# Security for “Seamless Global Connectivity and Services Anywhere, Anytime”


**Prof. Madjid Merabti**

**Network Security Group**
**School of Computing and Mathematical Sciences**
**Liverpool John Moores University**
**Byrom Street, Liverpool L3 3AF, UK.**
**Email: M.Merabti@livjm.ac.uk**

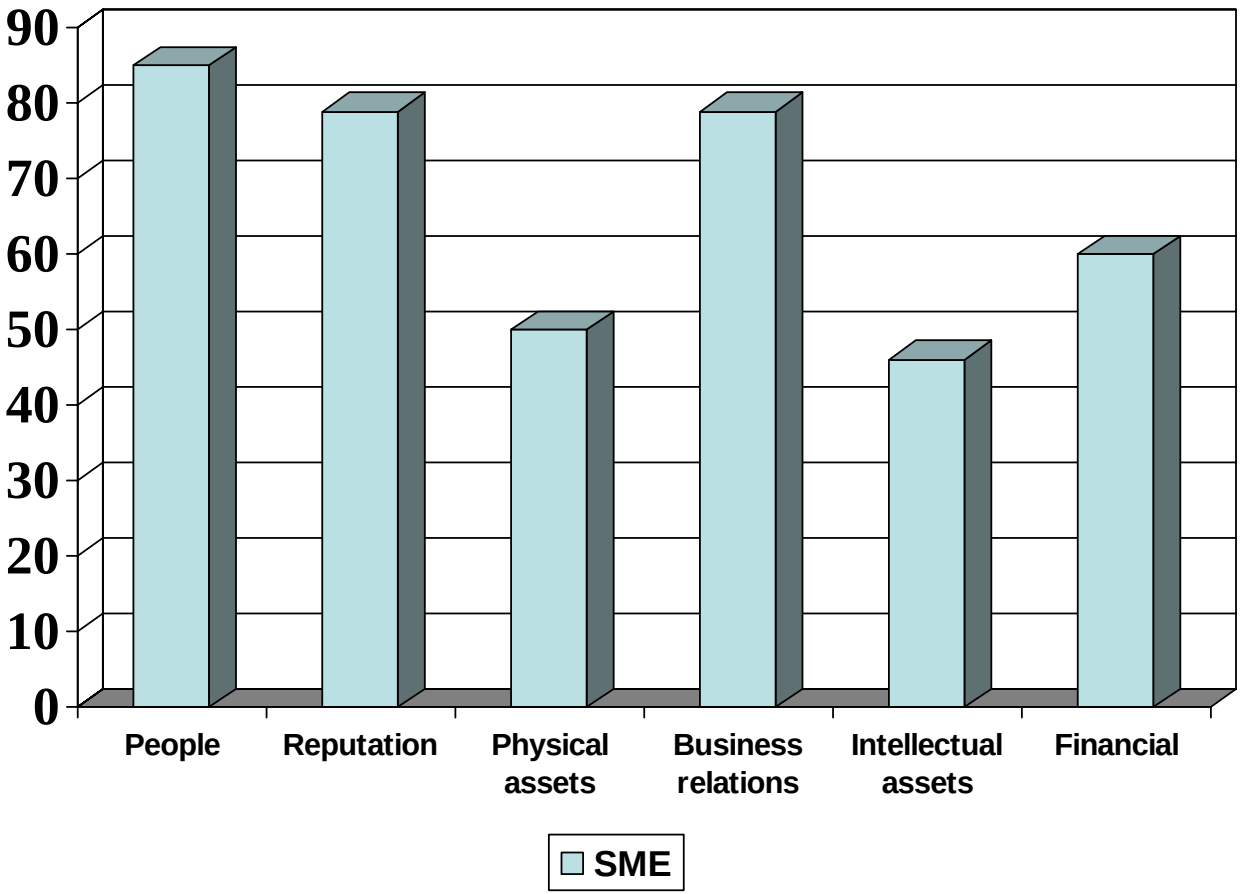

liverpool JMU

# Information Security – A New Thing…?

- The need for information security thousands of years old – the Caesar Code
- Rise in computing fed by information requirement
- 1960’s - ARPANET
- 1970’s - Security becomes an issue
- 1980’s – “UNIX OS System Security” (Grampp & Morris, 1984)
- 1990’s – WWW and the Internet, millions online
- 2000 and beyond – mobile security

