Information Assurance – A Key Imperative

Jaideep Srivastava

Army High Performance Computing Research Center
Department of Computer Science
University of Minnesota

Project Participants: V. Kumar, A. Lazarevic, J. Srivastava
P. Dokas, E. Eilertson, L. Ertoz, S. Iyer, S. Ketkar, P. Tan

Research supported by AHPCRC/ARL

Outline

- Emerging trends in networking
    - Network-centric view of the world
    - Network access devices
    - Emerging services on the New Network
- Global business collaboration
- Global network – “agile yet fragile”
- Need for information vigilance
- Research issues in information vigilance
- The MINDS project
- Conclusion

Outline

- Emerging trends in networking
  - Network-centric view of the world
  - Network access devices
  - Emerging services on the new network
- Global business collaboration
- Global network – “agile yet fragile”
- Need for information vigilance
- Research issues in information vigilance
- The MINDS project
- Conclusion

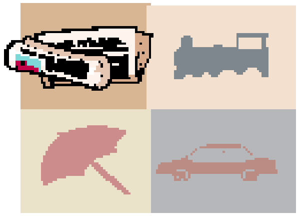
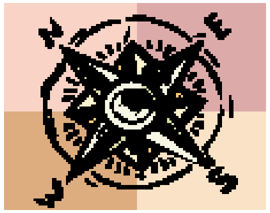
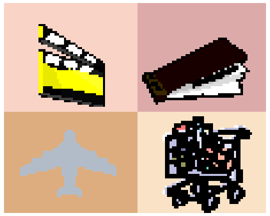
Traditional View of Networking [Katz 2002]

- All about protocols and the OSI seven layers
  - Protocol details: link-state vs. distance vector, TCP
  - Protocol layering
  - Multiaccess technology
  - Switching and routing
  - Naming
  - Error control
  - Flow control & scheduling
  - Special topics like multicast and mobility

The New Opportunity [Katz 2002]

- New things you can do inside the network
- Connecting end-points to “services” with processing embedded in the network fabric
- Not protocols but “agents,” executing in places in the network
- Location-aware, data format aware
- Controlled violation of layering necessary!
- Distributed architecture aware of network topology
- No single technical architecture likely to dominate: think overlays, system of systems

Services in Converged Networks [Katz 2002]

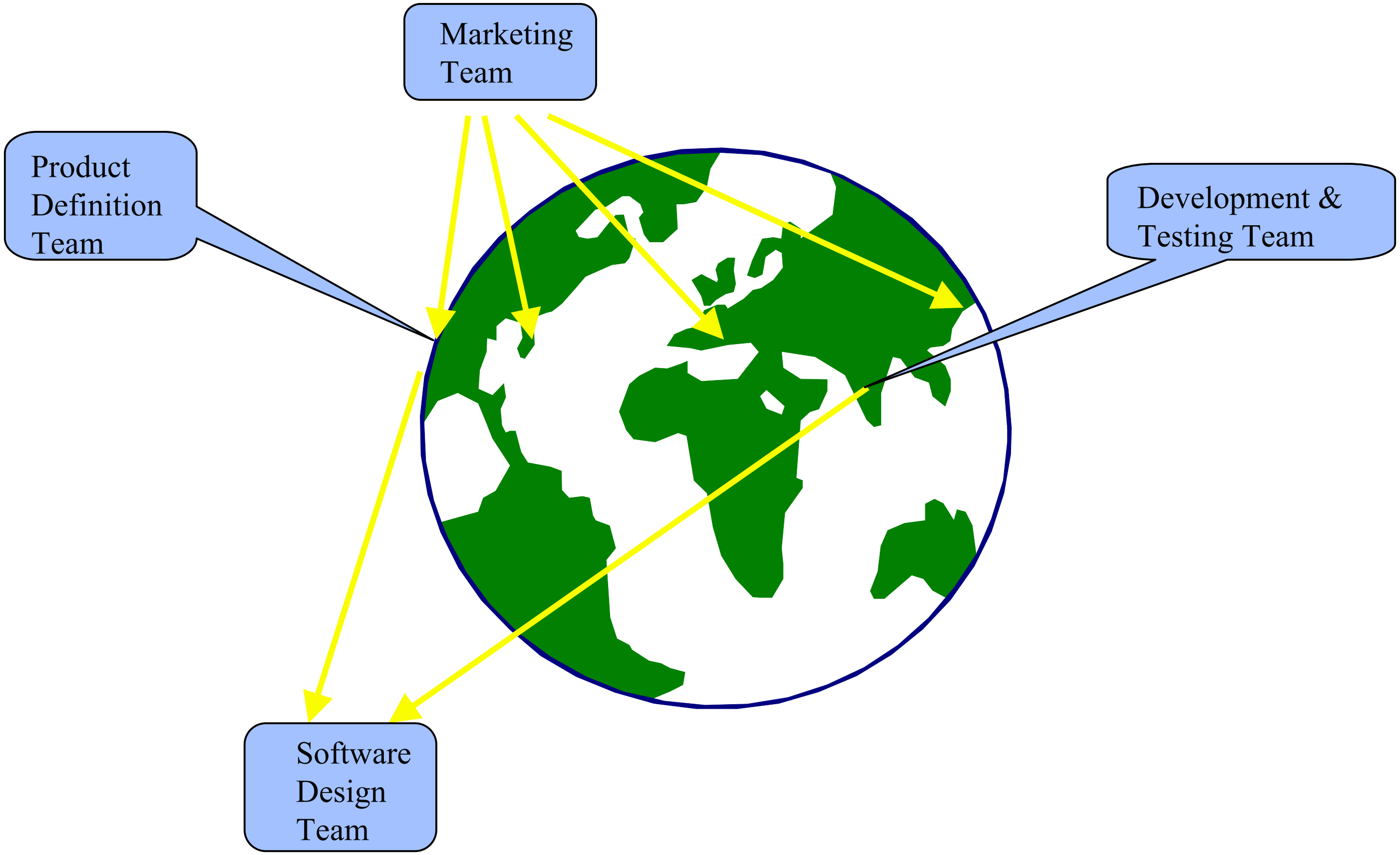
Net Access Services					
Information Services	Location-based Services	M-Commerce	M-Entertainment	Personal Information Management (PIM)	Other Internet / Intranet Access
					
