Document details

< Back to results | 1 of 1

Export Download Print E-mail Save to PDF ☆ Add to List More... >
View at Publisher

ICETAS 2019 - 2019 6th IEEE International Conference on Engineering, Technologies and Applied Sciences
December 2019, Article number 9117330
6th IEEE International Conference on Engineering, Technologies and Applied Sciences, ICETAS 2019; Kuala Lumpur; Malaysia; 20 December 2019 through 21 December 2019; Category numberCFP19N08-ART; Code 161181

Review of SCADA Systems and IoT Honeypots (Conference Paper)

Alquwatli, M.H. ✉, Habaebi, M.H. ✉, Khan, S. ✉

International Islamic University Malaysia, Department of Electrical and Computer Engineering, Jalan Gombak, Kuala Lumpur, 53100, Malaysia

Abstract

View references (26)

Internet of Things (IoT) is a massive technology that is being improved day by day. It connects different types of devices to the internet so that they can interchange data. The most feild that has been improved by implementing IoT 's technology is Supervisory Control and Data Acquisition (SCADA) Systems , or Industrial Control Systems (ICS). The application of these systems is to be used in controlling different elements that is connected to it (sensors, devices, and machines). However, connecting different types of devices of different physical circuitry and different communication technology, together raises various security issues that has been a place of concern for years. A famous technique that has been implemented in the field of security to further study Cyber Attacks, its causes, and effects is Honeypots . The Aim from this paper is to categorize Cyber-physical attacks and their effects, study SCADA /ICS systems ' architecture, highlight its security weaknesses, and how Cyber/Physical attacks make use of these weaknesses. Finally, a break down Honeypots and understand its implementation and effectiveness in the Field of Cyber Security. © 2019 IEEE.

SciVal Topic Prominence ⓘ

Topic: SCADA System | Supervisory Control | Intrusion Detection

Prominence percentile: 99.076 ⓘ

Author keywords

Conpot | Cyber Physical Attacks | Cyber Security | Honeypot | ICS | Industrial Control Systems | Modbus TCP Protocol | S7comm Protocol | SCADA | Supervisory Control and Data Acquisition

Indexed keywords

Engineering controlled terms: Computer crime | Network security | SCADA systems

Engineering uncontrolled terms: Communication technologies | Cyber physicals | Cyber security | Industrial control systems | Internet of Things (IOT) | Security issues | Security weakness | Supervisory control and dataacquisition systems (SCADA)

Engineering main heading: Internet of things

Funding details

Metrics ⓘ

View all metrics >

PlumX Metrics

Usage, Captures, Mentions, Social Media and Citations beyond Scopus.

Cited by 0 documents

Inform me when this document is cited in Scopus:

Set citation alert >

Related documents

HoneyPLC: A Next-Generation Honeypot for Industrial Control Systems
López-Morales, E. , Rubio-Medrano, C. , Doupé, A.
(2020) Proceedings of the ACM Conference on Computer and Communications Security

An overview of cyber-attack vectors on SCADA systems
Irmak, E. , Erkek, I.
(2018) 6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding

Application of low interaction honeypot for analysis of internet malicious activity
Parianou, A. , Li, B.
(2011) Proceedings of the 4th International Conference on Internet Technologies and Applications, ITA 11

View all related documents based on references

Find more related documents in Scopus based on:

Authors > Keywords >

Funding sponsor	Funding number	Acronym
International Islamic University Malaysia	P-RIGS18-003-0003	IIUM

Funding text #1

This work was conducted at the IOT and Wireless Communication Protocols Lab, and is partially funded by International Islamic University Malaysia (IIUM) Publication RIGS grant no. P-RIGS18-003-0003.

Funding text #2

VI. ACKNOWLEDGMENT This work was conducted at the IOT and Wireless Communication Protocols Lab, and is partially funded by International Islamic University Malaysia (IIUM) Publication RIGS grant no. P-RIGS18-003-0003.

ISBN: 978-172814082-7
Source Type: Conference Proceeding
Original language: English

DOI: 10.1109/ICETAS48360.2019.9117330
Document Type: Conference Paper
Publisher: Institute of Electrical and Electronics Engineers Inc.

References (26)

View in search results format >

□ All | Export | Print | E-mail | Save to PDF | Create bibliography

□ 1 Chung, B., Kim, J., Jeon, Y.
On-demand security configuration for IoT devices

(2016) *2016 International Conference on Information and Communication Technology Convergence, ICTC 2016*, art. no. 7763373, pp. 1082-1084. Cited 7 times.
ISBN: 978-150901325-8
doi: 10.1109/ICTC.2016.7763373

View at Publisher

□ 2 Ramachandruni, R.S., Poornachandran, P.
Detecting the network attack vectors on SCADA systems

(2015) *2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2015*, art. no. 7275694, pp. 707-712. Cited 8 times.
ISBN: 978-147998791-7
doi: 10.1109/ICACCI.2015.7275694

View at Publisher

□ 3 Pal, S., Hitchens, M., Varadharajan, V.
On the design of security mechanisms for the internet of things
(2017) *11th International Conference on Sensing Technology (ICST*. Cited 4 times.
IEEE

□ 4 Tryfonas, L.T., Li, H.
The internet of things: A security point of view
(2016) *Emerlad*

□ 5 Mokube, I., Adams, M.
Honeypots: Concepts, approaches, and challenges

(2007) *Proceedings of the Annual Southeast Conference*, 2007, pp. 321-326. Cited 92 times.
ISBN: 1595936297; 978-159593629-5
doi: 10.1145/1233341.1233399

View at Publisher

□ 6 Loukas, G.
(2015) *Cyber-Physical Attacks: A Growing Invisible Threat*. Cited 61 times.
Elsevier Inc