Cybersecurity Essentials and Management (Energy Sector)

CSP001

Topic 2/10: Foundational Knowledge and Taxonomy of Energy Cybersecurity.

PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)

Cybersecurity in Energy

Vulnerabilities

- **Vulnerability Assessment:** Systematic process of identifying, quantifying, and prioritizing vulnerabilities in a system, network, or infrastructure.
- **Purpose:** Identify weaknesses, measure potential impact, and provide guidance for mitigation.
- **Methodology:** Scanning, manual testing, and analysis.
- **Types:** Network, Application, Infrastructure.
- **Output:** Vulnerability report, risk assessment.
- **Benefits:** Proactive security, compliance, risk management.
- **Challenges:** False positives, resource-intensive, evolving threats.
- **Best Practices:** Regular assessments, collaboration, remediation plan.
- **Tools:** Automated scanners, manual testing tools, risk assessment tools. Nessus, OpenVAS, Qualys, Burp Suite and OWASP ZAP, Nmap

Assets in Energy

Assets in Energy Domain

Assets: Generators, Transformers, Substations, Transmission lines, Distribution lines, Meters, Control systems

- Modbus
- DNP3 (Distributed Network Protocol 3)
- IEC 61850

Modbus: Commonly used for communication between field devices and control systems.

DNP3: Prevalent in utility automation for SCADA (Supervisory Control and Data Acquisition) systems, particularly in electric power systems.

These protocols facilitate:

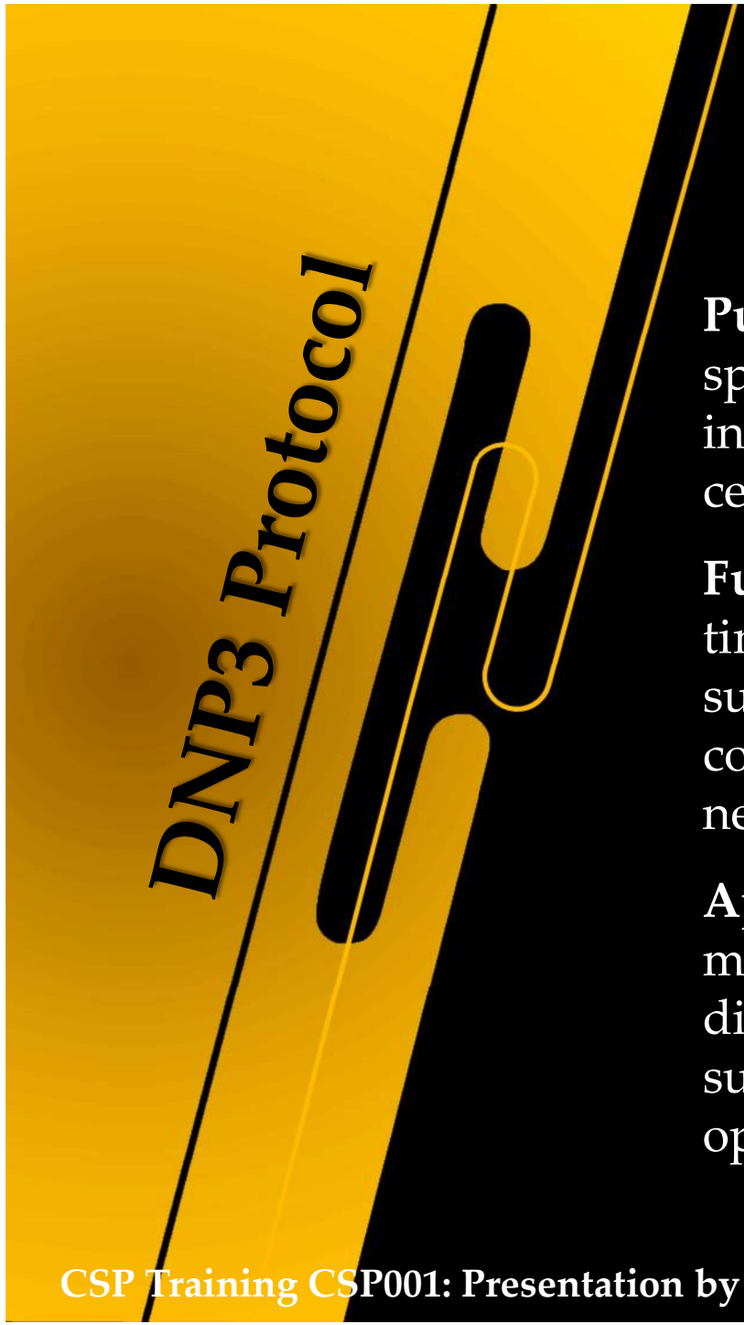
- Data exchange
- Control commands
- Efficient and reliable operations within energy infrastructure.

