UNITED STATES MILITARY ACADEMY

RESEARCH PAPER

CS389: IND STUDY IN COMPUTER SCI 3CR

SECTION Z

LTC BRUCE CHOJNACKI, MAJ ALEXANDER MASTER, DR. RYAN DOUGHERTY

BY

CDT HEAINZ MANOJ '2027, CO D4
CDT IAN CAMPBELL '2026, CO C1
CDT ZACHARY DAHER '2026, CO I1

WEST POINT, NEW YORK

11 DECEMBER 2024

HM IC
ZD I CERTIFY THAT I HAVE COMPLETELY DOCUMENTED ALL SOURCES THAT I USED TO COMPLETE THIS ASSIGNMENT AND THAT I ACKNOWLEDGED ALL ASSISTANCE I RECEIVED IN THE COMPLETION OF THIS ASSIGNMENT.

_____ I CERTIFY THAT I DID NOT USE ANY SOURCES OR RECEIVE ANY ASSISTANCE REQUIRING DOCUMENTATION WHILE COMPLETING THIS ASSIGNMENT.

SIGNATURE: MANOJ.HEAINZ.MARTIN.1623698080 Digitally signed by MANOJ.HEAINZ.MARTIN.1623698080 Date: 2024.12.11 22:26:30 -05'00' DATE: 12/11/2024

SIGNATURE: CAMPBELL.IAN.JOSEPH.1612449615 Digitally signed by CAMPBELL.IAN.JOSEPH.1612449615 Date: 2024.12.11 22:28:50 -05'00' DATE: 12/11/2024

SIGNATURE: DAHER.ZACHARY.RAFIC.1606230199 Digitally signed by DAHER.ZACHARY.RAFIC.1606230199 Date: 2024.12.11 22:39:27 -05'00' DATE: 12/11/2024

Digital Force Protection - Vehicle Privacy and Security

RESEARCHERS:
CDT IAN CAMPBELL
CDT ZAC DAHER
CDT HEAINZ MANOJ

ADVISORS:
LTC BRUCE CHOJNACKI
LTC JESSICA DAWSON

Abstract

This research explores what information modern vehicles transmit over the internet that can impact the privacy of service members who drive. To find the information, we connected to the car's on-board Wi-Fi and Bluetooth and then captured data packets using Wireshark's network analyzer. We also used Spectrum Guard Pro, which determines the radio frequencies transmitted in the air. We scanned several cars used at the United States Military Academy but found no indication that the vehicles were transmitting or revealing sensitive data over Wi-Fi or Bluetooth upon analyzing Spectrum Guard Pro and Wireshark results. However, we found that when a vehicle's Wi-Fi is turned on, it sends a Wi-Fi broadcast containing the vehicle's Mac address. Since a Mac address is a unique identifier, it can be used to recognize a vehicle within close proximity. Since the vehicles transmitted nothing of significance over Wi-Fi and Bluetooth to the internet, they may be sending significant data over LTE/Cellular instead, which is the next approach in our research.

Introduction

This research project aims to determine the privacy vulnerabilities associated with military members' personally owned or government vehicles. Congress has enacted significant legislation regarding cell phones and computers to protect user privacy. However, there has been little to no legislation protecting driver's personal information when using an automobile. In car manufacturers' privacy policies, they list data collected on their users, including geolocation, the driver's phone information, driving behavior, and many others.[1] Consumers can easily control privacy settings on devices such as phones and computers and are aware of the privacy risks. However, they have fewer options to control the data sent by their vehicles due to user agreements and are not as aware. This project focused on using specific tools to detect and analyze collected information and to make the vulnerabilities known to the Department of the Army.

Vehicle manufacturers have slowly been integrating more data collection technologies into each new vehicle model released. Vehicle owners are often unaware of the degree of this data collection and are, therefore, unlikely to choose a vehicle based upon its level of privacy. Since vehicles can collect a myriad of information, including potentially sensitive information, this poses a privacy risk to the American people and to operational security in the military. The American public and the military need to move from a "receiver-centric" view of vehicles, to a perspective that accounts for the weaponization of data in cyber-enabled warfare[2].

[1] Chiara Bodei et al. "Vehicle Data Collection: A Privacy Policy Analysis and Comparison."

