

# Cybersecurity: Memory and Data Protection

CS50 for JDs  
Winter Term 2019

# Agenda

- Hardware
- Memory
- Hard drives
- Data persistence
- File transfer
- Client data
- Compliance protocols

# Hardware

- When you talk about your system's memory, what exactly does that mean?

# Hardware

- When you talk about your system's memory, what exactly does that mean?
- How much memory does your computer have?

# Hardware

- When you talk about your system's memory, what exactly does that mean?
- How much memory does your computer have?
- There's a complete hierarchy of memory, from *RAM* to *cache* memory, as well as hard disk drives and/or solid state drives, on your system.
  - RAM > L3 cache > L2 cache > L1 cache > CPU memory

# Memory

- Every file on your computer lives on your disk drive, be it a hard disk drive (HDD) or a solid-state drive (SSD).

# Memory

- Every file on your computer lives on your disk drive, be it a hard disk drive (HDD) or a solid-state drive (SSD).
- Disk drives are just storage space; we can't directly work there. Manipulation and use of data can only take place in RAM, so we have to move data there.

# Memory

- Every file on your computer lives on your disk drive, be it a hard disk drive (HDD) or a solid-state drive (SSD).
- Disk drives are just storage space; we can't directly work there. Manipulation and use of data can only take place in RAM, so we have to move data there.
- Memory is basically a huge array of 8-bit wide bytes.
  - 512 MB, 1GB, 2GB, 4GB...



# Memory

Data Type	Size (in bytes)
int	4
char	1
float	4
double	8
long	8

# Memory

- Back to this idea of memory as a big array of byte-sized cells.

# Memory

- Back to this idea of memory as a big array of byte-sized cells.
- Arrays are useful for storage of information but also for so-called *random access*.
  - We can access individual elements of the array by indicating which index location we want.

# Memory

- Back to this idea of memory as a big array of byte-sized cells.
- Arrays are useful for storage of information but also for so-called *random access*.
  - We can access individual elements of the array by indicating which index location we want.
- Similarly, each location in memory has an *address*.

# Representation of Memory

- If you've ever head the term "32-bit system" or "64-bit system," it's referring to memory.

# Representation of Memory

- If you've ever heard the term "32-bit system" or "64-bit system," it's referring to memory.
- A 32-bit system processor can understand and process memory addresses up to 32 bits in length.

# Representation of Memory

- If you've ever heard the term "32-bit system" or "64-bit system," it's referring to memory.
- A 32-bit system processor can understand and process memory addresses up to 32 bits in length.
- With each bit being a 0 (off, no power) or a 1 (on, powered), that means there are  $2^{32}$  possible memory addresses, or about 4 billion.

# Representation of Memory

- Computers (and programmers!) often need a way to refer to specific addresses in memory, whether for random access or merely for reference purposes.



# Representation of Memory

- Computers (and programmers!) often need a way to refer to specific addresses in memory, whether for random access or merely for reference purposes.

- Rather than specifying an address as 32 bits:

**00101001 11010110 00101110 01010111**

# Representation of Memory

- Computers (and programmers!) often need a way to refer to specific addresses in memory, whether for random access or merely for reference purposes.

- Rather than specifying an address as 32 bits:

**00101001 11010110 00101110 01010111**

- Computer scientists often refer to such values using *hexadecimal notation*.

**0x**

# Representation of Memory

- Computers (and programmers!) often need a way to refer to specific addresses in memory, whether for random access or merely for reference purposes.

- Rather than specifying an address as 32 bits:

**00101001 11010110 00101110 01010111**

- Computer scientists often refer to such values using *hexadecimal notation*.

**0x 29D62E57**

Breakpoint 1, 0x004005af in main ()

(gdb) i r

eax	0xb7fb9dbc	-1208246852
ecx	0xbfffffff340	-1073745088
edx	0xbfffffff364	-1073745052
ebx	0x0	0
esp	0xbfffffff320	0xbfffffff320
ebp	0xbfffffff328	0xbfffffff328
...		

