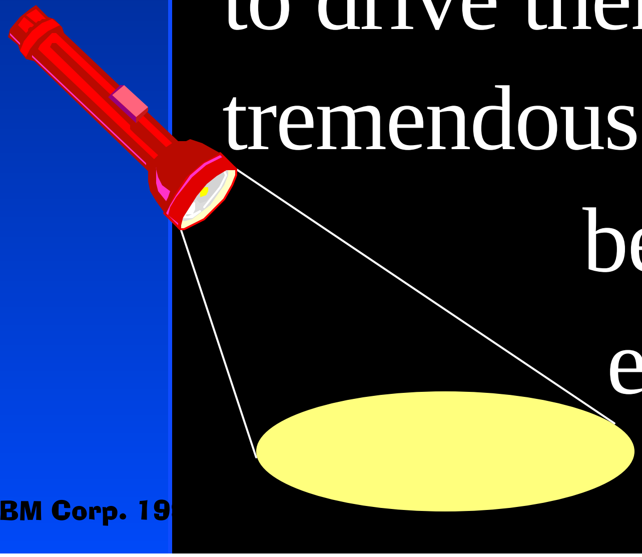
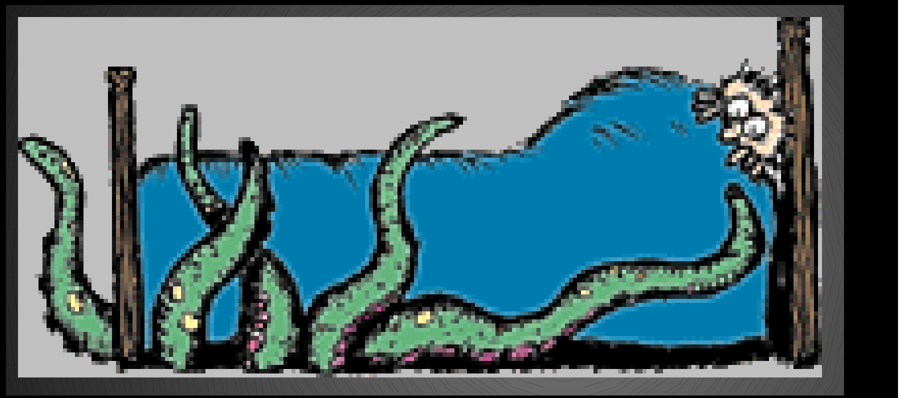
What hackers don't want you to know...

Jeff Crume
IBM
Advanced Tech Support
crume@us.ibm.com

Disclaimer

This presentation is not designed to **scare** but to **inform** (although it may do a bit of both). It is hoped that by shining a light on the monsters of Internet security we will be able to drive them away and ultimately realize the tremendous benefits of e-business.

