Gauntlet™
Product Overview

Frederick M. Avolio

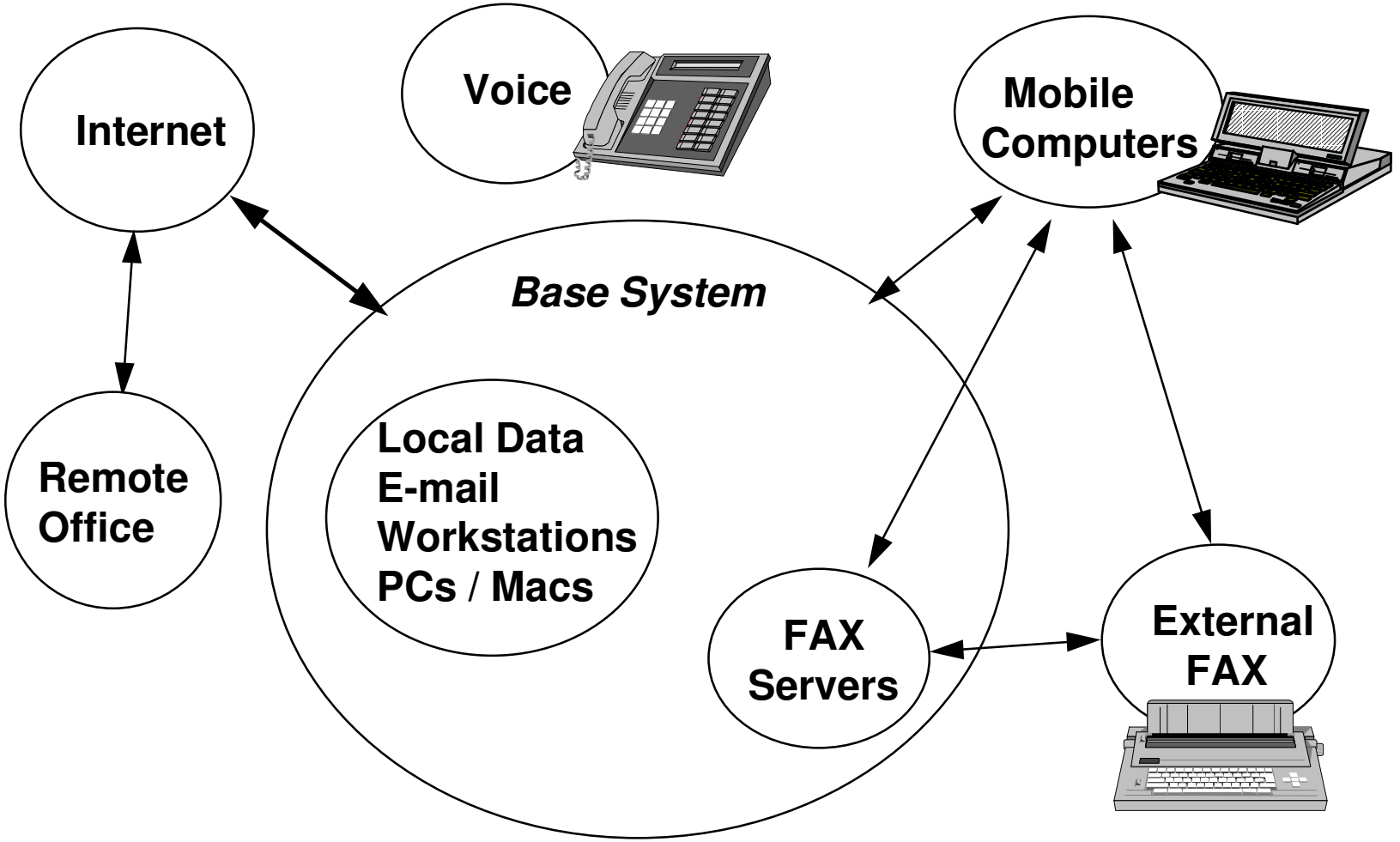
Trusted Information Systems, Inc.

