



# School of Computing Research Capabilities

The School of Computing has research interest in the following areas. USA is an NSA/DHS Center of Academic Excellence in Information Assurance / Cyber Defense and a participant in NSF's Cyber Corps Scholarships for Service. The following topics are of interest to both industry and academia.

## **1. Computing Forensics and Digital Investigations**

---

The SoC Digital Forensics Information Intelligence (DFII) Research Group meets weekly during the academic year. The research interest ranges from malware to cloud computing to SCADA devices, organizational investigations, hardware evolution, and the impact that all of these areas have on forensic tools, processes and investigations. SoC investigators collaborate to conduct basic and applied research that is brought into our classrooms. [Barnett, Black, Yasinsac]

## **2. Critical Infrastructure Protection**

---

Presidential Policy Directive 21 (2013) established protecting the nation's critical infrastructure as a national priority. SoC researchers examine risks to end user oriented critical cyber infrastructure components such as automobiles, airplanes, and medical devices. We also study computer systems that control water flow and that regulate electrical grids, lighting systems, traffic signals, and analogous sensors, actuators and control devices. [Andel, McDonald, Damopoulos]

## **3. Advanced Persistent Threats**

---

Advanced Persistent Threats (APT) may be the greatest single threat to effective use of the Internet today. Networks of rogue computers are created by attackers with vast resources, e.g. criminal and state-sponsored actors and are designed to carry out coordinated acts of malice. SoC researchers study technology that can combat APTs through malware analysis, reverse engineering, intrusion detection, secure software, and network security research. [McDonald, Andel]

## **4. Secure Software**

---

Most computing system threats manifest through implementation flaws resulting from poor software development practices. SoC researchers investigate techniques to improve rigor in software development, the impact of anti-forensic software, and potential detection solutions. [Andel, McDonald, Yasinsac]

## **5. Insider Threats**

---

Most Security approaches are based on the classic Maginot Line concept, where the defenders are inside the perimeter and the attackers are on the outside. SoC investigators study technology and man-machine interface sciences to prevent, detect, and respond to attacks made by trusted parties that violate privilege that is given to them. [Yasinsac]

## **6. Informatics (Healthcare, Bio, etc.)**

---

The USA Health Informatics Research Group is currently focused on two major areas of research, education and outreach: risk assessment of healthcare systems and health informatics curriculum development. The USA Health Informatics Group is emerging as a center of research for risk assessment of healthcare data and systems and pedagogical innovations in health informatics curriculum and education. We are seeking colleagues with mutual interests to pursue publication and grant opportunities in our identified research themes or closely related areas. [Campbell, Pardue, Bourrie, Sittig]

## **7. Big Data and Cloud Computing**

---

The volume and diversity of data being collected impacts an investigation. Rapid increases in computing and storage technologies have revolutionized the collection and processing of immense volumes of data. SoC investigators study advanced techniques to identify correlations in vast databases that can lead to improvements in cloud security, medical research, and other big data applications. [Johnsten, Benton, Huang, Bourrie, Black, Shropshire]

## **8. Internet Voting**

---

Driven by the pervasive distribution of personal computing devices, there is strong inertia to engage Internet voting in national elections in spite of spirited objections regarding security risks of counting electronically delivered ballots. SoC investigators study theoretical limitations that impacts voting system decisions along with security practices that may enable expanded engagement of technology in election processes. [Andel, Yasinsac]

## **9. Cyber-STEM Education**

---

In 2012, SoC established a K-12 Partner School Program to advance Cyber STEM research, education, and familiarization through local schools. This includes examining techniques for increasing STEM adoption by students in underrepresented groups and improving computing proficiency for K-12 teachers. [Chapman, Black, Barnett, Yasinsac]



## **I 0. Industry 4.0**

---

Driven by our Industry Partners seeking implementations of Industry 4.0 that realize the benefits of same, this research group enjoys presentations by participants of ongoing research and work being done in the field, presented as it relates or might relate to the application of Industry 4.0 objectives. These include Interoperability, information transparency, technical assistance, decentralized decision-making, machine to machine communication, human-machine interface and cyber physical systems. [Barnett, Black, Green, Damopoulos]

## **I 1. Predictive Analytics**

---

Driven by the Nation Science Foundation's Big Ideas (2017), Harnessing Data for 21<sup>st</sup> Century Science and Engineering looks for ways to incorporate data science with the current data revolution. Techniques from artificial intelligence, data mining, machine learning, predictive modeling, and statistics can be used to make predictions about unknown future events based on current data. SoC researchers harness these technologies to develop predictive systems to solve real-world problems that are intuitive to the end-users. [Benton, Bourrie, Huang, Johnsten, Segev, Sittig]

## **I 2. Machine Learning**

---

Machine Learning is the field of study that gives computers the capability to learn without being explicitly programmed, i.e. without any human assistance. The process starts with feeding good quality data and then training the machines (computers) by building machine learning models using the data and different algorithms. The choice of algorithms depends on what type of data you have and what kind of task you are trying to automate. SoC investigators are actively involved in (a) adopting existing methods to solve real-world applications and (b) developing new learning techniques that can generate more accurate models in less time. [Benton, Duraisamy, Johnsten, Segev]