Battery-Enabled Anti-Theft Vehicle Immobilizer

Liang He
University of Colorado Denver
Denver, CO, USA
liang.he@ucdenver.edu

Kang G. Shin
University of Michigan – Ann Arbor
Ann Arbor, MI, USA
kgshin@umich.edu

ABSTRACT

Auto thieves often exploit the cyber vulnerabilities of existing key/phone-based vehicle immobilizers. To prevent this exploitation of cyber vulnerabilities for auto thefts, we present *Battery Sleuth* (`Bleuth`), a novel *"physical"* vehicle immobilizer which is immune to the common cyber-attack vectors — avoiding the use of wireless communication between key/phone and vehicle as well as in-vehicle networks. `Bleuth` achieves this by using the common 12V vehicle batteries to authenticate the driver with encrypted power-line communication and then control the battery's output power based on the authentication results, hence (im)mobilizing the vehicle without requiring drivers to carry any additional token. `Bleuth` is also equipped with four alarms to detect, and respond to, illegitimate operations (i.e., theft attempts), including attempts of unauthorized cranking of the engine, removal/shorting of the authenticator from the battery, abuse of the PLC to drain the car battery, and removal of the dongle from the auxiliary power outlet. `Bleuth` recharges its power supply automatically to free drivers from the maintenance burden. We have prototyped `Bleuth` as an add-on module that can be installed on commodity vehicles and evaluated it via field tests on 8 vehicles. We have also demonstrated `Bleuth`'s utility and effectiveness via a survey of 612 car owners.

CCS CONCEPTS

• **Computer systems organization → Sensors and actuators**.

KEYWORDS

vehicle immobilizer, automotive batteries, power-line communication

ACM Reference Format:
Liang He and Kang G. Shin. 2022. Battery-Enabled Anti-Theft Vehicle Immobilizer. In *The 20th Annual International Conference on Mobile Systems, Applications and Services (MobiSys '22), June 25–July 1, 2022, Portland, OR, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3498361.3539772

1 INTRODUCTION

Wireless keys/keyfobs — and smartphones more recently — have been widely used as vehicle (im)mobilizers to prevent auto thefts by dis/enabling the driving of vehicles with three steps: (a) the vehicle's transponder electronic control unit (ECU) communicates wirelessly with the key/phone for authentication; (b) the transponder ECU notifies the vehicle's power control module of authentication success via an in-vehicle network (IVN), such as Controller Area Network (CAN); (c) the power control module enables the cranking of the engine.

These existing (im)mobilizers rely heavily on external wireless communication and IVNs, both of which are well-known to be susceptible to cyber-attacks. The wireless communication between the key/phone and the vehicle allows adversaries to hack the authentication system remotely via, for example, radio jamming/relaying [1, 14, 16, 26, 50, 55, 57]. The German General Automobile Club tested 237 vehicle models by 33 automakers in 2019 to find 99% of them suffering from the flaws of wireless communication [49]. Also, adversaries can intrude into the IVN (and thus sniff/inject/modify the information exchanged thereon) by exploiting its interface with the wireless modules and its inherent open accessibility via the OBD-II port [6, 30, 36, 38**?**]. These cyber vulnerabilities have led to the exploitation of existing immobilizers and then to ever-increasing auto thefts — 721,885 vehicles were stolen in the US in 2019, costing $6.4B in total [24]; a 9% further increase of auto thefts is observed in 2020; auto thefts increased even more significantly in the 1st half of 2021 in many cities, e.g., NYC (63%), DC (21%), Denver (73%), and San Jose (49%) [11, 12, 35, 44].

Unlike the traditional mitigation of cyber risks via cyber defense, we take a disruptive approach to develop *"physical"* vehicle (im)mobilizers without using wireless communication or IVNs, i.e., providing vehicles with physical isolation from common cyber attack vectors. Specifically, we propose *Battery Sleuth* (`Bleuth`), an after-market vehicle (im)mobilizer exploiting the common 12V automotive battery to immobilize the vehicle, which can be pervasively and easily installed on existing vehicles. `Bleuth` is inspired by the physical dependency between the operation of electric systems and the concomitant power consumption, using the 12V automotive battery as a physical and encrypted sensing/control channel — which is not accessible remotely/wirelessly or via IVNs — to validate driver's identity and then dis/enable vehicle driving based on validation results.

Fig. 1 provides an overview of `Bleuth`, consisting of two physical modules: a *front-end dongle* plugged into the auxiliary power outlet (a.k.a. the cigarette lighter port) to interact with the driver, and a *back-end authenticator* installed in the engine cabin (i.e., between the battery and the vehicle) to communicate with the dongle and control the battery's power capacity. Specifically, the dongle accepts the driver's input of authentication information (e.g., passcode and/or bio-fingerprint) and transmits it to the authenticator via the auxiliary power outlet with encrypted power-line communication (PLC) based on Multiple Frequency-Shift Keying (MFSK). The authenticator demodulates the driver's input from the battery's discharge current, matches it with the pre-defined authentication

MobiSys '22, June 25–July 1, 2022, Portland, OR, USA

ACM ISBN 978-1-4503-9185-6/22/06.
https://doi.org/10.1145/3498361.3539772

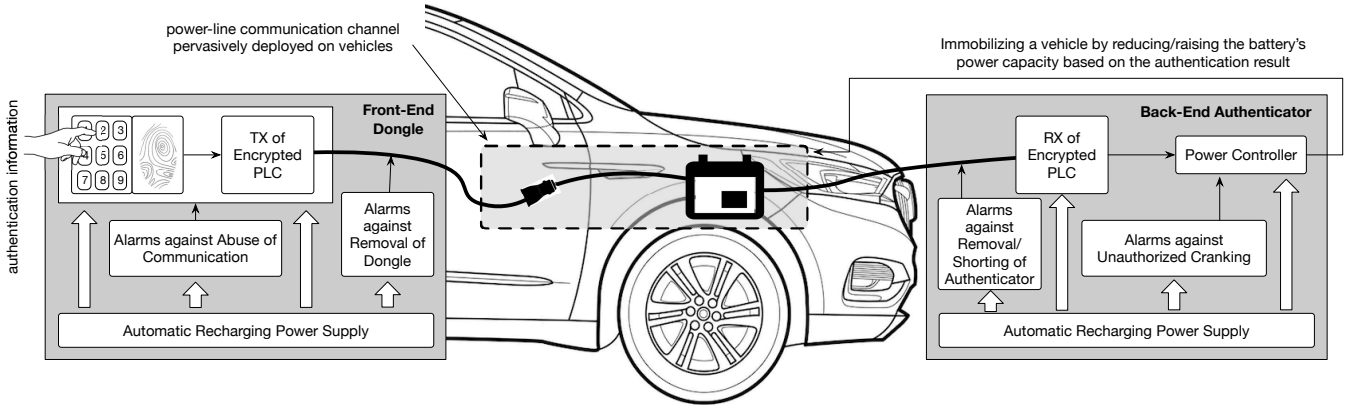


Fig. 1. `Bleuth` **consists of a front-end dongle interacting with the driver and a back-end authenticator interacting with the battery, which are connected via an encrypted PLC using battery current as the signal carrier.**

information, and reduces/raises the battery's power capacity to dis/enable the cranking of the engine based on the matching results. Note that `Bleuth`'s transmission of authentication information is *not observable* on the in-vehicle network as battery current is not the information monitored/exchanged thereon.

The challenges of `Bleuth` lie in the noises/dynamics caused due to battery aging/temperature/state-of-charge and the operation of the vehicle's other electric (e-) systems, which `Bleuth` addresses using a set of empirically validated principles that steer its optimal design/configuration. Moreover, as an end-to-end anti-theft protection provided to car owners, `Bleuth` must detect and deter attempts of auto thefts with high accuracy and timeliness, which is achieved with four circuit-driven alarms against illegitimate operations, including (i) attempts of unauthorized cranking of the engine, (ii) removal/shorting of the authenticator from the battery, (iii) abuse of the PLC to drain the car battery, and (iv) removal of the dongle from the auxiliary power outlet. `Bleuth` is also equipped with power supplies that recharge itself automatically for ease of use, i.e., relieving car owners from the burden of maintaining `Bleuth`.

We have prototyped `Bleuth` as an end-to-end vehicle immobilizer and evaluated it on 8 vehicles, with different e-systems of the vehicle operating in the background and using batteries that are of (i) more than 10-year difference in age, (ii) voltage varying from 9–12.8V, and (iii) temperature as low as 24^{o}F. Our experimental results show `Bleuth` to achieve a >99.9% success rate of transmitting the authentication information to the authenticator, immobilize the vehicles without failure, swiftly/reliably detect illegitimate operations, and be robust to the dynamics/noises caused by a vehicle's e-systems and battery aging/voltage/temperature. Our survey of 612 car owners also corroborates `Bleuth`'s utility and commercial potential in the $11.64B market of automotive anti-theft systems.

In summary, this paper makes the following contributions:

- Pioneering exploration of securing systems with physical isolation from common cyber-attack vectors;
- Development of a novel vehicle immobilizer, called `Bleuth`, that uses batteries as sensors/controllers, and a systematic way of optimally configuring `Bleuth`;
- Demonstration of `Bleuth`'s high level of security and robustness, as well as users' acceptability via extensive field tests and user study.

2 RELATED WORK

Car-makers have been improving, or even replacing, car keys or keyfobs [21]. `Bleuth` is closely aligned with these industrial trends, but very different in that the authentication is *physical* and built on the automotive battery. Table 1 compares `Bleuth` with existing vehicle immobilizers.

Commercial/Industrial Solutions. Car-makers have been using mobile phones/apps as a complementary solution of car keys [21, 22, 43, 54]. These solutions still rely on wireless authentication and IVNs, suffering from their cyber vulnerabilities as mentioned before. They also need phones whereas `Bleuth` does not require car owners to carry any token/device for vehicle immobilization.

Tesla launched, and deployed on its Model S/X via over-the-air (OTA) updates, a PIN-To-Drive feature in 2018, which allows the driver to set a 4-digit verification code that must be entered via a touchscreen on the control panel before starting the car [13]. This PIN-To-Drive feature requires wireless OTA updates for deployment and IVN for daily vehicle immobilization, both of which are vulnerable to cyber attacks as mentioned before. Also, this feature and/or its variants limit deployability, due to their requirements of (i) a pre-installed user interface that accepts the driver's input and communicates with the vehicle's engine control unit via the IVN and (ii) the subscription of OTA updates, neither of which is always available on other commodity vehicles.

