SAND2018-9324C

SNL Comments on Human Dimension: Experience in the Cyber-Physical Domain

Phil Bennett, Manager, Applied Cognitive Systems
Sandia National Laboratories
23 August, 2018

Presented to Resilience Week 2018
Denver, Colorado

Sandia is one of three national laboratories with a Nuclear Deterrence Mission

- Designs over 90% of the weapon components
- Science Base includes High Performance Computing

Sandia is concerned with the command and control of the weapons

- Developed strong and weak links in the arming/fusing/firing systems
- Working to assure reliability and security of the necessary communications with the weapons systems.

This leads SNL to pursue deep understanding of potential cyber threats, and application of the knowledge to system design.

- Sandia develops hardware and software systems, such as the recently deployed "Weasel Board," to help detect and mitigate attacks on control systems such as those in the electric power grid.

- Sandia is moving from classical to quantum technologies expected to be more robust in the cyber domain.

Most technical systems are designed to enable or enhance the human experience. As such, they frequently involve the human as an active user/controller, or incorporate the human as an analytic or decision component of a larger system.

- Operational success is affected by human preference, and when the technical system is designed as an extension of thinking, tends to be higher.
- Designing with humans as an integrated element introduces uncertainties which many design teams try to exclude.
- Surprisingly few engineers have a grasp of this and understand how to incorporate it into their system designs

Toward Design of a more robust system, Sandia is also building its strength in Human systems.

- Human Factors
- Applied Cognitive Science (ACS)

ACS Objectives Include

Understanding human decision making and behaviors
Modeling and simulation of human systems, and increasingly human-machine systems
Experimental exploration of behaviors in the networked computing/cyber domain

Recent experience in Human Systems in the Cyber-Physical Domain

Tularosa Project

Sponsor: NSA's Information Assurance Research organization

Objective: Building upon work of Ferguson-Walter, LaFon and Shade (1), further explore the use of deception in defensive cyber situations to increase the burden of the attacker while making the defender's job easier.

In an experiment of (what we believe to be) unprecedented scale, we are exploring perceptions, decisions made and actions taken by 130 professional red-teamers as they attack a network.

The defensive objective is to make them believe certain defenses are in place, whether true or not, to create a degree of concern and caution that forces additional actions that slow an attack, and increase the probability of detection.

The technical objective is to understand the attackers' cognitive biases and cognitive load, and how that affects their behaviors as they advance through the kill chain.

In the experiment, the red-team subjects' interactions with the network and their tools were recorded. This included keyed commands, screen video, references made to outside information, and a blog of their thoughts, all time-stamped to create the timeline for discoveries, assessments, and decisions.

All but a few of the subjects also agreed to wear monitors to measure physiological data, giving us an additional sense of their state of arousal in the course of the exercise. This may give us insight into which measures have an impact under what conditions.

In the future, we may also apply knowledge gained from previous experiments, including the "Wearables At The Canyon for Health" (WATCH), introduced at Resilience Week 2016. In WATCH, we were seeking to link physiological data from wearable sensors to the cognitive state of subjects who were physically stressed, in this case hiking from rim to rim of the Grand Canyon.

Terabytes of data taken during the Tularosa project are now being analyzed.

We expect this knowledge to be useful in designing more effective defenses in the cyber-physical domain.

1. KJ Ferguson-Walter, DS LaFon, TB Shade, "Friend or Faux: Deception for Cyber Defense", Journal of Information Warfare (2017) 16.2: 28-42