CENTER FOR **CYBERSECURITY**

AT THE UNIVERSITY OF WEST FLORIDA

Agent-based Modeling of Entity Behavior In Cyberspace

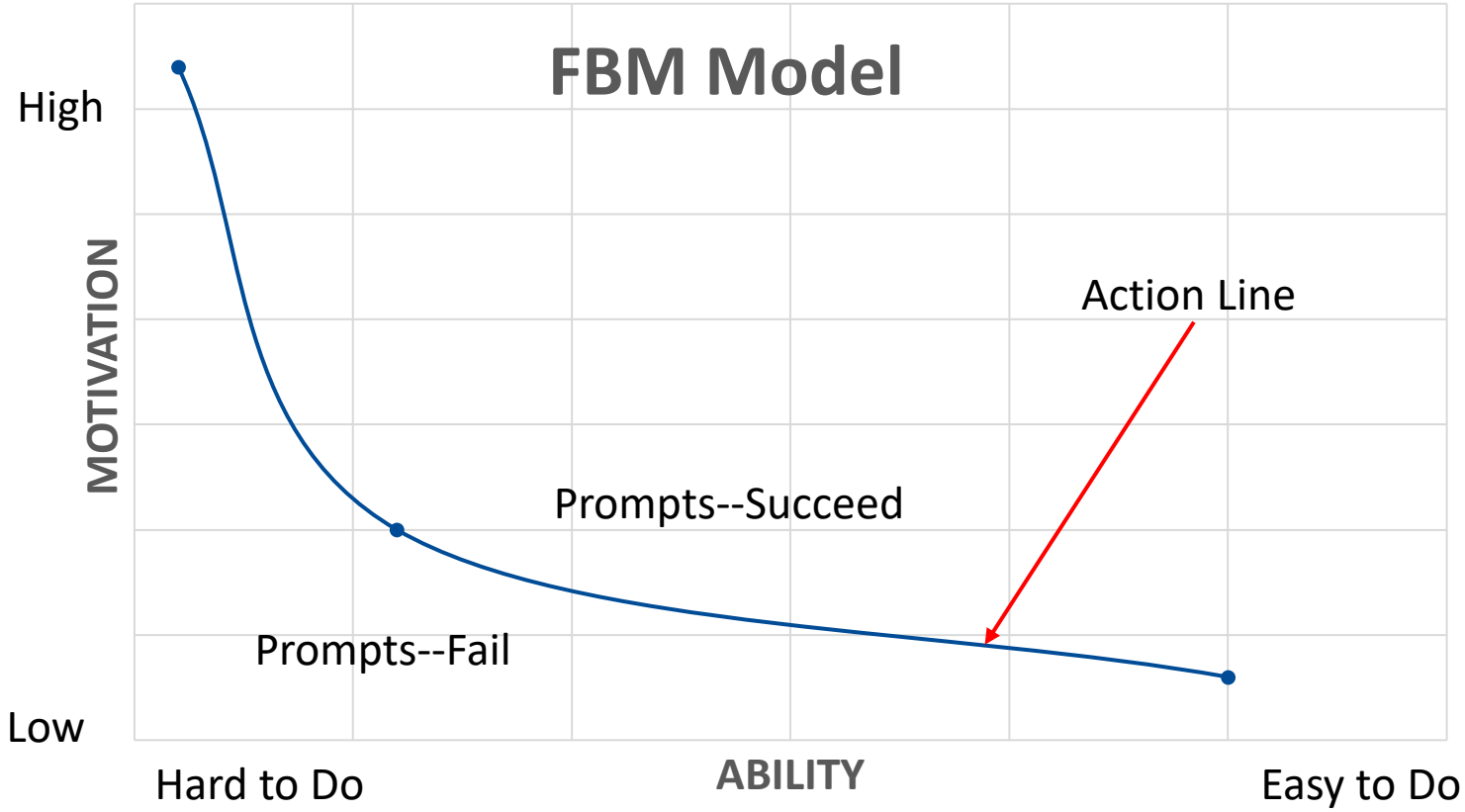
Guillermo Francia,III, Ph.D.