Breakpoint 1, 0x004005af in main ()

(gdb) i r

eax	0xb7fb9dbc	-1208246852
ecx	0xbfffffff340	-1073745088
edx	0xbfffffff364	-1073745052
ebx	0x0	0
esp	0xbfffffff320	0xbfffffff320
ebp	0xbfffffff328	0xbfffffff328
...		

Breakpoint 1, **0x004005af** in main ()

(gdb) i r

eax	0xb7fb9dbc	-1208246852
ecx	0xbfffffff340	-1073745088
edx	0xbfffffff364	-1073745052
ebx	0x0	0
esp	0xbfffffff320	0xbfffffff320
ebp	0xbfffffff328	0xbfffffff328
...		

Breakpoint 1, 0x004005af in **main** ()

(gdb) i r

eax	0xb7fb9dbc	-1208246852
ecx	0xbfffffff340	-1073745088
edx	0xbfffffff364	-1073745052
ebx	0x0	0
esp	0xbfffffff320	0xbfffffff320
ebp	0xbfffffff328	0xbfffffff328
...		

Breakpoint 1, 0x004005af in main ()

(gdb) i r

<b>eax</b>	0xb7fb9dbc	-1208246852
<b>ecx</b>	0xbfffffff340	-1073745088
<b>edx</b>	0xbfffffff364	-1073745052
<b>ebx</b>	0x0	0
<b>esp</b>	0xbfffffff320	0xbfffffff320
<b>ebp</b>	0xbfffffff328	0xbfffffff328
...		



Breakpoint 1, 0x004005af in main ()

(gdb) i r

eax	0xb7fb9dbc	-1208246852
ecx	0xbffff340	-1073745088
edx	0xbffff364	-1073745052
ebx	0x0	0
esp	0xbffff320	0xbffff320
ebp	0xbffff328	0xbffff328
...		

Breakpoint 1, 0x004005af in main ()

(gdb) i r

eax	0xb7fb9dbc	-1208246852
ecx	0xbffff340	-1073745088
edx	0xbffff364	-1073745052
ebx	0x0	0
esp	0xbffff320	0xbffff320
ebp	0xbffff328	0xbffff328
...		

# Hexadecimal

Decimal	Binary	Hex
0	0000	0x0
1	0001	0x1
2	0010	0x2
3	0011	0x3
4	0100	0x4
5	0101	0x5
6	0110	0x6
7	0111	0x7

Decimal	Binary	Hex
8	1000	0x8
9	1001	0x9
10	1010	0xA (a)
11	1011	0xB (b)
12	1100	0xC (c)
13	1101	0xD (d)
14	1110	0xE (e)
15	1111	0xF (f)

# How Memory Works

- With the exception of hard disk space, memory on your computer is *volatile*.



Image source: [howstuffworks.com](http://howstuffworks.com)

# How Memory Works

- With the exception of hard disk space, memory on your computer is *volatile*.
- Volatile memory requires *power*.



Image source: [howstuffworks.com](http://howstuffworks.com)

# How Memory Works

- With the exception of hard disk space, memory on your computer is *volatile*.
- Volatile memory requires *power*.
- After a limited amount of time with no power, the electrical charge dissipates, and "state" is lost.



Image source: [howstuffworks.com](http://howstuffworks.com)

# How Memory Works

- Processing of information can only happen, as you might expect, in the *processor*. A 32-bit processor can only process 32 bits (4 bytes) of information at a time.

# How Memory Works

- Processing of information can only happen, as you might expect, in the *processor*. A 32-bit processor can only process 32 bits (4 bytes) of information at a time.
- This means that data needs to be moved pretty constantly around between different parts of memory, feeding new information to the processor.



