

UNCLASSIFIED
AN AGENT-BASED VULNERABILITY ASSESSMENT SYSTEM
INTENDED FOR TACTICAL DIGITIZED NETWORKS

Binh Nguyen
U.S. Army Research Laboratory (ARL)
AMSRL-CI-CN
Adelphi, MD 20783-1197

and

Constantine Tzatzalos
U.S. Army Communications-Electronics Command (CECOM)
AMSEL-RD-ST-SP
Fort Monmouth, NJ 07703
June 21, 2002

Date of Submission _____
Derived from _____
Declassify on _____

(U) ABSTRACT

(U) Preliminary results, progress to date, and plans to develop CyberSleuth for tactical digitized communications and information networks are reported in this paper. CyberSleuth is a conceptual prototype of an autonomously adaptive agent-based vulnerability assessment system, developed by U.S. Army Research Laboratory and its partners, capable of providing continuous protection of resource-constrained tactical-network computing equipment using genetic algorithms, dynamic object mechanisms, and agent technologies. The system has been successfully demonstrated on nonmilitary networks consisting of heterogeneous hardware platforms running disparate operating systems. Technical features of CyberSleuth and procedural issues for its eventual deployment in a tactical network are described and discussed in this paper with special emphasis on its mobility, functionality and integrity.

(U) INTRODUCTION

(U) Tactical digitized communications and information networks are the front-end of the Global Information Grid from which tactical information is collected, processed, disseminated, and exchanged. The tactical digitized communications and information network is a network of computing and communication systems that enables the war fighter to maintain information superiority. It consists mainly of dispersed computers that interconnect by various types of tactical radios and routers providing mobile wireless voice and data communication at different speeds and often operating in hostile environments. Precluding adversaries from exploiting the vulnerabilities of these tactical computer systems is

paramount because they are primary enablers for the tactical digitized network, which is part of the 21st century network-centric warfare.

(U) Traditional tools and techniques for assessing system vulnerability are unsuitable for tactical digitized communications and information network systems that operate in resource-constrained environments. For example, automatically assessing system vulnerabilities by performing all the tests is effective, but continuously doing it is impractical in the tactical digitized network environments because these tests would consume practically all computing and data-communication resources, and periodically doing it would create predictable windows of vulnerability when the tests are not performed.

(U) To alleviate these problems, U.S. Army Research Laboratory (ARL) and its partners from industry and universities successfully developed a conceptual prototype of an autonomously adaptive agent-based vulnerability assessment system called "CyberSleuth" during the concept-exploration phase of the project. CyberSleuth is capable of providing continuous protection of resource-constrained tactical digitized communications and information network environments using genetic algorithms, dynamic object mechanisms, and several kinds of agent technologies such as mobile agents, intelligent agents, autonomous agents, and cooperative agents [1]. The system has been successfully demonstrated on nonmilitary networks consisting of heterogeneous hardware platforms running disparate operating systems—Windows, Linux, and Solaris. This proof-of-principle prototype system was a tangible result of a successful basic-research project.

UNCLASSIFIED

UNCLASSIFIED

(U) The project is now in the demonstration-and-validation phase, during which technical efforts are focused on demonstrating the system on a tactical digitized network in the laboratory at U.S. Army Communications-Electronics Command (CECOM). Preliminary results and concurrent technical and procedural activities are reported in this paper, which is organized as follows. The next section presents a brief overview of CyberSleuth and its capabilities, followed by a report of past accomplishments and current activities. Then future work and a conclusion are presented in the last sections.

(U) OVERVIEW

(U) CyberSleuth is designed to provide continuous vulnerability protection of tactical computing assets operating in resource-constrained environments. It operates in dual modes, paranoid mode and suspicious mode. When CyberSleuth is in the paranoid mode, the Paranoid Agent uses environmental factors to adaptively select a subset of assessment techniques, dynamically compose mobile assessment agents, and dispatch them to a target environment to search for the existence of any vulnerability of which it has no foreknowledge. These techniques are also known as paranoid techniques. The results of the operation form the basis for the subsequent mode of operation—the suspicious mode, which operates as follows.

(U) Using the results of the system's paranoid mode of operation to form a basis for directing specific vulnerability assessment activities, the Suspicious Agent, which has access to a pool of suspicious techniques, creates and dispatches investigative agents to the target host to perform a series of specific assessments related to the vulnerability discovered in the paranoid mode. The results of the operation are recorded and formatted according to the application's requirements such as displaying alerts to the operator.

