ENCRYPTION IN ICS NETWORKS

A Blessing or a Curse?

+ information from relevant papers

Introduction

Industrial Control Systems (ICS) are increasingly interconnected, enhancing efficiency but exposing vulnerabilities.

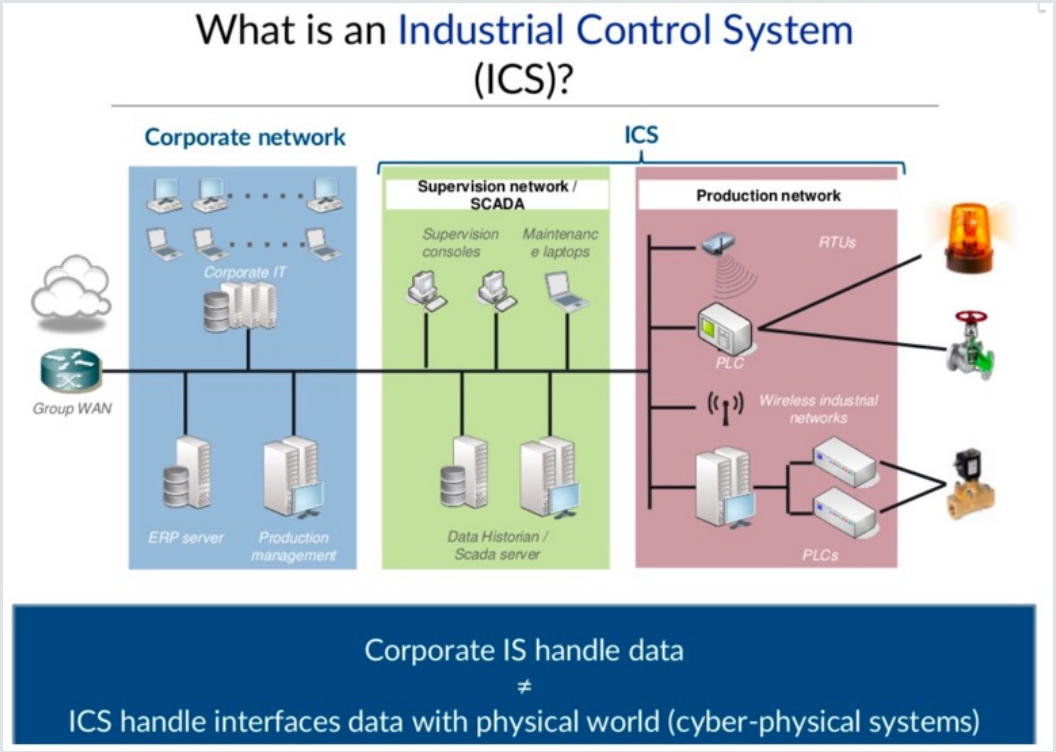
Encryption of network communication is a proposed mechanism to enhance security in ICS.

Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications were determined appropriate (NIST).

However, it raises concerns about usability, troubleshooting costs, and its actual impact on security given real-world attacker models.

SCADA Systems Overview

- SCADA systems oversee geographically distributed processes, connecting control centers and remote stations via IP-based networking.
  - *They include components like HMI, RTU/PLC, and gateways.*
  - *Their key communication categories include data acquisition requests, firmware updates, and control commands.*
- IT/OT Convergence Protocols:
  - *Modern ICS relies on protocols like DNP3, Ethernet/IP, and Modbus for communication between SCADA systems and remote devices.*
  - *These protocols enable real-time control, data sharing, and device configuration while addressing integration challenges.*



- Several geographically distributed remote stations are interconnected with a control center.
  - *This could be through a dedicated link or via the Internet.*
- Each of the stations deals with a different part of a physical process, gathering data through sensors
  - *(e.g. the pressure sensor in Remote Station 2), and/or controlling the process through actuators (e.g. the valve at the same station).*