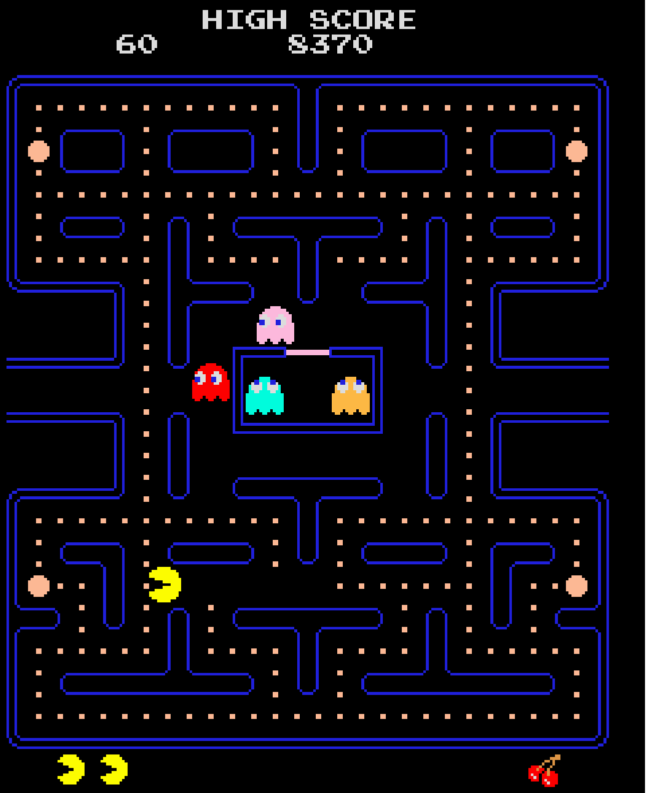




What is a Hacker?

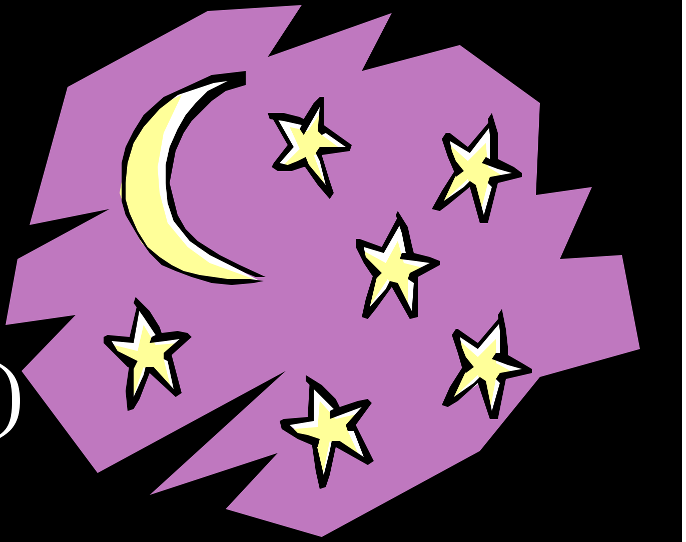
- Merriam-Webster's Collegiate Dictionary
  - an expert at programming and solving problems with a computer
  - a person who illegally gains access to and sometimes tampers with information in a computer system
- hacker types
  - novice, intermediate, elite
- work for:
  - self, hacker organizations, companies, governments, organized crime, political action groups ("hacktivists")
- tend to be:
  - antisocial, arrogant, cliquish, secretive

What do they want?



- fame (infamy)
  - cult status
- revenge
- sense of accomplishment
  - video game mentality
  - disembodied organizations are opponent
  - "the bigger they are, the harder they fall"
    - Who has the highest score?

When do they attack?



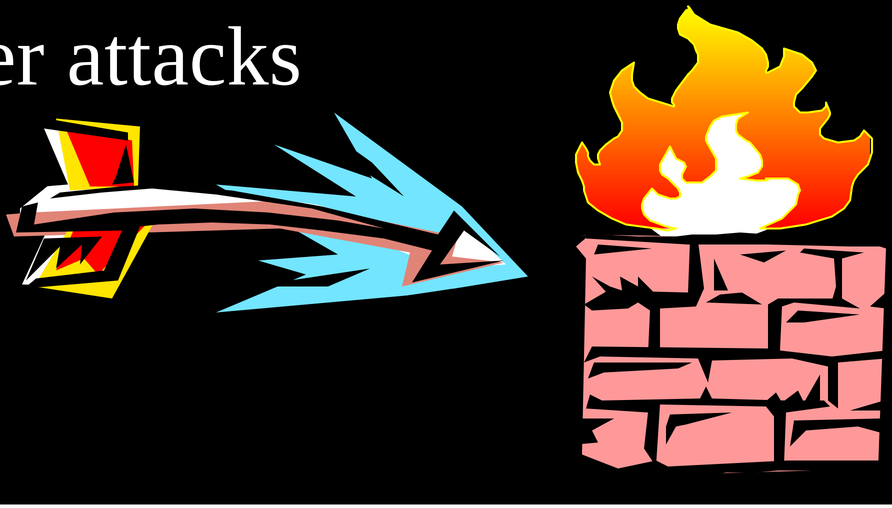
- usually not M-F 9-5
- they are
  - at work (I/T professionals)
  - at school
  - asleep
- attacks occur when you are most vulnerable

What you don't know can hurt you ...