# How Memory Works

- Processing of information can only happen, as you might expect, in the *processor*. A 32-bit processor can only process 32 bits (4 bytes) of information at a time.
- This means that data needs to be moved pretty constantly around between different parts of memory, feeding new information to the processor.
- Despite being only able to process limited information at a time, most processors today are about 2-3 GHz.

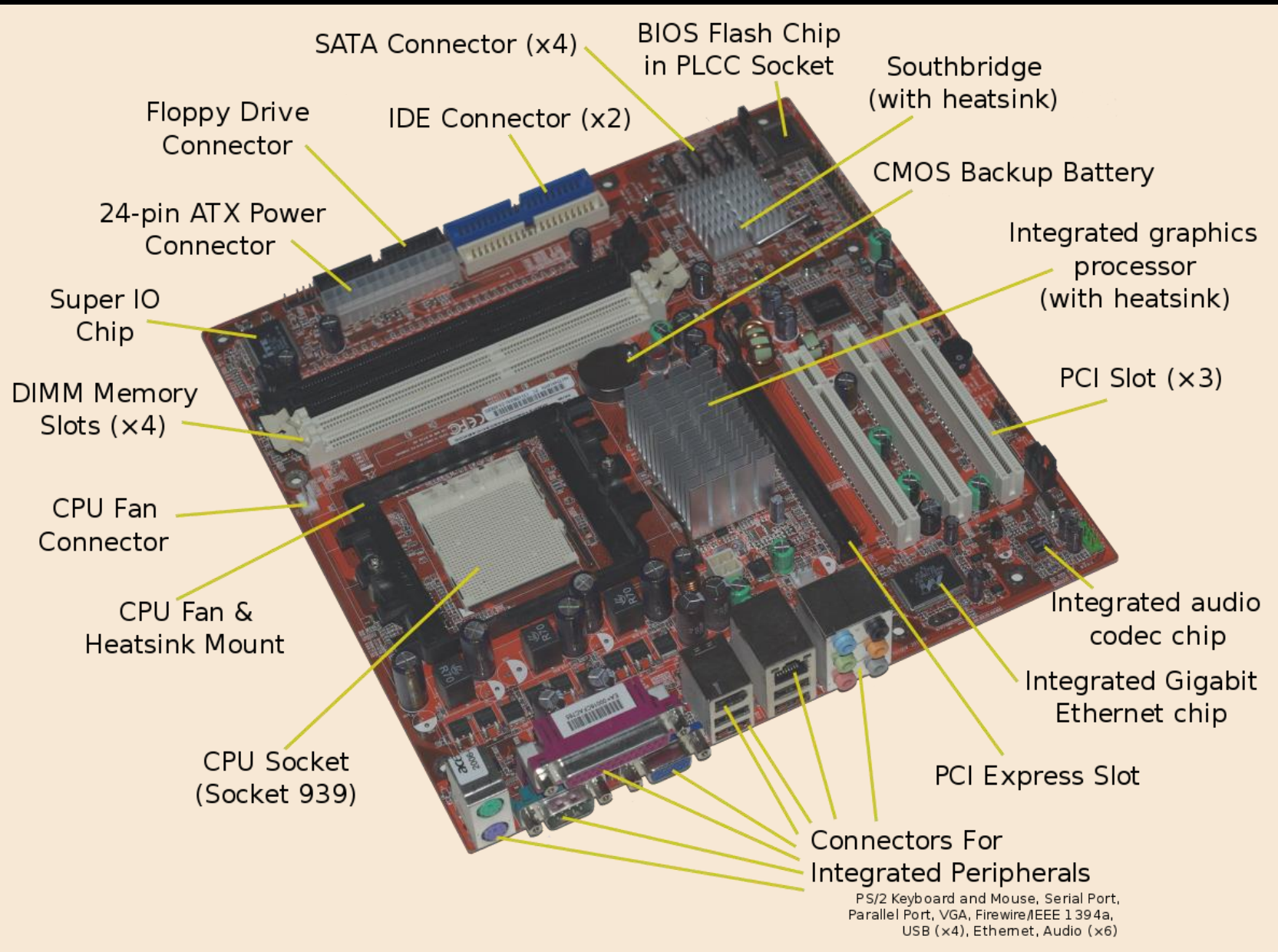


Image source: WikiMedia

# How Memory Works

- CPU memory is the fastest, least amount of memory on your machine.

