Future SPAM Distribution Methods and Issues

Dr. Bill Hancock, CISSP, CISM

Vice President, Security

Chief Security Officer

Cable & Wireless

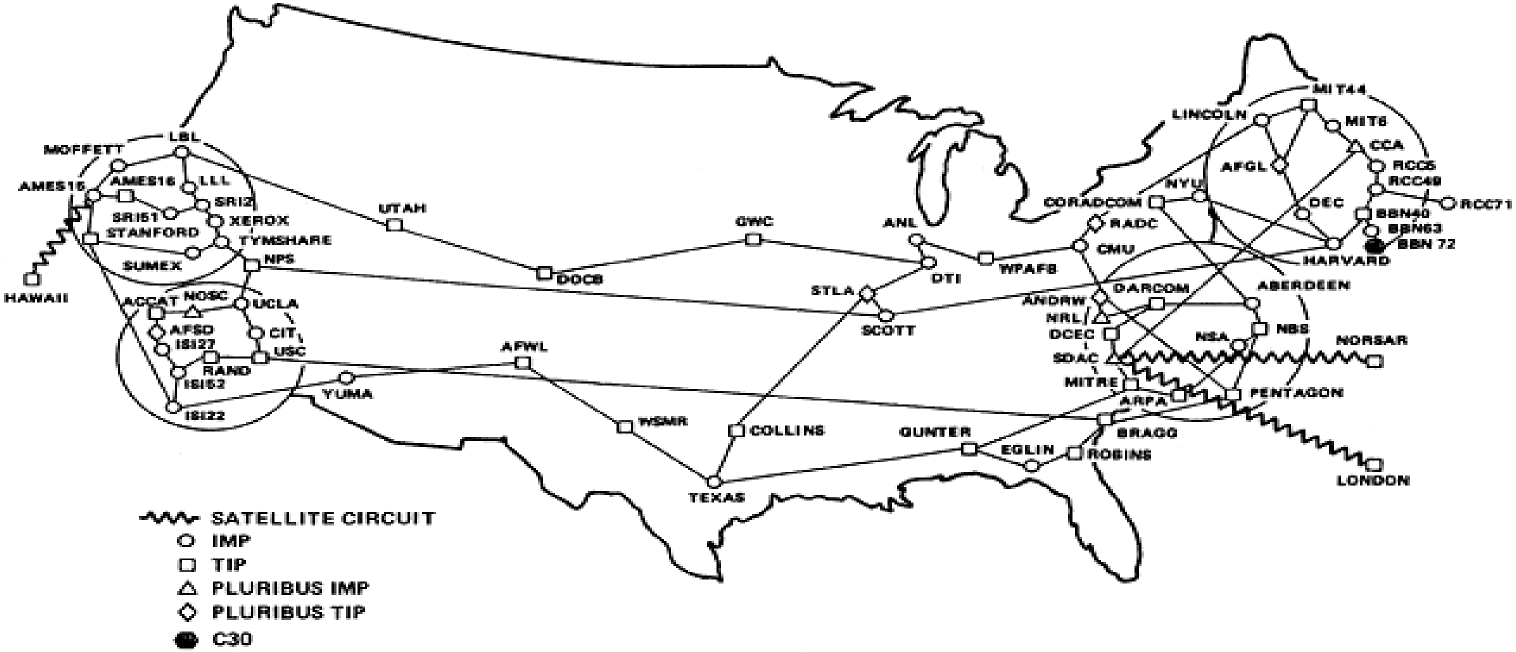
