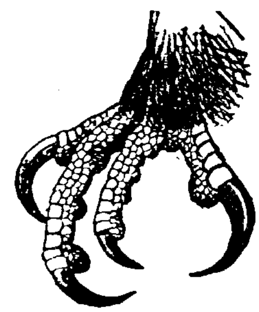
Active Security for Enterprise Networks

Eagle
Network Security
Management
System



Raptor Systems

So far, literally hundreds of attempted intrusions have been detected, reported, and thwarted at sites with the Eagle Network Security Management System

No known successful break-ins have occurred at these sites

The Problem : Business Risks in a Network Environment

Networks Security Risks = Business Risks

Business Risks

- Threats from economic espionage; outsider theft and vandalism; dishonest, disgruntled, or incompetent employees
- Vulnerability to competitor attack/exploitation, loss of customer confidence, questions of management competence, and stockholder suits

Inter-Network Security Risks

- WAN Security Devices -- the few available -- all require that you own and control the physical cables over which you are communicating; if you are using a common carrier for your inter-site communication, they can not help
- Routers -- often proposed as adequate "firewall" devices -- possess many inherent weaknesses as means for network security in that they:
  - store their control information in their own local memory; as such, if you wish to make a change in permissions, you either have to physically sit in front of each router and make the changes manually (tedious and error prone), or be able to reprogram them remotely (if you can, so can an abuser who has found the password)
  - provide a very limited logging capability that makes it difficult to detect/communicate trends indicative of suspicious activity
  - default to "allow" access, as their purpose is to push traffic -- not to secure
  - provide no ability to discriminate on the modes of file transfer

Intra-Network Security Risks

- No physical containment of external/internal access and mobility
- Most LAN security devices require smart card technology and/or encryption; if using a common carrier for inter-site communication, they can not help
- Ethernet "sniffing" is extremely hard to manage on an enterprise-wide basis because of the broadcast nature of the transmissions

Desktop Security Risks

- User accounts with easily guessed, privileged, or no passwords
- Individuals who have PCs on their desks with live modems attached leave open the very dangerous "back-door" to the entire network
- No practical way to provide security for every seat in the enterprise

The Solution : Active Security for Enterprise Networks

Eagle Network Security Management System

Inter-Network Protection: The Eagle Network Isolator™

- The Eagle is Unix-based software, a rules-based inference (expert) system, that requires a central Network/System Administrator to explicitly specify what kinds of communication will be allowed and when they will be permitted -- on a machine-by-machine basis
- Provides the ability to selectively control file transfer modes, capabilities, and access -- including specification of "put" and "get" authorizations
- Enables suspicious activity monitoring through the use of dynamic thresholds that can be specified in the rule base
- Supplements, and is compatible with, any other security products you may have
- The software sits on two dedicated workstations at the gateway -- not accessible remotely
  - the first workstation -- the G-Box -- runs the Gateway Controller software responsible for passing (and repackaging) all IP packets
  - the second workstation -- the A-Box -- maintains the sole Authorization File (for consistency) against which all connections must be approved
- The Administrator is immediately notified -- by screen alert, beeper, electronic mail, and/or facsimile -- about the specific details of attempted break-ins and suspicious activity
- The Eagle has self-protection built into it that ensures multiple levels of security -- including "physical" self-examination, destruction of non-root processes, self-encryption/decryption

Intra-Network Protection: The Eaglet Network Partitioner™

- The Eaglet, Unix-based software on a dedicated workstation at selected LANs, lets you partition your overall network into isolated subnets -- which are "hidden" from the rest of your network except where you specifically enable it
- Works in conjunction with the Eagle, performing functions similar to the "G-Box" and providing the same level of security
- Compartmentalizes LANs to secure departmental systems from each other, except as authorized by the Eagle
- Prohibits "sniffing" of a protected subnet

Intra-Network Protection: The EtherGuard Security Validator™

- EtherGuard is modified Telnet and FTP software -- residing on the Eagle and LAN-connected workstations, PCs, and Macs -- that contains desktop-level access
- Closes the very dangerous "back-door" left open by workstations, PCs, and Macs with modems -- EtherGuard checks for active modems and disables connections seeking access beyond the desktop, as dictated by site security policies
- Uses ARP to prove the physical identity of workstations, PCs, and Macs on your network (Ethernet-to-IP address verification) -- in order to prevent "spoofing"
- Engages a proven challenge-response system to confirm the identity of the hardware on workstations, PCs, and Macs -- requiring no action on the part of the user to accomplish this, nor can the user circumvent this at the software level

