Hacking

Professor Grimmelmann

Internet Law

Fall 2007

Class 15

Where we are

- Part I: Public Law
- Part II: Private Law
  - Control over Computers
  - Domain Names
  - Copyright
  - Innovation
  - Case Studies

In Today’s Class

- The history of hacking: good, bad, and Hollywood
- The Computer Fraud and Abuse Act
- The scary future of computer crime

A brief history of hacking

Originally, hacking was *good*

- A “hack” might be a quick-and-dirty way of getting a system to work
- Or, it might be a programming feat of unusual elegance
- Either way, a “hacker” was someone playing with computers and making them do neat things, and “hacking” was spending time programming
- So what happened?

The phone phreakers

- Combine a hacker’s interest in cool technologies with the phone system and the result was perhaps inevitable
- E.g., play a 2600Hz tone and the phone company’s switch will reset itself

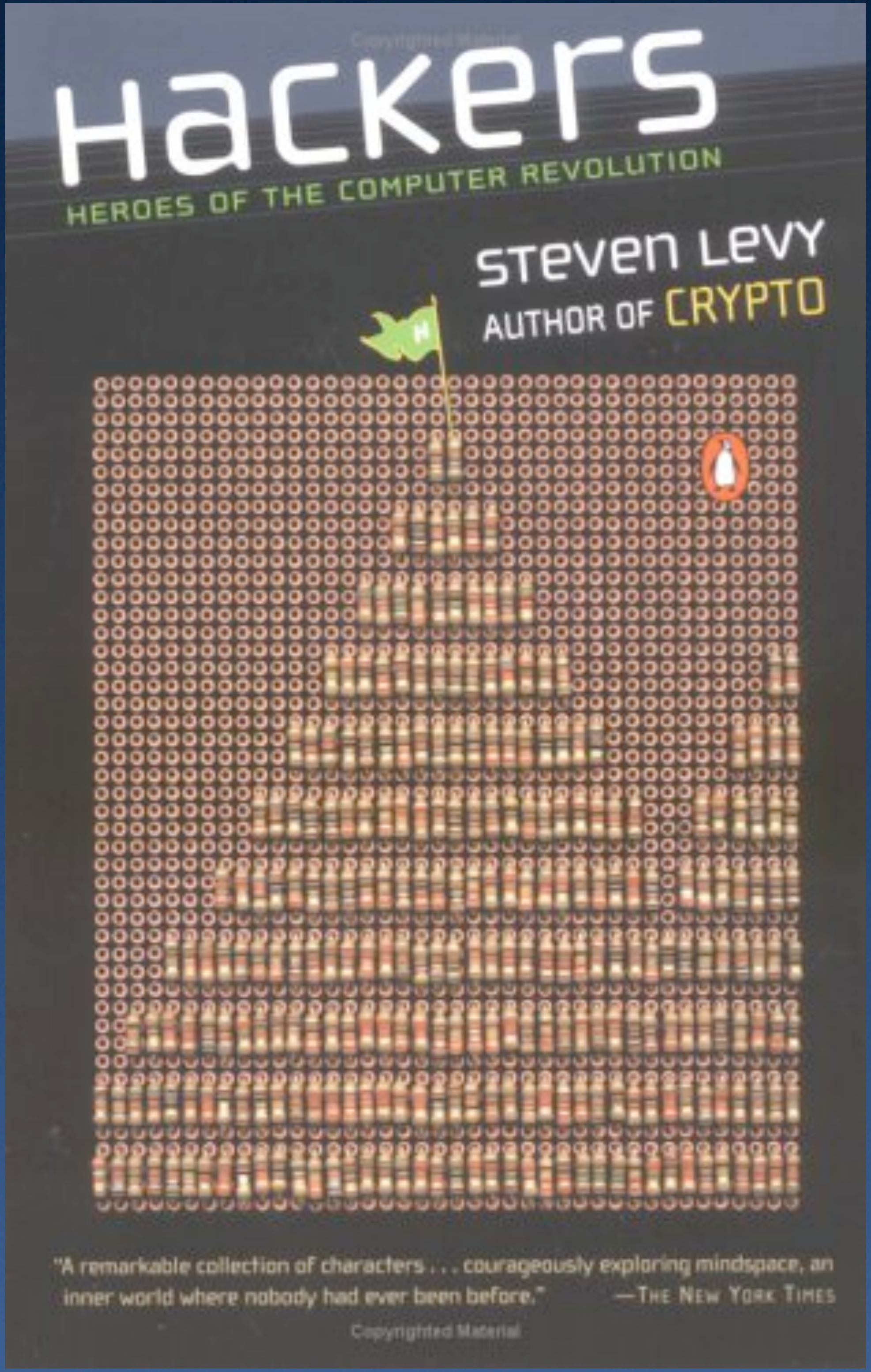
Who’d use a blue box?

