CAS CS 357

Class Note 1

1. CFAA- Computer Fraud and Abuse Act 1985
2. Intentionally access a computer without authorization or exceeds authorized access- and thereby obtain
3. Information contained in a financial record of a financial institution or contained in a file of a consumer reporting agency on a consumer
4. Information from any department or agency of US
5. Information from any protected computer
6. Protected computer under the CFAA
   1. 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
   2. 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 US, or that
   3. Is part of a voting system and is used for the management, support, or administration of a Federal election; or has moved in or otherwise affects interstate or foreign commerce
7. Exceeds Authorized Access
8. The term “exceeds authorized access” means to access a computer with authorization to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter
9. Civil Action
10. 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 damage 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 above
11. Damage for a violation involving only the conduct are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware
12. Criminal action
13. A fine under the title or imprisonment for not more than 5 years in the case of an offense or attempt to commit an offense punishable under the subparagraph if the offense was committed for the purpose of commercial advantage or private financial gain, the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the US or of any State or the value of the information exceeds obtained exceeds $5000
14. Things are changing
15. The *Van Buren* decision is especially good news for security researchers, whose work discovering security vulnerabilities is vital to the public interest but often requires accessing computers in ways that contravene terms of service. Under the Department of Justice’s reading of the law, the CFAA allowed criminal charges against individuals for any website terms of service violation. But a majority of the Supreme Court rejected the DOJ’s interpretation. And although the high court did not narrow the CFAA as much as EFF would have liked, leaving open the question of whether the law requires circumvention of a technological access barrier, it provided good language that should help protect researchers, investigative journalists, and others.
16. The Supreme Court rightly overturned the Eleventh Circuit, and held that exceeding authorized access under the CFAA does not encompass “violations of circumstance-based access restrictions on employers’ computers.” Rather, the statute’s prohibition is limited to someone who “accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him.” The Court adopted a “gates-up-or-down” approach: either you are entitled to access the information or you are not. If you need to break through a digital gate to get in, entry is a crime, but if you are allowed through an open gateway, it’s not a crime to be inside.
17. This means that private parties’ terms of service limitations on how you can use information, or for what purposes you can access it, are not criminally enforced by the CFAA. For example, if you can look at housing ads as a user, it is not a hacking crime to pull them for your bias-in-housing research project, even if the TOS forbids it. *Van Buren* is really good news for port scanning, for example: so long as the computer is open to the public, you don’t have to worry about the conditions for use to scan the port.
18. Jan 2022- In addition to robust internal testing programs, agencies should scrutinize their applications as our nation’s adversaries do. This requires welcoming external partners and independent perspectives to evaluate the real-world security of agency applications, and a process for coordinated disclosure of vulnerabilities by the general public

Powerpoint – Responsible disclosure

1. History
2. 1. 18th C. -Vulnerabilities in locks and safes
   * 1. “Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks offers a premium for dishonesty, by showing others how to be dishonest. This is a fallacy. Rogues are very keen in their profession, and know already much more than we can teach them respecting their several kinds of roguery.” - A. C. Hobbs, Boston, Ma, 1853
     2. Non-disclosure is the belief that the public should not be told of vulnerabilities.
     3. Non-Disclosure became standard practice in the locksmithing world to this day, but it is changing.
3. 1990’s -No one fixes vulnerabilities
4. “Before full disclosure was the norm, researchers would discover vulnerabilities in software and send details to the software companies -- who would ignore them, [..]
5. Later on, researchers announced that particular vulnerabilities existed, but did not publish details. Software companies would then call the vulnerabilities "theoretical" and deny that they actually existed.
6. Then, of course, some hacker would create an exploit using the vulnerability -- and the company would release a really quick patch, apologize profusely, and then go on to explain that the whole thing was entirely the fault of the evil, vile hackers” Bruce Schneier
7. Later - Full Disclosure: Wysopal/L0pht
8. Publishing vulnerabilities immediately to the public without restriction. - “Vendors have no economic incentive otherwise.” - Shortens time to patch gives attacks less time
9. 2004 - Responsible Disclosure: Wysopal/OIS
10. “Guidelines for Security Vulnerability Reporting and Response” 2004
11. Full Disclosure with a mitigation period.
12. Tell the vendor before the public, let them issue a mitigation before releasing. If they fail to release a patch within a responsable time then publicly disclose the vulnerability to protect the public (but talk to a lawyer first).
13. Present - Age of Bug Bounties
14. Many Companies care about security, encourage researchers to find vulnerabilities as long as the company gets a responsible time period to fix the issue (6 months for Google).
15. Companies publish responsible disclosure Policies.
16. Some will even pay you a bounty if find a vulnerability.
17. Some companies will still sue researchers vulnerability discovery (read their policies carefully)
18. Important
19. To defend a system, you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law or the university's rules, and it may be unethical. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time.