# Security Breaches

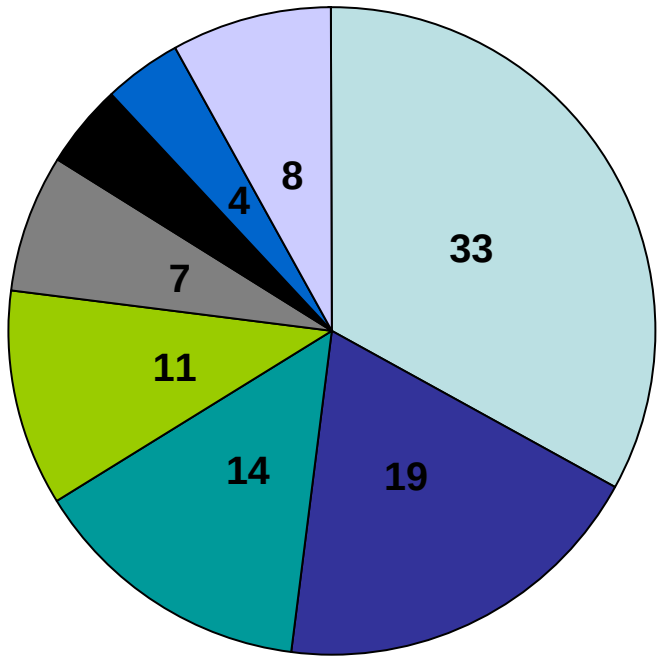
- Which assets are important to UK business




*Source: DTI/PCW Information Security Breaches Survey, 2002.*

# Security Breaches

- The worst security breaches in the last year




| | |
|---|---|
| Virus infection | Unauth access to conf data |
| Systems failure/data diruption | Hacking Web sites |
| Staff misuse | Fraud/theft |
| File deletion | Others |

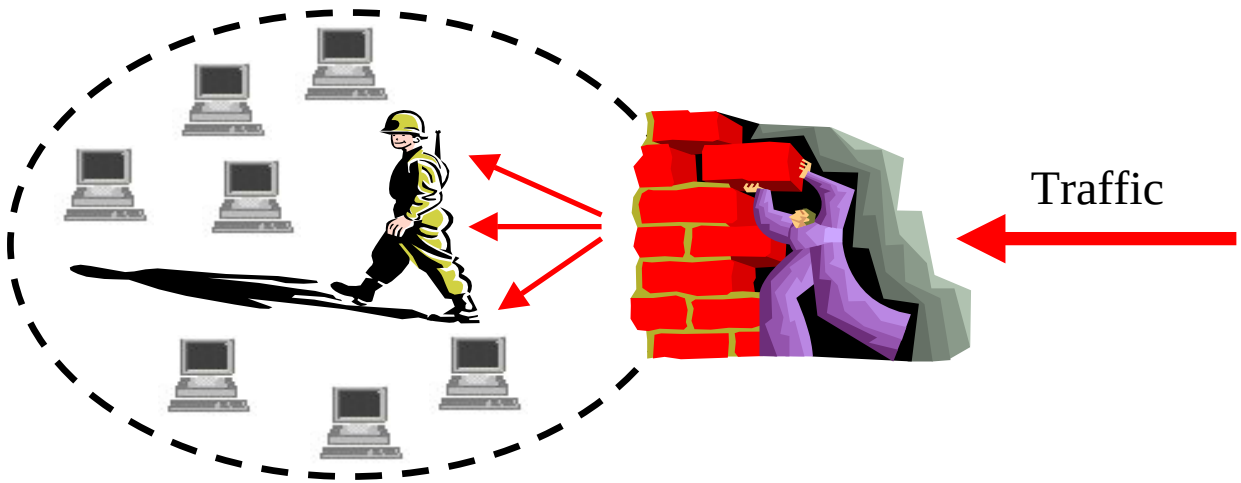
*Source: DTI/PCW Information Security Breaches Survey, 2002.*

# The Perimeter Model

- Accepted model of network security
- Define a perimeter, then place defence mechanisms to protect that perimeter
- Building “castles”
- Set policies enforced by security technologies, e.g. firewalls and IDS