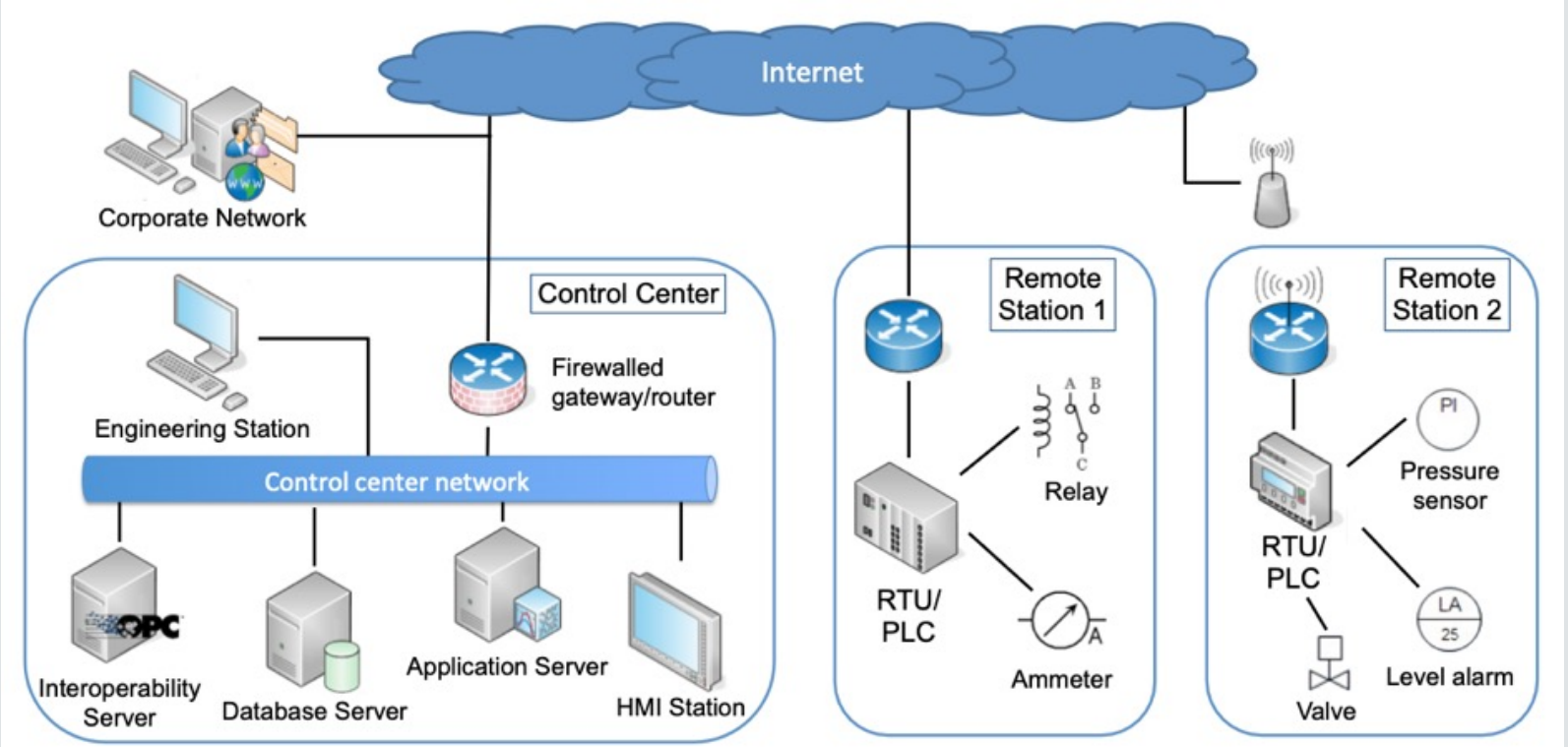


Fig. 1. Simplified architecture of a SCADA system[1]

- End devices monitored and controlled over a local network by Programmable Logic Controllers (PLC) and Remote Terminal Units (RTU).
- These turn interconnected to each other
  - *possibly in hierarchical master/slave architectures or*
  - *across remote stations,*

  in order to coordinate the monitoring of the process.