[2] Dawson, Jessica. "Data as Ammunition: A New Framework for Information Warfare."

Our research objective was to determine what information vehicles are transmitting by collecting network data from government-leased vehicles. This project will use networking and radio frequency tools to detect and determine what information is being collected from vehicles to increase public awareness of privacy vulnerabilities.

Literature Review

It is no secret that companies use technology to collect and sell valuable data on their users. Specifically, vehicle manufacturers have slowly been integrating more data collection technologies into each new vehicle model release. Users have little control over their data privacy, which is an increasing threat to the American public. The American public and the military need to move from a "receiver-centric" view of data to a perspective that accounts for the weaponization of data as cyber-enabled physical warfare[3,4].

The National Institute of Standards and Technology (NIST) defines *privacy* as "the right of a party to maintain control over and confidentiality of information about itself.[5]" However, in the automotive industry, little has been done to protect users' privacy. A wide range of vehicles across the automobile market collect information on the following categories: Personally Identifiable Information, Driver's Phone Information, Offenses and Violations, Vehicle Status, Voice and Messages, Geolocation, Financial, Driver's Behavior, Surrounding vehicle environment, and App Usage[6]. These companies disclose the information they collect in their Privacy Policy; however, these documents can be extensive and challenging to read. To address the data vulnerability in vehicles, we aim to expose the hidden risks that are often overlooked due to misconceptions. Our plan is to explore various methods of data transmission through GSA-contracted vehicles in the government fleet, focusing on individuals who are in key leadership positions, such as LTG Gilland (Supe).

In a recent study, the Controller Area Network (CAN) signals collected included vehicle speed, accelerator pedal position, brake pedal pressure, steering wheel angle, gear position, and engine RPM.[7] These signals were transmitted to the cloud for offline driver identification modeling. A list of driving metrics was developed to quantify driver behaviors. This paper demonstrates the possibility of identifying drivers from their on-road naturalistic driving behaviors with 100% accuracy within 6 minutes of driving by training the case's model with 4 hours of driving data.

---

[3] Dawson, Jessica. "Data as Ammunition: A New Framework for Information Warfare."

[4] U.S. Army. "ADP 3-13 INFORMATION HEADQUARTERS, DEPARTMENT of the ARMY."

[5] Chiara Bodei et al. "Vehicle Data Collection: A Privacy Policy Analysis and Comparison."

[6] Ibid.

[7] SAE International. "Driver Identification Using Vehicle Telematics Data."

One common method of data collection involves an On-Board Diagnostic (OBD) device, a direct connection to the car. In 2015, researchers from the University of British Columbia levied an OBD sensor to collect speed, engine RPM and geo-location from moving cars[8]. Although this research was aimed at developing accident prevention and transportation efficiency, this data collection poses severe surveillance threats if data is not anonymized and connected to a server, which could be accessed by third parties[9]. Further, a research group from the University of Michigan created a data collection app to support hardware based on an OBD connection[10]. This platform acts as a way for researchers to collect information primarily through subsections through an OBD-II port. However, it also contains possibilities for collection through Bluetooth, wired, cellular, and Wi-Fi abstraction layers.

A bad actor with physical access to a vehicle can easily plant an inexpensive and inconspicuous device into the vehicle to let them interact remotely. An article from Offensive Security, one of the most significant companies involved with the offensive aspect of cyber security, released an article in 2022 that detailed in depth how someone can do this with a relatively inexpensive device called a CANtact[11]. The article thoroughly explains and provides the exact code and commands required to control a vehicle by exploiting the CAN bus through the OBD-II (On-Board Diagnostics II) port[12]. This port exposes the internal network traffic between a car's subsystems[13]. However, through the CANtact hardware, one can capture and replay signals into the vehicular network, effectively allowing an attacker to control the car remotely as if they were the driver. They can also collect data on acceleration, speed, brakes, and turns that can be used to build a profile of the driver[14]. This indicates that a car's ODB-II port could be an attack vector for a bad actor. Additionally, an attacker with physical access to a car can potentially take control of the onboard Electronic Control Unit (ECU)[15]. The attacker can fully reprogram the car's systems by gaining access to the ECU. This could include transmitting data from the car's onboard sensors such as microphones, cameras, GPS, and other telemetry

[8] Michael Reininger et al. " A First Look at Vehicle Data Collection via Smartphone Sensors."

