

# Internet Security and Implications on Transportation Systems

Yan Chen

Department of Electrical Engineering and Computer  
Science

Northwestern University

Lab for Internet & Security Technology (LIST)

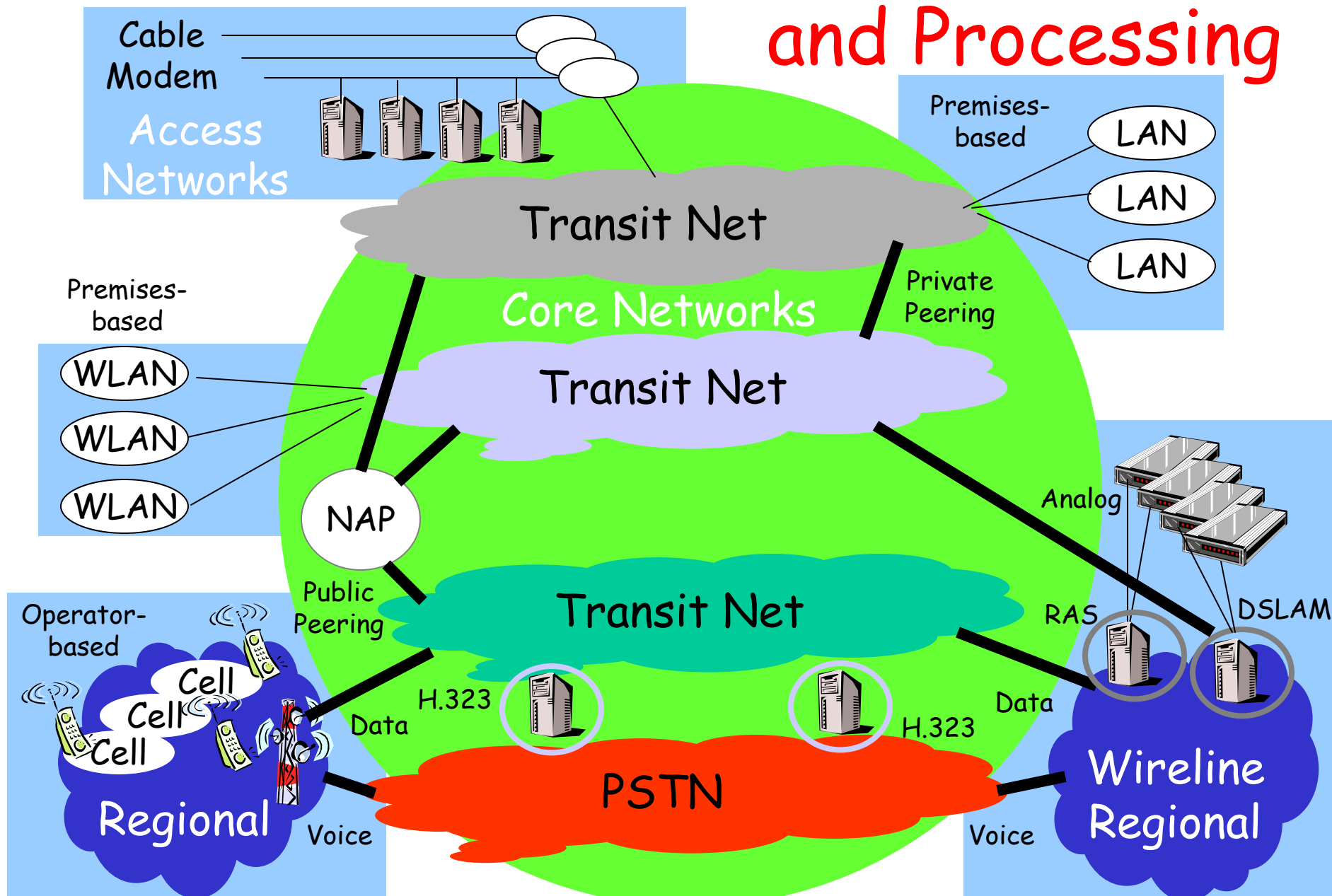
<http://list.cs.northwestern.edu>