# How Memory Works

- CPU memory is the fastest, least amount of memory on your machine.
- Caches (L3, L2, L1) are each successively slower, but each successively cheaper.

# How Memory Works

- CPU memory is the fastest, least amount of memory on your machine.
- Caches (L3, L2, L1) are each successively slower, but each successively cheaper.
- RAM is slower, but cheaper.

# How Memory Works

- CPU memory is the fastest, least amount of memory on your machine.
- Caches (L3, L2, L1) are each successively slower, but each successively cheaper.
- RAM is slower, but cheaper.
- Hard disk space is pure storage, but insanely cheap.

# How Memory Works

- Hard disk space (whether HDD, SSD, or Flash/USB), by contrast, is *non-volatile* or *persistent*.



Image source: [geek.com](http://geek.com)

# How Memory Works

- Hard disk space (whether HDD, SSD, or Flash/USB), by contrast, is *non-volatile* or *persistent*.
- It explicitly does *not* require power to work. Rather, each "cell" of memory is written to by way of using magnets.



Image source: [geek.com](http://geek.com)



# How Memory Works

- Hard disk space (whether HDD, SSD, or Flash/USB), by contrast, is *non-volatile* or *persistent*.
- It explicitly does *not* require power to work. Rather, each "cell" of memory is written to by way of using magnets.
- Because the magnets do not need power, when the computer shuts off, the data remains.



Image source: [geek.com](http://geek.com)

# How Memory Works

- As we've seen though, hard disk space cannot be directly manipulated; it has to move to the processor.

# How Memory Works

- As we've seen though, hard disk space cannot be directly manipulated; it has to move to the processor.
- This is done through a series of connections called *buses* that transfer data from one type of memory to another.

# How Memory Works

- As we've seen though, hard disk space cannot be directly manipulated; it has to move to the processor.
- This is done through a series of connections called *buses* that transfer data from one type of memory to another.
- In general, when working on a program, the data for that program (including the code for the program itself) is moved into RAM, and it's manipulated and moved around from there until the program is finished.

# Hard Drive Failure

- Because they have literal moving pieces, it's not uncommon for hard drives to fail after a period of time.

# Hard Drive Failure

- Because they have literal moving pieces, it's not uncommon for hard drives to fail after a period of time.
- Normally, this means that the read/write arm has jammed, or has "bumped" into the spinning platters, which destroys the mechanisms.

# Hard Drive Failure

- Because they have literal moving pieces, it's not uncommon for hard drives to fail after a period of time.
- Normally, this means that the read/write arm has jammed, or has "bumped" into the spinning platters, which destroys the mechanisms.
- But a hard drive failure doesn't necessarily mean the data is unrecoverable.

# File Deletion

- What happens when we delete files on our machines?



Image source: knowtechie.com



# *United States v. Flyer*

633 F.3d 911 (9th Cir., 2011)

# File Deletion

- What happens when we delete files on our machines?
- Overwriting hard disk space is an expensive and time-consuming operation for the machine.



Image source: knowtechie.com

# File Deletion

- What happens when we delete files on our machines?
- Overwriting hard disk space is an expensive and time-consuming operation for the machine.
- Instead, the system just conveniently "forgets" where that data lived, meaning at some point in the future, it may be eventually overwritten.