University of West Florida

uwf.edu/cybersecurity

Fogg Behavioral Model

- Convergence of 3 elements: Motivation, Ability and Prompt (MAP)



Source: https://behaviormodel.org/

Outline

- Background and Related Works
- Modeling of Human Behavior
- Modeling of System Behavior
- Agent-based Modeling (ABM)
- ABM Applications
- ABM and Simulations of Entity Behavior in Cyberspace
- Limitations of the Study
- Conclusions and Future Research Directions

Background and Related Works

- Behavioral heuristics to improve cyber safety (Goodman & Lin, 2007)
- Behavioral economic model (Farahmand, et al. , 2008)
- Influence of status quo bias on security settings (Kesan & Shah, 2006)
- Social preferences and feedback mechanisms in cyber trust (Francia & McKerchar, 2015)
- Optimal intervention strategies in cybersecurity (Borill & Testfatsion, 2011)
- Social affinity as a factor in cyber trust (Macal & North, 2009)

Modeling of Human Behavior

- Human is the weakest link in the cybersecurity chain
- Applications of human behavior modeling
  - Crowd evacuation (Pelechanoi & Badler, 2006)
  - Mobile computing virus propagation (Gao & Liu, 2013)
  - Physical security (Ustun, 2009)
  - Use of Bayesian Belief Networks to emulate causal relationships (Meshkat, et al., 2020)
  - Threat of personal data leakage (Xu, et al., 2014)
  - Financial fraud detection (Sanchez, et al., 2018)
  - Modeling and characterization of cyber-terrorists (Schudel & Wood, 2000)

Modeling of System Behavior

- Multi-unmanned Aerial Vehicle (UAV) surveillance systems (Humann & Spero, 2018)
- Financing scenarios in highway infrastructure systems (Mostavi, el al., 2016)
- Smart grid system of systems (Miller, Griendling, & Marvis, 2012)
- Modeling of Economic Systems using the Agent-based Computational Economics (ACE) modeling principles (Tesfatsion, 2017)

Agent-Based Modeling (ABM)

- ABM system consists of autonomous, interacting agents with predefined relationships
- Agents have programmed behaviors allowing for decision making or acting within the context of the simulated environment or scenarios
- Recursive Porous Agent Simulation Toolkit (RePAST) –an ABM toolkit for modeling social behavior
- RePAST was created at the University of Chicago and Argonne National Laboratory

ABM Applications

- Analysis of urban transportation policies (Nguyen et al., 2012)
- Simulation and assessment of crisis scenarios and emergency plans (Piccione & Pellegrini, 2020)
- Modeling of communication for road traffic management (Butt, et al., 2020)
- Simulation of macro level effects of social networking (Sibley & Crooks, 2020)
- Simulation of a virtual marketplace to distinguish the quality of supplier services (Danek, et al., 2010)

Agent Attributes

- Autonomous, self-directed, and independently functions within the specified environment
- Self-contained with a predefined attributes, behaviors and decision-making capability
- Social and able to interact with other agents
- Each agent has a state that varies over time

Agent-Based Modeling

- Inspired by the classical epidemiology model: Susceptible-Infectious-Susceptible (SIS) Model
- Markovian SIS model: at any time t, an agent is either infected or susceptible and that each infected agent infects its neighbors at an infection rate β and that the recovery rate is δ.
- The ratio $\tau = \beta / \delta$ is the effective infection rate.

