that exploits a vulnerability in:
  - An operating system,
  - System utility, and/or
  - Commonplace application
- They let worm spread throughout Internet
  - Self-propagating code enables it to spread automatically
- They execute their code on your computer
  - As well as a million others ..

From: How to Own the Internet in Your Spare Time,  
by Stuart Staniford, Vern Paxson, Nicholas Weaver;  
Proceedings of the 11th USENIX Security Symposium  
(Security '02).

John W. Lockwood



## What someone could do with a Million Computers

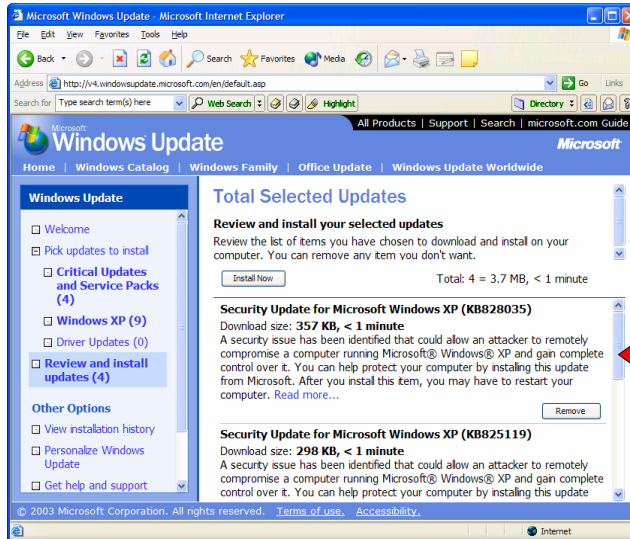
- Launch Distributed Denial of Service (DDoS) attacks
  - Bring down Electronic commerce sites
  - Cut off News outlets
  - Disable Root name servers
  - Disrupt Government sites
- Access Sensitive Material on any host
  - Access passwords
  - Obtain credit card numbers
  - Read address books
- Sow Confusion and Disruption
  - Send out false information
  - Make messages appear authentic

From: How to Own the Internet in Your Spare Time,  
by Stuart Staniford, Vern Paxson,  
Nicholas Weaver,  
Proceedings of the 11th USENIX  
Security Symposium  
(Security '02).

John W. Lockwood



# End system remain insecure



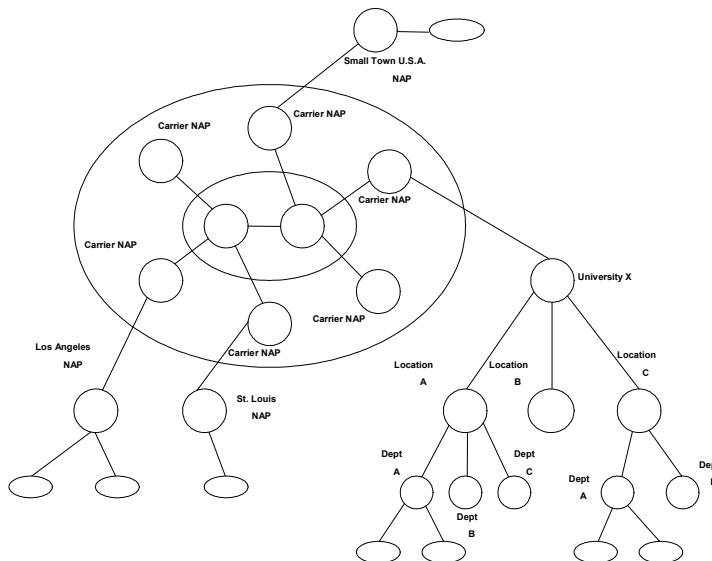
- Microsoft Windows XP
- Oct 2003
- 4 updates of *just this week* for known vulnerabilities

Do you Consider this to be acceptable security?

John W. Lockwood



# Virus/Worm/Data Spread in Unprotected Networks

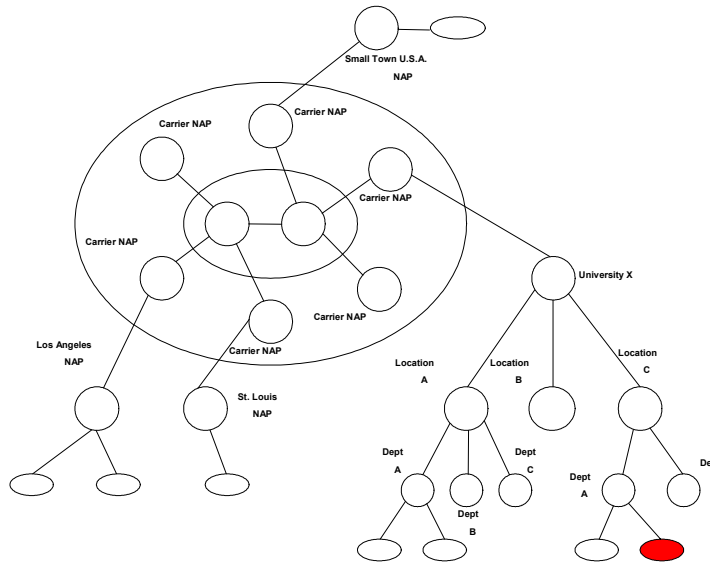


From: [System and Method for Controlling Transmission of Data Packets Over an Information Network](#).  
 Matthew P. Kulig,  
 Timmy L. Brooks,  
 John W. Lockwood,  
 David K. Reddick;  
 Filed: October 2001.