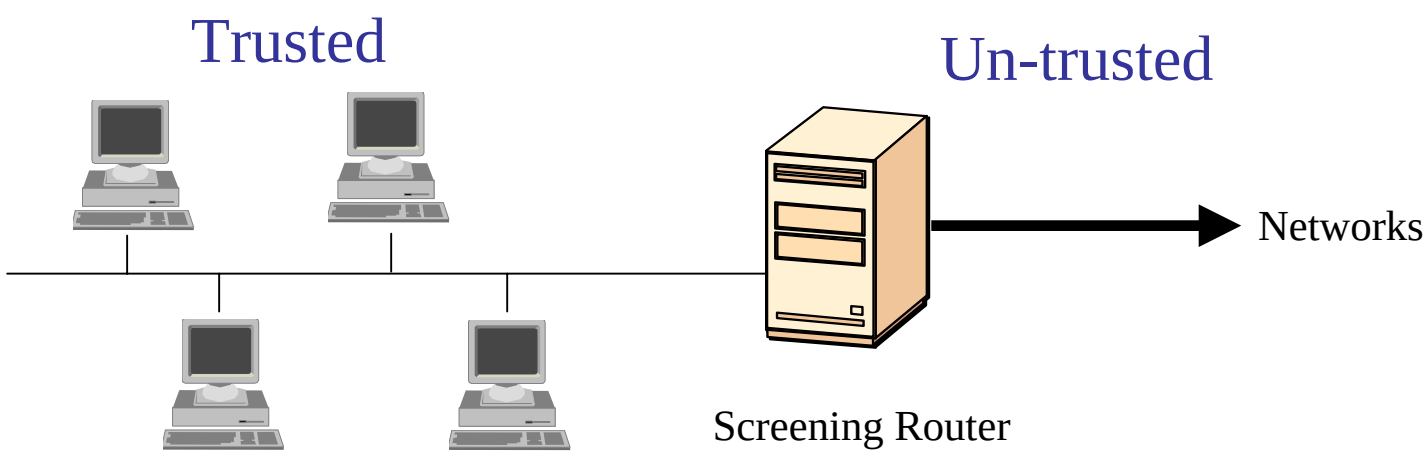
# The Perimeter Model

- Firewalls: enforce security policies regarding network traffic
- IDS: detect misuse or unacceptable behaviour within a network



# Firewalls

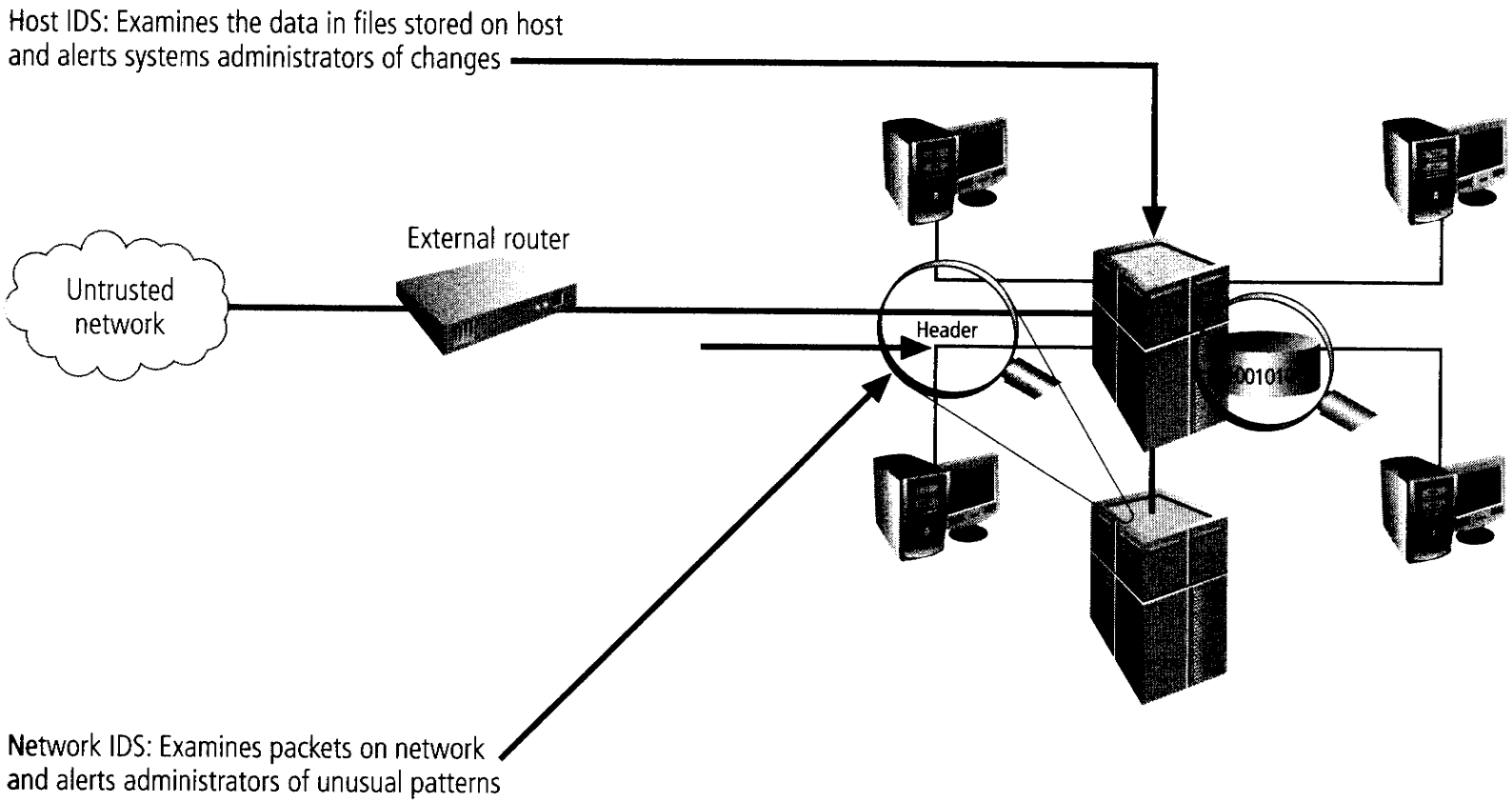
- Firewall is a process that filters traffic between trusted (inside) network and un-trusted (outside) networks
- Purpose is to keep ‘bad’ things outside the perimeter
- 3 types of firewall (different complexity): screening router, proxy gateway, and guards



