Introduction to Inside the Insider Threat Minitrack

Jason W. Clark
Carnegie Mellon University
jwclark@cert.org

This year we have an exciting mini-track entitled "Inside the Insider Threat" planned for you. The mini-track will discuss the topic of insider threats which are a present and growing concern to organizations worldwide. This is due in large part because trusted employees have the capability for inflicting devastating consequences to their employer's assets, data, and IT infrastructure, primarily because of their detailed knowledge and authorized access these systems. Any approach therefore must have not only a technical aspect, but also a non-technical (social, political, legal, cultural, and so forth) approach. Analyzing and detecting insider threats involve both technical and non-technical approaches across many different disciplines, including human-oriented ones. This mini-track accepted four papers emphasizing this cross-cutting work in this exciting and important research area.

The first paper is:
Federated Platooning: Insider Threats and Mitigations

Platoon formation is a freight organization system where a group of vehicles follows a predefined trajectory maintaining a desired spatial pattern. Benefits of platooning include fuel savings, reduction of carbon dioxide emissions, and efficient allocation of road. In this paper, the authors look at federated platooning from an insiders' perspective. First, they outline the basic elements of platooning and federation of platooning operators. Then, provide a comprehensive analysis to identify the possible insiders (employees, users, operators, and federated members) and the threats they pose. Finally, the authors propose two layered, composable technical solutions to mitigate those threats:

1) a decentralized overlay network that regulates the interactions among the stakeholders, useful to mitigate issues linked to data safety and trustworthiness and

(2) a dynamic federation platform, needed to monitor and interrupt deviant behaviors of federated members.

The second paper is:
Leader Member Exchange: An Interactive Framework to Uncover a Deceptive Insider as Revealed by Human Sensors

This study intends to provide a theoretical ground that conceptualizes the prospect of detecting insider threats based on leader-member exchange. This framework specifically corresponds to two propositions raised by Ho, Kaarst-Brown et al. [42]. Team members that are geographically co-located or dispersed are analogized as human sensors in social networks with the ability to collectively "react" to deception, even when the act of deception itself is not obvious to any one member. Close interactive relationships are the key to afford a network of human sensors an opportunity to formulate baseline knowledge of a deceptive insider. The research hypothesizes that groups unknowingly impacted by a deceptive leader are likely to use certain language-action cues when interacting with each other after a leader violates group trust.

The third paper is:
Modeling Expert Judgments of Insider Threat Using Ontology Structure: Effects of Individual Indicator Threat Value and Class Membership

The authors describe research on a comprehensive ontology of sociotechnical and organizational factors for insider threat (SOFIT) and results of an expert knowledge elicitation study. The study examined how alternative insider threat assessment models may reflect associations among constructs beyond the relationships defined in the hierarchical class structure. Results clearly indicate that individual indicators contribute differentially to expert judgments of insider threat risk. Further, models based on ontology class structure more accurately predict expert judgments. There is some empirical evidence that other associations among constructs—such as the roles that indicators play in an insider threat exploit—may also contribute to expert judgments of insider threat risk. Implications for research and practice are discussed.

The final paper is:
Connected Aircraft: Cyber-Safety Risks and Management Approaches

The past several years has witnessed significant growth in Internet Protocol (IP)-based wireless connections between airborne aircraft, satellites, and terrestrial information systems, a phenomenon some have termed "The Connected Aircraft" (Bellamy, 2014). Far eclipsing passenger high-speed internet service, this movement is integrating thousands of embedded automated sensors connected to safety-critical systems, such as engines, flight controls, cockpit displays, and life support systems into the on-line infrastructure. Airborne sensors continuously send data

packets to worldwide airframe, engine, and avionics manufacturers, airline control centers, and third-party suppliers (Orjih, 2006). The tremendous growth in the Internet of Things (IoT), small, low-power, programmable, internet-connected, smart devices, has accelerated the Connected Aircraft transformation (Lueth, 2014). In short, winged local area networks are expanding the internet to 30,000 feet. However, connecting aircraft to the internet is also exposing safety-critical airborne systems to serious cyber-physical safety risks, to which the traveling public is largely oblivious. This ignorance is likely to remain until, heaven forbid, a crash or other incident is directly linked to a successful cyberattack. This research paper will attempt to narrow this knowledge gap by shedding light on the growing cyber-physical safety risks of The Connected Aircraft. It will also suggest risk management approaches, some already underway, to help reduce these emerging cyber-safety risks so that the promising operational, economic, and business benefits of movement can be realized without exposing the traveling public to undue safety risk.