John W. Lockwood



# Virus/Worm/Data Spread in Unprotected Networks

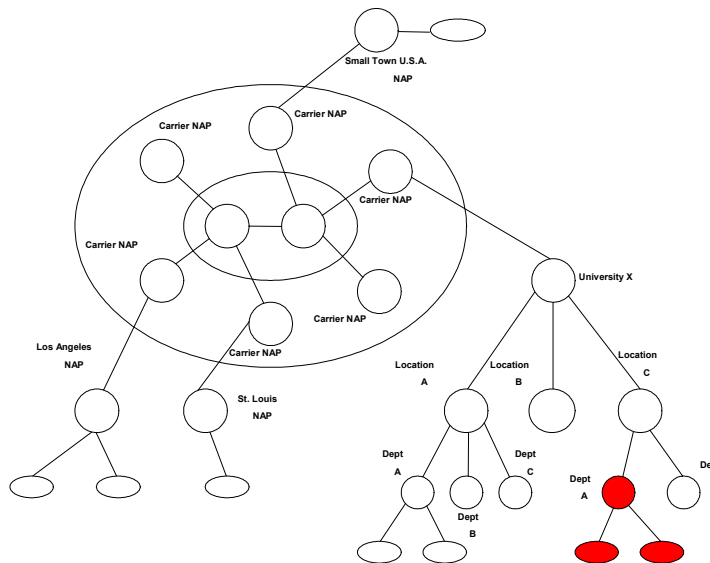


From: [System and Method for Controlling Transmission of Data Packets Over an Information Network](#),  
Matthew P. Kulig,  
Timmy L. Brooks,  
John W. Lockwood,  
David K. Reddick;  
Filed: October 2001.

John W. Lockwood



# Virus/Worm/Data Spread in Unprotected Networks

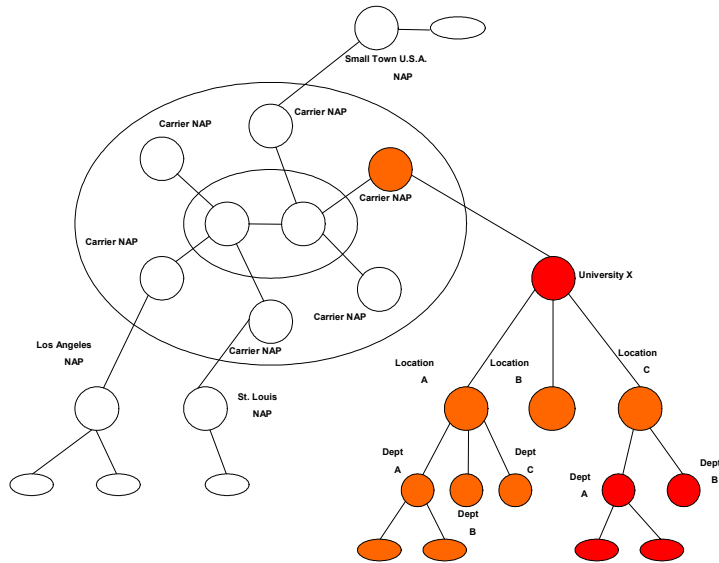


From: [System and Method for Controlling Transmission of Data Packets Over an Information Network](#),  
Matthew P. Kulig,  
Timmy L. Brooks,  
John W. Lockwood,  
David K. Reddick;  
Filed: October 2001.

John W. Lockwood



# Virus/Worm/Data Spread in Unprotected Networks

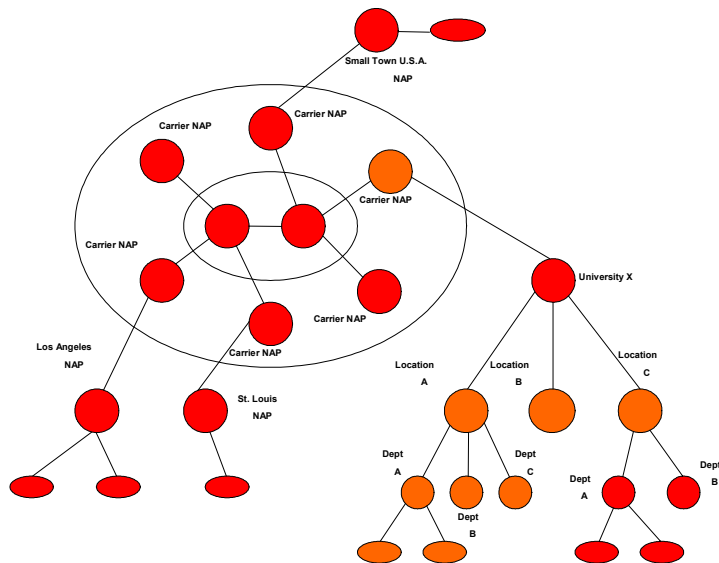


From: [System and Method for Controlling Transmission of Data Packets Over an Information Network](#),  
Matthew P. Kulig,  
Timmy L. Brooks,  
John W. Lockwood,  
David K. Reddick;  
Filed: October 2001.

John W. Lockwood



# Virus/Worm/Data Spread in Unprotected Networks



From: [System and Method for Controlling Transmission of Data Packets Over an Information Network](#),  
Matthew P. Kulig,  
Timmy L. Brooks,  
John W. Lockwood,  
David K. Reddick;  
Filed: October 2001.

