TECHNIQUES FOR ENHANCED VULNERABILITY MANAGEMENT FOR INDUSTRIAL INTERNET OF THINGS

GEETA

AMAR NATH & SHASHI KHOSLA SCHOOL OF INFORMATION TECHNOLOGY
INDIAN INSTITUTE OF TECHNOLOGY DELHI

June 2022

TECHNIQUES FOR ENHANCED VULNERABILITY MANAGEMENT FOR INDUSTRIAL INTERNET OF THINGS

by

GEETA

Amar Nath & Shashi Khosla School of Information Technology

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Delhi

June 2022

DEDICATED TO

My family.

Thank you for your eternal support.

Certificate

This is to certify that the thesis titled **Techniques for Enhanced Vulnerability Management for Industrial Internet of Things** being submitted by **Ms. GEETA** for the award of **Doctor of Philosophy** in **Information Technology** is a record of bona fide work carried out by her under my guidance and supervision at the Amar Nath and Shashi Khosla School of Information Technology, Indian Institute of Technology Delhi. The work presented in this thesis has not been submitted elsewhere, either in part or full, for the award of any other degree or diploma.

Kolin Paul
Professor
Department of Computer Science and Engineering
Indian Institute of Technology Delhi
New Delhi- 110016

Acknowledgements

A Ph.D. is a ride with a unique track of insightful, enriching, frustrating, enlightening and memorable years, where the co-passengers are a source of motivation and reinvigoration. I wish to acknowledge all the people who helped me in their ways in the journey of making my dream a reality.

First, I would like to thank my supervisor, the most cherished person I have ever met, Prof. Kolin Paul, for his invaluable guidance, exciting research discussions, words of encouragement, unwavering faith in my capability and continuous feedback that has led to the work in this thesis. He always provided a healthy work environment that motivated me to achieve my goals. The work flexibility that he allowed; let me balance my personal and professional life. He helped me grow as an independent researcher, allowing me to explore a new domain and work on ideas on my terms and pace. He always provided practical insights and feedback on my thesis work. I also thank him for the constant feedback he provided on my research writing and presentations that have helped me refine the skills necessary to succeed in research and academia. I thank him for teaching me to always look on the positive side of the coin. To summarize, I would say that this thesis is a result of my pursuance and his influence.

I would also like to thank my research collaborator Dr. Alaa Allakany (Kyushu University, Japan), Prof. Koji Okamura (Kyushu University, Japan) and Dr. Praveen Gauravram (TCS Australia) for the valuable discussion that helped me to refine my research works. The critic and thought-provoking review, along with an appreciation for work, motivated me towards continuous improvements.

I would also like to thank my SRC members ($Ranjan^3$ of my SRC committee) Prof. Smriti Ranjan Sarangi, Prof. Priti Ranjan Panda and Prof. Ranjan Bose for their insightful questions and excellent suggestions.

I am grateful to my thesis examiners Prof. Sandeep Kumar Shukla (IIT Kanpur, India) and Prof. Nilanjan Banerjee (University of Maryland, Baltimore County, USA) for providing detailed comments and recommendations to mold my thesis in a more interesting way.

I would like to thank the lab in-charge Manju Chopra and the administrative staff at SIT and CSE departments for facilitating administrative matters. I am also grateful to my friends Vijay Kumar, Aruna Bansal, Himanshu Gandhi, Shubhani Gupta, Dr. Chandrika Bhardwaj, Srishti Kulshrestha, Britty Baby, Priyanka Chauhan and Pooja Jangir at IIT Delhi with whom I shared precious learning years of my life. The never-ending discussions, presentation rehearsals, manuscript reviews, experience-sharing sessions and wonderful lab environment kept me motivated and reinvigorated throughout the journey. I take this opportunity to express my earnest gratitude to Dr. Madhulika Mohanty and Dr. Rajesh Kedia for their professional guidance.

I would also like to thank my siblings Anju Yadav and Dr. Manish Yadav and sister-in-law Pooja Yadav for always being there whenever I needed to confide in them. I am also grateful to my mother-in-law and father-in-law for their help when I have to attend conferences. I am thankful to them for never imposing family responsibilities and understanding when I could not attend a family function. I also appreciate Komal and Anand for always being available and helping me in many ways.

