Hardware Fingerprinting as an Untrustworthy Primitive for Device Authentication: The Wraith Attack

Author names withheld (working preprint)
Affiliation to be finalized before arXiv submission

Abstract—Physical layer device fingerprinting has become a leading proposal for retrofitting authentication onto shared medium buses that were designed without it. On the automotive CAN bus, the avionics MIL-STD-1553 bus, and ARINC 429, a transmitter is identified by the analog voltage or timing signature that manufacturing variation imprints on its signals, and recent studies report device identification accuracies as high as 100%, which is driving adoption in both research and commercial products. We argue that this entire class of defense rests on an assumption that does not hold on a shared medium: that a device's physical signature is a secret. It is not. The signature is broadcast on every transmission, and any adversary connected to the same bus observes the identical signal the defender measures. We formalize this as measurement symmetry and show that no feature extraction function can separate a legitimate transmission from a faithful recording of it once the attacker's sampling hardware matches or exceeds the defender's, a condition that commodity instruments now satisfy easily. The corresponding belief, stated in the literature as recently as 2026, that an adversary with full bus access cannot reproduce a device's analog voltage identity, is therefore wrong in principle and not merely in practice: by Proposition 1, an adversary who samples the shared signal at no less than the defender's rate and resolution reproduces every voltage feature the defender can compute. We demonstrate the consequence end to end on MIL-STD-1553, the most safety critical and most heavily defended of these buses, using commodity capture and replay hardware. Waveforms captured from a legitimate test platform were re-emitted onto a physical 1553 bus through a 14 bit digital to analog converter; more than 50 replayed transmissions were accepted as valid by independent test equipment, decoded identically to the originals, with zero protocol errors. Because the same shared medium symmetry governs CAN, MODBUS, LIN, and ARINC 429, we argue that fingerprinting is structurally unfit as an authentication primitive on any of them, and that only secret based mechanisms address the root cause: a cryptographic message authentication code, with freshness bound under the same key, cannot be forged or replayed without the key, whereas any defense reducible to an observable property of the signal can. We name the attack Wraith: Waveform Replay Attack Imitating Transmitted Hardware.

Index Terms—hardware fingerprinting, physical layer authentication, replay attack, shared medium buses, MIL-STD-1553, CAN bus, avionics security, Wraith

I. Introduction

A recurring idea now shapes how the security community proposes to protect legacy control buses. Many of these buses, including the automotive CAN bus, the avionics MIL-STD-1553 bus, and ARINC 429, were designed decades ago for determinism and fault tolerance, not for a threat model, and they carry no authentication. The proposed remedy is to authenticate devices by their physical behavior. Each transmitter, the argument goes, imprints a distinctive analog signature on its signals through minor and unavoidable manufacturing variation, so a classifier trained on that signature can tell which device sent a message and can flag any device that does not belong. This is hardware fingerprinting, and it is attractive precisely because it promises authentication without touching the protocol, the wiring, or the installed equipment.

The reported results are strong enough to drive adoption. On MIL-STD-1553, Evcil et al. [1] report 100% device classification accuracy from raw synchronization voltage samples captured on a real helicopter avionics platform, and Levy et al. [2] report 99.45% accuracy from convolutional features as part of their ANoMili defense in depth system. On CAN, voltage and clock based schemes report comparable numbers [3]–[5]. Commercial products now market physical layer fingerprinting as an intrusion detection layer for military buses. The common promise is that a device cannot be impersonated because its analog identity cannot be reproduced.

We show that this promise is unfounded, and that the reason is structural rather than a limitation of any particular classifier. The premise underlying every fingerprinting proposal on a shared bus is that the physical signature is intrinsic to the hardware and cannot be reproduced by a different device. The premise treats manufacturing variation as though it were a secret. Yet on a shared medium the signature is not secret in any sense that matters. It is broadcast in full on every transmission, and every terminal on the bus, including an adversary, observes the same physical waveform that the defender measures. The defender and the attacker are symmetric observers of one signal. An attacker therefore does not need to forge the fingerprint. The attacker needs only to record it, and to play it back. We formalize this observation as measurement symmetry in Section III and show that it holds against any feature the defender can compute. The consequence is that hardware fingerprinting can be bypassed by a recording adversary, and is therefore not the authentication guarantee it is claimed to be.

To make the argument concrete, and to test it against the strongest available form of the defense, we demonstrate the break on MIL-STD-1553. This bus is the hardest case for an attacker and the most consequential one to get right: it carries safety critical traffic on military aircraft, ships, spacecraft, and weapons systems [6]; its fingerprinting defenses are the most systematically evaluated in the literature, with reported accuracy up to 100% [1]; and it is impedance controlled and transformer coupled, which makes its signals cleaner and, as we explain, easier to reproduce than a noisy wireless channel. Using a capture and replay platform we call BusSpectre, assembled from a commodity USB oscilloscope with a 14 bit digital to analog converter and an inexpensive 1553 protocol board, we captured waveforms from a legitimate test platform and reemitted them onto a physical 1553 bus. Independent test equipment accepted more than 50 replayed transmissions as valid, decoded them identically to the originals, and reported no protocol errors. Because fingerprinting reads only the synchronization region of a message, capturing that region lets the adversary go beyond repetition and present a captured device's identity while carrying content the device never sent, a point we return to because it is what makes naive freshness defenses fail.

The demonstration is on one bus, but the conclusion is not confined to it. Measurement symmetry is a property of shared medium topology, not of MIL-STD-1553. The same reasoning applies to CAN, MODBUS, LIN, and ARINC 429, all of which are broadcast, multi drop, and unauthenticated or weakly so, and all of which have been proposed as candidates for physical layer fingerprinting [3], [4], [7]. The automotive literature has already walked this path once: clock based fingerprinting [3] was evaded by clock cloaking [8], and voltage based fingerprinting [4], [5] was evaded by the DUET attack [9]. Our contribution is to name the principle that unifies these results, to prove it from the measurement model, and to show that the most heavily defended bus of all is no more resilient than its automotive counterparts. The uncomfortable implication for practitioners is that a defense currently being sold and deployed as authentication is, on every shared bus we examine, reducible to a recording.

A. Contributions

C1. We state and prove measurement symmetry (Section III): on a shared medium, any feature a defender can extract from a device's transmission can be reproduced by an adversary whose sampling hardware matches or exceeds the defender's, so voltage and timing fingerprinting cannot serve as an authentication primitive. We show the associated cost asymmetry is permanent, because the attacker can filter residual replay artifacts more cheaply than the defender can measure them.