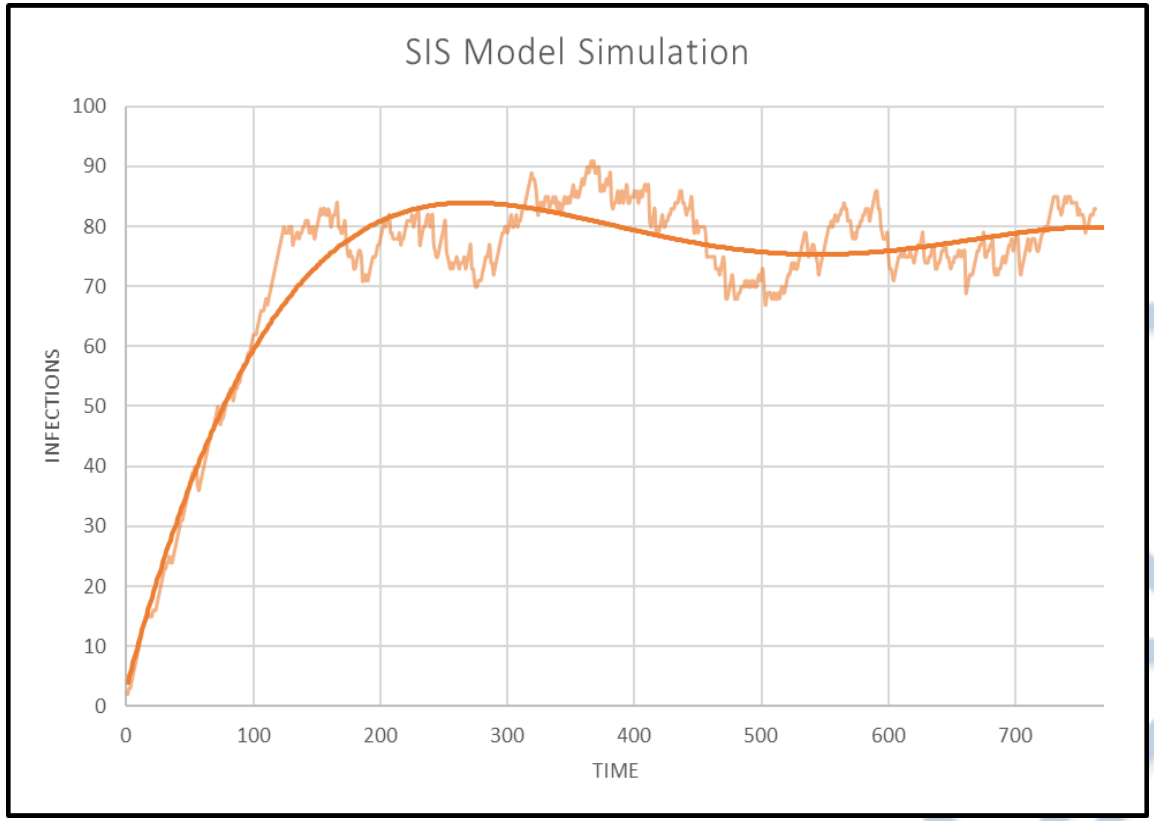


Figure 1. Rate of Infection in the SIS Model

ABM Modeling Objective

- To understand the propagation of a cyber-attack given certain user, system, and adversary attributes and behaviors encoded as agent parameters utilizing agent-based modeling and simulation techniques
- Simulations are performed with varying values of agent parameters
- Agent parameters include; adversary sophistication, trust level, quality of awareness training, and strength of cyber defense

ABM Modeling Assumptions

- Simulations are made on varying agent attributes or parameters
- Simulations are made on both ends of the spectrum: best-case and worst-case
- We assume that system infection goes unnoticed and unabated for a long period of time, so recovery is not part of the simulation