Even imagining the thought of starting a Ph.D. with a kid in the womb is very challenging. I started both the motherhood and Ph.D. journey together. I could handle both things because of four strong pillars behind me: my mother, father, husband Kamal, and little munchkin Lakshya. I am blessed with their love and support throughout the journey. I would not have started and survived this journey without my husband's continuous efforts. A night goodbye with a smile and saying, 'Don't worry about me'. while wishing to sleep

in mom's lap was a challenging moment of the day for Lakshya. I owe all those hours to my son. I tried to assimilate my father's ambition, mother's autodidact, husband's dedication, and son's curiosity to walk this path. I dedicate my thesis to my family.

Geeta

Abstract

Industrial Control Systems (ICS) are characterized by large numbers of tightly integrated, interdependent and heterogeneous components in a network. They act as a base system for safety and mission-critical Industrial Internet of Things (IIoT) applications such as smart grids, nuclear power plants, process control systems and robotics systems. The complex ICS, e.g., Supervisory Control and Data Acquisition (SCADA), consists of many interdependent subsystems. Modern SCADA systems are an amalgam of IIoT and legacy systems. IIoT is essentially a realization of advances in the connectivity of hardware and data networks that SCADA provides. Therefore, modern SCADA systems can be considered a use-case for IIoT-based systems. The modernization of the SCADA system, standardization of communication protocols and almost ubiquitous interconnectivity courtesy for IIoT has drastically increased the attack surface of the SCADA systems. Systematic Vulnerability Management (VM) of these attack surfaces minimizes risks and impacts associated with vulnerability exploitation. VM is a cyclical practice of identifying, analyzing, prioritizing and fixing/ monitoring possible exploitation of vulnerabilities in complex End-to-End (E2E) systems. State-of-art vulnerability discovery and real-time

exploitations monitoring approaches fail to discover and monitor Multi-Host Multi-Stage (MhMs) attacks since they rely on isolated systems testing and monitoring. The Central Monitoring System (CMS) needs each system log transmitted to the central server, hence having a significant network overhead. Moreover, the recent attacks demonstrate that whenever an adversary can not directly exploit a vulnerability, it exploits a series of vulnerabilities to reach the target node, generally referred to as MhMs attacks. In this thesis, we provide a three-level security solutions VM for MhMs attacks, including a detailed vulnerability analysis for SCADA with the help of various datasets, which clearly demonstrate the importance of the problem statement. We first discover all such vulnerabilities that lead to paths to the critical node, then prioritize the vulnerabilities for efficient patching, followed by monitoring the critical vulnerabilities.

We assess the SCADA system vulnerabilities leveraging the National Vulnerability Database (NVD) to understand the severity and characteristics of these vulnerabilities by using SCADA-related keywords such as SCADA, PLC, IIoT, ICS, etc. We analyze the extracted vulnerabilities by year-wise vulnerability count, attack-vector-wise analysis, impact analysis of the vulnerabilities on the CIA triad and CWE-count analysis. Based on this analysis outcome, we find answers to four critical questions regarding the SCADA system vulnerabilities. Next, we developed a possible MhMs attacks discovery framework *IoT-PEN*. This leverages the standalone system (discovered) vulnerabilities, network topology and target graphs. *IoT-PEN* also generates a security state report of each system and possible MhMs attacks. The framework evaluations demonstrate that the framework is efficient and scalable to larger networks.

To address the challenges in prioritizing patches in ICSs, we proposed two approaches: *SmartPatch* and *PatchRank*. *PatchRank* demonstrates that by incorporating domain-specific characteristics, a practical severity score is assigned to a vulnerability as compared to widely used scoring systems in industries, i.e., Common Vulnerability Scoring Systems (CVSS). *PatchRank* models the attacker-defender scenario as a two-player simultaneous non-cooperative game. However, patching is a repetitive process. Therefore, *PatchRank* is extended to *SmartPatch*. *SmartPatch* models the scenario as multiple attackers and multiple defenders repetitive games by considering the architectural features: functional dependencies, topological dependencies, vulnerabilities assessment features and patch dependencies. We validate the applicability of *SmartPatch* by considering the case study of an interdependent, complex SCADA chain in the smart grid system using the IEEE 5-Bus system. Our comparative analysis of the proposed approach with state-of-the-art approaches demonstrates that *SmartPatch* reduces Residual Impact Score (RIS) by a faster rate, i.e., after each iteration, the RIS value for *SmartPatch* is the least.

