LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-742007

Information Security Through Penetration Testing and Analysis Final Report CRADA No. TC-1217-95

S. Sparks, R. B. Miller

November 16, 2017

Disclaimer

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Information Security Through Penetration Testing and Analysis

Final Report
CRADA No. TC-1217-95

Date: December 4, 2000 Revision: 3

A. Parties

This project was a relationship between Lawrence Livermore National Laboratory and QUALCOMM Incorporated

The Regents of the University of California
Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94551
Sandy Sparks
Phone: (925) 422-6856
FAX: (925) 423-8002

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA 92121
Russell B. Miller
Principal Investigator
Phone: (858) 658-4833
FAX: (858) 658-5703

B. Project Scope

This project evaluated the information security posture of QUALCOMM regarding its Internet connections. It also enhanced and refined the ability of LLNL to perform these evaluations and add to its body of knowledge concerning Internet threats, vulnerabilities, and countermeasures.

The evaluations required a high degree of trust and cooperation between the assessors (LLNL) and the target organization (QUALCOMM). Without this high level of cooperation, the activity could easily have become an adversarial audit type situation and counterproductive to all parties.

C. Technical Accomplishments

There were four tasks in this project. Each task had its own deliverables.

Task 1: LLNL and QUALCOMM jointly assessed the secure nature of QUALCOMM's computers and networks to determine what improvements to the system were necessary.

> **Deliverable:** LLNL submitted an electronic assessment that evaluated and validated the QUALCOMM Firewall. Through its sampling technique, the assessment reflected the most prevalent current and near-term remote attacker capabilities. A written report was presented and discussed on site. The report assessed the information security posture of QUALCOMM and provided recommendations to improve the security of their applications and information based on the sampling information obtained. LLNL also provided a list of tools and techniques for protecting QUALCOMM IT resources.

Task 2: The Computer Security Technology Center (CSTC) jointly with QUALCOMM probed the firewall and previously vulnerable systems to determine if the recommendations were carried out effectively.

> **Deliverable:** A verbal report and unedited probe transcripts were submitted.

Task 3: The partners expanded Task 1 to explore all possible penetration paths and an extensive selection of workstations.

> **Deliverable:** There was a complete assessment based on a thorough exploration of QUALCOMM vulnerabilities. A more detailed report and presentation were submitted after consultations with relevant organizations.

Task 4: Task 3 was repeated after QUALCOMM responded to the recommendations.

> **Deliverable:** The parties completed an electronic re-assessment that effectively reflected existing and near-term remote and insider attacker capabilities. An addendum or updates to the written report were presented and discussed on site. The additional documentation indicated how QUALCOMM responded to the first assessment and described their revised (post initial assessment) security posture.

D. Expected Economic Impact

D.1 Specific Benefits:

QUALCOMM obtained information and methodologies to improve the security of their information systems, especially those directly or indirectly connected to the Internet. LLNL enhanced and improved their electronic penetration testing techniques and methodologies.

This work enhanced and improved the ability of the CSTC to perform electronic penetration assessments.

The cooperation of "real world" partners was significantly beneficial in the assessment process used throughout DOE. At the time of the CRADA, there were no effective realistic test environments to examine the latest tools and techniques. Industrial partners offered the latest computer environments and situations.

The information security response team for all DOE, the Computer Incident Advisory Capability (CIAC), was a part of CSTC and made immediate use of all new data and improvements in the assessments. CIAC performed many assessments each year for various DOE facilities. This project enabled CIAC to continue to provide DOE with that service. Secure Systems Services (S3) also provided assessments for many internal LLNL groups.

LLNL systems have been continuously modified, improved, and upgraded to meet the assessment findings. This clearly helped improve the Information Security posture of both external and internal DOE facilities, an overall security goal of the DOE mission.

E. Partner Contribution

For this effort, the Computer Security Technology Center /Secure Systems Services (CSTC/S3) of LLNL contributed its unique expertise, multi-disciplinary capabilities, and areas of technological strength. These unique resources included:

(1) the leading computing and network security product developers
(2) the DOE's response team — the Computer Incident Advisory Capability (CIAC)
(3) an extremely effective network of one-of-a-kind contacts available to address existing state-of-the-art computer and network security issues
(4) a staff of experienced, highly trained, extremely trustworthy individuals (Top Secret Security Clearance)
(5) an unbiased, customer oriented, vendor neutral perspective

CSTC/S3 applied its expertise in a highly leveraged and partner-oriented manner to:

(1) maximize cost-effective solutions to collaborating with QUALCOMM
(2) secure QUALCOMM 's information resources
(3) provide tools which QUALCOMM could utilize

F. Documents/Reference List

CRADA reports and other topic/periodic reports published for the project
None

Patent/copyright activity or pending applications
There was no patent/copyright activity.

Subject inventions disclosed by either the industrial partner or LLNL
There were no subject inventions disclosed by either partner.

Licensing status of Background Intellectual Property (BIP)
There were no licensing agreements.

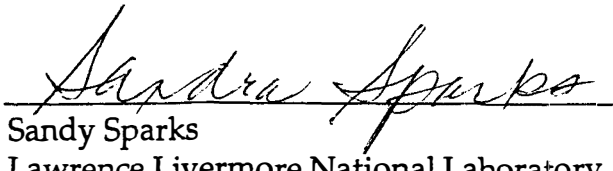
G. Acknowledgement

Participant's signature of the final report indicates the following:

1) The Participant has reviewed the final report and concurs with the statements made therein.
2) The Participant agrees that any modifications or changes from the initial proposal were discussed and agreed to during the term of the project.
3) The Participant certifies that all reports either completed or in process are listed and all subject inventions and the associated intellectual property protection measures generated by his/her respective company and attributable to the project have been disclosed and included in Section E or are included on a list attached to this report.
4) The Participant certifies that if tangible personal property was exchanged during the agreement, all has either been returned to the initial custodian or transferred permanently.
5) The Participant certifies that proprietary information has been returned or destroyed by LLNL.

March 1, 2001

Russell B. Miller — Date
QUALCOMM Incorporated



3/9/2001

Sandy Sparks — Date
Lawrence Livermore National Laboratory

Information Security Through Penetration Testing and Analysis

Abstract – Attachment I
CRADA No. TC-1217-95

Date: December 4, 2000 Revision: 3

A. Parties

This project was a relationship between Lawrence Livermore National Laboratory and QUALCOMM Incorporated

The Regents of the University of California
Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94551
Sandy Sparks
Phone: (925) 422-6856
FAX: (925) 423-8002

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA 92121
Russell B. Miller
Principal Investigator
Phone: (858) 658-4833
FAX: (858) 658-5703

B. Project Scope

This project evaluated the information security posture of QUALCOMM regarding its Internet connections. It also enhanced and refined the ability of LLNL to perform these evaluations and add to its body of knowledge concerning Internet threats, vulnerabilities, and countermeasures.

The evaluations required a high degree of trust and cooperation between the assessors (LLNL) and the target organization (QUALCOMM). Without this high level of cooperation, the activity could easily have become an adversarial audit type situation and counterproductive to all parties.