# Intrusion Detection Systems

- Intrusion detection: “art” of detecting and responding to computer misuse
- Identifies individuals using a computer system without authorisation or are misusing their privileges
- Intrusion Detection Systems (IDS) detect violations of the security policy within the trusted domain
- Two main types of IDS
  - Host-based IDS
  - Network-based IDS

# HIDS and NIDS



# NIDS and Firewall Signatures

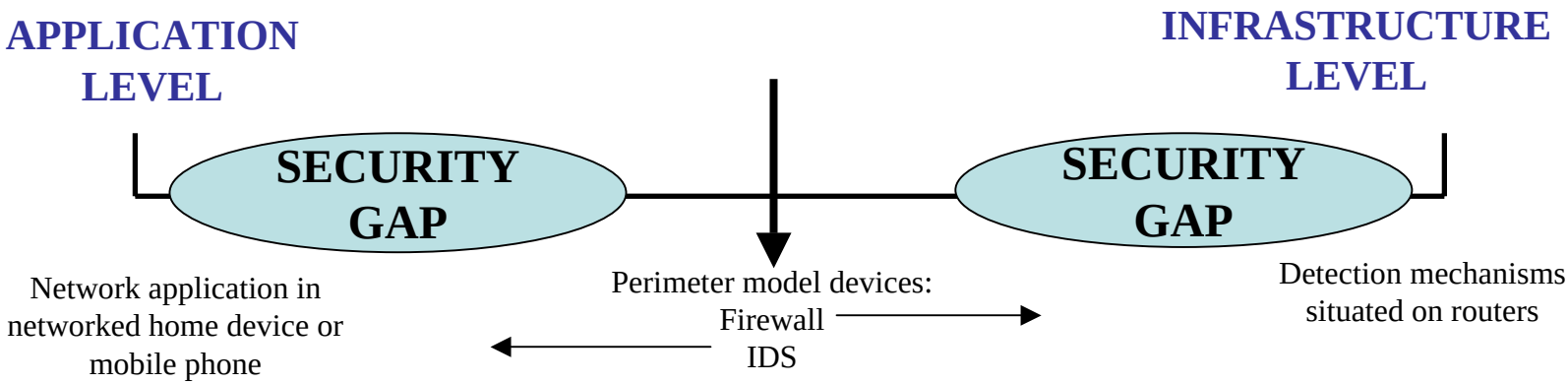
- Two types of signature: state-full and stateless
- State-full signature requires that state information is kept about the system being monitored
  - Code Red traffic upsurge
  - HIDS information for change management detection
  - Network traffic monitoring
- Stateless signature requires no state information about the system being monitored
  - IP Packet firewall header information
  - Code Red fixed byte sequence for HTTP request
  - Port 139 used in ‘winnuke’

# Current and Future Challenges

- Security in the future is going to be more complex
- Issues include:
  - Problems with the perimeter model – worms and denial-of-service attacks
  - Move to ad hoc, mobile networking – application-level security to WAN

