Partnership Opportunities

Agenda

- About The Center for Information Assurance and Joint Forensics Research
- Opportunities for Collaboration
- Partnerships and Advances
- Questions and Next Steps

The Center

- Operates within the College of Arts and Sciences at UAB
- Established in 2011
- Interdisciplinary research center born out of a joint computer forensics program created by the departments of Computer and Information Sciences and Justice Sciences
- Members are professors, students, community members, and professional partners across varying disciplines
- Founding member of the Alabama Cyber Research Consortium launched in 2013

Areas of Research

- Cybercrime
- Intelligence Analytics
- Forensic Science
- Geospatial Informatics and Imagery
- Information Assurance/Security
- Health Informatics
- Data Science

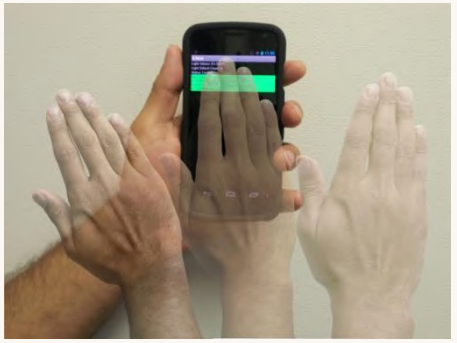
Research and Development Opportunities

Research is at the heart of the Center.
Through partnerships with corporations, agencies, and the community, the Center is able to create a first-class institution drawing the best and brightest researchers and students empowered to discover and create meaningful change.

SPIES: Security and Privacy In Emerging Systems

- Led by Dr. Nitesh Saxena (Associate Professor of Computer Science)
- Main focus
  - Device-Centered Security
  - User-Centered Security
- Practical, Transformative and Interdisciplinary approaches to security
- Over $4M in total funding from NSF as well industry including Google, Cisco, Nokia, RIM, Intel, and others
- Integration of research with education
  - leadership of educational programs (such as UAB CFSM; NYU-Poly CyberSec)

Selected SPIES Projects



- Smartphone Malware Defense
- Payment Token Security and Privacy
- Strong Password Authentication
- Secure and Private Cloud Storage
- Playful Security
  - e.g., game CAPTCHAs
- Neuroscience-Informed Security
- Mobile PoS Security

SPIES Contact Details

- Nitesh Saxena: saxena@uab.edu
- Visit: http://spies.cis.uab.edu

Social Media Phenomena

John Grimes, Lead P.I.

Concept(s)

* Financial services customers today have yet to fully understand or appreciate the potential consequence management trade-offs when they engage in mixing social media activities over common data platforms upon which they also conduct management of their financial affairs.

Objective(s)

- Financial services customers, like all of us, are motivated by *habit* and *convenience*;
- Expect 24/7/365 access to financial data services…
  - any time,
  - from any place,
  - with minimal user authentication steps, and
  - minimal personal information revealed.
- ***And All Completely Secure!***

Application(s) & Impact(s)

* The need to partner with customers is essential to successfully combat the levels of sophisticated threat(s) in the age of cyber.
* This evolving measure of trust relationship between both customer and financial service provider has now become more essential than ever to successfully *detect*, *assess*, *defend* and *defeat* the threat(s) of today and the future.

Targeted Result(s)

- **Empower the customer to assume more responsibility for managing the security of their own financial transactions.**
- **Develop tiered levels of *alacarte* financial services based upon proof of prerequisite cyber security savvy and risk assessment decision making.**
- **Reapportion the risk shared between customer and service provider commensurate with customer's demonstrated ability to avoid self-inflicted and preventable harm from high-risk behavior when comingling SM and financial affairs.**

CIA | JFR Intelligence Analytics ////////// POC: John Grimes ////////// 205.934.8509 ////////// jwgrimes@uab.edu ///////

Insider Threat Phenomena

John Grimes, Lead P.I.

Concept(s)

* The two greatest threats to Operational Security in any context remain **habit** and **convenience**. Our data suggests that the cyber security threat level only increases exponentially in risk and potential consequences when it originates from within the inner circle of the person or enterprise under attack, due to the unique placement and access of the insider/attacker(s). And nowhere is this threat vector more acute than in the context of the **Social Media Phenomena** (SMP). Increasingly, we face risks to our most critical personally identifiable information (PII), networks and systems from trusted "friends," frequent visitors and those who are "hiding in plain sight."

Objective(s)

Through adaptive application of counter-intelligence (CI) community analytics we develop a tailored predictive modeling diagnostic framework that integrates a diverse set of data sources from the cyber domain and inferred psychosocial/motivational factors underling malicious insider exploits. This comprehensive *threat v. vulnerability* assessment approach provides automated support for the detection of high-risk behavioral "triggers" or precursor signatures to target the CI analyst's attention and inform the risk analysis. Domain-independent, this system may be applied to diverse threat, warning and vulnerability problem set scenarios.

Application(s) & Impact(s)

Insider attacks are motivated by ***revenge*** (e.g., to harm) and ***greed*** (e.g., to steal). Current practice is forensic in nature, relegating to the analyst the bulk of the responsibility to monitor, analyze, and correlate an overwhelming amount of data from multiple sources and degrees of reliability (i.e., *"How do we connect the dots when the whole page is black?"*). Unfortunately, no single intrusion detection or threat assessment technique in wide use today gives a complete or actionable picture of the insider threat problem.

