Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2012**	2. REPORT TYPE	3. DATES COVERED **00-00-2012 to 00-00-2012**
4. TITLE AND SUBTITLE **Lincoln Open Cryptographic Key Management Architecture**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Massachusetts Institute of Technology,Lincoln Laboratory,244 Wood Street,Lexington,MA,02420-9108**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**2**	

LINCOLN LABORATORY
Massachusetts Institute of Technology

2012 | www.ll.mit.edu

Tech Notes

Lincoln Open Cryptographic Key Management Architecture

Solving the complex problem of cryptographic key management enables broad employment of cryptographic protections in devices as small as a miniature drone.

Modern cryptography offers a variety of encryption schemes for the protection of information. Each scheme requires keys to encrypt and decrypt information. Encryption works by scrambling information into unintelligible ciphertext by using an encryption algorithm and a short cryptographic key. Decryption restores original information from ciphertext by using a complementary decryption algorithm and a decryption key.

Although many efficient and ironclad secure encryption solutions have been standardized, these solutions are not universally used or embedded in miniature devices and computer systems. The main reason is the lack of generic, easy-to-deploy, and easy-to-use solutions for key management (KM). The MIT Lincoln Laboratory Open Cryptographic Key Management Architecture (LOCKMA) solves the KM problems by providing a highly portable software library that serves as a foundation for a secure communication system.

Key Management

Data located in storage devices and especially in transit between devices are vulnerable to exploitation and interception. An effective protection against interception and interpretation is encryption. The simple task of protecting data with encryption, however, is overshadowed by the more complex issue of key management, that is, of managing cryptographic keys and making them available to authorized entities. Besides being complex to "start from scratch," developing a secure and usable key management scheme for a new system may inadvertently introduce vulnerabilities that can compromise the security of the entire system. Transferring an existing key management scheme from one system to a new system may be incongruous or impractical.

The fundamental challenge that LOCKMA solves is the complex life cycle of cryptographic keys, thereby enabling broad employment of cryptographic protections in devices. For a

Seamless over-the-network key distribution to unmanned aerial vehicles (UAVs) and authorized terminals

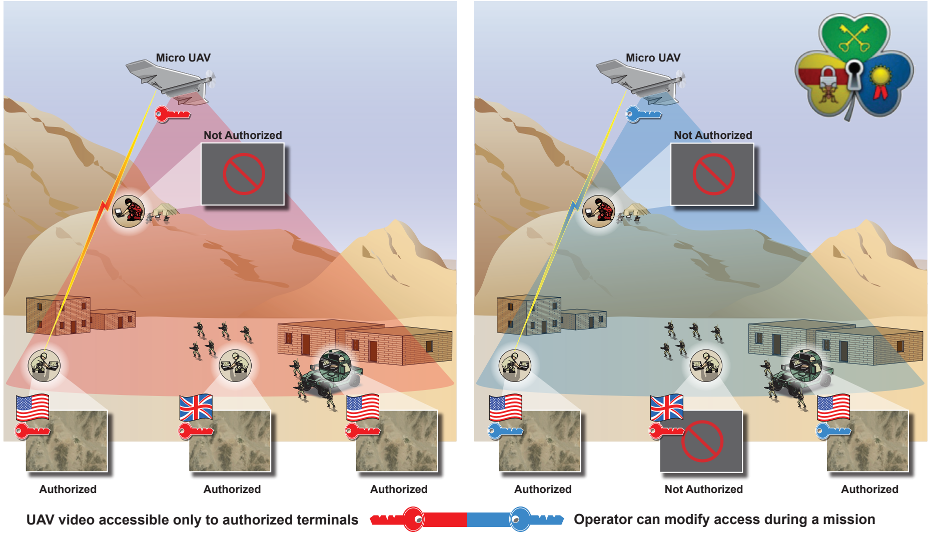

Figure 1. The initiator of LOCKMA, here shown on the left in each case, can provide access to unmanned aerial vehicles' (UAV) data stream by providing keys to authorized users and denying access to non-authorized users. The authorization confirmations and keys are transmitted in-band with the data stream.

Technical Points of Contact
Roger Khazan and Dan Utin
Cyber Systems and Technology Group
rhk@ll.mit.edu, danu@ll.mit.edu
781-981-5976, 781-981-6759

For more information, contact:
Communications and Community
Outreach Office
MIT Lincoln Laboratory
244 Wood Street
Lexington, MA 02420-9108
781-981-4204

given key, some of the KM functions involve cryptographic algorithms and other keys. Thus, a given device or system may have to deal with numerous keys for different users, different sessions, different communication channels, different communicants, or different data instances. It is this complexity of key management that has prevented the proliferation of standard cryptographic solutions into the mainstream.

