### “12 Possible Attack Vectors”

Critical Challenge Project Title : "Downjacking" | Analog and Digital Attacks That May Circumvent the CFAA

EMCS 2020, Cohort 3, CCP Research Notes

Timothy Edgar, Advisor

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

#### Overview

The CFAA requires that a “computer” be involved in interstate commerce to be protected under federal law. Many of the attacks list below may be exempt from this law because:

1. The device is not involved in any type of commerce at all, like a transit kiosk.
2. There is no device and there is no need for hacking, but there is storage of PII on a publicly displayed piece of media ( like a badge )
3. The target voluntarily gives ( or leaves behind ) their PII without the need for hacking, so there is no illegal action.
4. The target interacts with a compromised device that is not a protected computer ( like a car’s computer system )
5. The target buys a compromised device second hand “as-is”
6. The target system contains “features” that offer up PII without the need for hacking.
7. The attacker decompiles an application, modifies it, and uses valid credentials to access the system, but removes security, from the compromised application.

Items with a ~~strikethrough~~ have been counted out as an attack because they are prosecutable under the CFAA.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Attack Title** | **Target of Attack** | **Brief Description** | **Possible Damage/Loss** | **How it circumvents current law** | **Examples of attacks in the wild?** |
| “Smile for the BiRDy” | Corporate access credentials | People often wear their badges in public places exposing their full name, photo, company name and sometimes their badge insecurely broadcasts their credentials via NFC. . . The attacker reads the information when they are in close proximity, while on a train for example. | Impersonation, Breach of corporate systems, state-sponsored surveillance | **CFAA**  Since the victims are wearing their RFID badges in public, and it could be said they are broadcasting their information, there is no unauthorized access. [DA NOTE: THIS JUST MEANS THAT A DIFFERENT CRIME OCCURS IF THE CREDENTIALS ARE STOLEN AND USED. AND, IF THE STOLEN CREDENTIALS ARE USED TO ACCESS A PROTECTED COMPUTER WITHOUT AUTHORIZATION, THEN THERE CAN BE CFAA AND WIRE FRAUD] |  |
| “Soul Stealing Train” | Transit Kiosk Systems | Most Amtrak Kiosk run on Windows XP. I know this because 50% the time OS on the Kiosk encounters a fatal and exposes the network domain login to anyone walking by. Each time the Kiosk “breaks” it broadcasts sensitive domain controller information that can be sold to a nation-state or bad actor. | Breach of corporate systems, state-sponsored surveillance | **CFAA**  Since the system is exposing and broadcasting sensitive information, a person selling this information to a third party that may have malicious intent may not be prosecutable under the CFAA.[DA NOTE: NOT CLEAR WHOM YOU WOULD PROSECUTE HERE. AND AGAIN, DEPENDING ON THE INFORMATION REVEALED, WHAT IS DONE WITH IT, AND HOW IT IS USED IN FURTHERANCE OF CRIMINAL ACTIVITY, A VARIETY OF CHARGES MAY APPLY]] |  |
| “Guess Who’s Coming to Dinner” | Resold IoT Devices | IoT devices like the Brava Smart Oven, connect to the internet to get firmware updates. A technically savvy attacker could intercept this update request download malicious code and compromise the device firmware. The attacker then resells the device on eBay to a target and is able to see all their personal information over WiFi. | Exposure of personal information, state-sponsored surveillance | **CFAA**  An altered and resold device with a disclosure that it is sold “as-is” from a developer that was using it for testing may not be covered by the CFAA.  [DA NOTE: CRIMINAL CHARGES APPLY TO PEOPLE, NOT DEVICES. THE CONDUCT YOU DESCRIBE COULD POTENTIALLY BE PROSECUTED UNDER THE WIRETAP ACT AND/OR AS FRAUD] |  |
| “Stick It To ‘Em” | Corporate advertising using QR codes | An attacker simply places their own sticker over the target company’s public QR code, that redirects to the attacker website. | Exposure of personal information, state-sponsored surveillance | **CFAA**  Altering a display ad may be vandalism but would not be considered a violation of the CFAA.  [DA NOTE: DEPENDING ON HOW THIS IS ACCOMPLISHED, THERE COULD BE A CFAA VIOLATION, EG 1030(a)(4) OR (a)(5). AND THERE ARE OBVIOUS WIRE FRAUD CHARGES AVAILABLE] |  |