Targeted Result(s)

Rather than focus on detecting malicious acts after they occur, with the aim of identifying and disciplining the perpetrator(s), through application of CI analytics we are able to correlate multiple sources and patterns of behavioral data to recognize potential threats by early detection of precursor signature behaviors or "triggers" utilizing model-based decision propagation diagnostic modeling; using psychosocial indicators as well as cyber indicators of potential abuse of trusted resources to identify and proactively respond to possible malicious exploits. Some indicators may be observed directly, while others are inferred or postulated from observed data. Defining triggers in terms of observable cyber and psychosocial indicators and higher-level aggregated patterns of these behaviors is a major challenge, but also a critical ingredient of a predictive methodology.

CIA | JFR Intelligence Analytics ////////// POC: John Grimes ////////// 205.934.8509 ////////// jwgrimes@uab.edu ///////

Natural Language Phenomena

Steven Bethard and Thamar Solorio

Concept(s)

While engaging with online services, users produce a variety of pieces of natural language in large quantities, from emails to tweets to forum comments to support requests. Such natural language can implicitly reveal important attributes of the user and can help predict future user behavior.

Objective(s)

- Apply machine learning and computational linguistic techniques to identify common user patterns implicit in the language
- Leverage learned models of user language to predict user attributes (e.g. opinions of products) and behaviors (e.g. creation of invalid accounts)

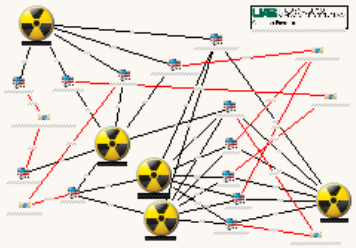
Application(s) & Impact(s)

- Identifying invalid duplicate accounts via idiosyncratic vocabulary or typing patterns
- Triaging support requests to route messages to potential answer sources
- Mining user discussions for opinions on products to assess confidence
- Aggregating facts across multiple languages

Targeted Result(s)

- Improved security through removal of invalid accounts
- Faster delivery of more accurate and helpful responses to support requests
- Better product targeting and development guided by user feedback
- Improved services for the global setting

Contact Information: bethard@uab.edu, solorio@uab.edu



Cybercrime Analysis

Gary Warner

Concept(s)

Cybercrime and traditional crimes leave behind many forms of digital evidence. Due to the unique ability of cybercrimes to impact thousands or even millions of victims, automated collection, preservation and analysis is necessary to assist law enforcement and other investigators. In our lab, we develop tools, techniques, and training to enhance our ability to detect, analyze, and respond to cybercrime.

Objective(s)

- Leverage our strengths in Data Mining and Big Data Analytics to preserve, analyze, and investigate artifacts of Cybercrime
- Focus areas include:
  - Malware Analysis & Intelligence
  - Open Source Intelligence
  - Best practices in Forensics Analysis

Application(s) & Impact(s)

- Mining logs & incident response data for evidence
- Analyzing malicious binaries to identify malware trends and relationships between binaries
- Identification of harmful network addresses that serve as indicators of infection
- Developing techniques for the automation of OSINT gathering and analysis

Targeted Result(s)

- Improved effectiveness in responding to malware and botnets through superior analysis
- Increased ability to protect networks through rapid identification of emerging threats
- Significant time-savings in gathering OSINT related to incidents or investigations
- Effectively trained workforce prepared to work as incident handlers, analysts or investigators

Contact Information: gar@uab.edu

Cloud Security and Forensics

Ragib Hasan, Lead P.I.

Concept(s)

* Cloud Computing has become the dominant computing technology, especially for Big Data. However, today's clouds are not secure, accountable, have support for forensic investigations, and do not comply with data regulations such as Sarbanes-Oxley Act (SOX) or HIPAA. This limits their use in business and healthcare.

Objective(s)

- By leveraging our expertise in securing data and provenance, we will create an architecture for making clouds accountable, trustworthy, and capable of allowing forensic investigations.
- We will implement the accountability architecture in industry-standard OpenStack platform and evaluate for performance and compliance.

Application(s) & Impact(s)

* An accountable cloud provides users with information about the history of their data and applications (e.g., who had access to data, who is responsible for specific modifications, where were the data located physically,
* An accountable cloud will comply with SOX, allowing financial companies to use public clouds for their data and also enable forensic audits.

Targeted Result(s)

- Bring transparency to financial transactions and data stored in a cloud by providing customers as well as financial companies with required information about what happens to their data inside a cloud.
- Enabling forensic audits and providing integrity guarantees will allow compliance with SOX and other regulations while save money through the use of cheap public cloud.
- Allow innovative and trustworthy payment systems through the use of accountable provenance and data processing in clouds

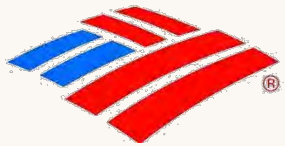
CIA | JFR Information Assurance ///// POC: Ragib Hasan ///// 205.934.8643 //// ragib@uab.edu ///// http://secret.cis.uab.edu

Advancement Opportunities

UAB looks to partner with corporations and organizations to create unique learning opportunities that capitalizes on the strengths of each institution and helps shape the next generation of cyber professionals through participation in experiential-based learning and internship programs.

- Scholarship support
- Internship Program

Partnerships and Collaborations



The Facebook Suite – Center Headquarters

Contact Information

thecenter.uab.edu

Rish Wood , Consultant (256) 441-8208

rwood@catalystdc.com