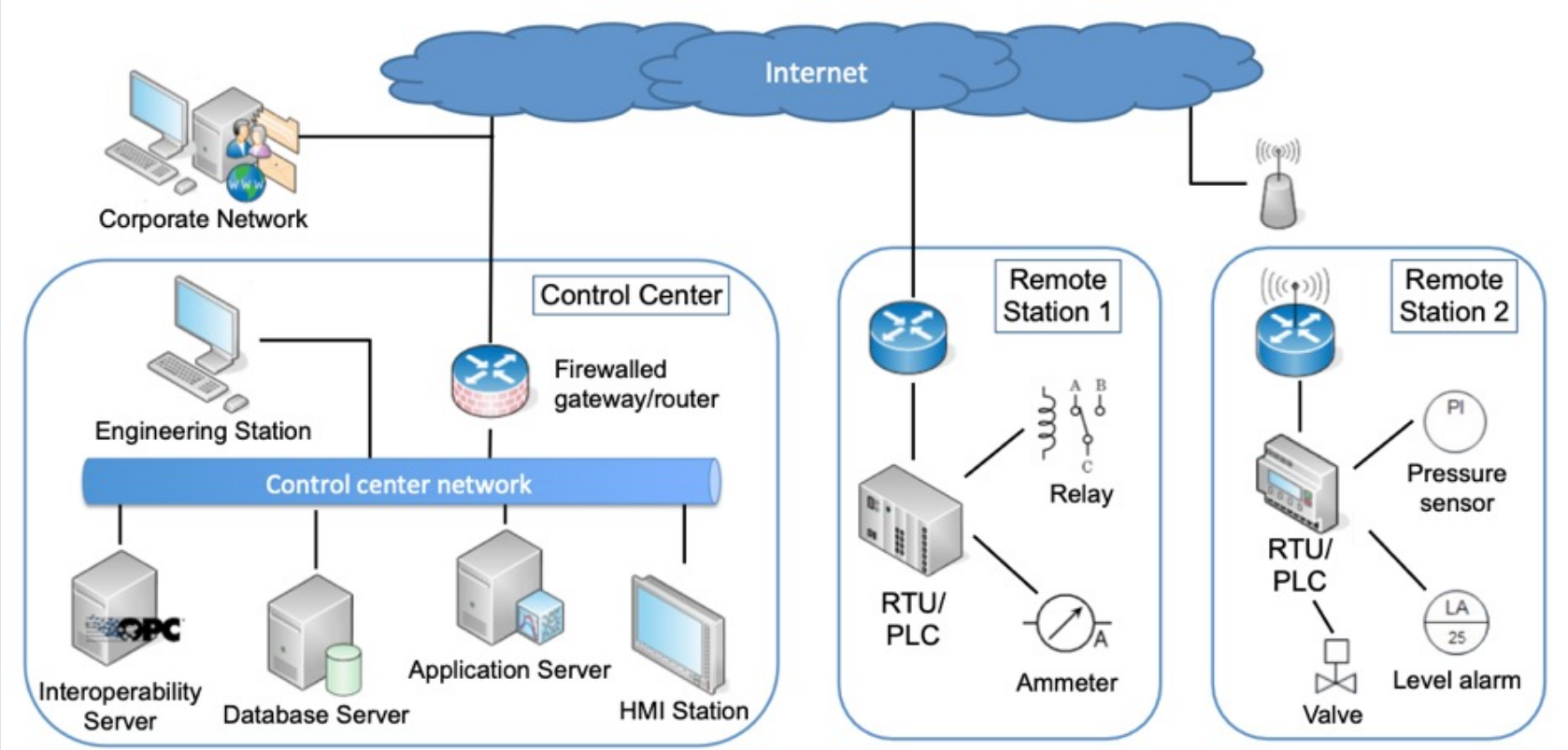


Fig. 1. Simplified architecture of a SCADA system[1]

ICS COMPONENTS

- **Sensors and actuators**: allow interaction with the physical world (pressure sensor, valves, motors, …)
- **Local HMI**: Human-Machine Interface, permits the supervision and control of a subprocess
- **PLC**: Programmable Logic Controller : manages the sensors and actuators
- **Supervision screen**: remote supervision of the industrial process
- **Data historian**: Records all the data from the production and Scada networks
- **RTU** : Remote Terminal Unit (standalone PLC)
- **IED** : Intelligent Electronic Device (smart sensor)

Key Security Properties

Security in ICS emphasizes the CIA triad:

- Confidentiality: Protect sensitive data.
- Integrity: Ensure data remains unaltered.
- Availability: Ensure system operation.

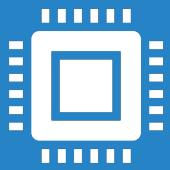
Authenticity is critical for trusted communications.

Correctness of data sent over an untrusted network requires message authenticity,

- a combination of source authentication, i.e. establishing the identity or role of the sender of a message, and message integrity i.e. assuring data has not been altered during transmission.

If the data is valuable, private, or otherwise confidential, we also need message confidentiality.

Resource Constraints



ICS and their real time OSs are often resource-constrained systems that do not include typical contemporary IT security capabilities.

Many systems may not hav

Legacy systems are often lacking resources common on modern IT systems.

feat ures inclu ding encr yptio n, avail able ports, and erro

Indiscriminate use of IT security practices in ICS may cause availability and timing disruptions.

ents to retro fit thes e syst ems with curr ent

Industrial Protocols

DNP3 (Distributed Network Protocol 3)	Ethernet/IP	Modbus
• Designed for SCADA communication, it features hierarchical addressing, robust error-checking mechanisms, and supports time synchronization for event recording.	• Built on Ethernet, supports TCP/UDP, uses CIP (Common Industrial Protocol), and excels in high-speed and scalable applications, though it requires additional security measures.	• A simple protocol supporting RS-485 and TCP/IP communication, widely used for PLCs and RTUs, but lacks advanced security and scalability.

