SECURITY & FORENSICS
IS SSD A FRIEND OR A FOE?

Presented by:
Avinash Srinivasan
Cyber Science, USNA

DISCLAIMER

The views expressed in this presentation are those of the authors and do not reflect the official policy or position of the U.S. Naval Academy, Department of the Navy, the Department of Defense, or the U.S. Government.

PRESENTATION AGENDA

- The Central Questions – Motivation
- Covert Channels 101
- SSD Security and Forensics
- Future SSD Technology Trends and Challenges

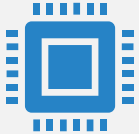
THE CORE QUESTION(S)

Are SSDs more secure?

Do they hinder digital forensics?

Is there a trade-off between protecting data and recovering it?

THE CENTRAL CONFLICT



SSD Flash Translation Layer (FTL) abstracts physical NAND from the OS unlike HDDs

FTL is a black box

boosts performance and endurance

also creates security blind spot(s)

- traditional forensic & detection tools lose visibility

COVERT CHANNELS 101

Covert Channel is an unauthorized communication path that violates security policy by leveraging shared resources or physical state.

Key Properties: out-of-band, bypasses access controls

Types of CC

Storage Channels

Timing Channels

COVERT STORAGE CHANNELS

Signaling types:

- attacker writes/modifies a resource;
- receiver later reads state to decode, i.e., asynchronous.

Persistence:

- encoded signal remains until overwritten;
- enables delayed exfiltration.

Storage CC examples:

- file-system [54], slack-space [55], hidden partition [44]
- network protocol fields [1, 2, 7, 52]
- (SSD) physical modification [17]
- (SSD) over-provisioned space [59]

Detection footprint:

- altered on-disk state, metadata, device use/wear patterns (SSD)

COVERT TIMING CHANNELS

Timing-based signaling:

- attacker modulates timing/perf of a shared resource;
- receiver measures latency/throughput to decode.

Transient (non-persistent):

- signal exists only during Tx window — no durable on-disk artifact;
- requires synchronized sampling.

Timing CC examples:

- resource contention
- network-based – inter-packet gap [10]
- forced GC (SSD)
- power/thermal throttling

Detection footprint:

- correlated latency/throughput patterns, synchronized GC/TRIM spikes.

SSD AS A SECURITY ALLY (FRIEND)

- **Self-Encrypting Drives (SEDs):** hardware-based (AES-256) encryption built into the controller; protects data at rest.
- **Cryptographic Erase (NIST Recommended for SSD)** instantly sanitizes data by deleting crypto keys.

Tactical Scenario:

- **UAV Remote Crypto-Erase:** Upon detecting imminent capture, operator remotely triggers crypto-erases on UAV SSD, destroying its key and rendering onboard data unreadable instantly–even if physically extracted.

SSD AS A SECURITY HURDLE (FOE)

- **Firmware-Level Malware:** persistent, stealthy, and difficult to detect or remove.
- **DMA Abuse (NVMe/PCIe):** leverage DMA to bypass OS protections for high-privilege actions; hard to monitor from the host.

Tactical Scenario:

- **Compromised NVMe in UAV:** A supply-chain-tampered NVMe SSD on a drone can lie dormant during normal flights, covertly exfiltrating crypto keys and mission data.

SSD AS A FORENSICS ALLY (FRIEND)

- **No Mechanical Degradation** ensures high data integrity even after physical shock.
- **Power-Loss Protection (PLP)** preserves data during sudden shutdowns—vital for incident capture.

Tactical Scenario:

- **Rugged UAV SSD Forensic Recovery:** A forensic team recovers SSD from a crashed recon UAV – data intact and unaltered despite the crash.

SSD AS A FORENSICS HURDLE (FOE)

- **TRIM & GC** actively erase deleted data, making recovery nearly impossible
- **Wear-Leveling** scatters file fragments by obfuscating logical-to-physical mappings

Tactical Scenario:

- **Captured Sleeper-Cell Laptop (SSD Anti-Forensics):** After seizure, deleted ops plans/maps on the laptop are unrecoverable due to TRIM+GC, while wear-leveling disperses file fragments defeating carving and other forensic actions.

SSD AS ACTIVE ATTACK VECTOR: FROM STORAGE TO SUBVERSION

SSDs can function as active attack vectors via reprogrammable firmware – beyond passive data storage

BadUSB (Black Hat 2014): Showed how USB firmware can be reprogrammed to impersonate other devices (e.g., keyboard, NIC)

SSDs inherit the **BadUSB threat model +** underexplored attack surface

THE FUTURE: EMERGING MEMORIES

Non-NAND memories (ReRAM, MRAM, PCM) bring **new physics** and **new attack surfaces**.

- **ReRAM:** Targets resistive states
- **MRAM:** Exploits magnetic domains
- **PCM:** Manipulates phase-change properties

Implication:

- Forensics and security tools must evolve with the hardware.

New Hardware, New Threats

CONCLUDING REMARKS

Security of an SSD lies not in the hardware itself, but in how its capabilities are understood, managed, and leveraged by both attackers and defenders.

Key Takeaway:

- Move from treating SSDs as passive storage to treating them as active, intelligent endpoints in our security architecture.
- Integrate SSD acquisition and analysis into the overarching organizational Forensics Readiness Plan.

THANK YOU!!!

I AM HAPPY TO TAKE QUESTIONS

For questions, contact:
Avinash Srinivasan, Ph.D.
U. S. Naval Academy