301–489–5215

<avolio@tis.com>

tis

Domains of Threat



Domains of Threat

Network and System Security and Integrity

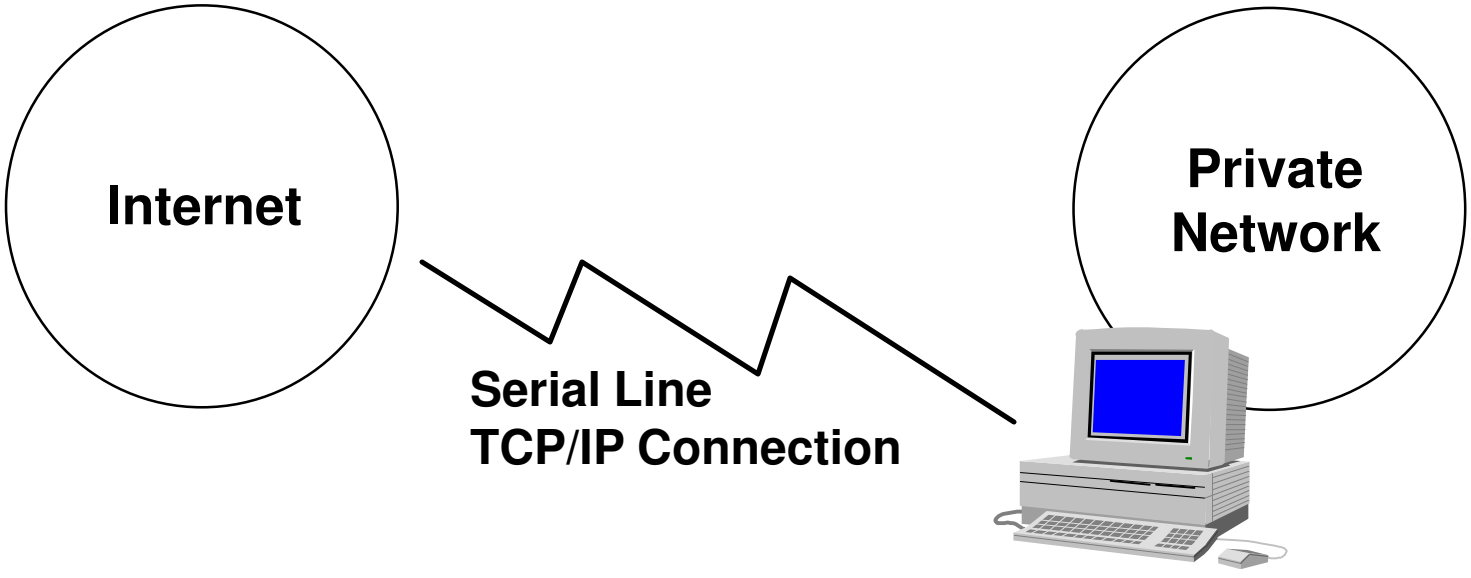
- **Connect a private network with another "outside" network**
- **Prevent unauthorized access to private data and resources**
- **Prevent or log export of private data (from "inside")**
- **Log any tampering**