DNP3 (Distributed Network Protocol 3)

- DNP3 is a protocol specifically designed for communication between SCADA systems and remote devices.
- It is commonly used in utilities (water and electric) and other industries for real-time monitoring and control of Operational Technology assets.
- It has the capability of remote monitoring and control of OT assets, including devices like meters, substation equipment, and Remote Terminal Units (RTUs).
- DNP3 provides some security features, robustness, and reliable data transmission, making it a good choice for IT/OT integration in utilities sector.

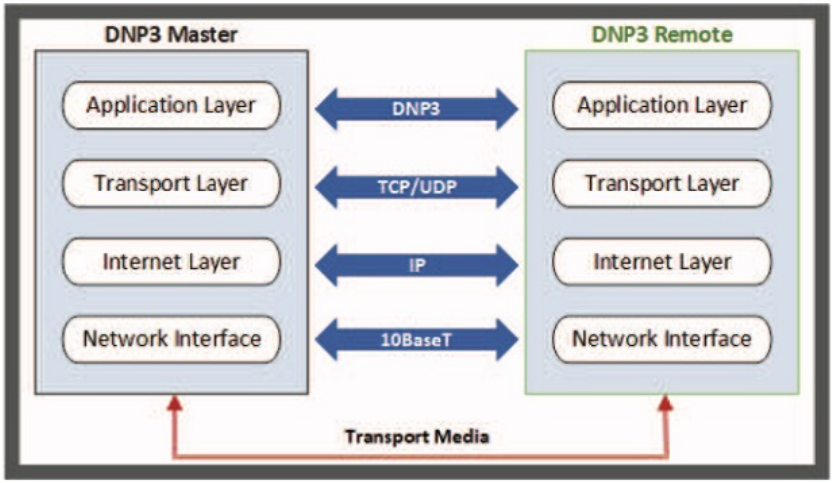
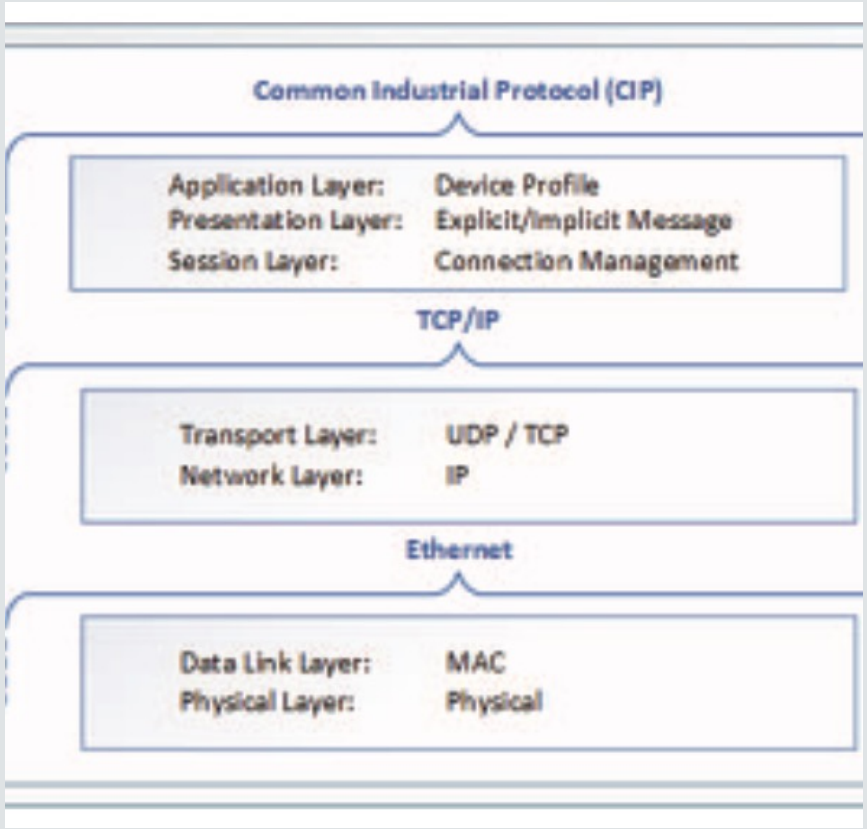


