Novel Security Mechanisms for Mobile Code and Mobile Ad Hoc Network Environments

F. Sheldon[1], M. Neergaard[1], Richard R. Brooks[2] and A. Mili[3]

[1]*Computer Science and Engineering Division*
[2]*Electrical and Computer Engineering, Clemson University*
[2]*College of Computing Sciences, New Jersey Institute of Technology*

Principal Investigator and Point of Contact: Frederick T. Sheldon (sheldonft@ornl.gov, 576-1339)

Requested Budgets and Duration

FY 2006 Budget:	$ K
FY 2007 Budget:	$ K
Total Budget:	$ K

Initiative: Cyberspace Science / Knowledge Management

Invention Disclosures/Patents: None at this time, however, we expect intellectual property to arise from this project

Abstract: This proposal is submitted in furtherance of the *knowledge discovery thrust*, specifically in the area of mobile code security. The CSE division (CSED) has adopted a dual approach to knowledge discovery –from *questions* to *data* (formulating questions, then collecting sufficient data to answer the questions) and from *data* to *questions* (analyzing extant data to understand what questions can be answered). This approach is particularly timely in the field of mobile code security, where the exaggerated promises of COTS security products have usually led to unexpected compromises. Effective security is achieved using a dual approach: When a system is envisioned, the designers can define the *questions* (i.e., the required security properties) and demand sufficient *data* to provide the answers. Conversely, when a new security protocol or product is introduced, security analysts must understand what *questions* (i.e. what security properties) are answered by this particular set of *data* (i.e., the introduction of a new security product). For this project, ORNL researchers propose to follow this dual approach to develop novel security mechanisms for mobile code that ensure confidentiality, integrity, availability authentication and reliability. *Data will be used* to authenticate trust among trusted entities (mobile code) so that the trusted enterprise system cannot be compromised in a way that creates a new threat or exposes vulnerabilities. Untrusted mobile code may be isolated/inoculated to render it ineffective and non-threatening. Knowledge will be gained enabling real-time actionable decisions in the realm of enforcing security policies.

Program development and future funding from sponsors like DHS, ARDA, DARPA, DoD ONR and ARL will depend heavily on our ability to demonstrate proof of principle as well as complimentarity with ongoing CSED projects/research thrusts. Here we describe our tasking focus/plans. Proof of concept in the areas of security mechanisms for mobile code and ad hoc networks environments can be generalized, and will allow ORNL to successfully compete for solicitations from sponsors such as those listed above. In terms of science, the proposed research intersects areas like Knowledge Discovery, Cyber Security and Information Infrastructure, which are strategically important areas for ORNL. While ORNL is well-positioned to be a key participant in these areas based on prior successes and existing capabilities, these are also areas of intense competition that require a focus on critical application solutions, identifying gaps and advancing science to address the gaps. Clearly, in view of these considerations, the proposed research is essential, timely, and well-aligned with ORNL's strategic objectives and sponsor requirements.

Background: Mobile code refers both to code that migrates from platform to platform and to mobile platforms that carry code with them. Furthermore, mobile platforms often participate within a Mobile Ad-hoc NETwork (MANET). Consequently, as code/platforms have become increasingly mobile, the question of securing mobile code has become well known as a difficult problem. Indeed, a seminal paper in mobile agent security asserts that security concerns may outweigh the advantages of mobile code [1]. The Federal

Information Processing Standards endorse *confidentiality*, *availability*, and *integrity* as the core information security categories (challenges). Further, many computer security experts include *reliability* and *authentication* to the list of canonical security properties. These security standards have proven difficult to achieve or even meaningless in a mobile code environment.