[9] Ibid.

[10] Mert D. Pesé et all. "CarLab: Framework for Vehicular Data Collection and Processing."

[11] Offensive Security. "Introduction to Car Hacking: The CAN Bus."

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Karl Koscher, et al. "Experimental Security Analysis of a Modern Automobile."

over the internet to a server of their choosing[16]. This would be especially dangerous if an exploited vehicle was authorized to enter a government or military installation.

As for wireless attack vectors, one study found that strong vectors for wireless attacks against a vehicle include Wi-Fi, Bluetooth, and Cellular Radio, which are not difficult to exploit[17]. One difficulty an attacker may face is that they need to be close to the vehicle while it is on, but this can be mitigated by attaching a relatively inexpensive remote exploitation toolkit magnetically to the car, which may go undetected. Through this, an attacker could begin to work towards exploiting the vehicle's Wi-Fi and Bluetooth capabilities, as well as any other devices that connect to those services. Attackers can also use radio frequency sniffing tools like HackRF to capture and replay frequencies from a vehicle or its accessories[18]. For example, one article goes into depth on how a normal person can use a HackRF to capture and replay the signal from a key fob to remotely unlock a car door[19].

Modern vehicles collect extensive personal data and pose significant privacy and security risks. Information such as driving behavior, location, and personal identifiers, can be exploited due to insufficient protection and public awareness. Adversarial malicious actors can exploit these vulnerabilities through OBD ports, wireless connections like Bluetooth and Wi-Fi, and even remotely control vehicles using inexpensive tools like CANtact. These risks primarily concern military personnel or individuals handling sensitive information. To mitigate this risk, a policy that considers data-enabled physical warfare must be implemented. Stricter regulations, more transparent privacy policies, and stronger security measures are essential to protect military members' data. By doing so, we can ensure that technological advancements in vehicles do not come at the cost of privacy and security.

Research Background

This research continues from the research conducted by a team of ROTC cadets during the summer of 2024, where they tried to collect the data being transmitted from government vehicles over Wi-Fi. The ROTC cadets used Spectrum Guard, which allows the user to determine the radio frequencies a vehicle is transmitting. We also were told that they were able to capture packets over the car's Wi-Fi using a tool called Wireshark, which captures packets sent over a network. They stored these network packets in PCAP (packet capture) files, which we analyzed. After we analyzed their PCAP capture, we discovered

[16] Ibid.

[17] Stephen Checkoway, et al. "Comprehensive Experimental Analyses of Automotive Attack Surfaces."

[18] James A. Chambers. "Use HackRF SDR to Lock / Unlock Car."

[19] Ibid.

that the PCAP files from the cars were not helpful for our research because they had used Windows devices, tainting the network with requests from services like Grammarly.

Additionally, creating a spider map (Figure 1) of their PCAP file revealed a structure similar to a standard enterprise router and not that expected from a vehicle. This meant that the cadets thought they were captured from a vehicle, but instead, it was likely they ran Wireshark while connected to an actual network different from the vehicles. From this, we concluded that this data was unreliable, so we decided to produce our own PCAP files using a reliable methodology.

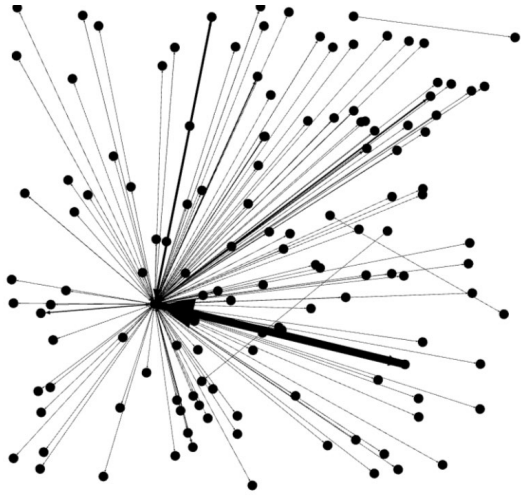

Figure 1: The visualization of the ROTC cadet's PCAP file. A central node communicates with tens of other devices, typical of a router, not a vehicle.

