Transitions

A ROUNDUP OF LINCOLN LABORATORY TECHNOLOGY TRANSFER OPPORTUNITIES IN CYBER SECURITY

Technology Transfer

As a federally funded research and development center, Lincoln Laboratory is chartered to make technology available to both government agencies and commercial entities. Here is a sampling of some of the technologies that are ready for this transition.

For more information on these technology transfer opportunities, please email cyber-tech-transfer@ll.mit.edu.

Scalable Cyber Analytic Processing Environment (SCAPE)

Network defense requires rapid sensemaking of large amounts of data from disparate sources. This sensemaking is especially challenging in networks that are established ad hoc or that lack enterprise network monitoring and security, and an event management infrastructure. The core problem that the Scalable Cyber Analytic Processing Environment (SCAPE) solves is the following: Given a number of available network sensor data sources, such as NetFlow records from routers, logs from web proxies, and alerts from intrusion-detection systems, how can an analyst with little prior knowledge about the network or the data sources immediately begin ingesting and analyzing the data while continuously refining his or her understanding to enhance downstream data query and analysis?

SCAPE provides data storage and a suite of knowledge engineering, query, analysis, and visualization capabilities to meet an analyst's needs. The technology uses Accumulo, a Bigtable-like NoSQL database, as the storage back end and provides a variety of out-of-the-box parsers and utility functions for ingesting cyber data. SCAPE pioneers a knowledge-engineering framework, called the Knowledge Registry, that uses domain-specific data types and descriptive tags to describe data sources. For a domain-specific view of the data, SCAPE provides an application programming interface (API) that leverages the information in the Knowledge Registry. As the analyst gains intuition about the data sources through ad hoc data exploration, he or she can expand the Knowledge Registry with metadata about the sources and, in turn, assert fine-grained control over how data are interpreted and exposed through the API. This iterative process allows the analyst to home in on interesting data by continually tuning the data processing pipeline as new data source relationships are discovered.

SCAPE was developed under the Lincoln Laboratory cyber situational awareness program that is funded by the Assistant Secretary of Defense for Research and Engineering line. It is now available as an open-source project.

Lincoln Open Cryptographic Key Management Architecture

There is a strong market need for cryptographic technology that is secure and efficient. While modern cryptography offers proven ways to secure applications and devices, it lacks easy-to-deploy and easy-to-use key-management solutions. Making cryptographic keys available to authorized remote devices when needed and securing the keys in storage and in transit are complicated tasks. Existing cryptographic software libraries provide only a partial solution, lacking built-in support for key management and authorized user-identity management. Developers must figure out how to combine low-level cryptographic functions into a secure design that supports all of the high-level security functions required by the application, such as data protection, cryptographic user-identity management, and key management, and that prevents key development errors resulting in insecure applications and security breaches.

Lincoln Open Cryptographic Key Management Architecture (LOCKMA) provides a seamless solution by combining the following functions into a self-contained, rigorously architected and verified component: powerful cryptography to enable applications to protect their data at rest and in transit over communication channels; standards-based identity management to help applications create, establish, and verify identity credentials; and advanced key-management functions for generating, protecting, and securely distributing cryptographic keys to authorized recipients.

With a simple, intuitive interface, LOCKMA handles all low-level cryptographic functions "under the hood" in a design successfully realized in several advanced military communication applications. LOCKMA is highly portable, is extremely resource efficient, and is decoupled from specific types of operating systems and communication channels. It is beneficial to a wide variety of applications, such as military operations, household-management automation, and network security.

LOCKMA focuses on making the addition of strong, usable cryptographic protections to applications as easy and as inexpensive as possible. As such, LOCKMA implements only those algorithms approved by the National Institute of Standards and Technology and the National Security Agency. Furthermore, unlike existing key-management enterprise solutions, LOCKMA enables devices and applications to secure their data end to end, without having to trust any centralized key servers.

LOCKMA was honored with an R&D 100 Award, was realized as a field-programmable gate array core, was submitted for two U.S. Patent and Trademark Office patent applications, and won an MIT Lincoln Laboratory Best Invention Award.