LOCKMA offers the following KM functionality to its applications:

- Creating cryptographic keys
- Associating keys with their purposes
- Protecting keys at rest in both volatile and nonvolatile memory
- Making the keys available for authorized encryptions and authorized decryptions
- Delivering keys securely to authorized remote locations
- Archiving keys
- Evolving keys with time
- Retiring expired keys

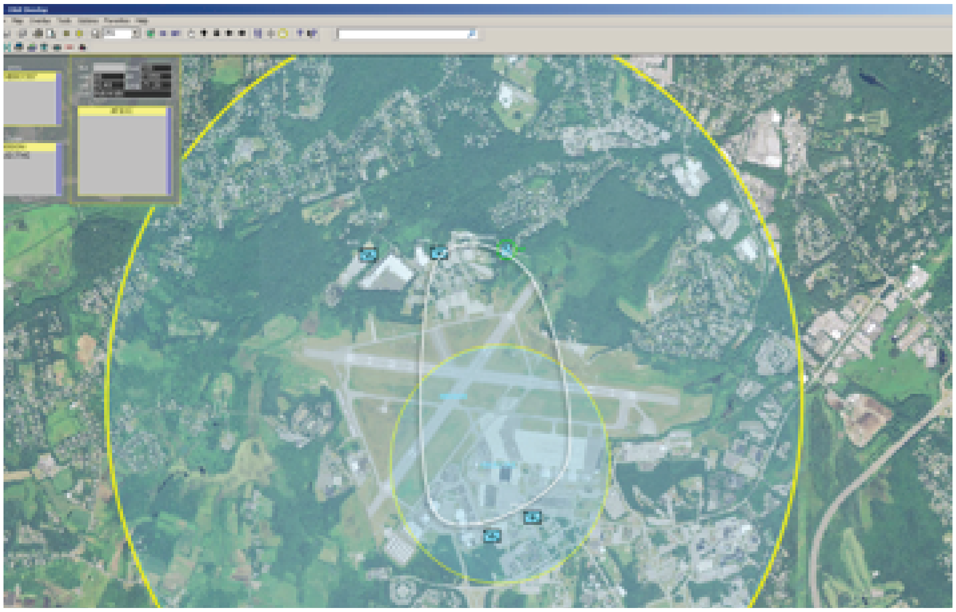

Figure 2. An operator, as part of mission planning, can specify not only the UAV's flight path (white line), but also which receivers or groups of receivers (e.g., a special forces unit) should have access to the UAV's video broadcast in which regions (circles). Lincoln Laboratory's dynamic group keying over-the-air-keying protocol implemented in LOCKMA can be used to automatically modify receivers' accesses on the basis of the UAV's GPS coordinates.

> Armed with LOCKMA and a very basic understanding of digital security, a competent engineer should be able to avoid myriad pitfalls that lead to compromised security of so many modern systems. This work aims to clear the last hurdles on the path to having cryptographic data protections being ubiquitous in devices and applications.

In short, LOCKMA enables cryptographic protections of static and dynamic data through key management.

Usability

LOCKMA was designed to simplify the task of integrating key management into applications. As such, it defines a small, intuitive programming interface to its KM functions. Furthermore, LOCKMA is not tied to any specific type of application data or any specific communication channel, thus allowing for it to be utilized in a wide variety of applications, including small, embedded devices such as microcontrollers and field-programmable gate arrays (FPGAs), and software systems.

LOCKMA was also designed so that application developers and end-users do not need to understand KM. By using LOCKMA, applications can provide users with only those concepts that are relevant to the users without encumbering them with notions of cryptographic keys or other lower-level technical concepts. LOCKMA is application agnostic, user-friendly, simple to apply to a multitude of problems, and transparent to higher-level user-defined software development.

For example, one application allows users to draw regions on a map and to specify which devices should have access to information in which regions (see Figures 1 and 2). This high-level information is translated into key management tasks in which LOCKMA automatically creates and securely distributes cryptographic keys to the right devices in real time on the basis of devices' geographical positions, time, and other considerations. This is all done transparently from the users.

Extensibility

LOCKMA is an "open architecture," meaning that it can be easily integrated into existing and new devices. This goal is achieved by defining all the messages and data elements by using highly extensible and interoperable Abstract Syntax Notation 1 and Cryptographic Message Syntax standards. Thus, if required by some application, LOCKMA can be extended to use new cryptographic algorithms, modes, or key lengths in a straightforward manner. ■

This work is sponsored by the Department of the Air Force Cryptographic Modernization Program Office (AFCMPO) under Air Force contract FA8721-05-C-0002. Opinions, interpretations, conclusions, and recommendations are those of the author and are not necessarily endorsed by the United States Government.