Research Methodology

To determine information on data transmitted from vehicles, we replicated the ROTC cadets' methodology but applied networking knowledge to ensure we did not collect tainted data. To do this, we would first perform an analysis of the frequencies a vehicle emits by using the Spectrum Guard Pro. Spectrum Guard Pro would analyze the frequencies when the car is off, then analyze the frequencies when the car gets turned on, and show the difference, which are the frequencies emitted by the car. This would reveal what frequencies or services the car uses.

To gather networking data, we used Wireshark, a packet sniffer tool, to collect any packets the vehicle sent over Wi-Fi and Bluetooth. If the vehicle were transmitting sensitive data over these services, we would see that. Finally, we also used an on-board diagnostics (OBD) scanner to see what data could be collected through a wired connection.

Figure 2: Our research group utilizes the Spectrum Guard Pro (left) and Wireshark (right) to collect data on a Tesla Model 3.

Data Analysis

Our research group examined several cars from the West Point motor pool. The United States Military Academy Superintendent's Vehicle was the first vehicle from which we collected data. It was a 2020 Ford Explorer with a corresponding vin number of 1FMSK8BH8LGC68547. The OBD scanner provided general information on the vehicle, including tire pressure, oil life, battery status, and transmission fluid temperature. As ODB is not collected over a wireless network connection, the ODB port is not a point of vulnerability without physical access. However, these are data points that we then looked for to understand the vehicle further. After using Wireshark to analyze the 2020 Ford Explorer's on-board Wi-Fi, we found that it broadcast itself on mDNS. mDNS allows devices like Apple to find compatible AirPlay receivers, such as the "Ford Explorer" on the same network. Since this is a local network broadcast and does not attempt to broadcast to the larger internet, this is not a serious privacy vulnerability since it never leaves the car's local Wi-Fi network. No other packets of significance were sent over Wi-Fi or Bluetooth.

The second vehicle we collected data from belongs to the Commandant of the United States Military Academy Preparatory School. It was a 2023 Chrysler Pacifica, with a corresponding vin number of 2C4RC1L70PR513522. The OBD scanner was able to provide the vehicle's battery status. Again, unless an attacker had the physical address to the vehicle, the ODB port is not a privacy vulnerability in and of itself. Unfortunately, since this was one of the first iterations of data collection, poor data handling, and storage resulted in the loss of the Spectrum Guard, and Wireshark captures from this vehicle. However, from our notes, we found that there were no packets sent to the internet when conducting a Wireshark packet capture of the vehicle's on-board Wi-Fi and Bluetooth.

The next vehicle that we collected data from was a Tesla Model 3 from the West Point Department of Public Works with a corresponding VIN number of 5YJ3E1EA5PF401786. This vehicle was interesting because, unlike most vehicles, it had an Ethernet port for on-board diagnostics instead of an ODB port. Plugging in an ethernet capable of entering the vehicle and a laptop caused Tesla to enter diagnostics mode (similar to the ODB port of other vehicles). Conducting a Wireshark capture of this ethernet port revealed the standard and minimal network behavior expected when plugging a device into Ethernet (packets that establish a connection over Ethernet). No packets indicated that data transmission to the larger internet over Ethernet. Additionally, the Wi-Fi and Bluetooth data captured by Wireshark also showed no indication that Tesla transmitted personal over Wi-Fi or Bluetooth to the larger internet. However, we observed standard Wi-Fi broadcasts over the 802.11 Wi-Fi protocol advertising itself as "Tesla_6c:4b:f1," a behavior when a Wi-Fi hotspot or access point is enabled. For reference, this is the equivalent of when a person turns on their phone's hotspot, allowing other people to see the presence of the hotspot. These generic Wi-Fi broadcast packets don't signify that any personal data is being sent to the internet, but the Mac addresses could be used to identify the vehicle in near proximity, which could be significant for vehicle privacy.