Adversary Attack Simulation

- A measure of the capability of an adversary to mount a successful attack

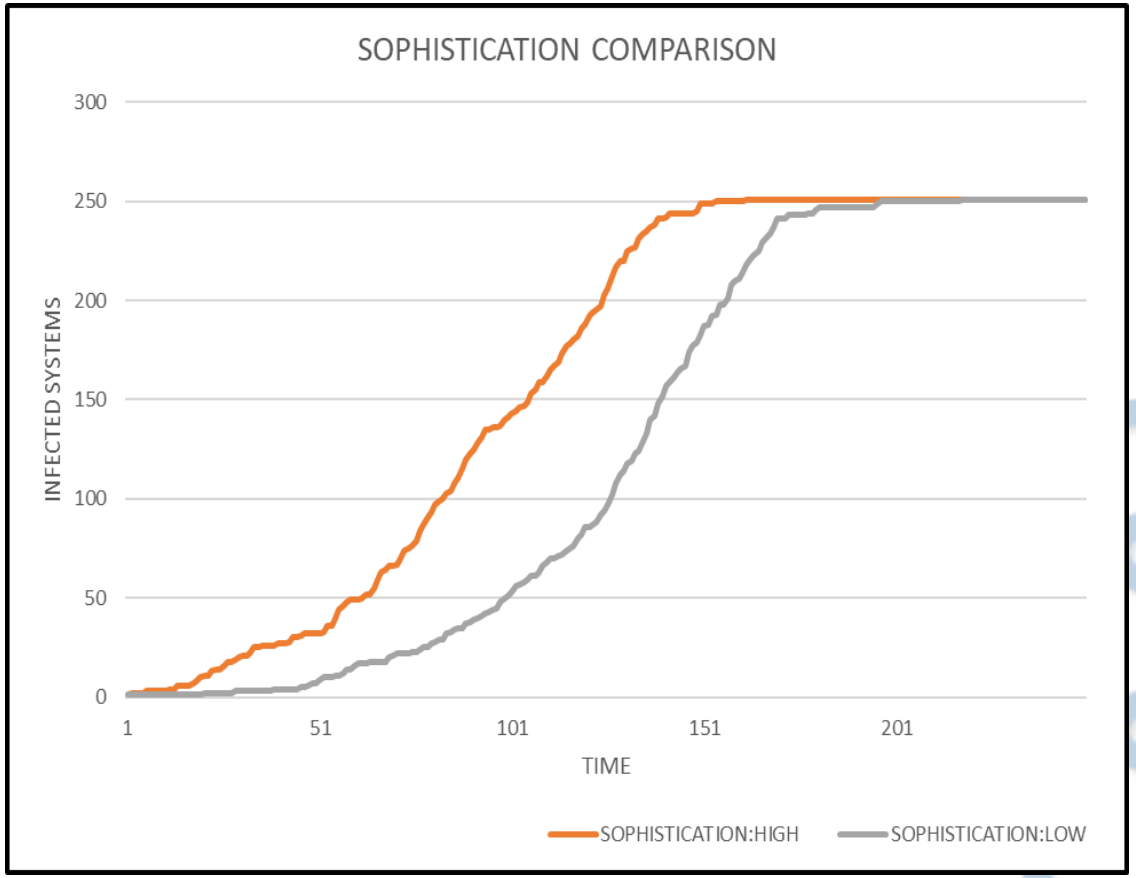


Figure 2. Infection Rate with Attack Sophistication

Trust Level Simulation

- The trust level refers to the degree of confidence users put into the system