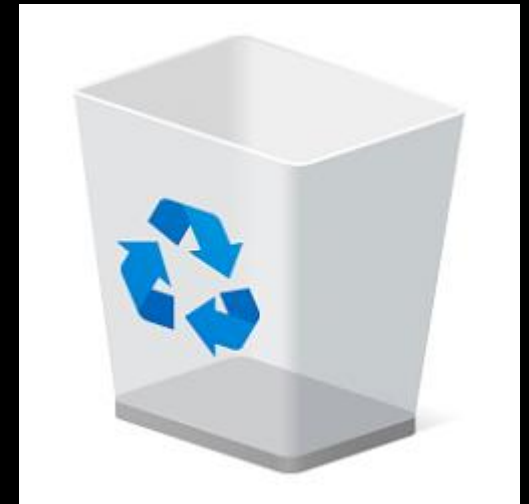


Image source: knowtechie.com

# File Deletion

- What happens when we delete files on our machines?
- Overwriting hard disk space is an expensive and time-consuming operation for the machine.
- Instead, the system just conveniently "forgets" where that data lived, meaning at some point in the future, it may be eventually overwritten.



Image source: microsoft.com

# File Deletion

- What happens when we delete files on our machines?
- Overwriting hard disk space is an expensive and time-consuming operation for the machine.
- Instead, the system just conveniently "forgets" where that data lived, meaning at some point in the future, it may be eventually overwritten.



Image source: microsoft.com

Break

# Agenda

- Hardware
- Memory
- Hard drives
- Data persistence
- File transfer
- Client data
- Compliance protocols

# Digital Forensics

- So when a hard drive is "damaged" or files are "deleted," how is it possible to recover information from it?



# Digital Forensics

- So when a hard drive is "damaged" or files are "deleted," how is it possible to recover information from it?
- There are specialized tools out there that can be used to incredibly systematically (and incredibly slowly) read off of "damaged" hard drives bit-by-bit.

# Digital Forensics

- So when a hard drive is "damaged" or files are "deleted," how is it possible to recover information from it?
- There are specialized tools out there that can be used to incredibly systematically (and incredibly slowly) read off of "damaged" hard drives bit-by-bit.
- In both cases, a *forensic image* (essentially, a huge file) that replicates the bit-by-bit content of the hard drive can be created and put onto a functional machine.

# Digital Forensics

- Most files have some sort of an identifying "signature" associated with them, also known as a *magic number*.

# Digital Forensics

- Most files have some sort of an identifying "signature" associated with them, also known as a *magic number*.
- Odds are, if this specific sequence appears (it's usually 4-8 bytes), it's the beginning of a file of that type, and it can be read.

# Deleting Files



Image source: dr-fone.com

# Deleting Files

- If ordinarily files are not deleted from a hard drive, what can we do to actually really go out of our way to delete data?

# Deleting Files

- If ordinarily files are not deleted from a hard drive, what can we do to actually really go out of our way to delete data?
- Physical destruction of the hard drive

# Deleting Files

- If ordinarily files are not deleted from a hard drive, what can we do to actually really go out of our way to delete data?
- Physical destruction of the hard drive
- Use a *degausser*



# Deleting Files

- If ordinarily files are not deleted from a hard drive, what can we do to actually really go out of our way to delete data?
- Physical destruction of the hard drive
- Use a *degausser*
- Overwrite with random bits (but not all 0s and not all 1s)

# Deleting Files

- If ordinarily files are not deleted from a hard drive, what can we do to actually really go out of our way to delete data?
- Physical destruction of the hard drive
- Use a *degausser*
- Overwrite with random bits (but not all 0s and not all 1s)
- Practice note: Maybe don't do this with client data! 😊

# File Transfer

- What are some ways that we can migrate data from one machine to another?