| “Call You Right Back” | Automotive HUD | Target connects their phone via Bluetooth to a rental car which downloads all their contacts in the cars memory. Any non-technical attacker can see all of the information from the previous renter. A technically savvy attacker can exploit the connected phone. | Exposure of personal information, Impersonation | **CFAA**  Because the victim left the information behind and exposed it, an attacker would not be prosecutable under the CFAA  [DA NOTE: WHY SHOULD SIMPLY ACCESSING THIS DATA SUBJECT AN INDIVIDUAL TO CRIMINAL PROSECUTION? IF THE INDIVIDUAL MISUSES IT, NON-CFAA CHARGES MAY APPLY. BUT NEGLIGENT CONDUCT BY THE PREVIOUS RENTER SHOULD NOT, ON ITS OWN, SEND SOMEONE TO PRISON, SHOULD IT?]] |  |
| ~~“Alexa Dog Whistle”~~ | ~~Voice Assistant~~ | ~~The attacker broadcasts a command only Alexa can hear that is actually a SQL injection attack.~~ | ~~Exposure of personal information~~ | **~~CFAA~~** |  |
| ~~“Decompile, Clone, Repeat”~~ | ~~Ride Sharing Apps~~ | ~~The attacker is a rideshare driver that de-compiles the target app, logins into a compromised and uncompromised version of the app and logs to steal riders personal information.~~ | ~~Exposure of personal information~~ | **~~CFAA~~** |  |
| “autocomplete-and-tell-me-all-your-secrets” | Visitor Check-In Apps | Some of the more popular visitor check-in app offers autocomplete. By typing random names I can get a complete list of everyone who visited a location, including their name, email address, mailing address and phone number. | Exposure of personal information, Impersonation | **CFAA**  Since the system is showing the PII of previous logins by simply typing, there is no unauthorized access.  [DA NOTE: WHO WOULD YOU BE LOOKING TO PROSECUTE HERE? SHOULD SOMEONE GO TO PRISON FOR THE CONDUCT YOU DESCRIBE? IF THEY MISUSE THE INFORMATION THEN THEY ARE ALREADY SUBJECT TO NON-CFAA LIABILITY]] |  |
| “Will The Real Slim Shady Please Stand Up” | Conference Check-In Systems | Common names like “Brian Davis” are often duplicated at large conference like RSA. I was able to enter my name and see 2 other people with my name, I could have selected their badge, shown my ID and got their level of registration. | Exposure of personal information, Impersonation, Theft | **CFAA**  Since the system is showing the PII of previous logins by simply typing, there is no unauthorized access.  [DA NOTE: SAME POINT; THERE ARE NUMEROUS POTENTIAL VIOLATIONS WITHOUT CHANGING CFAA] |  |
| “PWND-Per-View ” | Hotel Room TVs | The attacker plugs a malicious device to a hotel room TV HDMI input. When the target interacts with the TV they get prompts to connect to the attacker's WiFi or expose personal information. | Exposure of personal information, state-sponsored surveillance | **CFAA**  Since the TV is not being “hacked” the malicious device is simply using the open input port to broadcast the malicious software. If the victim doesn’t realize the display is not from the hotel, the attacker can retrieve sensitive information from the victim without violating the CFAA.  [DA NOTE: SAME POINT; THERE ARE NUMEROUS POTENTIAL VIOLATIONS WITHOUT CHANGING CFAA. POTENTIALLY INTERESTING QUESTION OF WHETHER PHYSICALLY CONNECTING A DEVICE IS “UNAUTHORIZED ACCESS,” BUT UNNECESSARY TO REACH IN REAL WORLD] |  |
| "New Phone, Who Dis?" | Hotel Room Phones | The attacker adds a phone to the hotel room that looks like a phone from the hotel but it has been compromised to record personal information and relay the info to the attacker. | Exposure of personal information, state-sponsored surveillance | **CFAA**  Since the victim doesn’t not check to see if the attackers phone is malicious, and the attacker does not infiltrate any hotel systems, this “attack” would not be covered by the CFAA.  [DA NOTE: SAME POINT; THERE ARE NUMEROUS POTENTIAL VIOLATIONS WITHOUT CHANGING CFAA] |  |
| “We All Live in a PWND Submarine” | Online Corporate Directories | The attacker scrapes a corporate directory and cross-references the list with Social Media to compile a valuable database which is sold to a malicious actor. | Exposure of personal information, state-sponsored surveillance | **CFAA**  Since the system is exposing and broadcasting sensitive information, a person selling this information to a third party that may have malicious intent may not be prosecutable under the CFAA.  [DA NOTE: ARE YOU SUGGESTING THAT IT SHOULD BE A CRIME TO LOOK AT TWO PUBLIC DATASETS?] |  |