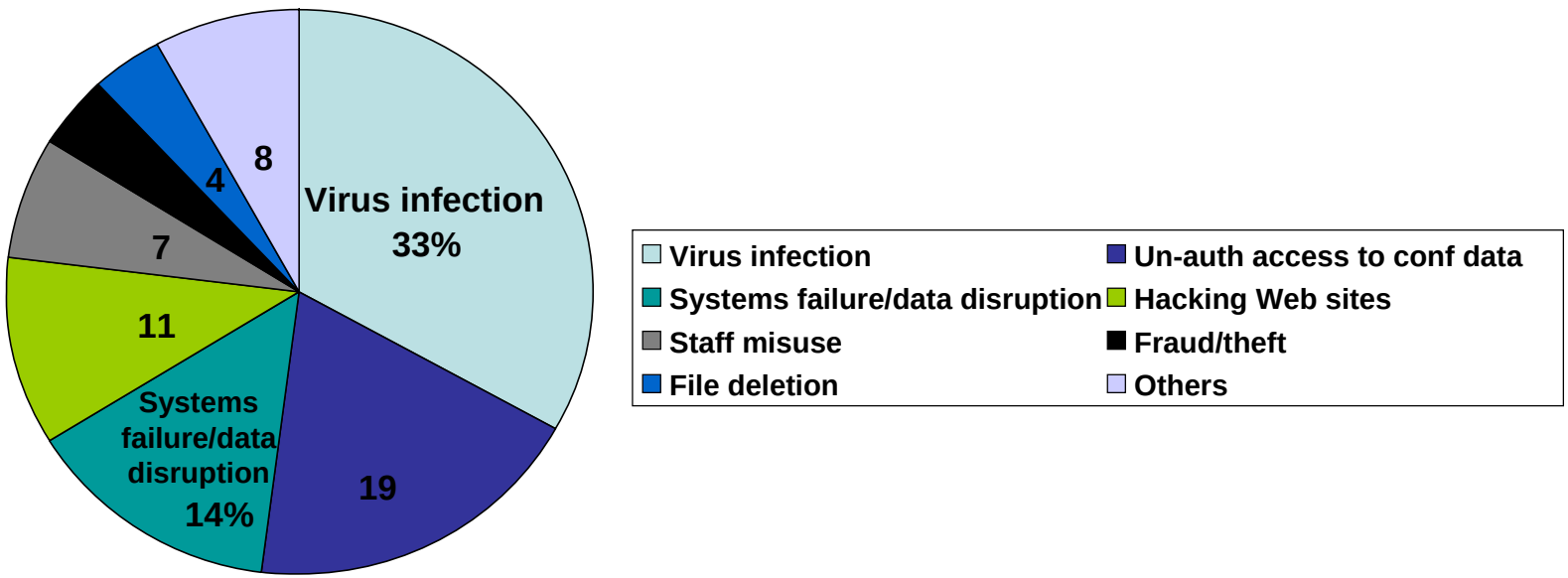
# Scale Issues

- Move to IPMSA and Ubiquitous Computing (UC) means that many devices may connect
- Security required at all levels of network device, from UC application in networked fridge to routing infrastructure
- This scaling not addressed by current security models such as perimeter model



# Perimeter Model Challenges

- Perimeter model is widely deployed by organisations as main defence
- False sense of security – rely on KNOWN attacks with particular payloads that can be quickly identified
- Impact of worms and denial-of-service attacks demonstrate severe limitations – yet account for 47% of attacks