C2. We demonstrate the consequence on physical MIL-STD-1553 hardware (Section V). Using Wraith and the BusSpectre platform, built from commodity equipment, more than 50 captured waveforms replayed through a 14 bit converter were accepted as valid MIL-STD-1553 communications by independent test equipment, with identical decoding and zero protocol errors. A single captured message suffices, and because the fingerprint lives in the synchronization region, the same capture supports forging messages the device never sent under its own identity.

C3. We generalize the result by structural analogy to CAN, MODBUS, LIN, and ARINC 429 (Section VI), unifying the prior automotive evasion results and the avionics case under a single principle rather than a collection of protocol specific tricks.

C4. We specify the countermeasures that address the root cause (Section VII) and, importantly, explain why the obvious partial measures do not: a plaintext sequence number is forgeable by the same mechanism that forges the message, so freshness has force only when it is authenticated under a per device secret key.

II. The Fingerprinting Doctrine and Why It Is Trusted

A. What Hardware Fingerprinting Claims

Hardware fingerprinting rests on a genuine and well documented physical fact. Two transmitters of the same model, built from the same design, produce measurably different analog waveforms because component tolerances, layout parasitics, and transceiver characteristics differ slightly between units. As Evcil et al. put it, each transmitter demonstrates distinct signal characteristics due to minor defects during production [1]. A classifier trained on these characteristics can, under benign conditions, identify the transmitting device with high accuracy. Two feature families appear in the literature. The first uses raw voltage samples of the synchronization region directly as a feature vector [1], [10]. The second derives physical descriptors from the same waveform, such as rise time, overshoot, ringing frequency, and spectral shape, and classifies on those [2]. Both families operate on the same underlying observable: the voltage trace of the transmission.

The reported performance is high. On MIL-STD-1553, Stan et al. [10] introduced voltage fingerprinting of sync bits; Evcil et al. [1] conducted the most systematic evaluation to date, comparing eight machine learning methods on raw sync voltage from a real helicopter platform and reporting 100% accuracy for all supervised classifiers across their attack scenarios, with accuracy retained down to 25 voltage samples per sync; and Levy et al. [2], [11] built ANoMili, a defense in depth system whose per device classifier reports 99.45% accuracy and which retrains continuously to track environmental drift. On CAN, Cho and Shin [3] fingerprinted electronic control units by clock skew, while Choi et al. [5] and Kneib and Huth [4] exceeded 99% accuracy from voltage. The claim is current, not historical. Writing in 2026, Yang et al. [12] authenticate CAN-FD control units by voltage hardware

fingerprints, report above 99% single frame recognition and 100% attack type identification, and argue that an adversary with full bus access cannot forge a device's voltage identity because its analog properties cannot be reproduced in software. Their threat model does not consider an adversary who reproduces those properties in hardware, by recording the signal and replaying it, which is the gap we exhibit, and Section VI shows that their own measurement setup makes the contradiction exact. For ARINC 429, Gilboa-Markevich and Wool [7] found that hand crafted raw voltage features gave the best fingerprinting results. The idea has also reached the market: Sital Technology's BRM1553D-SnS core learns physical layer fingerprint parameters during a training phase and then monitors for deviations, which is exactly the approach we examine.

B. The Shared Medium and the Implicit Secret

Every bus named above shares one property that the fingerprinting doctrine quietly depends on and never secures. The medium is shared. MIL-STD-1553 is a dual redundant 1 MHz serial bus on which terminals transmit and receive over a common transformer coupled pair, and every connected terminal sees every word [13], [14]. CAN is a broadcast multi drop differential pair on which all nodes observe all frames. In each case the defender extracts its fingerprint from a signal that is, by construction, delivered in full to every device on the bus. The physical signature is therefore not a secret held by the legitimate device. It is public information, retransmitted on every message, available to anyone with a probe on the wire.

This is the crux of the argument developed in Section III. A secret based authenticator, such as a message authentication code, remains secure even when the adversary can read every message, because the adversary lacks the key. A fingerprint based authenticator has no such reserve. What the defender uses to decide identity is the very thing the adversary already holds a perfect copy of. The only quantity that could distinguish the legitimate transmission from a recording of it is the fidelity of the two measurement and reproduction chains, and, as we show, that quantity favors the attacker.

C. MIL-STD-1553 in Brief

We include only the detail needed for the attack. MIL-STD-1553 [13] is a command and response protocol. A single Bus Controller issues commands to Remote Terminals, each addressed by a 5 bit field, and terminals reply in assigned time slots. A passive Bus Monitor can record all traffic without transmitting. Messages are sequences of 20 bit words, each carrying a 3 bit time synchronization field, 16 content bits, and 1 parity bit, using Manchester II encoding (Fig. 1). The synchronization field is what fingerprinting classifiers evaluate. At the 1 MHz bit rate it spans roughly 3 microseconds, though its exact duration scales with the transmitter and

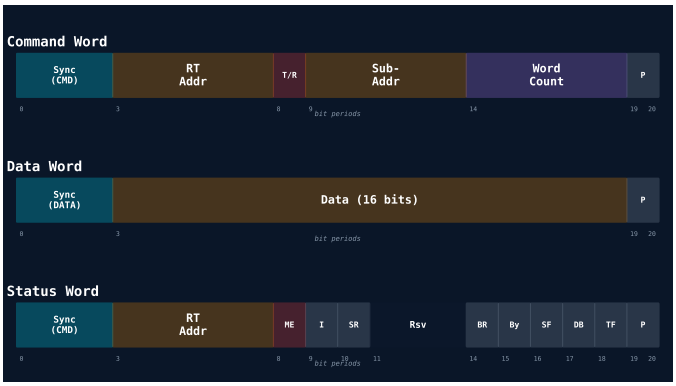

Fig. 1. MIL-STD-1553 word formats. Each word is 20 bit times: a 3 bit time sync field, 16 content bits, and 1 parity bit. Command and Status words use a positive then negative sync; Data words use the opposite. The sync field is the analog region that voltage fingerprinting measures.

the sampling configuration, and its analog shape is set by the transmitting hardware's electrical characteristics. The protocol provides no authentication, encryption, or integrity protection. Device identity is asserted by the address field alone, which any device with bus access can set to any value.

III. Measurement Symmetry: The Structural Flaw

The failure of voltage fingerprinting against a recording adversary is not a weakness of one classifier or one feature set. It follows from the measurement model itself.