Various physical locks, such as tire/steering/pedal locks, are available to reduce a vehicle's drivability, but they suffer poor usability as drivers need to (un)install locks each time leaving the vehicle unattended. Kill-switches prevent auto thefts by cutting off the vehicle's electric current flow, which also disables the monitoring function of parked vehicles, thus becoming unsuitable for daily usage. After-market alarm systems are also available, such as Viper [53] and Pandora [40]. Ironically, both of them are built on vulnerable wireless communication and have been proven hackable for auto thefts [17].

Compared to these commercial solutions, `Bleuth` has distinct advantages in that it is *secure* (i.e., physically isolated from the common cyber-attack vectors), *convenient* (i.e., no need to carry any token/device), and *pervasively deployable*. Besides being used as 2nd-factor driver authentication (as with Phone-As-Key and

Table 1: Comparison of `Bleuth` with existing vehicle immobilizers.

Existing/Potential Solutions	Technical Design					Security		Usability		Potential	
	Collector (or Form of Identify)	Betw. Collector & Authenticator	Authenticator	Betw. Authenticator & Controller	Controller (or Control Knob)	Resist. To Wireless Attacks	Resist. To OBD Hacking	Pervasively Deployable	Carry-less	Replacing Keys/Keyfobs	Identifying Drivers
RF Keys/Keyfobs	Digital Code via RF Keys	Wireless signal	Transponder ECU	In-Vehicle Network	Power Control ECU	No	No	Yes	No	N.A.	Yes
Phone-As-Key	Digital Code via Phone	Wireless signal	Transponder ECU	In-Vehicle Network	Power Control ECU	No	No	No	No	No	Yes
Tesla's Pin-2-Drive	Digital Code via Control Panel	In-Vehicle Network	Transponder ECU	In-Vehicle Network	Power Control ECU	No	No	No	Yes	No	Yes
After-Market Alarms, e.g., Pandora/Viper	Digital Code via Token/Phone	Wireless signal	Special OBD Dongle	In-Vehicle Network	Power Control ECU	No	No	No	No	No	Yes
Tire/Steering Locks	Metal Keys	N.A.	Metal Locks	N.A.	Metal Locks	Yes	Yes	Yes	No	No	No
Kill-Switch	Digital Code via Token	Wireless signal	Special Controller	N.A.	Switch	No	Yes	Yes	No	No	No
	Control Code via Hidden Button	Additional Wiring	Special Controller	N.A.	Switch	Yes	Yes	Yes	Yes	No	No
	Button Switch in Engine Cabin	N.A.	Switch	N.A	Switch	Yes	Yes	Yes	Yes	No	No
BAuth [19]	Operation of Vehicle's E-System	Battery Voltage on Pre-Deployed Powerline	Special Controller	N.A.	Battery Power as Control Knob	Yes	No	Yes	Yes	No	Yes
Bleuth	Digital Code or Fingerprint via Front-End Dongle	Battery Current on Pre-Deployed Powerline	Back-End Authenticator	N.A.	Battery Power as Control Knob	Yes	Yes	Yes	Yes	Yes	Yes

Table 2: Detailed comparison of `Bleuth` with [20].

	Property	[20]	Bleuth
Design	User Interface	(mostly) before-market e-systems	customized dongle
	Authentication Information	e-operation observed in voltage, no modulation	current modulated with MFSK
	Encryption	no	yes
	Power Controller	requires power distribution, no surge protection	no power distribution required, surge protection
	Alarms against Illegitimate Operations	two software-driven alarms	four circuit-driven alarms
	Automatic Recharging Power Supply	no	yes
Performance	Authentication Accuracy (True/False Positive)	98.17/2.84% (average)	99.90/0% (worst-case)
	Observable on in-vehicle network	yes (e.g., via the message ID of CAN)	no
	Vulnerability to Observation Attack	high	low
Potential	Extensibility to Controlling Entry to Vehicle	no	yes
	Extensibility to Biometric Authentication	no	yes
	Replacing car keys/keyfobs	no	yes

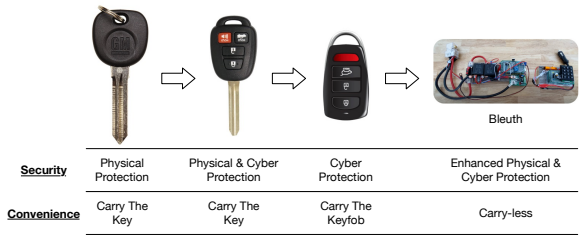


Fig. 2. `Bleuth` opens a new era of vehicle usage.

PIN-To-Drive), `Bleuth` can also replace car keys/keyfobs, and thus open the new era of vehicle usage illustrated in Fig. 2 as we will corroborate in Sec. 11.

Academic Solutions. There have been significant efforts on vehicle security in academia, many of which focus on vehicles' cyber vulnerabilities/defenses with regard to the wireless accessibility/connectivity [23, 39, 45] or in-vehicle communication and processing [8–10, 27–29, 31, 34] — i.e., the key motivational observation of `Bleuth`. Research on vehicle immobilization is, however, very limited: [52] reverse-engineered the proprietary security mechanisms of existing car keys/keyfobs and corroborated their cyber vulnerabilities empirically; [25] secured the keys/keyfobs using their RF fingerprints. `Bleuth` differs from these in that it does not rely on vulnerable wireless communication or IVNs at all. The closest to `Bleuth` is BAuth [20], which uses customized e-system operations (e.g., *"swipe the wiper twice"*) as the passcode to authenticate drivers. `Bleuth` improves [20] holistically, as compared in Table 2 from the perspectives of security, usability, and potential for introducing new functions. Although extensive work has been done on the analysis of in-vehicle PLC channels [3, 32, 41, 48], to the best of our knowledge, `Bleuth` is the first end-to-end PLC system with the battery as one end, which usually suffers from high attenuation, large noise, and low impedance. `Bleuth` overcomes these difficulties.

3 PRELIMINARIES

Design Insights. `Bleuth`'s design is grounded on the physical dependency between the operation and power consumption of electric systems which allows immobilization of vehicles by using their batteries as a physical sensing/control channel. Two fundamental functions for vehicle immobilizers are to (i) accept the driver's input of authentication information and (ii) dis/enable the cranking of the vehicle's engine. To defend against cyber attacks, a *"physical"* vehicle immobilizer must provide these two functions without using wireless communication or IVN. Our following observations of 12V automotive battery — which is pervasively deployed on all

gasoline/hybrid/electric vehicles — have led us to develop such a physical vehicle immobilizer.

Observation 1: A vehicle's engine is not crankable without sufficient power, making it possible to dis/enable vehicle driving by regulating the output power of its battery.

It is, however, challenging to design and install such a battery-based vehicle immobilizer because the battery is commonly located in the engine compartment, requiring a convenient and reliable communication channel for the driver to send the battery the authentication information without opening the hood every time. A possible way to provide this driver–battery communication is to install an additional wire through the engine and passenger cabins. We eliminate the need for this additional wiring by making the following (second) observation:

Observation 2: The auxiliary power outlet allows the driver–battery communication by providing a pervasively deployed PLC channel that cannot be accessed remotely or via IVNs.

Threat Model. We classify adversaries whose goal is to steal vehicles according to their knowledge of `Bleuth`.

Bleuth-Oblivious Attackers. `Bleuth`-oblivious attackers attempt to steal vehicles by voiding the key/phone-based immobilizers. The attackers can achieve this using either (i) cyber approaches such as jamming/replaying the authentication signal between the key/phone and the vehicle [42], hacking vehicles' wireless interfaces for OTA updates to invade the IVN [46], cloning the keys via the OBD-II port after forcibly entering the vehicle [33], illegitimately pairing the vehicle's remote control system with a malicious phone (e.g., for rental cars [15]), etc., or (ii) traditional approaches such as using stolen keys, hot-wiring (for old cars), towing, or even carjacking.

Bleuth-Aware Attackers. `Bleuth`-aware attackers have sufficient knowledge of `Bleuth` to mount customized attacks, such as uninstalling or shorting `Bleuth`'s authenticator from the battery after gaining access to the passenger and engine compartments (e.g., by opening/breaking windows), mounting DoS attacks by removing `Bleuth`'s dongle from the auxiliary power outlet and/or abusing `Bleuth`'s PLC to drain the vehicle battery, voiding `Bleuth` by connecting a second battery in parallel with the original battery, or even physically tampering with `Bleuth` to disable its normal function. However, we assume adversaries cannot mount a targeted attack to hack `Bleuth`'s individual modules, such as erasing the control algorithms from its authenticator or disconnecting its power supply/alarm. This assumption is justified because `Bleuth` can be (i) installed with a protective case if provided as an add-on module to commodity vehicles, and (ii) integrated with vehicles if provided by automakers as a before-market product (and thus hidden from the attacker), to thwart attacks on `Bleuth`'s individual components. Also, we assume car owners keep their authentication information (e.g., password/bio-fingerprint) secure from adversaries — no authentication system will otherwise be secure.

4 SYSTEM OVERVIEW

With the dongle plugged in the auxiliary power outlet and the authenticator installed on the battery, `Bleuth` is comprised of the following four functional components.

(1) An encrypted PLC system which allows the dongle to send the driver-inputted passcode to the authenticator using the battery's discharge current as the signal carrier. The dongle/authenticator's heterogeneous location in a vehicle's power network, especially the DC/DC converter in between (see Fig. 3(a)), makes the PLC between them challenging: the power-line channel connecting battery suffers high attenuation, large noise, and low impedance [3, 32, 41, 48], all of which degrade communication reliability. Fig. 3(b) shows attempts of using two off-the-shelf MAX20340 IC to implement the dongle-to-authenticator communication: the communication succeeds (fails) when the battery is disconnected (connected) to the circuit. Also, letting the dongle match the driver-inputted passcode and sending the matched result to the authenticator is not a good option, as thieves could undo the anti-theft protection by replacing the dongle with their own. As a rule-of-thumb, we should make the front-end as "thin" as possible.

(2) A power controller at the authenticator to reduce/raise battery's power capacity using a power control circuit to (dis)allow engine cranking based on authentication results.