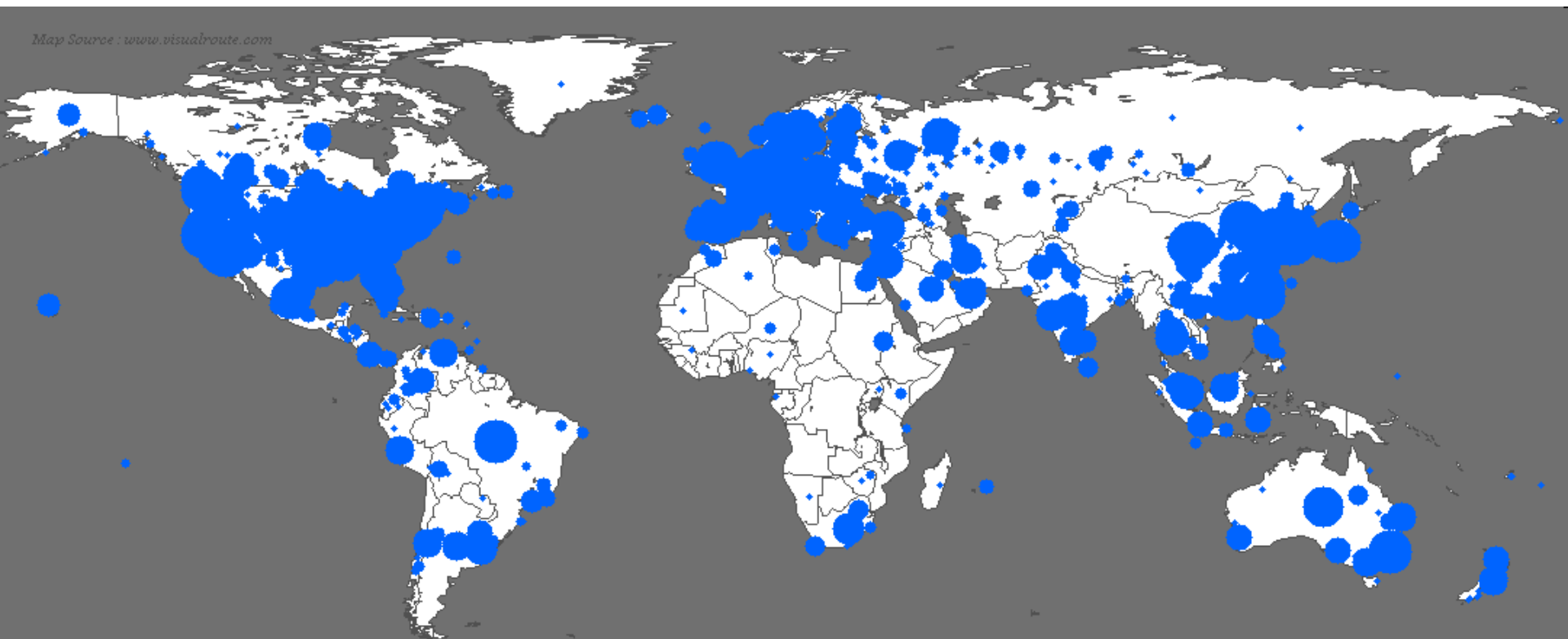
# Outline

- ❑ Internet Threat Landscape
- ❑ Security regulations
- ❑ System Diagnosis

# The Current Internet: Connectivity and Processing



# The Spread of the Sapphire/Slammer SQL Worm



Sat Jan 25 06:00:00 2003 (UTC)

