This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

Impact of a Malware Attack on a Utility Network

How a Cyber Incident Affects a Utility Network

Sandra König

CIP Workshop

Vienna, 20.09.2017

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Overview

- Motivation
- Malware Spreading in Interconnected Networks
- Utility Network Use Case – Network Analysis
- Utility Network Use Case - Optimal Ways of Protection

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

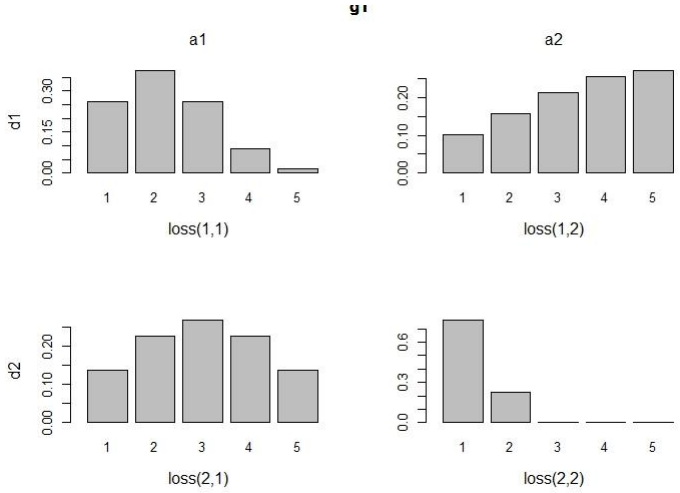
Overview

- Motivation
- Malware Spreading in Interconnected Networks
- Utility Network Use Case – Network Analysis
- Utility Network Use Case - Optimal Ways of Protection

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Motivation

- Protection of a utility network against a malware attack
- Game-theoretic model with random payoffs
- How to get these payoffs?
  - Expert opinions
  - Data collection
  - Simulation



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Overview

- Motivation
- Malware Spreading in Interconnected Networks
- Utility Network Use Case – Network Analysis
- Utility Network Use Case - Optimal Ways of Protection

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Malware Spreading

HyRiM

- Malware attacks have increased over recent years
  - Not yet targeted to any specific user group (private and economic sector)
  - Malware attack can cause severe damage to a company

- Use Case Scenario
  - Power provider falls victim to a malware attack
  - One system gets infected by the malware (e.g. office network)
  - Estimation of the consequences in other networks (e.g. SCADA)

- Assumptions about the malware
  - Malware tries to propagate and infect as many systems as possible (e.g., by sending emails or copying itself to network shares)
  - Increased damage due to this novel “propagation ability feature”

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Malware Spreading in Interconnected Networks

HyRiM

- Modelling the different technical and social networks within the company
  - ICT network (including central data storages, etc.)
  - SCADA networks (including interconnections with ICT network)
  - Employees' social network
- Considering the human factor for the infection and the propagation steps
  - Infection based on social engineering (e.g., phishing mails)
  - Modelling the trust among employees in the company
- Looking at standardized vulnerability information (i.e., CVE data and CVSS scores) to evaluate the initial compromising likelihood and the probability for propagation

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Overview

- Motivation
- Malware Spreading in Interconnected Networks
- Utility Network Use Case – Network Analysis
- Utility Network Use Case - Optimal Ways of Protection

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Network Model

- Network consists of
  - 8 employees
  - 4 laptops (may be used for BYOD)
  - 3 PCs
  - A shared server for file exchange and a router
  - A SCADA server
  - 3 cameras and a camera server
  - 2 concentrators and 4 smart meters (illustrative)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