• News • Stocks • Financial • Weather • Travel	• The nearest ATM? • The quickest way to East Coast? • The best restaurant? • The nearest available parking?	• M-banking • M-brokering • M-ticketing • M-tailing	• Downloadable and interactive entertainment services – Mp3 audio files Mp4 video clips – M-icons – Interactive Games	• Address book • Business card • Personal Web Space • Management services	• Corporate Intranet connectivity • General web browsing, not just own portal • Remote secure access for Intranet

Outline

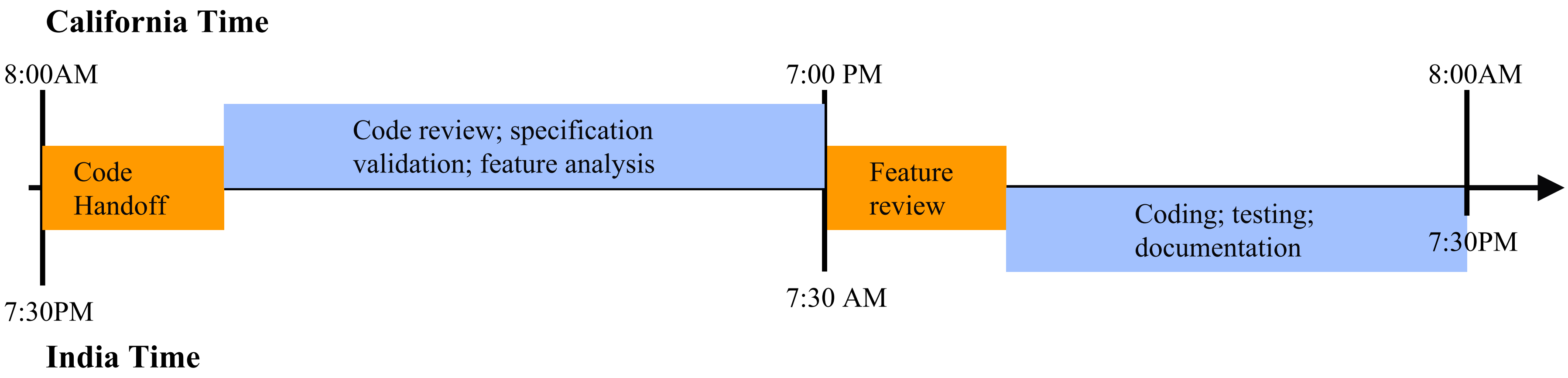
- Emerging trends in networking
  - Network-centric view of the world
  - Network access devices
- Emerging services on the new network
- Global business collaboration
- Global network – “agile yet fragile”
- Need for information vigilance
- Research issues in information vigilance
- The MINDS project
- Conclusion

Global Business Collaboration

Software Company of the Future



24/7 Operation


California Time

8:00AM

7:00 PM

8:00AM

Code Handoff

Code review; specification validation; feature analysis

Feature review

Coding; testing; documentation

7:30PM

7:30 AM

7:30PM

India Time

The future is here today – and began yesterday!