The final vehicle we analyzed was an electric vehicle owned by COL Hamilton, the Technical Director of the Army Cyber Institute at the United States Military Academy. His vehicle is a 2023 Subaru Solterra, with the VIN number JTMABABA8PA008118. The Spectrum Guard data revealed that it used the 2.4 GHz frequency, which is the frequency for Wi-Fi, as well as 953.97583 Mhz frequency, which we suspect is likely a key fob or a radio frequency identifier device (RFID) used to detect (for example, a push to start identifier). After using Wireshark to analyze the Wi-Fi behavior, we found that the Wi-Fi broadcasts sent by this vehicle when the vehicle's Wi-Fi hotspot was enabled revealed the Extended Service Set Identifiers (ESSIDs) "SOLTERRA-2.4g_350d8f" and "SOLTERRA-5g_350d8e," which are the names of the vehicle's Wi-Fi hotspots. We also found the vehicle's Mac address, "Alpsalpine_35:0d:8f". After analyzing the vehicle's on-board Wi-Fi packets with Wireshark revealed that this vehicle created a connection to the IP Address 34.107.221.82, which seems to be a Google Content Delivery Network. However, analyzing the packet and IP address indicated that it was likely just a request for a resource the car uses. Although we were able to collect more information due to more familiarity with the tools we had, the collected packets were still typical for an internet-connected device (they were the packets used when a device connects to a network) and did not show evidence of personal data being transmitted to the internet over Wi-Fi or Bluetooth

Vehicle	VIN	Collected Data	Findings
2020 Ford Explorer	1FMSK8BH8LGC68547	- Tire pressure - Oil life - Battery status - Transmission fluid temperature	- Broadcasted itself on mDNS. - mDNS enables compatibility discovery (e.g., Apple devices finding AirPlay receivers).
2023 Chrysler Pacifica	2C4RC1L70PR513522	- Battery status	- No data transmission over Wi-Fi or Bluetooth. - Wireshark analysis revealed no data.
Tesla Model 3	5YJ3E1EA5PF401786	- Standard Ethernet behavior - Wi-Fi broadcast detected: "Tesla_6c:4b:f1"	- No user data transmitted over Wi-Fi or Bluetooth. - 802.11 Wi-Fi broadcast typical for hotspot functionality.
2023 Subaru Solterra	JTMABABA8PA008118	- Detected frequencies: - 2.4 GHz (Wi-Fi) - 953.97583 MHz - Wi-Fi hotspots: - "SOLTERRA-2.4g_350d8f" - "SOLTERRA-5g_350d8e" - MAC Address: Alpsalpine_35:0d:8f - Connection to IP: 34.107.221.82	- No evidence of data transmission to manufacturers. - Behavior typical of an internet-connected device.

Table 1: Summary of Vehicle Data Analysis and Findings.

Conclusions, Recommendations, and Future Work

Analyzing all the data collected from these modern vehicles showed that the only packets they emitted used network protocols typical for any internet-connected device, such as ARP, DHCP, and DNS. These are typical protocols seen when a device first connects to a network. Most of these packets were from our Linux device connected to the vehicle's hotspot. There were no irregular TCP or UDP packets, no irregular application-

level packets, and nothing indicating any user data was sent to the larger internet over Wi-Fi and Bluetooth. This indicated that if these vehicles transmitted any private data, it was likely over cellular/LTE, not Wi-Fi or Bluetooth. This makes sense since the vehicle's on-board Wi-Fi cannot provide an internet connection, while the on-board LTE/Cellular can provide an internet connection. Given this, our next step should be to attempt to intercept the communication between vehicles and mobile/cellular towers. The best approach will likely be acquiring a cellular base station or repeater and running Wireshark. If vehicles do communicate over cellular, we should be able to see all the network requests, which may contain encrypted or unencrypted packets. The packets will likely be encrypted, but we may be able to find information like the IP address the packets are sent to and make inferences on what data is being sent by finding packet bursts when compared to specific vehicle actions. With our findings, we can provide evidence that vehicles are programmed to send user data over the Internet, which could raise privacy concerns.

The only data that was transmitted over Wi-Fi and Bluetooth that can serve as a privacy risk were the Wi-Fi beacons sent when the users manually enabled a vehicle's on-board Wi-Fi hotspot feature. These Wi-Fi beacons reveal the vehicle's unique Mac Address (unique hardware identifier) and ESSID (hotspot name). If the user sets the vehicle name or hotspot name to something personal, then people around the vehicle can see the name of the hotspot when the vehicle is running a hotspot. Additionally, devices in the vicinity of the vehicle could use the broadcasted Mac address to log that the vehicle was there. There are open-source intelligence websites such as WiGLE, where anyone can upload Wi-Fi activity data at their location, creating a large searchable database of access point data. With proper resources and time, a researcher or attacker could build profiles of when different vehicles pass by common roads by placing Wi-Fi hotspot trackers near those roads. To mitigate this risk, we recommend pushing for legislation that requires vehicle manufacturers to make it easy to let a user randomize their Mac address.