John W. Lockwood



## History of Worms

- “Worm” first coined in 1982 at Xerox PARC
  - “Tapeworm” program performed system maintenance on PARC workstations
  - Name based on 1972 novel “The Shockwave Rider” by John Brunner
- Initial academic experiments
  - In 1984, Fred Cohen Publishes “Computer Viruses – Theory and Experiments”

John W. Lockwood



## First Internet Worm

- Written by Robert Morris, Jr.,
  - 23 year old Graduate student in Computer Science at Cornell
  - Son of Robert Morris
    - Head of the National Computer Security Center
    - Expert in UNIX security
- Experimental, self-propagating program
- Injected into Internet: November 2, 1988

John W. Lockwood



## Recent worm : *Code Red v1*

- Released July 13, 2001
- Self-propagating Worm
- Exploited vulnerability in Microsoft IIS Web Server
- Generated 100 Threads
  - 1 Thread to defaced local web server
  - 99 Threads to targeted random IP Addresses
- Contained a bug
  - Random number initialized with a fixed seed
  - Always scanned same sequence of hosts

John W. Lockwood



## Characteristics of the *Code Red v2*

- Released July 19, 2001 (six days later)
- Also
  - Self-propagating Worm
  - Exploited vulnerability in Microsoft IIS Web Server
  - Generated 100 Threads
    - But 1 thread to perform DDoS attack on `whitehouse.gov`
    - Other 99 threads had random number generator fixed
- Corrected the propagation rate problem
  - Infected 360,000 hosts within 14 hours
  - Spread at rate of 2,000 hosts/minute
- Direct cost of recovery
  - \$2.6 Billion

John W. Lockwood



## Why Worms can Spread

- Homogeneous software base
  - Past: Exploit software design flaws of commonly used Internet tools
  - Microsoft controls 90% + of computers
- High-bandwidth interconnections
  - Machines are very “close” to each other
  - Makes it easy for a virus to spread

John W. Lockwood



## Modeling Worms with SI Epidemic Model

- Equations used for public health
- Applied to digital pathogens since 1991
- Model dictates that new infections (or incidence) determine by product of
  - Infected individuals (infectives)
  - Fraction of uninfected individuals (suseptibles), and
  - Average contact rate.

John W. Lockwood



## Variables relevant to Infection Spread

- $N$  = Number of Vulnerable Servers  
( Total Population Size )
- $K$  = Initial rate at which infected host can spread  
( Measured in infections/hours )
- $A$  = fraction of vulnerable machines compromised  
[ 0 to 1 ] = (None to 100%)
- $t$  : Time  
( hours, since start of outbreak)

John W. Lockwood



## Differential Equation for Spreading

- $N da = (N a) K (1 - a) dt$
- Gives Differential Equation

$$\frac{da}{dt} = K a (1 - a)$$

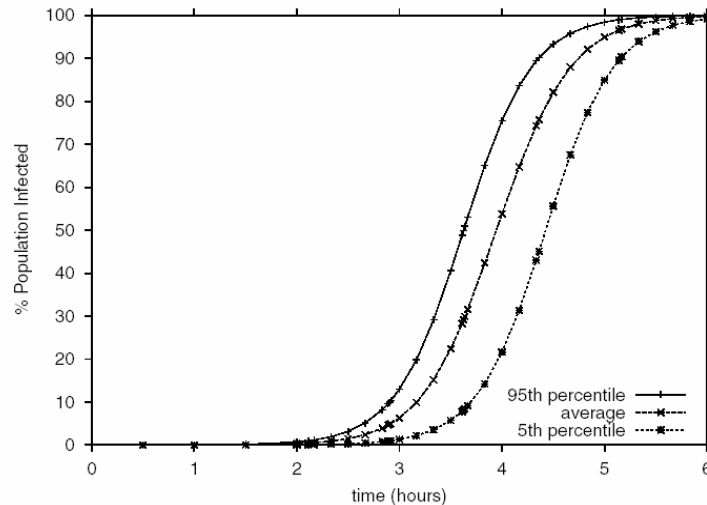
- With a Solution of

$$a = \frac{e^{K(t-T)}}{(1 + e^{K(t-T)})}$$

John W. Lockwood



# Population Infection



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

John W. Lockwood



# Fast and Sneaky Worm Spreading

- Warhol Worms
  - “15 Minutes of Fame”
  - Machines targeted by list generated with earlier reconnaissance
- Flash Worms
  - Contain complete list of hosts to infect
- Surreptitious Worms
  - Hide in existing communication patterns

John W. Lockwood



## Challenges with Worm Containment

- Must react quickly
  - Within minutes
- Must interdict many paths
  - Nearly all Internet links
- Forecast
  - Aggressive worms of the future cannot be contained using existing firewalls or software-based intrusion detection systems.

John W. Lockwood



## 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..

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

John W. Lockwood



## Containment can Work

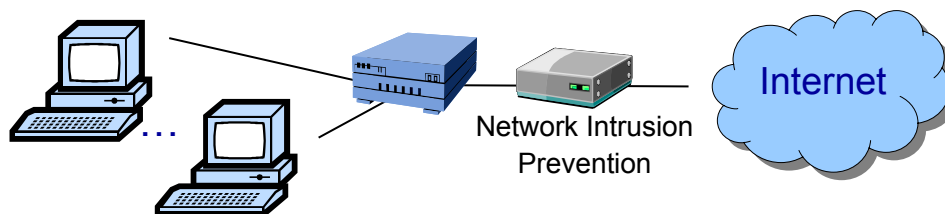
- Detection is easier than Prevention
  - Containment system does not need to understand how the worm itself works
- Containment can be deployed incrementally
  - Does not require universal deployment
- Effectiveness Depends on
  - Time to Detect and React
  - Strategy used to ID and contain pathogen
  - Breadth and placement of system deployment