Proposition 1 (Measurement Symmetry). Let F be any feature extraction function computable from voltage samples $V = \{v_1, \ldots, v_N\}$ captured at sample rate f_s with resolution b bits. If a defender can compute $F(V)$ from bus measurements, then an adversary with capture hardware of resolution $b' \geq b$ and sample rate $f'_s \geq f_s$ can record samples V' such that $|F(V) - F(V')| \leq \epsilon$, where ϵ is bounded by the combined quantization error of the two conversion stages. Consequently, any classifier C trained to accept $F(V)$ with tolerance $\delta > \epsilon$ also accepts $F(V')$.

The proposition follows directly from shared medium topology. Defender and adversary observe the same physical signal on the same bus and differ only in their sampling parameters. When the adversary's converter equals or exceeds the defender's, the reproduction error ϵ is smaller than the intra device variance δ that any usable classifier must already tolerate, because a real device's own successive transmissions are not bit identical. No choice of F escapes this bound. Raw voltage samples, rise and fall times, spectral centroid, ringing descriptors, and any feature yet to be invented are all functions of the same observable voltage trace, so a faithful copy of the trace carries all of them at once. This is why replay, and not any form of computational imitation, is the operative attack: the adversary does not model or approximate the

fingerprint, the adversary re-emits the exact signal that produced it.

The condition $b' \geq b$, $f'_s \geq f_s$ is not a stretch; on these buses it is the normal case. ANoMili's embedded oscilloscope samples at 32 MHz with 8 bit depth [2], and typical benchtop instruments in the class Evcil et al. describe are 8 bit. The commodity Analog Discovery 3 we use captures at up to 125 MS/s with 14 bit resolution, which is 64 times the voltage resolution of ANoMili's instrument and at least the sample rate of either defender, 1.25 times Evcil et al.'s 100 MS/s and nearly four times ANoMili's 32 MHz. The adversary therefore records the fingerprint at higher fidelity than the defender can measure it, and any artifact the adversary's own output introduces falls below the defender's noise floor.

This is not a new observation in isolation. Danev et al. [15] showed in 2010 that physical layer identification of wireless devices reaches nearly 100% impersonation accuracy under replay, and their survey [16] established that both modulation based and transient based identification fall to a replaying adversary whose hardware matches the defender's. Urbina et al. [17] formalized the analogous point for cyber physical anomaly detection at CCS 2016: a sufficiently capable adversary can always remain within the accepted region. What has been missing is the recognition that wired control buses are the easy case for this attack, not the hard one. The survey notes that wireless channel variability, through multipath and fading, provides the only partial defense against physical layer replay. A MIL-STD-1553 bus is impedance controlled and transformer coupled and has essentially none of that variability, so faithful reproduction is strictly easier there than on the wireless links where replay was first shown. The doctrine is therefore weakest on exactly the buses now being secured with it.

A. Why Better Defender Hardware Does Not Help

A natural objection is that the defender could learn to detect the artifacts a real converter introduces during replay, such as quantization steps, output impedance signatures, or settling anomalies. This does not change the outcome. The Analog Discovery 3's 14 bit converter introduces artifacts near $10\,\mathrm{V}/2^{14} \approx 0.6$ mV, while an 8 bit defender oscilloscope has a noise floor near $10\,\mathrm{V}/2^{8} \approx 39$ mV, about 65 times larger, so the artifacts are simply invisible to it. Suppose the defender upgrades to a 14 or 16 bit instrument. A passive low pass filter on the attacker's output, a resistor and capacitor costing a few dollars, then smooths any residual step below the new floor. Since MIL-STD-1553 occupies about 1 MHz, a first order filter with a cutoff at 2 to 3 MHz passes the entire signal while attenuating converter quantization noise, which appears at harmonics of the output sample rate, by 20 to 40 dB. The arithmetic is one sided. Each increment of defender resolution costs a substantial instrument upgrade, while the matching attacker countermeasure is a passive analog filter. The attacker can always filter more cheaply than the defender can measure, and the gap widens as commodity converter resolution improves with each hardware generation.

TABLE I
Attack Platform Components

Component	Function	Cost
Digilent Analog Discovery 3	Capture and replay	$379
Commodity 1553 board	Passive bus monitoring	approx. $100
Transformer stub	Bus coupling	approx. $20
Host laptop	Signal processing	existing
Total		under $500

IV. Wraith: Demonstrating the Break on MIL-STD-1553

A. Threat Model

The adversary's goal is to place messages on a MIL-STD-1553 bus that are accepted as originating from a legitimate device, evading voltage fingerprinting. The adversary has physical access to the bus, for example through a maintenance access point or a stub connected during servicing; can passively monitor traffic to record legitimate transmissions; and can drive analog signals onto the bus. The complete kit is a commodity USB oscilloscope with analog input and output (the Analog Discovery 3, $379), an inexpensive 1553 protocol board used mainly as a passive monitor during reconnaissance (approximately $100, design details withheld), a transformer stub (approximately $20), and an ordinary laptop, for a total under $500 (Table I). This is strictly weaker than the adversary assumed in prior fingerprinting work [1], [2], which presumes dedicated bus controller capable protocol hardware. Our adversary needs no firmware exploit, no protocol expertise beyond bus level access, and no military grade equipment. The single commodity instrument that performs both capture and replay is shown in Fig. 2.

B. Attack Phases

The attack chain, from passive capture to analog injection, is shown in Fig. 3.

Phase 1, passive reconnaissance. The adversary connects a differential probe and records raw bus voltage. A Manchester decoder recovers message boundaries and address mappings. No transmission occurs, so the adversary is indistinguishable from a legitimate bus monitor.