tis

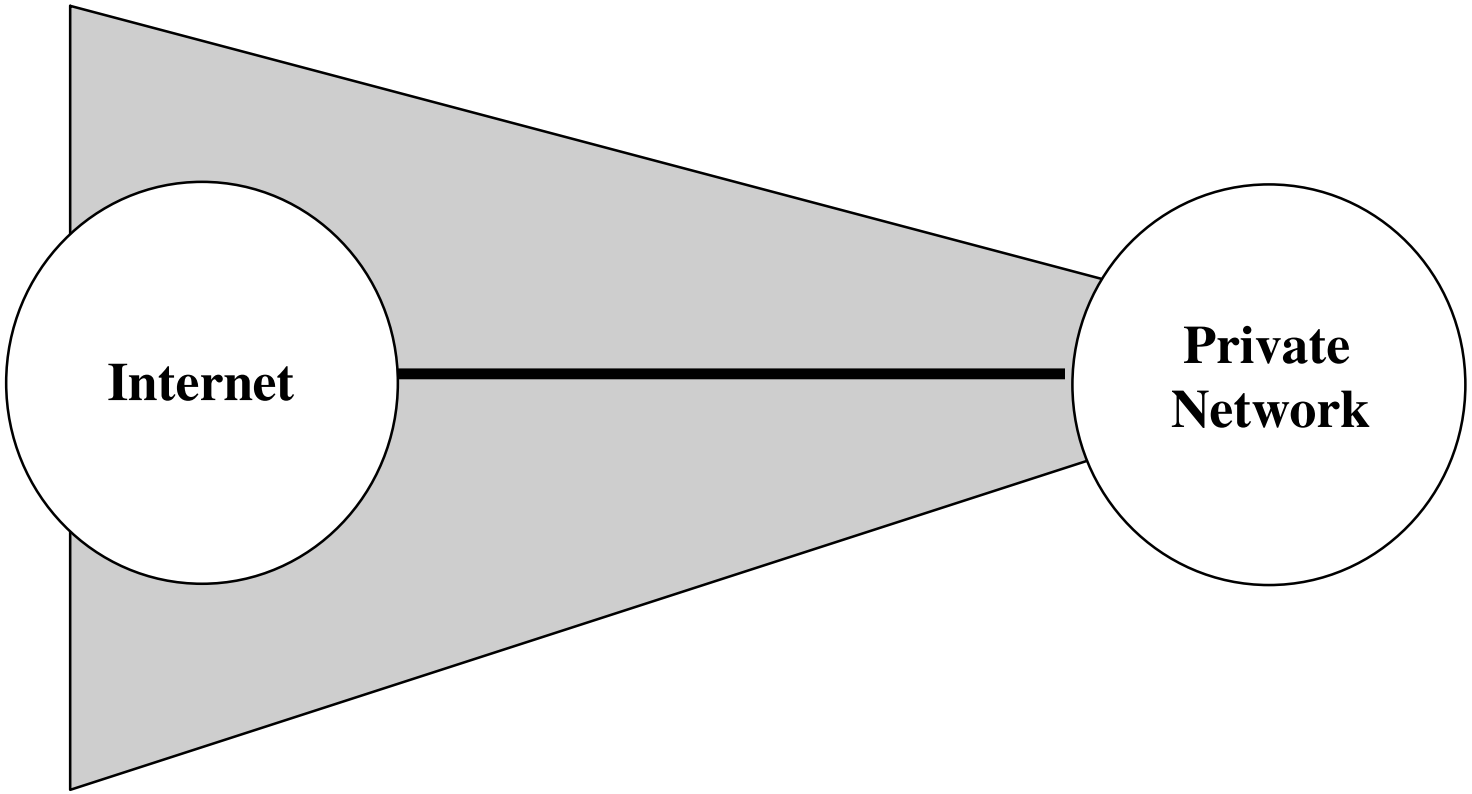
Domains of Threat

Domains of Threat

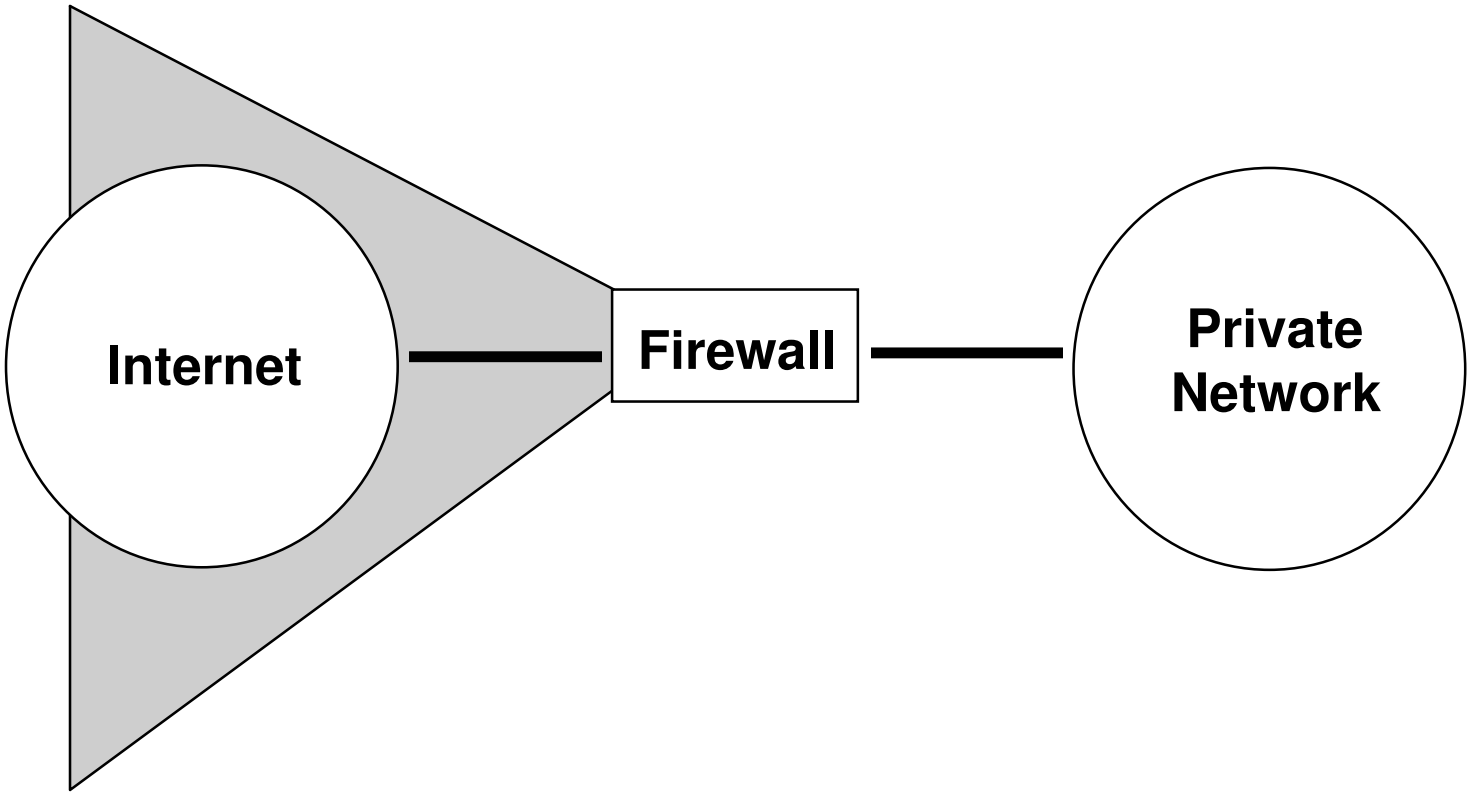
....And a single enterprising user



Domains of Threat



Domains of Threat



Why a Firewall?

- To protect one network from another
  - Keep out unauthorized users
  - Keep in private or sensitive data
- To comply with existing organizational policies
- To audit or log Internet usage
  - Justify connection through usage statistics
  - Pinpoint bottlenecks
- To act as a central point of contact for an organization (ex: *gatekeeper.dec.com, whitehouse.gov*)

tis

What are the threats?

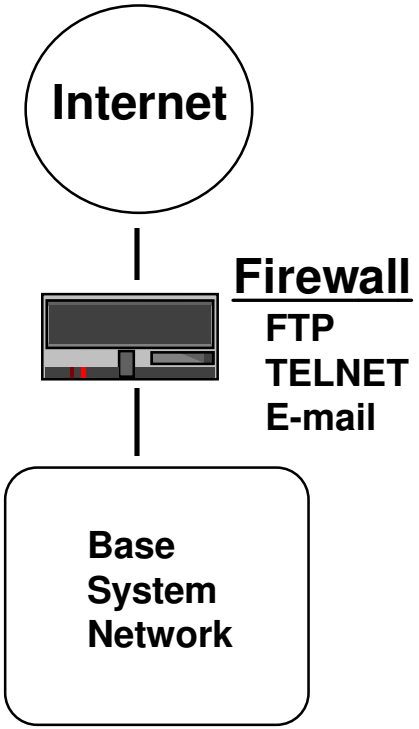
- **Curious crackers**
  - **Just poking around to see what they can get into**
- **Vandals**
  - **System downtime**
  - **Network outages**
  - **Telephone line use**
- **Industrial spies**
  - **Loss of trade secrets**
  - **Loss of competitive information**
  - **Loss of reputation**
- **Accidental data disclosure**
  - **Lawsuits**

Types of firewalls

- **Type 1: Packet Filtering Gateways**
  - **Screening Routers**
  - **Screening Hosts**
- **Type 2: Application Gateways**
- **Type 3: Circuit Gateways**

Internet Firewall

- Blocks direct traffic between Internet and base network
- All services are logged and audited
- Transparent to users
- Services can require strong user authentication