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

John W. Lockwood



## Protect your Network !

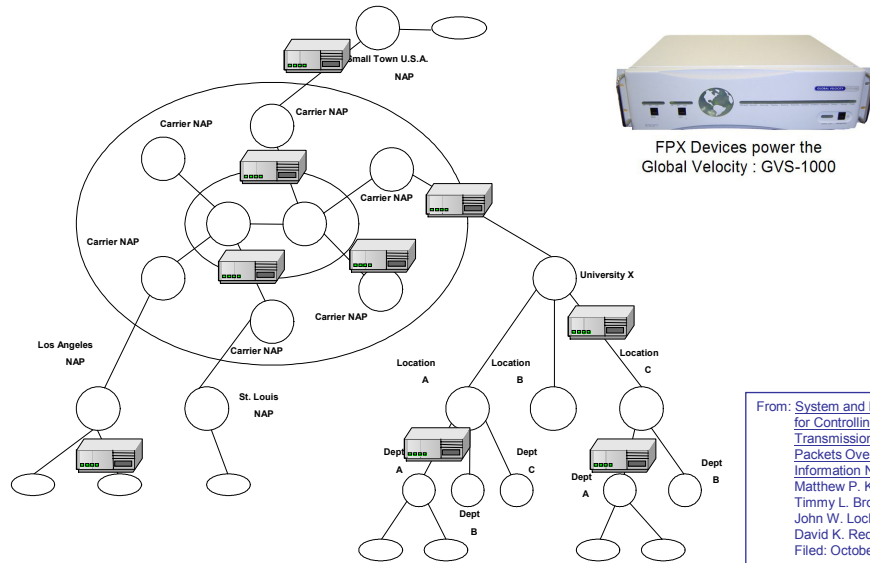


Quarantine a network to stop or slow worm outbreak and to secure data

John W. Lockwood



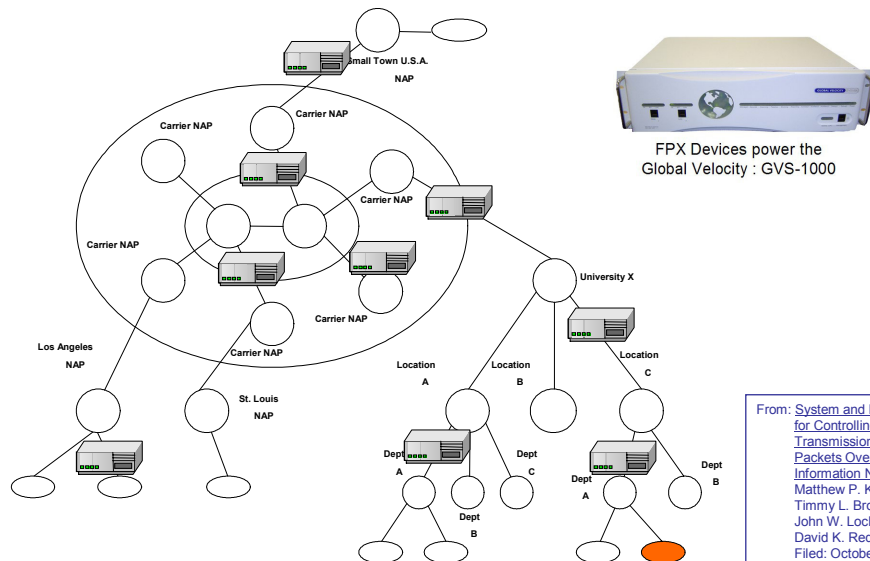
# Quarantine in Protected Networks



John W. Lockwood



# Quarantine in Protected Networks (2/3)

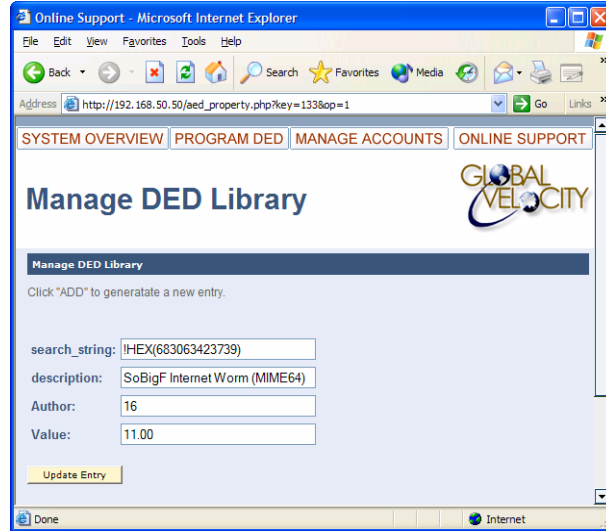


John W. Lockwood





# Edit Search strings

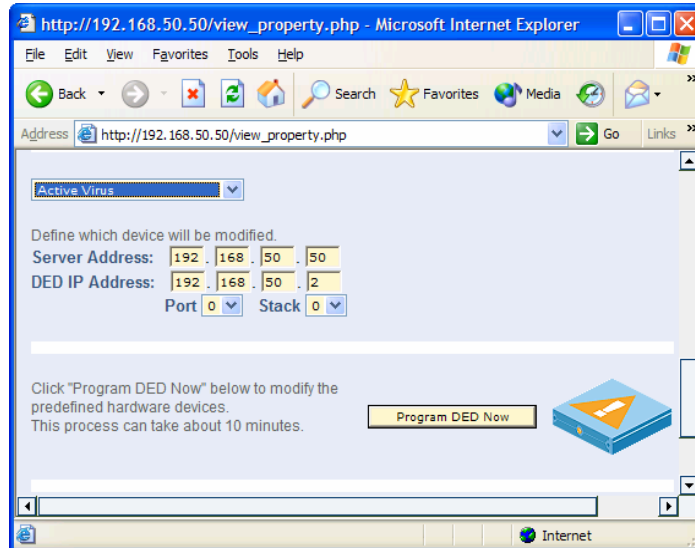


From: [Internet Worm and Virus Protection in Dynamically Reconfigurable Hardware](#); by John W. Lockwood, James Moscola, Matthew Kulig, David Reddick, Tim Brooks, *Military and Aerospace Programmable Logic Device (MAPLD)*, Washington DC, 2003, Paper E10, Sep 9-11, 2003