bill.hancock@cw.com

+1-972-740-7347

CABLE & WIRELESS

The Past

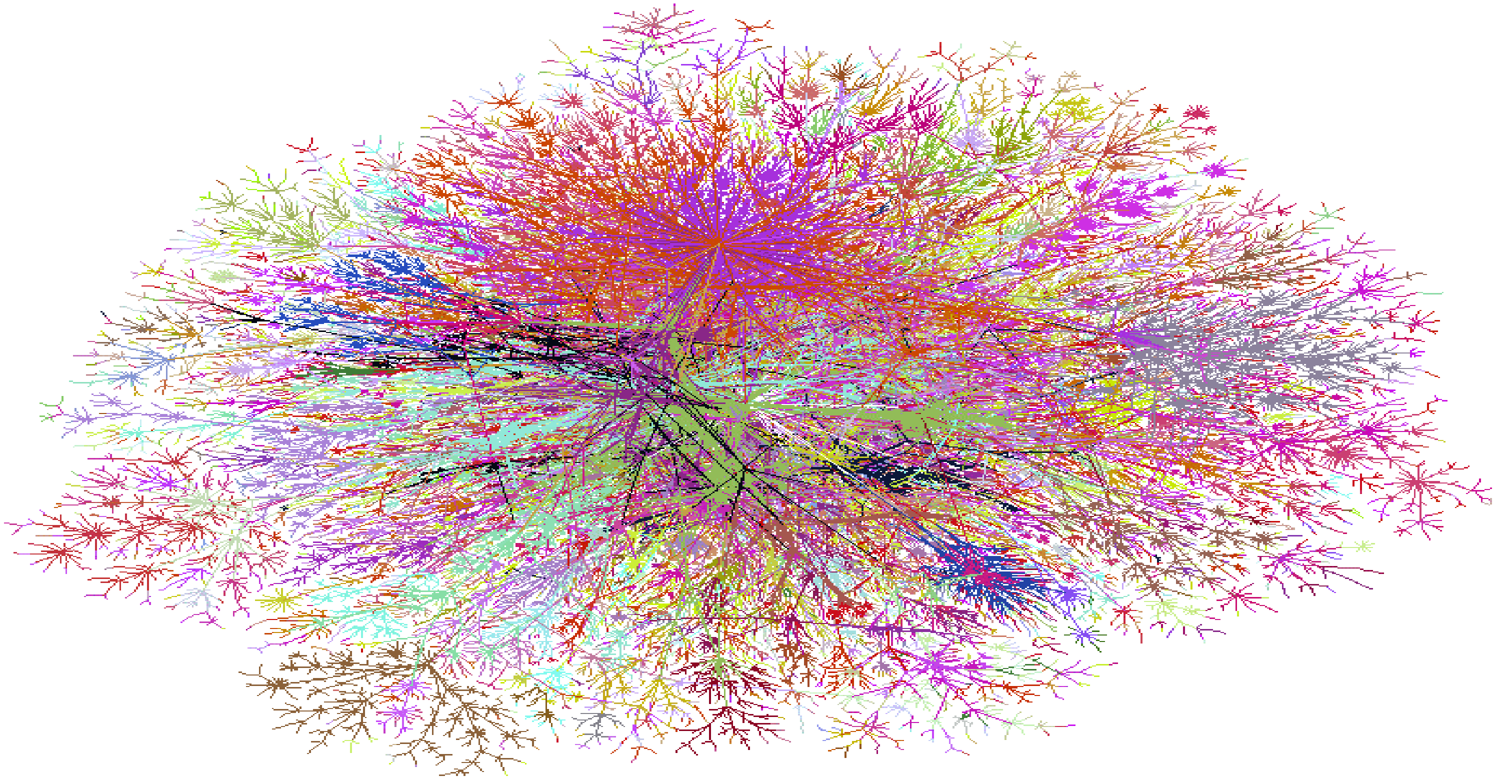
ARPANET GEOGRAPHIC MAP, OCTOBER 1980



(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