The Eagle Network Security Management System

Enterprise-wide Active Security for TCP\IP-based Networks

A rules-based Unix software system which provides a secure gateway between your network and the outside world, based on the TCP\IP protocol -- the fastest growing network standard

The Eagle provides mathematically provable levels of security in this environment

Raptor Systems Customers Represent a Cross-Section of Industries

Federal Government

Pharmaceutical Industry

Rubber and Plastics Industry

Chemical Industry

Defense Industry

Computer Industry

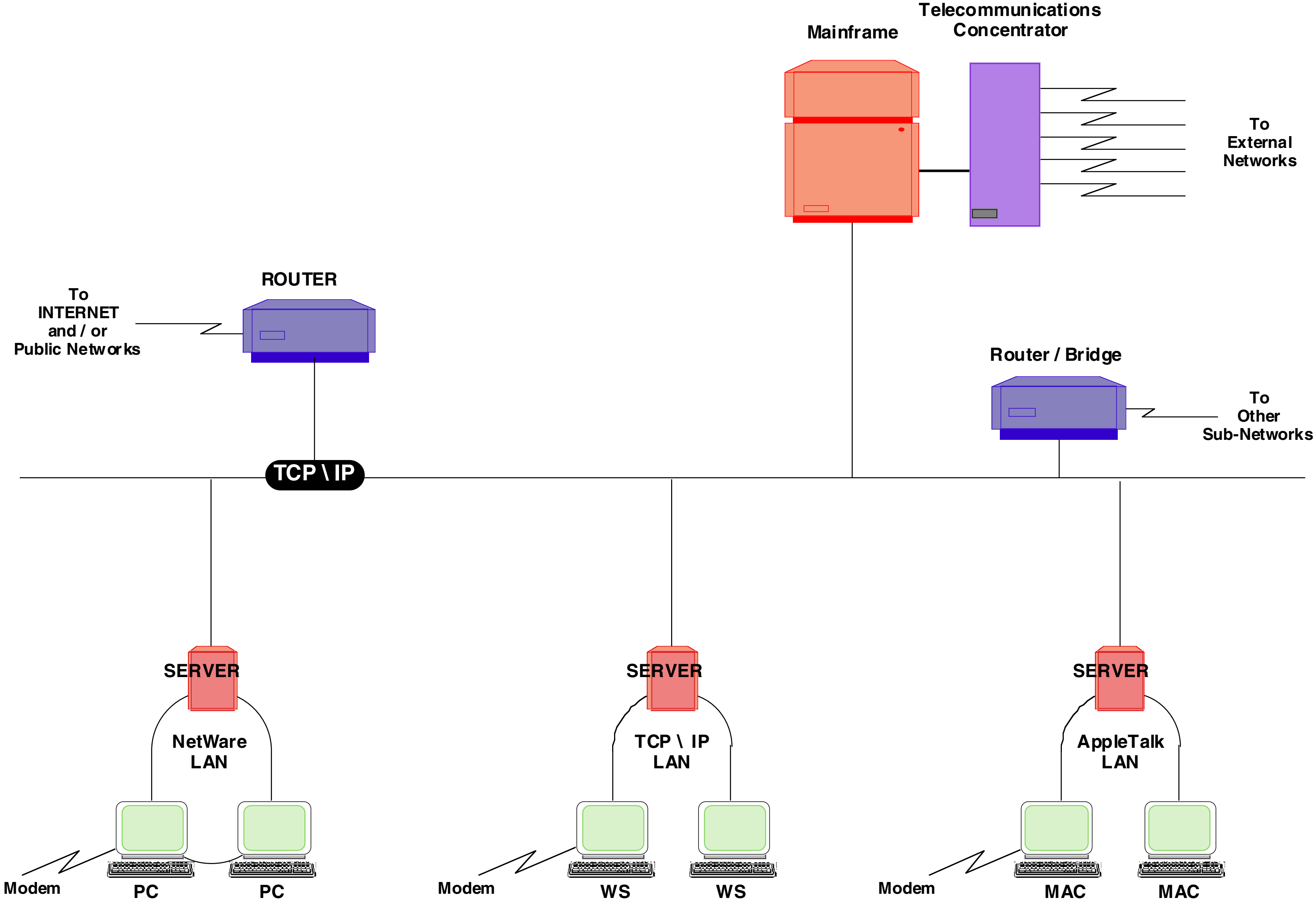
Utility Industry

Financial Services Industry

Management Consulting Industry

Raptor Systems

The Problem : Networks Are At Risk



The Solution : Enterprise-wide Active Security

Product Architecture
- Easy to Implement
- Easy to Use
- Easy to Maintain
- No Remote Login