Fig. 1. DNP3 Structure

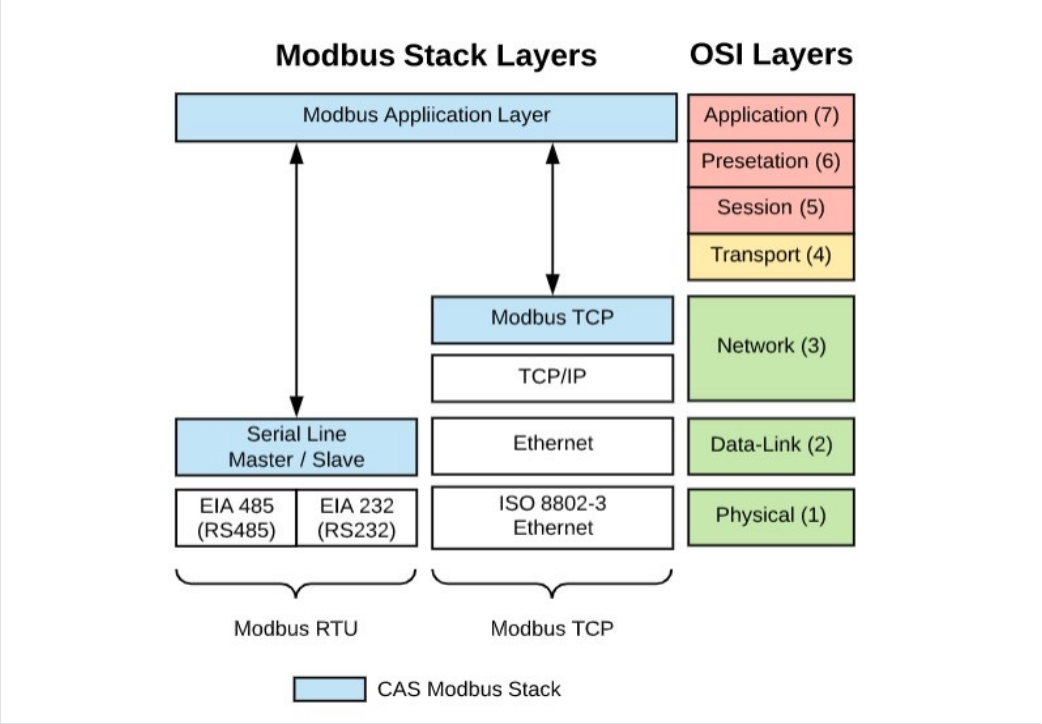
Ethernet/IP

- Ethernet/IP is an industrial protocol built on the foundation of standard Ethernet and TCP/IP technologies.
- It provides a common language for communication between industrial devices and IT systems, allowing for interoperability and integration.
- Ethernet/IP supports real-time control, data sharing, and device configuration which makes it handy for establishing reliable connections between IT and OT



Modbus

- Modbus is a common serial communication protocol widely used in industrial automation for connecting electronic devices.
- It allows communication between devices such as
  - *programmable logic controllers (PLCs) and*
  - *supervisory control and data acquisition (SCADA) sy*
  - *stems,*
  - *Human-Machine Interface Systems (HMI), and*
  - *Remote Terminal Units (RTUs).*
- Modbus supports both binary transmission modes and ASCII, making it flexible to support IT/OT convergence



Encryption Protocols for ICS

- IEC 62351 recommends encryption protocols like TLS and IPsec to secure communications in SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems).
- These systems manage critical infrastructure, such as energy grids and industrial automation, where reliable and secure data exchange is essential.
- Historically, SCADA and ICS networks were isolated, but modern integration with IT systems has increased exposure to cyber threats, necessitating robust encryption mechanisms.

SCADA and ICS Context:

- SCADA and ICS networks rely on real-time communication to monitor and control geographically distributed assets.
- Typical components include Human-Machine Interfaces (HMIs), Remote Terminal Units (RTUs), and Programmable Logic Controllers (PLCs).
- These systems prioritize availability and integrity over confidentiality, as downtime or data tampering can disrupt critical operations.
- The adoption of IP-based networks has made encryption essential for protecting communications over untrusted channels while maintaining operational efficiency.

Encryption Protocols for ICS

- Logical network separation enforced by encryption or network device-enforced partitioning.
  - *Virtual Local Area Networks (VLANS).*
  - *Encrypted Virtual Private Networks (VPNs) use cryptographic mechanisms to separate traffic combined on one network.*
  - *Unidirectional gateways restrict communications between connections to a single direction, therefore, segmenting the network.*

- As a longer-term solution, systems should be designed to include encryption between devices in order to make it very difficult to reverse engineer protocols and forge packets on control system networks.
  - *Encrypting the communications between devices would make it nearly impossible to perform this attack.*
  - *Protocols that provide strong authentication also provide resilience to man-inthe-middle attacks.*
  - *The impact of encryption on network and operational performance needs to be considered*

Encryption Protocols for ICS

- **TLS (Transport Layer Security):** Widely used for point-to-point encryption in SCADA protocols like MMS, DNP3, and IEC 60870-5-104.
  - *It establishes secure sessions between endpoints, protecting data integrity and confidentiality during transmission.*

- **IPsec (Internet Protocol Security):** Suitable for site-to-site communication in SCADA systems.
  - *It can be deployed in tunnel mode to encrypt entire packets, ensuring security across untrusted networks while maintaining compatibility with legacy systems.*

Key encryption in protocols:

TLS: End-to-end encryption with authentication and integrity checks.