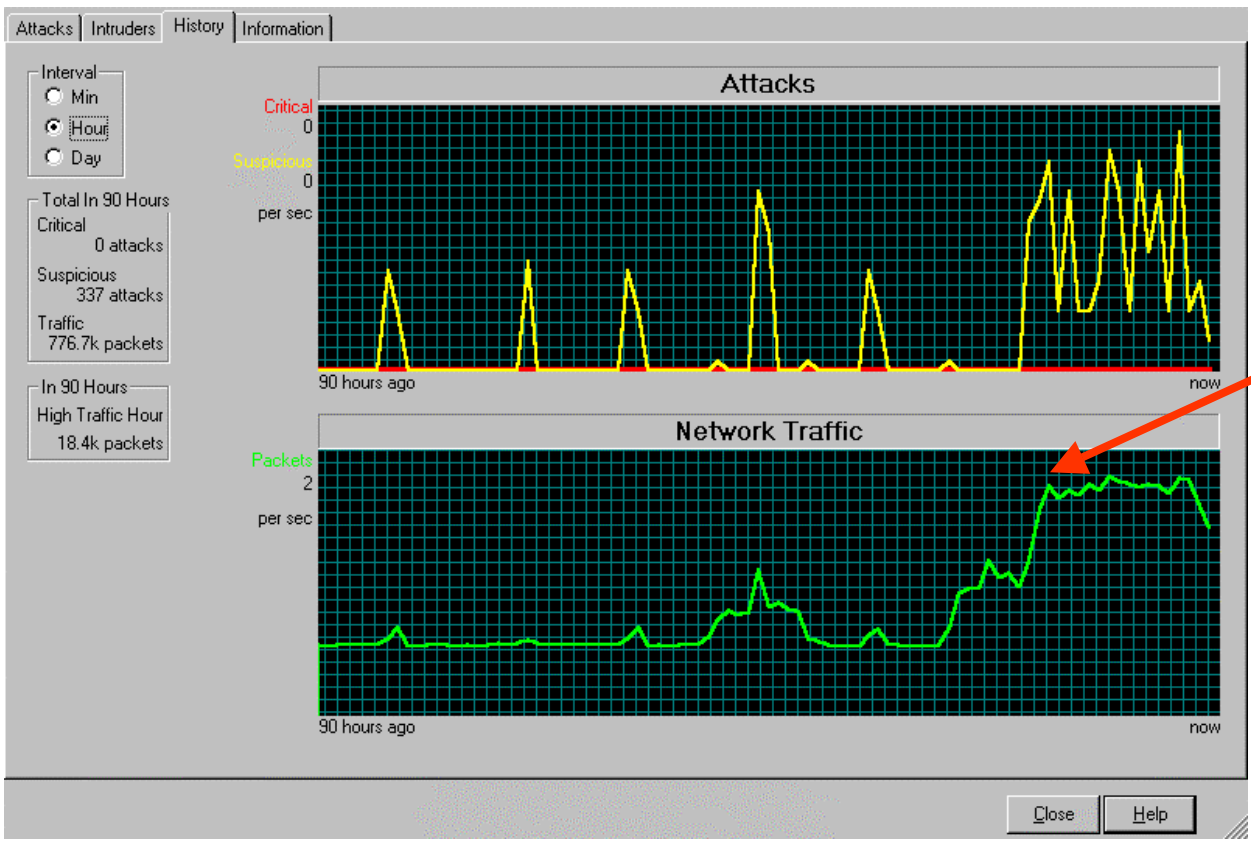


# Perimeter Model Challenges – Worms

- Worms are malicious programs that move rapidly through networks and automate the infection process
- For example, Code Red pervasive network worm causing widespread damage in 2001
- Infected over 360,000 vulnerable IP addresses in just 12 hours despite widespread deployment of firewalls and IDS
- Sent HTTP GET request to vulnerable Microsoft machines running IIS Web servers
- New worms released since (MS Blaster, Slammer, etc.)
- Propagate very quickly – Slammer worm in 2003 had an early doubling time of 8.5s

# Perimeter Model Challenges – Worms

- Impact of Code Red Worm on a network severe
- Large upsurge in network traffic as worm is triggered and attempts to infect other vulnerable machines




Attack starts

# Perimeter Model Challenges – Worms

- Traditional defence against worms is Anti-Virus software
- Code Red and other worms move through a network too quickly for AV software to be effective
- Firewalls and IDSs (like AV software) rely on KNOWN signatures, but this approach is too slow when defending against worms
- Therefore, new approach required

# Perimeter Model Challenges – Denial of Service

- Denial-of-Service (DoS) attacks prevent legitimate users from accessing data, systems, or resources
- Launched across networks or the Internet
- High-rate of data transfer leads to target paralysis
- Distributed Denial-of-Service (DDoS) attacks combine computers into attack networks to increase amount of data sent to the victim
- Easy to launch but difficult to defend against

# Perimeter Model – a Solution

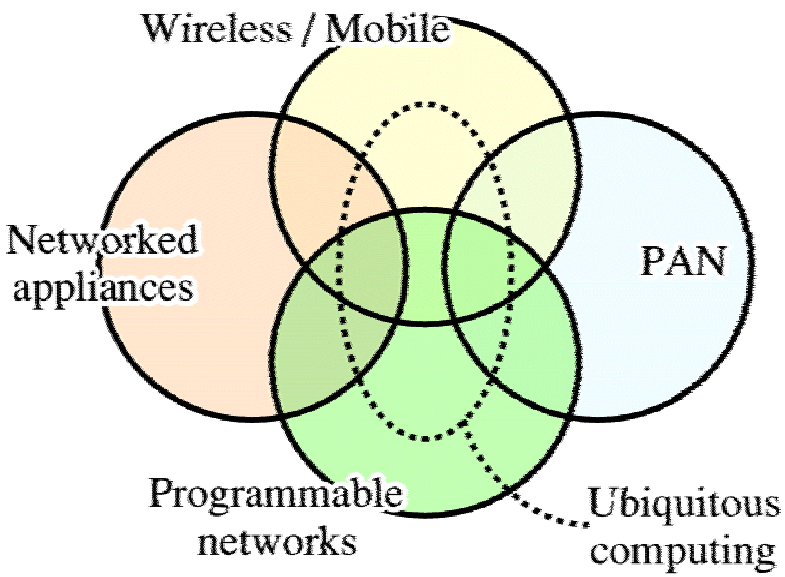
- Worms and denial-of-service attacks high upsurge in traffic to indicate an attack
- Use both state-full and stateless signatures
- We combine the two techniques to achieve fast and reliable detection of network worms and denial-of-service attacks:
  - Integrate detection system with congestion algorithm at the router to detect traffic upsurge
  - Apply fast string matching to suspicious traffic to verify the attack

# Wireless Networks

- Past few years have seen world become increasingly mobile
- Physical cables severely restrict users' movements
- Advantages of mobile networking: mobility, flexibility in rapid network deployment, cost reduction in physical components, etc.
- From known network topologies (fixed networks) to chaotic network topologies (wireless)

# Ubiquitous Computing

- Ubiquitous Computing lies at the natural convergence of
  - Personal Area Networks
  - Widespread networked appliances
  - High Bandwidth Mobile Networks
  - Programmable and Active Networks