# File Transfer

- What are some ways that we can migrate data from one machine to another?
- Emailing files

# File Transfer

- What are some ways that we can migrate data from one machine to another?
- Emailing files
- Physical device-to-device connection

# File Transfer

- What are some ways that we can migrate data from one machine to another?
- Emailing files
- Physical device-to-device connection
- USB transfer

# File Transfer

- What are some ways that we can migrate data from one machine to another?
- Emailing files
- Physical device-to-device connection
- USB transfer
- FTP

# File Transfer

- What are some ways that we can migrate data from one machine to another?
- Emailing files
- Physical device-to-device connection
- USB transfer
- FTP
- What are some upsides and downsides of each approach?



# File Transfer

- FTP, or the file transfer protocol, is one standard means of migrating data between devices over the internet, and also for some businesses to actually host material for others to download.

# File Transfer

- FTP, or the file transfer protocol, is one standard means of migrating data between devices over the internet, and also for some businesses to actually host material for others to download.
- It uses a client-server model, where files are hosted on the server and downloaded to the destination device (client).

# File Transfer

- FTP, or the file transfer protocol, is one standard means of migrating data between devices over the internet, and also for some businesses to actually host material for others to download.
- It uses a client-server model, where files are hosted on the server and downloaded to the destination device (client).
- FTP is not an inherently secure protocol; if username and password are required, they are sent "in the clear."

# Protecting Client Data

- Odds are, if you end up taking a job in a firm environment or as in-house counsel, this will not all fall to you, but it's very important (and indeed an ABA Model Rule!) to take active steps early on to protect client data.

# Protecting Client Data

- Odds are, if you end up taking a job in a firm environment or as in-house counsel, this will not all fall to you, but it's very important (and indeed an ABA Model Rule!) to take active steps early on to protect client data.
- Here are a variety of ways that you as a practitioner can begin instituting best practices for data security.

# Protecting Client Data

- Encrypt your hard drive

# Protecting Client Data

- Encrypt your hard drive
- Most operating systems provide you with built-in ways to do this now, no reason not to do it!

# Protecting Client Data

- Encrypt your hard drive
- Most operating systems provide you with built-in ways to do this now, no reason not to do it!
- Require a password immediately after turning your computer on, before it boots and loads the OS.



# Protecting Client Data

- Encrypt your hard drive
- Most operating systems provide you with built-in ways to do this now, no reason not to do it!
- Require a password immediately after turning your computer on, before it boots and loads the OS.
- Some of these systems actually initiate a multi-pass hard drive wipe after  $n$  incorrect password entries, so don't forget!