- *Confidentiality* protects against unauthorized disclosure of information [9]. One of the most serious threats to confidentiality is infiltration. An insider could compromise an end node [3] and plant hostile code. MANET end nodes could easily be compromised because routing is dynamic and ad-hoc, man-in-the-middle attacks are feasible and expected.
- *Integrity* protects against unauthorized modification or destruction of information [9]. The integrity of data relies in large part on the quality of the routing network. But mobile code routing networks are not guaranteed to function. A MANET could easily be faulty, could garble messages, or could drop messages. Since MANETs can be in constant flux, it is neither possible to assign blame nor to intervene to fix network problems.
- *Availability* protects against disruption of access to or use of information or an information system [9]. But mobile nodes cannot guarantee availability. The communications abilities of mobile nodes are limited by the physical capabilities of their communications devices, so nodes can expect to be cut off from the network from time to time.
- *Authentication* is the process of establishing confidence in electronically presented identities [10]. If an adversary can hijack mobile nodes, confidence in identity becomes meaningless. A formerly trustworthy node does not lose any information, knowledge, or capability after falling into enemy hands yet a hijacked node can *also* provide any representation or reassurance that the trustworthy node could have provided.
- *Reliability* measures a systems ability to maintain stated performance objectives under stated environmental conditions for a stated period of time [11]. Mobile code runs on small platforms with inferior batteries, small memories, limited computing power, and faulty software, which presents the essential dilemma for deploying reliable mobile code/platforms.

Important and challenging research hurdles remain for defining novel cutting edge security primitives that can be used to demonstrate compelling revolutionary approaches that provide sound (including resilient/survivable) and dependable security assurances for real-world MANET deployments.

Research Tasks: The tasks enumerated below represent the first year of work on this LDRD. ORNL researchers anticipate a second year of funding devoted to follow-on work (i.e., second year will be scoped based on the results of the first year effort). Expected outcomes include a set of security targets (requirements), prototypes designed to satisfy a subset of targets for mobile ad hoc networks (trust gradients, clone detection, route tracing), proof of concept and technology demonstration/validation including interim and final reports (in addition to publication of any unclassified results).

Task 1: (Months 1-3) Develop a security target[1]

Much of the security analysis in the literature postulate codes that run on untrusted platforms, platforms that run untrusted code, or both [2]. These assumptions, however, do not completely describe many mobile code implementations. In many real-world applications, a limited number of mobile platforms are deployed pre-loaded with a small number of known software packages. Additional software packages could potentially be loaded if needed, but many mobile platforms will never load any additional software. The platforms are of known provenance, and are in the physical custody and control of their owners until they are deployed. Fielded sensors, mobile units given to first responders, and mobile battlefield units all fit this description. Accordingly, the security requirements and analysis are substantively different from the analysis in most of the literature. ORNL researchers will formulate security targets using the context of real world deployments.

Task 2: (Months 1-6) Develop specific approaches to help achieve the security targets

ORNL researchers will design and prototype a novel trust mechanisms based on the more realistic assumptions enumerated in Task 1. ORNL researchers will collaborate with Clemson professor R.R. Brooks, author of two books on mobile code and sensor security [6], [7] and with New Jersey Institute of Technology professor Ali Mili, associate editor of *IEEE Transactions on Software Engineering* since 2001,

[1] A *security target* is a set of security requirements and specifications to be used as the basis for evaluation of an information system and its associated resources [12].

and author of five books on software engineering. ORNL researchers have identified several novel security mechanisms to include in a prototype mobile network:

- *Trust gradients*: Consider a network with mobile, unattended sensors. The sensors can be accessed, cloned, or destroyed. The same network could incorporate fixed servers, constantly attended and surrounded by physical security. It is intuitively obvious that the servers are more trustworthy than the unattended sensors. Typical security models, however, find it difficult to distinguish multiple levels of intercommunicating trust[2]. ORNL researcher Frederick Sheldon and Professor Ali Mili can extend their collaborative relationship to formally define a gradient of trust, in which some units are trust worthier than others [13].
- *Clone detection*. Professor Robert Brooks has defined a novel method for key management that can help diagnose large numbers of copies cryptographic keys. He believes that use of this protocol and similar protocols can help mitigate the insider threat to mobile code networks [8]. ORNL researchers have discovered that the packet interchanges in Brooks' protocol can provide far more information about ad-hoc mobile networks than originally envisioned. Indeed, it may be possible to diagnose even one cloned node.
- *Route tracing*. Since the mobile code units were in the custody and control of friendly forces before their deployment, each unit can be pre-loaded with unique identifiers. These identifiers could be useful for a variety of reasons. For example, using recursive fixed size cryptographic hashes similar to Bloom filters, it is possible to probabilistically record the path taken through the network by each message. This information could reveal man-in-the-middle attacks, as well as identify units that are handling traffic in suspicious ways, such as asking to route traffic that should be routed in a different direction. These probabilistic records also allow calculations using a trust calculus such as the trust gradient noted above.