Modbus

Purpose: Modbus is a serial communication protocol commonly used in industrial automation applications, including the energy sector. It facilitates communication between various electronic devices such as programmable logic controllers (PLCs), sensors, and meters.

Functionality: Modbus uses a client-server architecture where a master device (client) communicates with multiple slave devices (servers) over a serial connection. It supports different data types and functions for reading and writing data to/from registers within devices.

Applications: In the energy domain, Modbus is often used for monitoring and control of distributed energy resources, such as solar inverters, wind turbines, and energy storage systems. It enables real-time data exchange between these devices and supervisory control systems, allowing operators to monitor performance and adjust settings as needed.



DNP3 (Distributed Network Protocol 3)

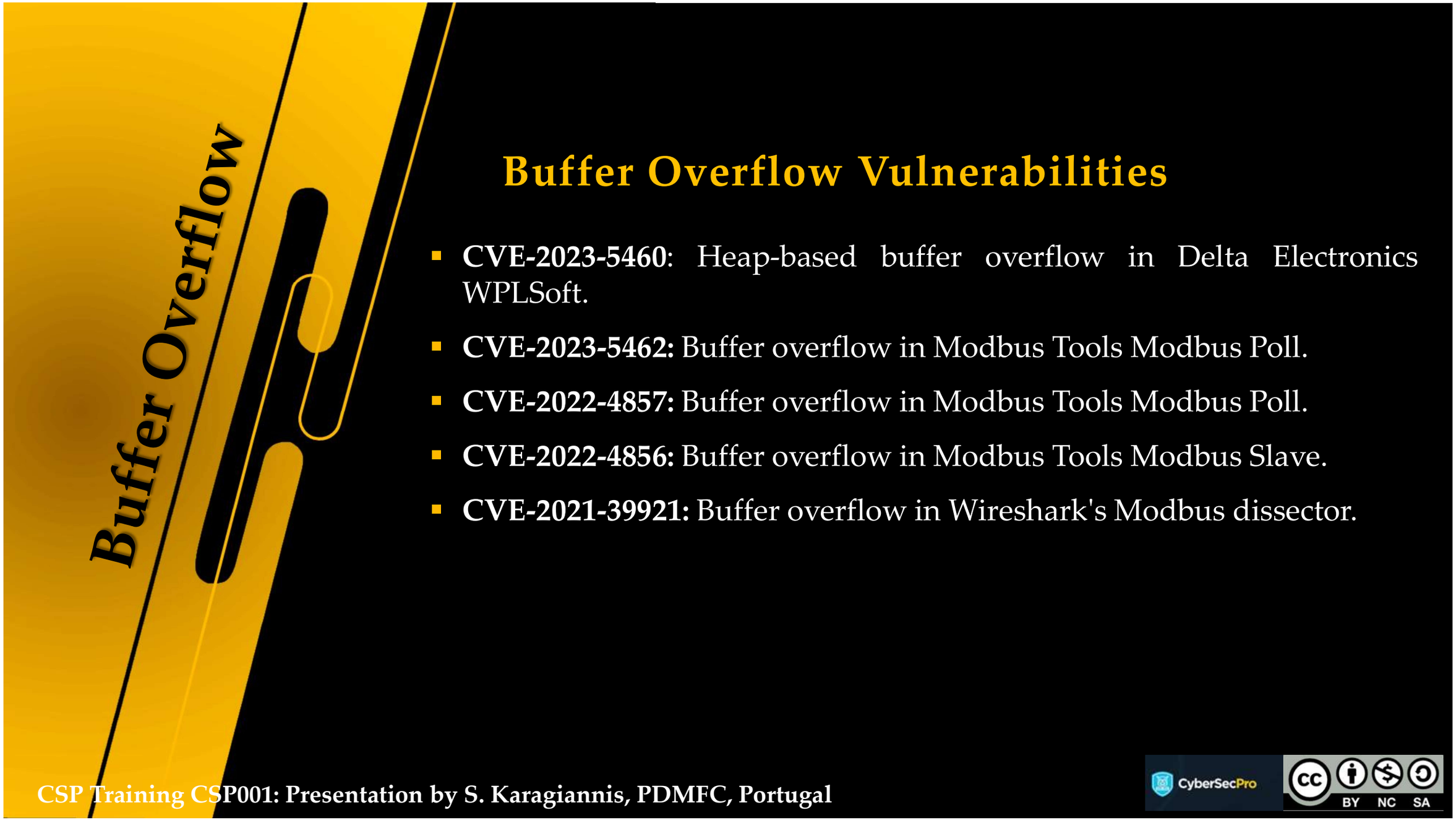
Purpose: DNP3 is a robust and reliable communication protocol designed specifically for use in SCADA systems, particularly in the electric power industry. It provides secure and efficient communication between control centers and remote field devices.