CABLE & WIRELESS

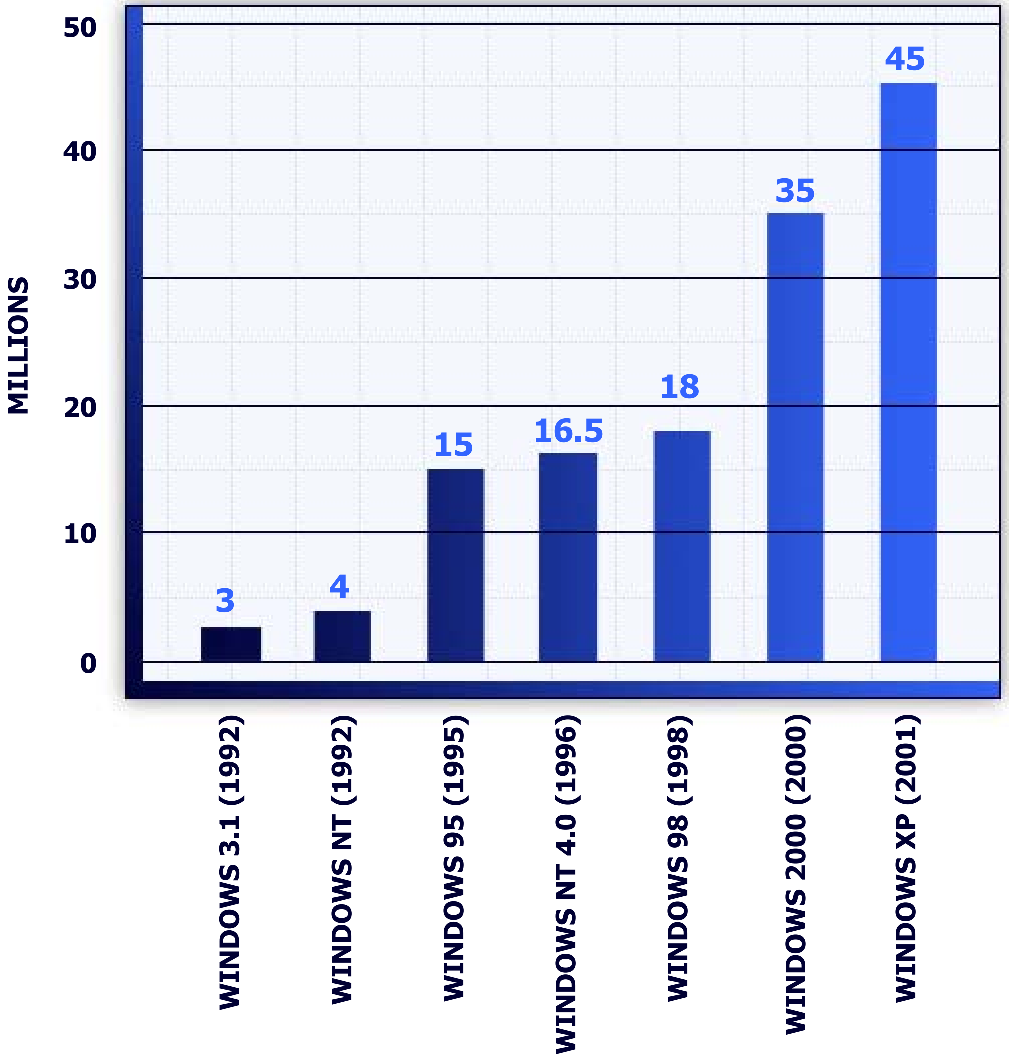
The Present



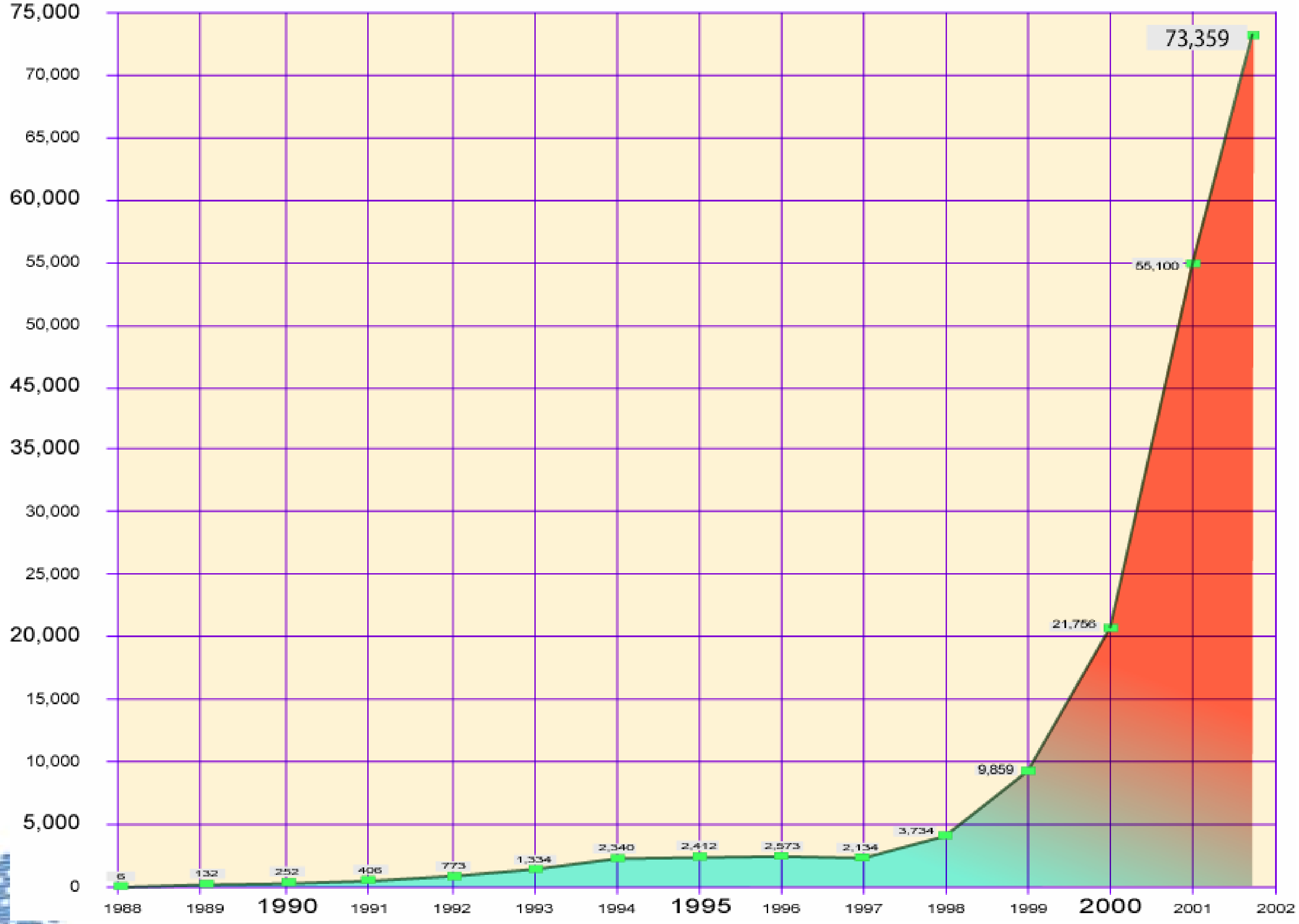
Source: http://cm.bell-labs.com/who/ches/map/gallery/index.html