To detect ongoing attacks, we propose *GLoM* : A Global Monitor using SpatioTemporally Correlated Local Monitor that can detect ongoing MhMs attacks on the connected systems. It leverages deep learning-based algorithms to detect anomalies with high accuracy and attack graphs to map various anomalous behavior to detect MhMs attacks. GLoM is a two-stage deep learning-based model, where the workload is divided between Local Monitors (LM) and Global Monitors (GM). LMs use LSTM to detect the abnormal behavior of a system leveraging syslogs. Parallelly, GM discovers possible vulnerabilities on the devices using vulnerability scanners in the network, followed by generating Possi-

ble Attack Graphs (PAG) by mapping the prerequisites and post-conditions required to exploit a vulnerability. The framework highlights MhMs possible attacks if there is an attack path from the source to the target node. In last, critical paths are identified using exploitability scores. The similarity index between possible attack-paths and evidence from logs identifies the most probable attack scenario an adversary may be following. Using LMs, network communication overhead decreased by 88% on the publicly available dataset OpenStack (Loghub). LSTM-based anomaly detection shows 99% accuracy in detecting the anomalous logs with an average anomalous log prediction overhead of 0.6 msec. We achieved 98% and 97% accuracy in generating the prerequisites and post-conditions of a vulnerability, respectively. We evaluated $GLoM$ efficiency in MhMs attack detections using a local testbed.

In brief, this thesis aims at building techniques for efficient vulnerability management to discover MhMs possible attacks. It provides vulnerability prioritization techniques by considering the domain context. It also proposes a global monitoring system to detect ongoing multi-host exploitations using system logs.

सार

औद्योगिक नियंत्रण प्रणाली (ICS) एक नेटवर्क में बड़ी संख्या में कसकर एकीकृत, अन्योन्याश्रित और विषम घटकों की विशेषता है। वे सुरक्षा और मिशन-महत्वपूर्ण औद्योगिक इंटरनेट ऑफ थिंग्स (IIoT) अनुप्रयोगों जैसे स्मार्ट ग्रिड, परमाणु ऊर्जा संयंत्र, प्रक्रिया नियंत्रण प्रणाली और रोबोटिक्स सिस्टम के लिए एक आधार प्रणाली के रूप में कार्य करते हैं। जटिल ICS, जैसे, पर्यवेक्षी नियंत्रण और डेटा अधिग्रहण (SCADA), में कई अन्योन्याश्रित उप-प्रणालियाँ शामिल हैं। आधुनिक SCADA सिस्टम IIoT और विरासत प्रणालियों का एक मिश्रण हैं। IIoT अनिवार्य रूप से SCADA द्वारा प्रदान किए जाने वाले हार्डवेयर और डेटा नेटवर्क की कनेक्टिविटी में प्रगति की प्राप्ति है। इसलिए, आधुनिक SCADA सिस्टम को IIoT- आधारित सिस्टम के लिए उपयोग-मामला माना जा सकता है। SCADA प्रणाली के आधुनिकीकरण, संचार प्रोटोकॉल के मानकीकरण और IIoT के लिए लगभग सर्वव्यापी इंटरकनेक्टिविटी शिष्टाचार ने SCADA सिस्टम की हमले की सतह को काफी बढ़ा दिया है। इन आक्रमण सतहों का व्यवस्थित भेद्यता प्रबंधन (VM) भेद्यता शोषण से जुड़े जोखिमों और प्रभावों को कम करता है। VM जटिल एंड-टू-एंड (E2E) सिस्टम में कमजोरियों के संभावित शोषण की पहचान, विश्लेषण, प्राथमिकता और निर्धारण/निगरानी का एक चक्रीय अभ्यास है। अत्याधुनिक भेद्यता खोज और रीयल-टाइम शोषण निगरानी दृष्टिकोण मल्टी-होस्ट मल्टी-स्टेज (MhMs) हमलों की खोज और निगरानी करने में विफल होते हैं क्योंकि वे पृथक सिस्टम परीक्षण और निगरानी पर भरोसा करते हैं। केंद्रीय निगरानी प्रणाली को केंद्रीय सर्वर को प्रेषित प्रत्येक सिस्टम लॉग की आवश्यकता होती है, इसलिए एक महत्वपूर्ण नेटवर्क ओवरहेड होता है।

