Purdue University

Center for Education and Research in Information Assurance and Security

Musings on Disclosure & Vulnerabilities

<http://www.cerias.purdue.edu>

Eugene H. Spafford

13 December 2000

Metacomments

- There are basically 4 reasons you invite someone as a featured speaker
  - He's someone senior, with lots of experience you want to hear before he rides off into the sunset
  - She's recently done something very noteworthy
  - He's likely to say something outrageous or controversial that will be amusing to everyone
  - The ballots were miscounted

Metacomments

- There are basically 4 reasons you invite someone as a featured speaker
  - He's someone senior, with lots of experience you want to hear before he rides off into the sunset
  - She's recently done something very noteworthy
  - He's likely to say something outrageous or controversial that will be amusing to everyone
  - The ballots were miscounted
- In this talk, I will not demand a recount

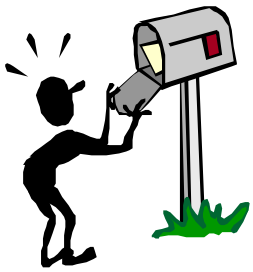
Metacomments

- I don't know the key to success, but the key to failure is trying to please everybody.
  - Bill Cosby
- The toughest thing about success is that you've got to keep on being a success.
  - Irving Berlin
- If all else fails, immortality can always be assured by spectacular error.
  - John Kenneth Galbraith
- Nothing succeeds like excess.
  - Oscar Wilde

State of Security: Poor

- Examples abound:
  - DoD reports 22,000 attacks on Pentagon systems in 2000
  - 2 Break-ins at Microsoft, October 2000
  - Israel/Palestinian sites attacked, October 2000
  - Feb 2000, Denial of Service against eBay, Yahoo, Amazon
- CSI/FBI figures
  - Less than 20% sites report no unauthorized use

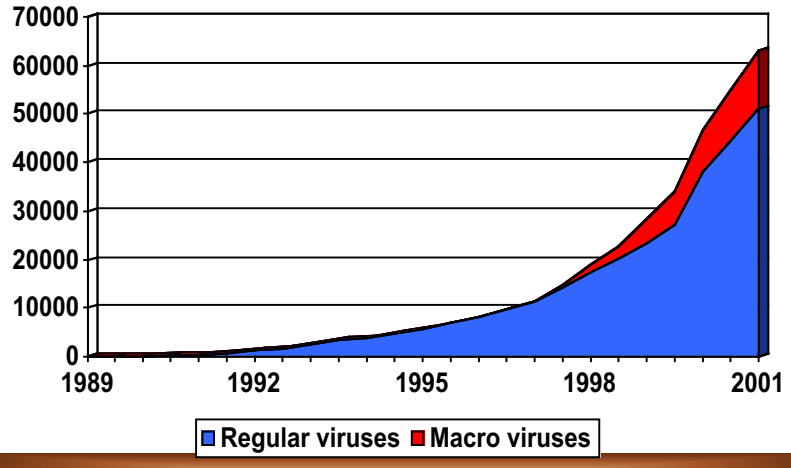
Real losses



- Melissa, March 1999
  - Word 97, Word 2000
  - $300 million in damages
  - Approximately 4 days, 150,000 systems
- ILOVEYOU, May 2000
  - Outlook
  - As much as $10 billion in damages
  - Approximately 24 hours, > 500,000 systems

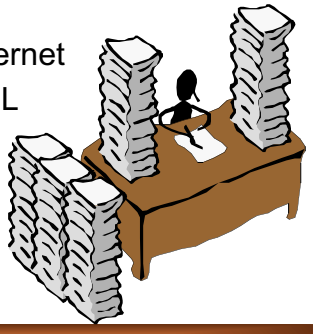
("Brain" took 5 years to do $50 million)

Growth of Viruses "In the Wild"



More data

- CERT/CC fielded 10,000 incidents in 1999
  - On-track for 20,000 in 2000
- On-going probes (via Intel)
  - 50-60 incidents per day on Internet
  - 10-12 incidents per day on DSL
  - 5-6 incidents per day on dial-up

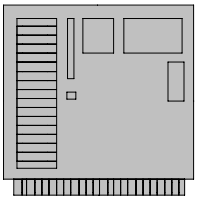


Should I Share the Blame?

- Morris Worm analysis (late 1988)
- COPS (1990)
- Practical Unix Security (1991)

These discussed vulnerabilities in detail, and made the case that computing users needed more information about vulnerabilities.

Vulnerabilities in 1990

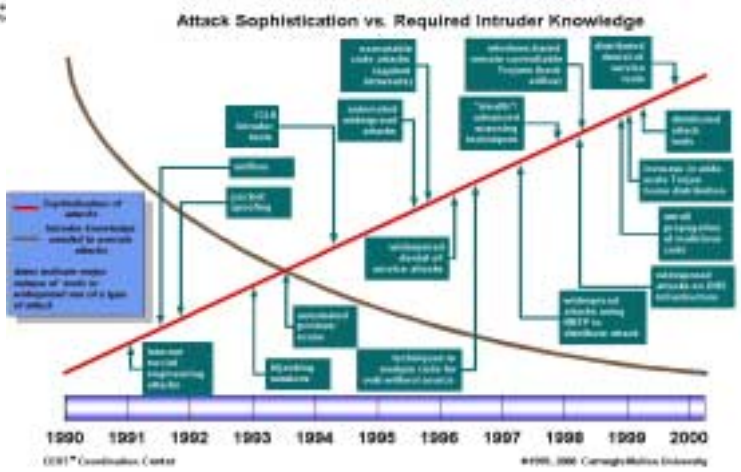


- Platforms
  - Mainframes
  - BSD Unix
  - AT&T Unix
  - VMS
- A few dozen vulnerabilities in low-circulation
- Network access by "trained" and "trusted"
- Limited security info exchanged ("zardoz")
- Little or no automated hacking

Vulnerabilities Now

- CERT/CC is on track to take over 1000 vulnerability reports in 2000
- Buffer overflows still rampant
- Users not installing patches
  - CDUniverse hack in February as example
- About 15 new viruses being reported daily
- Infrastructure attacks increasing

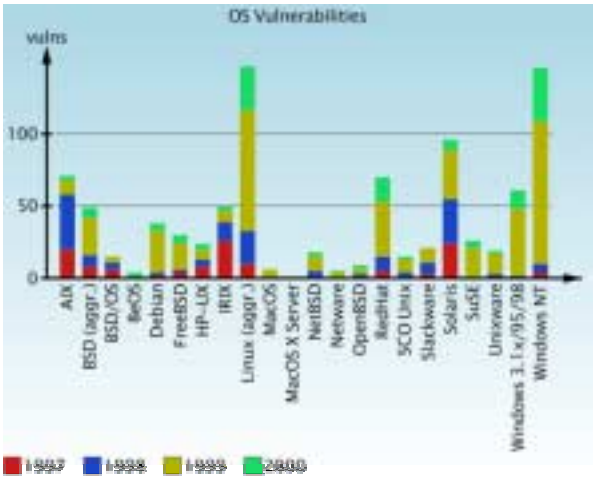
Point & Click Attacks



About 30% are buffer overflows or unchecked data

Over 90% are coding/design flaws.

Source: Securityfocus.com



Note about open source

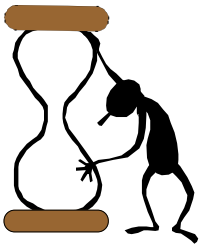
- S/COMP
- Trusted VMS
- CMWS Ultrix and SunOS

…all are closed source systems

The key is quality, and that depends on training, methodology, and control. NOT OS vs. CS

The Future? (ca. 2004)

- 100,000 computer viruses
  - 99% for one vendor's software
  - New viruses @ more than 1 per hour
- Most common desktop system
  - Almost 100 million LOC, 1Ghz+
  - 1 security patch announced per day
- Attacks over network exceed 10 per hour
- Losses to business and government will exceed $100 billion per year



Medical Lessons

- Consider another profession dealing with widespread dangers from systemic flaws and malicious agents
- What can we learn from the medical profession?