Software Is Too Complex

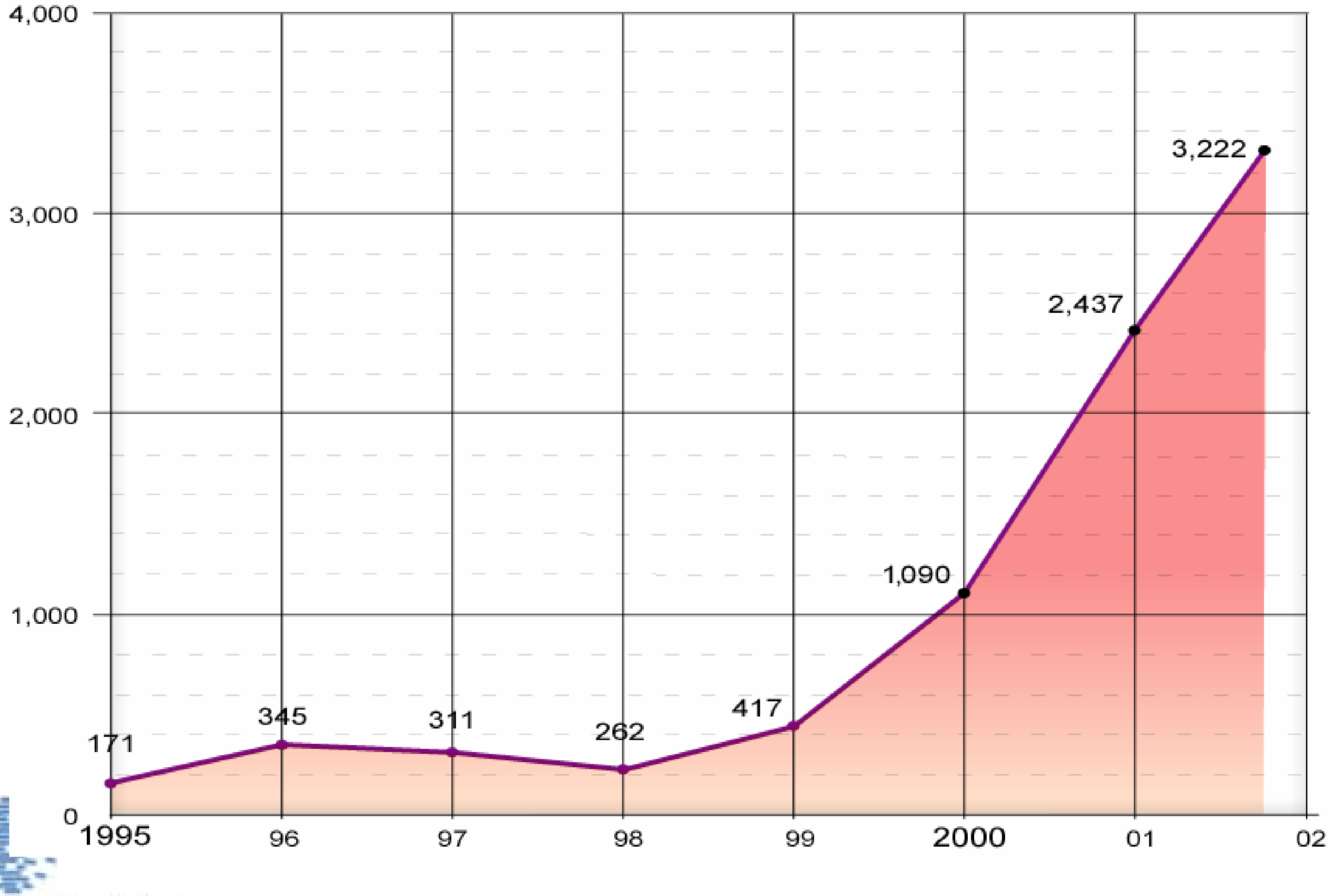
- Sources of Complexity:
  - Applications and operating systems
  - Data mixed with programs
  - New Internet services
    - XML, SOAP, VoIP
  - Complex Web sites
  - Always-on connections
  - IP stacks in cell phones, PDAs, gaming consoles, refrigerators, thermostats