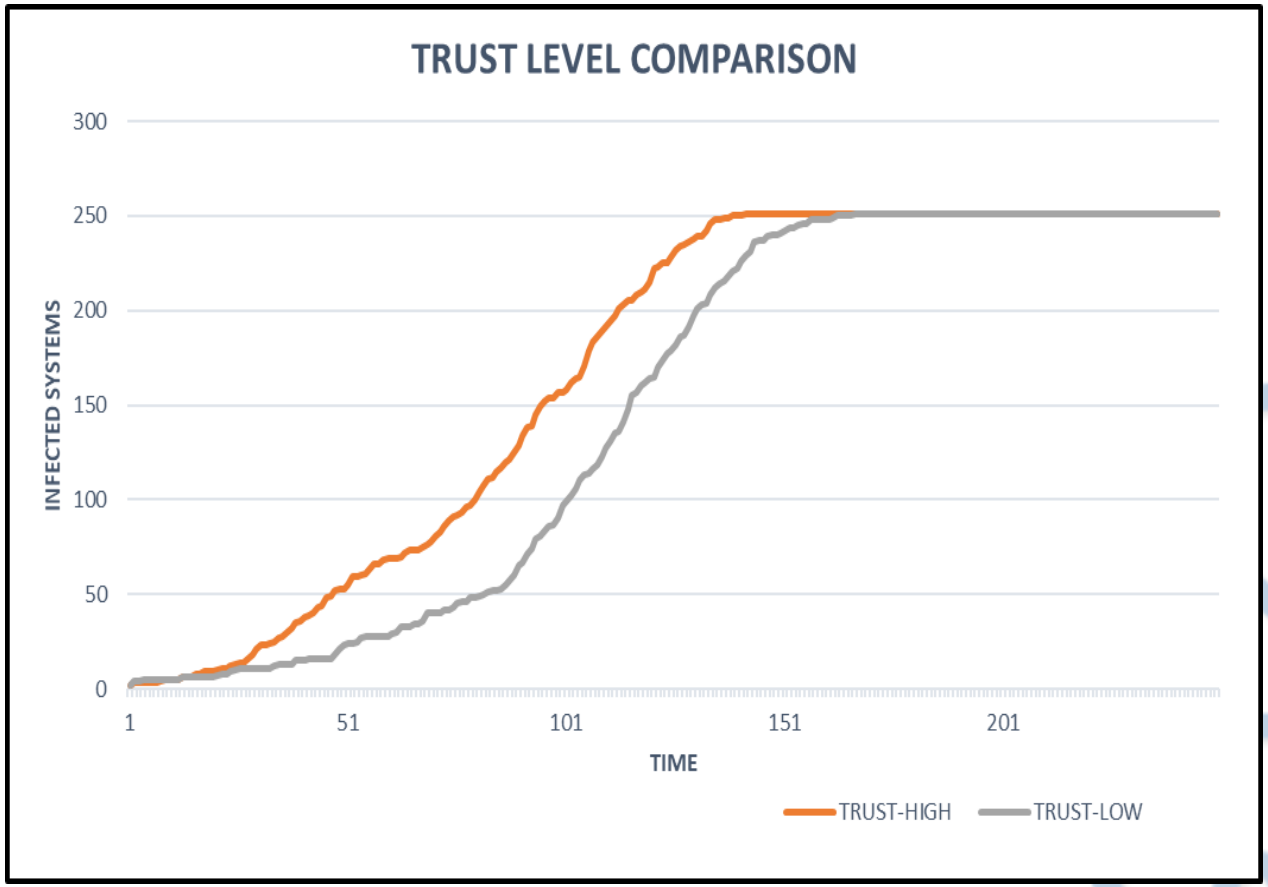
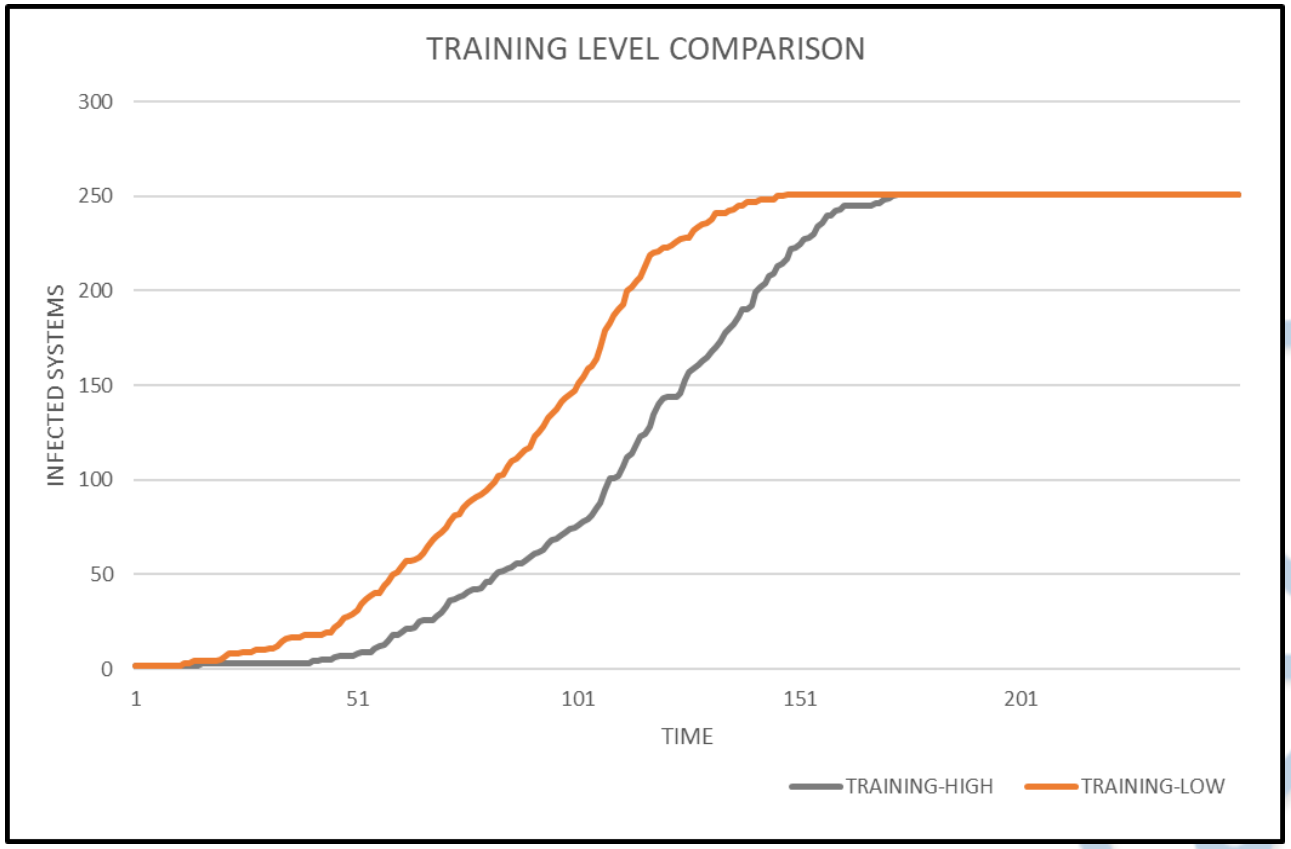


Figure 3. Infection Rate with Varying Trust Level

Quality of Awareness Training Simulation

- The quality of user awareness training is an attribute that was implemented into the simulation process.