John W. Lockwood



# Programming the DED

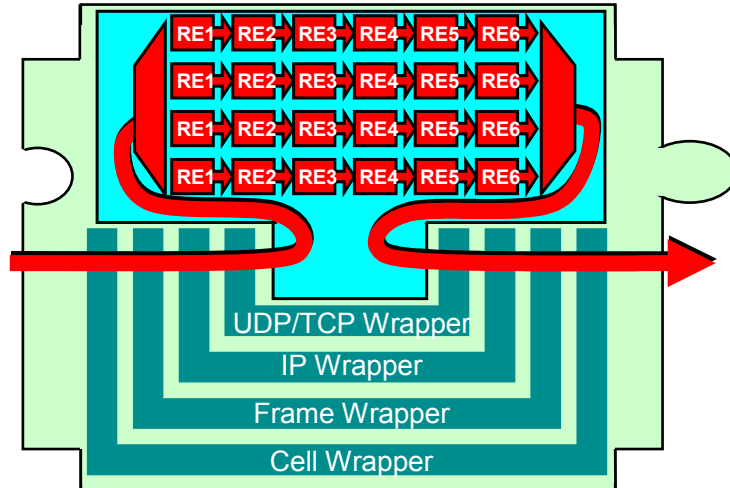


From: [Internet Worm and Virus Protection in Dynamically Reconfigurable Hardware](#); by John W. Lockwood, James Moscola, Matthew Kulig, David Reddick, Tim Brooks, *Military and Aerospace Programmable Logic Device (MAPLD)*, Washington DC, 2003, Paper E10, Sep 9-11, 2003

John W. Lockwood



# Configuration of Content Scanning Module

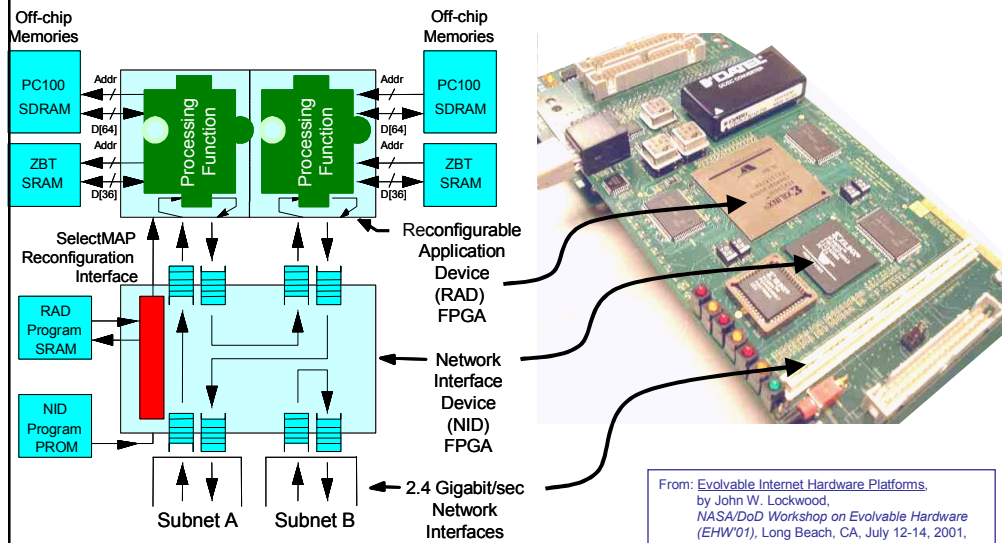


From: [Implementation of a Streaming Content Search-and-Replace Module for an Internet Firewall](#), by James Moscola, Michael Pachos, John W. Lockwood, Ron P. Loui; *Hot Interconnects 11 (HotI)*, Stanford, CA, USA, pp. 122-129, Aug. 2003.