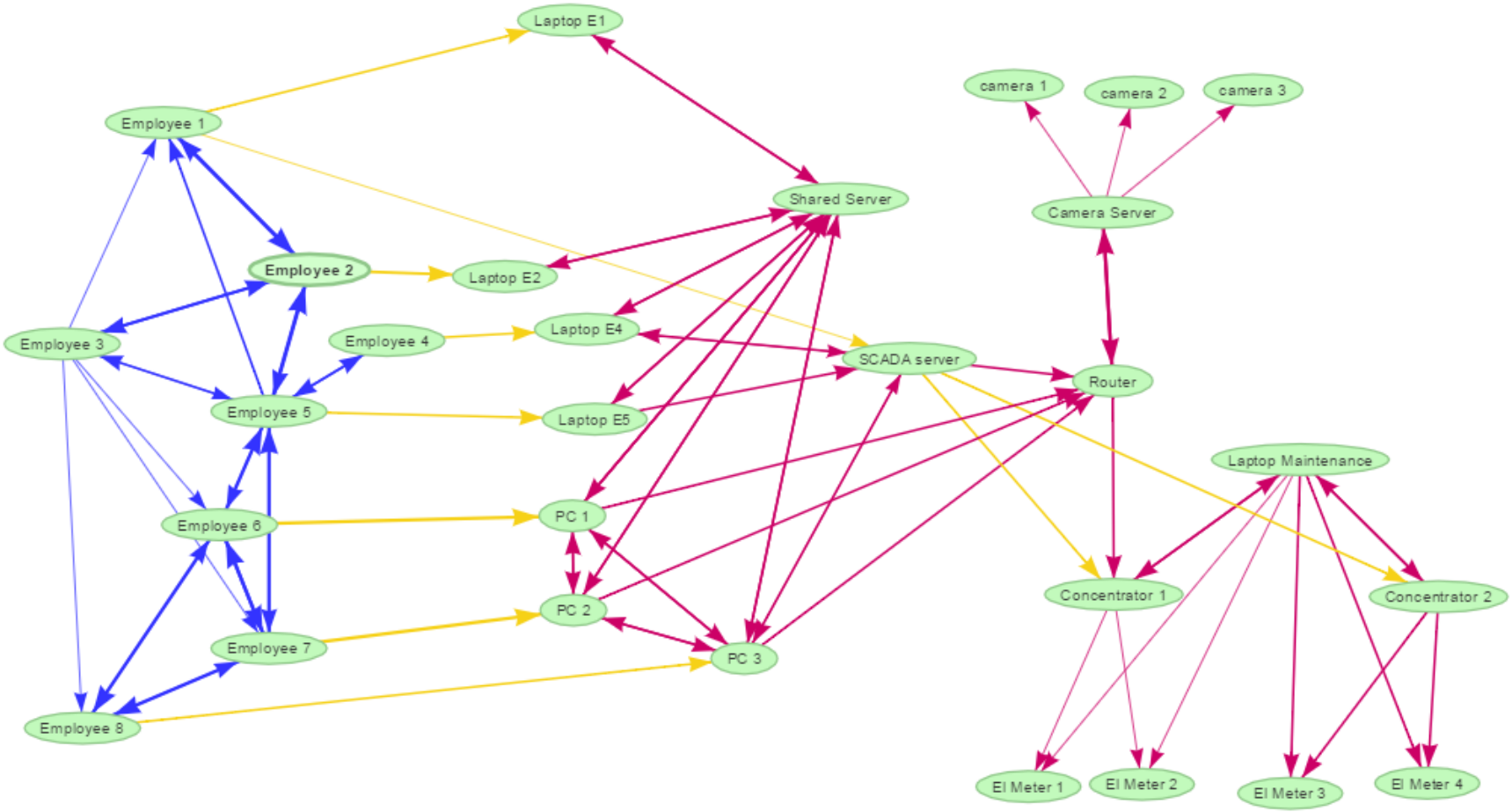
Network Model

- Connections are distinguished depending on their properties
  - various classes (social, logical, network)
  - Different levels of trust (low, medium, high)

- Characterization of edges based on social and technical analysis
  - Interviews with employees (phishing emails)
  - Vulnerability analysis of devices (spreading inside network)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Network Model



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Overview

- Motivation
- Malware Spreading in Interconnected Networks
- Utility Network Use Case – Network Analysis
- Utility Network Use Case - Optimal Ways of Protection