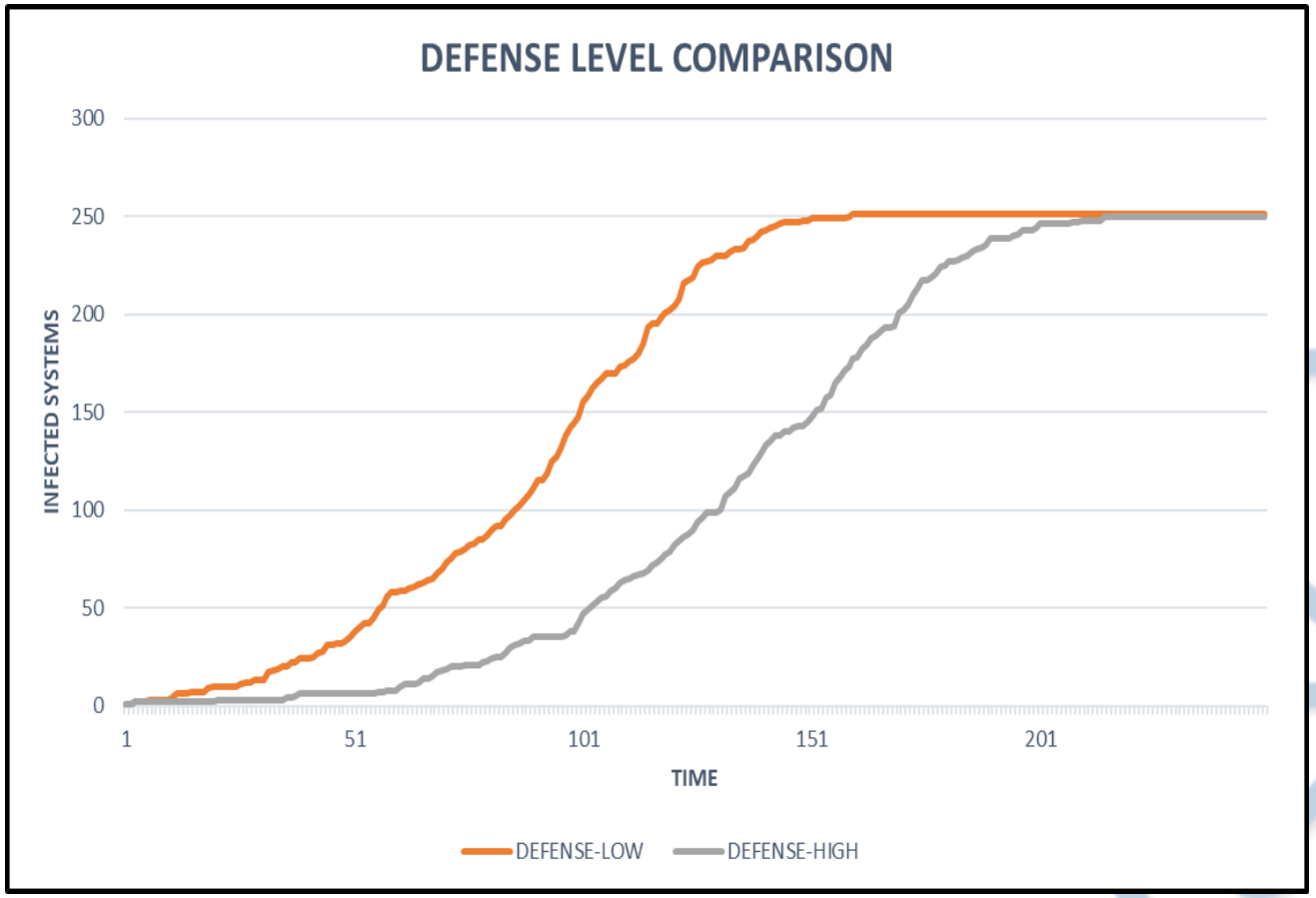
Figure 4. Infection Rate with Varying Training Level