John W. Lockwood



# Field programmable Port Extender (FPX)

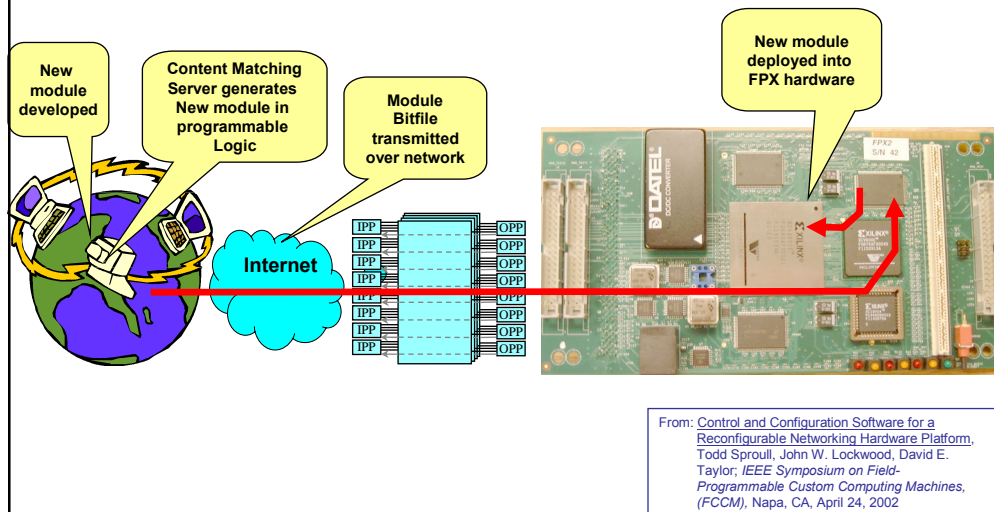


From: [Evolvable Internet Hardware Platforms](#), by John W. Lockwood, NASA/DoD Workshop on Evolvable Hardware (EHW'01), Long Beach, CA, July 12-14, 2001, pp. 271-279.

John W. Lockwood



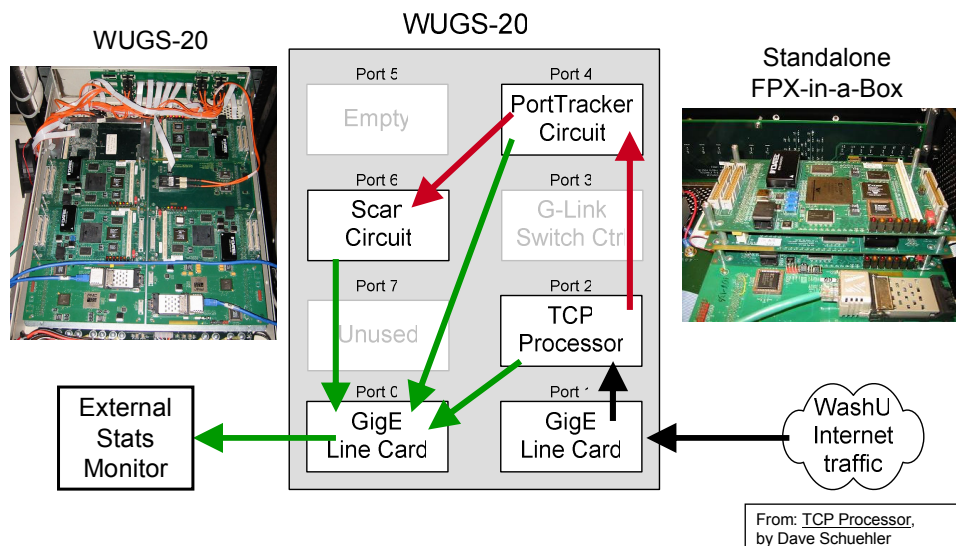
## Remotely reprogram hardware over network



John W. Lockwood



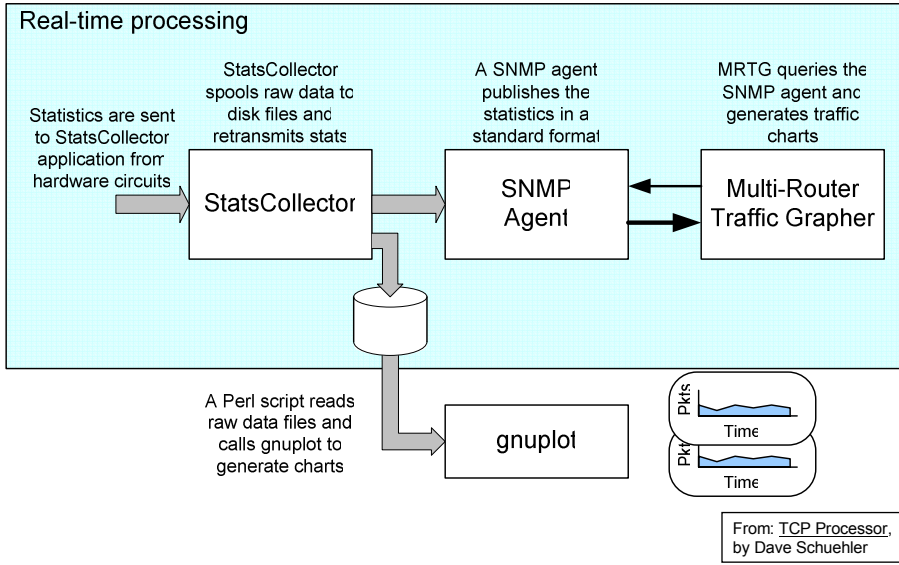
## Live Internet Traffic Analysis



John W. Lockwood



# Data Collection



John W. Lockwood

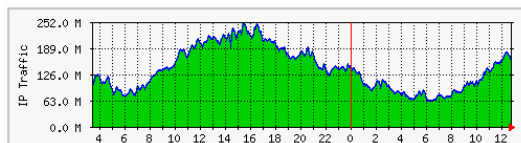


# Current Live Traffic

## IP Traffic

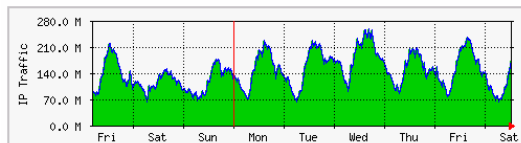
The statistics were last updated **Saturday, 30 October 2004 at 12:48**

'Daily' Graph (5 Minute Average)



Max IP Traffic: 250.5 Mb/s Average IP Traffic: 140.3 Mb/s Current IP Traffic: 157.5 Mb/s

'Weekly' Graph (30 Minute Average)