(U) The adaptability and intelligence of the CyberSleuth were mainly based on genetic algorithms; hence, genetic-algorithm terminologies such as "gene, genotype, and phenotype" are often used to describe its characteristics. A "gene" refers to a vulnerability assessment technique, and a "gene pool" is a repository of available assessment techniques. Whenever a new assessment technique is made available, it is simply added to the gene pool. A "GeneBean" refers to an assessment technique implemented as a JavaBeans™ component [2]. A "genotype" refers to a combination of some selected assessment techniques for constructing a "phenotype," which is an assessment agent.

(U) The mobility of an assessment agent was made possible by using a Java technology called "aglet" [3], a mobile-agent technology implementing a relatively novel network-computing paradigm. Mobility provides flexibility [4], and the benefits of which can be summed up by Lange and Oshima, the creators of aglets, that mobile agents can reduce network overload, overcome network latency, encapsulate protocols, execute asynchronously and autonomously, adapt dynamically, be naturally heterogeneous, and be robust and fault-tolerant [5].

(U) The ability of the correlator to search and analyze reported assessment results, and infer whether vulnerability exists was enabled by using an analyzing tool called Amzi! Prolog + Logic Server [6].

(U) This section briefly described CyberSleuth, a vulnerability assessment system that is mobile and intelligent. A more complete description of CyberSleuth can be found at [1].

(U) ACCOMPLISHMENTS

(U) Previous concept-exploration work resulted in a successful conceptual prototype of CyberSleuth running in non-military networks connecting disparate hardware platforms running disparate, popular operating systems such as Windows™ on Intel processors, Solaris™ on Sparc processors, and Linux on Intel processors. The targets for vulnerability assessment were performed only on Solaris and Linux systems because the assessment techniques were derived from the Computerized Oracle and Password System (COPS) security checker system [7], designed mainly for Unix systems.

(U) During development of CyberSleuth, several important milestones were attained. First, a dozen new vulnerability assessment mechanisms were fruitfully developed. Ten of these were an addition to an existing gene pool of assessment techniques for Unix systems, and the other two were a brand-new development for Windows platforms. All of these mechanisms were integrated and run successfully.

(U) Second, an evaluation of currently available toolkits for building mobile agents was carried out and concluded that the Aglet Software Development Kit (ASDK), now an open source, was still the most practical toolkit for developing CyberSleuth.

(U) Third, a diagram depicting the relationship among the Java classes used to create CyberSleuth was generated for technical documentation purposes using Unified Modeling Language (UML).

UNCLASSIFIED

UNCLASSIFIED

(U) Fourth, an acquisition of knowledge about the technical and procedural requirements for setting up a tactical digitized network and a decision about setting up a test bed implementing a small network reflecting the nature of the tactical digitized network have been completed.

(U) Last, it was realized that a number of important assessment criteria for CyberSleuth were needed to determine its viability on a tactical digitized network laboratory at CECOM. Important criteria for CyberSleuth and its subsystems include integrity, minimal bandwidth consumption and performance over imperfect tactical radio links.

(U) CURRENT PROGRESS

(U) The system continues to be evaluated on a wired network. New vulnerability assessment mechanisms for operating systems continue to be developed because exploiting operating-system vulnerability is still the most common method of attack used by intruders [8] and new vulnerabilities inherent in existing systems continue to be discovered. This is a recurrent event, which usually entails each potentially affected computing system be manually scanned and updated—a lengthy and laborious process that can be substantially alleviated by CyberSleuth. Whenever a newly developed assessment mechanism is developed, it is simply implemented as a JavaBeans component. The component becomes a GeneBean when it is stored in the gene pool. Once having been placed in the gene pool, the new GeneBean is used by CyberSleuth to create an evolving payload for its assessment agents.

(U) The mobility of these assessment agents enables an automatic and convenient method for assessing and updating every potentially affected computing system whose path is reachable from the node hosting the dispatcher of CyberSleuth. The scalability of CyberSleuth facilitates its deployment in any size of the network—from a small experimental network to a much larger operational one.

(U) Activities concurrent to the technical improvement of CyberSleuth include setting up an experimental network simulating a subnet of the tactical digitized network and acquiring essential knowledge, skills, hardware, and software for building one. A decision to build this network using Single Channel Ground and Airborne Radio System (SINCGARS) and Pentium-based computers running Solaris operating systems has been made, and software for running a digital command and control system has been acquired for testing connectivity purposes. Work has just been begun to install critical

software and hardware for enabling interactions between a computing host and a tactical radio.

