April 18, 2005 -- Lecture 34

22C:169
Computer Security

Douglas W. Jones

Department of Computer Science

Some Laws

Computer Fraud and Abuse Act

As amended Oct 3, 1996

Section 1030. Fraud and related activity in connection with computers

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

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

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(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;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, 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;

(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, 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;

(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;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

Computer Fraud and Abuse Act

Whoever knowingly

Accessed a computer and
Exceeding authorized access and
Obtains information from
government or
financial records of a bank or
a protected computer
(BUT ONLY IF IN INTERSTATE COMMERCE)
And by means of such conduct
furthers intention to defraud and
obtains anything of value
(UNLESS THE OBJECT OF FRAUD IS MERE USE OF COMPUTER RESOURCES WITH VALUE UNDER $5000)

Or whoever intentionally

Accesses a protected computer
Causing damage

Or whoever knowingly

With intent to defraud
Traffics in passwords or equivalent

Or whoever with intent to extort

Transmits threat to damage computers

Is subject to a five year prison sentence

CALEA

Communications Assistance for Law Enforcement Act of 1994

Telecommunications carrier

- excepting information services
- excepting private networks

Must expeditiously enable government

(WITH A COURT ORDER OR OTHER LAWFUL AUTHORIZATION)

- *To intercept traffic of specific subscriber*
- *To monitor call identifying information*
- *To access above remotely and securely*
- *To access above covertly*

CALEA Comments

The borderline is vague between

- *Information Provider*
- *Private Network*
- *Telecommunication Carrier*

Opponents to this act included most

- Telecommunications carriers
- Civil liberties groups

Proponents were

- *"Spooks" and law enforcement agencies*

Digital Millenium Copyright Act of 1998

Criminalizes

- *Circumvention of anti-piracy measures*
- *Manufacture or sale of cracking devices*
  - (EXCEPTION FOR EDUCATION, RESEARCH AND TESTING)

Limits liability of ISPs, prividing they

- *promptly remove infringing material*

Requires webcasts to pay licensing fees

Preserves fair use doctrine

Abuse of DMCA

Online Policy Group versus Diebold

Internal corporate memo leak from Diebold

Spring-summer 2003

Directly touched on issues of public policy

Students at many universities posted memos

Diebold forced take-down under DMCA

Described as game of Whack-a-Mole

Court eventually decided in favor of students

But deterrent value of DMCA is high

even if such use is ultimately illegal!