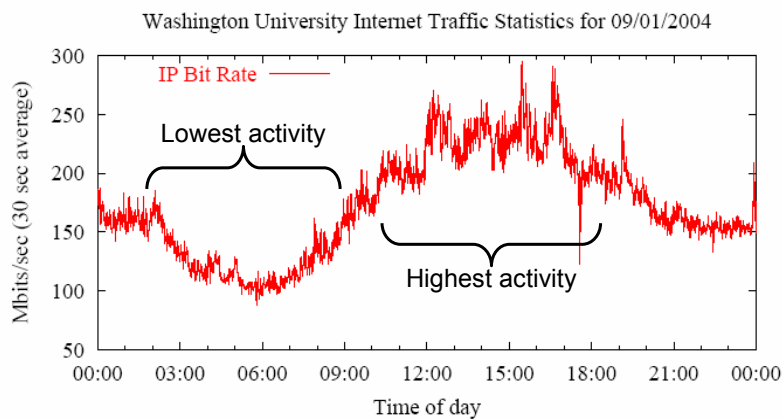


Max IP Traffic: 258.8 Mb/s Average IP Traffic: 145.2 Mb/s Current IP Traffic: 174.6 Mb/s

John W. Lockwood



## Typical Daily Traffic Pattern



From: TCP Processor,  
by Dave Schuehler

John W. Lockwood



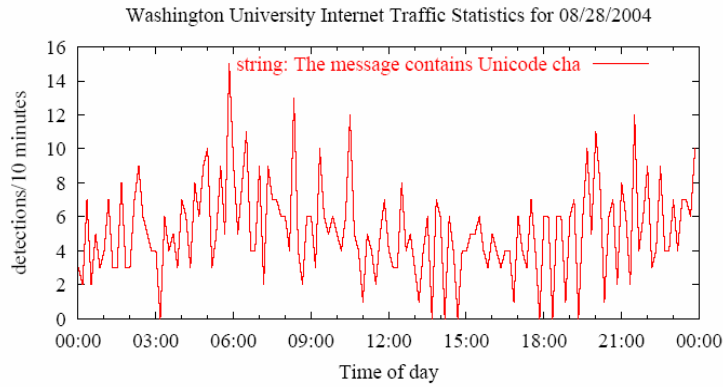
## Worm/Virus Detection

- Search for digital signatures
- MyDoom (appeared 1/26/04)
  - Spread via email attachment
  - Opens back door via ports 3127-3198
  - Contains SMTP engine to replicate itself
  - Contains denial of service attack (25% operational)
  - At Peak, 1 in 12 emails contained virus
- Netsky (appeared 3/1/04)
  - Spread via email attachment
  - Scans drives C through Z looking for email addresses
  - Contains SMTP engine to replicate itself

John W. Lockwood



# MyDoom Virus Detection

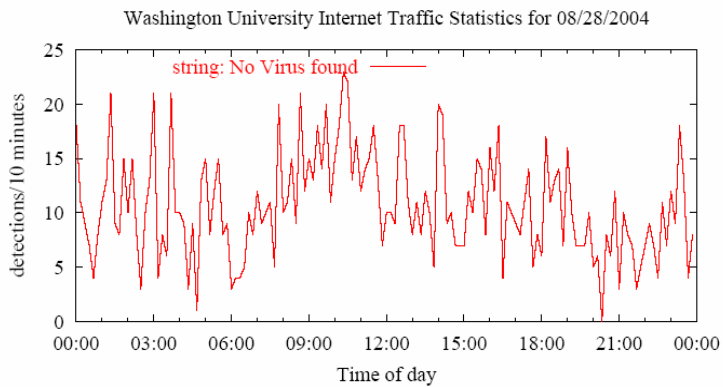


From: TCP Processor,  
by Dave Schuehler

John W. Lockwood



# Netsky Virus Detection



From: TCP Processor,  
by Dave Schuehler

John W. Lockwood



# Denial of Service Attack

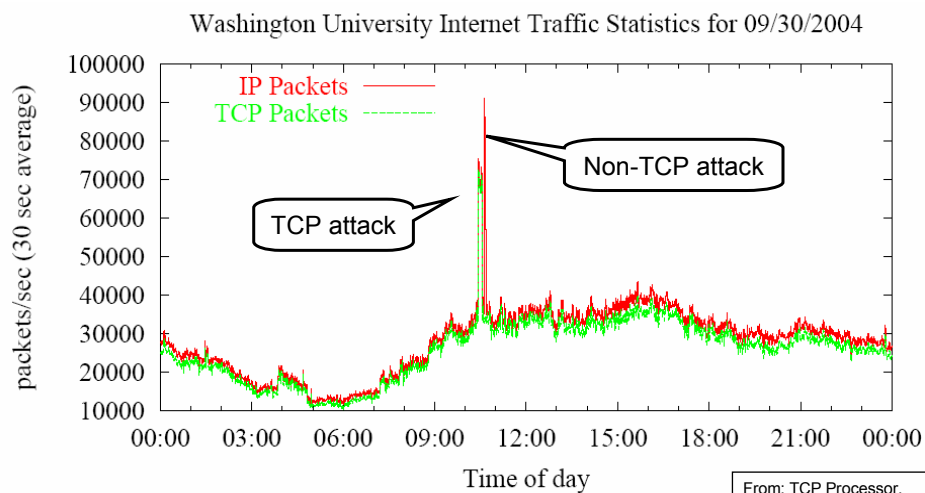
- TCP SYN Attack
  - 8 minutes in duration
  - 71,000 TCP pkts/sec avg (34,000 normal)
  - 40,000 TCP SYN pkts/sec avg (2,000 normal)
- IP attack (non TCP traffic)
  - 3.5 minutes in duration
  - 91,000 IP pkts/sec peak (36,000 normal)
  - 57,000 Non-TCP pkts/sec peak (2,000 normal)

