Proceedings

Cybersecurity Applications and Technology Conference for Homeland Security

Washington, D.C.
March 3-4, 2009

CPS Conference Publishing Services

Los Alamitos, California

Washington • Tokyo

IEEE computer society

TABLE OF CONTENTS

SECURITY OF OPERATIONAL SYSTEMS

SECURITY AND TRUSTWORTHINESS FOR CRITICAL INFRASTRUCTURE PROTECTION

INVESTIGATIVE AND PREVENTION TECHNOLOGIES

NETWORK ATTACK FORENSICS (E.G., TRACEBACK)

TECHNOLOGIES TO DEFEND AGAINST IDENTITY THEFT

BROAD AGENCY ANNOUNCEMENT 07-09

BOTNETS AND OTHER MALWARE: DETECTION AND MITIGATION

COMPOSABLE AND SCALABLE SECURE SYSTEMS

NETWORK DATA VISUALIZATION FOR INFORMATION ASSURANCE

INTERNET TOMOGRAPHY / TOPOGRAPHY

ROUTING SECURITY MANAGEMENT TOOL

PROCESS CONTROL SYSTEM SECURITY

REAL-TIME SECURITY EVENT ASSESSMENT AND MITIGATION

DATA ANONYMIZATION TOOLS AND TECHNIQUES

INSIDER THREAT DETECTION AND MITIGATION

SMALL BUSINESS INNOVATION RESEARCH (SBIR)

SBIR 4.1-008: ADVANCED SECURE SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) AND RELATED DISTRIBUTED CONTROL SYSTEMS

SBIR 4.2-001: CROSS-DOMAIN ATTACK CORRELATION TECHNOLOGIES

SBIR 5.2-004: HARDWARE-ASSISTED SYSTEM SECURITY MONITOR

SBIR 6.1-007: NETWORK-BASED BOUNDARY CONTROL

SBIR 6.1-008: BOTNET DETECTION AND MITIGATION

RAPID TECHNOLOGY APPLICATION PROGRAM (RTAP)

RTAP CS1: BOTNET DETECTION AND MITIGATION

RTAP CS2: EXERCISE SCENARIO MODELING TOOL (ESMT)

EXTENDED ABSTRACTS FOR OTHER FUNDED RESEARCH