- **HP – started division in Bangalore, India in about 1981**
- **Honeywell started division in Bangalore, India in about 1994**
- **Microsoft started division in Beijing, China in about 1998**
- **IBM started research labs in Beijing, China and Delhi, India in the past 3 years**
- **Motorola investing heavily in China; has division in India**

International Divisions of MN Corporations

Medtronic, Shanghai, China

- In order to apply the latest research result of biotechnology to Chinese medical care area, Medtronic is devoted to developing the Champion pacemaker which is cost effective and suitable for Chinese patients
- Investment of 10million USD by Medtronic Inc. in Medtronic, Shanghai

Honeywell Software Solutions Lab, Bangalore, India

- a wholly owned subsidiary of Honeywell Inc, one of the world's premier global and progressive companies
- shared corporate resource providing software Product development and Support, Research and Technology development, Digitizing support and consultation
- Honeywell charts $50m India plan

Outline

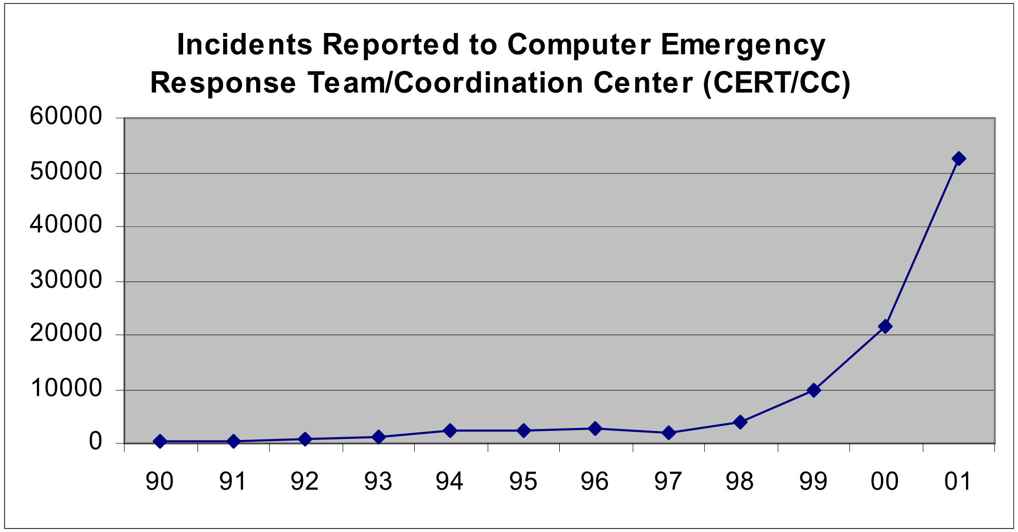
- Emerging trends in networking
  - Network-centric view of the world
  - Network access devices
- Emerging services on the new network
- Global business collaboration
- Global network – “agile yet fragile”
- Need for information vigilance
- Research issues in information vigilance
- The MINDS project
- Conclusion

Global Network: Agile yet Fragile [Katz 2002]

- **Baltimore Tunnel Fire, 18 July 2001**
  - **"… The fire also damaged fiber optic cables, slowing Internet service across the country, …"**
  - **"… Keynote Systems … says the July 19 Internet slowdown was not caused by the spreading of Code Red. Rather, a train wreck in a Baltimore tunnel that knocked out a major UUNet cable caused it."**
  - **"PSINet, Verizon, WorldCom and AboveNet were some of the bigger communications companies reporting service problems related to 'peering,' methods used by Internet service providers to hand traffic off to others in the Web's infrastructure. Traffic slowdowns were also seen in Seattle, Los Angeles and Atlanta, possibly resulting from re-routing around the affected backbones."**
  - **"The fire severed two OC-192 links between Vienna, VA and New York, NY as well as an OC-48 link from, D.C. to Chicago. … Metromedia routed traffic around the fiber break, relying heavily on switching centers in Chicago, Dallas, and D.C."**

Global Network: Agile yet Fragile

- **Hacker attacks close operations of Amazon.com and Yahoo! In March 2000**
- **Hacker threatened CD Universe with blackmail, and then posted over 10,000 customer credit card numbers on public web site**
- **Largest ring of identity thieves caught in New Jersey area, over 30,000 identities were stolen**
- **Regular attacks against military and government sites**
  - **Intrusion**
  - **Denial of service**
  - **Defacement**
  - **…**



