



CALTECH-MIT/VOTING TECHNOLOGY PROJECT

Established by Caltech President David Baltimore and MIT President Charles Vest in December 2000 to prevent a recurrence of the problems that threatened the 2000 U.S. Presidential election. Specific tasks of the project include:

- *Evaluate the current state of reliability and uniformity of U.S. voting systems.*
- *Establish uniform attributes and quantitative guidelines for performance and reliability of voting systems.*
- *Propose specific uniform guidelines and requirements for reliable voting systems.*

TALK TITLE:

ATTACKDOG - A THREAT MODELING TOOL FOR SECURITY RESEARCH AND ANALYSIS ON VOTING TECHNOLOGY AND OTHER VULNERABLE SYSTEMS

DATE:

FRIDAY FEB 16TH

TIME:

4PM-5PM LECTURE, 5PM-6PM WORKING SESSION

PLACE:

DE ROTHCHILD ROOM, E-15 283A

ABSTRACT -

This talk will describe AttackDog is a multi user shared environment for evaluating the security of systems by developing threat models and evaluating countermeasures to attacks. It is currently being used to explore the security capabilities of voting technologies including the effort to understand the impact of deploying End-to-End Cryptographic Election technology. This threat modeling is being done in partnership with NIST and involves a team of more than 15 people from many institutions including Harvard, Yale, Stanford, UC Davis, and Microsoft Research.

The talk will explore how the tool and threat modeling in general can be used.

Speaker bio:

Eric Lazarus is a software architect who has consulted to such firms as: IBM, Prudential, JP Morgan, Millennium Management, Unilever/Lipton, GM, BMW, Ralston Purina / Nestlé Purina PetCare Company, and the New York Times. He is also Principal Investigator on The Machinery of Democracy: Protecting Elections in an Electronic World, is a veteran in the field of technology evaluation and the president of DecisionSmith, a consulting firm that builds computer systems that perform decision support and data warehouse functions and/or involve complex workflow. He was the technical lead on the Recommendations of the Brennan Center for Justice and the Leadership Conference on Civil Rights for Improving Reliability of Direct Recording Electronic Voting Systems

published in 2004 and continues his analysis of election technology threats currently with researchers at Stanford under an NSF grant.

The Machinery of Democracy study can be found at:

http://www.brennancenter.org/stack_detail.asp?key=97&subkey=36343

After a short break, the talk will be followed by an optional 1.5 hour training class in the use of AttackDog for those who are interested. It will cover:

- Building an example attack tree
- Linking attack trees together
- Parameterize nodes
- Employing trees to evaluate countermeasures
- Making threat models reusable

People completing this training will be in a position use the software to model potentially thousands of diverse attacks rapidly and simply and will be in a position to use it in their on research and consulting.

This research was performed under [The ACCURATE](#) NSF grant and with researchers David Dill and Tim King of Stanford University.

Talk Sponsor: Ted Selker, Caltech/MIT Voting Technology Project,
vtpadmin@media.mit.edu