CERIAS

The Center for Education and Research in Information Assurance and Security

RiFT: Cyber Adversary Likelihood

Phoebe Abbruzzese, Madhu Joshi, Gabe Samide, Courtney Falk, Rick Kennell

Motivation

The Cyber Adversary Likelihood project has the goal of identifying methods for modeling adversaries in attacks on critical infrastructure and using those models to help determine the likelihood of various adversary actions. Specifically, the project will examine adversary actors in the context of cyber systems (including information systems and control networks) and propose modeling approaches to approximate their behaviors. The project will develop a method to estimate likelihoods of various adversary actions in relevant contexts and then characterize and demonstrate that method. The ultimate use case of the model(s) and tool(s) is to estimate likelihood parameters in a broader model that will be used to assess risk to critical infrastructure from malicious and non-malicious hazards.

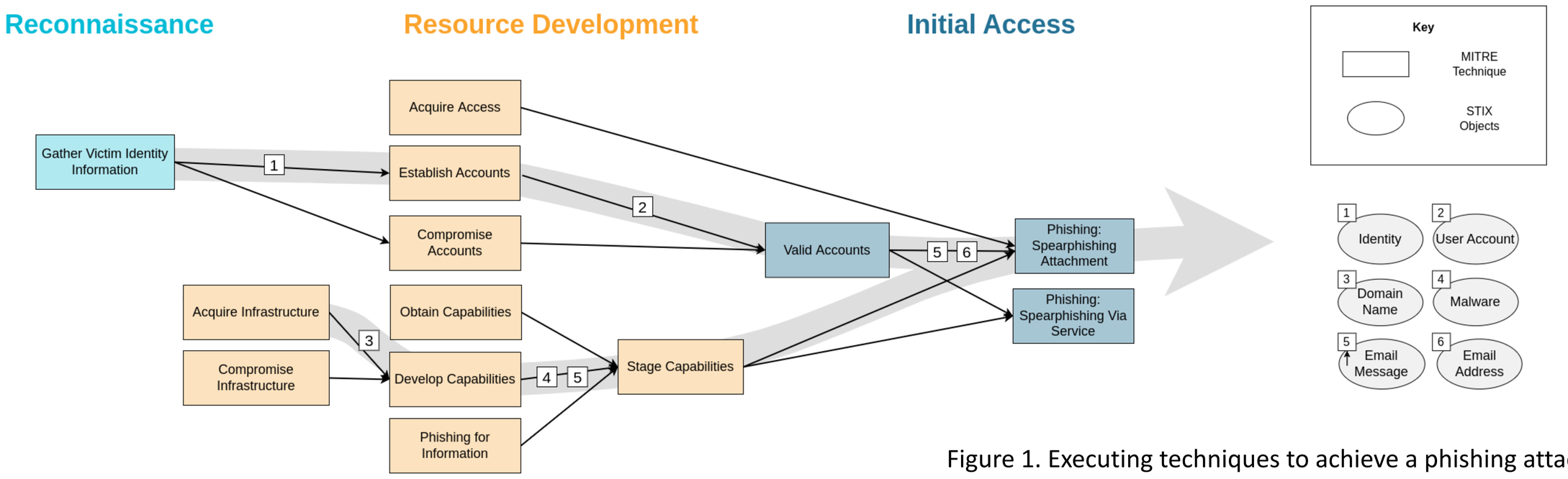

Figure 1. Executing techniques to achieve a phishing attack

Cyber Adversary Modeling

- Figure 1 above depicts an attack flow through a graph whose nodes are techniques taken from the MITRE ATT&CK framework.
- The graph demonstrates the possible paths an attacker may take when carrying out a spearphishing with attachment attack (T1566.001). The grey arrow in the figure shows one possible combination of techniques an attacker may use to get to the spearphishing technique.
- STIX Data Objects (SDOs) and STIX Cyber Observable Objects (SCOs), are permanent objects defined by the MITRE STIX standard that serve as inputs and outputs for each of the techniques an attacker may execute.
- The graph uses a combination of boolean logic with and/or operations to determine if the attacker can move to the following technique.

Critical Infrastructure

- CISA defines 16 critical infrastructure sectors, three of which we selected for in-depth analysis and modeling:
  - Healthcare Sector: Hospitals
  - Manufacturing Sector : Pharmaceutical Manufacturing Plants
  - Emergency Services Sector: Emergency Dispatch Services
- Inputs and outputs necessary for the operation of each of the sectors were identified to determine the maximum operating efficiency.
- Dependencies exist between these three sectors. Attacks on one infrastructure of the healthcare sector could greatly impact another infrastructure.
  - For example, a distributed denial-of-service (DDoS) attack on emergency dispatch services would create delays for emergency patients a hospital is able to treat, impacting patient outcomes.

Simulation

- We used AnyLogic software to create per-sector models before combining them into a single, unified model.
  - Models both physical processes and organizational policies.
  - Dependencies between the sectors cause events to cascade from one sector to another.
- Each model has initial parameters configurable for experimentation.
- Future work will focus on deriving experimental data and results:
  - Testing competing hypotheses to determine efficacy of mitigations or likelihood of the attacker choosing one target over another.
  - Allowing hacker models to interact with the different networked environments, finding different ways to achieve their end goals.

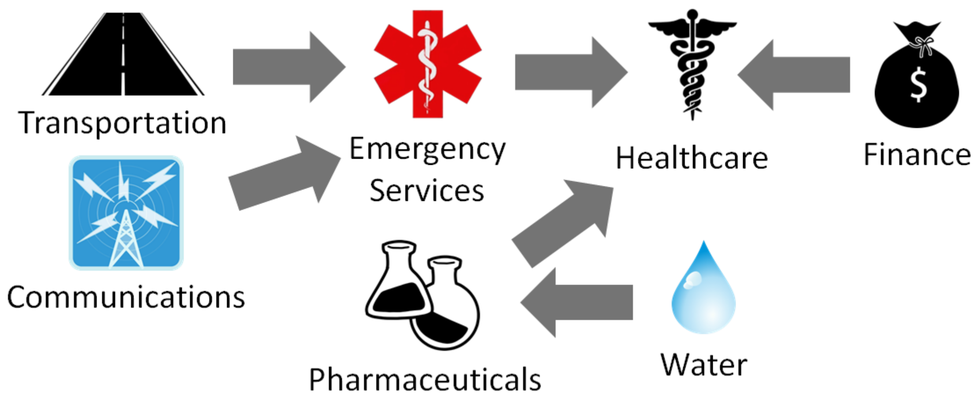

Figure 2. Dependencies among critical infrastructure sectors

PURDUE UNIVERSITY

CERIAS