Global Network: Agile yet Fragile

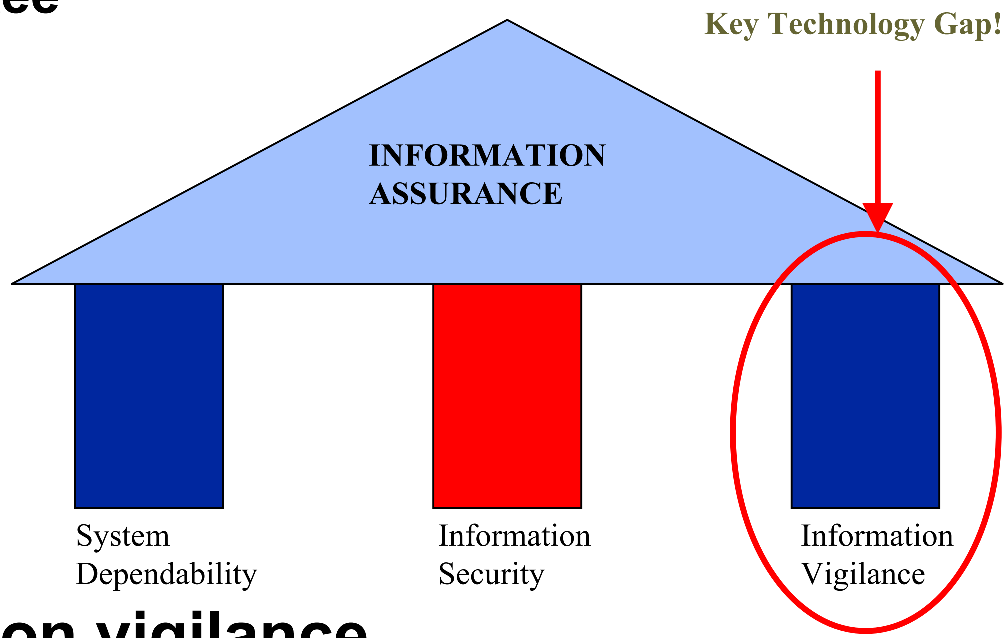
- Detected scanning for Oracle server
  - Reported by CERT, June 13, 2002
- Detected a distributed windows networking scan from multiple source locations
  - Reported by CERT, August 8, 2002
- Detected scanning for Microsoft DS service on port 445/TCP
  - Reported by CERT, August 9, 2002
- Identified machine that was running Microsoft PPTP VPN server on non-standard ports, which is a policy violation
  - Detected by UMN, August 8, 2002
- Identified compromised machines that were running FTP servers on non-standard ports, which is a policy violation
  - Detected by UMN, October 30, 2002

Outline

- Emerging trends in networking
  - Network-centric view of the world
  - Network access devices
- Emerging services on the new network
- Global business collaboration
- Global network – “agile yet fragile”
- Need for information vigilance
- Research issues in information vigilance
- The MINDS project
- Conclusion

Information Assurance – A Key Imperative

- Information assurance
  - a (high-level) of guarantee that information is accurate and safe
  - policies, mechanisms and processes that provide this guarantee



- Information vigilance
  - mechanisms and processes that proactively provide this guarantee

Issues in Information Vigilance – (partial list)

- detecting attacks and intrusions against the network
- identifying malicious insiders
- thwarting attacks and containing damage
- techniques for graceful degradation and damage recovery
- techniques to link together and identify groups of malcontents
- identifying and thwarting cyber frauds
- …

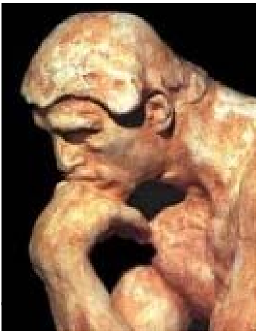
Outline

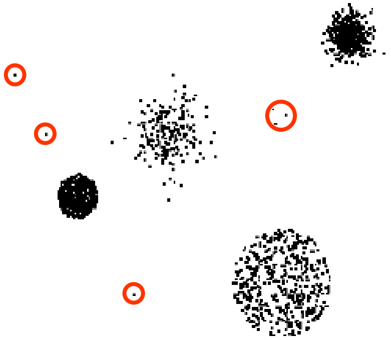
- Emerging trends in networking
  - Network-centric view of the world
  - Network access devices
- Emerging services on the new network
- Global business collaboration
- Global network – “agile yet fragile”
- Need for information vigilance
- Research issues in information vigilance
- The MINDS project
- Conclusion

AHPCRC

The MINDS Project

- **MINDS – MINnesota INtrusion Detection System**
  - **Learning from Rare Class – Building r class prediction models**
  - **Anomaly/outlier detection**
  - **Summarization of attacks using association pattern analysis**