- common misconceptions
- hacker techniques
- well-known security holes

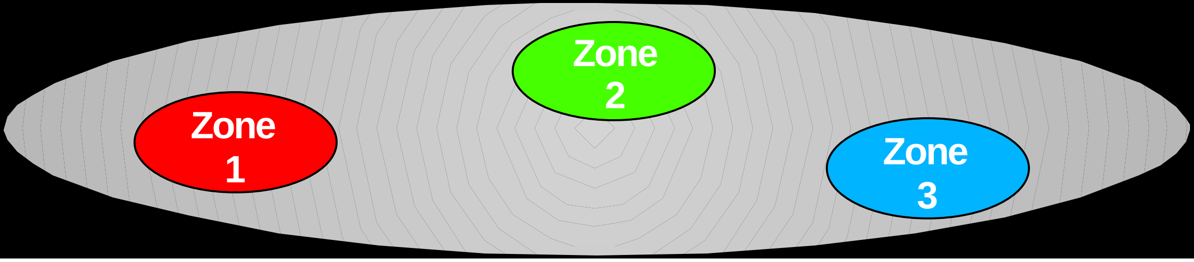
Firewalls are just the beginning

- first line of defense
  - could be single point of failure
- filter rules are error-prone
- can't detect many types of attacks
  - can't tell if the packet is malicious
  - insider attacks

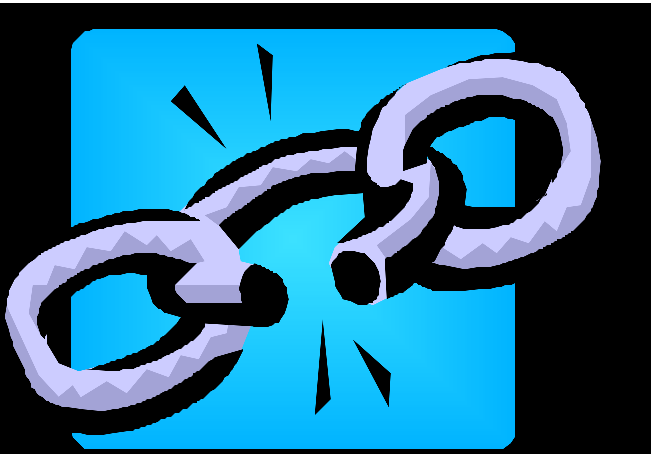


Many attacks occur from within

- perimeter firewalls don't help
  - intranet firewalls
  - security zones
- access privilege admin critical
  - "single action management"
  - periodic review
- well-known policy needed

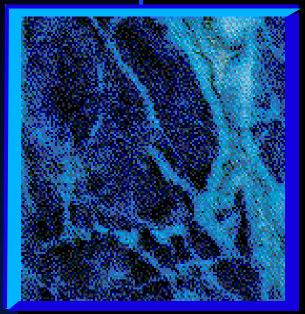


Humans are the weakest link



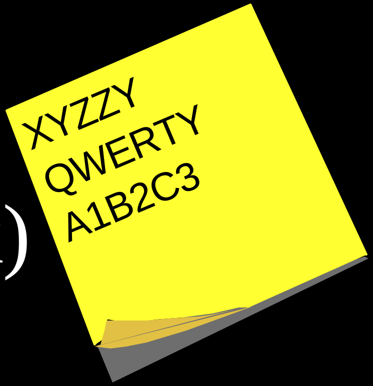
- social engineering
  - HD call #1: "I lost my pw..."
  - HD call #2: "I forgot my id ..."
- "dumpster diving"
- newsgroups
  - info leaks
  - incriminating info
- policies are inadequate or nonexistent

inetdog2.g

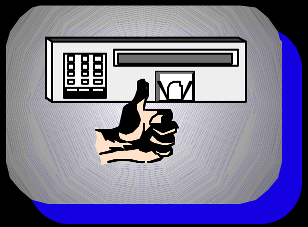


Passwords aren't secure

- problems
  - trivial pw's
  - offline attacks (L0phtCrack)
    - some claim 30% success rate
  - yellow sticky pads



