SAND2013-8820P

Unlimited Release

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

Project Accomplishment Summary

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories
Operated for the U.S. Department of Energy by
Sandia Corporation
Albuquerque, New Mexico

PROJECT ACCOMPLISHMENTS SUMMARY

Cooperative Research and Development Agreement (#1651.25.00)

between **Sandia National Labs** and **The Boeing Company**

Note: This Project Accomplishments Summary will serve to meet the requirements for a final abstract and final report as specified in Article XI of the CRADA.

Title: Cyber Concept Development and Evaluation

Final Abstract:

This project (called Krell within Sandia) was intended to develop techniques to predict malware exploits against or attacks on computer networks and to evaluate techniques for studying such attacks, with an eye toward attribution of the attack to a particular attacker. Sandia and Boeing each have networks that are subject to attack attempts; comparing and contrasting techniques used at each should provide guidance to each for doing that job better. Predicting such attacks is harder and much depends upon what data is used. Since data sharing is often difficult, we attempted to share tools and techniques so that each site could evaluate its own data using the others' tools.

Background:

Attribution and prediction are difficult in the realm of cyber intrusions. "Lies" are common on the Internet. Finding characteristics that are reliable in spite of incorrect or misleading information has been a continuing research problem. Since SNL has been relatively successful in cyber security of its own networks, it was appealing to see if any distillation and transfer of techniques would help another network-centric enterprise. Some of the less-operationally-focused techniques used by SNL 5600 were deemed appropriate to help concentrate the successful techniques into an appropriate instantiation for modeling of and application to the Boeing networks.

Description:

We explored computer network defense mechanisms by applying Live Virtual Construction (LVC) technology to a model of Boeing networked systems, and by sharing exploratory techniques that might provide value in predicting networked exploits. The characteristics of Boeing systems were provided by Boeing, and the LVC model was built to match and exercised by SNL. Prediction models (using email or social media as input) were typically machine learning models with added Predictive Behavioral Analysis techniques.

Benefits to the Department of Energy:

This project supports improving cyber defense at SNL and DoE by expanding modeling and simulation of computer networks, and by attempting to use predictive models to help with indications and warnings of network attacks. Research continues in the predictive models and the techniques introduced in the LVC model already reflect much of the state-of-the art in cyber defense used at SNL.

Economic Impact:

Exposure to SNL techniques may change Boeing computer network techniques, hopefully for the better. The shared work on predictive modeling has produced encouraging results that will need extra work before being incorporated into existing methods.

Project Status:

Krell is complete. We do not expect follow-on.

ADDITIONAL INFORMATION

Laboratory/Department of Energy Facility Point of Contact for Information on Project

Declan Rieb, 05952

Company Size and Points of Contact

Boeing Company, Information Assurance R&D, Computing Systems Technology
Randall E. Smith, randall.e.smith@boeing.com, 425-965-1353

CRADA Intellectual Property

None

Technology Commercialization

None

Project Examples

None

PROJECT ACCOMPLISHMENTS SUMMARY
Cooperative Research and Development Agreement (SC02/01651.25)
between **Sandia National Laboratories** and **The Boeing Company**

This summary has been approved for public release by Sandia and The Boeing Company

Sandia National Laboratories

By ______________________ 2013-07-26
Declan Rieb Date
Principal Investigator

Sandia National Laboratories

By ______________________ 7.15.13
Manager Date
WFO/CRADA Agreements

The Boeing Company

By Randall E Smith 8/9/2013
Title: Randall E. Smith Date
Principal Investigator

In order to expedite the process, if we do not receive your signed reply by 08/28/2013 we will assume your concurrence for the release of this document to the public.