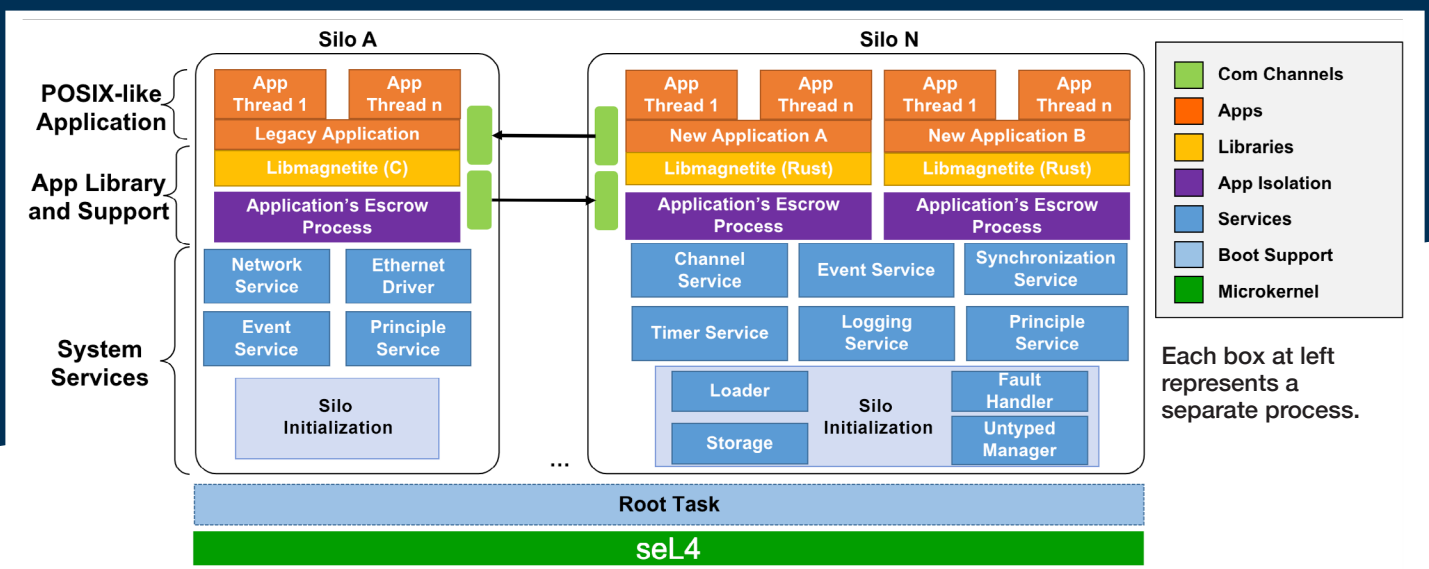
MIT LINCOLN LABORATORY

INNOVATION HIGHLIGHT

Technology in Support of National Security

WWW.LL.MIT.EDU

Advanced Security for Embedded Computing



Magnetite provides featureful system services on seL4. Both legacy C and new Rust applications can run on Magnetite's POSIX-like application programming interface (API). Applications can run in separate isolation constructs called silos for separation, with only pre-established channels allowed for communication.

Lincoln Laboratory has developed an operating system (OS) architecture that builds security into every layer. Built on seL4, a microkernel with verified security properties, the secure-by-design, real-time Magnetite OS isolates services such as timing, data movement, and storage by applying the principle of "least privilege," i.e., access is restricted to just the data a service needs. Magnetite enables components to share hardware without becoming mutually vulnerable to security breaches that could cascade into system-wide failure. Magnetite's isolation approach offers the resiliency to cyberattacks needed to safeguard computers embedded in systems supporting critical missions and infrastructure.

