ECE 498KL: eCrime and Internet Service Abuse

Computer Fraud and Abuse Act

Kirill Levchenko

November 1, 2018

ILLINOIS
Electrical & Computer Engineering
COLLEGE OF ENGINEERING

Reading

- **18 U.S. Code § 1030 —**
  Fraud and related activity in connection with computers
- Amended by Computer Fraud and Abuse Act (CFAA)
- Main law used to prosecute “hacking”
- Derives authority from Commerce Clause of US Const.
  - “The Congress shall have Power … To regulate Commerce with foreign Nations, and among the several States …”

Reading Questions

- What kind of computer access does the CFAA prohibit?
- Which computers are protected by the CFAA?
- What other acts does the CFAA prohibit?

18 US Code § 1030

- **18 US Code § 1030(a) describes offenses**
- 18 US Code § 1030(c) describes punishments
- **18 US Code § 1030(e) defines key terms**
- 18 US Code § 1030(g) provides civil cause of action

18 US Code § 1030(a)(1)

- Whoever—
  - having *knowingly* accessed a computer without authorization or exceeding authorized access,
  - and by means of such conduct having obtained information
  - that has been determined … to require protection against unauthorized disclosure for reasons of **national defense** or **foreign relations …**
  - willfully communicates … to any person not entitled to receive it
- *Prohibits accessing a computer to commit espionage*

Definitions

18 US Code § 1030(e)

- (1) **Computer:** an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

Definitions

18 US Code § 1030(e)

- (6) **Exceeds authorized access:** 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

Intent in CFAA

- Violations require willful intent
  - Acts must be committed “knowingly” or “intentionally”

18 US Code § 1030(a)(2)

- Whoever—
  - *intentionally* accesses a computer without authorization or exceeds authorized access, and thereby obtains—
    - (A) information contained in a financial record of a financial institution …
    - (B) information from any department or agency of the United States; or
    - (C) information from any protected computer ~~if the conduct involved an interstate or foreign communication~~ (2008 amendment)

- *Most general prohibition on unauthorized access*

Definitions

18 US Code § 1030(e)

- (2) **Protected computer:** a computer —
  - exclusively for the use of a financial institution or the US Government; or, in the case of a computer not exclusively for such use, used by or for a financial institution or the US Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
  - which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the US that is used in a manner that affects interstate or foreign commerce or communication of the US

18 US Code § 1030(a)(3)

- Whoever—
  - *intentionally*, without authorization to access any nonpublic computer of a department or agency of the United States,
  - accesses such a computer …
  - that … is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States
- *Prohibits unauthorized access to Government computer*

18 US Code § 1030(a)(4)

- Whoever—
  - knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access,
  - and by means of such conduct furthers the intended fraud and obtains anything of value,
  - unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
- *Prohibits fraud involving unauthorized access*

18 US Code § 1030(a)(5)

- Whoever—
  - (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, **recklessly causes damage**; or
  - (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, **causes damage and loss.**
- *Prohibits damage, including by means of malware*

Definitions

18 US Code § 1030(e)

- (8) **Damage:** any impairment to the integrity or availability of data, a program, a system, or information;

US v. Morris

- First case brought under the CFAA
- Convicted of violating 18 US Code 1030(a)(5)(A) by District Court for the Northern District of New York (May 1990)
- Morris was sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision.
- Appealed to Second Circuit Court of Appeals (March 1991)

18 US Code § 1030(a)(5)

(1986)

(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby—

(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

18 US Code § 1030(a)(5)(C) (today): Whoever—
intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

US v. Morris

In the fall of 1988, Morris was a first-year graduate student in Cornell University's computer science Ph.D. program. Through undergraduate work at Harvard and in various jobs he had acquired significant computer experience and expertise. When Morris entered Cornell, he was given an account on the computer at the Computer Science Division. This account gave him explicit authorization to use computers at Cornell. Morris engaged in various discussions with fellow graduate students about the security of computer networks and his ability to penetrate it.

US v. Morris

In October 1988, Morris began work on a computer program, later known as the INTERNET “worm” or “virus.” The goal of this program was to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered. The tactic he selected was release of a worm into network computers. Morris designed the program to spread across a national network of computers after being inserted at one computer location connected to the network. Morris released the worm into INTERNET, which is a group of national networks that connect university, governmental, and military computers around the country. The network permits communication and transfer of information between computers on the network.

Morris identified four ways in which the worm could break into computers on the network:

(1) through a “hole” or “bug” (an error) in SEND MAIL, a computer program that transfers and receives electronic mail on a computer;

(2) through a bug in the “finger demon” program, a program that permits a person to obtain limited information about the users of another computer;

(3) through the “trusted hosts” feature, which permits a user with certain privileges on one computer to have equivalent privileges on another computer without using a password; and

(4) through a program of password guessing, whereby various combinations of letters are tried out in rapid sequence in the hope that one will be an authorized user's password, which is entered to permit whatever level of activity that user is authorized to perform.