Functionality: DNP3 supports various data types and features such as time synchronization, event reporting, and authentication, making it suitable for critical infrastructure applications. It operates over various communication mediums including serial (RS-232/485) and TCP/IP networks.

Applications: In the energy domain, DNP3 is extensively used for monitoring and control of power generation, transmission, and distribution systems. It allows utilities to collect real-time data from substations, meters, and other field devices, enabling efficient grid operation, fault detection, and response.

Denial of Service (DoS) Vulnerabilities

- **CVE-2023-5462:** Critical DoS vulnerability in XINJE XD5E-30R-E causing service denial.
- **CVE-2023-5460:** DoS due to heap-based buffer overflow in Delta Electronics WPLSoft.
- **CVE-2023-1285:** Race condition in Mitsubishi Electric India GC-ENET-COM leading to DoS.
- **CVE-2023-1150:** Uncontrolled resource consumption in Series WAGO 750-3x/-8x.
- **CVE-2022-37301:** Denial of service due to integer underflow in SolaX Pocket WiFi.



Buffer Overflow Vulnerabilities

- **CVE-2023-5460**: Heap-based buffer overflow in Delta Electronics WPLSoft.
- **CVE-2023-5462:** Buffer overflow in Modbus Tools Modbus Poll.
- **CVE-2022-4857:** Buffer overflow in Modbus Tools Modbus Poll.
- **CVE-2022-4856:** Buffer overflow in Modbus Tools Modbus Slave.
- **CVE-2021-39921:** Buffer overflow in Wireshark's Modbus dissector.

Authentication Bypass Vulnerabilities

- **CVE-2022-45789:** Authentication bypass in EcoStruxure Control Expert.
- **CVE-2022-37300:** Weak password recovery mechanism in various products.
- **CVE-2021-22779:** Authentication bypass in EcoStruxure Control Expert.
- **CVE-2021-22772:** Authentication bypass in Easergy T200.
- **CVE-2020-7523:** Authentication bypass in Schneider Electric Modbus Serial Driver.

Information Exposure Vulnerabilities

- **CVE-2023-5461:** Cleartext transmission of sensitive information in Delta Electronics WPLSoft.
- **CVE-2022-30938:** Memory corruption exposing sensitive information in EN100 Ethernet module.
- **CVE-2022-30937:** Memory corruption exposing sensitive information in EN100 Ethernet module.
- **CVE-2021-22786:** Exposure of sensitive information in Modicon M340 CPU.
- **CVE-2019-7225:** Undocumented credentials exposing sensitive information in ABB HMI.

Code Injection and Privilege Management Vulnerabilities

- **CVE-2019-6549:** Retrieval of plain-text credentials through FTP in PR100088 Modbus gateway.
- **CVE-2019-6547:** Read and write access to Modbus values without authentication in PR100088 Modbus gateway.
- **CVE-2019-6545:** Retrieval of passwords via HTTP GET request in PR100088 Modbus gateway.
- **CVE-2019-6543:** FTP request causing crash in PR100088 Modbus gateway.
- **CVE-2020-7523:** Privilege escalation in Schneider Electric Modbus Serial Driver.

SIMATC and SIPLUS

Denial-of-Service in SIMATIC and SIPLUS

- **CVE-2023-38380:** Affects SIMATIC and SIPLUS products, leading to a denial-of-service issue due to incorrect memory release in the webserver implementation.
- **CVE-2022-43768:** Another denial-of-service vulnerability in SIMATIC and SIPLUS products' webserver implementation.
- **CVE-2022-43767:** Denial-of-service vulnerability affecting SIMATIC and SIPLUS products' webserver.
- **CVE-2022-43716:** Affects webserver functionality in SIMATIC and SIPLUS products, potentially leading to a denial-of-service situation.
- **CVE-2022-30938:** Affects EN100 Ethernet modules, causing memory corruption when parsing HTTP packets and leading to application crashes.

SCADA and IED

Authentication Bypass in SCADA and IED Devices

- **CVE-2021-22772:** Easergy T200 series devices allows unauthorized operation when authentication is bypassed. It poses a significant security risk by potentially granting attackers unauthorized control over critical functions.
- **CVE-2020-6996:** Triangle MicroWorks DNP3 Outstation Libraries allows attackers to exploit a stack-based buffer overflow, potentially leading to unauthorized access to affected systems.
- **CVE-2020-10613:** Triangle MicroWorks SCADA Data Gateway allows remote attackers to disclose sensitive information due to improper validation of user-supplied data, potentially compromising the confidentiality of the system.
- CVE-2020-10611: STriangle MicroWorks SCADA Data Gateway allows remote attackers to execute arbitrary code due to improper validation of user-supplied data, potentially leading to unauthorized access and control over the system.

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

Please send all questions to:
stylianos.karagiannis@pdmfc.com