Phase 2, capture. The adversary records the target device's transmission at full converter resolution. A key point, and a departure from how fingerprinting is usually framed, is that no large dataset is required. If the adversary knows the address mapping of the bus, information obtained during Phase 1, a single valid message from the target is sufficient to mount the attack. Additional captures add redundancy but are not needed. The corpus we describe in Section V exists to characterize the defense

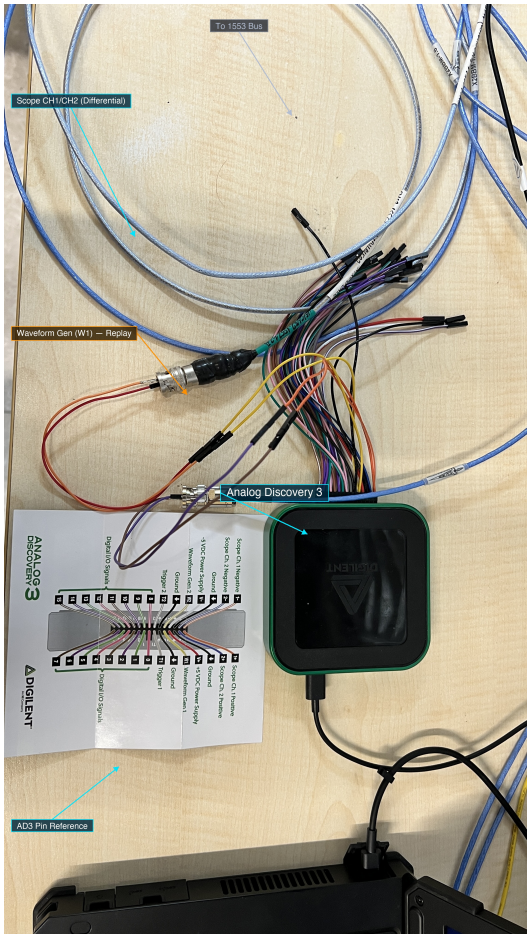

Fig. 2. The commodity USB oscilloscope used for the attack, with its flywire harness. The differential scope inputs capture bus voltage and a single analog output channel, referenced to ground, drives replay. One device implements both the capture and the replay stages.

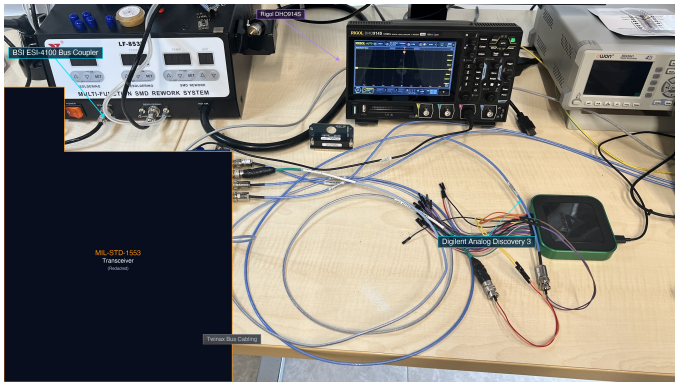

Fig. 3. The Wraith attack chain. The 1553 transceiver (redacted) connects to the bus through a BSI ESI-4100 coupler. The Analog Discovery 3 passively captures bus voltage and later replays it through the same coupler. A Rigol DHO914S oscilloscope provides independent verification. All replayed signals were accepted as valid by the independent equipment.

and to validate the decoder, not because the attack depends on it.

Phase 3, selection. The operator selects any captured signal from the target as the source. There is no automatic quality metric and no averaging across captures. Averaging would smooth away the micro variations, in overshoot, ringing, and edge timing, that fingerprinting is trained to read, so a single instance is retained at full resolution with no filtering or normalization. The captured synchronization region is the part that carries the device's fingerprint, because the synchronization region is what the classifiers evaluate.

Phase 4, replay and injection. The selected waveform is emitted onto the bus through the Analog Discovery 3's 14 bit analog output and ground reference by way of the transformer stub, with amplitude scaled to bus levels. In the direct case the adversary replays a captured message in full, and the resulting transmission carries the original device's analog identity because it is the original device's waveform. To go beyond repetition, the adversary combines the captured synchronization fingerprint of the target with protocol compliant data words carrying attacker chosen content. Because fingerprinting operates on the synchronization region, a message assembled this way presents the target's voltage identity while conveying content the target never sent. This raises Wraith from replay to identity forgery: the adversary wears a captured device's fingerprint while transmitting chosen messages. We report the direct replay result, which we validated on hardware, as the primary evidence, and we treat the forgery extension as a consequence of the same capture, since the fingerprinted region is identical in both cases.

The platform's architecture also supports a real time trigger and override mode. The commodity 1553 board, operating as a monitor, can pattern match on a target data sequence, at which point the Analog Discovery 3's output injects a replacement message that carries the original transmitter's synchronization characteristics but modified data, producing a targeted manipulation on the live bus under a stolen fingerprint. We have validated the individual components, bus monitoring, pattern matching, and converter replay, independently. Their integration into a single automated real time chain is ongoing engineering work and we do not claim it as a completed result here.

C. The BusSpectre Platform

BusSpectre integrates the capture, analysis, and replay chain end to end (Fig. 4); its operator interface is shown in Fig. 5. We keep the description at the level needed to interpret the results. Capture uses a continuous sliding window over the analog input rather than event triggering, and the Manchester decoder is compiled to native code with a just in time compiler. The compilation serves throughput and concurrency, bypassing the interpreter's global lock and sustaining decode rates far above the input data rate; it does not alter or enhance the oscilloscope's output capability. Both representations of every capture are persisted: the raw analog waveform is saved to disk as

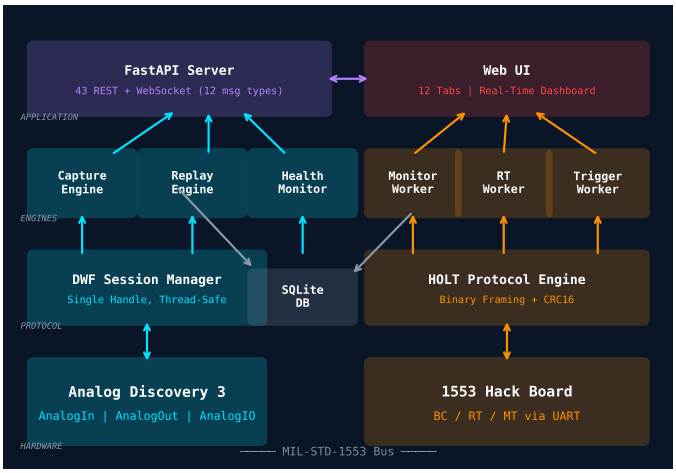

Fig. 4. BusSpectre architecture. A single device handle multiplexes capture, replay, and health monitoring on the commodity oscilloscope. The attacker's 1553 protocol board provides passive monitoring; its internal design is withheld.