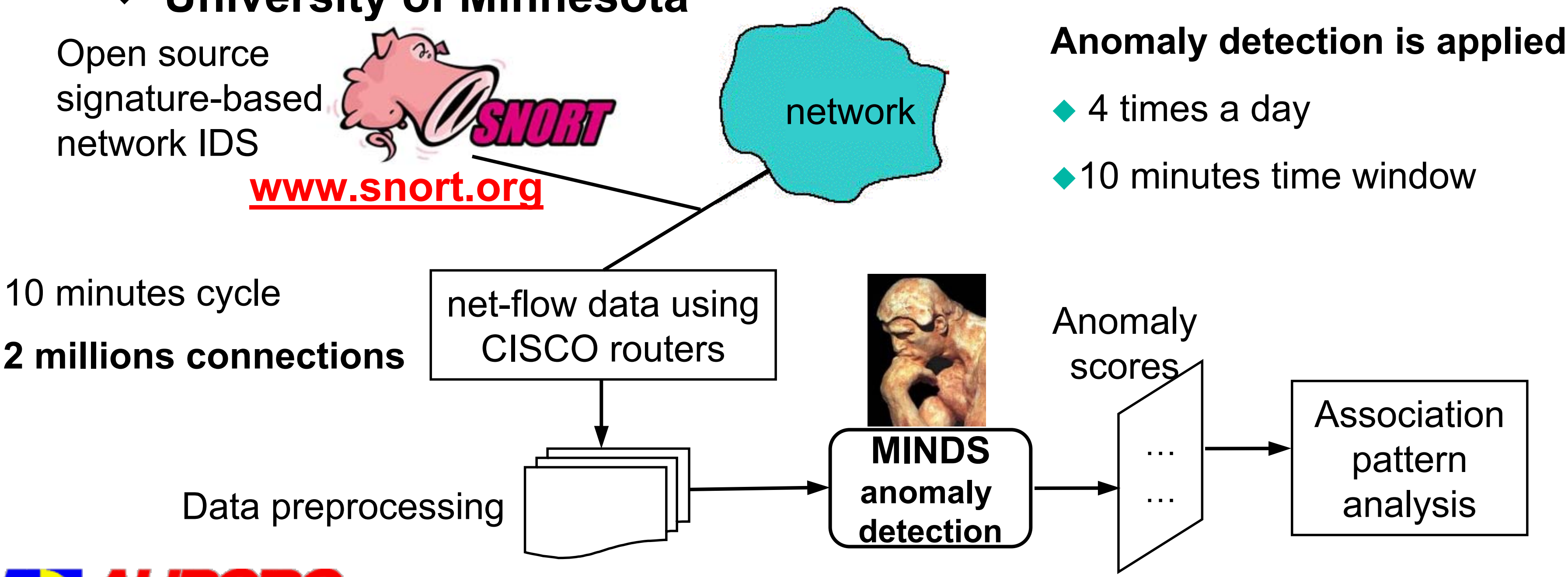


TID	*Items*
1	Bread, Coke, Milk
2	Beer, Bread
3	Beer, Coke, Diaper, Milk
4	Beer, Bread, Diaper, Milk
5	Coke, Diaper, Milk

Rules Discovered:
{Milk} --> {Coke}
{Diaper, Milk} --> {Beer}

Experimental Evaluation

- **Publicly available data set**
  - **DARPA 1998 Intrusion Detection Evaluation Data Set**
    - **prepared and managed by MIT Lincoln Lab**
    - **includes a wide variety of intrusions simulated in a military network environment**
- **Real network data from**
  - **University of Minnesota**



Open source signature-based network IDS

www.snort.org

Anomaly detection is applied

- 4 times a day
- 10 minutes time window

10 minutes cycle

2 millions connections

net-flow data using CISCO routers
Data preprocessing
MINDS anomaly detection
Anomaly scores
…
…
Association pattern analysis

Other Applications of MINDS Research

- Credit card fraud detection
- Insurance fraud detection
- Transient fault detection for industrial process control
- Detecting individuals with rare medical syndromes (e.g. cardiac arrhythmia)

Conclusion

- Vision of a globally connected world
  - Network is the key infrastructure
  - Accessed from a wide variety of devices, portable, special function
  - Growing collaboration of individuals and organizations
  - Increased dependence on network reliability and information guarantee
- Globally connected world – agile yet fragile
  - Increasing attacks and frauds
  - Various “single-points-of-failure”
  - → Increased vulnerability
- Information assurance – a key imperative
- Information vigilance
  - Emerging area
  - Data mining is key technology