Contents lists available at ScienceDirect

Process Safety and Environmental Protection

journal homepage: www.elsevier.com/locate/psep

A novel probabilistically timed dynamic model for physical security attack scenarios on critical infrastructures

Y.F. Khalil

Physical Sciences Department, United Technologies Research Center (UTRC), 411 Silver Lane, East Hartford, CT, USA

ARTICLE INFO

Article history:
Received 14 February 2016
Received in revised form 25 April 2016
Accepted 1 May 2016
Available online 6 May 2016

Keywords:
Physical security
Critical infrastructures
High-value assets
Probabilistic models
Time to compromise
Mission time

ABSTRACT

This study proposes a novel probabilistically timed dynamic model for physical security attack scenarios on critical infrastructures (CIs). The model simulates attacker's attempts to compromise exploitable vulnerabilities in targeted CIs. Attacker's times to successfully compromise physical barriers, intrusion detection systems, and standby safety systems are modeled as random variables represented by user-defined probability distributions. The model assumes a highly skilled attacker, tracks his cumulative time to compromise targeted assets relative to an estimated mission time, and calculates mission success probability under imperfect information. The model uses Monte Carlo sampling technique to propagate uncertainties of input parameters to calculate statistics of mission success probability. Model's utility is demonstrated by a postulated case study in which an attacker attempts to launch undetected and unmitigated fire in 1-out-of-4 protected areas within a chemical process plant. Destroying one of these protected areas represents attacker's mission success in disrupting plant operation in addition to causing property damage. Visual flowcharting and dynamic attack tree logic are used to describe systematic execution of the attack. Simulation results show 64.4% mission success probability with 4.7% standard deviation. Benefits of proposed model include its use in security training to quantify probabilistic outcomes of "*what if*" scenarios, uncover exploitable vulnerabilities, and implement defensive strategies to improve CI's resilience under attack. The modeling framework can be extended to cyber security applications.

Abbreviations: BE, basic event; CB, circuit breaker; CI, critical infrastructure; CPS, cyber-physical systems; CS, cutsets (in fault tree analysis); DAT, dynamic attack tree; DiD, defense in depth; ET, event tree; ETA, event tree analysis; FL, flammable liquid; FSS, fire suppression system; FT, fault tree; FTA, fault tree analysis; FW, firewater; FWP, firewater pump; HVAC, heating, ventilation, and air conditioning; IDS, intrusion detection system; MCS, Monte Carlo sampling technique; MOV, motor-operated value; MS, mission success from attacker's viewpoint denotes achieving his malicious intent within a predetermined mission time; MTTSC, mean time to successfully compromise an exploitable vulnerability; MT, mission time, represents the window of opportunity available to attacker to accomplish a malevolent goal; MV, manual valve; PAN, priority AND Gate (used in dynamic fault trees); QRA, quantitative risk assessment; SDAS, smoke detection and alarm system; T-1, flammable liquid storage tank; T-2, firewater storage tank.

E-mail address: khalilyf@utrc.utc.com
http://dx.doi.org/10.1016/j.psep.2016.05.001
0957-5820/

1. Introduction

Cyber and physical security attacks on critical infrastructures (CIs) continue to take place because security is a negative goal (Devadas, 2015)[1] that is hard to achieve. Hence, security defenders of CIs need to think the unthinkable by considering all possible scenarios in which adversaries might attempt to compromise cyber and physical systems (CPS) to achieve their malicious goals. In this context, existing systems' vulnerabilities in CIs represent gold mines to be exploited by skilled cyber and physical security attackers who recognize the fact that any CI cannot be more secure than its weakest link.

The interdependency between cyber and physical systems brings to bear the importance of protecting physical systems (like power lines, electric substations, power generation plants, just to name a few) from physical security attacks. Unfortunately however, our review of the cyber-physical systems (CPS) literature reveals that the largest body of research has been focused on cyber security attacks and exploitation of vulnerabilities in digital information and much less (<24%) attention has been given to the physical security component of CPS. For example, our "*Web of Science*"[2] literature search shows 1,871 published papers on cyber security and only 444 papers on physical security over the period January 2000 to January 2016. Over the same period, our literature search using the "*Engineering Index/Compendex*"[3] shows 4,794 published papers on cyber security and only 667 published papers on physical security. In our opinion, physical security matters because an exploitable vulnerability in a physical component, such as a smart meter, could be an attacker's backdoor entry point to access and compromise cyber components in CPS like microgrids interoperability. Because the opposite is also true, that is a cyber-attack could be the entry point prior to launching a physical security attack, it would not be unreasonable for CPS researchers to consider scenarios with hybrid cyber and physical attacks.

