Legal Tactics in Cybersecurity Research

Andy Sellars
BU/MIT Technology Law Clinic
Boston University School of Law

- sites.bu.edu/techlaw
- techlaw@bu.edu
- sellars@{bu.edu, mit.edu}
Hacking the Xbox

More Idiotic Tricks

Monetize without ads.

DEFCON 16

The Anatomy of a Subway Hack:

there is almost always a free way to get in
what this talk is not:
evidence in court (hopefully)
The Computer Fraud and Abuse Act

Roots of the CFAA

1. Sitting in front of his home computer console, a teenage boy feverishly types in password after password in an attempt to access the mystery computer he has stumbled upon. Although he is somewhat discouraged by his vain attempts to solve this particular Rubik's cube, he finally cracks the code and he is "in." Like a kid in a candy store, he excitedly applies his small amount of knowledge of computers obtained through a summer course and "browses" through the system. After a thorough look, he hangs up the phone, finishes his algebra homework, and goes to bed, satisfied with his computer safe cracking achievement.

2. Does this sound like a scene from the popular movie, War Games? As impossible as it seems, our mental image of the computer "hacker" (so-named for the ability to hack-up computer systems) is not so far from reality, but not as glamorous as it looks. Hacking should be recognized as nothing more than what it really is—breaking and entering, invasion of privacy, and in some cases, theft and destruction of property. It should also show why there is a need for government regulation of home computers.
**The CFAA Today**

18 U.S.C. § 1030(a)

1. access a computer without authorization or exceeding authorized access, and obtain classified or atomic energy information, with reason to believe that information could be used to injure the United States
2. access a computer without authorization or exceeding authorized access, and obtain "information from any protected computer"
3. access without authorization any nonpublic computer of an agency of the United States government
4. with intent to defraud, access a computer without authorization or exceeding authorized access, and by doing so further the intended fraud and obtain a thing of value

**The CFAA Today**

18 U.S.C. § 1030(a)

5. (A) knowingly cause transmission of a program, and intentionally cause damage
   (B) intentionally access computer without authorization, and as a result, recklessly cause damage
   (C) intentionally access a computer without authorization, and as a result cause damage and loss
6. trafficking in passwords through which a computer may be accessed without authorization
7. with an intent to extort, transmit a threat to cause damage to a computer or obtain information from a computer without authorization

**The CFAA Today**

Putting them together

1. the “espionage, but with computers” one
2. the “obtaining information” one
3. the access to nonpublic fed. computers one
4. the “fraud, but with computers” one
5. the three “damage” crimes
6. password trafficking
7. the “extortion, but with computers” one

**The CFAA Today**

Putting them together

1. the “espionage, but with computers” one
2. the “obtaining information” one
3. the access to nonpublic fed. computers one
4. the “fraud, but with computers” one
5. the three “damage” crimes
6. password trafficking
7. the “extortion, but with computers” one
CFAA Claims

§ 1030(a)(4)  
"exceeds authorized access"

§ 1030(a)(2)  
"without authorization"

§ 1030(a)(5)(B)  
computer damage

§ 1030(a)(5)(C)  
computer damage

§ 1030(a)(5)(A)  
computer damage

The 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 accessor is not entitled so to obtain or alter;
(e) As used in this section —

(6) the 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;

Van Buren’s account of “so”—namely, that “so” references the previously stated “manner or circumstance” in the text of §1030(e)(6) itself—is more plausible than the Government’s. “So” is not a free-floating term that provides a hook for any limitation stated anywhere. It refers to a stated, identifiable proposition from the “preceding” text; indeed, “so” typically “[r]epresent[s]” a “word or phrase already employed,” thereby avoiding the need for repetition. 15 Oxford English Dictionary, at 887; see Webster’s Third New International Dictionary 2160 (1986) (so “often used as a substitute . . . to express the idea of a preceding phrase”). Myriad
Van Buren’s account of subsection (a)(2) makes sense of the statutory structure because it treats the “without authorization” and “exceeds authorized access” clauses consistently. Under Van Buren’s reading, liability under both clauses stems from a gate-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system. And reading both clauses to adopt a gate-up-or-down approach aligns with the computer-context understanding of access as entry. See supra, at 11–12.

Van Buren’s account of subsection (a)(2) makes sense of the statutory structure because it treats the “without authorization” and “exceeds authorized access” clauses consistently. Under Van Buren’s reading, liability under both clauses stems from a gate-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system. And reading both clauses to adopt a gate-up-or-down approach aligns with the computer-context understanding of access as entry. See supra, at 11–12.

That reading, moreover, is perfectly consistent with the way that an “appropriately informed” speaker of the language would understand the meaning of “exceeds authorized access.” Nelson, What Is Textualism? 91 Va. L. Rev. 347, 354 (2005). When interpreting statutes, courts take note of terms that carry “technical meaning[s].” A. Scalia & B. Garner, Reading Law: The Interpretation of Legal Texts 73 (2012). “Access” is one such term, long carrying a “well established” meaning in the “computational sense”—a meaning that matters when interpreting a statute about computers. American Heritage Dictionary 10 (3d ed. 1992). In the computing context, “access” references the act of entering a computer “system itself” or a particular “part of a computer system,” such as files, folders, or databases. It is thus consistent with that meaning to equate “exceed[ing] authorized access” with the act of entering a part of the system to which a computer user lacks access privileges. The Government and the dissent’s broader interpretation is neither the only possible nor even necessarily the most natural one.
For present purposes, we need not address whether this inquiry turns only on technological (or “code-based”) limitations on access, or instead also looks to limits contained in contracts or policies. Cf. Brief for Orin Kerr as Amicus Curiae 7 (urging adoption of code-based approach).