# Ubiquitous Computing

- In such an environment we find the fluid movement of data throughout the network
- This includes both passive data and active executable code

Internet

# Wireless Security Challenges

- No policy enforcement
- Restriction of access to networks – authenticate all/restrict all?
- Deployment of perimeter devices in “perimeter-free world”
- The physical medium – anyone can intercept data in transit
- Lack of expertise in establishing and using wireless networks
- Privacy
- Integrity
- e-Commerce

# Wireless Security - Authentication

- Move towards Integrated Personal Mobility Services Architecture (IPMSA)
- Requirement to authenticate both the services we connect to (user view) and services we allow (administration view)
- WEP has shortcomings for authentication so move towards IETF's Extensible Authentication Protocol (EAP) for 802.1x
- However, EAP not without problems
  - Does not provide authenticity and integrity of any frames on the wireless network
  - Designed to authenticate the user – assumption that users will only connect to the "right" network or services

# e-Commerce

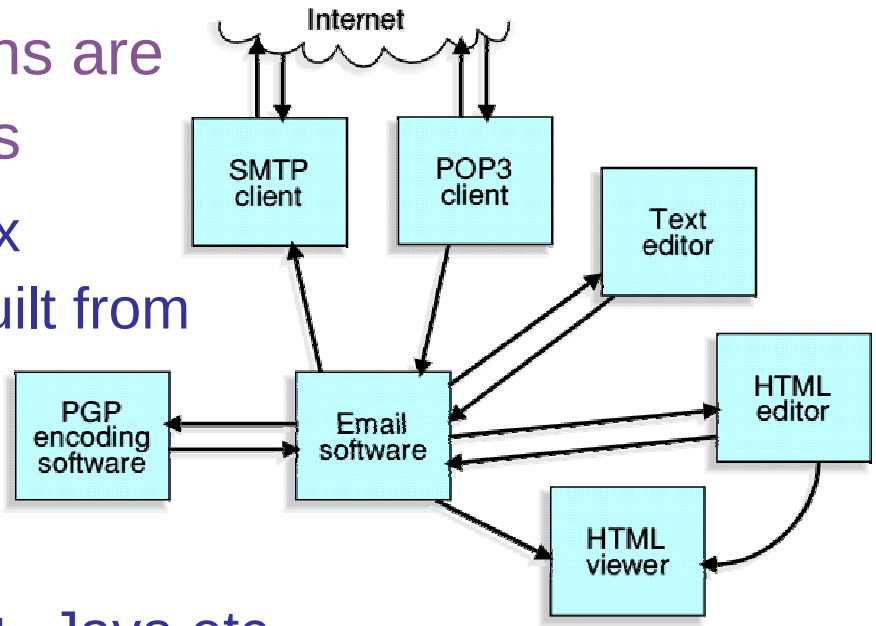
- The Internet and WWW has a wide range of users (500 million + worldwide and growing)
- Two important issues for e-commerce:
  - Non-repudiation of receipt: a recipient of a message/doc cannot falsely deny having received the message/doc
  - Fair exchange: for a fair doc exchange (e.g. payment for e-goods) between two parties A and B, if A has got B's doc, then B has got/can get A's doc, and vice versa

# Mobility

- The major downsides associated with executable mobility all relate to security issues
  - Currently the most common application for executable mobility in the user environment is that of viruses.
  - Executable mobility in the form of mobile agents present difficult privacy and QoS questions
  - In a mainstream environment, users are generally unwilling or unable to tackle all of the security issues

