Comp 199: info security

Topic 5: Antiforensics

Anti Forensics

- My former book uses label “anti forensics”
  - Most people use the word “security”
  - Its anti-forensics when you're being investigated.
- Security Laws:
  - If you have personally identifiable financial data on your 'computer' you must use these techniques
    - Destroy the data when you are done
    - Encrypt the data till then.

Basics of Anti-forensics

- In class I'll colloquially use :
  - running in paranoid mode
  - Use your computing device as if you feared it might be stolen.
  - How might you do this when browsing?

Basics of Anti-forensics

- In class I'll colloquially use :
  - running in paranoid mode
  - Use your computing device as if you feared it might be stolen.
  - How might you do this when browsing?
    - Private browsing
    - Clear private data
    - Manual removal
    - Etc
  - Legitimate and illegitimate uses?

Basics of Anti-forensics

- In class I'll colloquially use :
  - running in paranoid mode
  - Use your computing device as if you feared it might be stolen.
  - How might you do this when browsing?
    - Private browsing
    - Clear private data
    - Manual removal
    - Etc
  - Legitimate and illegitimate uses?
    - Remember the laid-off woman visited by the police because of her work computer used by family?

Encryption

- Encryption: changing the bits and bytes on the computer to hide what is on it.
  - Uses?

Encryption

- Encryption: changing the bits and bytes on the computer to hide what is on it.
  - Uses?
    - Private identifiable data
    - Trade secrets
    - Privacy
    - Hiding bad behavior

Need for encryption

- Encryption more and more needed.
  - Desktops
    - Who uses them?

Need for encryption

- Encryption more and more needed.
  - Desktops
    - Who uses them?
      - Gamers
      - Software developers
      - Computer artists
      - Publishers
      - Scientists
      - What used to be called workstations
  - What does everyone else use?
    -

Need for encryption

- Encryption more and more needed.
  - Desktops
    - Who uses them?
      - Gamers
      - Software developers
      - Computer artists
      - Publishers
      - Scientists
      - What used to be called workstations
  - What does everyone else use?
    - Laptops/tablets/phones etc.

More data mobility

- How do you transfer data from machine to machine?

More data mobility

- How do you transfer data from machine to machine?
  - Most people
    - Cloud
    - Usb stick
    - Sych phone/tablet with local host
  - Cloud is a different issue, but USB sticks easy enough to lose or steal.

Need for encryption III

- Suppose a criminal steals a laptop
  - It is password protected
  - How do you get in and get to all the files?
  - Bragging rights for the most painless solution

bitlocker

- Windows encryption
  - Built in to Windows 7 enterprise and ultimate
  - Also Windows 8 Pro, Windows 8 Enterprise, and in all editions of Windows Server 2012
  - Can encrypt all hard drives on these machines
    - Also external USB drives

Windows 7 Bitlocker

- Windows 7 Bit Locker relies on a hardware component.
  - Trusted Platform Module
  - http://www.webopedia.com/TERM/T/Trusted_Platfor
  - Without this added device – the software bails
  - Show demo.

Windows 8 Bitlocker

- Doesn't appear to need TPM
  - Disclaimer
- Works more like other encryption systems.
  - Has trusted key
  - As backup for password

Bitlocker Backdoors

- The FBI pressured MS to build in a backdoor
  - Shades of the russian system we just looked at?
  - http://mashable.com/2013/09/11/fbi-microsoft-bitlock
  - Discuss a backdoor

Filevault 2

- Sucessor to FileVault
  - Which was nicknamed VileFault
- MacOS encryption for hard drives and USB drives.
  - Need password
  - Also can use master key
  - Apple will store your master Key if you like
  - Works on all recent MacOS versions
  - By default auto logs out in user-chosen amount of time
- Analysis?

Getting in to Encrypted drive

- Best way:
  - Seize the computer while running and logged in
  - Immediately put a digital examiner on the machine – determine if the drive is encrypted, if so copy/clone before powerdown.
- Another painless way.
  - Elcomsoft Forensic Disk Decryptor
  - http://www.informationweek.com/security/encryption/fo
  - Wanna guess the price?

Breaking Encryption

- Actually breaking the encryption is the worst part
- Breaking the master keys is really really hard
  - Those 240x10 to the 20^{th} numbers your book was throwing around
- Fortunately there is usually an easier point of entry
  - What is the most vulnerable part of any computer security system?

Breaking Encryption

- Actually breaking the encryption is the worst part
- Breaking the master keys is really really hard
  - Those 240x10 to the 20th numbers your book was throwing around
- Fortunately there is usually an easier point of entry
  - What is the most vulnerable part of any computer security system?
    - People
    - Review dictionary attacks and password cracking
    - Show xkcd cartoon

reading

- Read chapter 6 to page 92

Admin

- Quiz
- Today's topics in current issues in privacy.
- Monday's issue finders/presenters
  - Craig, Rachel

Steganography

- The art of hiding one file inside of another.
  - Many binary files (reminder: what are common binary file types?)

Steganography

- The art of hiding one file inside of another.
  - Many binary files (pdfs, mp3s image files etc)
    - Have areas of redundant information
    - Or areas ignored by file.
  - Put other data in this file in those places.
  - Data becomes very hard to find.
  - Have to kind of know to look at the file in order to see that something is wrong.
  - Gina Trapani likens it to invisible ink

Steganography terms

- Stegnonography uses jargon terms
  - Carrier file: the visible file that the other file is hidden inside of
  - Stealth file: the hidden file inside of the carrier file.

Steganography vs. Encryption

- Just from the basic description what are the tradeoffs between Steganography and Encryption?

Steganography vs. Encryption

- Tradeoffs between Steganography and Encryption that I see:
  - Encryption: really hard to break. Looks like a giant safe and acts like one – tells everyone, the secret is here!
  - Steganography: the fact that something is hidden is hidden from view.
    - Often easy to retrieve the data

Common Uses for Steganography

- People use Steganography for
  - Digital Watermarking
    - Placing identifying markers into your intellectual property to keep it from being stolen or copied and sold.
  - Exchanging passwords over email
    - Email is very insecure – send this way or encrypted.
  - Secret club communicating via public forum
  - Impressing your friends and family.
  - Hiding misdeeds.
  - As with most of these information security techniques – most of the uses are benign.

Steg

- Steg is a free cross platform Stego tool
  - Open source
  - Portable executable
  - Carrier file formats:
    - Images (BMP, JPG)
  - Encrypts stealthed file.
  - Lets take a look.
- Other tools can handle
  - Audio support (AIFF, MP3, NEXT/SUN, WAV)
  - Video support (3GP, MP4, MPG, VOB)
  - Flash-Adobe support (FLV, SWF, PDF)

Drive wiping

- Writes zeros to every location on drive
  - For magnetic drives needs to make several passes
  - For SSDs needs only a single pass.
- dban

Reading

- Please finish chapter 6.