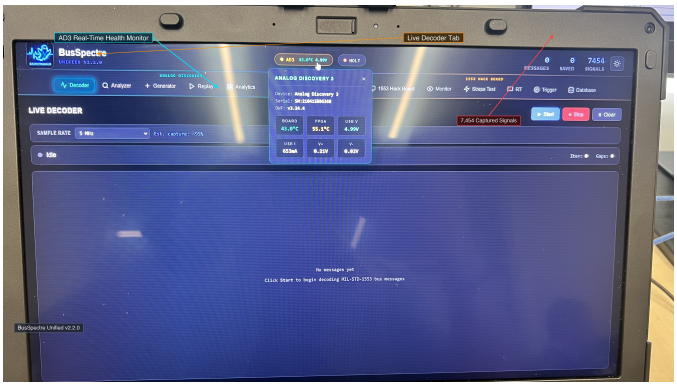

Fig. 5. The BusSpectre operator interface during a live capture session, with real time decoding and device health telemetry. The platform spans analog capture, signal analysis, replay, and protocol level 1553 operations.

a numerical array at full resolution, preserving the analog fingerprint for later use, and the decoded protocol fields are indexed in a database for search. The replay engine takes an operator selected capture, scales it to bus voltage, and emits it through a single analog output channel and ground; no per bit template library is built and no synthetic reshaping is applied, so the recorded voltage shape passes through to the bus essentially unaltered.

V. Experimental Evaluation

A. Setup and Corpus

Experiments were conducted on an isolated bench (Fig. 6). The legitimate infrastructure, whose signals are the target of the attack, is a UEI PowerDNA platform hosting a Bus Controller and a Remote Terminal that communicate on Bus A through transformer coupling (Fig. 7). The Analog Discovery 3 captures on Bus A through differential probes and replays through a transformer coupled stub. The attacker's commodity 1553 board runs as a

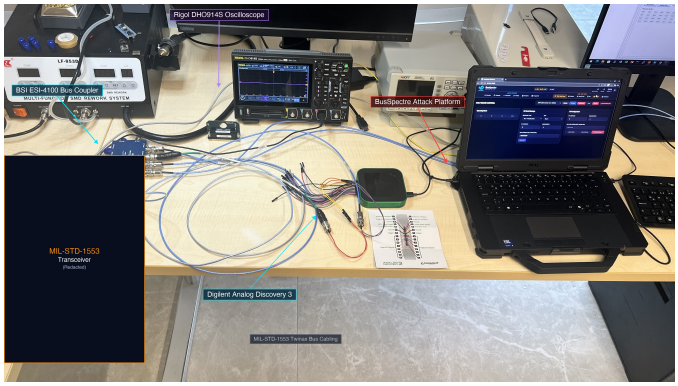

Fig. 6. Laboratory bench for the Wraith experiments. The 1553 transceiver (redacted) connects to the bus through a BSI ESI-4100 coupler. The Analog Discovery 3 performs both capture and replay. A Rigol DHO914S provides independent waveform verification. The BusSpectre platform runs on the laptop at right.

passive Monitor Terminal to assist reconnaissance. A Rigol DHO914S oscilloscope provides independent verification separate from the replay path. Primary acquisition is at 20 MS/s with a 16,384 sample buffer; we did not capture at 100 MS/s, and the analysis below reflects the rates actually used. At the 1 MHz MIL-STD-1553 bit rate, 20 MS/s already gives twenty samples per bit, sufficient to reconstruct and replay the signal for protocol acceptance; matching a defender who samples faster, such as Evcil et al.'s 100 MS/s, is a capability of the same Analog Discovery 3 rather than a requirement of this 1553 demonstration.

The evaluation corpus comprises 11,349 captured signals totaling 258 MB, of which the primary set is 7,442 captured MIL-STD-1553 messages totaling 185 MB, acquired from the test infrastructure across nine Remote Terminal addresses at 5, 10, and 20 MS/s. As stated in Section IV, the attack itself needs only one message; this corpus exists to characterize the fingerprint and to validate the decoder. Of the 7,442 messages, 6,682 (89.8%) decode successfully, the remainder falling below the sync detection floor in low signal to noise captures. Over the decoded words the decoder achieves a 99.8% parity pass rate (188,533 of 188,923 words) and a 98.9% match against ground truth capture metadata, with zero decode errors. Live decoding during a capture session is shown in Fig. 8. Measured signal to noise across the corpus averages 17.2 dB, far inside the Analog Discovery 3's 84.3 dB theoretical dynamic range, which itself shows that the bus and its environment, not the attacker's instrument, set the fidelity ceiling.

B. The Fingerprint Is Real and Stable

For the attack to be meaningful the defense must first work, so we confirm that the target has a strong and consistent fingerprint rather than a noisy one. Over 15,931 pairwise comparisons among captured feature vectors, intra device cosine similarity is 0.941 mean and 0.993

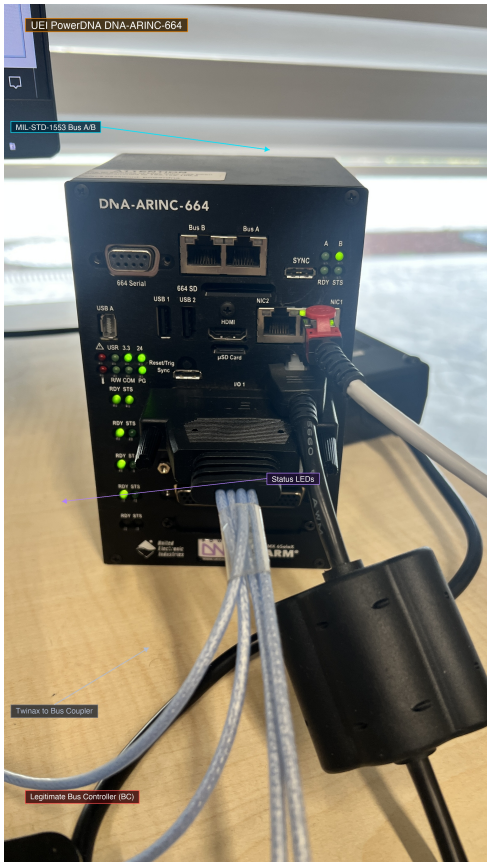

Fig. 7. The UEI PowerDNA unit that serves as the legitimate test infrastructure. It hosts a Bus Controller and a Remote Terminal that communicate on Bus A through the coupler. Its transmissions are the target that the attack captures and replays.