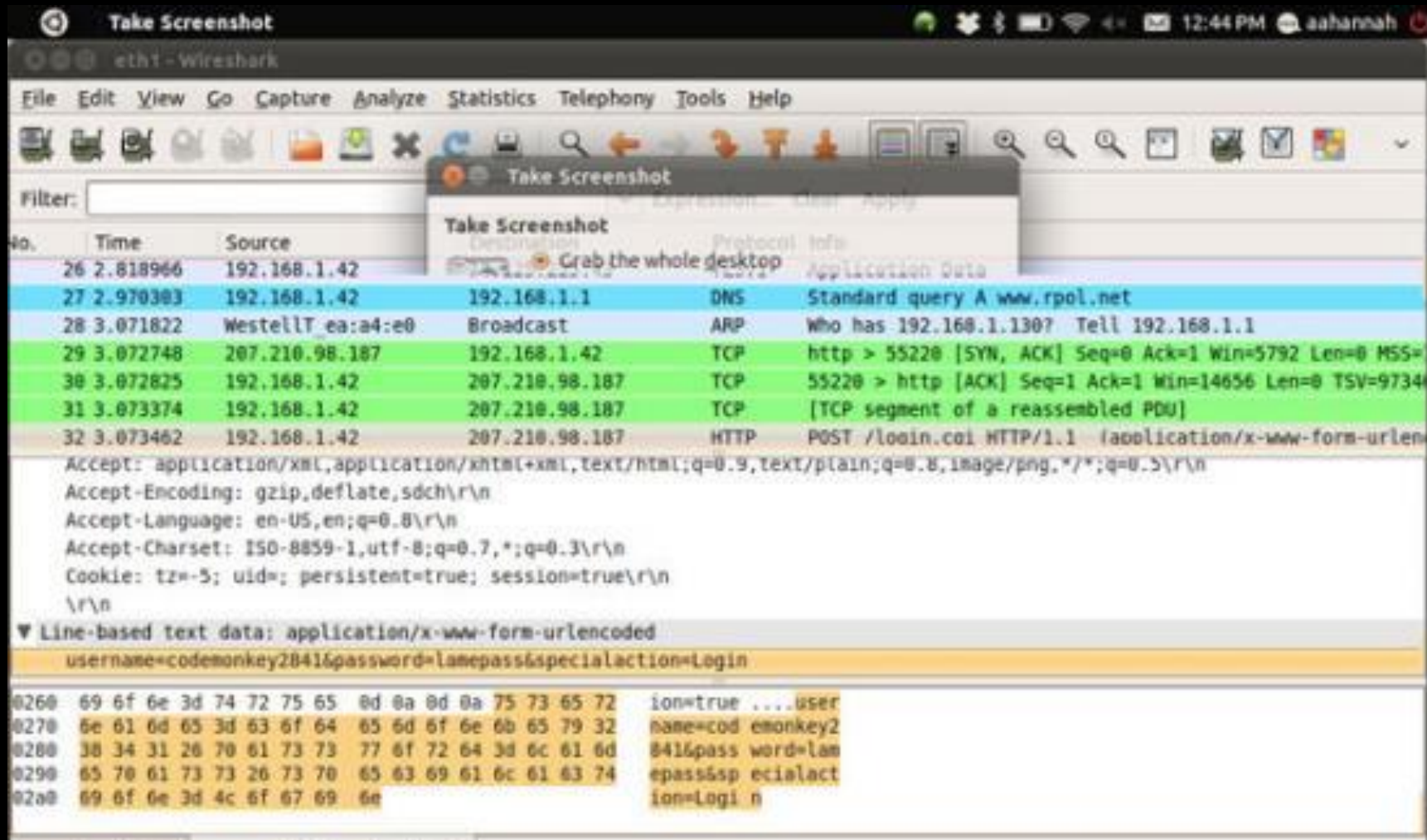
# Protecting Client Data

- Avoid insecure wireless networks

# Protecting Client Data

- Avoid insecure wireless networks
- Though uncommon, unsecured networks provide opportunities for data to be "plucked" out of the air.

# Protecting Client Data



# Protecting Client Data

- Avoid insecure wireless networks
- Though uncommon, unsecured networks provide opportunities for data to be "plucked" out of the air.
- Whenever in an unfamiliar location, rely on private or work-provided VPN services.

# Protecting Client Data

- Use password managers

# Protecting Client Data

- Use password managers
- LastPass, 1Password, and others are great services that make it quite easy to more generally secure your access to anything that requires a login.

# Protecting Client Data

- Use password managers
- LastPass, 1Password, and others are great services that make it quite easy to more generally secure your access to anything that requires a login.
- Most of these tools also support two-factor authentication.



# Protecting Client Data

- Use password managers
- LastPass, 1Password, and others are great services that make it quite easy to more generally secure your access to anything that requires a login.
- Most of these tools also support two-factor authentication.
- Though they sound great, be skeptical. What's one potential problem with tools like this?

EDITION: [US](#) ▼



[CES 2019](#)

[VIDEOS](#)

[5G](#)

[WINDOWS 10](#)

[CLOUD](#)

[INNOVATION](#)

[SECURITY](#)

[MORE](#) ▼

[NEWSLETTERS](#)

CES 2019: [What happens when the cops get hit with malware, too?](#)

# Data of 2.4 million Blur password manager users left exposed online

Company says data breach didn't expose any actual passwords stored inside users' Blur accounts.