KEY FEATURES

- Delivers a full set of OS services on top of seL4 without modifying the verified kernel, preserving the formal assurance chain that makes seL4 trustworthy
- Breaks the OS into isolated services to prevent an intrusion into one service from spreading throughout the entire system
- Limits privileges to a component/service to the instance of a request, further reducing opportunities for intruders to gain widespread access to data
- Utilizes Rust, a memory-safe language, but accommodates legacy code to allow adopters to conduct a phased migration to Magnetite

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

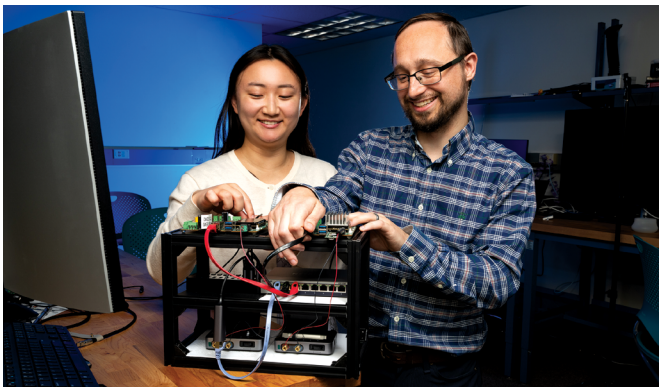
Motivation

Embedded computers run systems that maintain the nation's security and standard of living: satellites, drones, tactical networks, radars, and critical infrastructure. In these systems, a cyberattack causes not just a loss of data; it poses a potentially life-threatening loss of services and missions. The explosion in artificial intelligence (AI) tools is accelerating the pace at which adversaries and criminals can discover vulnerabilities in software. Currently, computers are vulnerable to privilege escalation and manipulation because access into one OS component or software service can allow access to the whole system.

Consequences of this access liability can be severe for critical embedded systems. For example, a breach into a system running the power grid could leave millions without electricity, or a cyberattack on a satellite could paralyze time-sensitive military communications. Many embedded systems are complex—built on years of design modifications or reliant on components from diverse suppliers—making it hard for analysts to diagnose bugs and patch them.

Innovative Solution

Researchers at Lincoln Laboratory have developed Magnetite, an OS architecture that mitigates the access liability. Built on the principle of "least privilege," Magnetite is configured to limit access to just the data and the duration of time needed to fulfill a specific task. At the core of Magnetite is seL4, a microkernel for which security has been rigorously verified (via generation of 200,000 lines of machine-checked mathematical proof for roughly 9,000 lines of kernel code). Among other properties, this verification ensures that the seL4 kernel is free from entire classes of common software vulnerabilities, and Magnetite builds upon this secure foundation.



Andrea Lin and Samuel Jero adjust a ground-to-space test bed running Magnetite. The test bed demonstrates encrypted end-to-end communication between a ground station and a notional satellite using NASA's core flight software.

Magnetite's Advantages

- The least privilege design thwarts the rapid expansion of AI-driven attack capabilities, lessening the time pressures for analysts trying to respond to these constantly evolving intrusions.
- Magnetite offers security to embedded systems fielded in locations where it is difficult or impossible for analysts to physically investigate and patch breaches (e.g., at remote sites or in space).
- Magnetite provides a solution for integrating software-based cryptography on platforms too size-, weight-, and power (SWaP)-constrained to host dedicated cryptographic hardware.
- Magnetite's siloed architecture fosters resiliency, locking down a compromised component while allowing the system to keep operating.

U.S. PATENT #12,314,734

More Information

J. Furgala et al., "Porting NASA's Core Flight System to the Formally Verified seL4 Microkernel," Workshop on Security of Space and Satellite Systems 2026, February 23, 2026.

This technology is an R&D 100 Award Winner

INTERESTED IN WORKING WITH MIT LINCOLN LABORATORY?

Scan the QR code to learn more
www.ll.mit.edu/partner-us

Contact the Technology Transfer Office
tto@ll.mit.edu

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This material is based upon work supported under Air Force Contract No. FA8702-15-D-0001 or FA8702-25-D-B002. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. Air Force.
© 2026 Massachusetts Institute of Technology