- solutions
  - single sign on
  - "strong" authentication based on combination of something you:
    - know (pw, PIN)
    - have (smart card, token)
    - are (biometrics)



They can see you but you can't see them

- sniffing (good)
  - tools originally designed for network PD
- snooping (bad)
  - same techniques used to gather info
  - L0phtCrack's SMB packet capture
- inherent weakness of shared media
- solutions:
  - VPN technology
  - highly segmented LAN's
  - physical security

Downlevel software is vulnerable

- buffer overflows
  - Eudora, MS Outlook, NS Communicator
- false fixes
  - bogus MS Outlook fix from Bulgarian hackers
- fragmented, spoofed packets
  - teardrop, land
- service mismatch
  - telnet to unexpected port

Defaults are dangerous

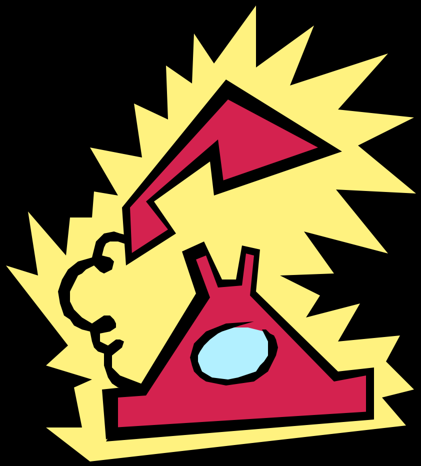
- default settings for many products are inappropriate
  - default userids/pw's
  - default services turned on
- webmasters may be more concerned with content than with security

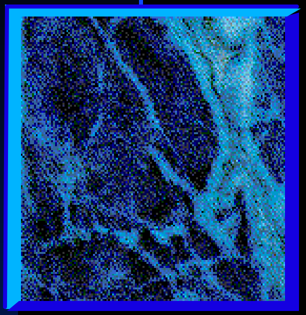
It takes a thief ...

- well-known attacks
  - teardrop, land, snork, smurf, ping of death, bonk, boink, etc.
- bugtraq (www.geek-girl.com/bugtraq/)
- phrack (www.phrack.com)
- 2600 (www.2600.org)
- CERT (www.cert.org/advisories/)