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Game-theoretic Model

HyRiM

In order to find optimal ways to protect a system identify

- Goals of analysis
- Attack vectors
- Defense mechanisms

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Goals

- Find optimal protection
  - Minimize data loss
  - Minimize cost
  - Minimize reputation damage

- Prioritization of goals possible

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Attacks and Defenses

HyRiM

- Attack vectors
  - Send phishing email to employee
  - Infect shared server
  - Infect SCADA server
  - Place infected USB stick near PC or laptop

- Defense mechanisms
  - Regular training of employees to reduce success of social engineering attack
  - Regular backup of important data
  - Regular patching of devices
  - Compare with current state (status quo)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Game-theoretic Analysis

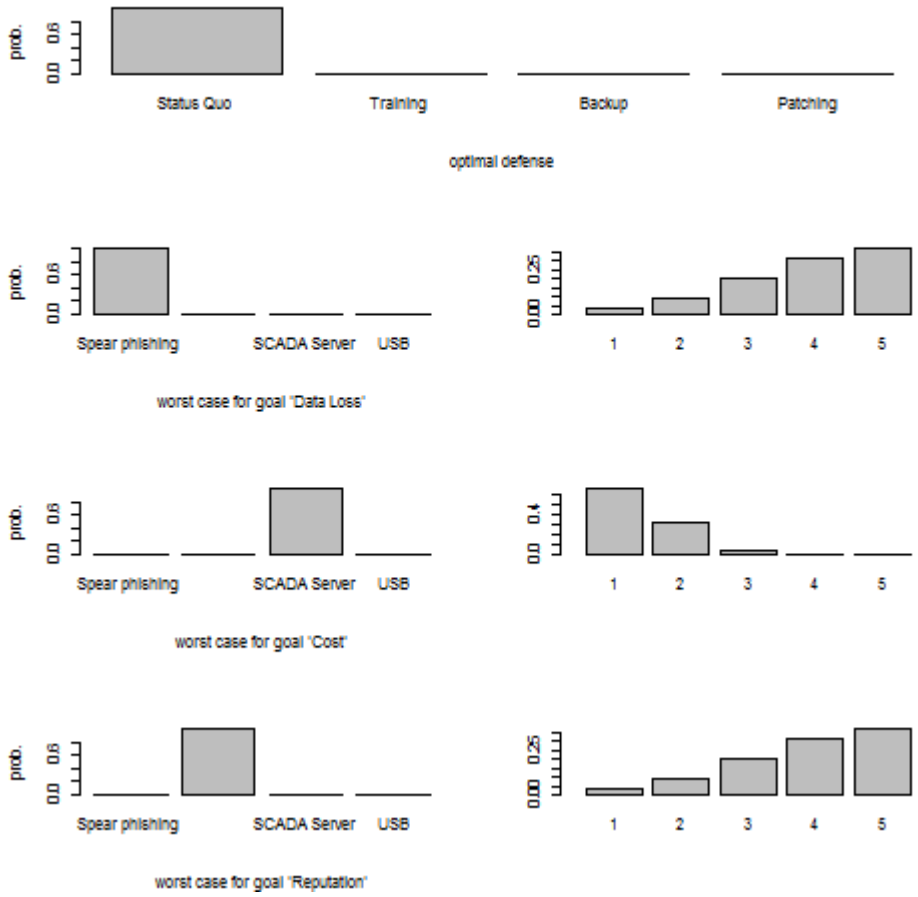
- Compute solution with help of fictitious play algorithm
  - Can be generalized if payoffs (damage) are uncertain
  - Implementation in R available (HyRiM package)

- Solution contains the following information
  - Optimal defense strategy
  - Optimal attack for each goal
  - Worst case damage for each of these attacks can be computed **if** optimal defense is used

- Worst case damage is often a lower bound since we only face one attacker at a time

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Game-theoretic Analysis



worst case attack worst case damage

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

Impact of a Malware Attack on a Utility Network

How a Cyber Incident Affects a Utility Network

Sandra König

sandra.koenig@ait.ac.at
AIT Austrian Institute of Technology
Donau-City-Straße 1
1220 Vienna
Austria

CIP Workshop
Vienna, 20.09.2017