IPsec: Secures network-layer communications, suitable for site-to-site tunnels.

OPC-UA: Recommended for industrial automation, ensuring secure interoperability.

Challenges in Operations

- Encrypted networks hinder:
  - *Anomaly detection in encrypted traffic.*
  - *External troubleshooting access without decryption keys.*
  - *Diagnosis of network congestion or device health using standard tools.*

- Operational Concerns with Protocols:
  - *DNP3: Limited bandwidth efficiency and complex implementation impact large-scale systems.*
  - *Ethernet/IP: Real-time performance challenges due to non-deterministic Ethernet behavior.*
  - *Modbus: Security vulnerabilities such as lack of encryption and manual device management pose risks.*

Recommendations

- Adopt encryption selectively in ICS:
  - *Use encryption for long-haul connections over untrusted networks.*
  - *Focus on integrity and authentication within trusted internal networks.*
  - *Ensure balance between security and operational visibility.*

- Tailored Use of Protocols:
  - *Leverage DNP3 for robust SCADA communication where synchronization and event recording are critical.*
  - *Deploy Ethernet/IP in high-speed industrial environments with proper security hardening.*
  - *Use Modbus for simple, resource-efficient communication in less critical environments, supplemented with additional security.*

Recommendations

- Before deploying encryption in Industrial Control Systems (ICS), it is crucial to evaluate its suitability as authentication and data integrity often take precedence.
  - *Alternatives like cryptographic hashes should be considered.*
- Encryption introduces latency, which may impact ICS performance, and this latency must be assessed through extensive testing to ensure operational reliability.
  - *To minimize delays, encryption at OSI Layer 2 is recommended over Layer 3.*
- Encryption has some disadvantages:
  - *Enlarges message sizes due to additional cryptographic overheads like checksums, control protocols, padding, and authentication data.*
  - *It also complicates key management, especially in geographically dispersed systems, making remote key management essential.*
- Effective cryptographic solutions should
  - *comply with standards like NIST/CSE CMVP*
  - *ensure robustness against attacks and secure key management throughout their lifecycle.*

Recommendations

- An encryption strategy must align with a comprehensive and enforced security policy, such as those outlined in the American Gas Association (AGA) report 12-1.
- Cryptographic key lengths should deter brute-force attacks by making guessing infeasible relative to the value of the protected asset.
- Hardware implementing encryption must be safeguarded against physical tampering and unauthorized access, and
- certified modules like those compliant with FIPS 140-2 should be used.
- When feasible, plaintext and ciphertext traffic should use separate ports unless operational constraints dictate otherwise.
- Ultimately, cryptographic deployment should be guided by a thorough risk assessment and tailored to ICS constraints and asset value.

References

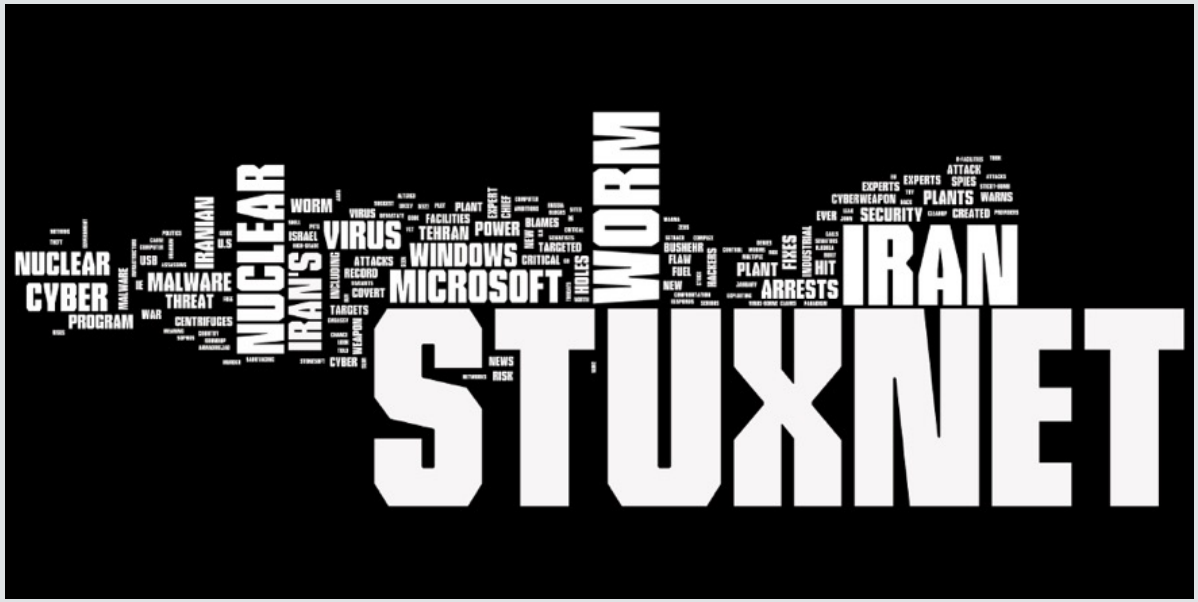
1. National Institute of Standards and Technology. (2015). *Guide to Industrial Control Systems (ICS) Security* (NIST Special Publication 800-82 Rev. 2). Gaithersburg, MD: U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-82r2