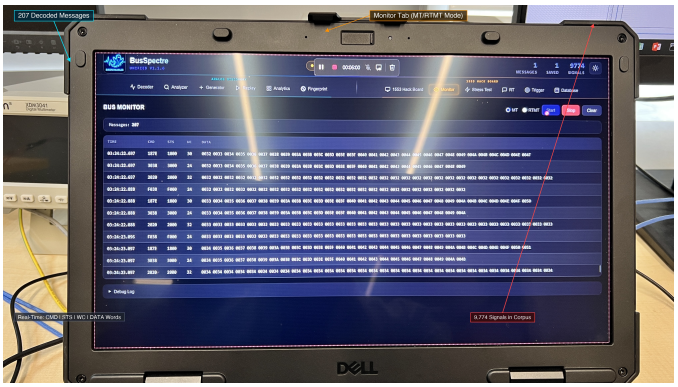

Fig. 8. Live decoded MIL-STD-1553 traffic during a capture session. Each row is a decoded message with timestamp, command word, status, word count, and payload. Every decoded message is also stored as a raw voltage array, preserving the analog signature for later capture and replay.

median. The device's own emissions are highly self consistent, which is the precondition fingerprinting needs; if they were not, fingerprinting would fail on its own terms, independent of any attack. Our concern is the opposite regime: the fingerprint is strong, and that is exactly why it is worth capturing.

TABLE II
Reported Fingerprinting Accuracy versus Wraith Outcome

Defense	Reported Accuracy (foreign hardware)	vs. Wraith Replay
Evcil et al. (RF/KNN/SVM/CNN)	100%	Bypassed
Evcil et al. (LOF)	99.9%	Bypassed
ANoMili (CNN)	99.45%	Bypassed

Reported accuracy is against a different physical device, the scenario the original papers evaluate. "Bypassed" denotes converter replay of captured waveforms accepted as valid by independent test equipment across more than 50 tests with zero protocol errors; by Proposition 1 a classifier reading the same voltage trace cannot separate the replay from the original. LOF, Local Outlier Factor.

C. The Break: Hardware Replay Is Accepted

The central result is that waveforms replayed through the Analog Discovery 3's 14 bit converter onto the physical bus are accepted as valid. Captured waveforms from the legitimate infrastructure were loaded into the Analog Discovery 3's output stage and emitted through the transformer stub onto Bus A. The Rigol oscilloscope and the BusSpectre decoder, both operating independently of the replay path, evaluated each transmission for sync recognition, Manchester decoding, and parity. More than 50 replay tests were run across message types, word counts from 1 to 32, and multiple target addresses. Every replayed signal was accepted as a valid MIL-STD-1553 communication. The independent equipment decoded each one identically to the original, with the same addresses, subaddresses, data words, and status responses, and no protocol error, sync failure, or parity violation was observed in any test.

The link from this result to fingerprinting evasion is Proposition 1, and it is worth stating precisely rather than by empirical analogy. The replayed signal is not an imitation of the captured waveform; it is the captured waveform, emitted again. Whatever voltage feature a fingerprinting classifier extracts from the legitimate transmission, it extracts the same feature, within two stages of 14 bit quantization, from the replay. A classifier that accepts the original must therefore accept the replay, because the distance between their feature vectors is smaller than the intra device spread the classifier already tolerates (Section V-B). We validated protocol level acceptance directly on hardware; the step from protocol acceptance to classifier acceptance is the content of Proposition 1, and a direct per classifier measurement on re-captured replay signals is the natural confirming experiment, which we identify as follow up work. Table II places the outcome beside the accuracy prior work reports: the same recording that fingerprinting was built to exclude walks back onto the bus unchallenged.

D. The Fidelity Gap Favors the Attacker

Two measurements make the asymmetry of Section III concrete on our bench. First, the captured signal to noise

TABLE III
Fingerprinting and Evasion Across Shared Buses

Bus	Fingerprinting Defense	Evasion	Years
CAN	Clock skew [3]	Cloaking [8]	’16 / ’18
CAN	Voltage [4], [5]	DUET [9]	’18 / ’21
1553	Voltage [1], [2]	Wraith (ours)	’22 / ’26
CAN-FD	Voltage VHF [12]	Wraith (predicted)	’26 / ’26

The CAN-FD entry is predicted by Proposition 1 under matched 125 MS/s sampling (Section VI), not a separate hardware demonstration; the other rows are demonstrated evasions.

ratio averages 17.2 dB, while the Analog Discovery 3’s theoretical dynamic range is 84.3 dB. The channel, not the instrument, is the limiting factor, so the attacker has ample headroom to reproduce the signal within the noise the defender must already tolerate. Second, the attacker’s converter resolves the waveform at 14 bits against the 8 bit depth of the defender hardware described in prior work [2], so any artifact the replay introduces sits a full 6 bits below the defender’s least significant bit. The adversary is not merely matching the defender’s view of the signal; the adversary sees it more clearly than the defender does.

VI. The Same Break on Other Buses

The demonstration used MIL-STD-1553, but nothing in the argument of Section III is specific to it. Measurement symmetry needs only a shared medium on which the defender’s authenticator is a physical property of the transmitted signal. Every widely deployed control bus of this family meets that condition, and the automotive case has already produced the same result twice.

Table III lays out the pattern. On CAN, clock skew fingerprinting [3] was evaded by cloaking [8], later given a formal probabilistic footing [18]; voltage fingerprinting [4], [5] was evaded by the DUET attack [9], which reported impersonation of the majority of targets using two compromised on bus nodes. Each time, a physical layer authenticator was proposed, reported high accuracy under benign conditions, and was then shown reproducible by an adversary on the same medium. Wraith completes the pattern for MIL-STD-1553, the bus whose defenses were the most elaborate and the most confidently reported.

A current example, made exact. The most recent incarnation of the doctrine is also the sharpest test of it. Yang et al. [12] authenticate CAN-FD control units by voltage hardware fingerprints drawn from the control field and the data field edges, and argue that an adversary with full bus access cannot impersonate a device because the fingerprint is rooted in analog properties that cannot be faked in software. Two facts turn their scheme into a direct instance of Proposition 1. First, their defender samples the differential bus at 125 MS/s on a Red Pitaya acquisition board, the same rate our attacker’s converter reaches, so the two observers see the signal at the same temporal resolution and the reproduction error is bounded by the shared quantization. Second, all four attacks they evaluate, substitution, masquerade, injection, and wire tapping, assume the adversary transmits with different hardware or only listens; none records a legitimate node’s own waveform and replays it. Their detector succeeds precisely because foreign hardware carries a foreign fingerprint, which is the blind spot we identify across this literature. A recording of the legitimate node carries the legitimate fingerprint by construction, and we demonstrated exactly that capture and replay on MIL-STD-1553; with the sampling matched, measurement symmetry carries the same result to their CAN-FD scheme by the same proof. Their scheme does add an impedance check, but it reacts to hardware being added to the bus rather than deciding which device a signal claims to be; it is a coarse topology alarm, and it is evaded when the replay is driven from a node already present on the bus, for example a compromised legitimate transmitter, rather than from an added stub.