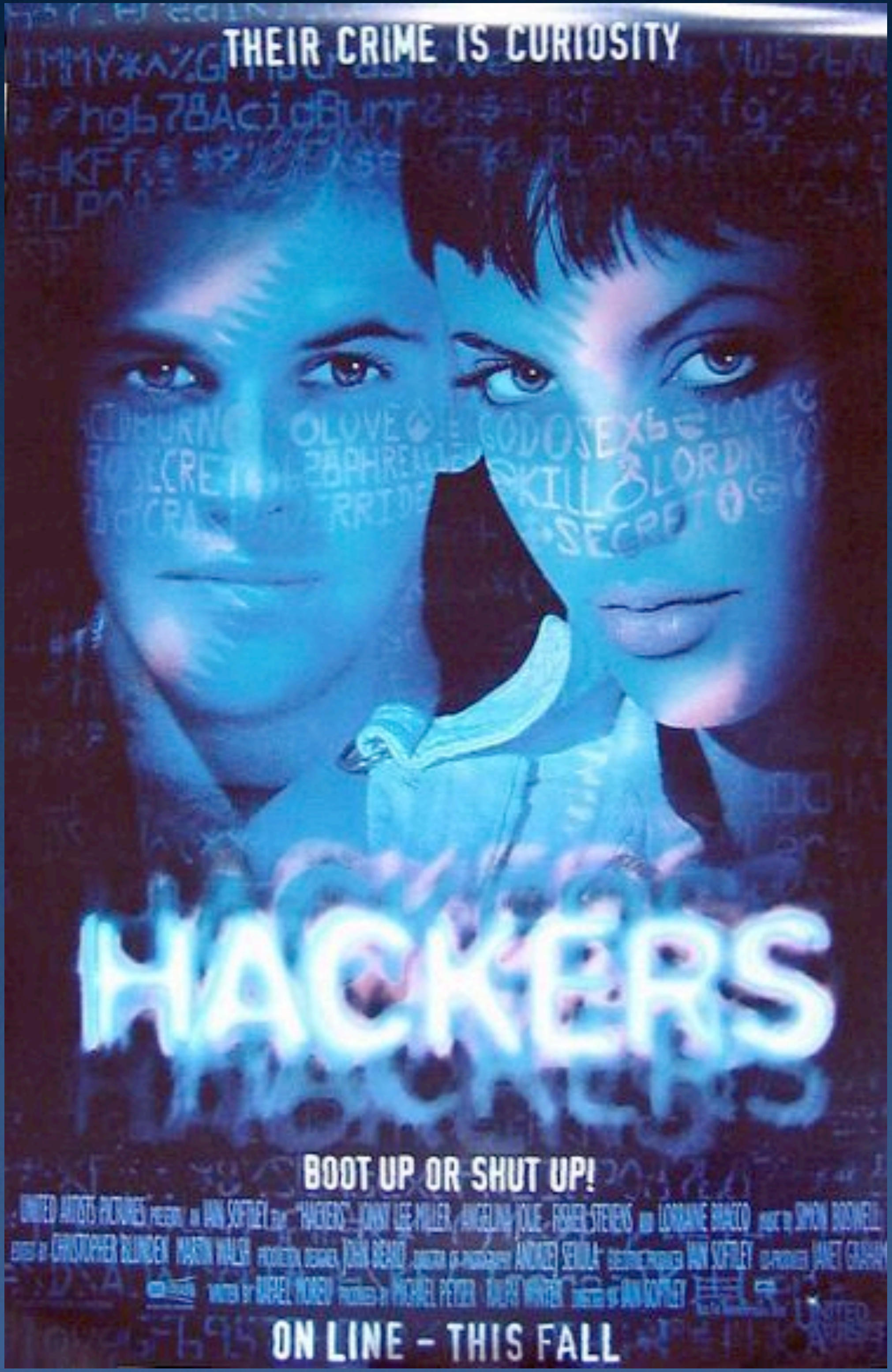
- The good: hackers interested in the phone system
- The bad: everyday schlubs who want to make free phone calls
- The ugly: people who want to destroy the phone network