इसके अलावा, हाल के हमलों से पता चलता है कि जब भी कोई विरोधी सीधे तौर पर भेद्यता का फायदा नहीं उठा सकता है, तो वह लक्ष्य नोड तक पहुंचने के लिए कमजोरियों की एक श्रृंखला का फायदा उठाता है, जिसे आम तौर पर MhMs हमलों के रूप में जाना जाता है। इस थीसिस में, हम MhMs हमलों के लिए तीन-स्तरीय सुरक्षा समाधान वीएम प्रदान करते हैं, जिसमें विभिन्न डेटासेट की सहायता से एससीएडीए के लिए विस्तृत भेद्यता विश्लेषण शामिल है, जो स्पष्ट रूप से समस्या कथन के महत्व को प्रदर्शित करता है। हम पहले ऐसी सभी कमजोरियों का पता लगाते हैं जो महत्वपूर्ण नोड तक ले जाती हैं, फिर कुशल पैचिंग के लिए कमजोरियों को प्राथमिकता देते हैं, इसके बाद महत्वपूर्ण कमजोरियों की निगरानी करते हैं।

हम SCADA से संबंधित कीवर्ड जैसे SCADA, PLC, IIoT, ICS, आदि का उपयोग करके इन कमजोरियों की गंभीरता और विशेषताओं को समझने के लिए राष्ट्रीय भेद्यता डेटाबेस (NVD) का लाभ उठाते हुए SCADA सिस्टम कमजोरियों का आकलन करते हैं। हम वर्ष-वार द्वारा निकाली गई

कमजोरियों का विश्लेषण करते हैं। भेद्यता गणना, हमले-वेक्टर-वार विश्लेषण, CIA ट्रायड पर कमजोरियों का प्रभाव विश्लेषण और सीडब्ल्यूई-गिनती विश्लेषण। इस विश्लेषण के परिणाम के आधार पर, हमें SCADA सिस्टम की कमजोरियों के बारे में चार महत्वपूर्ण सवालों के जवाब मिलते हैं। इसके बाद, हमने एक संभावित MhM अटैक डिस्कवरी फ्रेमवर्क *IoT-PEN* विकसित किया। यह स्टैंडअलोन सिस्टम (खोजी गई) कमजोरियों, नेटवर्क टोपोलॉजी और लक्ष्य ग्राफ का लाभ उठाता है। *IoT-PEN* प्रत्येक सिस्टम और संभावित MhM हमलों की सुरक्षा स्थिति रिपोर्ट भी तैयार करता है। ढांचे के मूल्यांकन से पता चलता है कि ढांचा बड़े नेटवर्क के लिए कुशल और मापनीय है।

ICS में पैच को प्राथमिकता देने में चुनौतियों का समाधान करने के लिए, हमने दो दृष्टिकोण प्रस्तावित किए: *SmartPatch* और *PatchRank*। *PatchRank* दर्शाता है कि डोमेन-विशिष्ट विशेषताओं को शामिल करके, उद्योगों में व्यापक रूप से उपयोग किए जाने वाले स्कोरिंग सिस्टम, यानी कॉमन वल्नरेबिलिटी स्कोरिंग सिस्टम (CVSS) की तुलना में एक व्यावहारिक गंभीरता स्कोर एक भेद्यता को सौंपा गया है। *PatchRank* हमलावर-डिफेंडर परिदृश्य को दो-खिलाड़ी एक साथ गैर-सहकारी खेल के रूप में मॉडल करता है। हालाँकि, पैचिंग एक दोहराव वाली प्रक्रिया है। इसलिए, *PatchRank* को *SmartPatch* तक बढ़ा दिया गया है। *SmartPatch* वास्तुशिल्प सुविधाओं पर विचार करके कई हमलावरों और कई रक्षकों के दोहराव वाले खेलों के रूप में परिदृश्य को मॉडल करता है: कार्यात्मक निर्भरता, टोपोलॉजिकल निर्भरता, कमजोरियां मूल्यांकन सुविधाएँ और पैच निर्भरता। हम IEEE 5-बस प्रणाली का उपयोग करते हुए स्मार्ट ग्रिड सिस्टम में एक अन्योन्याश्रित, जटिल एससीएडीए श्रृंखला के केस स्टडी पर विचार करके *SmartPatch* की प्रयोज्यता को मान्य करते हैं। अत्याधुनिक दृष्टिकोणों के साथ प्रस्तावित दृष्टिकोण का हमारा तुलनात्मक विश्लेषण दर्शाता है कि *SmartPatch* अवशिष्ट प्रभाव स्कोर (RIS) को तेज दर से कम करता है, अर्थात, प्रत्येक पुनरावृत्ति के बाद, *SmartPatch* के लिए RIS मूल्य सबसे कम है।