(3) Circuit-driven alarms to detect, and respond to, illegitimate operations in real-time: the authenticator detects any unauthorized attempt of cranking of the engine and its removal (or shorting) from the battery, and the dongle detects the abuse of the PLC (which drains the battery) and its removal from the auxiliary power outlet.

(4) Rechargeable power supplies for the dongle and authenticator, which recharge automatically with the power generated by the vehicle's alternator, thus freeing drivers from maintenance burden.

For ease of presentation, we will assume a 4-digit passcode (i.e., same as Tesla's Pin-To-Drive) is used as the authentication information and then corroborate `Bleuth`'s feasibility of using other types of authentication information, such as bio-fingerprints, in Sec. 11.

5 ENCRYPTED PLC SYSTEM

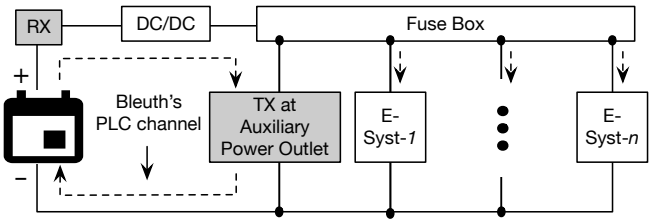
`Bleuth` uses a PLC system to allow the driver (with the front-end dongle as the transmitter (TX)) to send his/her authentication code to the battery (equipped with the back-end authenticator as the receiver (RX)). As depicted in Fig. 4, this PLC system consists of circuit, (de)modulation, and application layers.

5.1 Circuit Layer

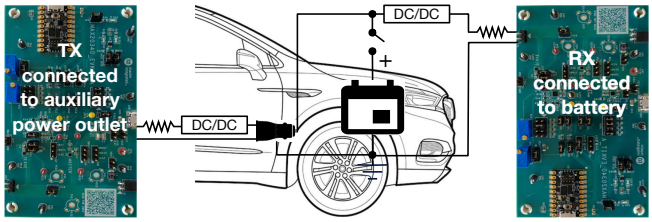
The circuit layer allows the control of battery discharge to generate a regulated battery voltage/current as the communication signal, as shown in Fig. 5.

TX Circuit. The TX circuit controls the connection of a load resistor R_{load} to the auxiliary power outlet using a power transistor: applying a control voltage V_{in} to the power transistor will connect R_{load} to the power outlet, adding a discharge current of $V_{\text{aux}}/R_{\text{load}}$ to the vehicle's background current, where V_{aux} is the voltage of the auxiliary power; on the other hand, removing V_{in} from the power transistor will disconnect R_{load} from the power outlet, and thus no additional discharge current will be produced. This transmission circuit allows the modulation of battery current/voltage by (de)energizing the transistor at a specific frequency.

Then, the first question we need to address is: should the battery current or voltage be used as the communication carrier signal? We



(a) Heterogeneous logical locations of dongle and authenticator



(b) Failed attempts of using off-the-shelf MAX20340

Fig. 3. It is non-trivial to design the dongle-to-authenticator PLC.

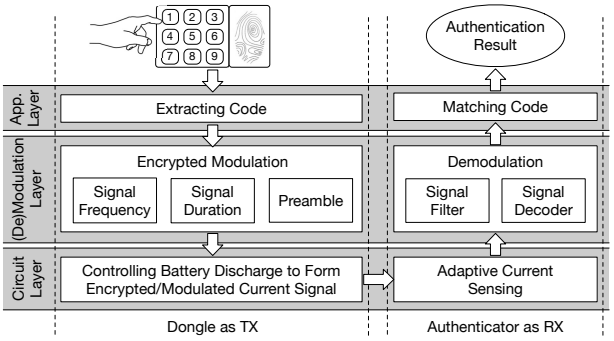


Fig. 4. Three-layer architecture of `Bleuth`'s PLC system.

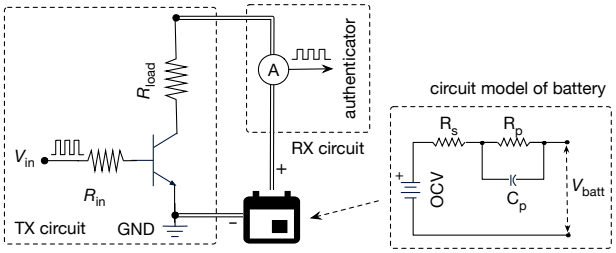


Fig. 5. Circuit schema of `Bleuth`'s MFSK-based PLC system.

choose current because battery voltage reacts slower than current to load stimulus due to its capacitive behavior, i.e.,

$$V_{\text{batt}}(t) = OCV - (R_s + R_p) \cdot I + R_p \cdot C_p \cdot dV_{\text{batt}}(t)/dt, \quad (1)$$

where OCV is the battery's open-circuit voltage and $\{R_s, R_p, C_p\}$ are the battery's equivalent serial resistance, parallel resistance, and capacitance, respectively, as shown in Fig. 5. The time constant τ=R_p·C_p dictates how quickly the battery voltage stabilizes. Ideally, battery voltage supports a maximum signal frequency of $1/\tau$, as a higher frequency would prevent the voltage from stabilizing, and thus increase the signal variance. Note that battery voltage is also more sensitive to the dynamics caused by the battery's State-of-Charge (SoC), temperature, and age [2, 20]. Fig. 6 plots the results after applying FFT to the current/voltage collected (and then filtered with a 0.01Hz high-pass filter) when operating the transistor at 10Hz: one can clearly observe the 10Hz operating frequency from the current, but not from the voltage. Fig. 6 also plots the peak frequency identified from the current/voltage while varying the cutoff frequency of the high-pass filter, again showing that current is a more reliable signal carrier than the battery voltage.

Another issue to address is the sizing of the resistor R_{load}, which determines the magnitude of the thus-formed current, i.e., I_{signal} =

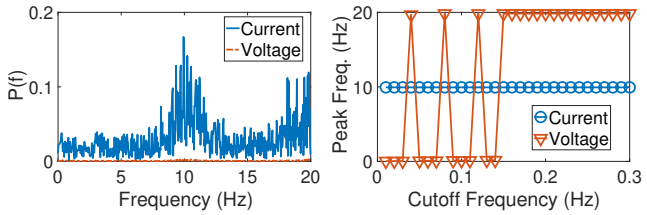


Fig. 6. Current is a more reliable signal carrier than voltage.

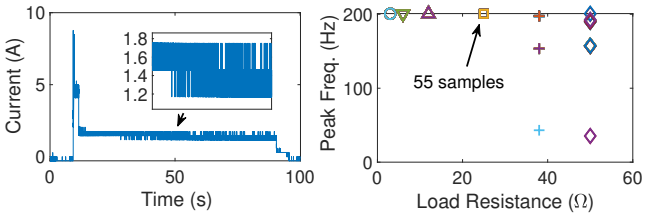


Fig. 7. `Bleuth` needs a current larger than the variance of vehicle's idle current.

$V_{\text{aux}}/R_{\text{load}}$. A current signal with a larger amplitude — i.e., using a smaller R_{load} — improves the robustness of communication but consumes more power. We optimize this trade-off based on the conjecture that the amplitude of the current signal should be larger than that of the channel variance/noises, i.e., the fluctuating magnitude of a vehicle's idle current I_{idle}:

$$I_{\text{signal}} = V_{\text{aux}}/R_{\text{load}} > \max(I_{\text{idle}}) - \min(I_{\text{idle}}). \quad (2)$$

Let us consider the idle current of 2008 Honda Fit plotted in Fig. 7, which has a ≈0.6A fluctuating magnitude. Eq. (2) implies an R_{load}< $12V/0.6A$=20Ω is needed to ensure the communication reliability (assuming a standard V_{aux} of 12V). To validate this, we transmit signals modulated at 180Hz with different R_{load} while keeping the vehicle idle and V_{aux}≈12.2V. Fig. 7 summarizes the peak frequency demodulated from the current signal, showing a resistor of {3, 6, 12, 25}Ω — leading to a I_{signal} of {4.07, 2.03, 1.02, 0.49}A — achieves reliable demodulation, while those with larger resistances (i.e., 38Ω and 50Ω) cannot due to too small a current (i.e., 0.32A and 0.24A), corroborating Eq. (2) except for the case of R_{load}=25Ω. We will, in Sec. 9, show that a R_{load} of 25Ω, albeit achieving 100% demodulation accuracy, causes miss-detection of the transmitted signal.

RX Circuit. The RX circuit is responsible for monitoring the battery current and then reporting it to the (de)modulation layer. To reduce power consumption, the RX activates its high-frequency current sensing only when driver authentication is needed, which is, in turn, determined based on the event of turning on the vehicle. The RX determines the vehicle's turn-on when the battery's

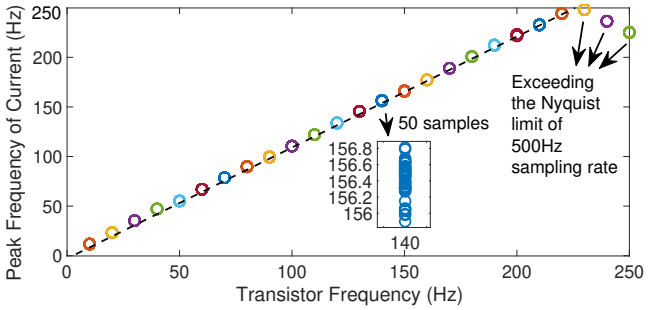


Fig. 8. Corroborating the feasibility of MFSK-based PLC.

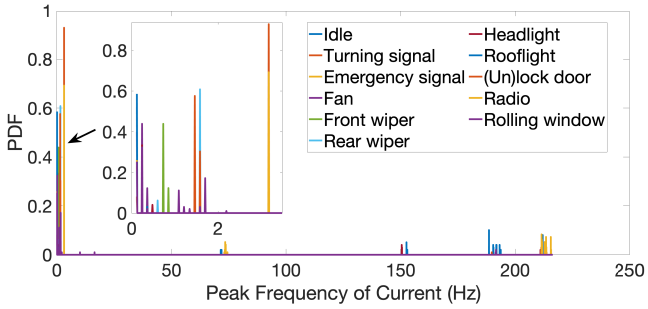


Fig. 9. Peak frequency of current when operating the e-system of 2008 Honda Fit.

discharge current increases from ≈0A to a few amperes, as a result of activating the vehicle's e-systems. The RX moves to sleep mode after the engine is cranked successfully (which is possible only after passing the authentication).