2. Fauri, Davide, et al. "Encryption in ICS networks: A blessing or a curse?." *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2017.

3. Annual Threat Report. Technical report, Dell, 2015.

4. IEC 62351: OPC Unified Architecture. International Electrotechnical Commission, 2015

5. Li, Yang, Shihao Wu, and Quan Pan. "Network security in the industrial control system: A survey." *arXiv preprint arXiv:2308.03478* (2023).



Ο ΙΟΣ STUXNET

The first cyber weapon / Το πρώτο κυβερνόπλο

Τι είναι ο Stuxnet?

- Ιδιαίτερα εξελιγμένος, κακόβουλος ιός (Advanced Persistent Threat /APT).
- Σχεδιάστηκε για να προκαλεί ζημιά όχι μόνο στον ψηφιακό, αλλά και στον πραγματικό κόσμο.
- Δημιουργήθηκε το 2008 ***μάλλον*** με συνεργασία ΗΠΑ-Ισραήλ, αν και αυτό δεν έχει αποδειχτεί ποτέ.
- Βασικός στόχος οι εγκαταστάσεις ουρανίου στο Ιράν
- Στόχευε βιομηχανικά συστήματα ελέγχου (PLC) υλικές ζημιές.

- Διείσδυσε σε ηλεκτρονικούς υπολογιστές, που ελέγχουν τα συστήματα φυγοκέντρισης στις πυρηνικές εγκαταστάσεις της Νατάνζ, προκαλώντας όχι μόνο δυσλειτουργίες, αλλά και υλικές ζημιές.

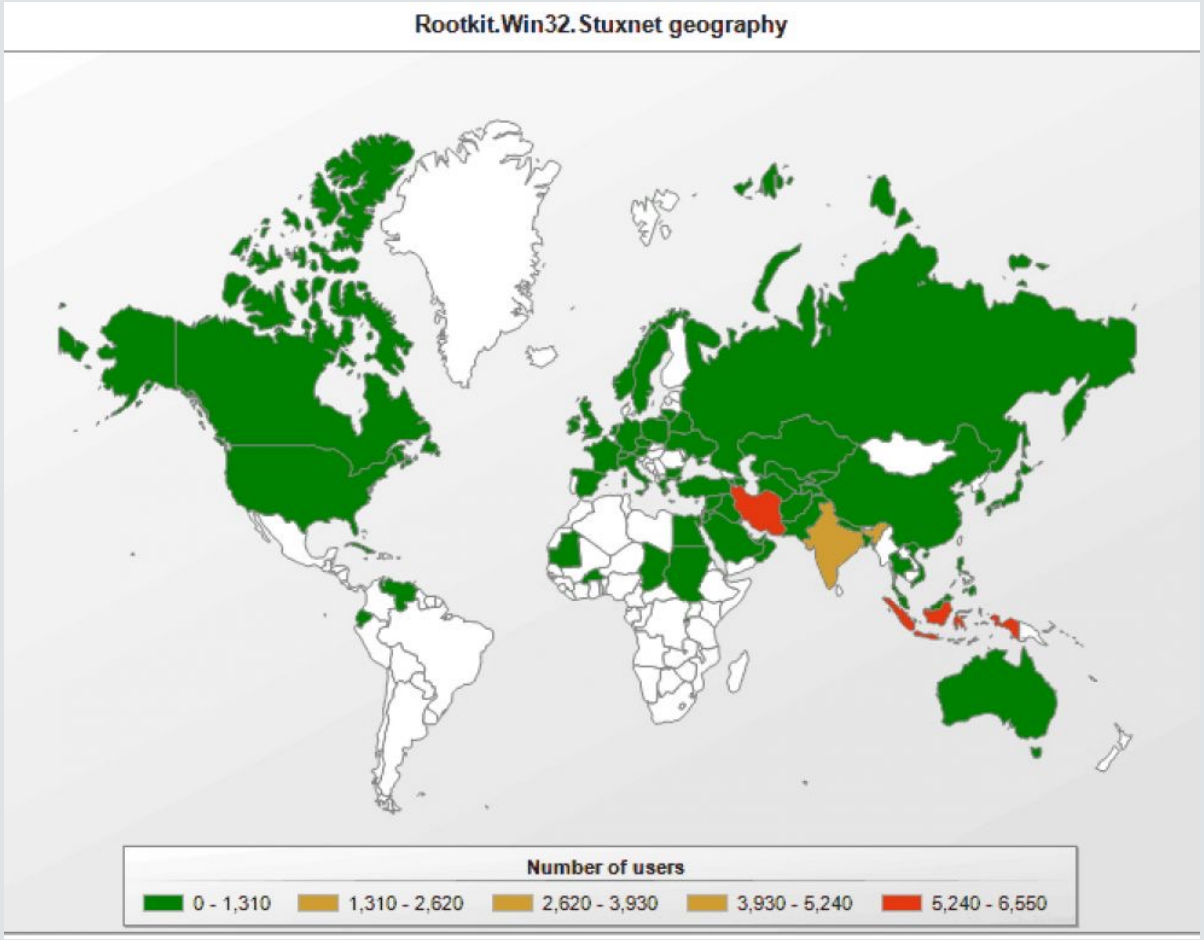
Χαρακτηριστικά Stuxnet?