चल रहे हमलों का पता लगाने के लिए, हम *GLoM* का प्रस्ताव करते हैं: SpatioTemporally सहसंबद्ध स्थानीय मॉनिटर का उपयोग करने वाला एक वैश्विक मॉनिटर जो कनेक्टेड सिस्टम पर चल रहे MhM हमलों का पता लगा सकता है। यह MhMs हमलों का पता लगाने के लिए विभिन्न विषम व्यवहारों को मैप करने के लिए उच्च सटीकता और हमले के ग्राफ के साथ विसंगतियों का पता लगाने के लिए गहन शिक्षण-आधारित एल्गोरिदम का लाभ उठाता है। *GLoM* एक दो चरणों वाला गहन शिक्षण-आधारित मॉडल है, जहाँ कार्यभार को स्थानीय मॉनिटर्स (LM) और ग्लोबल मॉनिटर्स (GM) के बीच विभाजित किया जाता है। LMs सिस्टम का लाभ उठाने वाले syslogs के असामान्य व्यवहार का पता लगाने के लिए LSTM का उपयोग करते हैं। समानांतर रूप से, GM नेटवर्क में भेद्यता स्कैनर का उपयोग करने वाले उपकरणों पर संभावित कमजोरियों का पता लगाता है, इसके बाद संभावित हमले के ग्राफ़ (पीएजी) उत्पन्न करके एक भेद्यता का फायदा उठाने के लिए आवश्यक पूर्वापेक्षाओं और बाद की स्थितियों का मानचित्रण करता है। यदि स्रोत से लक्ष्य नोड तक कोई हमला

पथ है, तो फ्रेमवर्क MhM के संभावित हमलों पर प्रकाश डालता है। अंत में, शोषकता स्कोर का उपयोग करके महत्वपूर्ण पथों की पहचान की जाती है।

संभावित हमले के रास्तों और लॉग से सबूत के बीच समानता सूचकांक सबसे संभावित हमले के परिदृश्य की पहचान करता है जिसका एक विरोधी अनुसरण कर सकता है। LM का उपयोग करते हुए, सार्वजनिक रूप से उपलब्ध डेटासेट OpenStack (Loghub) पर नेटवर्क संचार ओवरहेड 88% तक कम हो गया। LSTM-आधारित विसंगति का पता लगाना 0.6 msec के औसत विषम लॉग भविष्यवाणी के साथ विषम लॉग का पता लगाने में 99% सटीकता दिखाता है। हमने भेद्यता की पूर्वापेक्षाएँ और बाद की स्थितियाँ उत्पन्न करने में क्रमशः 98% और 97% सटीकता हासिल की। हमने स्थानीय टेस्टबेड का उपयोग करके MhMs हमले का पता लगाने में *GLoM* दक्षता का मूल्यांकन किया।

संक्षेप में, इस थीसिस का उद्देश्य MhMs संभावित हमलों की खोज के लिए कुशल भेद्यता प्रबंधन के लिए तकनीकों का निर्माण करना है। यह डोमेन संदर्भ पर विचार करके भेद्यता प्राथमिकता तकनीक प्रदान करता है। यह सिस्टम लॉग का उपयोग करके चल रहे बहु-होस्ट शोषण का पता लगाने के लिए एक वैश्विक निगरानी प्रणाली का भी प्रस्ताव करता है।