The 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;

Per Van Buren v. United States (2021)...
• “so” in “not entitled so to obtain” means “in the same manner”
• should be geared towards “inside hackers” as a “gates-up-or-down” inquiry
• and when Congress uses technical words courts should give them their technical meanings
• but SCOTUS is not saying this has to be “code based,” at least for now.

“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;”

• “so” is “in the same manner”
• should be a “gates-up-or-down” inquiry
• when Congress uses technical words courts should give them their technical meanings
• but SCOTUS is not saying this has to be “code based,” at least for now.

“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;”

• “so” is “in the same manner”
• should be a “gates-up-or-down” inquiry
• when Congress uses technical words courts should give them their technical meanings
• but SCOTUS is not saying this has to be “code based,” at least for now.
"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"

- "so" is "in the same manner"
- should be a "gates-up-or-down" inquiry
- when Congress uses technical words courts should give them their technical meanings
- but SCOTUS is not saying this has to be "code based," at least for now.
“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”

- “so” is “in the same manner”
- should be a “gates-up-or-down” inquiry
- when Congress uses technical words courts should give them their technical meanings
- but SCOTUS is not saying this has to be “code based,” at least for now.

The company that makes it sent more than $9 million of these crime predictions to law enforcement agencies across the country—from California to Florida, Texas to New Jersey—and we found those reports on an unsecured server.

The evidence permitted the jury to conclude that Morris’s use of the SEND MAIL and finger demon features constituted access without authorization. While a case might arise where the use of SEND MAIL or finger demon falls within a nebulous area in which the line between accessing without authorization and exceeding authorized access may not be clear, Morris’s conduct here falls well within the area of unauthorized access. Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both

“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”

- “so” is “in the same manner”
- should be a “gates-up-or-down” inquiry
- when Congress uses technical words courts should give them their technical meanings
- but SCOTUS is not saying this has to be “code based,” at least for now.
CFAA Claims

§1030(a)(4) Computer fraud

Per Van Buren v. United States (2021)
- "so" in "not entitled so to obtain" means "in the same manner"
- should be geared towards "inside hackers" as a "gates-up-or-down" inquiry
- and when Congress uses technical words courts should give them their technical meanings
- but SCOTUS is not saying this has to be "code based," at least for now.

(a) Whoever--

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains [...] (C) information from any protected computer

(4) 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 [not counting use of the computer, if that use is not worth more than $5000]

(5) (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;

(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

shall be punished as provided [...]

Instacart

http://instacart.com

Security Vulnerability Disclosure Program

Overview

Vulnerability Reporting

Systems or services which are not owned or maintained by Instacart, such as third-party blogs or micro-sites, are not eligible, and we can’t give you permission to test against. These include (but not limited to):

* brands.instacart.com
* careers.instacart.com and www.careers.instacart.com
* commbiners.instacart.com and www.commbiners.instacart.com
* corporate.instacart.com
* covidresponsee.instacart.com
Disclosure Policy

- As this is a private program, please do not discuss this program or any vulnerabilities (even resolved ones) outside of the program without express consent from the organization.
- Follow HackerOne’s disclosure guidelines.
(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 set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. […]

(c) The punishment for an offense under subsection (a) or (b) of this section is—
(4)(A) [with some exceptions,] a fine under this title, imprisonment for not more than 5 years, or both, in the case of—
(i) an offense under subsection (a)(5)(B), [if a first offense,] if the offense caused [or would have caused]—
(I) loss to 1 or more persons during any 1-year period [and for criminal cases, loss affecting 1 or more protected computers] aggregating at least $5,000 in value;
(II) impairment or modification of medical technologies
(III) physical injury to any person;
(IV) a threat to public health or safety;
(V) government computers used in administration of justice, national defense, or national security]
The Anatomy of a Subway Hack: Selecting Crypto RFID’s and Magstripes of Ticketing Systems
Zach Anderson, Student, MIT
BJ Ryan, Student, MIT
Alessandro Chiesa, Student, MIT

We'll take subway rides for $1 in this talk, we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and share how we reverse engineered the data on magnetic cards, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in every subway around the world, and we discuss physical security problems. We will discuss practical brute-force attacks using FPGA and how to use software radios to read RFID cards. We go over social engineering attacks we executed on employees, and we present a novel new method of hacking WiFi: WACKCASTING. We will release several open source tools we wrote to perform these attacks. With live demos, we will demonstrate how we broke these systems.

THE COURT: Just a moment. They may think that that was cute at the time that they drafted that up but that's what they undertook to do and they have to accept the consequences of that because as far as I'm concerned if someone does end up doing this, they are aiding and abetting, yet, they have undertaken to provide this information.

THE COURT: I haven't made judgment. It's not before me. I'm making a set of observations which inform my judgment about whether or not somebody else has to exercise some supervision over these kids.

approach. Sometimes we can’t expect people in their early 20’s to have sufficient judgment or experience to avoid causing those clashes of interest between something as broad and as important as the First Amendment and the need to avoid actual criminal conduct of which words are the constituent elements.
More on April 8!

- sites.bu.edu/techlaw
- techlaw@bu.edu
- sellars@{bu.edu, mit.edu}

- “Code as speech” and First Amendment overlays with source code
  [Leah Gervin]
- Reverse engineering and “anticircumvention” laws
  [Anastassia Korin]

- sites.bu.edu/techlaw
- techlaw@bu.edu
- sellars@{bu.edu, mit.edu}