NPS-CS-03-005

NAVAL POSTGRADUATE SCHOOL
Monterey, California

Emergency Response For Cyber Infrastructure Management

by

George W. Dinolt
Cynthia E. Irvine
Timothy E. Levin

February 2003

Approved for public release; distribution is unlimited.

Prepared for: U.S. Department of Justice Office of Justice Programs and Office of Domestic Preparedness, under the aegis of the Naval Postgraduate School Homeland Security Leadership Development Program

20030401 060

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

RADM Admiral David R. Ellison
Superintendent

R. Elster
Provost

This report was prepared for Naval Postgraduate School Homeland Security Leadership Development Program and funded by the U.S. Department of Justice Office of Justice Programs and Office for Domestic Preparedness under interagency agreement no. 2002-GT-R-057.

This report was prepared by:

George W. Dinolt
Associate Professor

Cynthia E. Irvine
Associate Professor

Timothy E. Levin
Research Associate Professor

Reviewed by:

Neil C. Rowe
Professor
Department of Computer Science

Peter J. Denning, Chair
Department of Computer Science

Released by:

D. W. Netzer
Associate Provost and
Dean of Research

REPORT DOCUMENTATION PAGE

Form approved

OMB No 0704-0188

Public reporting burden for this 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, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	February 27, 2003	Technical Report

4. TITLE AND SUBTITLE

Emergency Response for Cyber Infrastructure Management

5. FUNDING

2002-GT-R-057

6. AUTHOR(S)

George W. Dinolt, Cynthia E. Irvine, Timothy E. Levin

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Center for Information Systems Security Studies and Research (NPS CISR)
Naval Postgraduate School, 833 Dyer Road, Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER

NPS-CS-03-005

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U. S. Department of Justice
Office of Justice Programs
810 Seventh St., NW
Washington, DC 20531

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words.)

The objective of this research is to investigate architectural mechanisms to provide an emergency response capability for Cyber Infrastructure management through the use of distributed, highly secure, protected domains. Instead of creating a costly physically separate cyber domain, logical separation is used. This work developed an architecture and prototype demonstration in the context of an open source operating system.

14. SUBJECT TERMS

Homeland security, security architecture, software ring, execution domain

15. NUMBER OF PAGES

4

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unclassified

Summary Report for

Emergency Response For Cyber Infrastructure Management

Period of Performance:

1 July 2002 to 31 December 2002

Principal Investigators:

George W. Dinolt, Associate Professor

Cynthia E. Irvine, Associate Professor

Timothy Levin, Research Associate Professor

1 Project Summary/Abstract

The objective of this research is to investigate architectural mechanisms to provide an emergency response capability for Cyber Infrastructure management through the use of distributed, highly secure, protected domains. Instead of creating a costly physically separate cyber domain, logical separation is used. This work developed an architecture and prototype demonstration in the context of an open source operating system.

2 Project Description

Introduction

Currently our national cyber infrastructure is vulnerable at both the node and router levels to attacks by adversaries ranging from untutored script-wielding novices to sophisticated threats from well-funded, well-organized groups and nation states. These attacks can result in the exposure of sensitive information, corruption of critical data, and the denial of system and network use by authorized entities. Although considerable effort has been devoted to the detection of attacks, little has been invested in infrastructure architectures that would permit a well-managed response to these attacks.

In a speech presented at the Microsoft Conference Center in Redmond, Washington on 4 June 2002, Richard Clarke, Special Advisor to the President for Cyber Space Security and Chairman, President's Critical Infrastructure Protection Board, called for research to create separate protected channels for the administration of critical components of the National Information Infrastructure. Such channels would permit the management of computers and networks even when the infrastructure was under attack and would permit the management components to allocate resources to services critical for local, state, and national response.

Current computer and network architectures do not provide separation of resource management services from those supporting run-time activities. Thus, through the corruption of payload and

runtime facilities, the ability to manage the information infrastructure or provide critical emergency functions can be sabotaged. Although a physically separate resource management / emergency response channel could be constructed, its cost would be prohibitive. Logical separation of management and runtime channels provides an alternative that can be implemented in the near term and can be integrated into existing and emerging network components.

Objective

The goal of this project is to develop an architectural mechanism to support separate protected communication and computation channels for *emergency response* that will automatically become available to local authorities during a time of crisis when the standard systems become unavailable because of natural disaster or human (terrorist?) activity. Use of this mechanism will allow resulting systems to operate in a fashion that is analogous to the emergency lighting system in a building. When the power goes out, enough lighting comes on to ensure that a safe exit of the building is possible. When standard communication and computer facilities are disrupted, then the emergency system should automatically become available for use to provide limited, temporary support to the local authorities so that they can continue to function.

The emergency-response capability we envision will be a managed subset of the national information infrastructure using the same physical components but logically separated as an independent out-of-band domain. Key network nodes, both processing and routing, will be emergency enabled by way of this multi-domain capability. Intrusion detection and other means will provide emergency response triggers for the transition of these nodes to a "safe" mode. Once in the safe mode, the protected nodes can process emergency and management functions without interference from other system and network activities, which will be temporarily halted. After the emergency situation is resolved, the non-critical activities can be re-enabled, perhaps gradually, to bring the system back to a normal state. For protected nodes, the logical separation of the protected domain will be their most critical and highly assured security function.