Number of hosts infected with Sapphire: 74855

<http://www.caida.org>

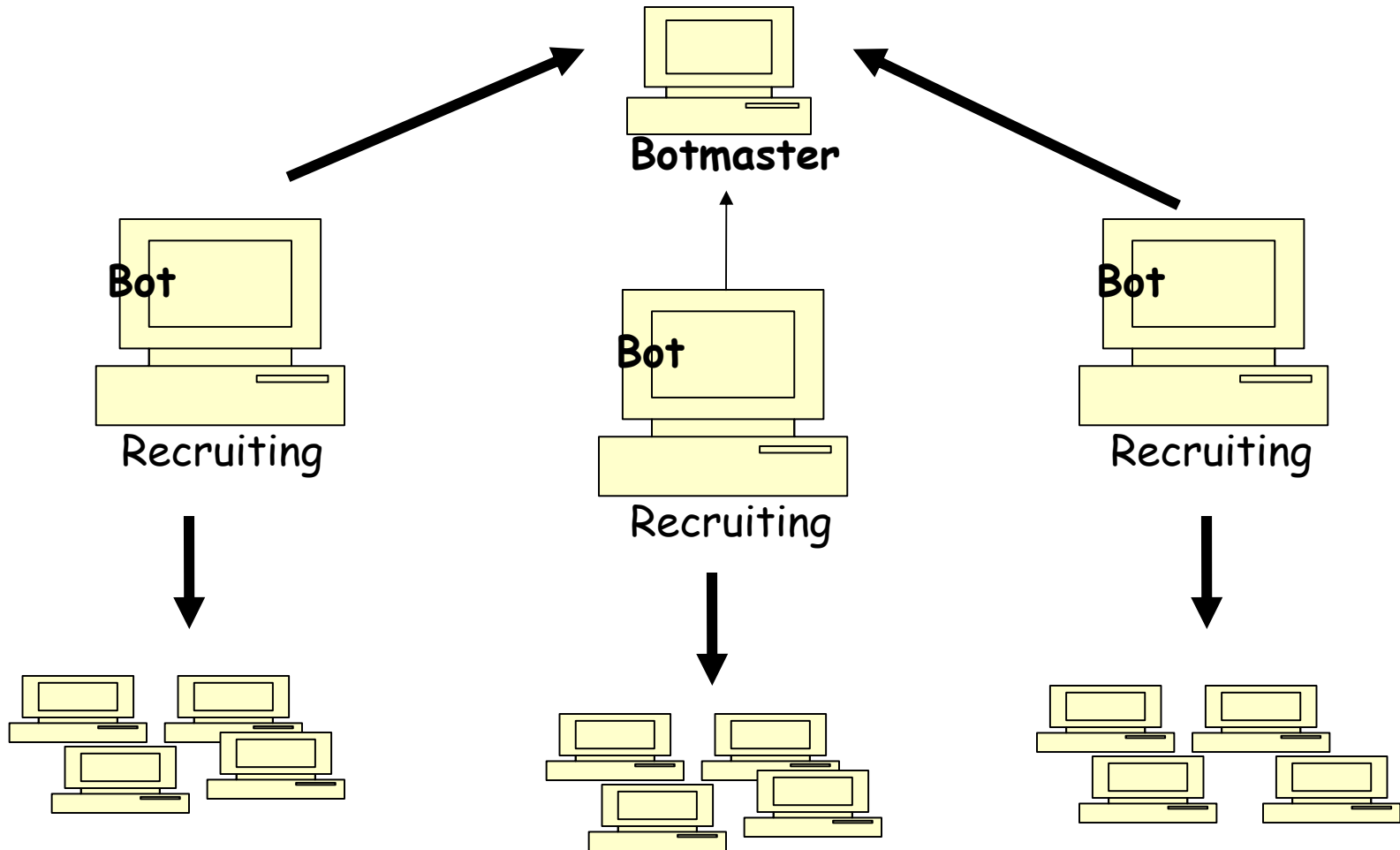
Copyright (C) 2003 UC Regents

# Evolution of Botnets

- Motivation change in computer hacking
  - Vandalism → Financial gains
  - Loss of \$67.2 billion (2006 figure)