On November 2, 1988, Morris released the worm from a computer at the Massachusetts Institute of Technology. MIT was selected to disguise the fact that the worm came from Morris at Cornell. Morris soon discovered that the worm was replicating and reinfecting machines at a much faster rate than he had anticipated. Ultimately, many machines at locations around the country either crashed or became "catatonic." When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent reinfection. However, because the network route was clogged, this message did not get through until it was too late. Computers were affected at numerous installations, including leading universities, military sites, and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000.

US v. Morris

18 US Code § 1030(a)(5) (1986)

(5) *intentionally accesses* a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or *prevents authorized use* of any such computer or information, and thereby

(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period;

Morris argues that the Government had to prove not only that he intended the unauthorized access of a federal interest computer, but also that he intended to prevent others from using it, and thus cause a loss. The adverb "intentionally," he contends, modifies both verb phrases of the section. The Government urges that since punctuation sets the "accesses" phrase off from the subsequent "damages" phrase, the provision unambiguously shows that "intentionally" modifies only "accesses."

US v. Morris

18 US Code § 1030(a)(5) (1986)

(5) *intentionally accesses* a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or *prevents authorized use* of any such computer or information, and thereby

(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period;

Morris contends that his conduct constituted, at most, "exceeding authorized access" rather than the "unauthorized access" that the subsection punishes.

…

Morris was authorized to communicate with other computers on the network to send electronic mail (SEND MAIL), and to find out certain information about the users of other computers (finger demon). *The question is whether Morris's transmission of his worm constituted* ***exceeding authorized access*** *or* ***accessing without authorization.***

US v. Morris

- Second Circuit ruled against Morris
  - Legislative history suggests Congress intended that only unauthorized access need be intentional to be in violation of 18 US Code § 1030(a)(5) (1986)
  - "Morris's conduct here falls well within the area of unauthorized access. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers."
- **Precedent:** intent to cause damage not required for violation
- **Precedent:** "intended function test" for unauthorized access
- **Legacy:** Congress clarified statute

18 US Code § 1030(a)(1–5)

§	COMP. CATEGORY	ACCESS	AND —
(a)(1)	ANY	UNAUTH or EXAUTH	obtains and communicates national sec. information
(a)(2)	ANY	UNAUTH or EXAUTH	obtains information: (A) financial, (B) gov't,(C) from prot. computer
(a)(3)	nonpub. gov't	UNAUTH	—
(a)(4)	prot.	UNAUTH or EXAUTH	obtains something of value in attempt to defraud
(a)(5)(B)	prot.	UNAUTH or EXAUTH	recklessly causes damage
(a)(5)(C)	prot.	UNAUTH or EXAUTH	causes damage or loss

18 US Code § 1030(a)(5)

- Whoever—
  - (A) knowingly causes the ***transmission*** *of a program, information, code, or command*, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

- *Prohibits unauthorized damage by transmitting malware*

US v. Drew

- **Lori Drew:** adult mother of teenage daughter Sarah
- **Megan Meier:** 13-year-old classmate of Sarah
- Lori and Sarah Drew:
  - Created MySpace profile for fictitious 16-year-old “Josh Evans”
    - Posted photograph of a boy without his knowledge or consent
  - Contacted Megan as “Josh Evans” and began to flirt with her
  - About a month in “Josh” tells Megan that he no longer liked her and that “the world would be a better place without her in it.”
- Megan Meier committed suicide shortly after

US v. Drew

- Lori Drew charged under 18 US Code § 1030(a)(2)(C)
  - (a) Whoever—

    …
  - (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains –

    …
  - (C) information from any protected computer if the conduct involved an interstate or foreign communication

US v. Drew

- Drew violated MySpace Terms of Service
  - Prohibits harassment and using photo without permission
- Drew obtained information from MySpace site
  - Loading a Web page is obtaining information
- MySpace servers are protected computers
  - Any computer on the Internet “is used in or affecting interstate or foreign commerce or communication”

US v. Drew

- Does using a site in a way prohibited by a site's Terms of Service constitute *unauthorized access* or *access exceeding authorization*?
- **Yes:** ToS clearly spells out authorized uses
- **No:** CFAA would criminalize civil breach of contract

US v. Drew

As discussed in Section IV(A) above, terms of service which are incorporated into a browsewrap or clickwrap agreement can, like any other type of contract, define the limits of authorized access as to a website and its concomitant computer/server(s). However, the question is whether individuals of "common intelligence" are on notice that a breach of a terms of service contract can become a crime under the CFAA. Arguably, they are not.