Plagues and Trades

- Bubonic/pneumonic plague, 1347–1350: The "Black Death"
- 10 million dead in Europe, perhaps 1/2 the population of China and India
- The populace blamed the Jews or imagined sins
- Again in 1665, London had 100,000 dead
  - Saved by the Great Fire

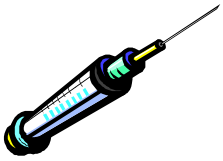
Epidemeology

- Pandemics of cholera
- Quarantine did not help
- John Snow in 1854
  - Broad Street pump

(Who will remove the handle from Word and other faulty software?)

Vaccines and Prevention

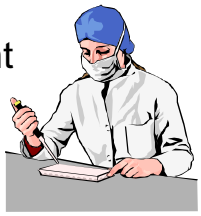
- Preventative care is better than response
- Goal is to reach threshold immunity
- "Live vaccines" are often not the best choice
  E.g., polio
- The disease is not distributed with the vaccine
- Killing the bugs is more effective than treating the disease
  - DDT is still the most effect malaria and dengue countermeasure



Autopsies & Reporting

- Why did the patient die?
- What did the treatment do?
- What is the incidence of disease?

- Pathology is intended to prevent the spread of pathogens and increase knowledge of diseases



Disclosure and Response

- "Full disclosure"
  - Full details of the flaw
  - Often includes exploit script
  - Often released before patches are available
- Typified by
  - Bugtraq
    - 19000+ postings since 11/93
    - 4800 this year
  - Rootshell.com
  - PacketStorm

Argument #1

"Vendors won't fix flaws. Full disclosure is the only way to get fixes."

- Not in recent history
- Bigger problem is bad design
- Exploits are not needed for this goal
- There are other ways to address this problem

Argument #2

"This is the only way to ensure we have fixed the flaws."

- No guarantee
- Most users cannot take advantage of this info
- Exploits are not needed for this goal
- Better not to have the flaws in the first place

Argument #3

"This helps us learn to avoid similar flaws in the future."

- See the growing incidence of security flaws.
  - CERT/CC is on track for 1000 vulnerability reports for 2000
  - Still seeing buffer overflows after 20 years
- Exploits are not needed for this goal

Argument #4

"I need the exploit to program my firewall/IDS/etc and protect myself."

- Self-fulfilling condition.
- Better to fix underlying systems
- Practice endangers the whole community
  - Consider case of 500 people using it vs. 250,000 using it

Argument #5

"All the bad guys know about it already. We should let the 'white hats' know."

- Untrue for most things for years
- Underground more fragmented, less talented
- Disclosure is also to the thousands (more?) of script kiddies
- See paper by Arbaugh, et al. in IEEE Computer

Legal picture

- Council of Europe Convention
  - Making hacking programs and information illegal
- DMCA in US
- UCITA
  - Negative effect

Some conclusions

1. "Above all, do no harm" good idea here too

Some conclusions

1. "Above all, do no harm" good idea here too
2. Some individuals die in epidemics. That is not a reason to infect the rest

Some conclusions

1. "Above all, do no harm" good idea here too
2. Some individuals die in epidemics. That is not a reason to infect the rest
3. Prevention is better than cure. Start now.

Some conclusions

1. "Above all, do no harm" good idea here too
2. Some individuals die in epidemics. That is not a reason to infect the rest
3. Prevention is better than cure. Start now.
4. The world has changed in 10 years, and will change more in the next few -- get used to it

Some conclusions

1. "Above all, do no harm" good idea here too
2. Some individuals die in epidemics. That is not a reason to infect the rest
3. Prevention is better than cure. Start now.
4. The world has changed in 10 years, and will change more in the next few -- get used to it
5. In a few years, lawyers might be the best friends of security practitioners

My concluding conclusions

- Full disclosure is of unproven value in today's Internet, and may lead to harm
  - We need science here, not folklore

•My concluding conclusions

- Full disclosure is of unproven value in today's Internet, and may lead to harm
  - We need science here, not folklore
- More specifically, publication of exploits is antisocial and harmful to the general public

•My concluding conclusions

- Full disclosure is of unproven value in today's Internet, and may lead to harm
  - We need science here, not folklore
- More specifically, publication of exploits is antisocial and harmful to the general public
- Legal backlash may be unpleasant and overbroad. We'd be better to clean up on our own.

Thank you!