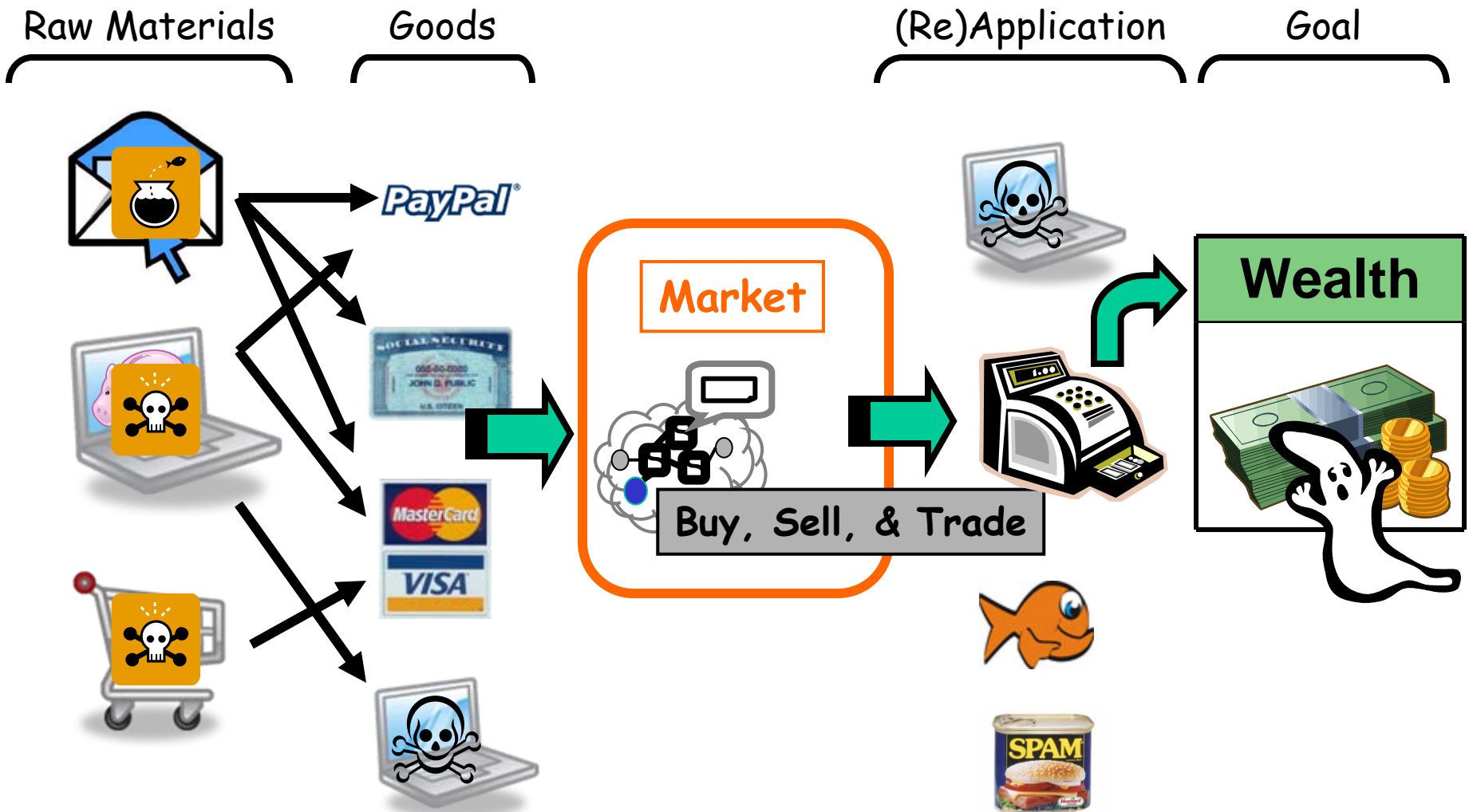
# Botnet Architecture



# Attack Behaviors

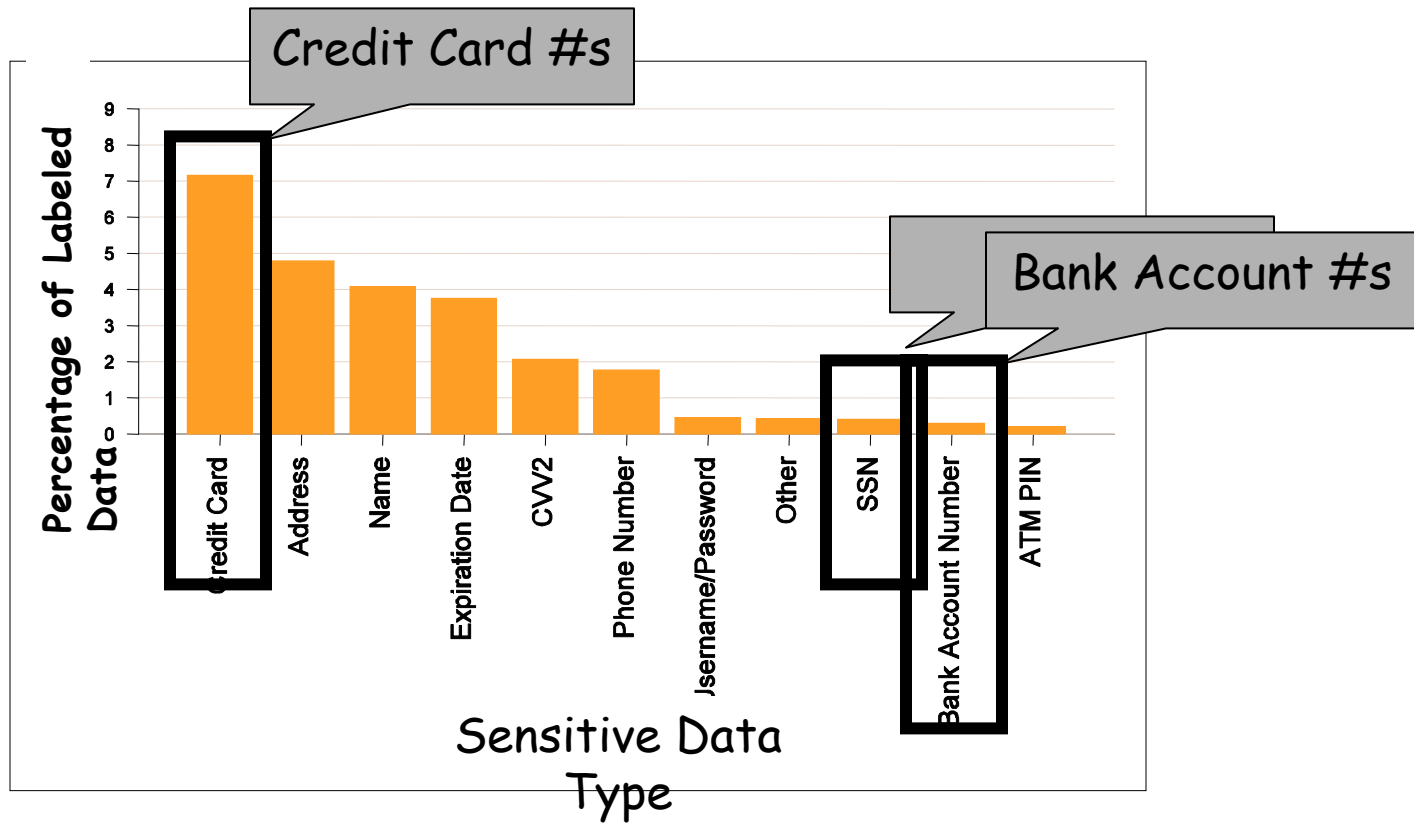
- ❑ Stealing personal information
  - Keylogger and Network sniffer used on compromised systems to spy on users and compile personal information
- ❑ Phishing and spam proxy
  - Aggregated computing power and proxy capability allow spammers to impact larger groups without being traced.
- ❑ Distributed Denial of Service (DDoS)
  - Impair or eliminate availability of a network to extort or disrupt business

# eCrime Market Operation





# Sensitive Data and Market Significance



## Al-Qaeda Poses Threat to Net

Pay heed to warning from bin Laden associate, experts say

Dan Verton [Today's Top Stories](#) or [Other Security Stories](#)

**November 25, 2002** ([Computerworld](#)) -- Intelligence and security experts last week said new warnings of potential cyberattacks against Western economic targets by al-Qaeda sympathizers should be taken seriously by government policy-makers and the managers of the targeted systems.