Attacks are getting easier

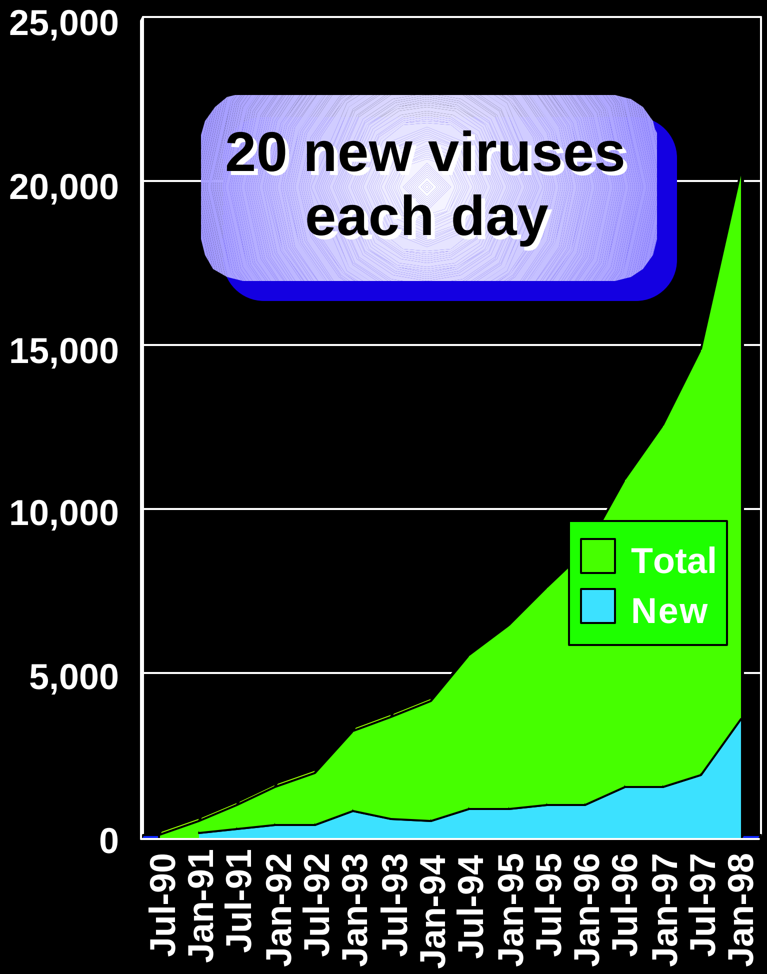
- scanners (e.g. SATAN)
- Back Orifice
  - reveals cached pw's to hacker
  - remains hidden (not on C-A-D task list)
- other Denial of Service attacks
  - mail bombs
  - SYN flood
  - ping variants
  - "the phone is ringing ... I'll answer it"





Virus protection is inadequate

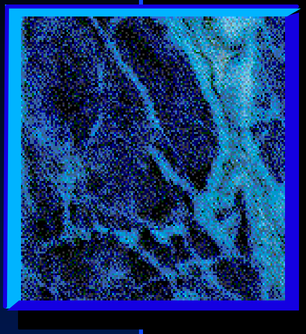
- virus stats
- danger increases
  - e-mail, CIH, Remote Explorer
- virus hoaxes
  - www.av.ibm.com/ BreakingNews/HypeAlert
- need automated updates



20 new viruses each day

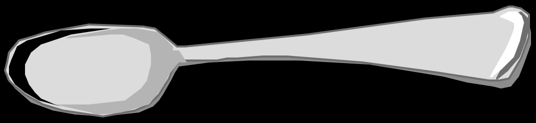
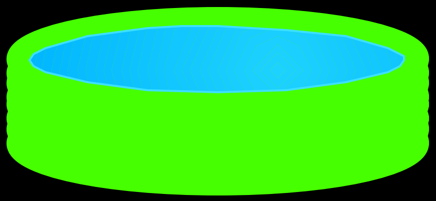
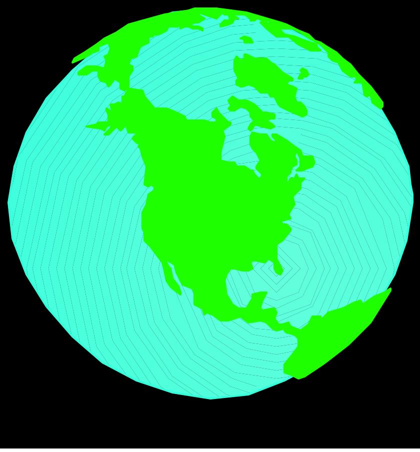
Source: www.drsolomon.com/vircen/