From: TCP Processor,  
by Dave Schuehler

John W. Lockwood



# Both Attacks Visible

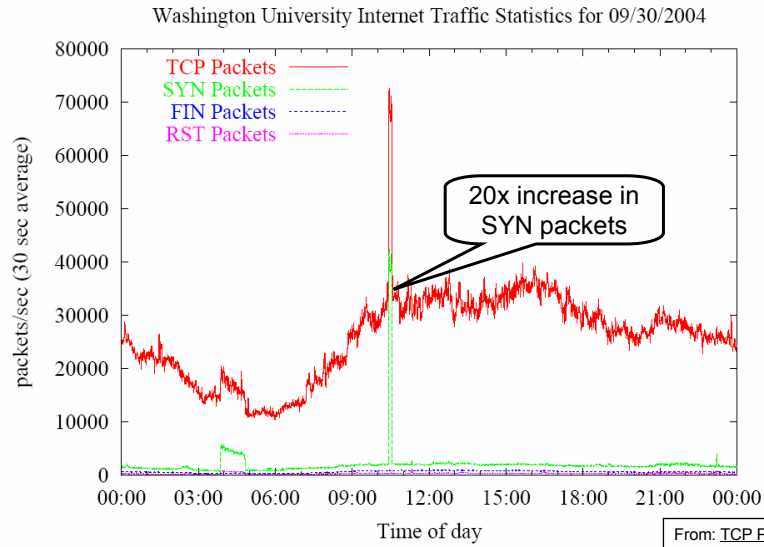


From: TCP Processor,  
by Dave Schuehler

John W. Lockwood



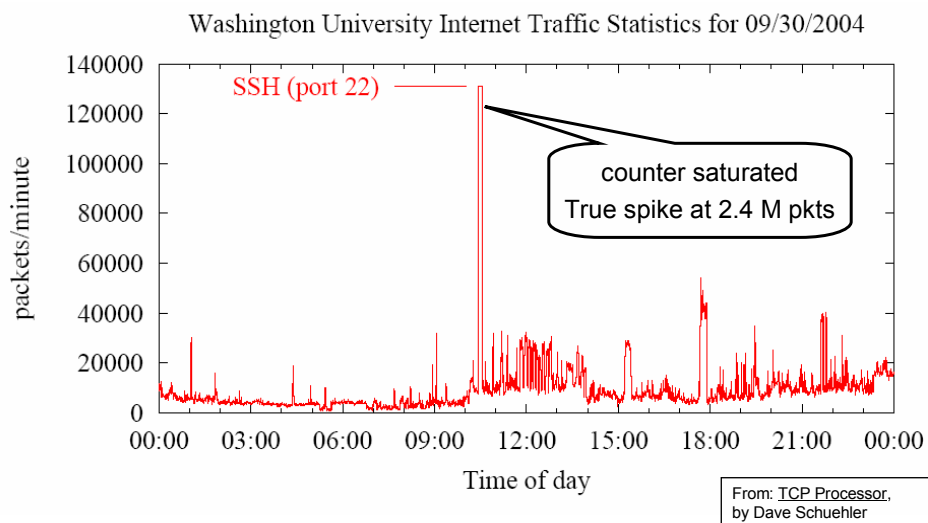
# TCP SYN Attack



John W. Lockwood



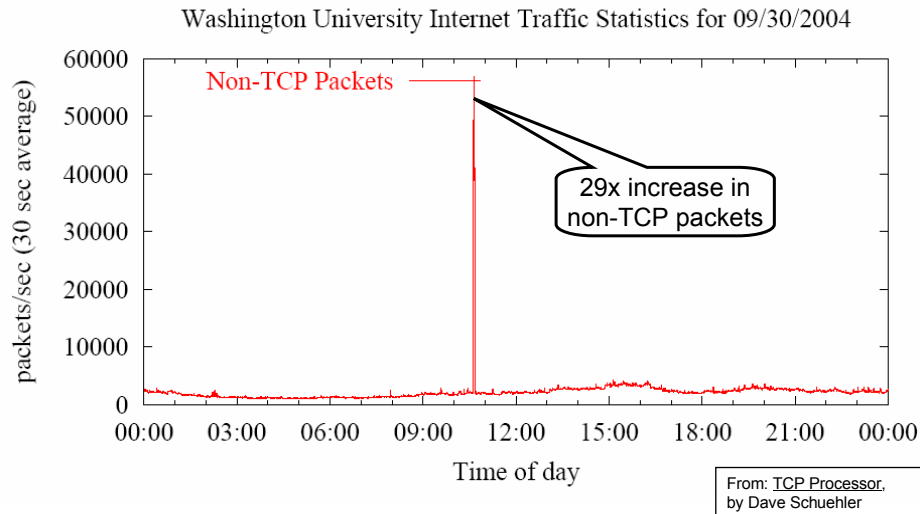
# Attack Directed at SSH Port



John W. Lockwood



# Non-TCP Attack



John W. Lockwood

Washington  
University in St. Louis

# For More Information

Publications, technical reports, recent news, and opportunities:

## Reconfigurable Network Group

<http://www.ar1.wustl.edu/ar1/projects/fpx/reconfig.htm>



This work was supported by a grant from:

**Global Velocity**

<http://www.GlobalVelocity.com>



John W. Lockwood

Washington  
University in St. Louis