Vulnerabities

Are you safe?

John Steele

What we will cover

- Overview on Security
- What is a “Vulnerability”
- What does it mean to me
- What can I do
- Questions

Introduction

- Security concerns have been with with us for a long time
- A document outlining 10 “laws” for security was published by Microsoft in 2000 and updated in 2008
  - https://technet.microsoft.com/library/cc722487.aspx
- The content has since been debated and re-interpreted but is essentially still valid! [see link]
  - http://www.edgeblog.net/2006/10-new-immutable-laws-of-it-security/
- We need to keep these in mind as we discuss security

Laws on Security (Microsoft)
Laws 1 to 3

Law #1:

- If a bad guy can persuade you to run his program on your computer, it's not your computer anymore

- Law #2:
  - If a bad guy can alter the OS on your computer, it's not your computer anymore
- Law #3:
  - If a bad guy has unrestricted physical access to your computer, it's not your computer anymore
- Link
  - https://technet.microsoft.com/en-us/magazine/2008.10.securitywatch.aspx

Laws on Security (Microsoft)
Laws 4 to 7

- Law #4:
  - If you allow a bad guy to upload programs to your Web site, it's not your Web site anymore.
- Law #5:
  - Weak passwords trump strong security.
- Law #6:
  - A computer is only as secure as the administrator is trustworthy.
- Law #7:
  - Encrypted data is only as secure as the decryption key.
- Link
  - https://technet.microsoft.com/en-us/magazine/2008.11.securitywatch.aspx

Laws on Security (Microsoft)
Laws 8 to 10

- Law #8
  - An out-of-date virus scanner is only marginally better than no virus scanner at all
- Law #9
  - Absolute anonymity isn't practical in real life or on the Web
- Law #10
  - Technology is not a panacea
- Link
  - https://technet.microsoft.com/en-us/magazine/2008.12.securitywatch.aspx

What is a Vulnerability

- A vulnerability is something that allows someone to gain access to your system without your knowledge or permission
- This could be for
  - Direct gain
    - Stealing bank account details
  - Indirect malicious use - using your computer to attack another
    - Part of a “zombie” network to perform a denial of service attack

What is a Vulnerability

- Almost all software contains “bugs”
  - Software is very complex
  - Code may have errors in it
- Software may contain design weaknesses
  - Accidental
    - Some case is overlooked
    - Wrong type of data supplied
  - Deliberate
    - Security agencies
    - Software writer with ulterior motives

How else can I be vulnerable

- You may click on a link that is not what it appears to be and it runs a program on your computer
  - Hyperlinks cannot always be trusted
- You may deliberately install software believing it to be something that it is not
  - Fake link to Avast from a google search
- You may try out some software that looks interesting
  - It also installs additional unwanted software

Software vulnerabilities

- Known vulnerabilities are recorded in a standard format
  - Common Vulnerabilities and Exposures (CVE®)
    - https://cve.mitre.org/about/index.html
    - https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures
- Searchable database against products/vendors
  - CVE Details
    - http://www.cvedetails.com/index.php
  - Secunia (registration required)
  -

Buffer Overflow exploits

- Presenting too much data in response to an input request can overflow the end of the space reserved for it
  - This can overwrite non related data included a return address from a subroutine
  - Code can then be executed from the buffer and you may have lost control of your computer
    - Especially if you are using an administrator account
- Code SHOULD prevent this from happening

Distributed Denial of Service Attacks

- This type of attack has minimal impact on your computer but….
  - It requires a malware program to be installed and be dormant on your computer and many others
  - It is typically triggered from a remote coordinator to start repeatedly sending data to a target computer
    - One computer sending at 1 megabit per second may have minor impact on your computer's performance
    - Just 100,000 computers doing the same thing would create a load of 100 gigabits per second on the target
    - Probably this would bring the Internet to a halt
    - It is difficult to defend against such an attack

What can I do?

- BE CAREFUL
  - Make sure that you are using an account with User privileges (Standard or Limited)
  - Do not use an Administrator account for normal day to day use
    - See this link
  - Be careful to only install software from reputable places
  - When there are checkboxes make sure there are no sneaky additional programs you are permitting to install
- Remove Java unless you REALLY need it
- Install all software patches as soon as possible

What can I do (continued)?

- You are one of the major vulnerabilities
- When clicking on links especially in emails be aware that the text displayed and the underlying URL may be different
- Watch out for suspicious emails that contain things like “Pay this Invoice”
  - NEVER open the attachment if you are not absolutely sure it is genuine
- Watch our for Phishing emails asking you to validate your bank credentials via a link

Passwords

- Do not use the same password on every site
  - If one site is compromised then attackers might try other sites
  - Especially between forums (very low security) and banks
- Password managers like KeePass can simplify use of multiple passwords
  - Can partially automate logging in on most sites
  - Can therefore use very complex passwords which are different for each site

Certificate Exploits

- Always use HTTPS as this encrypts data?
  - This not a total guarantee that the data is safe!
- Certificates are issued by a Certificate Authority
  - You rely on this via a Chain of Trust by to a main provider
  - Computers have a set of Root certificates installed that are used to validate the top of the chain
    - Public keys of these certificates
    - Typically updated via security updates
    - Contain an expiry date
  - Check the certificate on the padlock
    - Avast does not display this with Internet Explorer