The Dilemma: Growth in Number of Incidents Reported to the CERT/CC

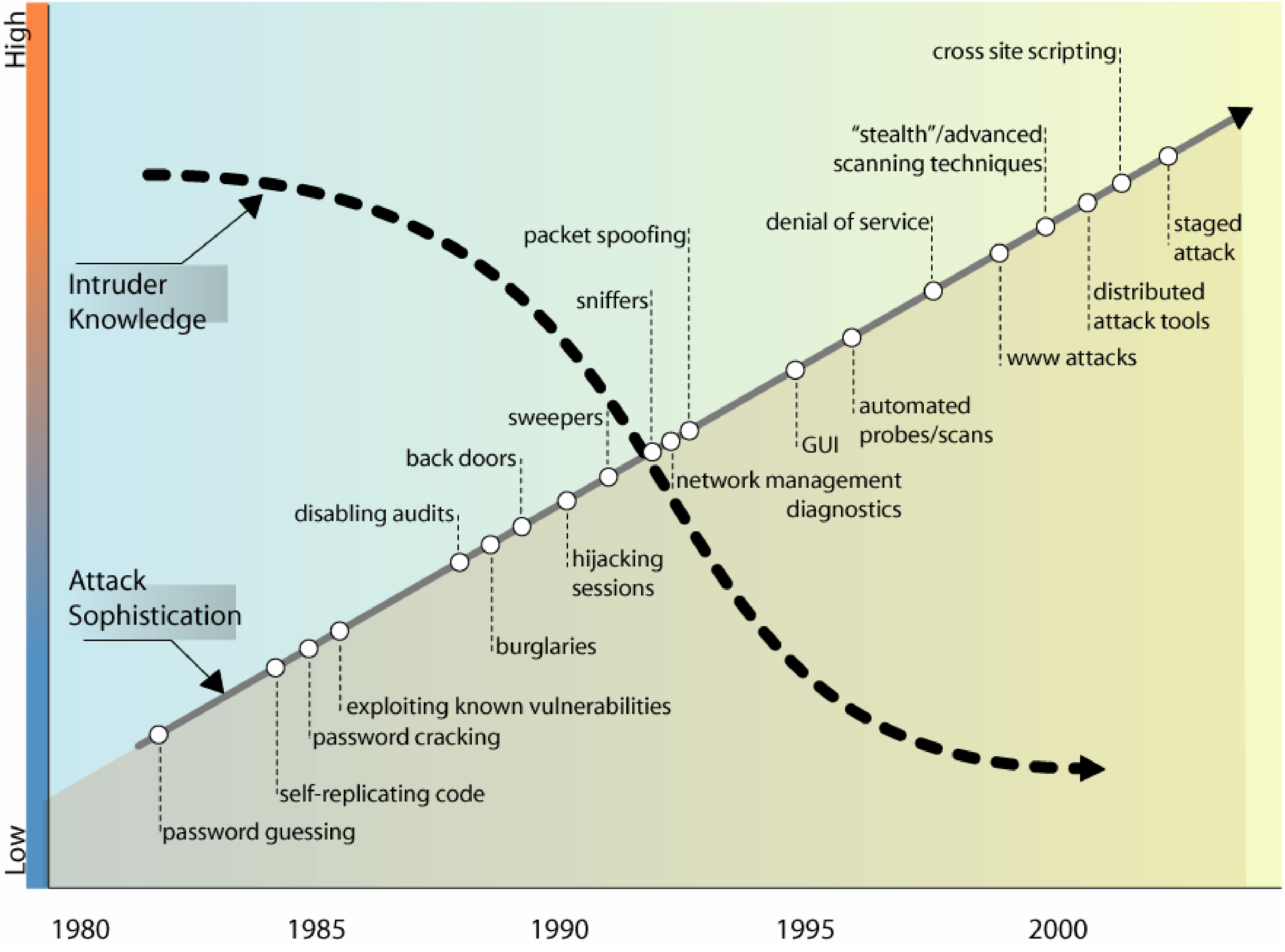


The Dilemma: Growth in Number of Vulnerabilities Reported to the CERT/CC



CABLE & WIRELESS

As Systems Get Complex, Attackers are Less Mentally Sophisticated…



CERT/CC

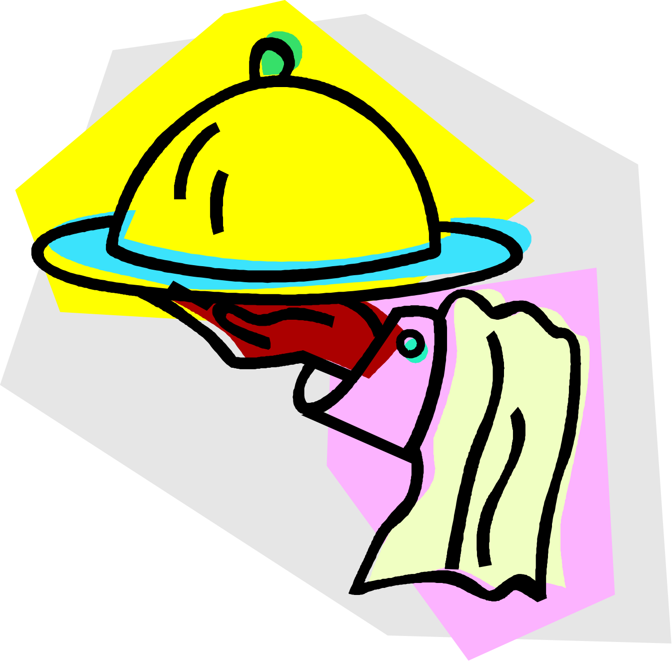
LOW

1980

Entry Point Cost to SPAM

- A PC
- Internet access
- Harvesting tools
- Open relay/proxy scanning tool(s)
- Currently:
  - Open mail relay
  - Open mail proxy
- Unsuspecting relay provider
- Marketing methodology
- Quick movement of SPAM source system(s)
- Other miscellaneous items of small cost