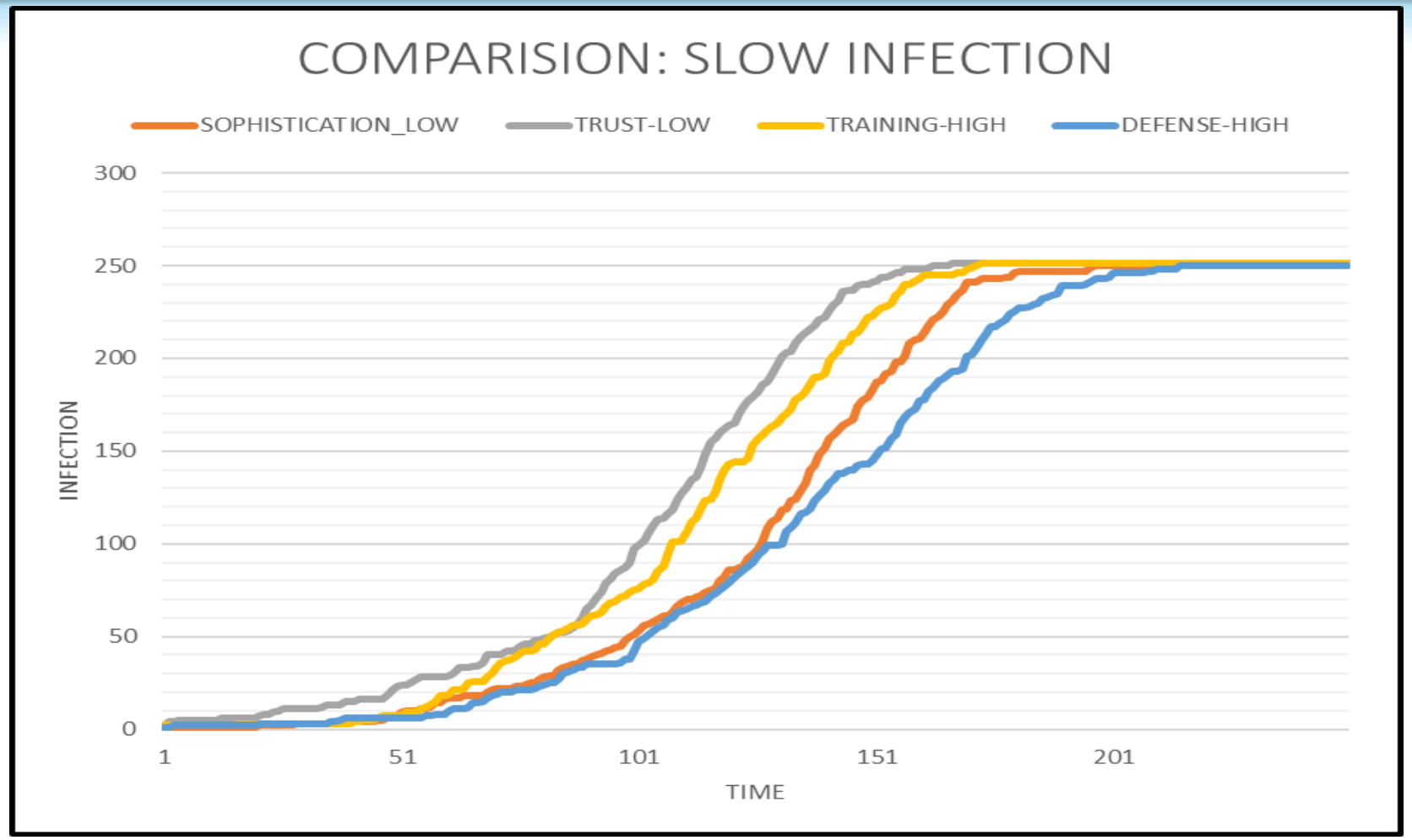
Quality of Cyber Defense Simulation

- Cyber defense is a collection of tools, processes, and capabilities necessary for the protection of information assets from malicious activities.