The same reasoning extends by structural analogy, without new experiments, to the remaining buses in this class. MODBUS over serial, LIN, and ARINC 429 are all shared or point to multipoint media whose signaling is observable to connected devices, and physical layer fingerprinting has been proposed or would be proposed for each on the same premise of hardware intrinsic signatures; Gilboa-Markevich and Wool’s ARINC 429 study, which found raw voltage features most effective [7], is precisely the feature a recording adversary reproduces. There is moreover a counterintuitive ordering to exposure. These wired buses lack the channel variability that gives wireless links their only partial resistance to physical layer replay [16], so they are more exposed, not less, than the radio systems where replay was first demonstrated. Automotive security in particular continues to advance voltage and timing fingerprinting as a practical intrusion defense; the DUET result already showed voltage IDS to be evadable, and measurement symmetry explains why that outcome is generic rather than incidental.

The asymmetry compounds in the attacker’s favor. One capture kit can impersonate any device on a bus by recording it, while each device the defender adds requires enrollment and retraining. A single capture carries the authentic signal to every voltage classifier at once, regardless of which feature the classifier computes. And the commodity trend is monotone: a 14 bit instrument already exceeds both defenders’ equipment, and each hardware generation widens the resolution advantage while lowering price.

VII. What Actually Works

The lesson is not that these buses cannot be defended. It is that they cannot be defended by a property the adversary can observe and reproduce. Authentication must rest on a secret the adversary cannot extract from the wire. This single requirement also explains why the intuitive

partial measures fail, so we state the reasoning before the mechanisms.

The attack does not merely replay a fixed message; it can present a captured device's fingerprint while carrying attacker chosen, protocol compliant content (Section IV). Any field the defender adds in the clear is therefore just more content the adversary controls. A plaintext sequence number does not stop Wraith, because the adversary writes the next expected counter value into the forged message exactly as it writes any other data word. Freshness has force only when the adversary cannot produce a valid authenticator for the new counter, which returns the problem to a secret key. The mechanisms below all reduce to holding such a key.

Cryptographic message authentication. A message authentication code computed with a per device key gives unforgeable proof of origin that a recording cannot supply and that a forgery cannot reconstruct, because neither contains the key. The timing budget is not the obstacle. Within the 4 to 12 microsecond response window of MIL-STD-1553, AES-128-CMAC on a Cortex-M4 class core is marginal at roughly 14 microseconds for a 16 byte message, but Chaskey [19], designed for 32 bit microcontrollers, produces a code in roughly 1.1 microseconds, and Ascon [20], the NIST lightweight standard (SP 800-232), does so in under 0.5 microseconds. The real constraint is bandwidth: a full 128 bit code consumes 8 of the 32 data words available in a transfer, though a truncated 32 bit code fits in 2 words and suffices for most operational needs.

Freshness bound under the key. A sequence number or a nonce stops replay of a previously valid message, but, as argued above, only when it is carried inside the authenticated payload so that its value cannot be changed without invalidating the code. Combined with a message authentication code this gives both origin authentication and replay resistance; alone it gives neither.

Challenge and response. The controller issues a nonce through a mode code, and the terminal returns an authenticated function of it. Mode codes that carry a data word already provide a 16 bit nonce channel, so with a preshared key and a lightweight code this gives per transaction authentication and freshness in one exchange, inside the existing protocol, without changing the physical layer.

Table IV rates the proposed and deployed defenses against Wraith. Voltage fingerprinting, including the commercial products that implement it, is bypassed. Timing and protocol anomaly detection [21], [22] and rule based filtering are partial: they can catch malformed or mistimed traffic but cannot distinguish a voltage faithful replay of a valid message, timed to an expected slot, from the original. Only cryptographic authentication with bound freshness addresses the root cause. This matters commercially and not only academically. Products that learn physical layer fingerprint parameters and then watch for deviation, such as Sital Technology's BRM1553D-SnS, implement exactly the defense our attack bypasses, and the same critique applies to any vendor on any bus that sells a reproducible physical property as an identity. The trajectory of the field points the same way. Yang et al. [12], having argued that their CAN-FD voltage fingerprint cannot be faked, nonetheless name lightweight message authentication codes as the route to a complete defense. Proposition 1 explains why that is the only route that authenticates: the fingerprint is reproducible, and the key is not.

TABLE IV
Defense Robustness Against Wraith

Defense Type	Example	vs. Wraith
Voltage fingerprinting	[1], [2]	Bypassed
Commercial voltage IDS	Sital BRM1553D-SnS	Bypassed
Plaintext sequence number	counter in the clear	Bypassed
Timing anomaly	MAIDENS [21]	Partial
Protocol anomaly	[22]	Partial
Rule based filtering	Peraton Bus Defender	Partial
Keyed MAC with freshness	[19], [20]	Effective

"Bypassed": accepted across more than 50 hardware replay tests, or forgeable in the clear by an adversary who controls the data words. "Partial": catches protocol or timing anomalies but accepts voltage faithful replays timed to expected slots. "Effective": cannot be forged or replayed without the key, regardless of waveform fidelity.

VIII. Limitations

Our hardware evaluation uses one legitimate test platform rather than a fleet of diverse transmitters; a multi device testbed would strengthen the empirical picture, though the argument that a captured waveform carries its source's fingerprint does not depend on device count. The bench is a laboratory environment, and operational cabling, coupling, and interference differ, although those factors degrade the defender's fingerprinting as much as the attacker's replay. We validated protocol level acceptance of the replayed signals directly; the step to classifier level acceptance rests on Proposition 1, and a direct per classifier measurement on re-captured replay signals is the natural confirming experiment and is left as follow up work. We report direct hardware replay as the validated result and treat arbitrary message forgery and the real time trigger and override mode as consequences of the same capture whose full automated integration is ongoing. The cross protocol extensions of Section VI are argued by structural analogy rather than demonstrated, and are stated as such.