5.2 (De)Modulation Layer

The (de)modulation layer (de)modulates the communication signal (i.e., current) with the optimized configuration.

Encrypted Modulation at TX. Unlike the traditional Binary FSK (BFSK) that uses two frequencies to modulate the bit of "1" and "0" and then transmits the symbol via, for example, binary coding, `Bleuth` uses M-ary FSK (MFSK) to improve throughput, i.e., modulating a driver's input of symbol $s \in \mathbb{S} = \{\text{"0"}, \text{"1"}, \text{"2"}, \ldots, \text{"9"}\}$ with a frequency selected from a pre-defined set $\mathbb{F} = \{f_0, f_1, f_2, \ldots, f_9\}$. This MFSK is feasible because of the fixed/limited authentication symbols and the relatively sufficient frequency spectrum. `Bleuth` identifies $\mathbb{F}$ following the principle of

$$f_{i+1} = f_i + 2f_d \ (i = 0, 1, \ldots, 9), \tag{3}$$

where f_d is the frequency shift. As a larger f_d increases the modulation order/index and thus allowing a higher bit rate, we steer the selection of $\mathbb{F}$ by:

$$\begin{aligned} & \text{maximize } f_d \\ \text{s.t.} \quad & f_d > \max\{\max\{f_i^{99}/2\},\ f_{\text{resolution}}/2\}, \\ & \forall i,\ f_{\min} < f_i < f_{\max}, \end{aligned} \tag{4}$$

where f_i^{99} is the 99% bandwidth of f_i, $f_{\text{resolution}}$ is the frequency resolution determined by the sampling frequency and the FFT size when demodulating the signal, and $f_{\min}$ and $f_{\max}$ are the minimum and maximum feasible modulation frequency, respectively.

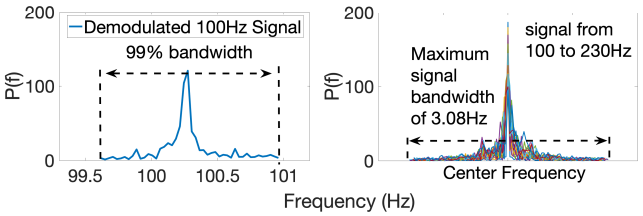


Fig. 10. Modulated current has a 99% bandwidth of 3.08Hz.

Let us use our implementation of `Bleuth`, in which the battery current is sampled at 500Hz, to illustrate the selection of $\mathbb{F}$ based on the above principles. We first examine the maximum feasible frequency $f_{\max}$. Specifically, we collect the discharge current when (de)energizing the transistor at 10–250Hz, and apply FFT to identify the peak frequency thereof. Fig. 8 summarizes the results, showing (i) the linearity between f_{peak} and $f_{\text{transistor}}$, i.e.,

$$f_{\text{peak}} = a \cdot f_{\text{transistor}} + b, \tag{5}$$

and (ii) the consistency of f_{peak} with a given $f_{\text{transistor}}$. Besides corroborating the feasibility of the MFSK-based modulation, these results also show that operating the transistor at a high frequency of, for example, ≥230Hz, is not reliable, because a≈1.1 in Eq. (5) — a >230Hz transistor frequency leads to >250Hz peak frequency of current, exceeding the Nyquist limit when sampling at 500Hz. This way, we know $f_{\max}$<230. Next, we examine the minimum feasible frequency $f_{\min}$, which is mainly determined by the potential interference caused by the operation of the vehicle's e-systems. Fig. 9 plots the peak frequency of the current when operating the e-systems of 2008 Honda Fit: unsurprisingly, the e-system frequency is clustered at the low end of the spectrum, which `Bleuth` should avoid, i.e., $f_{\min}$>5Hz. We have also examined the 99% bandwidth of the signal modulated at 20–230Hz, as shown in Fig. 10, showing `Bleuth`'s need for f_d>1.54Hz. Lastly, as we will show later, at least 64 samples are needed to ensure the demodulation accuracy, leading to a frequency resolution of 500/64≈7.8Hz when sampling at 500Hz, i.e., f_d>3.9Hz. Based on these observations, we use $\mathbb{F}$={20:20:200}Hz to implement `Bleuth`. Note these low frequencies of $\mathbb{F}$ will not interfere with other vehicle systems operating in a pre-allocated frequency range, e.g., 87.5–108MHz for FM radio.

With the thus-identified $\mathbb{F}$, `Bleuth` transmits an authentication symbol s using frequency f_s selected from $\mathbb{F}$ based on a randomly-generated preamble. Specifically, `Bleuth` randomly selects a preamble frequency $f_{\text{preamble}} \in \mathbb{F}$ and transmits s at frequency

$$f_s = f_{(\text{preamble}+s)\%|\mathbb{S}|}. \tag{6}$$

This way, a given authentication symbol with be modulated at frequency $f_i \in \mathbb{F}$ with a probability of $1/|\mathbb{S}|$, achieving the maximum entropy. Note that this preamble, besides injecting randomness (and hence security) in the communication, is also required to ensure the RX's detection of the transmission — `Bleuth`'s PLC is needed only when the driver keys in the passcode, which happens at irregular times and thus requires an asynchronous communication protocol.

Lastly, we need to determine the transmission duration, i.e., the time to send the preamble (at frequency f_{preamble}) and a given authentication symbol (at frequency $f_i \in \mathbb{F}$), as illustrated in Fig. 11. We use a symbol duration of T_s=$\theta \cdot T_w$(θ>1), where T_w is the size of the moving window which the receiver at the authenticator uses to

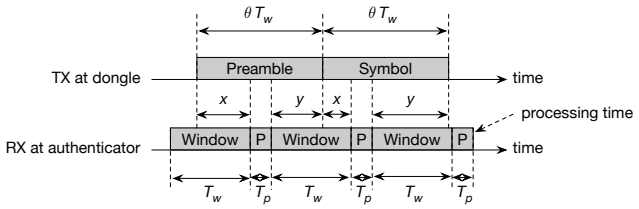


Fig. 11. Asynchronous communication.

demodulate the current signal, and θ>1 is a transmission coefficient used to ensure demodulation accuracy. We will elaborate on how to set T_w and θ when describing the receiver in detail.

Demodulation at TX. The RX demodulates the collected battery current to recover the transmitted authentication symbol using a moving window of size T_{w}. For a given window, the receiver first checks if the fluctuation of current thereof is larger than I_{signal} (i.e., it will otherwise not contain the transmitted signal), in which case the receiver applies a 5Hz high-pass filter (steered by Fig. 9) to remove the noises caused by e-operations, and then identifies the peak frequency of the remaining signal (denoted as f_{peak}) using FFT. The receiver concludes the detection of the preamble if $|f_{\mathrm{peak}} - a \cdot f_i - b| \leq f_\delta$ for certain i, after which the receiver will attempt to identify the transmitted authentication symbols in the next window(s) by checking if $|f_{\mathrm{peak}} - a \cdot f_j - b| \leq f_\delta$ for certain j, and if yes, demodulate the authentication symbol as:

$$s' = ((j - i) + |\mathbb{S}|)\%|\mathbb{S}|. \tag{7}$$

Next, we describe how to set $\{f_\delta, T_{\mathrm{w}}, \theta\}$. The signal threshold f_δ must be determined jointly with window size T_w, because a smaller T_w increases the variance of detected peak frequency and thus requires a larger f_δ to ensure demodulation accuracy (see Fig. 12 which plots the demodulation of a 100Hz signal with different-size windows). Note that the choices of window size are limited to the power of 2 in Fig. 12 to facilitate the implementation of FFT on the authenticator's microcontroller (MCU). The window size T_{w} is desired to be small to allow a high data rate but needs to be large enough to collect sufficient signal samples for accurate demodulation, e.g., at least 128ms to collect 64 signal samples at 500Hz in Fig. 12. We use a conservative setting of T_w=256ms to ensure communication reliability, which, in turn, implies f_δ of 1Hz according to Fig. 12. The transmission coefficient θ is also desired to be small but must be sufficiently large to ensure that for any preamble/symbol transmission, there must be a window at the receiver capturing at least 64 signal samples. Taking Fig. 11 as an example, where the transmitting signal for a preamble/symbol is collected in two consecutive windows at the receiver — for any transmission j, we need to ensure at least one of $\{x_j, y_j\}$ is larger than 64/500Hz=128ms (or $T_{\mathrm{w}}/2$). Clearly, at least one window will contain only the transmitting signal if a transmission is captured in more than 2 consecutive windows, thus making the transmission detectable by the receiver. Letting T_{p} be the computation time for the RX to process a collected window, our objective is to:

$$\begin{aligned} & \text{minimize } \theta \\ \text{s.t.} \quad & \forall j,\ \max\{x_j, y_j\} \geq T_{\mathrm{w}}/2, \\ & \forall j,\ x_j + y_j = \theta \cdot T_{\mathrm{w}} - T_{\mathrm{p}}, \end{aligned} \tag{8}$$

which leads to the requirement of

$$\theta \geq (T_{\mathrm{w}} + T_{\mathrm{p}})/T_{\mathrm{w}}. \tag{9}$$

Fig. 13 plots the computation time when using Arduino Mega as the authenticator's MCU to process different-size windows, showing a (slightly) super-linear relationship between T_{w} and T_{p} (i.e., FFT has $\mathbb{O}(n \log n)$ complexity). We approximate this relationship with linear regression and obtain $T_{\mathrm{p}} \approx 0.23 T_{\mathrm{w}}$, i.e., we need $\theta \geq 1.23$. We will empirically validate the settings of these variables in Sec. 9. Note that although these empirical settings are determined for the hardware we used to prototype `Bleuth`, our approaches of identifying them are general.

5.3 Application Layer

At the TX side, the application layer is responsible to extract the communication payload from the authentication information collected from the driver, which is straightforward if the authentication information is defined in form of a password. If other forms of authentication information, such as bio-fingerprints or face images, are used, the application layer needs to process the raw information and extract their features as the payload. The RX-side application layer matches the received authentication information with the pre-defined authentication code. In our case of using a 4-digit password as the authentication code, this matching is done each time a total of 4 symbols have been received.