Task 3: (Months 4-10) Generate proof of concept demonstrations
ORNL researchers and collaborators will explore novel approaches, including those enumerated above. Those approaches that prove worthy of further investigation will be implemented as prototypes for further testing in Task 4.

Task 4: (Months 10-11) Validation Testing
The new technologies developed in Task 2 are designed to meet the security targets defined in Task 1. Using the prototypes generated in Task 3, ORNL researchers will evaluate these novel security mechanisms, understanding how the new technologies help security approach the security targets.

Task 5: (Month 12) Final report and publication.
This LDRD project represents an opportunity for ORNL to invent and prototype novel mobile code security solutions for a realistic environment. The expertise and technology developed through the course of this LDRD project will place ORNL in the forefront of a field of immediate and growing concern to the Department of Defense, the Intelligence Community, the law enforcement community, and the Department of Homeland Security. Through publication, ORNL can take their place as the premier research institution in mobile code security for realistic environments, securing standing and funding to provide security solutions to stakeholders throughout the US government.

References

[1] D. Chess, C. Harrison, A. Kershenbaum, "Mobile Agents: Are They a Good Idea?" IBM Research Division, T.J. Watson Research Center, Yorktown Heights, New York, March 1995, URL: http://www.research.ibm.com/massive/mobag.ps

[2] M. Hefeeda, B. Bhargava, On Mobile Code Security, CERIAS TR 2001-46, Purdue University, October 2001. (Discusses protecting mobile code and platforms from each other) (CERIAS, Purdue)

[3] Mads Dam and Pablo Giambiagi, 'Confidentiality for Mobile Code: The Case of a Simple Purchasing Applet.' Proceedings of the 13th IEEE Computer Security Foundations Workshop, Cambridge, 3-5 July 2000, pp. 233--244. (Encrypted functions)

[2] The field of Multi-Level System (MLS) design is similar, as it deals with multiple security levels. However, MLS design is fundamentally different in that such systems are designed to incorporate a small number of discrete levels, with minimal information interchange among levels. Only recently have policy makers considered obtaining technology that would allow information to flow from highly classified networks to unclassified networks.

[4] P. Kotzanikolaou, M. Burmester and V. Chrissikopoulos, \Secure transactions with mobile agents in hostile environments ", Proc. of ACISP http://citeseer.ist.psu.edu/kotzanikolaou00secure.html

[5] N. Borselius, "Multi-Agent System Security for Mobile Communication", Royal Holloway, University of London, September 2003, http://www.ma.rhul.ac.uk/techreports/2003/RHUL-MA-2003-5.pdf

[6] R. R. Brooks, Disruptive Security Technologies with Mobile Code and Peer-to-Peer Networks, CRC Press, Boca Raton, FLA, 2005.

[7] S. S. Iyengar and R. R. Brooks, ed.'s, Distributed Sensor Networks, CRC Press, Boca Raton, FLA, 2005.

[8] R. R. Brooks, Private Communication with M. Neergaard

[9] FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 199, STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS, February 2004, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[10] W. Burr et al., Electronic Authentication Guideline, NIST Special Publication 800-63, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

[11] Software Engineering Institute Open Systems Glossary, Carnegie Melon University, January 2005, http://www.sei.cmu.edu/opensystems/glossary.html

[12] Common Criteria for Information Technology Security Evaluation Version 2.1, Part 1: Introduction and general model, http://csrc.nist.gov/cc/Documents/CC%20v2.1/p1-v21.pdf

[13] R. Ben Ayed, A. Mili, F.T. Sheldon and M. Shereshevsky , "An Integrated Approach to Dependability Management", Foundations of Empirical Software Engineering: The Legacy of Victor R. Basili. St Louis, MO, May 16, 2005.