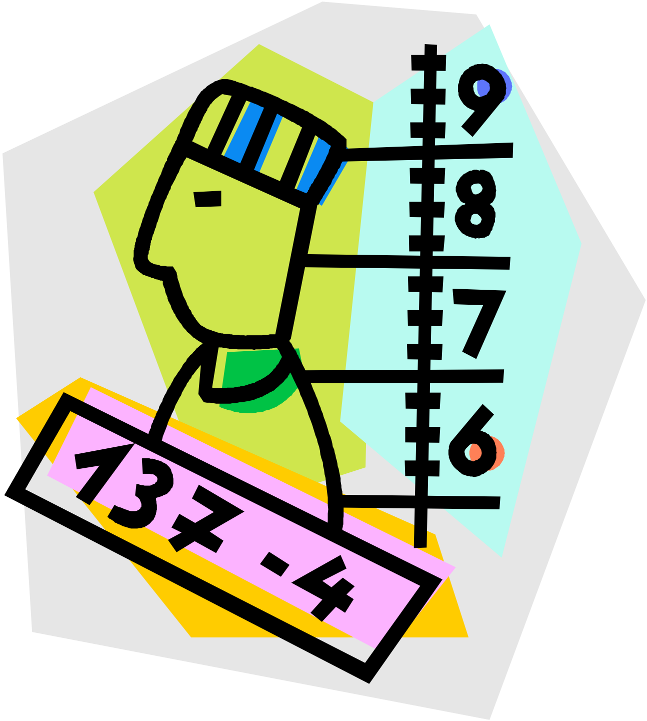
Core SPAM Need: A Server



- Without an e-mail server to send the mail, it's pretty hard to SPAM someone
- Most email uses the SMTP method, X.400 or similar MTA
- Source code for email servers is now widely available
- It is trivial to set up an email server today compared to 5 years ago

CABLE & WIRELESS

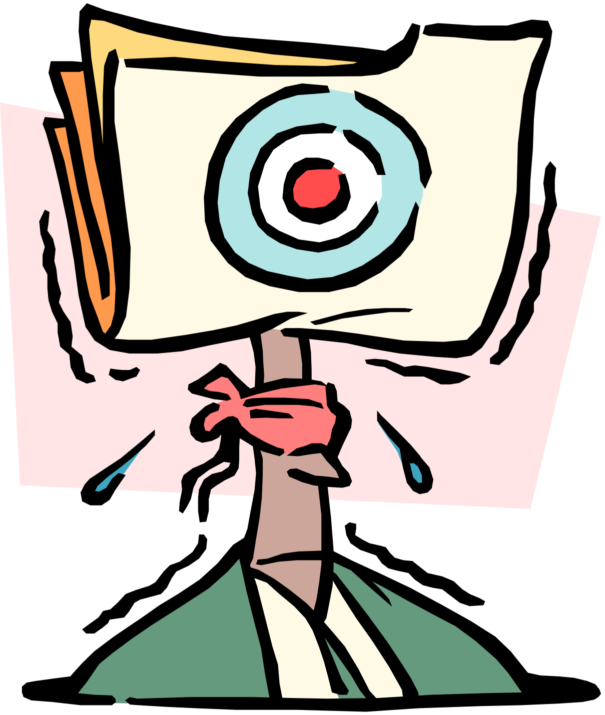
Spammers Must Evade Capture



- Can’t use your own server – too easy to get caught
- Need to constantly find and use new email servers to evade capture
- Currently depend on someone else to set up an email server to relay SPAM messages
- This means that at any given date, the email server of choice may not be available
- Top SPAMmers move a lot and stay mobile