Contents

List of Figures

List of Tables

List of Acronyms

AC Access Complexity

AEI Actual Exploit Index

Au Authentication

AV Access Vector

BC Betweeness Centrality

CAPEC Common Attack Pattern Enumeration and Classification

CI Critical Infrastructure

CMS Central Monitoring Systems

CPE Common Platform Enumeration

CVE Common Vulnerability Enumeration

CVE-ID Common Weakness Enumeration Identifier

CVSS Common Vulnerability Scoring System

CWE Common Weakness Enumeration

DER Distributed Energy Resource

DoS Deniel of service

EL Evidence List

FTW Fixed Timing Window

GM Global Monitor

GUI Graphical User Interface

ICS Industrial Control System

IDS Intrusion Detection Systems

IIoT Industrial Internet of Things

IoT Internet of Things

IT Information Technology

KNC K-Neighbors Classifier

LAN Local Area Network

LM Local Monitor

LCS Lowest Common Subsequence

LR Logistic Regression

LSTM Long-Short Term Memory

LVI Local Vulnerability Index

MhMs Multi-host Multi-stage

ML Machine Learning

MLP Multi-layer Perceptron classifier

NCC Nearest Centroid Classifier

NVD National Vulnerbaility Database

OT Operational Technology

PAG Possible Attack Graph

PR Privilege Requird

RAPR Repository for Attack Pattern Rules

RF Random Forest classifier

RIS Residual Impact Score

RISI Repository of Industrial Security Incidents

Sc Scope

s.t. such that

SCADA Supervisory Control and Data Acquisition

SGDC Stochastic Gradient Descent Classifier

SSW Session Specific Window

TCP Transport Layer Protocol

TTC Time-To-Compromise

UDP User Datagram Protocol

UI User Interaction

VM Vulnerability Managenment

VSM Viable System Model

VSMS Viable System Model for SCADA

w.r.t. with respect to

WIVSS Weighted Impact Vulnerability Scoring System

WAN Wide Area Network

List of Symbols

A^v Availability impact of vulnerability v

AC^v Attack complexity of vulnerability v

AV^v Attack vector of vulnerability v

B^v_{Score} Base score of vulnerability (Basescore parameter of CVSS)

C^v_A Cost of attacking a vulnerability v

C^v_D Cost of defending a vulnerability v

C^v Confidentiality impact of vulnerability v

$CVSS_{v_i}$ CVSS severity score of vulnerability v_i

$EI_A(j,k)$ Effective impact of attack when attacker chose strategy j and defender chose strategy k

$EPr_A(j,k)$ Effective profit of attack when attacker chose strategy j and defender chose strategy k

$Vul^{v}_{exploit}$ Exploit score of vulnerability v

ESC Exploitability subscore of vulnerability v

G_{adj} Adjacency matrix of VSMS graphical model

I^{v}_{A} Impact of successful exploitation a vulnerability v

I^{v} Integrity impact of vulnerability v

I Inspection space

ISC Impact subscore of vulnerability v

K Log Key set

N_{rank} Node rank for patching

$N_{topology}$ Network topology

N_{A} Number of attackers

N_{D} Number of defenders

N_{V} Number of vulnerabilities

NV_{chrono} Normalised chronological age of vulnerability v

P^{j}_{A} Probability of attacking systems using strategy j

P^{v}_{A} Probability of successful attack on vulnerability v

P_{A} Probability of successful attack

P_D^k Probability of defending system using strategy k

P_D^v Probability of defending vulnerability v

P_D Probability of successful defend

$Payoff_A$ Payoff of attacker

$Payoff_A^i$ Payoff of the attacker in i^{th} iteration

$Payoff_D$ Payoff of defender

$Payoff_D^i$ Payoff of the defender in i^{th} iteration

PO_A Expected payoff of attacker

PO_D Expected payoff of defender

Pr_A^v Profit gained by attacker by successful exploitation of a vulnerability v

PR^v Privilege associated with vulnerability v

R_{adj}^s Risk associated with a subsystem s

R_{adj} Associted Risk

R_A Resources available to attacker

R_D Resources available to defender

R Set of rules to detect a CVE exploitation

Re_A^v Revenue generated by attacker by successful exploitation of a vulnerability v

RIS^t Residual impact score after iteration t

S^s_{FunDep} Functional dependency score of subsystem s

S^s_{TDep} Topological dependency score of subsystem s

s^j_A j^{th} strategy of attacker

s^k_D k^{th} strategy of defender

Sc Set of attack scenarios

$Vul^v_{severity}$ Severity Score of vulnerability v

$S1, S2, S3, S3^*, S4, S5$ System instances

t_1, t_2, t_3 Time instances

UI^v User interaction of vulnerability v

V_{chrono} Chronological age of a vulnerability v

V_{rank} Vulnerabilities rank for patching

v_i Vulnerabuility instance $\in$ V

V Vulnerability set

W Node severity matrix