In an exclusive interview with *Computerworld* on Nov. 18, Sheikh Omar Bakri Muhammad, a London-based fundamentalist Islamic cleric with known ties to Osama bin Laden, said al-Qaeda and various other radical Muslim groups around the world are actively planning to use the Internet as a weapon in their "defensive" jihad, or holy war, against the West.

"In a matter of time, you will see attacks on the stock market," said Bakri, referring specifically to the exchanges in New York, London and Tokyo. "That is what al-Qaeda is skillful with. I would not be surprised if tomorrow I hear of a big economic collapse because of somebody attacking the main technical systems in big companies."



Sheikh Omar Bakri  
Muhammad, founder of the

The White House declined to comment. However, U.S. Navy Cmdr. David Wray, a spokesman for the FBI's National Infrastructure Protection Center (NIPC), said the NIPC is "concerned about the potential for terrorists to use the Internet to inflict damage, as well as

The *Science* of CERTAINTY

NO HARDWARE. NO  
SOFTWARE. NO-ONE  
CAN TOUCH YOU.

We call it The Science of Certainty.  
Take our instant security assessment and find out  
how it will benefit your business. [Click here.](#)

Be certain



MessageLabs®

# Electricity Grid in U.S. Penetrated By Spies

Article

Video

Comments (145)

Email

Printer  
Friendly

Share:

facebook

Save This

- Text +

By SIOBHAN GORMAN



Associated Press

Robert Moran monitors an electric grid in Dallas. Such infrastructure grids across the country are vulnerable to cyberattacks.

- ❑ Cyber spies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system.
- ❑ Transportation systems (air, truck, bus) the next?
  - Next generation 9/11 without suicide bombers!

# Security Regulations

- Business and security compliance is top-of-mind for executives
- Protecting sensitive business & customer data is the key focus of regulatory compliance requirement

Sarbanes-Oxley	<p>Publicly Traded Companies Must:</p> <ul style="list-style-type: none"><li>• Maintain an adequate internal control structure and procedures for financial reporting</li><li>• Assess the effectiveness of internal control structures</li></ul>
HIPAA	<p>For Patient Information, Firms Must:</p> <ul style="list-style-type: none"><li>• Maintain administrative, technical and physical safeguards to ensure integrity and confidentiality</li><li>• Protect against threats or hazards; unauthorized uses or disclosures</li></ul>
PCI	<p>All Merchants Using Payment Cards, Must:</p> <ul style="list-style-type: none"><li>• Build and maintain a secure network</li><li>• Protect and encrypt cardholder data</li><li>• Regularly monitor and test networks, including wireless</li></ul>

# Business Impact of Lack of Compliance

- ❑ Direct financial ramifications
  - FTC fines
  - Compensation payout to customers
  - Cost of external security audits
  - Lost customer confidence
- ❑ Research shows substantial indirect costs associated with brand damage