6 POWER CONTROLLER

The authenticator matches the driver's input it received, with his/her pre-defined passcode, and then (im)mobilizes the vehicle by controlling the battery's power capacity based on the result of matching. This power control builds on the fact that the cranking of the engine requires a much higher current than the vehicle's e-systems (including the PLC for authentication), e.g., cranking the engine requires 2–9kW for 0.3–3s depending on vehicle type [5]. Fig. 14 summarizes our measurements of the battery's discharge current to operate the e-systems of 2008 Honda Fit, showing cranking the engine requires a >3x current of that for operating all other e-systems together (i.e., (1.4+147.6)/43.45=3.43)! This fact encompasses a current level that supports the PLC-based driver authentication but does not crank the engine, allowing the use of the battery's power capacity as the control knob to dis/enable the cranking of the engine based on the authentication result.

We design the power controller as depicted in Fig. 15. The controller connects the battery and the vehicle with low and high power paths, each of which uses a relay to control its dis/connection (i.e., by applying/removing $V_{\mathrm{in}}^{\mathrm{low}}$ and/or $V_{\mathrm{in}}^{\mathrm{high}}$). The low-power path further uses a circuit breaker to limit the maximum current allowed thereon (i.e., $I_{\mathrm{low}}^{\mathrm{max}}$), exceeding which will disconnect the breaker (and hence the path). Note that a circuit breaker can be reset (e.g., by pressing a button) without replacing any physical component. `Bleuth` connects the low-power path by default to allow only the current up to $I_{\mathrm{low}}^{\mathrm{max}}$, where $\sum I_i < I_{\mathrm{low}}^{\mathrm{max}} < I_{\mathrm{crank}}$ and I_i is the current necessary to operate the i-th e-system of the vehicle. In the case of successfully validating a driver's identity, `Bleuth` disconnects (connects) the low (high) power path to restore the maximum current that can be drawn from the battery, thus enabling the cranking of

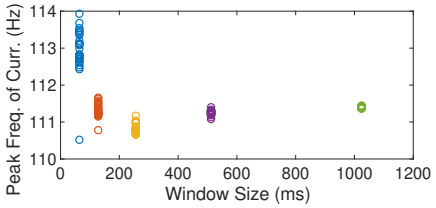


Fig. 12. A larger variance of peak freq. is observed with a smaller window.

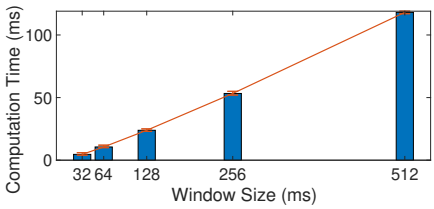


Fig. 13. Computation time to process windows of different sizes.

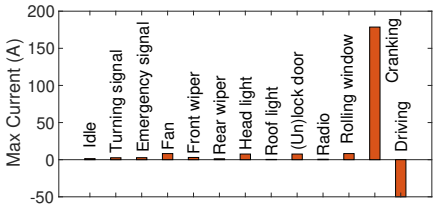


Fig. 14. Battery current when operating the e-systems of 2008 Honda Fit.

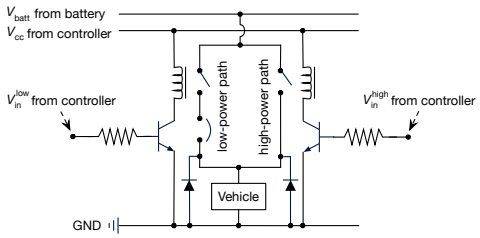


Fig. 15. Controlling battery power by (dis)connecting low/high-power path.

the engine. Bleuth keeps the battery in the high-power mode and switches back to the low-power mode if the engine is not cranked soon enough after the authentication, or the engine is cranked and then stopped after completing the driving (observed as the battery voltage decreases from about 15V to below 13V). Fig. 16 summarizes the logic of Bleuth's power controller. A reverse surge voltage may be generated when switching the path connectivity due to the vehicle's inductive load, reducing the power controller's lifetime. We use two protective diodes to protect the circuit from voltage surges.

7 ALARMS

Bleuth uses four alarms to detect illegitimate operations. These alarms are designed with low-cost/complexity electrical circuits (see Fig. 17) to ensure reliable/fast detection/response, disconnecting/shorting the alarms in normal cases and connecting (and hence activating) them in case of illegitimate attempts/operations. See [19] for step-by-step explanations/case-studies of these alarm circuits and Bleuth's power supplies.

Alarm Upon Unauthorized Cranking. The battery and the vehicle are connected by the low-power path before the driver is authenticated successfully — cranking the engine without passing the authentication overloads/breaks the low-power path. Bleuth exploits this fact and uses the alarm circuit shown in Fig. 17(a) — consisting of a protective resistor R_1 and a siren connected in parallel with the low/high power paths — to detect unauthorized cranking.

Alarm Upon Removal/Short of Authenticator. Bleuth-aware thieves may attempt to disable its anti-theft protection by uninstalling/shorting the authenticator from the battery/vehicle. Bleuth uses a Single Pole Double Throw (SPDT) relay to detect, and respond to, such illegitimate operations, as depicted in Fig. 17(b).

Alarm Upon Abuse of Communication. Thieves who have broken into the passenger compartment and activated the auxiliary power outlet — e.g., using stolen/cloned keys — may abuse the PLC by using the dongle to transmit consistently, thus draining the vehicle battery and mounting a deny-of-service (DoS) attack.[1] Bleuth defends against this abuse by using the fact that the transmission causes discharging and thus heating. Specifically, Bleuth uses the circuit in Fig. 17(c) to disable automatically the dongle's transmission, and trigger a siren, when the resettable PTC fuse heats up too much due to the transmission current.

Alarm Upon Removal of Dongle. Thieves who gained access to the passenger cabin may attempt to remove Bleuth's dongle from the auxiliary power outlet, trying to mount another DoS attack. Bleuth uses the alarm circuit shown in Fig. 17(d) to detect such illegitimate dongle removal.

8 POWER SUPPLY

Bleuth's power consumption consists of two parts: the power discharged from the 12V vehicle battery to form the PLC signal for driver authentication, and the power from Bleuth's power supply to run the immobilization service — both the dongle and the authenticator are equipped with rechargeable power supplies to ensure a 24/7 operation, which relieve drivers from the maintenance burden and eliminate the noises to the PLC caused by the power consumption of the dongle/authenticator. These power supplies operate in two states: disconnecting (or connecting) a power relay when the engine is stopped (or running). The dongle determines a stopped (or running) engine when observing V_{aux}<13V (or $V_{\text{aux}}\approx$15V); the authenticator concludes the same based on whether the battery is charging (i.e., a running engine) or not (i.e., a stopped engine). The charge of Bleuth's power supplies reduces the power to charge the vehicle battery, which may prevent the vehicle battery from being sufficiently charged to crank the engine. Fig. 18 plots the current distribution when driving a 2008 Honda Fit, showing the battery is not always charging during driving. This shows the alternator's power generation is not fully used on vehicles, corroborating the availability of power to charge Bleuth without affecting sufficient charging of vehicle battery. People in the US drive 52min per day [47], providing an ample opportunity to charge Bleuth.

9 EVALUATION

We have prototyped and evaluated Bleuth on 8 vehicles, as summarized in Table 3, of which V-1 is used as the default vehicle in our evaluation. Fig. 19 shows the installation of Bleuth on a 2018 Subaru XV as an example. We list a few key implementation details as follows: the low-power path is rated at 50A; the dongle/authenticator's sleep mode is implemented by disabling the ADC and blown-out

[1] Thieves with stolen keys may also operate other e-systems of the vehicle to drain the battery. This alarm circuit ensures Bleuth does not enlarge the attack surface.

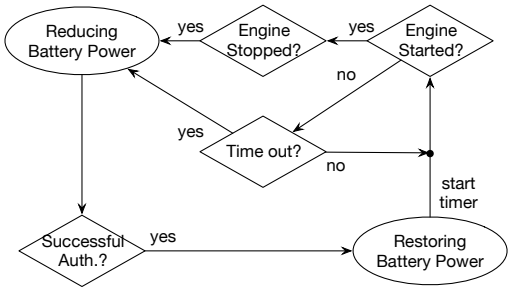


Fig. 16. Logic flow of `Bleuth`'s power control.

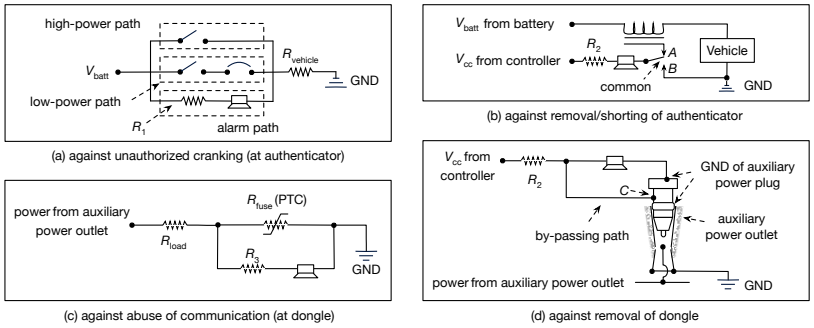


Fig. 17. `Bleuth` uses four alarm circuits to detect illegitimate operations.

Table 3: Performance of `Bleuth`'s PLC on 8 vehicles, obtained with 6,200 transmissions on each vehicle.

Index	Model	Type	Driver Authentication			Success Rate of Cranking	
			Detection Rate	Demodulation Accuracy	Success Rate	Authorized	Unauthorized
V-1	2008 Honda Fit	Gasoline	100%	100%	100%	100%	0%
V-2	2018 Subaru XV	Gasoline	99.97%	100%	99.97%	100%	0%
V-3	2018 Volvo XC60	Gasoline	99.94%	100%	99.94%	100%	0%
V-4	2017 VW Passat	Gasoline	99.98%	100%	99.98%	100%	0%
V-5	2019 Dodge Caravan	Gasoline	99.90%	100%	99.90%	100%	0%
V-6	2019 Nissan Frontier	Gasoline	100%	100%	100%	100%	0%
V-7	2015 Chevrolet Volt	Hybrid	100%	100%	100%	—	—
V-8	2016 Nissan Leaf	Electric	99.94%	100%	99.94%	—	—

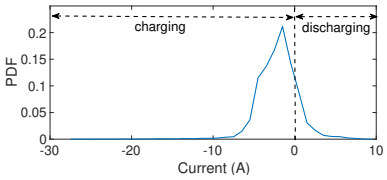


Fig. 18. The alternator's power generation capacity is not fully utilized.