CABLE & WIRELESS

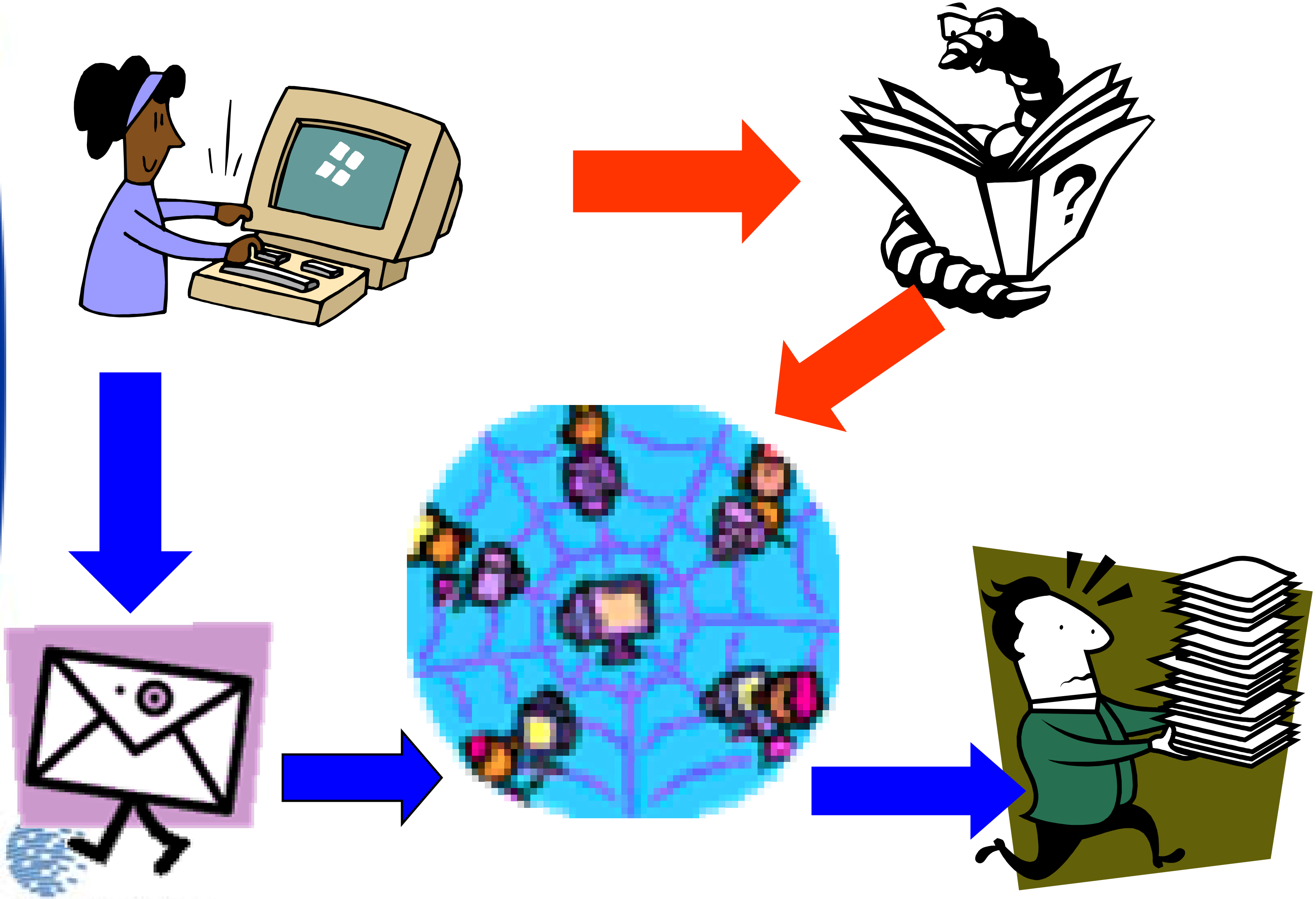
Upcoming SPAM Methods



- SMTP server "injection" to Internet-based systems
  - Via hack
  - Via worm
  - Zombie distribution network
  - Email server 'bot
- What these do:
  - Create email distrbution "networks"
  - Allow SPAMmer to aggressive "move"

CABLE & WIRELESS

Creating an SMTP Automated Distribution "Network"



Issues with AML SPAM Approach

- Uses automated distribution method of SMTP server facility for SPAMmer
  - Causes millions of e-mail servers to appear in a very short amount of time
  - Worms are an effective distrbution method (sharp increase in worms in 2003)
  - Entry methods change with each new bug in software
- Extremely difficult to trace
- Can be activated and controlled via stealth means
- Can be shared or access to “network” sold to others
- Difficult to clean or delete
- Known science

CABLE & WIRELESS

Legislation is not a Problem

- SPAM ‘bots can infect millions of computers in a short amount of time
- Federal or state anti-SPAM legislation only works in US
  - Many tagrest for SMTP “zombies” will be overseas
  - Most countries have no adequate hacking laws to deal with infestation
- With aperiodic SPAM ‘bot use, most users will not know they are the source of SPAM activities
- Legislation that targets email source (e.g. unsuspecting user) will have serious blowback problems

CABLE & WIRELESS

Future SPAM Problems

- In the next 5 years, computing will be mostly mobile and increasingly wireless
- A handset will be an Internet “node” on the network
- SPAM will reach all technology in different ways
  - Pop-up ads on phones with IP capability when a number is dialed
    - Havesting of personal address books in portable technologies
    - Re-direction of calls, lookups and other directory services to SPAM operators

CABLE & WIRELESS

Why is SPAM Protection Needed?

CABLE & WIRELESS

Summary

Dr. Bill Hancock, CISSP, CISM
Vice President, Security
Chief Security Officer
Cable & Wireless
bill.hancock@cw.com
+1-972-740-7347

CABLE & WIRELESS