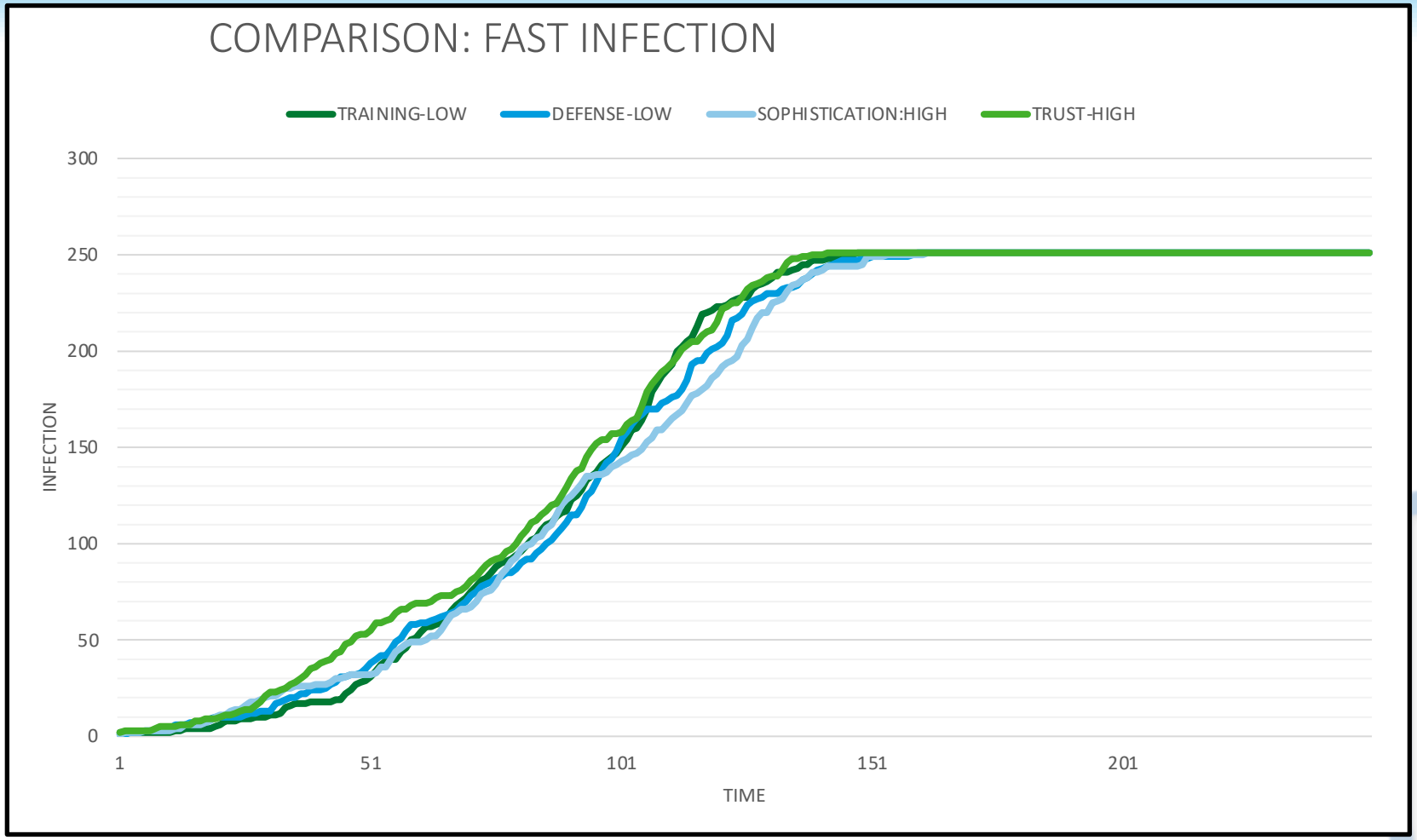
Figure 5. Infection Rate with Varying Cyber Defense Level



Comparison of Slow Infections



Comparison of Fast Infections



Limitations of the Study

- This is a work in progress
- Although the initial intuitions are supported, empirical data are yet to be collected and analyzed to validate the results of the ABM models and simulations
- The formal underpinnings of the ABM system need to be validated

Conclusions

- A method that encodes and simulates entity behaviors in cyber space using Agent-Based Modeling and Simulation system is presented
- A groundwork for future applications of ABM on social behavior is provided
- The impact of the four major system and user attributes are explored
- The study provided a glimpse on how entity behavior can influence the optimal allocation of cybersecurity resources
- Opportunities to explore future research avenues abound

Future Research Directions

- Validate the results of the simulations by gathering and analyzing empirical data
- Apply machine learning systems to augment the ABM system
- Derive mathematical models that will support the validity of the ABM system
- Expand the four parameters with other pertinent factors that define the security of cyberspace

Q & A