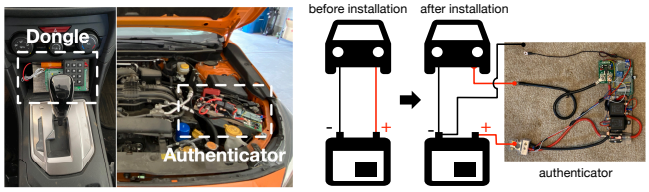


Fig. 19. Prototype and installation of `Bleuth` on Subaru XV.

detection of their MCUs; the dongle/authenticator is powered by Li-ion batteries whose recharging is implemented using TP5100; the driver-customized passcode is stored in the authenticator's non-volatile EEPROM; a pre-defined 4-digit reset code is also stored in the EEPROM, keying in of which triggers `Bleuth`'s initiation/reset mode to allow its un/installation on the vehicle and the customization/update of a driver's passcode.

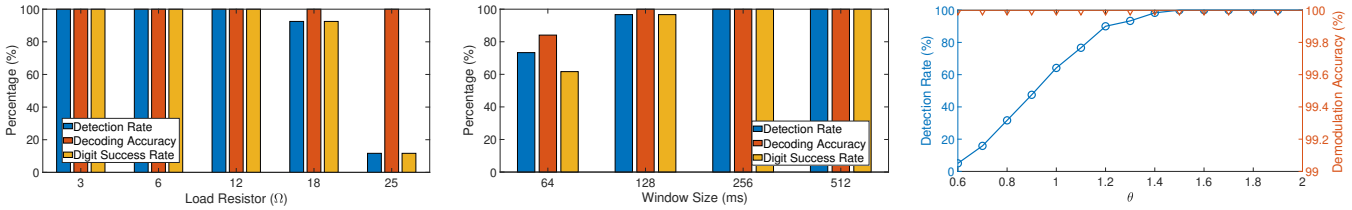
9.1 MFSK-based PLC

We evaluate the optimal configuration and communication performance of `Bleuth`'s PLC, as well as its robustness to the dynamics caused by vehicle e-operations and battery aging/voltage/temperature, using the following three metrics:

- *Detection Rate:* The authenticator's ability to detect the dongle's transmission of a symbol.
- *Demodulation Accuracy:* The authenticator's ability to accurately demodulate each detected transmission.
- *Success Rate:* The authenticator's ability to accurately receive the dongle's transmission of a symbol, which is jointly determined by the above two metrics.

Optimal Configuration. We first examine the effectiveness of our principles of steering the configurations of `Bleuth`'s PLC system, i.e., the amplitude of the current signal (determined by the load resistor R_{load}), the size of the moving window the authenticator uses to demodulate the current signal (T_{w}), and the duration for the dongle to transmit a symbol ($\theta \cdot T_{\text{w}}$). We have the dongle constantly transmit a symbol modulated at 100Hz while varying $\{R_{\text{load}}, T_{\text{w}}, \theta\}$, and check if the authenticator can accurately detect/demodulate the transmission/symbol from battery current. Fig. 20 summarizes the results. First, a smaller R_{load} improves the communication but increases power consumption, as observed with a 100% success rate when $R_{\text{load}} \leq 12$ (see Fig. 20(a)); although a 100% demodulation accuracy is achieved with R_{load} of 18Ω and 25Ω as well, miss detections did occur in such cases. Second, a window of ≥256ms achieves a 100% success rate (see Fig. 20(b)); too small a window not only misses transmission but also prevents accurate demodulation. Lastly, a larger θ increases the detection rate: a 92.5% detection rate is achieved with the minimum θ determined in Sec. 5 (i.e., θ=1.23); a 100% success rate is achieved with a slight increase of θ to 1.5 (Fig. 20(c)). These observations steer a default setting of R_{load}=12Ω, T_{w} =256ms, and θ=1.5 for our `Bleuth` prototype.

Communication Performance. We first use an automated script at the dongle to transmit numeric symbols "0"–"9", each 100 times. No wait time is inserted between two consecutive transmissions to magnify the potential interference, thus evaluating `Bleuth` in a harsh setting. `Bleuth` achieves a 100% success rate with these 100×10=1,000 transmissions. We have further evaluated `Bleuth` by keying in (and hence triggering the transmission of) the symbols "0"–"9" using the dongle's keypad. These inputs follow the 5 different patterns as depicted in Fig. 21, each for 10 rounds. All the 10×10×5=500 transmissions are successfully received by the



(a) Load resistance (b) Window size (c) TX coefficient

Fig. 20. Exploring the optimal configuration of `Bleuth`.

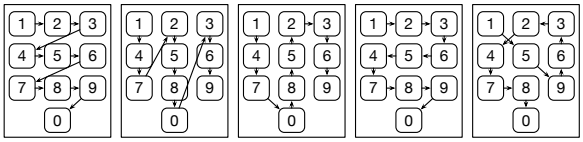


Fig. 21. Keying in with 5 different patterns.

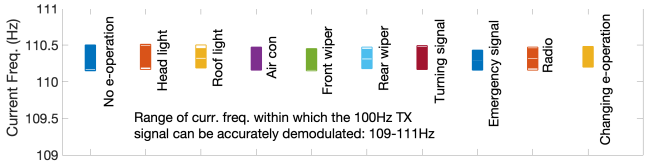


Fig. 22. `Bleuth`'s PLC is robust to the vehicle's e-operations.

authenticator. Lastly, we evaluate `Bleuth` on 8 vehicles with 31 randomly-generated 4-digit passcodes by transmitting each code 50 times (i.e., 31×4×50= 6, 200 transmissions) on each vehicle. Table 3 summarizes the results, showing `Bleuth`'s worse-case success rate of 99.9%.

Robustness to Noises/Dynamics. We have evaluated `Bleuth`'s robustness to the noises caused by the vehicle's e-system operations and battery aging/voltage/temperature.

E-System Operation. We first check if operations of a vehicle's e-systems interfere with the PLC communication. Fig. 22 plots the frequency of the decoded current when transmitting a 100Hz signal with different background e-operations, including the case when the e-operation is changed during the transmission, i.e., turning on sequentially the headlight, air-con, wiper, etc. The independency of decoded current frequency from background e-operations corroborates `Bleuth`'s robustness. We also checked if the e-operation will cause false detection of the authentication code. Each of the e-systems listed in Fig. 14 was operated for ≈10 minutes on the 8 vehicles in Table 3. No false detection occurred during these 10×10×8=800 minute experiments.

Battery Aging. We use two batteries of V-1 made in the year 2008 and 2018 to examine `Bleuth`'s robustness to battery aging. Having the dongle transmit a signal constantly at a fixed frequency, Fig. 23(a) plots the current frequency identified by the authenticator, exhibiting close results for the two batteries despite a 10-year difference in age.

Battery Voltage. We test `Bleuth`'s robustness to battery voltage variations — an indicator of battery's remaining capacity — by using a fully charged battery to transmit a 100Hz signal until the battery voltage drops to 9V, which is usually regarded as completely drained. Fig. 23(b) plots the results, showing `Bleuth`'s accurate demodulation of the transmission despite the low battery voltage.

Battery Temperature. We test `Bleuth`'s robustness to battery temperature variations by transmitting a 100Hz signal overnight in a cold outdoor environment, where the battery temperature dropped to as low as 24°F (see Fig. 23(c)). We observed no dependency between the communication performance and battery temperature.

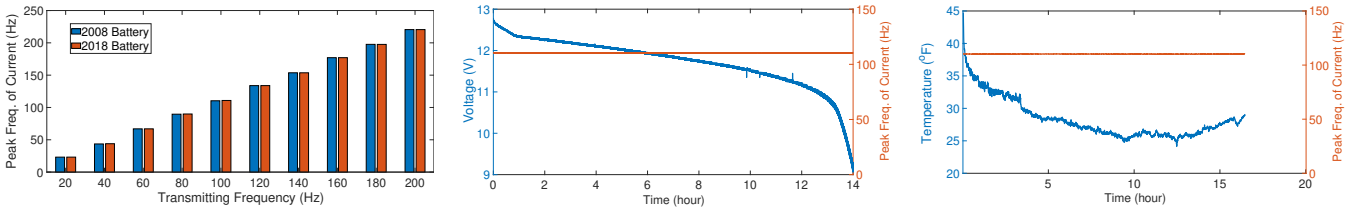
9.2 Power/Drivability Control

We now investigate `Bleuth`'s control of the battery's power capacity, hence dis/enabling the cranking of engine. We first crank the engine without passing the authentication, i.e., when only the low-power path is connected, as shown in Fig. 24(a). After turning on the vehicle, we activate (cumulatively) some e-systems of the vehicle, like headlight, fan, rear wiper, and emergency signal. The low-power-mode battery can provide sufficient power to operate these e-systems, as shown in the first 26s of Fig. 24(a). We then attempted to crank the engine using the low-power-mode battery, which failed instantaneously due to the overloaded and then disconnected low-power path. Next, we crank the engine with a low-power-mode battery after turning off as many e-systems as possible (and hence reducing the power necessary to complete the cranking), which failed as well (see Fig. 24(b)). Note that it takes a longer time for the engine-cranking to fail than that in Fig. 24(a), because of the reduced power requirement. Lastly, we crank the engine after passing the authentication and thus with the high-power path/battery. We kept the e-systems on to increase the total power needed. This cranking with the high-power-mode battery was successful, as shown in Fig. 24(c). We have repeated the same experiments on V1–V6 in Table 3 to find all crankings with low-power-mode battery failed, while those with high-power battery succeeded, corroborating `Bleuth`'s reliable vehicle immobilization by controlling the battery's power capacity. Although we have not tested the power controller on HEVs (e.g., V-7 and V-8 in Table 3) due to their high voltage (hence safety risk), the philosophy of using battery power as the control knob to dis/enable driving still applies — HEVs also require a (relatively) large power to activate all related e-modules to initialize driving.