Hacking’s never been that big

- It’s mostly:
  - Kids
  - People obsessed with the phone network
- Natural transition to computer networks, which control the phones and turn out to be cool in their own right
- Lots of swagger and bravado, most of it around proving what you *could* do

But compare:


Hackers
HEROES OF THE COMPUTER REVOLUTION
STEVEN LEVY
AUTHOR OF CRYPTO
"A remarkable collection of characters . . . courageously exploring mindspace, an inner world where nobody had ever been before." —THE NEW YORK TIMES


THEIR CRIME IS CURIOSITY
HACKERS
BOOT UP OR SHUT UP!
ON LINE - THIS FALL

Some notable incidents

- 1986: Cliff Stoll finds $.75 missing on the accounts at a lab computer, and tracks it back to a German hacking gang
- 1989–90: Legion of Doom / Masters of Deception crackdown
- 1995: Kevin Mitnick tracked down and arrested

White hats or black hats?

- Cult of the Dead Cow: intrusion tools or intrusion-prevention tools?
  - Hacktivismo: hacking for human rights
- 2600 Magazine, which we'll meet again
- Kevin Mitnick, security consultant
- Kevin Poulsen, former cracker, catches a pedophile soliciting children on MySpace

The Computer Fraud and Abuse Act (1986)

CFAA, 18 U.S.C. § 1030

- Various overlapping provisions prohibit "accessing" a "protected computer" "without authorization"
  - Primarily criminal (penalties depend on various aggravating factors)
  - § 1030(g) gives a civil remedy where the violation causes "damage or loss"
- Every state has its own computer-misuse statute

An apology

- The casebook has the pre-USA PATRIOT Act text of § 1030
    - It’s my fault for not catching this
- *For purposes of this course only*, treat the text in the casebook as authoritative
- In real life, always look it up!

Five interpretive questions

1. What’s a “protected computer?”
2. What’s “access?”
3. What’s “authorization?”
4. Is “exceeds authorized access” different from “accesses without authorization?”
5. What’s “damage or loss?”

Some common fact patterns

- *Port-scanning*: sending a series of requests to a networked computer to see what (possibly vulnerable) services it provides
- *Spamming*: sending thousands of emails through a computer that has email software installed on it
- *Password-guessing*: trying common passwords on an account to see if any of them happen to be the actual one

1. What’s a “protected computer”?

- § 1030(e)(2):
  - Either a computer used by “a financial institution or the United States Government,” or
  - A computer “used in interstate or foreign commerce or communication”
- Can you think of a computer that isn’t a “protected computer?”

2. What’s “access?”

- Did Morris “access” various computers?
- Did the *Shurgard* defendants “access” Shurgard’s computers?
- Did Doubleclick “access” users’ computers?
- Yes, yes, and yes.
- How about password-guessing? Port-scanning? Spamming? Failed spamming?