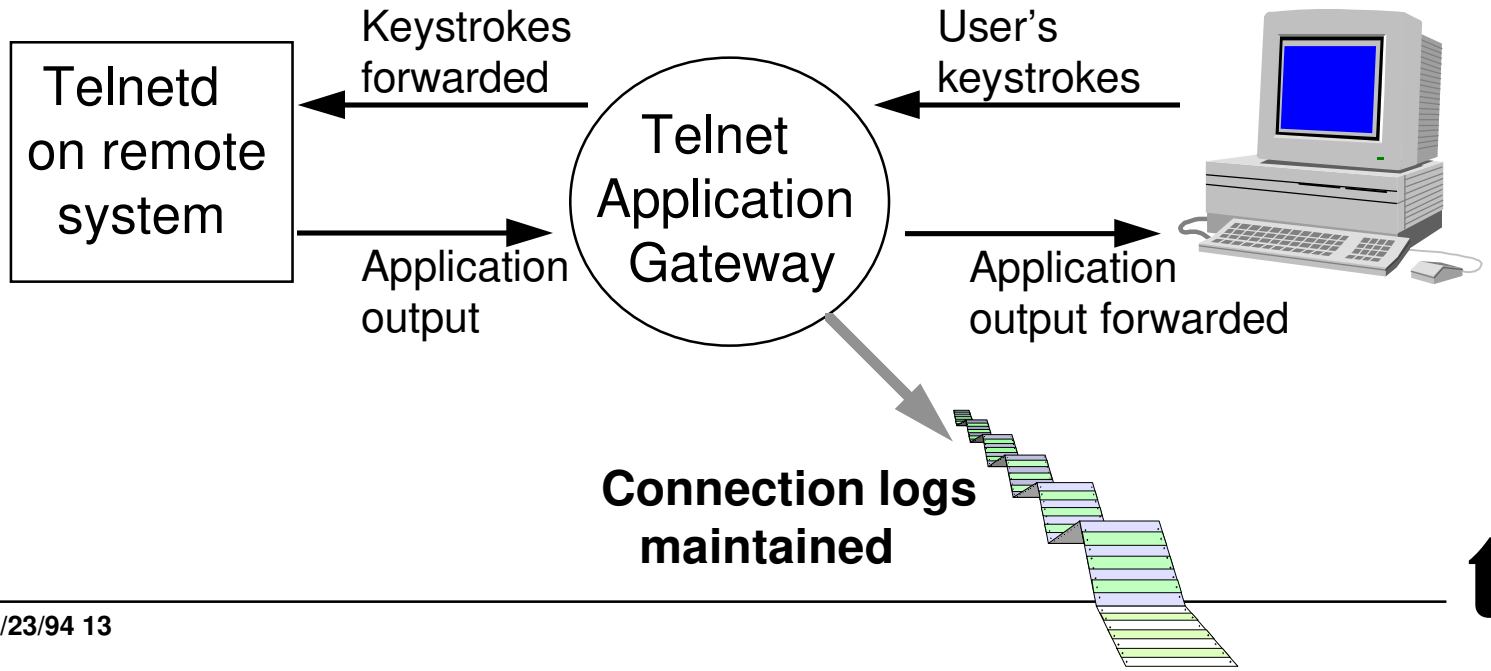
Type 2: Application Gateways

- **Bastion Hosts are systems identified as network “strong points”**
- **Often act in capacity of Email relays, name servers, FTP servers, USENET News servers, etc.**
- **Generally, a Bastion Host is one that is recognized as a potential point of attack (e.g., *whitehouse.gov* or *dockmaster.ncsc.mil*)**

tis

Type 2: Application Gateways

- **Application Gateways (AKA Proxies) handle store and forward traffic and some types of interactive traffic**



tis

Proxies / Application Gateways

- Since Application Gateways handle traffic at an application level, they understand the protocol of that application, and can log/audit traffic
- Application Gateways can have extra security/Authorization built into them as needed
- Examples:
  - E-mail
  - Tereminal Service
  - File tranfer

Strong User Authentication

- **"To establish the validity of a claimed identity or to provide protection against fraudulent transactions by establishing the validity of … [the] individual …" — NCSC "Red Book"**
- **Ideal security combines something secret that a user *knows* with something physical that a user *has* in their possession**

tis

Strong User Authentication

- Passwords should never be transmitted in clear over untrusted networks
- Requires applications to support chosen authentication mechanism
- Often hard to integrate with existing hardware base (ex: terminal servers)
- Lack of standards

TIS Internet Firewall Toolkit

- Made freely available on the Internet October 1, 1993
- Provide a freely available set of tools for building internetwork firewalls
- Focus on components that are flexible enough to be useful in different types of firewall configurations
- Improve security for the Internet community by providing a common starting point that is widely used and understood
- Provide a centerpiece for further development and enhancement

tis

TIS Internet Firewall Toolkit

- Retrieved by over 2000 sites (as of July 23, 1994)
- Over 500 installations on 6 continents
- De facto standard for Type 2 Internet firewalls

tis

TIS Internet Firewall Toolkit

- **Design Philosophy**
  - A framework for thinking about firewalls
  - Based on practical experience
- **Configuration Practice / Verification Strategy**
  - Approaches to systems management that minimize risk
  - Software and system security that is empirically verifiable
- **Software Tools**
  - Proxy servers for FTP, TELNET, rlogin, FTP
  - Compartmented SMTP exchanger
  - User authentication server
  - TCP service access control
  - Common configuration for all components

