Risk Analysis of DNP3 Attacks

Authors: Vasiliki Kelli, Panagiotis Radoglou-Grammatikis, Thomas Lagkas, Evangelos K. Markakis, Panagiotis Sarigiannidis

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936 (ELECTRON)

IEEE CSR 2022

July 27-29, 2022 // Virtual Conference

Overview

- The DNP3 Protocol
- DNP3-related Vulnerabilities
- DNP3 Risk Assessment

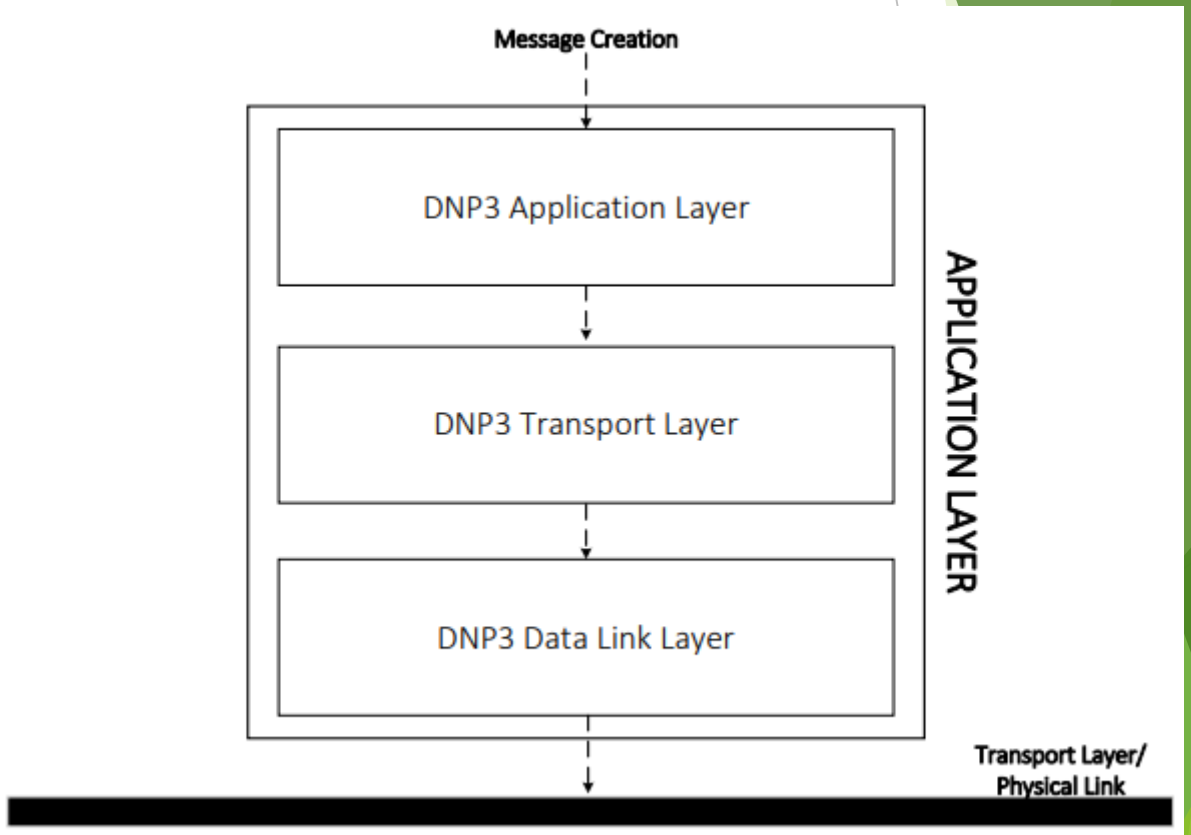
The DNP3 Protocol & Related Vulnerabilities

IEEE CSR 2022

July 27-29, 2022 // Virtual Conference

The DNP3 Protocol

- Protocol utilized in ICS/SCADA systems
- Serial or TCP transportation
- Client-Server communication model
  - Master-Outstation in DNP3 terminology
- Composed by 3 layers
  - Data Link Layer
  - Transport Layer
  - Application Layer



Attacks Against DNP3

- Disable Unsolicited Messages
  - Instruct the outstation to disable the functionality of sending unsolicited messages to the master
- Cold Restart
  - Instruct the outstation to perform a full restart
- Warm Restart
  - Instruct the outstation to restart DNP3 applications
- Slave Discovery
  - Nmap NSEs for DNP3 outstation discovery

Attacks Against DNP3

- Data Initialization
  - Reset outstation data to default values
- Stop Application
  - Instruct outstation to cease the operation of the DNP3 application
- Replay
  - Delay the transmission of a legitimate packet

DNP3 Risk Assessment

IEEE CSR 2022

July 27-29, 2022 // Virtual Conference

DNP3 Risk Assessment: CVSS

- Open framework for assessing vulnerabilities against software
- CVSS metrics refer to the quantitative assessment of the **exploitability** and the **impact** of an attack against a system
- Exploitability
  - Attack Vector (AV)
  - Attack Complexity (AC)
  - Privileges Required (PR)
  - User Interaction (UI)
  - Scope (S)
- Impact
  - Confidentiality (C)
  - Integrity (I)
  - Availability (A)