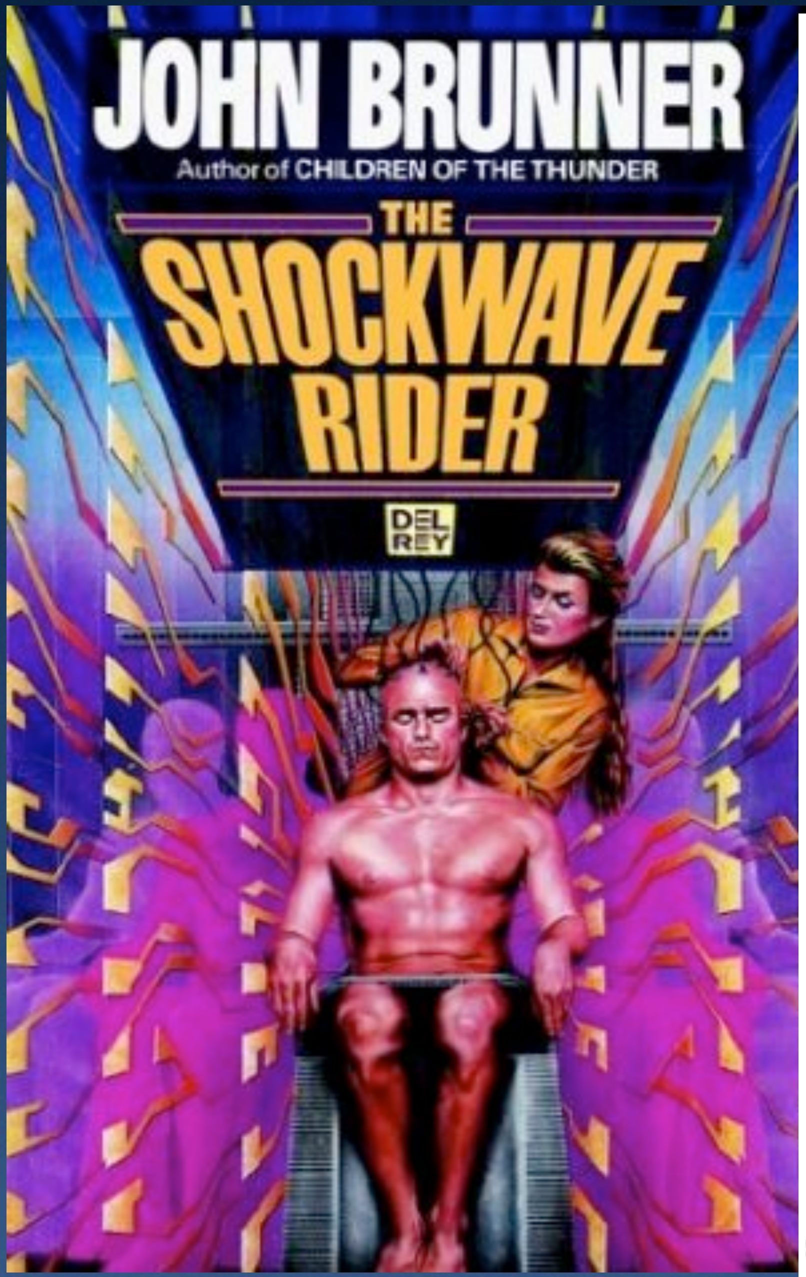
2. What's "access?" (cntd.)