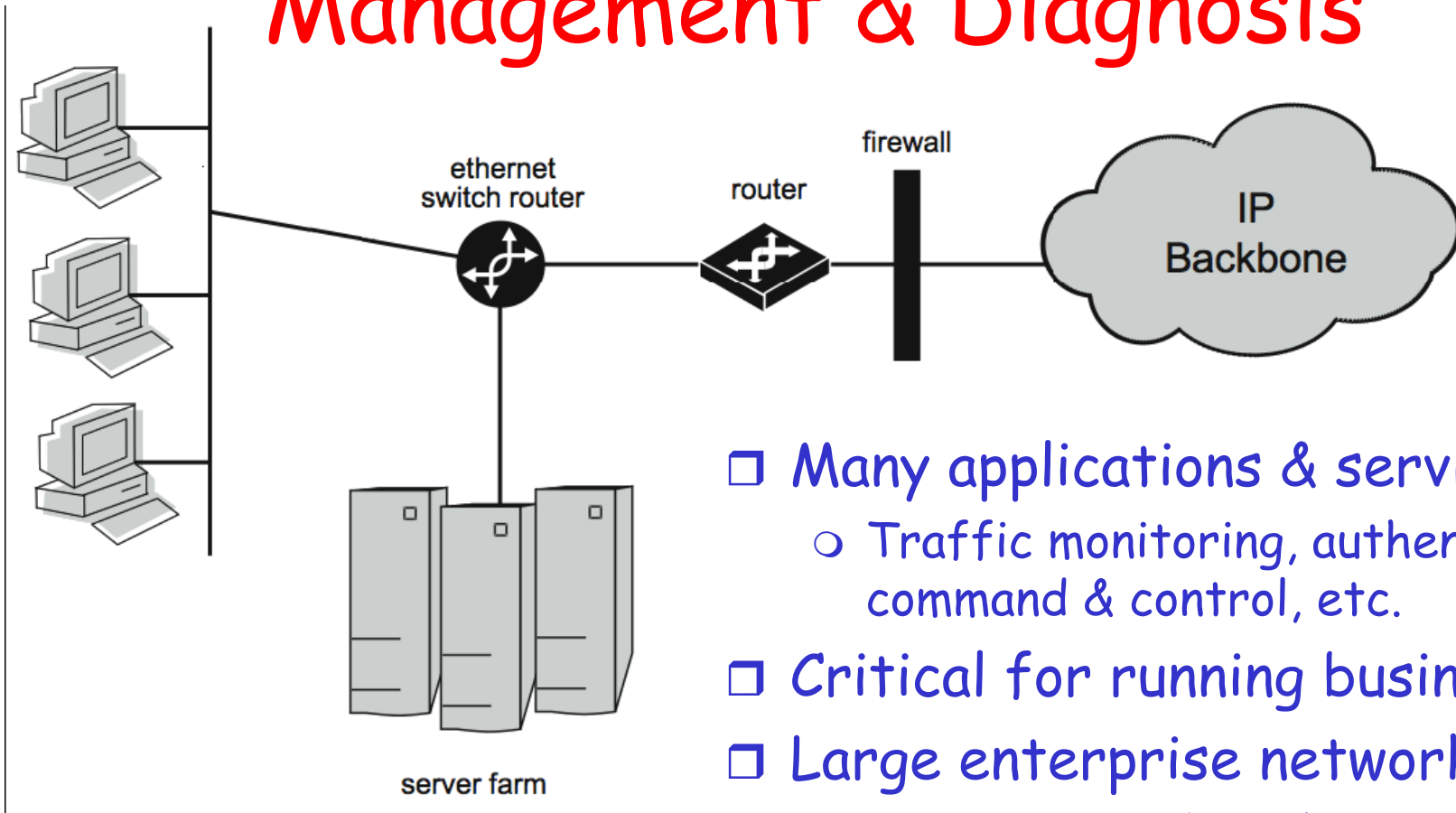
## Case Study

- Company:  
Large retailer
- Issue: Data breach due to poor wireless security
- Ramifications:
  - 20 years of third-party security audits mandated by FTC
  - Compromise of 1.4 million credit cards and 96,000 checking accounts
  - Company losses related to security breach ranged from \$6.5m to \$9.5m

# Do We Have Any Security Regulations for Transportation Systems?

- E.g., any FAA rules?

# Transportation Control System Management & Diagnosis



- ❑ Many applications & services
  - Traffic monitoring, authentication, command & control, etc.
- ❑ Critical for running business
- ❑ Large enterprise networks
  - 1,000s network applications
  - 1,000s staffs in IT support
  - \$\$ millions of dollars spent every year