Proactively secure Accumulo with Cryptographic Enforcement

The Proactively secure Accumulo with Cryptographic Enforcement (PACE) project uses cryptographic techniques to enhance the security of the Accumulo database against a malicious server or system administrator. Accumulo, a scalable distributed database, offers fast ingest rates and cell-level access control, giving users the ability to quickly store large datasets and to establish fine-grained access control for authorized users. Because Accumulo is widely used within the federal government, it is important that its stored data cannot be learned, modified, or leaked at the whim of an adversary. The PACE team uses efficient, well-understood cryptographic algorithms to secure Accumulo against threats to stored datasets.

PACE has two primary focuses. The first is to enable users to validate the integrity of their stored data and the results of their queries, ensuring that these results contain only the correct requested data. The second focus is to guarantee the confidentiality of users' data by providing a flexible encryption library for Accumulo cells and cryptographically enforcing Accumulo's access control. The PACE team is also developing a seamless interface with Accumulo's API to enable users to cryptographically secure aspects of their Accumulo servers with minimal changes to their existing code. This seamless integration, combined with the PACE software's security guarantees, has already allowed some of the PACE integrity work to be transitioned to a government customer. Looking ahead, Lincoln Laboratory plans to transfer the rest of the PACE technology to the same seamless interface while finding new ways to deliver powerful, usable security to Accumulo users.

Self-Enforcing Security for the Cloud with Cryptographic Access Control

Commercial cloud storage offers many benefits, such as data ubiquity, data backups, and low storage costs. However, many users are reluctant to relinquish their data to the cloud because of security concerns, fearing a loss of control over data access and protection. Most current cloud storage services rely on explicit or implicit trusted third parties to protect data and to enforce access control policies that define who can obtain the data and the type of access, e.g., read-only or write-only permission. However, third parties may not be trustworthy because they can be corrupted by insider threats and security breaches.

The cryptographic access control (CryptAC) framework returns data control to users. CryptAC redefines authentication and authorization by making permissions into "self-enforcing" cryptographic objects, negating the need for a trusted third party. CryptAC can also improve local storage resilience against insider threats; for example, system administrators can manage files on a local system but cannot access the files' contents without the owner assigning the administrators explicit permissions. If attackers gain access to stored data, they cannot read the information; they can only destroy the data. To mitigate data destruction, CryptAC uses erasure codes that encode data in blocks so that if some blocks are erased (up to a predefined threshold), the data can be reconstructed from the remaining blocks. CryptAC employs erasure codes to efficiently distribute data over multiple clouds, allowing the data to be efficiently retrieved even if some clouds are unavailable or the data are corrupted.

CryptAC works seamlessly with the cryptographic keys stored on Department of Defense (DoD) Common Access Cards (CACs), allowing DoD users to authenticate and manage permissions with ease. Keys derived from other sources, including passwords and biometric data, are also compatible with CryptAC.

CryptAC provides secure support even for traditional access policies, such as file permissions in standard operating systems. More importantly, it not only improves current policy enforcement but also enables technology for developing and supporting novel trust infrastructures that are flexible, explicit, and secure.

Timely Randomization Applied to Commodity Executables at Runtime (TRACER)

When cyber attackers exploit typical programming bugs in common applications, they can obtain and leak sensitive information that determines how a program runs and how it is protected. Researchers have observed numerous advanced persistent threats that bypass modern operating systems' (OS) defenses. The resulting data leakages are especially difficult to mitigate in proprietary OS, e.g., Windows, and closed-source applications because existing defensive techniques rely on analyzing the source code.

Timely Randomization Applied to Commodity Executables at Runtime (TRACER) is a prototype technology that prevents information-leakage attacks by frequently rerandomizing the encoding of sensitive program data in closed-source applications. The rerandomization is tied to program outputs, e.g., network packets. When the program generates and releases an output, allowing an attacker the opportunity to steal and potentially leak information, all sensitive regions of the program are rerandomized. As a result, any leaked program data immediately become stale and unusable.

TRACER can work with proprietary applications, such as Adobe Reader, Internet Explorer, and Java, on top of Windows without requiring the source code or modifying the OS. TRACER also minimally impacts performance; the current prototype does not add a noticeable slowdown to protected applications. It has been tested on a variety of popular applications, including Adobe Reader, Internet Explorer, Firefox, and Adobe Flash.

TRACER prevents sophisticated attacks that can otherwise bypass OS defenses as has been observed in many persistent attacks.