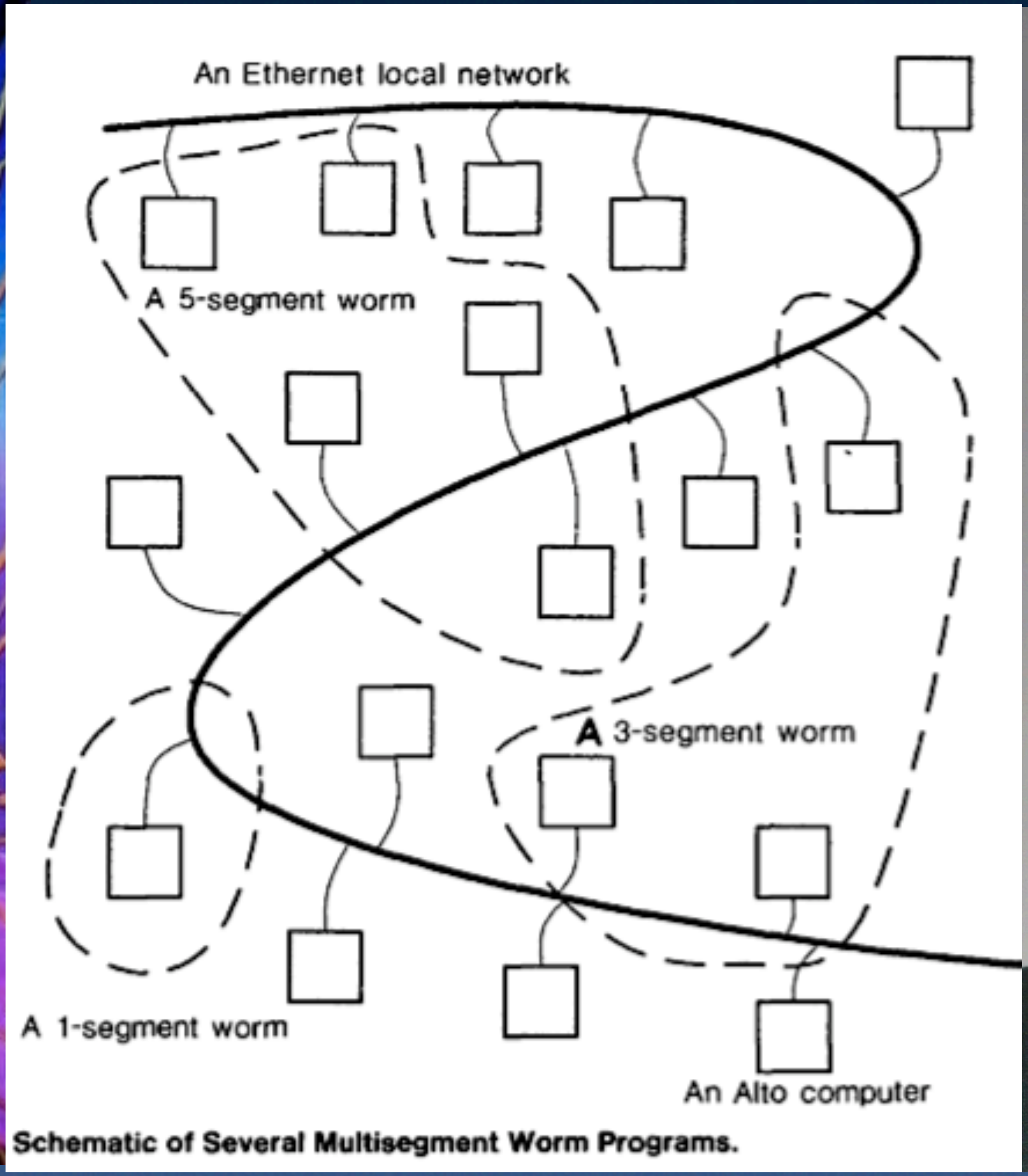
- What's "access" from the internal perspective? From the external perspective?
- How do the various scanning techniques fare under an internal definition of "access?" Under an external one?
- Which rule makes more sense?
    - Can this question be answered in isolation?

3. What's "authorization?"

- There are some easy cases:
  - Fred Felon breaks into a bank at night, find's a loan officer's password in a desk drawer, and logs into a computer in an attempt to issue himself a check
  - (But what about the argument that the computer "authorized" him to access it when it accepted his login?)
- Why is this an easy case?

The Internet Worm





Schematic of Several Multisegment Worm Programs.

Sci-fi: 1975 Research: 1982 Real life: 1988

Robert Tappan Morris

- *Wunderkind* grad student and programmer
  - His program is a masterpiece of clever hacking techniques
  - And also contains *two* boneheaded technical mistakes
- Ig Nobel Awards Editorial Board member
- Dot-com multi-millionaire
- MIT professor

Authorization: Morris

- He’s allowed to use the MIT computer
  - Sendmail normally sends email
  - Morris finds a way to make it also install and replicate copies of the worm
- He concedes that he “exceeded authorized access, but did he “access without authorization?”
- Held: *yes*

Morris: the “intended function” test

- “Morris did not use either of these features in any way related to their intended function.”
- How does a court determine the “intended function” of a program?
- Under this test, is logging in with a guessed password “authorized?” How about using sendmail to send spam? How about using it to send a harassing email?