Additionally, if we can acquire a vehicle to disassemble, a promising approach could be to physically extract the vehicle's infotainment system or the ECU and perform hardware hacking to gain access to the vehicle's infotainment computer. This may reveal what data is stored on the vehicle, the code for software on the vehicle, and other information that shows what user information vehicles might be sending over the internet. While this could reveal a significant level of data, it will require more expertise and specialized equipment that we will need to look into, which will let us collect data from the vehicle's hardware.

Policy Recommendations Post Initial Research

As of now, the unencrypted information we could capture wirelessly was the name of the hotspot (ESSID) and the Mac address of the car when Wi-Fi was enabled, either as an access

point or as a client. Some sites like WiGLE allow anyone to upload Wi-Fi access point information near their vicinity, which, in conjunction with their GPS location, provides details on where Wi-Fi devices are located. This could be used against cars by setting up Wi-Fi scanners around areas with heavy traffic, which can detect what vehicles are near the tracker. Over time, these could provide intelligence on patterns and behaviors for vehicles of interest. The best way to mitigate this is to turn off on-board Wi-Fi/Bluetooth capabilities (not feasible and unideal) or to mandate that users can easily randomize their vehicle's Mac address.

Conclusion

To conclude, we set out to find what information a car transmits about itself over the Internet. We explored common wireless features such as Wi-Fi and Bluetooth, which revealed that vehicles did not transmit packets to the Internet. Our next step will be exploring LTE/Cellular, as this is likely how the vehicle transmits data to the Internet and will expose the sensitive information we were seeking to find. There is a potential privacy issue in that when the vehicle has the Wi-Fi hotspot enabled, its Mac address can be used to recognize the vehicle. This can be mitigated by randomizing the vehicle's Mac address. Additionally, if it's possible to get an unwanted vehicle, we could also explore taking the vehicle apart to attempt to exploit the car's hardware to access on-board memory, services, and data.

BIBLIOGRAPHY

Bodei, Chiara et al. "Vehicle Data Collection: A Privacy Policy Analysis and Comparison." Dipartimento di Informatica, Universita di Pisa, Largo Bruno Pontecorvo 3, Pisa, Italy. https://www.scitepress.org/Papers/2023/117795/117795.pdf.

Checkoway, S., Mccoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (n.d.). Comprehensive Experimental Analyses of Automotive Attack Surfaces. https://www.usenix.org/legacy/event/sec11/tech/full_papers/Checkoway.pdf

Dawson, Jessica, and Katie Matthew. "Data as Ammunition: A New Framework for Information Warfare." The Cyber Defense Review, Summer 2024, Dawson_Matthew_CDRV9N2-SE-Summer-2024.pdf (army.mil).

James A. Chambers. "Use HackRF SDR to Lock / Unlock Car." James A. Chambers, August 15, 2022. https://jamesachambers.com/use-hackrf-sdr-to-lock-unlock-car/.

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., & Kantor, B. (2010). Experimental Security Analysis of a Modern Automobile. 2010 IEEE Symposium on Security and Privacy. https://doi.org/10.1109/sp.2010.34

Offensive Security. "Introduction to Car Hacking: The CAN Bus." *Offensive Security*, August 1, 2022. https://www.offsec.com/blog/introduction-to-car-hacking-the-can-bus/.

Pesé, Mert D. et al. "CarLab: Framework for Vehicular Data Collection and Processing." The University of Michigan – Ann Arbor. (October 20, 2017). https://ssl.engineering.nyu.edu/papers/reininger_sensevis_sas15.pdf.

Reininger, Michael et al. " A First Look at Vehicle Data Collection via Smartphone Sensors." NYU Polytechnic School of Engineering, University of British Columbia. https://ssl.engineering.nyu.edu/papers/reininger_sensevis_sas15.pdf.

SAE International. "Driver Identification Using Vehicle Telematics Data", (January 2017), https://www.sae.org.

U.S. Army. "ADP 3-13 INFORMATION HEADQUARTERS." 2023. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN39736-ADP_3-13-000-WEB-1.pdf.