Virus.r

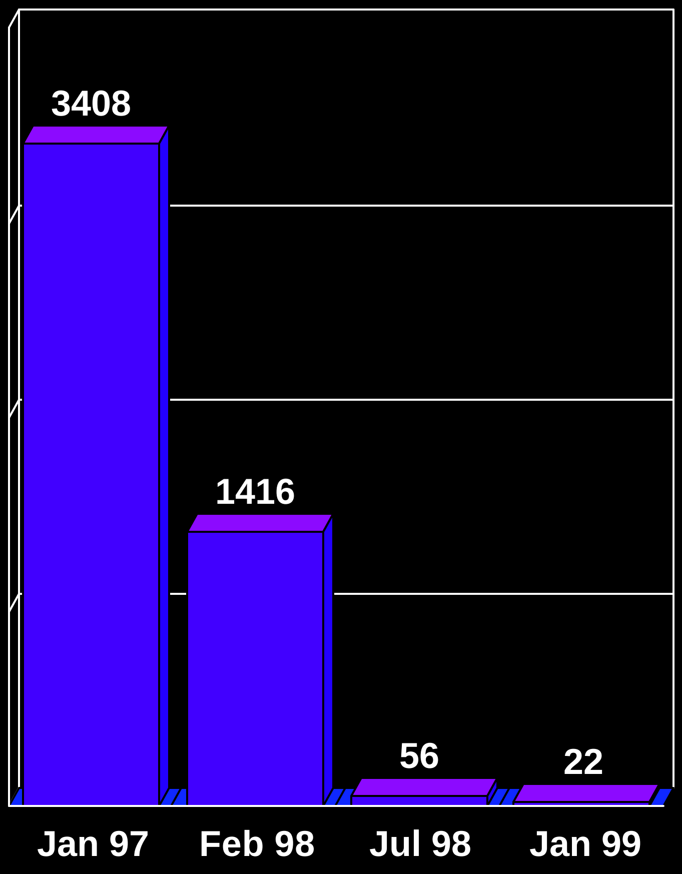


Yesterday's strong crypto is today's weak crypto

DES

- 40 bit = 
- 56 bit = 
- 128 bit = 

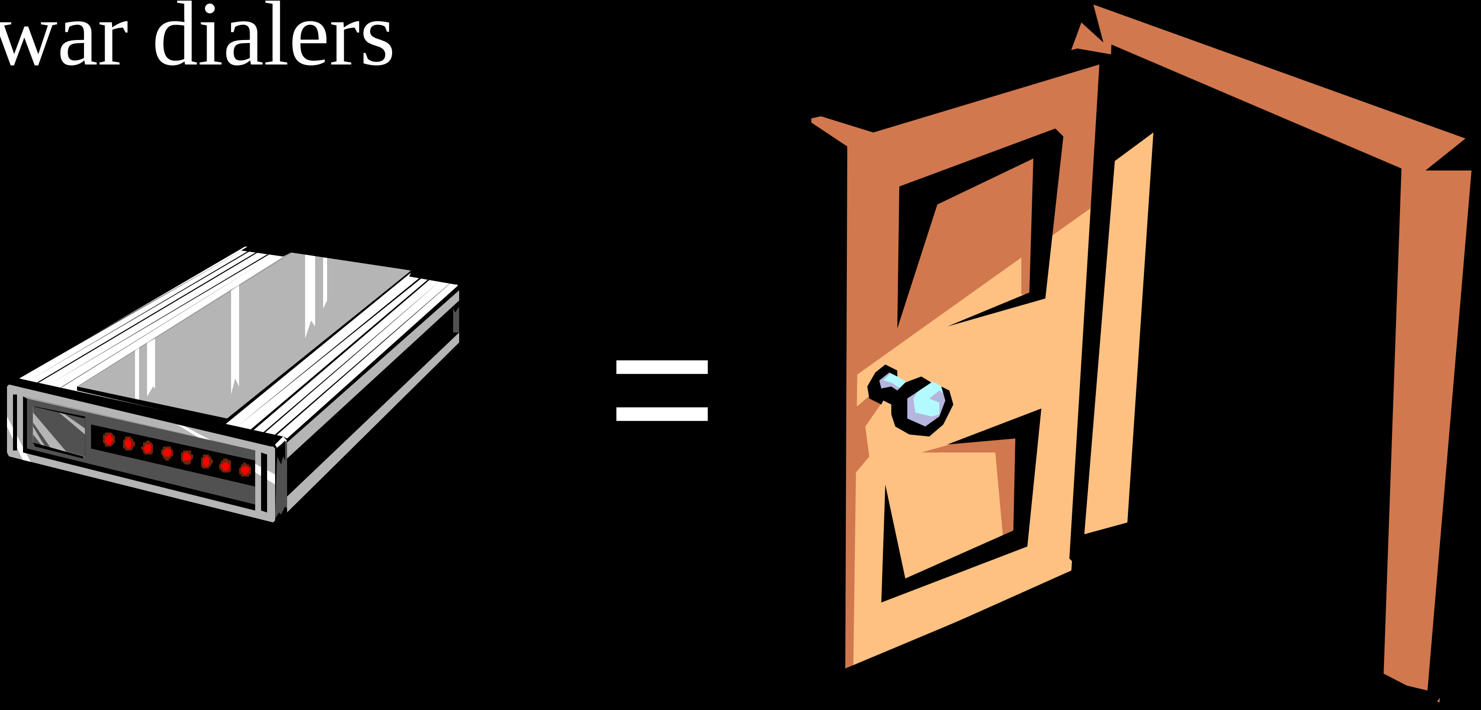
Hours to Crack DES



* Based on RSA's DES Challenge

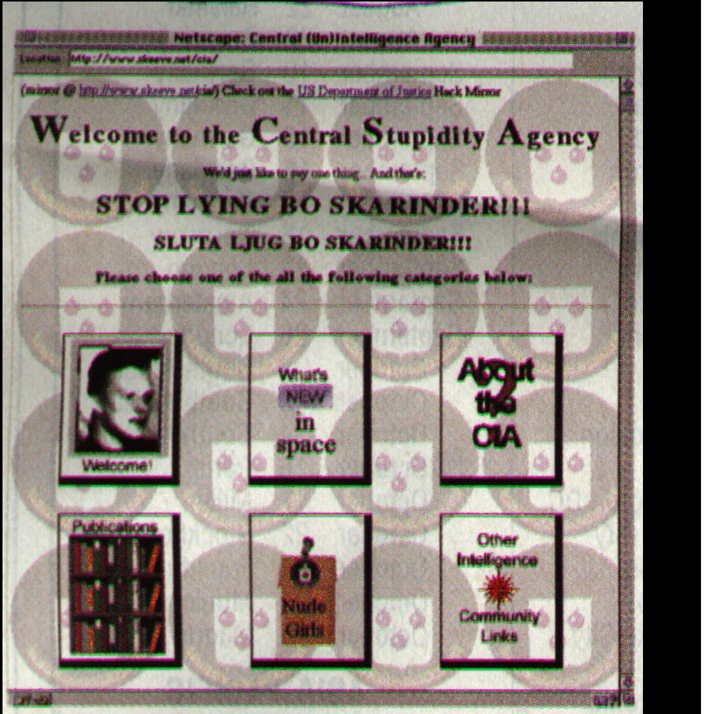
The back door is open

- auto-answer modems
  - fax software starts in auto-answer mode
- war dialers



There's no such thing as a harmless attack

- PR damage
  - hacked web site
- leads to further attacks
  - establishes a "stepping stone" for further exploration
  - attack appears to originate from your system
  - same pw's may be used on other systems



Netscape: Central (Un)Intelligence Agency

Location: http://www.skeeve.net/cia/

(mirror @ http://www.skeeve.net/cia/) Check out the US Department of Justice Hack Mirror

Welcome to the Central Stupidity Agency

We'd just like to say one thing... And that's:

STOP LYING BO SKARINDER!!!

SLUTA LJUG BO SKARINDER!!!