TIS Internet Firewall Toolkit

Design Philosophy

- Simple and understandable methods and mechanisms (minimalism)
- Complex applications more likely to have bugs and bugs are harder to find; Run services without special permissions if possible (reductionism)
- Source code for security-related software must be available, readable, and able to be examined ("Crystal Box")
- Don't impose a security policy (configurable)

tis

Network Security Paradigms

- **That which is not expressly prohibited is permitted**
  - **Firewall blocks services that are known security risks**
  - **Users can potentially introduce security holes in system**

- **That which is not expressly permitted is prohibited**
  - **Firewall blocks everything**
  - **Administrator must take steps to support each service**
  - **Implicitly “dis-empowers” users**

tis

Defense Paradigms

- **Defense in Depth:**
  - **Protect all access to hosts, enforcing strict security policies on each system that is on network**
  - **Within the network, hosts require strong authentication for trust**
  - **Restrict connection to the network**
  - **Centrally manage all desktop computers**

- **Perimeter Defense:**
  - **Protect all access paths leading into the network**
  - **Consider internal network "safe" environment**
  - **"Crunchy shell around soft, chewy center"** ***(Cheswick, Bell Labs)***

tis

Gauntlet™ Firewall

- Commercial Firewall product from TIS
- Version 1.0 = (TIS Internet FWTK) + …
  - Commercial Quality Documentation
  - Management Tools
  - Reporting Tools
  - Full software maintenance and update services from TIS
- Features
  - Terminal Services — Telnet, rlogin
  - File Transfer — FTP
  - Electronic Mail — SMTP
  - Usenet News — NNTP
  - User Authentication Server

tis

Gauntlet™ Design

- **Part of a security perimeter that can be built and defended**
- **Minimalism**
  - **"That which is not expressly permitted is prohibited."**
  - **Easier to guard 10 "paths" than 1000 "paths"**
- **Reductionism**
  - **Small, readable, software modules for all security related software**
  - **Anything that must remain large is run in a "steel cage"**
- **"Crystal Box"**
- **Auditable**
- **Configurable**

tis

Gauntlet™ Proxies

- **Tn-gw**
  - **TELNET protocol proxy**
  - **May be configured to require authentication based on origin of connection**
  - **All connections and amount of data transferred are logged**
- **Rlogin-gw**
  - **Rlogin proxy**
  - **May be configured to require authentication based on origin of connection**
  - **Supports transparent pass-through with *user@host***
  - **All connections and amount of data transferred are logged**

tis

Gauntlet™ Proxies

- **Ftp-gw**
  - **FTP protocol proxy**
  - **Can require authentication based on origin of connection and type of operation requested**
  - **May selectively block FTP commands based on origin of connection**
  - **All connections and traffic logged**
  - **May selectively log and summarize specified FTP commands**
- **Plug-gw**
  - **Generic TCP "plug-board" proxy**
  - **Useful for transparently "gatewaying" USENET news through a firewall**

tis

Gauntlet™ User Authentication

- "One-time passwords"
  - S/Key
    - » Freely available software from Bellcore
  - SecurNet Key
    - » Digital Pathways
    - » "Crystal Box" Algorithm
    - » Challenge/Response
  - SercurID
    - » Security Dynamics
    - » Time-based
    - » ACE Server Required

tis

Gauntlet™ Firewall

- **Next Version**
  - **Intel 486 Platform (Pentium upgradeable)**
  - **Additional Proxies**
    - » **World Wide Web — HTTP**
    - » **X Window System — X11**
  - **User Installable**

- **Federal Government Clients**

- **Commercial Clients**
  - **Financial**
  - **Pharmaceutical**
  - **Chemical**
  - **Manufacturing**
  - **Legal**

Gauntlet™ Firewall

- "Crystal Box"
- Configurable
- Verifiable
- Audit Capabilities
- Application Gateways
  - Terminal Services
  - File Transfer
  - Electronic Mail
  - Usenet News
  - World Wide Web
  - Other Services

TIS Packages Security Services

- Gauntlet™ Firewall
- Security Survey
- Security Survey With Policy Development
- Network Security Analysis
- Firewall Security Analysis
- Firewall Vulnerability Testing
- Security Training

tis