IX. Conclusion

Hardware fingerprinting is being adopted as an authentication layer on exactly the buses least able to support it. The doctrine assumes that a device's physical signature is unforgeable, and on a shared medium that assumption is simply false. The signature is broadcast on every transmission, and an adversary on the same wire records

the identical signal the defender measures. We formalized this as measurement symmetry and showed that no feature function escapes it once the attacker's converter matches the defender's, a condition that commodity hardware now satisfies comfortably.

We demonstrated the consequence on the hardest and most consequential case, MIL-STD-1553, using commodity capture and replay hardware. More than 50 captured waveforms replayed onto a physical bus were accepted as valid by independent test equipment, decoded identically to the originals, with zero protocol errors. Because the replayed signal is the captured signal, any voltage classifier that accepts the legitimate device must, within quantization error, accept the replay. The same symmetry governs CAN, MODBUS, LIN, and ARINC 429, and the automotive record already shows the pattern completing twice before us.

The corrective is to stop treating a reproducible physical property as an identity. Authentication on these buses should rest on a secret, through a keyed message authentication code with freshness bound under the same key, which remains secure precisely because the adversary can read every message and still cannot produce the key. Anything less, including a fingerprint or a plaintext counter, is reproducible by an adversary who shares the medium. Until that shift happens, a defense now marketed and fielded as authentication reduces, on every shared bus we examined, to a recording played back.

References

[1] M. Evcil, Z. Y. Tök, İ. C. Babir, M. A. Gökyer, B. Bozkurt, and S. Akleylek, "Hardware fingerprinting using machine and deep learning methods on MIL-STD-1553," in 2024 IEEE/AIAA 43rd Digital Avionics Systems Conference (DASC). IEEE, 2024, pp. 1–9.

[2] E. Levy, N. Maman, A. Shabtai, and Y. Elovici, "ANoMili: Spoofing prevention and explainable anomaly detection for the 1553 military avionic bus," arXiv preprint arXiv:2202.06870, 2022.

[3] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in 25th USENIX Security Symposium (USENIX Security 16), 2016, pp. 911–927.

[4] M. Kneib and C. Huth, "Scission: Signal characteristic-based sender identification and intrusion detection in automotive networks," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, 2018, pp. 787–800.

[5] W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Lee, "VoltageIDS: Low-level communication characteristics for automotive intrusion detection system," IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2114–2129, 2018.

[6] D. Bracknell, "The MIL-STD-1553 data bus: What does the future hold?" The Aeronautical Journal, vol. 111, no. 1118, pp. 231–246, 2007.

[7] N. Gilboa-Markevich and A. Wool, "Hardware fingerprinting for the ARINC 429 avionic bus," in European Symposium on Research in Computer Security (ESORICS). Springer, 2020, pp. 42–62.

[8] S. U. Sagong, X. Ying, A. Clark, L. Bushnell, and R. Poovendran, "Cloaking the clock: Emulating clock skew in controller area networks," in 2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS). IEEE, 2018, pp. 32–42.

[9] R. Bhatia, V. Kumar, K. Serag, Z. B. Celik, M. Payer, and D. Xu, "Evading voltage-based intrusion detection on automotive CAN," in Network and Distributed System Security Symposium (NDSS), 2021.

[10] O. Stan, Y. Elovici, A. Shabtai, G. Shugol, R. Tikochinski, and S. Kur, "Protecting military avionics platforms from attacks on MIL-STD-1553 communication bus," arXiv preprint arXiv:1707.05032, 2017.

[11] E. Levy, N. Maman, A. Shabtai, and Y. Elovici, "ANoMili: Spoofing hardening and explainable anomaly detection for the 1553 military avionic bus," IEEE Transactions on Aerospace and Electronic Systems, vol. 60, no. 6, pp. 7738–7753, 2024.

[12] Y. Yang, R. Zhou, J. Yu, and Y. Ding, "CAN-FD ECU authentication using voltage-characteristic hardware fingerprints," Electronics, vol. 15, no. 5, p. 1094, 2026.

[13] AFLCMC/EN, "MIL-STD-1553C: Department of Defense interface standard: Digital time division command/response multiplex data bus," Department of Defense, 2018, http://everyspec.com/MIL-STD/MIL-STD-1500-1599/MIL-STD-1553C_55783/.

[14] K. Lounis, S. H. Ding, M. Mansour, M. Wrana, M. A. Elsayed, and M. Zulkernine, "A review and analysis of attack vectors on MIL-STD-1553 communication bus," IEEE Transactions on Aerospace and Electronic Systems, vol. 58, no. 6, pp. 5586–5606, 2022.

[15] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in Proceedings of the Third ACM Conference on Wireless Network Security (WiSec '10). Hoboken, NJ: ACM, 2010, pp. 89–98.

[16] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," ACM Computing Surveys, vol. 45, no. 1, pp. 1–29, 2012.

[17] D. Urbina, J. Giraldo, A. Cardenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, and H. Sandberg, "Limiting the impact of stealthy attacks on industrial control systems," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). ACM, 2016, pp. 1092–1105.

[18] X. Ying, S. U. Sagong, A. Clark, L. Bushnell, and R. Poovendran, "Shape of the cloak: Formal analysis of clock skew-based intrusion detection system in controller area networks," IEEE Transactions on Information Forensics and Security, vol. 14, no. 9, pp. 2300–2314, 2019.

[19] N. Mouha, B. Mennink, A. Van Herrewege, D. Watanabe, B. Preneel, and I. Verbauwhede, "Chaskey: An efficient MAC algorithm for 32-bit microcontrollers," in Selected Areas in Cryptography (SAC 2014). Springer, 2015, pp. 306–323.

[20] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight authenticated encryption and hashing," Journal of Cryptology, vol. 34, p. 33, 2021.

[21] S. J. J. Genereux, A. K. H. Lai, C. O. Fowles, V. R. Roberge, G. P. M. Vigeant, and J. R. Paquet, "MAIDENS: MIL-STD-1553 anomaly-based intrusion detection system using time-based histogram comparison," IEEE Transactions on Aerospace and Electronic Systems, vol. 56, no. 1, pp. 276–284, 2020.

[22] T. Rogers and K. B. Rasmussen, "Targeted detection for attacks on the MIL-STD-1553 bus," IEEE Transactions on Aerospace and Electronic Systems, vol. 60, no. 1, pp. 548–562, 2024.