Morris: the “no account” test

- “Moreover, there was also evidence that the worm was defined to gain access to computers at which he had no account by guessing their passwords.”
- Under this test, is port-scanning authorized? How about spamming? How about forcing someone to give your their password at gunpoint? How about using someone else’s password with their permission and encouragement?

Authorization: *Shurgard*

- Leland works for Shurgard and has access to a corporate computer system with all sorts of juicy trade secrets on it
    - Safeguard hires him in secret.
    - While still on Shurgard's payroll, he logs on to Shurgard's computers and emails the juicy trade secrets to Safeguard
- Was his access "without authorization?"

Shurgard: the purpose test

- Citing the Restatement of Agency:
  - “The authority of the plaintiff's former employees ended when they allegedly became agents of the defendant.”
- I.e., if you break a condition of your access, it becomes unauthorized
  - Does this make sending personal email from a work computer a federal crime?

We’ve seen three tests so far:

- Intended function: you’re authorized to do whatever the software is intended to let people do
- No account: it’s “unauthorized” to use a program without an appropriate account
- Purpose: it’s unauthorized to use the computer for a purpose the owner disapproves of (e.g. in terms of service)

Hypothetical: Bluebeard’s computer

- Mr. Bluebeard lets Mrs. Bluebeard use his computer but tells her not to open the “ClosedDoor” folder
  - She opens it
- On the intended-function test, has she “accessed without authorization?”
  - On the no-account test?
  - On the purpose test?

4. “Exceeds authorized access”

“[T]he term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;”

18 U.S.C. § 1030(e)(6)

“Exceeds authorized access” (cntd.)

- Some scholars and courts say “exceeds authorized access” means exactly the same thing as “accesses without authorization”
- Others draw a line between having any permission to use a computer and having none
- Does that line make sense on the Internet?
- Can you think of any other possible lines?

5. “Damage”

- § 1030(a)(5): “causes damage” (criminal)
  - § 1030(g): “who suffers damage or loss” (civil)
- § 1030(e)(8): “[T]he term ‘damage’ means any impairment to the integrity or availability of data, a program, a system, or information;”

A puzzle

- The civil remedy has a $5,000 threshold
  - What kinds of “damage or loss” count?
- Easy cases:
  - Crashed computers
  - Deleted data
- Senate Report: efforts to resecure the system are “loss” but not “damage”