- Jury found Drew guilty of misdemeanor violation of 18 US Code § 1030(a)(2)(C)
- Defense argued that law was too vague
- Judge dismissed verdict

Third, by utilizing violations of the terms of service as the basis for the section 1030(a)(2)(C) crime, that approach makes the website owner - in essence - the party who ultimately defines the criminal conduct. This will lead to further vagueness

ToS as Authorization

- Courts ambivalent about violation of ToS defining auth. access
- Terms of Service spell out exactly what owner authorizes
  - "Most courts have held that a conscious violation of a website's terms of service/use will render the access unauthorized and/or cause it to exceed authorization." (*US v. Drew*, C.D. Ca. 2009)
- But allowing ToS to define what is criminal conduct is problematic
  - "It is unlikely that Congress, given its concern 'about the appropriate scope of Federal jurisdiction' in the area of computer crime, intended essentially to criminalize state-law breaches of contract." (*Brett Senior & Associates v. Fitzgerald*, E.D. Pa. 2007)

US v. Auernheimer

AT&T decided to make it easier for customers to log into their accounts by prepopulating the user ID field on the login screen with their email addresses.
…
If AT&T's servers recognized the ICC–ID as associated with a customer who had registered her account with AT&T, then AT&T's servers would automatically redirect the customer's browser away from the general login URL to a different, specific URL. That new specific URL was unique for every customer and contained the customer's ICC–ID in the URL itself. Redirecting the customer's browser to the new specific URL told AT&T's servers which email address to populate in the user ID field on the login page. This shortcut reduced the amount of time it took a customer to log into her account because, with her user ID already populated, she had to enter only her password.

US v. Auernheimer

Spitler then directed his computer's web browser to the registration URL and inserted his iPad's ICC–ID in the requisite place. AT&T's servers were programmed only to permit browsers that self-identified as iPad browsers to access the registration URL. This required him to change his browser's user agent. A user agent tells a website what kind of browser and operating system a user is running, so servers that someone is attempting to access can format their responses appropriately.

After changing his browser's user agent to appear as an iPad, Spitler was able to access the AT&T login page. He noticed that his email address was already populated in the login field and surmised that AT&T's servers had tied his email address to his ICC–ID. He tested this theory by changing the ICC–ID in the URL by one digit and discovered that doing so returned a different email address. He changed the ICC–ID in the URL manually a few more times, and each time the server returned other email addresses in the login field.

US v. Auernheimer

Spitler shared this discovery with Auernheimer, whom he knew through Internet-based chat rooms but had never met in person. Auernheimer helped him to refine his account slurper program, and the program ultimately collected 114,000 email addresses between June 5 and June 8, 2010.

…

While Spitler's program was still collecting email addresses, Auernheimer emailed various members of the media in order to publicize the pair's exploits. Some of those media members emailed AT&T, which immediately fixed the breach. One of the media members contacted by Auernheimer was Ryan Tate, a reporter at Gawker, a news website. Tate expressed interest in publishing Auernheimer's story. To lend credibility to it, Auernheimer shared the list of email addresses with him. Tate published a story on June 9, 2010 describing AT&T's security flaw, entitled "Apple's Worst Security Breach: 114,000 iPad Owners Exposed." The article mentioned some of the names of those whose email addresses were obtained, but published only redacted images of a few email addresses and ICC–IDs.

US v. Auernheimer

- Auernheimer (a.k.a. weev) charged in N.J. District Court with conspiracy to violate the CFAA, 18 US Code § 1030(a)(2)(C)
  - Whoever—
    intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
    information from any protected computer if the conduct involved an interstate or foreign communication
- Auernheimer "[changed] the ICC–ID in the URL by one digit" to access Web pages prepopulated with other users' email addresses

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Crim. No. 11-470 (SDW)
	:	
v.	:	Hon. Susan D. Wigenton
	:	
ANDREW AUERNHEIMER	:	VERDICT

We, the Jury find:

COUNT 1
(Conspiracy to Access Computers without Authorization)

GUILTY ✓ NOT GUILTY _____

COUNT 2
(Identity Theft)

GUILTY ✓ NOT GUILTY _____

US v. Auernheimer

- Aurnheimer appealed to 3rd Circuit Court of Appeals
  - Argued New Jersey not the right venue (among other arguments)
  - Neither AT&T servers nor Aurnheimer were in New Jersey
- "Because we conclude that venue did not lie in New Jersey, we will reverse the District Court's venue determination and vacate Auernheimer's conviction."

18 US Code § 1030(a)(6)

- Whoever—
  - knowingly and with intent to defraud *traffics in any password* or similar information through which a computer may be accessed without authorization, if—
  - (A) such trafficking affects interstate or foreign commerce; or
  - (B) such computer is used by or for the Government of the United States
- *Prohibits trafficking in passwords*

18 US Code § 1030(a)(7)

- Whoever—
  - with *intent to extort* from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—
  - (A) threat to cause damage to a protected computer;
  - (B) threat to obtain information from a protected computer without authorization or in excess of authorization …
  - (C) demand or request for money or other thing of value in relation to damage to a protected computer …
- *Prohibits extortion involving unauthorized access*

18 US Code § 1030(g)

- Any person who suffers damage or loss by reason of a violation of this section may maintain a *civil action against the violator* to obtain compensatory damages and injunctive relief or other equitable relief.
- A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors …