IARPA Reimagining Security with Cyberpsychology-Informed Network Defenses (ReSCIND)
Proposers' Day 28 February 2023

Michael Sieffert

Chief Engineer

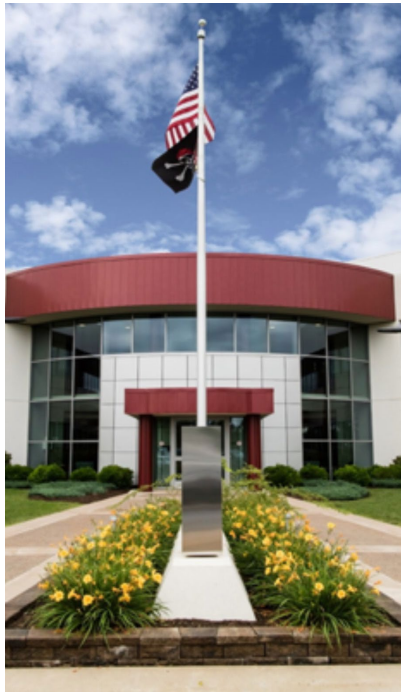
WWW.AINFOSEC.COM

Assured Information Security, Inc.

Capabilities in Cyber Security, Artificial Intelligence, Offensive and Defensive Cyber Operations, Penetration Testing/Red Teaming, and Cognitive Psychology and Behavioral Science

About AIS

Technology Pioneers and Cybersecurity Innovators



- Founded in 2001
- Headquartered in Rome, NY
- 200+ Employees

AIS specializes in high-risk research and development. We provide industry-leading cyber and information security services and innovations to counter next-generation threats.

Supporting the Department of Defense and Intelligence Community

+

Performers on more than 35 DARPA contracts since 2005 as well as IARPA CAUSE and SCITE

Capabilities

- **Offensive Cyber Operations**
- **Defensive Cyber Operations**
- **Cyber Security**
- **Artificial Intelligence**
- **AI and Automated Decision Making for Cyber Defense**
- **Machine Learning**
- Cutting Edge Cyber Research
- Autonomy
- Reverse Engineering
- Embedded System Security
- Trusted Computing Technologies
- Rapid Prototyping
- Advanced UAS Research and Capabilities
- **Software Development and Integration**
- **Cognitive Psychology and Behavioral Science**
- Malware Analysis
- Signals Technology
- Biometrics
- **Penetration Testing/Red Teaming Services**
- Signal Exploitation and Analysis (SIGINT)
- Audio Processing and Linguistics
- Multi-Level Domain Solutions
- Cyber Core Services
- **Cyber Attack Modeling**
- **Semantic Modeling**

AIS – IntroVirt®

AIS Introspective hypervisor (API) for writing tools that monitor user behavior and activity within VMs

Cornerstone of numerous DoD and IC technologies

Granular monitoring/manipulation of code executing in VMs

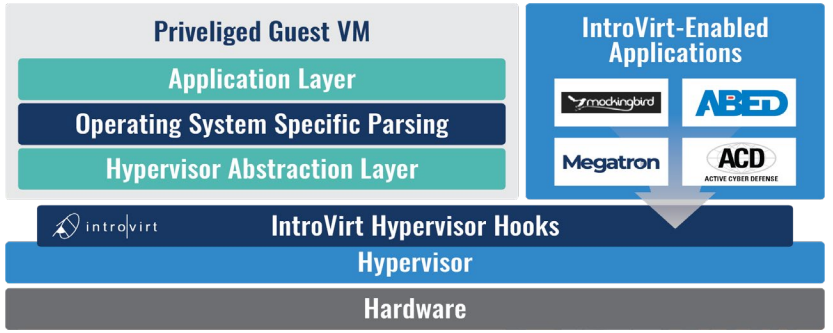
- API for rapid capability development
- Control the data flow through system calls and APIs
- Effect cyber deceptions, code monitoring, data flow, etc.

Ideal platform for building code monitoring tooling

- Will not conflict or interfere with code inside VM

ReSCIND benefits:

- Monitor operator activity and attacker progress
- IntroVirt is open-source software (no vendor lock-in)



DARPA/I2O Active Cyber Defense (ACD)

User and cyber attacker monitoring for adversary manipulation

Leveraged IntroVirt® to monitor production network user activity

- Intercept system call behavior of specific applications
- Translate system call sequences to *high-level semantic behaviors*
  - Emails sent and received, files accessed/moved, web browsing activity
- Actuated user activity on surrogate network to maintain realism

Experience implementing novel cyber defense paradigms

ReSCIND benefits:

- Defensive Cyber Operations Technology
- User and user activity monitoring technology
- Environment for influencing adversary trust and elicitation of tactics, techniques, and procedures

Megatron

Cyber Deception Framework

Framework to monitor malicious actors and control their view of the system/network

- Pluggable collection of single-purpose deceptions
- Host-based deceptions control how the system behaves for attacker software
- Deception-based deceptions control the appearance of network resources

API for integrating third-party deceptions

Focused on ‘aiming’ deceptions *only* at malicious code (not normal stuff)

ReSCIND benefits:

- Manipulate cyber adversary cognitive state and trust by manipulating the appearance of targeted networks
- Modify user behavior, trust, and cognitive states

DARPA/I2O Cyber Genome

Malware modeling and recognition

Recognize, defend, and respond to malware

- Builds comprehensive phylogeny of known malware
- Rapidly assess new digital artifacts
- Predict properties of new attacks using attacker models

Relevant because of the experience detecting malicious code and *inferring an effective defense* for defensive operators

ReSCIND benefits:

- Cyber Attack Modeling Technology
- Offensive and Defensive Cyber Operations expertise
- Techniques applicable to monitoring user behavior and activity, to contextualize user cognitive state and/or load

DARPA/I2O Configuration Identification Normalization & Enforcement (ConfINE)

Inferring and Effecting Secure Network Configurations

Gather network and host configurations

- Leverage AIS's pluggable cyber-operations mission distribution framework, Metasponse (TRL 9)
- Metasponse accesses large numbers of hosts (<500k), running small collectors
- Collected data used to infer formal specs and to generate a secure config
- Push out configuration updates in similar manner as they were gathered

Monitor hosts for deviations in secure configuration

Relevant experience in reducing attack surfaces and eliminating configuration-based vulnerabilities

ReSCIND benefits:

- Defensive Cyber Operations Experience
- Cyber Attack Modeling

VIC3TORS Project

Major DARPA effort for behavioral monitoring and identification of adversary cyber actors across systems

Developed techniques to track adversary cyber operators across their personal and operational systems

- Mobile devices, laptops, desktop systems, tablets, etc.

Developed a collection of biometric techniques using commodity device sensors to verify users through unique patterns in movement and other behaviors

- Gait detection techniques
- Mouse behaviors
- Keystrokes
- Touch screen/swipe behaviors

ReSCIND benefits:

- Supports accurate models of human behavior and movement, particularly gait
- Designed to detect features unique to the individual
  - Expand to create population specific anomaly detection
- Human subject research

Prediction and Analysis of Cyber Scenarios (PACCS)

Passive techniques to measure cognitive load through behavioral biometrics and unobtrusive sensors

Conducted under internal research funding

Designed experiments to induce cognitive load in test subjects

- e.g., memorization of a multi-digit number while performing a typing-focused task

Ground truth established via EEG

Passive sensors used to collect behavioral patterns of subjects

- e.g., keystroke data

Models developed to classify cognitive load

- Models for varying levels of cognitive load
  - Four-state model
  - Two-state model (Low/High cognitive load)
- Models for generalized cognitive load, across all users, and for specific cognitive load (per user)

The generalized model that applied across all users was not predictive, however models trained for individual users were predictive

- In distinguishing between all users, the predictive accuracy was 0.69 (+/- 0.15),
- Distinguishing between low (control) and high (5- and 6-digits) workload was significantly more accurate and less varied at 0.88 (+/- 0.08)

ReSCIND benefits:

- Passive techniques for monitoring user behavior to detect cognitive load
- Human subject research

National Cyber Range (NCR)

Active as Cyber Security Evaluation Team (CSET) at NCR

NCR is the de facto environment for testing and evaluating cyber operations technologies for the DoD and IC

AIS provides vulnerability assessment and penetration testing

- Red-team assessments and testing and evaluation through
- Focus on software throughout the operations lifecycle
- Bring architecture and source code audits expertise
- Exploitation expertise against operating systems, networks, embedded systems, etc.

ReSCIND benefits:

- Vulnerability Assessment and Penetration Testing Expertise
  Red Teaming Expertise
- OCO/DCO
- In addition, AIS serves as a red team on multiple DARPA programs

Contact Us

Mr. Michael Sieffert

Chief Engineer

sieffertm@ainfosec.com

ais

WWW.AINFOSEC.COM