- Οι μέσοι ιοί είναι περίπου 10k bytes σε μέγεθος. Ο Stuxnet ήταν 500 KB (χωρίς γραφικά).
- Συνήθως ο ιός περιέχει 1 zero-day vulnerability. Ο Stuxnet είχε 5!
- Αλλοίωσε 2 ψηφιακά πιστοποιητικά
- Ενήργησε σαν rootkit, κρύβοντας τις ενέργειές την παρουσία του
- Ήταν ο πρώτος ιός που συμπεριέλαβε κώδικα για να επιτεθεί συστήματα εποπτείας ελέγχου και εξαγοράς δεδομένων (SCADA).

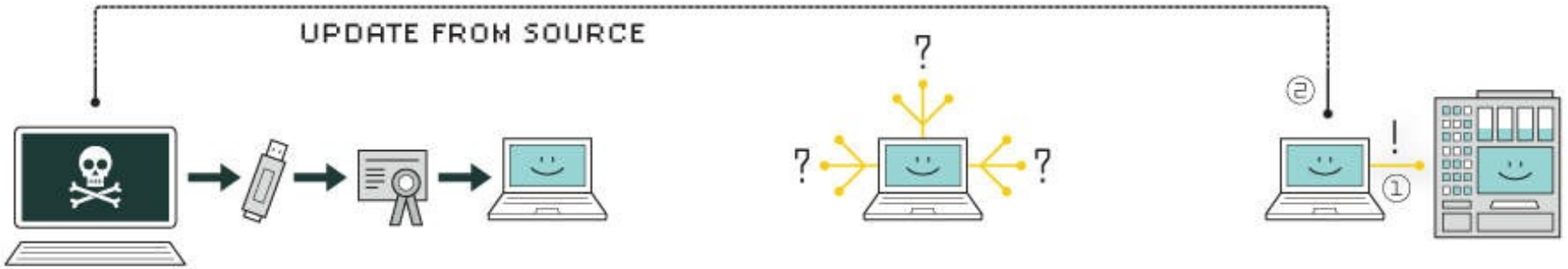
Evolution of Stuxnet exploits

Vulnerability	0.500	1.001	1.100	1.101	Description
CVE-2010-3888			X	X	Task scheduler EOP
CVE-2010-2743			X	X	LoadKeyboardLayout EOP
CVE-2010-2729		X	X	X	Print spooler RCE
CVE-2008-4250		X	X	X	Windows Server Service RPC RCE
CVE-2012-3015	X	X	X	X	Step 7 Insecure Library Loading
CVE-2010-2772		X	X	X	WinCC default password
CVE-2010-2568			X	X	Shortcut .lnk RCE
MS09-025		X			NtUserRegisterClassExWow/NtUserMessageCall EOP

Παγκόσμια διασπορά του Stuxnet



HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Πώς γίνεται ο έλεγχος/ updates ?

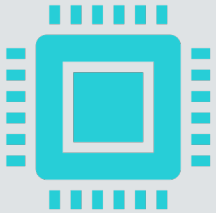
Επικοινωνεί με τους servers:

Smartclick.org

Best-advertising.net

Internetadvertising4u.com

Ad-marketing.net



Χρήση http για επικοινωνία με Command and Control (http-c2)

Messages sent to server which immediately forwards message to some other (unknown) server.

Embeds upload information on infection and download updates to virus through

Information passed back in encrypted with AES using 1 of several keys.

ΠΏΣ ΓΊΝΕΤΑΙ Ο ΈΛΕΓΧΟΣ/ UPDATES?