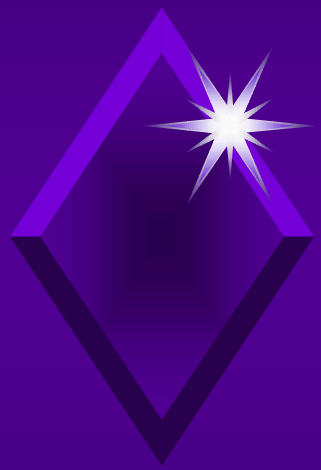
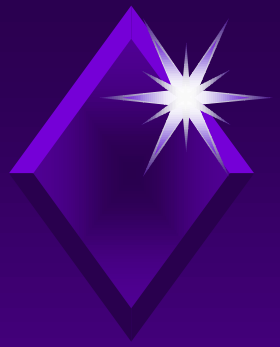
Internet Security
PITAC NGI Committee

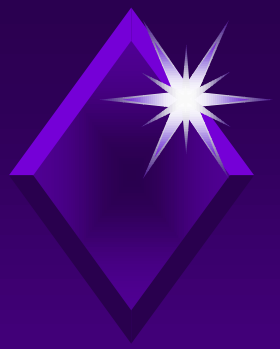


February 2000



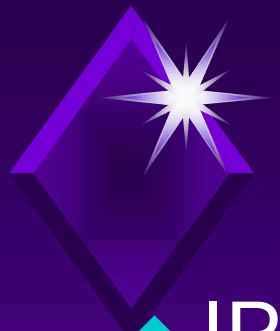
Observations

- No panaceas - security and reliability are big challenges
- Denial of Service hard to defend against
  - Mostly “legal” traffic, just too much
  - Insecure hosts infected w/zombie diseases
- Vulnerabilities
  - insecure configurations (shipped!)
  - lack of cyber hygiene (periodic self-exam)
  - Operating system holes (upgrade problem)



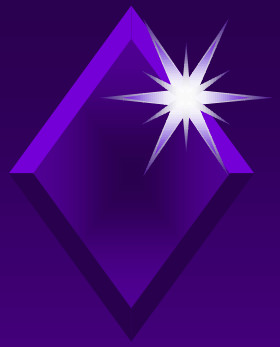
Observations (2)

- Onerous, Complex Security Procedures (rituals) - anything but transparent
- Failure to take into account “inside” risk
  - Firewall mentality
  - NAT boxes interfere w/end-end security
- Physical security holes (e.g. satchel bombs against 13 root servers)



Challenges

- IP spoofing
  - Source validation - heavy CPU demand
- DOS Attacks
  - Deny access/use of zombies
  - Tools to trace (real-time or post-attack)
- Social Engineering
- OS Vulnerabilities
- Physical Vulnerabilities



Challenges

- Create Public Key Infrastructure
- Educate System Operators
- Supply Motivation for Cyber Hygiene
  - In many cases, hygiene protects OTHERS from attack using your resources. You get the expense but no specific gain
- Simplification of Security Procedures