Please choose one of the all the following categories below:

Hacked! The CIA's defaced home page

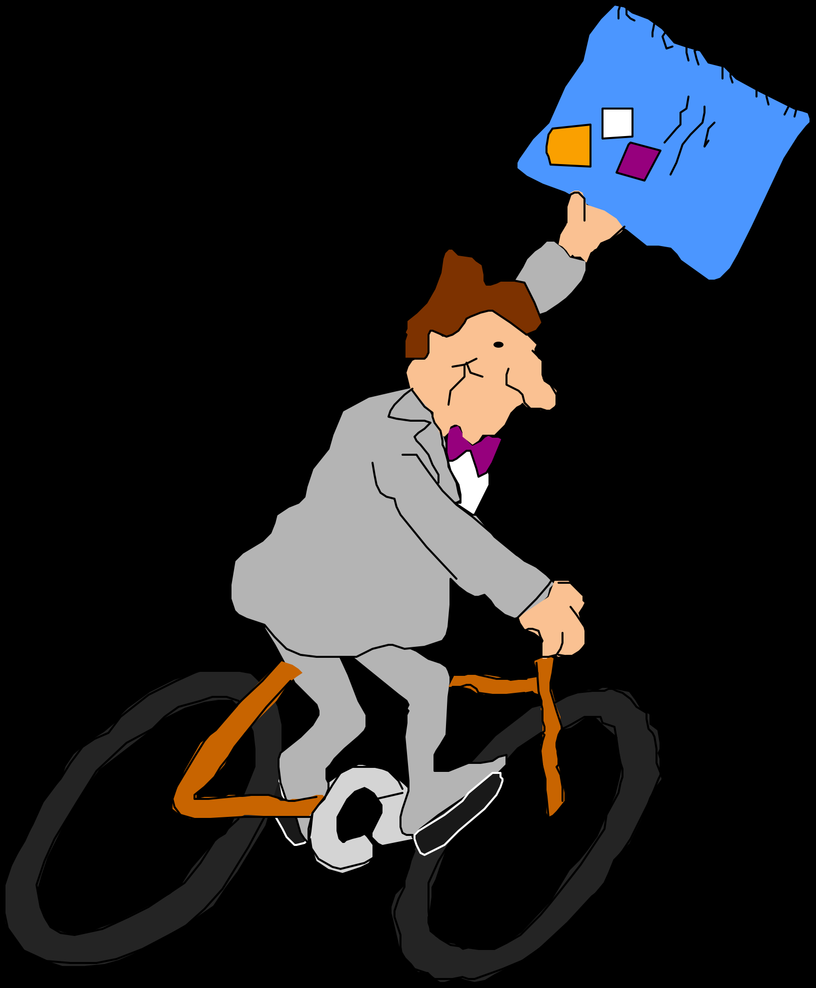
Information is your best defense

- In the "Information Age" **information** is:
  - the hacker's prize
  - your best defense
- informed I/T staff
  - "batten down the hatches"
- informed users
  - centralized incident reporting/tracking
- expert resources

IBM Security Services

- Assessment & Planning
  - Health Check
  - Ethical Hacking
  - Workshops
- Architecture & Design
  - Policy Definition
- Implementation
- Management
  - Emergency Response Service

Additional Information



URL's

- "Inside the VPN Tunnel" Article
  - www-1.ibm.com/support/tcp/fall98/vpntunel.html
- "Cryptography and SET: Safe Surfing?" Article
  - d02xdgcl01.southbury.ibm.com/support/tcp/assets/pdf/setwebpa.pdf
  - www.software.ibm.com/commerce/payment/cryptset.html
- IBM SecureWay home page
  - www.ibm.com/security
- IBM Security Services
  - www.ibm.com/security/html/consult.html

References

- ***The Cuckoo's Egg***, Clifford Stoll
- ***Firewalls and Internet Security,*** Cheswick and Bellovin (Addison-Wesley 1994)
- ***Applied Cryptography,*** Bruce Schneier (Wiley 1996)
- ***Maximum Security***, Anonymous (SANS 1997)
- ***Network Security,*** Kaufman, Perlman, Speciner (Prentice Hall 1995)