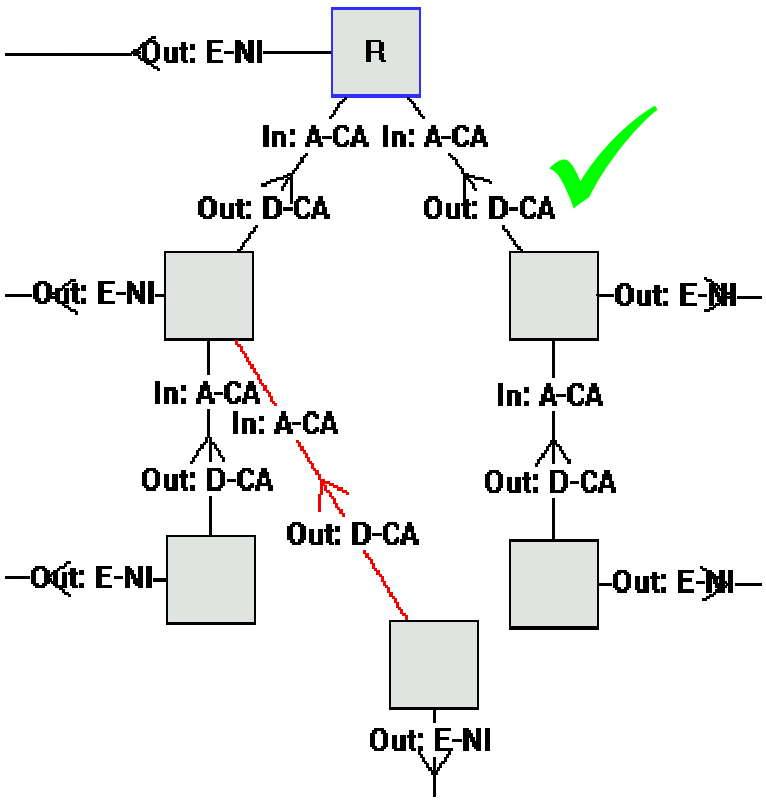
# Wireless Security – a solution

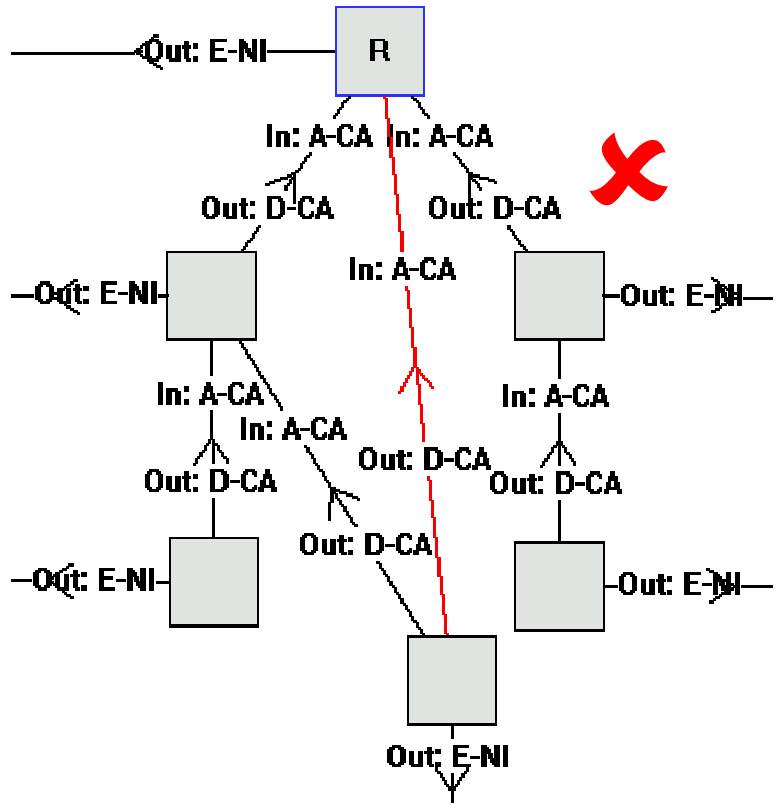
- Component composition
- All modern applications are built from components
  - They allows complex applications to be built from simpler parts
  - It suits the top-down procedural and OO paradigms of C, C++, Java etc.
  - Components can be reused, such as with OLE or DLLs
- In a Ubiquitous Computing environment, devices can be seen as components of a larger networked structure



# Wireless Security – a solution

- Our system uses component patterns that can be determined dynamically
- For example, for CA we must distinguish between various tree structure patterns



# Privacy

- Two different types of privacy in networks
  - Message/Content Privacy
    - E.g. I don't want you to read my email
    - Commonly termed "Confidentiality"
  - Behavioural/Contextual Privacy
    - E.g. I don't want you to know who I am talking to
    - "Untraceable Communications"
    - E.g. I don't want you to know my location
    - "Mobility Privacy"

# Privacy – a Solution

- Mobile Network Privacy Architecture (MNPA)
- System Security
  - Prevention of Fraudulent Activity
  - Mutual Authentication of Users and Networks
  - Emphasis is on the ‘network side’
- User Privacy
  - Privacy-enhanced Mobility Management
  - Privacy-enhanced Billing
  - Privacy-enhanced Routing
  - Emphasis on the ‘user side’

# Privacy – a Solution

- PRC : Privacy Routing Capability
  - End-to-end untraceable communications
- PTIA : Privacy Token Issuing Authority
  - Third party support for user activity, tokens allow pseudonymous access to Mobility and Billing
- Registration/Update
  - Mobility management maintaining privacy, and strong mutual authentication
- Billing
  - Services can be charged for but in an anonymous way, using the above components

# Summary

- Increasing need for security to protect our information needs from wide range of threats
- Legal infrastructure not in place to help us so must take charge of our own security
- Current accepted practice is to employ perimeter model devices, but not without its problems
- The future is going to require a security re-think due to the challenges we face
- Security from the application level through to routing infrastructure is required
- For more information: http://www.cms.livjm.ac.uk