By [Catalin Cimpanu](#) | January 2, 2019 -- 19:51 GMT (11:51 PST) | Topic: [Security](#)

EDITION: US ▼



[CES 2019](#)

[VIDEOS](#)

[5G](#)

[WINDOWS 10](#)


[CLOUD](#)

[INNOVATION](#)

[SECURITY](#)

[MORE ▼](#)

[NEWSLETTERS](#)

 [CES 2019](#): What happens when the cops get hit with malware, too?

# Data of 2.4 million Blur password manager users left exposed online

Company says data breach didn't expose any actual passwords stored inside users' Blur accounts.



By [Catalin Cimpanu](#) [January 2, 2019](#) 19:51 GMT (11:51 PST) | Topic: [Security](#)

The background of the image is a dark, atmospheric landscape. It features a silhouette of a mountain range in the foreground, with a jagged, dark ridge line. Above the mountains, the sky is filled with soft, layered clouds in shades of blue and grey, suggesting a twilight or dawn setting. The overall mood is somber and mysterious.

TRUST NO ONE

# Protecting Client Data

- Use complex passwords

# Protecting Client Data

- Use complex passwords
- If you would prefer not to use a password manager, at least be certain to use complex passwords.

# Protecting Client Data

- Use complex passwords
- If you would prefer not to use a password manager, at least be certain to use complex passwords.
- Passwords with  $\leq 7$  characters, you should consider effectively broken already, especially if they only contain letters and numbers.

# Protecting Client Data

- Change your passwords



# Protecting Client Data

- Change your passwords
- Easier said than done in most cases without a password manager, but rotating through new passwords every 90 days is a good defense.

# Protecting Client Data

- Create backups

# Protecting Client Data

- Create backups
- Periodically backing up client data preserves your work and their data in the event of a catastrophic hardware failure or "ransom" hack.

# Protecting Client Data

- Create backups
- Periodically backing up client data preserves your work and their data in the event of a catastrophic hardware failure or "ransom" hack.
- Back data up to non-network connected machines or to flash drives or disks. (Or to paper files!)

# Protecting Client Data

- Have an archival/deletion plan for data

# Protecting Client Data

- Have an archival/deletion plan for data
- We tend to think these days that data exists in digital form permanently, but that's not entirely true.

# Protecting Client Data

- Have an archival/deletion plan for data
- We tend to think these days that data exists in digital form permanently, but that's not entirely true.
- Develop a consistent plan for deleting and archiving data after a period of time (e.g., 5 years)

# Protecting Client Data

- Make talking about data security a priority



# Protecting Client Data

- Make talking about data security a priority
- Many people are not as educated about technology as they should be. You don't have to be an expert to have a meaningful discussion about technology in the legal field.

# Protecting Client Data

- Make talking about data security a priority
- Many people are not as educated about technology as they should be. You don't have to be an expert to have a meaningful discussion about technology in the legal field.
- Share your knowledge with those around you, and with your clients.

# Protecting Client Data

- Establish compliance protocols

# Protecting Client Data

- Establish compliance protocols
- It's not all that hard to set up most of this stuff early on, it gets a bit harder to do it regularly on top of everything else you do.

# Protecting Client Data

- Establish compliance protocols
- It's not all that hard to set up most of this stuff early on, it gets a bit harder to do it regularly on top of everything else you do.
- Set regular intervals for "checkups" to ensure this data is protected to the best of your ability.

# Protecting Client Data

- Establish compliance protocols
- It's not all that hard to set up most of this stuff early on, it gets a bit harder to do it regularly on top of everything else you do.
- Set regular intervals for "checkups" to ensure this data is protected to the best of your ability.
- Volunteer to work with the compliance team if at a bigger firm.

*ABA Formal Opinion No. 477R*

# *ABA Formal Opinion No. 483*



# Cybersecurity: Memory and Data Protection

CS50 for JDs  
Winter Term 2019