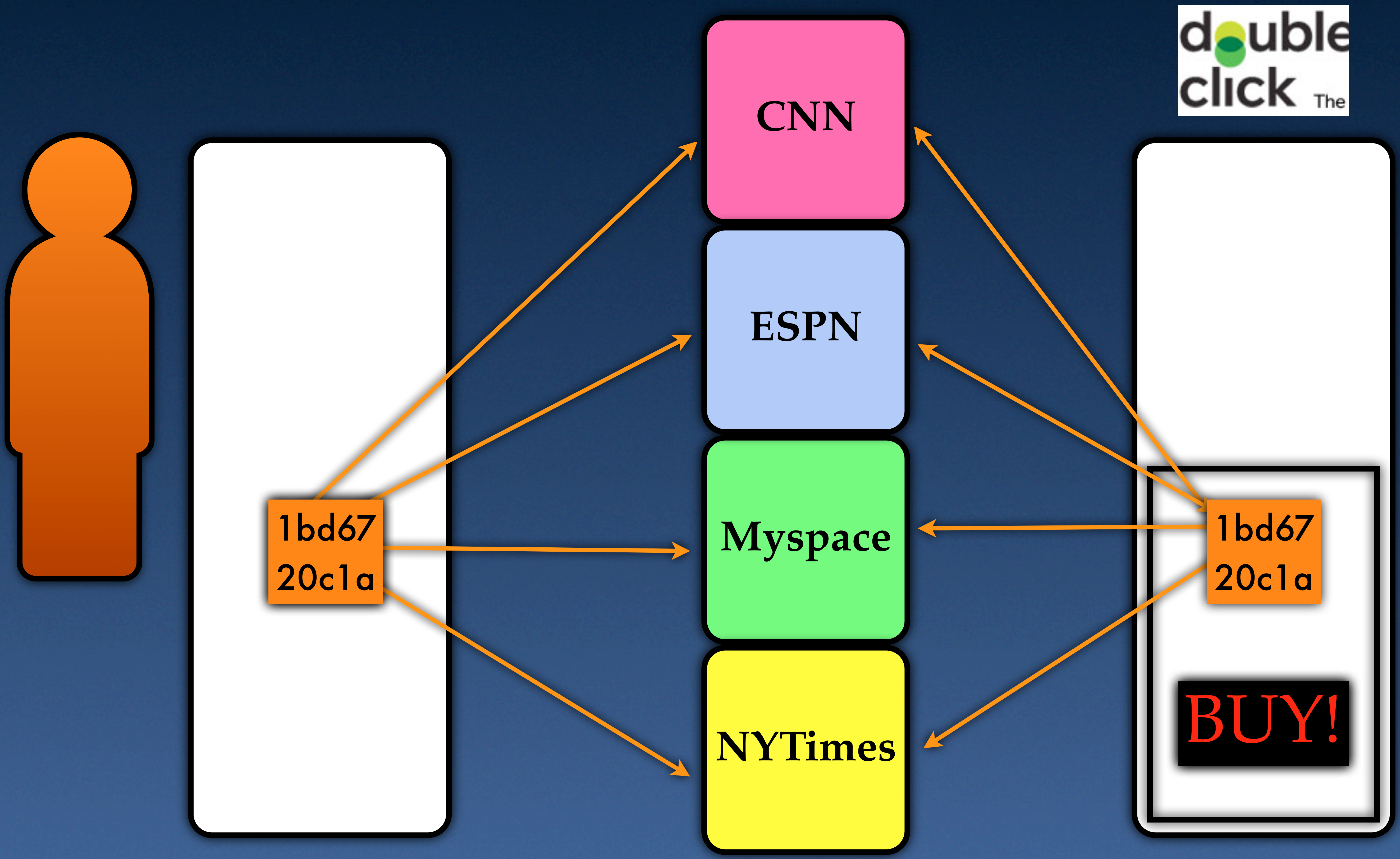
Damage: *Shurgard*

- The court finds that defendant's copying of plaintiff's trade secrets was "damage"
  - First reason: by glossing "integrity"
    - Do you buy it?
  - Second reason: by analogy to the Senate Report, where there was also no change to the data
    - Or was there?

Damage: *DoubleClick*

- Remember those cookies?

(for your reference)



Damage: *DoubleClick*

- Remember those cookies?
- DoubleClick doesn't dispute "access," "unauthorized," or "protected computer"
  - Could it have?
- Instead, it convinces the court that "damage or loss" can't be aggregated across multiple victims
  - Why, and do you buy it?

Damage: *Shurgard* and *DoubleClick*

- Do *Shurgard* and *DoubleClick* provide consistent guidance?
- After Mrs. Bluebeard looks in the ClosedDoor folder, Mr. Bluebeard spends $7,500 for a security consultant who provides a report on what she did, and then secures the folder with a password
- "Damage or loss" according to *Shurgard*? To *DoubleClick*?

CFAA wrap-up

- The statute is almost painfully dense
    - The original version was ingenious, but also a little early and a little ambiguous
    - The revised version is a dog’s breakfast
- Don’t forget:
    - The casebook’s version is out-of-date
    - There are state statutes on point, too

Botnets, viruses, and cyberwarfare

Cyber-attack on Estonia

- The article is a little overhyped, but some elements of it are very real:
  - Organized crime uses viruses and worms to capture home computers
  - Which then become part of botnets
  - Which are for rent to spammers, etc.
  - Or can be used for distributed denial-of-service attacks

What do we do about botnets?

- I don’t know
- CFAA-style statutes are one tactic, but they have some limits, which should sound familiar:
  - Jurisdiction
  - Intermediary responsibility
  - Anonymity
- Cybersecurity is a difficult problem

Next times

Thursday: (Common-law anti-intrusion law)

Next Tuesday: Contractual limits on computer use