



# Computer & Internet Security

Sean Lanham, CISSP - ISO

University of Texas Arlington

The Office of Information Technology – Security Services

## Today's Situation – Universal Access...

- There are millions of people with Internet access. (Do we know the actual number?)
- All of them can communicate with your internet connected computer.
- Anyone can rattle the door to your computer to see if its locked.
- On the UTA network, someone tries on a hourly basis.



## Today's Situation – Vulnerable Computers...

- A large number of computers are vulnerable to being taken over remotely because of:
  - Unfixed software defects
  - Operating and configuration errors
  - Core architectural vulnerabilities
- Exploitation of **vulnerable** computers is increasingly trivial, quick, and almost risk-free by relatively unsophisticated individuals. One person or one program can wreak havoc.

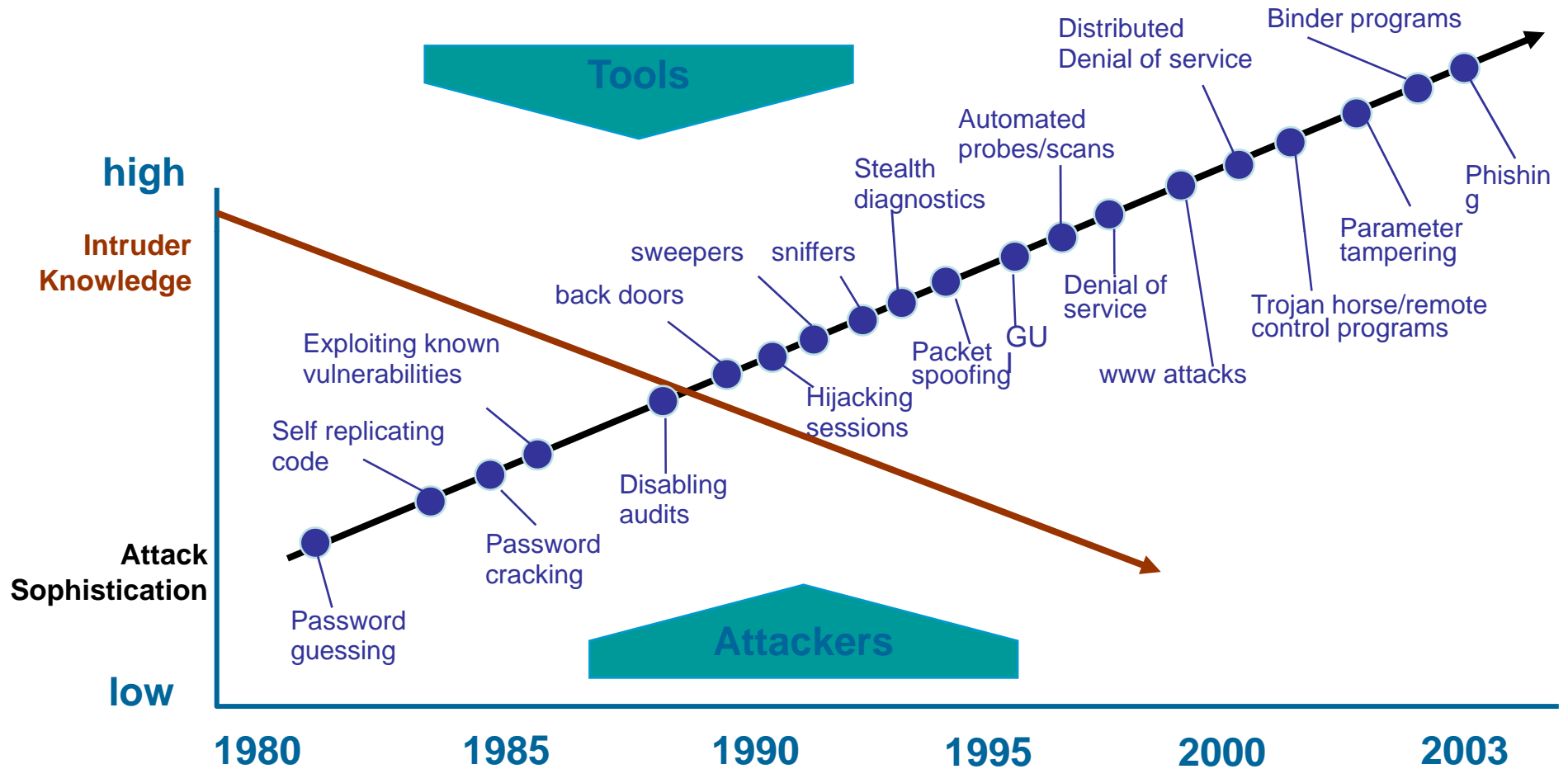


## Today's Situation – Opportunities for Abuse...

- To break into a safe, the safe cracker needs to know something about safes.
- To break into a computer, the computer cracker often only needs to know where to download a program written by someone else who knows something about computers.
- Such programs are freely available all over the Net.



# Today's Situation – Opportunities for Abuse...



Source: Defense Information System Agency



## How Can the Situation Affect You?...

- A compromised computer provides access to all accounts, keystrokes, and resident data. Account and keystroke information can be used to access other resources.
  - Operational Difficulties
  - Email and documents
  - Financial transactions
  - Identity Theft
  - Criminal Use of Computer



## Practical Aspects of Securing Our Computers...

- We can secure something so well that it is unusable.
- Security is relative, not absolute.
  - Some amount of money, time, and/or motivation will surmount almost any security measure.
  - Luckily, a lot of computer crime is not targeted at a specific victim but is instead a crime of opportunity.
- “Security is a process, not a product.” Bruce Schneier
  - We can’t buy security. We have to live it.