To name but a few examples of our review of published literature on cyber security of CPS, Dacier et al. (1996) developed a methodology based on adversary's privilege graphs to assess security of operational vulnerabilities in computing systems like Unix™. They converted privilege graphs into Markov models that correspond to all possible successful attack sequences. However, the assumptions considered in their Markov models are not pertinent to skilled attackers. They described the probability of a successful attack in a given time (t) by the memoryless exponential distribution with a constant attack success rate equals the reciprocal of mean time to successful attack. Also, they used stochastic Petri Nets to construct intrusion state graphs from the privilege graphs. Jonsson and Olovsson (1997) characterized security by behavioral and preventive components and assumed times between system's breaches to be exponentially distributed and, thus, conventional reliability prediction methods could be employed. They carried out a practical intrusion experiment and generated data representing number of attempts and number of successful breaches as a function of time, taking into account attacker's skill level. The experimental results were used to construct hypothesis on attacker's behavior using three attack phases, namely, a learning phase (for a low-skilled attacker), a standard phase, and an innovative phase. Their data showed that time to breach during the attack standard phase is exponentially distributed. In the innovative phase, the attacker is assumed to be willing to take on new methods and exploit unknown vulnerabilities and, hence, requires more time to achieve successful attacks. Jonsson and Olovsson (1997) arrived at the key conclusion that known system's vulnerabilities must be eliminated to confine adversaries in the innovative attack phase which requires much longer times to successfully achieve their malicious intent. Phillips and Swiler (1998) introduced the concept of attack graphs to simulate sets of system states and paths that adversary could exploit to achieve a malicious goal. Subsequently, Jha et al. (2002) offered an algorithm for generating attack graphs using off-the-shelf model checking tools. Each path in the attack graph represented a sequence of exploits, which the authors called atomic attacks (these could be either stealthy or detectable). The insights generated from the attack graphs were used to identify the minimum set of security measures to improve system safety. Jha et al. (2002) also developed an algorithm for calculating network (containing multiple computers, routers, firewalls, databases, and intrusion detection systems) reliability which denotes probability that adversary is not successful in accomplishing his goal. Madan et al. (2002) modeled security intrusion and described time and effort spent by the attacker as a random variable. Their model enabled calculation of mean time to security failure and probability of security failure and assumed that attacks could arrive at random points in time in a fashion similar to system' failures that could happen randomly. Moreover, the authors assumed that time and effort spent by the attacker to exploit system's vulnerability is also a random variable that follows one of several probability distributions such as the exponential, gamma, log-logistic, or Weibull distributions. McQueen et al. (2005) proposed a random process model, using a graph theoretical approach, for calculating time to compromise a system as a function of adversary's skill level, whether component vulnerability is known or attacker has to probe for vulnerability, and whether the attacker has/has not at least one exploit readily available for each vulnerability. They applied their model to the supervisory control and data acquisition system (SCADA) before and after implementation of specific security measures. Their methodology involve ten steps that start with establishing system's configuration and end with estimating the risk reduction resulting from generating compromise graphs and estimating dominant attack paths and time to compromise each component in the system before and after improving system's security. Three time-to-compromise probability distributions (beta, gamma, and exponential) were assumed depending on availability of exploits by the attacker and his skill levels (novice, beginner, intermediate, and expert).

With respect to literature examples on cyber and physical threats, Jones et al. (2006) developed a Markov decision process (MDP) model to calculate probability of successful breaches in the case of an adversary's attempt to launch an attack on an airplane. They represented the system as a network of arcs (denoting attacker's probabilistic pathways between

[1] Devadas, S. (2015). Cybersecurity: challenges, attacks, and defenses. Computer Science and Artificial Intelligence Laboratory (CSAIL), Massachusetts Institute of Technology (MIT), Cambridge, MA 02139.

[2] Web of Science is an online subscription-based scientific citation indexing service maintained by Thomson Reuters that provides a comprehensive citation search.

[3] Engineering Village, the essential engineering research database maintained by Elsevier, provides a searchable index of the most comprehensive engineering literature and patent information available.