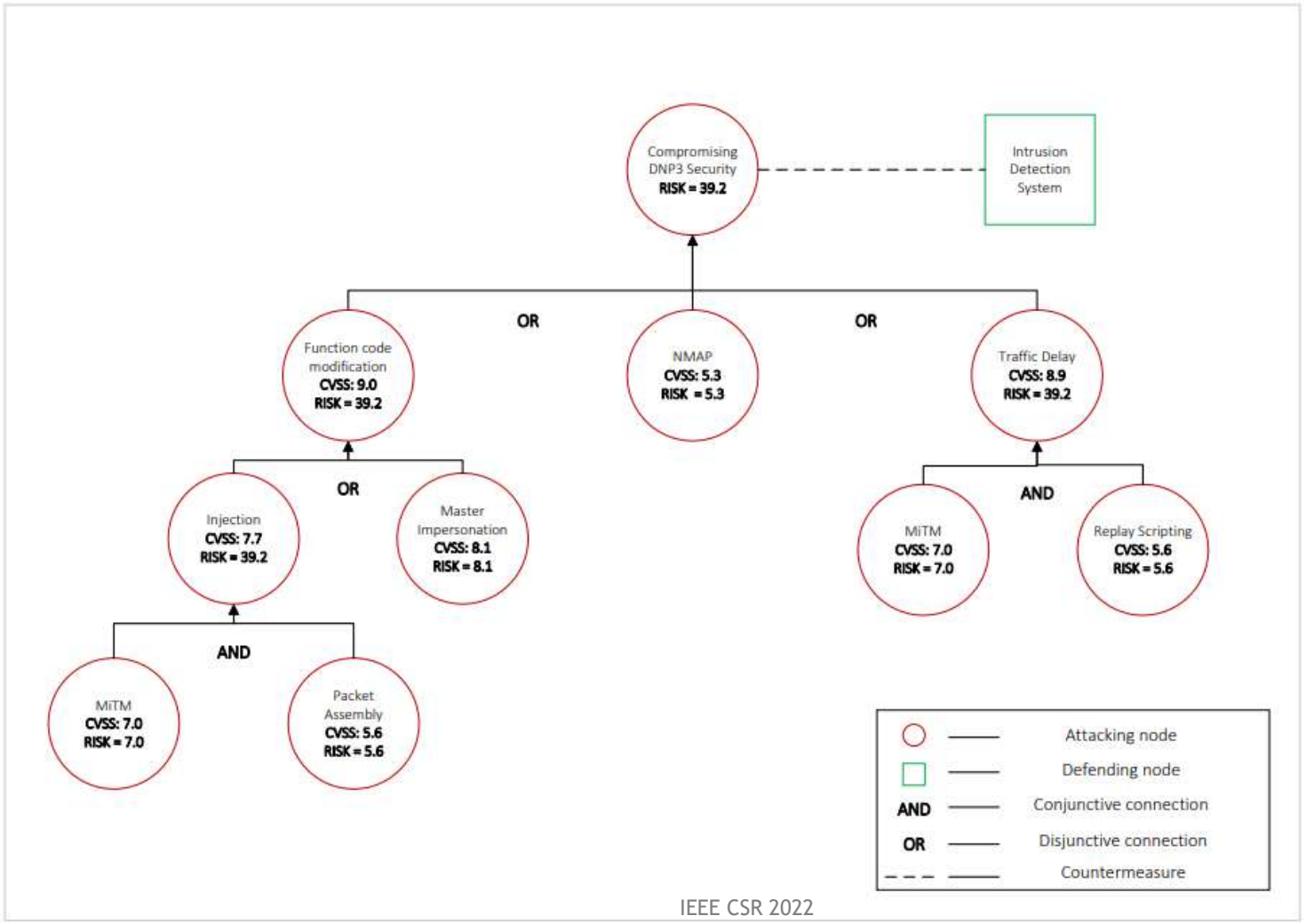
DNP3 Risk Assessment: ADT

- Attack modeling technique following tree analysis
- Visualization of the actions an attacker has to follow to reach their objective
- Nodes represent a malicious action or a countermeasure
- Root node represents the attacker's objective
- The objectives of parent nodes are achievable through the completion of at least one child node's objective
  - Conjunctive (AND) → All of the children's aims must be fulfilled
  - Disjunctive (OR) → At least one child's aim must be fulfilled

Risk Assessment through CVSS & ADT

DNP3 Cyberattack	Description	CVSS Score	CVSS Representation
MiTM	The intentional placement of a malicious entity between two communicational endpoints with the aim of intercepting their network traffic	7.0	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L
Packet assembly	Generation of a packet with the desired attributes	5.6	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
Injection	Insertion of the crafted packet in the traffic stream	7.7	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L
Master impersonation	The operations and behavior of a legitimate master is immitated by a malicious entity	8.1	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Function code modification	The desired function code reaches the slave thus resulting in operations including the full or partial restart of the outstation, initializing data, ceasing operations, and disabling the ability to send unsolicited messages	9.0	AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
Nmap	Gathering intelligence regarding whether the targeted IP address belongs to a DNP3 outstation	5.3	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Replay scripting	Generation of a script to replay or delay packets	5.6	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
Traffic delay (Replay)	The traffic of the targeted endpoint is being maliciously delayed to obstruct regular communication	8.9	AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:L

Risk Assessment through CVSS & ADT



$$Risk_{ParentNode} = \prod_{n=1}^{N} Risk_n$$

$$Risk_{ParentNode} = max(Risk_1, Risk_2 \ldots, Risk_N)$$

Conclusions

Conclusions

- Identification of 8 cyberattacks and vulnerabilities-by-design of DNP3
- DNP3 cyberattack risk calculation technique
  - ADT
  - CVSS

Thank you!