(U) FUTURE WORK

(U) The current transformation of the Army into the Objective Force necessitates flexible design and implementation of CyberSleuth to operate in a different environment. CyberSleuth must operate in a Mobile Ad-hoc Network (MANET) environment since MANET is being identified as a promising technology that enables on-the-move communications for the Army's future highly mobile tactical forces.

(U) While the MANET technology is being developed, a SINCGARS network is being installed and will be completed at ARL in FY03. Once completed, the performance of CyberSleuth in this network will be evaluated, and its capabilities will be experimentally corroborated. Subsequently, CyberSleuth will be installed and tested in the tactical digitized network laboratory of CECOM. The network will provide a more realistic environment for judging CyberSleuth because the tactical digitized network has multiple routers connecting different tactical radios systems operating at different speeds. In this tactical digitized network environment, the concept of CyberSleuth will be furthermore developed, evaluated, and its performance will be used as a basis for transitioning it into tactical digitized networks and FCS communication systems.

(U) Security technologies and policies are also needed for integration into CyberSleuth to increase its chances for adoption by the end-user. CyberSleuth is now solely dependent on the security services provided by its hosting operating systems and the Java virtual machine on which it runs. CyberSleuth as of today has not incorporated any of the security technologies although they are described and discussed in the final report [1]. The described security technologies include public-key cryptography, digital certificates and signatures, access control, agent integrity, protection of mobile agents from hostile hosts, and protection of hosts from hostile agents. Future efforts will be concentrated on researching the most expedient security technologies for future tactical digitized communications and information network environments.

(U) CONCLUSIONS

(U) Primary results, current progress, and plans to develop an agent-based vulnerability assessment system called "CyberSleuth" have been briefly described in this paper. The use of genetic and artificial life algorithms will enable CyberSleuth to provide continuous protection of tactical digitized computing assests. Given the

UNCLASSIFIED

UNCLASSIFIED

topology of the Army's future combat systems (FCS) communications as mobile and fully dispersed in an ad-hoc manner, the mobile-agent paradigm could be well suited for maintaining constant connectivity in this exciting but challenging computing environment. The mobility of assessment agents provides an automatic and convenient method for assessing every computing system whose path is reachable from the node hosting the dispatcher of CyberSleuth. The bandwidth consumption and integrity of CyberSleuth is of paramount importance and needs to be assured. Security technologies and policies also need to be developed for integration into CyberSleuth to increase its chances for adoption by the end-user.

(U) ACKNOWLEDGEMENTS

(U) The authors appreciate Dr. Karamchetty and Dr. Gowens of ARL for reviewing this paper and for making changes to improve its quality.

(U) DISCLAIMER

(U) The findings in this paper are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

(U) Citation of manufacturer's trade names does not constitute an official endorsement or approval of the use thereof.

(U) REFERENCES

- [1] M. Little, M. Gaughan, G. Ferrari, A. Tardif, M. Conner, G. Cirincione, M. Younger, and C. Tzatzalos, "CyberSleuth: an Adaptive Agent-based Vulnerability Assessment System for Military Networks," *Advanced Telecommunications and Information Distribution Program (ATIRP) Final Report 1996-2001*, pp. 5.1-5.25, U.S. Army Research Laboratory, Adelphi, MD, June 2001.
- [2] Sun Microsystems, Inc., JavaBeans™ Component Architecture, <http://java.sun.com/products/javabeans>
- [3] IBM Japan, Aglet Software Development Kit Home, <http://www.trl.ibm.com/aglets/index.html>
- [4] Dejan Milojicic, Frederick Douglass, and Richard Wheeler, editors, *Mobility – Processes, Computers, and Agents*, Reading, MA: Addison Wesley, 1999.
- [5] Lange and Oshima, Seven Good Reasons for Mobile Agents, *Communications of the ACM*, Mar 1999.
- [6] Amzi!, <http://www.amzi.com/index.html>
- [7] D. Farmer and Eugene H. Spafford, "The COPS Security Checker System," *Proceedings of the Summer 1990 Usenix Conference, the USENIX Association*, pp. 165-170, Jun 1990. <http://www.cerias.purdue.edu/homes/spaf/tech-reps/993.ps>
- [8] Hulme, "Software's Challenge – It's Time for Developers to Think and Act Differently," *Information Week*, pp. 22-24, CMP Media LLC, 21 Jan 02, <http://informationweek.com/story/IWK20020120S0003>.