3 Approach

This project encompassed several interrelated tasks.

1. Analysis and design of domain architecture for infrastructure management
2. Implementation of extended attributes for domain management
3. Demonstration of domain separation to protect emergency response capabilities

The implementation task of the project is based on the OpenBSD code line. OpenBSD provides a stable development environment, and its emphasis on security and security auditing provide additional assurance, over and above that available through other commercial and open source operating systems, that trivial security errors such as buffer overflow do not occur. Many commercial entities rely upon open source platforms from the BSD family. This includes Yahoo, which runs 6000 BSD-based systems, and Hotmail, a Microsoft-owned email system.

Domain Architecture for Infrastructure Management

The protection domains provided at individual processing nodes is based on a *ring* architecture [Organick72]. In a generalized ring mechanism, the system binds subjects and objects to specific rings, and restricts accesses of subjects to objects based on their respective ring bindings. A *ring*

bracket mechanism extends rings to provide specific limitations based on the access mode (e.g., read, write, or execute). Thus, rings provide *protection domains* in which each object may be used.

In this task, a *software ring architecture* [Clark03] was developed to map specific elements of the general ring mechanism to the protection structures provided by OpenBSD [Watson01] (including our mandatory access control extensions), to provide a limited ring mechanism. This mechanism is of sufficient functionality to support emergency response domain separation, while allowing later extension to support a general ring bracket mechanism. The overall strategy is to leverage the assurances provided by the OpenBSD extended attribute and mandatory access control mechanisms, in support of global and persistent ring policy.

Extended Attributes For Domain Management

In this task, the extended-attribute label space provided by OpenBSD extended attributes was extended to define separate domains (rings) for critical and non-critical processing.

Demonstration

In this task, different security related programs were instrumented to take advantage of domain protection [Nguyen03]. A small-scale network environment was constructed to demonstrate the effectiveness of these mechanisms for protecting security-critical resources, processes and communication.

4 Results

Deliverables for Phase I of this work include:

1. Description of domain architecture for infrastructure management [Clark03]
2. Implementation of extended attributes for domain management
3. Demonstration and description [Nguyen03] of the use of domain management for protecting security-critical resources, processes and communication.

5 Future Work

Under this proposal, emergency protection domains have been designed and demonstrated for general-purpose processing (viz., end-system) nodes. Future work in support of emergency response for cyber infrastructure management, based on capabilities provided here, will be to control process scheduling based on domain attributes during emergencies, address the integration of intrusion detection and other network health-status triggers, the automated intercommunication of network status among protected nodes, and the domain protection of interior (e.g., router) nodes.

6 Value to the Objectives of the HS Program

This project has produced results that will directly increase capability of the US to defend and effectively respond to terrorist attacks against the national critical infrastructure. Specifically, using the techniques developed here, the information infrastructure can be better protected and

more resilient, and as a result, other infrastructures dependent on the information infrastructure can also be better protected. Thus, the national capacity to maintain emergency response capabilities in the face of cyber and other attacks is increased.

7 References

[Clark03] Paul Clark, et.al., Execution Policies Research and Implementation, NPS Technical Report NPS-CS-03-003, February 2003.

[Nguyen03] Thuy Nguyen, et.al, Policy Enforced Remote Login, NPS Technical Report NPS-CS-03-004, February 2003.

[Organick72] Organick, Elliot, The Multics System: An Examination of its Structure, MIT Press, Cambridge, MA, 1972

[Watson01] Watson, Robert, TrustedBSD Adding Trusted Operating System Features to FreeBSD, Proceedings of the USENIX Annual Technical Conference, USENIX, Boston, Mass, Jun-01.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library, Code 013
   Naval Postgraduate School
   Monterey, CA 93943-5100

3. Research Office, Code 09
   Naval Postgraduate School
   Monterey, CA 93943-5138

4. Darrell Darnell 1
   U.S. Department of Justice
   Office of Justice Programs
   810 Seventh St., NW
   Washington, DC 20531
   darnelld@ojp.usdoj.gov

5. Paul Stockton, Code 04 1
   Naval Postgraduate School
   Monterey, CA 93943
   pstockton@nps.navy.mil

6. Ted Lewis, Code CS/Lt 1
   Department of Computer Science
   Naval Postgraduate School
   Monterey, CA 93943-5118
   tlewis@nps.navy.mil

7. Dr. Cynthia E. Irvine
   Code CS/Ic
   Department of Computer Science
   Naval Postgraduate School
   Monterey, CA 93943-5118
   Irvine@nps.navy.mil

8. Mr. Timothy E. Levin
Code CS/TL
Department of Computer Science
Naval Postgraduate School
Monterey, CA 93943-5118
Levin@nps.navy.mil

9. George W. Dinolt
Code CS/Dg
Department of Computer Science
Naval Postgraduate School
Monterey, CA 93943-5118
gwdinolt@nps.navy.mil