9.3 Power Consumption

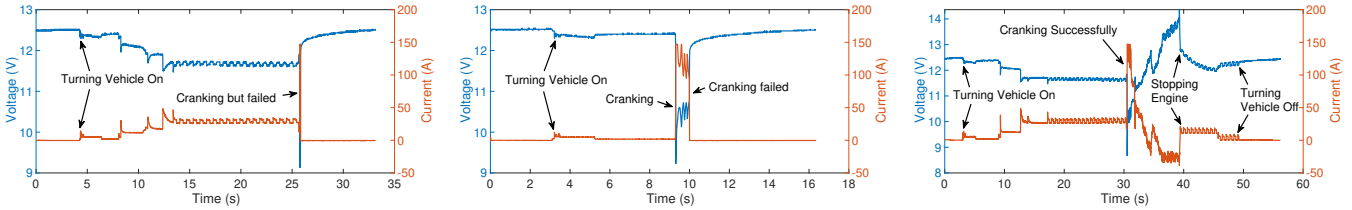
We examine `Bleuth`'s power consumption from two perspectives: the power discharged from the vehicle battery to form the PLC signal for driver authentication, and the power from `Bleuth`'s power supply to run the immobilization service.

Power Drawn from Automotive Battery. According to the optimal PLC configuration identified in Sec.9.1, a power of ≈12W is required for the authentication, which is smaller than that of



(a) Age (b) Voltage (c) Temperature

Fig. 23. `Bleuth`**'s PLC is robust to battery age/voltage/temperature.**



(a) Unsuccessful cranking (with e-syst. on) (b) Unsuccessful cranking (with e-syst. off) (c) Successful cranking (with e-syst. on)

Fig. 24. `Bleuth`**'s power controller regulates effectively the battery's power capacity and dis/enables the cranking of engine.**

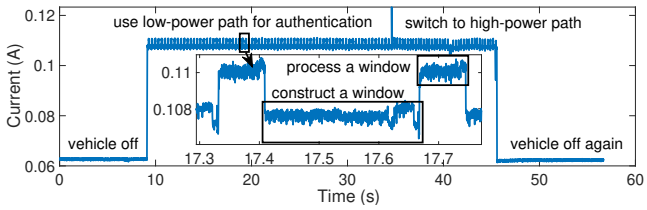


Fig. 25. Power consumption of `Bleuth`**'s authenticator.**

cranking the engine (i.e., 2–9kW [5]) by over two orders of magnitude, indicating almost no chance for the authentication to drain a battery from strong enough to deficient for a successful cranking of the engine, especially considering the battery's recovery effect [56] and `Bleuth`'s alarm against abuse of communication. To shed more light on the transmission power consumption, let us consider a 16Ah battery and an idle current of 2A (see Fig. 7): with a 25% standard depth-of-discharge of automotive battery, the battery can transmit the number of authentication symbols equal to:

$$16 \times 25\%/(V_{\text{aux}}/R_{\text{load}}/2 + I_{\text{idle}})/(\theta \cdot T_{\text{w}} \times 5/4) \approx 12,000.$$

Power Drawn from Bleuth's Power Supply. Fig. 25 plots the power consumption of `Bleuth`'s authenticator, showing a 62mA sleep-mode current when the vehicle is kept off, 107mA to collect the current at 500Hz and keep connected the relay of the low/high-power path, and an additional 3mA to process the collected current data. The dongle consumes much less power than the authenticator, i.e., drawing a 16mA current when transmitting in addition to the MCU's consumption in sleep mode. Note that MCU's sleep-mode power consumption can be reduced by using low-power controllers, e.g., to 0.023mA with Arduino ProMini.

9.4 User Study

Opinion on Key-based Immobilizers. We surveyed 30 car owners recruited via Amazon MTurk and identified 10 limitations of keys/keyfobs from them. We then asked another 582 participants to rate each of these limitations with a score of 1–5, with "5" for

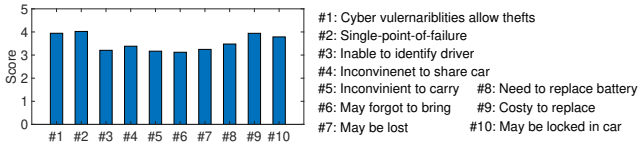


Fig. 26. Cyber vulnerabilities and single-point-of-failure are the top concerns of car owners on key-based immobilizers.

"strongly agree", and "1" for *"strongly disagree"*. Fig. 26 plots the average ratings, showing that cyber vulnerability is the top concern of car owners about keys/keyfobs. Also, the participants view auto theft as a really bad problem with an average score of 4.1/5.

User Acceptance. We have also instructed the above 582 car owners on `Bleuth`'s use-cases and asked if they are willing to install `Bleuth` in their cars. The results show an average rating of 4.1/5 on users' acceptance of `Bleuth`.

Usability Study. We also evaluate the usability of `Bleuth` with *System Usability Scale* (SUS), a metric to assess industry products/services, which contains 10 standard questions and is known to provide reliable results even with a small sample size [51]. We conducted this usability study virtually (due to COVID-19) by playing a demo video of `Bleuth` [18] to 16 participants, answering their questions if any, and then collecting their feedback using the standard questions of SUS. We then calculated the SUS score based on their feedback to find `Bleuth` achieving a score of 92.5, which represents *"excellent"* usability according to [4].

10 DEFENSES AGAINST AUTO THEFTS

Next, we analyze `Bleuth`'s security against auto-thefts. We consider `Bleuth`'s anti-theft protection successful if it thwarts the theft attempts, or, in the worst case, detects and deters theft attempts by activating a siren alarm. We will discuss the extension of `Bleuth` to other forms of thwarting theft attempts in Sec. 11.

Against Bleuth-Oblivious Attackers. As a second-factor vehicle immobilizer without using wireless communication or IVNs,

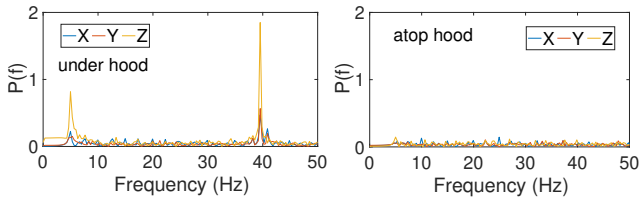


Fig. 27. Magnetic field collected under and atop engine hood.

Bleuth is resistant to most of Bleuth-oblivious attackers listed in Sec. 3, except towing and carjacking. Note that it is commonly advised to give up the vehicle without resistance in the case of carjacking, although Bleuth remains intact so long as the authenticating code is kept secret from robbers. Bleuth's alarms can also scare away robbers in the case of carjacking.

Against Bleuth-Aware Attackers. Summarized below are possible ways for Bleuth-aware attackers to hack Bleuth.

Attack-1: Removing Bleuth's authenticator (dongle) from the vehicle (from the auxiliary power outlet), or shorting the authenticator from the vehicle. Bleuth's alarm modules detect such removals/shorting and then turn on a siren. Bleuth could also be integrated with vehicles if it is provided as a before-market product, in which case Bleuth will not be exposed to attackers, thus voiding the removal attacks.

Attack-2: Mounting DoS attacks by abusing Bleuth's PLC to drain the vehicle battery. Bleuth's alarm upon PLC abuse will automatically/physically disable this attack after excessive transmissions owing to the heating of, or blowing out PTC fuse.

Attack-3: Mounting DoS attacks by physically tampering with Bleuth's authenticator. Keeping the vehicle battery in the low-power mode by default, Bleuth's anti-theft capability remains intact even if attackers break Bleuth physically, in which case the battery would be either disconnected or connected in low-power mode, from/to the vehicle, both of which prevent the cranking of the engine (and hence the theft).

Attack-4: Evading Bleuth by connecting a second battery in parallel with the original battery. Although feasible in theory, this attack is impractical because the connection of the original battery to Bleuth/vehicle cannot be disrupted *during* and *after* the installation of the second battery — otherwise, the alarm upon removal of authenticator will be triggered.

Attack-5: Stealing the passcode by: (i) sneakily breaking into the vehicle to install a non-invasive current sensor on the battery to monitor its current, (ii) decoding the passcode using the collected current after a sufficient number of successful authentications by the intended driver, (iii) gaining access to the vehicle again and using the decoded passcode to steal the vehicle. Bleuth's randomization of modulation frequency makes it difficult for adversaries to decode the passcode even after stealthily collecting the current signal with the above tedious procedure — a given authentication symbol will be modulated with frequency f_i $(i = 0, 1, \ldots, 9)$ with the possibility of 1/10.

Attack-6: Stealing the passcode by analyzing the electro-magnetic field generated by the communication signal/current. Fig. 27 plots the frequency of the magnetic field collected by attaching a magnetic sensor (i) besides the battery in the engine cabin and (ii) on top of the engine hood, during which the dongle is transmitting data at 20Hz — although the 20Hz current signal can be observed from the ≈40Hz magnetic field in close proximity of the battery, it cannot be observed from outside of the engine cabin. As a result, attackers have to collect the magnetic field data from under the hood and very close to the battery, making it similar to Attack-5, but even more difficult because attackers must also decode the current frequency from the collected magnetic field data.

11 EXTENSIONS

Authenticating Drivers Using Biometrics. Bleuth is orthogonal to the specific form of authentication code and can be implemented to authenticate drivers using other information than a passcode, as we have corroborated by adding a PM10A fingerprint sensor to the dongle (see [18]) — the dongle transmits the customized passcode when the bio-fingerprint-based authentication is successful. Also, Bleuth can be implemented to send the extracted fingerprint features for authentication.

Deterring Theft Attempts. Besides the alarm siren, Bleuth can also be implemented — following the same logic circuit as in Fig. 17 — in other ways to deter theft attempts, such as sending alert messages to car owners' mobile phones or an OEM-provided vehicle service (e.g., GM's OnStar). In particular, the integration of Bleuth with an OEM service will allow the timely activation of vehicle tracking, facilitating the recovery of stolen vehicles even if adversaries were able to void Bleuth. Clearly, this extension requires partnerships with automakers, which will also facilitate Bleuth to become a before-market product.

Controlling Vehicle Entry. Bleuth can be extended further to provide an entry control to vehicles, e.g., by integrating the dongle with door(s). The extended Bleuth will improve and have the potential for replacing existing car keys/keyfobs. This extension is based on the fact that unlocking the vehicle doors requires an electric current of several amperes (e.g., 7.6A in Fig. 14), while monitoring a parked vehicle requires only in the order of milli-ampere [5, 7] — we can connect the vehicle and the battery with a very-low-power path which is only strong enough to support these monitoring functions but not unlocking doors, and switch to the low-power path (and hence allow unlocking doors) after validating a driver's entry privilege using the PLC. We have already implemented and validated this extension (see [18]).