## Basic Security Recommendations...

- There is no substitute for common sense.
  - Giving out bank or credit card numbers over the Internet is no different than giving them out over the telephone.
  - Taking action based on the apparent sender of email is little different than taking action based on the return address of a typewritten postcard.
  - Running a program from an unknown source is little different than eating food found on the street.
  - Not maintaining our computers is little different than not maintaining broken windows and doors. Unfortunately, computers need much more maintenance...the vendors just don't include that fact in their marketing literature.



## ...Basic Security Recommendations...

- Run anti-virus software that automatically updates itself.  
<http://www.uta.edu/antivirus>
- Visit the Windows Update Site once a month.
- Treat all email attachments with caution.
- Treat file downloads with caution.
- Choose strong passwords.
- Be careful where you type your passwords or any other personal information.



## ...Basic Security Recommendations

- If you receive unwanted email (SPAM) don't reply to it. Just delete it. If it continues, save copies and notify OIT Security Services.
- Don't believe everything you see on the Internet. Email addresses are easily falsified. Professional looking web pages can be put up by almost anyone these days.
- Don't ignore warnings from your computer.

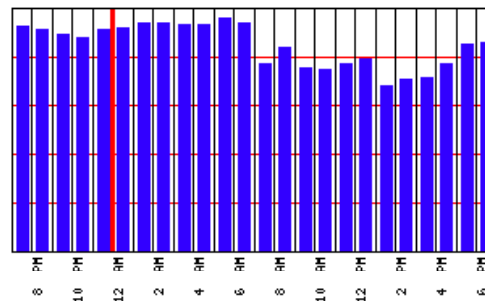


# Email Security

- **Antispam**

- Symantec Brightmail (old)

- False positives
    - Unreliable statistics
    - 1 year of data



Total messages processed since 12/4/2005: 93,846,685  
Messages identified as spam: 71,438,594 (76.1%)  
Messages identified with viruses: 3,255,561 (3.5%)

- IronPort (new)

- 1<sup>st</sup> Q. 145.1M / 137.4M – 95%
    - 2<sup>nd</sup> Q. 176M / 168.1M – 96%
    - 3<sup>rd</sup> Q. 292M / 283.2M – 97%
    - Projected for entire year 940M / 895.7M – 94%



Questions?

Sean Lanham  
Office of Information Technology  
Information Security Office  
[www.uta.edu/security](http://www.uta.edu/security)  
(817) 272-2271