12 CONCLUSION

We presented Bleuth, a vehicle (im)mobilizer that neither involves any wireless communication nor requires access to the in-vehicle network. It uses the vehicle battery *as sensor* to validate a driver's identity, and *as controller* to dis/enable the cranking of the engine based on the validation results. Bleuth offers a novel way of physically isolating systems from common cyber attack vectors, laying a foundation for physical security in an increasingly cyberized/connected world.

ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers and the shepherd for their insightful feedback.

REFERENCES

[1] A. I. Alrabady and S. M. Mahmud. 2003. Some attacks against vehicles' passive entry security systems and their solutions. *IEEE Transactions on Vehicular Technology* 52, 2 (2003), 431–439.

[2] Donkyu Baek, Yukai Chen, Alberto Bocca, Alberto Macii, Enrico Macii, and Massimo Poncino. 2018. Battery-Aware Energy Model of Drone Delivery Tasks. In *ISLPED'18*.

[3] N. Bahrani and V. Gaudet. 2014. Measurements and channel characterization for in-vehicle power line communications. In *ISPLC'14*.

[4] Aaron Bangor, Philip Kortum, and James Miller. 2018. Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale. *Journal of Usability Studies* 4, 3 (2018), 114–123.

[5] Robert Bosch. 2014. *Bosch Automotive Electrics and Automotive Electronics*. Springer.

[6] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *USENIX Security'11*.

[7] K. T. Cho, K. Shin, Y. S. Kim, and B. H. Cha. 2020. Off is Not Off: On the Security of Parked Vehicles. In *CNS'20*.

[8] Kyong-Tak Cho and Kang G. Shin. 2016. Error Handling of In-vehicle Networks Makes Them Vulnerable. In *CCS'16*.

[9] Kyong-Tak Cho and Kang G. Shin. 2016. Fingerprinting Electronic Control Units for Vehicle Intrusion Detection. In *USENIX Security'16*.

[10] Kyong-Tak Cho and Kang G. Shin. 2017. Viden: Attacker Identification on In-Vehicle Networks. In *CCS'17*.

[11] DC. 2022. District Crime Data. https://mpdc.dc.gov/page/district-crime-data-glance.

[12] New York DMW. 2022. DMV WARNS MOTORISTS OF RISE IN AUTO THEFTS IN NYC AND STATEWIDE. https://dmv.ny.gov/press-release/press-release-07-13-2021.

[13] Mike Epstein. 2022. How to Keep Your Tesla From Getting Stolen. https://lifehacker.com/how-to-keep-your-tesla-from-getting-stolen-1829940649.

[14] A. Francillon, B. Danev, and S. Capkun. 2011. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. In *NDSS'11*.

[15] DAN GOODIN. 2022. Five months after returning rental car, man still has remote control. https://arstechnica.com/information-technology/2019/10/five-months-after-returning-rental-car-man-still-has-remote-control/.

[16] Andy Greenberg. 2022. Hackers Can Steal a Tesla Model S in Seconds by Cloning Its Key Fob. https://www.wired.com/story/hackers-steal-tesla-model-s-seconds-key-fob/.

[17] Leonid Grustniy. 2022. Hacking smart car alarm systems. https://usa.kaspersky.com/blog/hacking-smart-car-alarm-systems/17362/.

[18] Liang He and Kang Shin. 2022. Demo video of Bleuth. https://youtu.be/OnWs1rVZlLU.

[19] Liang He and Kang Shin. 2022. Description of Bleuth's alarm and power supply. https://www.dropbox.com/s/sps8tmvcwr4fpmn/Appendix.pdf?dl=0.

[20] Liang He, Yuanchao Shu, Youngmoon Lee, Dongyao Chen, and Kang Shin. 2021. Authenticating Drivers Using Automotive Batteries. In *UbiComp'21*.

[21] Aaron Holmes. 2022. Elon Musk says the Tesla 2020 Roadster "maybe won't need a key at all". https://www.businessinsider.com/elon-musk-tweets-tesla-roadster-might-not-need-key-2019-11.

[22] Bill Howard. 2022. Volvo's truly keyless entry: your smartphone. https://www.extremetech.com/extreme/224665-volvos-truly-keyless-entry-your-smartphone.

[23] Shengtuo Hu, Qi Alfred Chen, Jiachen Sun, Yiheng Feng, Z. Morley Mao, and Henry X. Liu. 2021. Automated Discovery of Denial-of-Service Vulnerabilities in Connected Vehicle Protocols. In *USENIX Security 21*.

[24] Insurance Information Institute. 2022. Facts and Statistics: Auto theft. https://www.iii.org/fact-statistic/facts-statistics-auto-theft.

[25] Kyungho Joo, Wonsuk Choi, and Dong Hoon Lee. 2020. Hold the Door! Fingerprinting Your Car Key to Prevent Keyless Entry Car Theft. In *NDSS'20*.

[26] M. Kasper, T. Kasper, A. Moradi, and C. Paar. 2009. Breaking KeeLoq in a Flash: On Extracting Keys at Lightning Speed. In *AFRICACRYPT 2009*.

[27] Arslan Khan, Hyungsub Kim, Byoungyoung Lee, Dongyan Xu, Antonio Bianchi, and Dave (Jing) Tian. 2021. M2MON: Building an MMIO-based Security Reference Monitor for Unmanned Vehicles. In *USENIX Security 21)*.

[28] Taegyu Kim, Chung Hwan Kim, Junghwan Rhee, Fan Fei, Zhan Tu, Gregory Walkup, Xiangyu Zhang, Xinyan Deng, and Dongyan Xu. 2019. RVFuzzer: Finding Input Validation Bugs in Robotic Vehicles through Control-Guided Testing. In *USENIX Security 19*.

[29] Marcel Kneib and Christopher Huth. 2018. Scission: Signal Characteristic-Based Sender Identification and Intrusion Detection in Automotive Networks. In *CCS'18*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3243734.3243751

[30] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. 2010. Experimental Security Analysis of a Modern Automobile. In *S&P'10*.

[31] X. Li, Y. Yu, G. Sun, and K. Chen. 2018. Connected Vehicles' Security from the Perspective of the In-Vehicle Network. *IEEE Network* 32, 3 (2018), 58–63.

[32] M. Lienard, M. O. Carrion, V. Degardin, and P. Degauque. 2008. Modeling and Analysis of In-Vehicle Power Line Communication Channels. *IEEE Transactions on Vehicular Technology* 57, 2 (2008), 670–679.

[33] Pandora London. 2022. How cars are stolen through OBD port theft and key cloning. https://www.youtube.com/watch?v=dvmSOEKfkug.

[34] Mulong Luo, Andrew C. Myers, and G. Edward Suh. 2020. Stealthy Tracking of Autonomous Vehicles with Cache Side Channels. In *USENIX Security 20*.

[35] Nate Lynn. 2022. Report shows sharp increase in metro Denver auto thefts. https://www.9news.com/article/life/automotive/auto-theft-report/73-913f3078-6087-4510-a24c-114a5674bf2b.

[36] T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi. 2012. A Method of Preventing Unauthorized Data Transmission in Controller Area Network. In *VTC Spring'12*.

[37]]caninjection Charlie Miller and Chris Valasek. [n. d.]. CAN Message Injection. http://illmatics.com/can%20message%20injection.pdf.

[38] Charlie Miller and Chris Valasek. 2011. Adventures in automotive networks and control units. In *DEFCON'11*.

[39] Charlie Miller and Chris Valasek. 2015. Remote exploitation of an unaltered passenger vehicle. In *Black Hat USA'15*.

[40] Pandora. 2022. Pandora Car Alarms. https://www.pandoracaralarm.com/.

[41] Alberto Pittolo, Marco De Piante, Fabio Versolatto, and Andrea M. Tonello. 2016. In-Vehicle PLC: In-Car and In-Ship Channel Characterization. *CoRR* abs/1603.02260 (2016). arXiv:1603.02260

[42] West Midlands Police. 2022. Relay attack. https://www.youtube.com/watch?v=8pffcngJJq0.

[43] Matt Posky. 2022. Automakers Working Feverishly to Make Car Keys Disappear. https://www.thetruthaboutcars.com/2018/06/automakers-feverishly-working-getting-rid-keys/.

[44] Madelyn Reese. 2022. San Jose car thefts on the rise, beating national trends. https://sanjosespotlight.com/san-jose-car-thefts-on-the-rise-beating-national-trends/.

[45] Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. 2010. Security and Privacy Vulnerabilities of In-car Wireless Networks: A Tire Pressure Monitoring System Case Study. In *USENIX Security'10*.

[46] BERTEL SCHMITT. 2022. Top OTA Expert Shows How State Actors Hack into Your Car and What Happens Next: "People Will Die". https://www.thedrive.com/tech/29120/top-ota-expert-shows-how-state-actors-hack-into-your-car-and-what-happens-next-people-will-die.

[47] Sean Szymkowski. 2022. Americans are spending more time than ever behind the wheel. https://www.thecarconnection.com/news/1121763_americans-are-spending-more-time-than-ever-behind-the-wheel.

[48] N. Taherinejad, R. Rosales, S. Mirabbasi, and L. Lampe. 2011. A study on access impedance for vehicular power line communications. In *ISPLC'11*.

[49] John Tallodi. 2022. Only One Carmaker Is Impossible To Hack. https://carbuzz.com/news/only-one-carmaker-is-impossible-to-hack.

[50] Trustonic. 2022. Top 10 Security Challenges in the Automotive Industry for Connected Cars. https://www.trustonic.com/news/blog/top-10-security-challenges-for-connected-cars/.

[51] Usability. 2022. System Usability Scale. https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html.

[52] R. Verdult, F. D. Garcia, and B. Ege. 2015. Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer. In *USENIX Security'15*.

[53] Viper. 2022. Viper Vehicle Security. https://www.viper.com/.

[54] ANDREW WENDLER. 2022. Lincoln Phone As A Key Technology Aims to Eliminate Traditional Key Fobs. https://www.caranddriver.com/news/a28751902/lincoln-phone-as-a-key/.

[55] J. Wetzels. 2014. Broken keys to the kingdom: Security and privacy aspects of RFID-based car keys. *CoRR* abs/1405.7424 (2014).

[56] Wikipedia. 2022. Recovery effect. https://en.wikipedia.org/wiki/Recovery_effect.

[57] T. Yang, L. Kong, W. Xin, J. Hu, and Z. Chen. 2012. Resisting relay attacks on vehicular Passive Keyless Entry and start systems. In *ICFSKD'12*.