Cyber / Analytical Presentation

By: Duchess Rodgers, Seth Moore, Derrick Amissah

CIA Triad

By: Duchess Rodgers

What is the CIA Triad ?

- A model used to protect information security
- (C)onfidentiality - ensuring that sensitive information is accessible only authorized users and processes.
- (I)ntegrity - maintaining the accuracy and trustworthiness of data, preventing unauthorized modification or destruction
- (A)vailability - guaranteeing that authorized users can access data and resources when they need them.

Why is it Important?

- ensures data security (checks and balances)
- serves as a model for developing and implementing security policies and controls
- helps identify and mitigate potential vulnerabilities and risks
- improves incident response
- essential for business continuity

How it is Used (daily life)

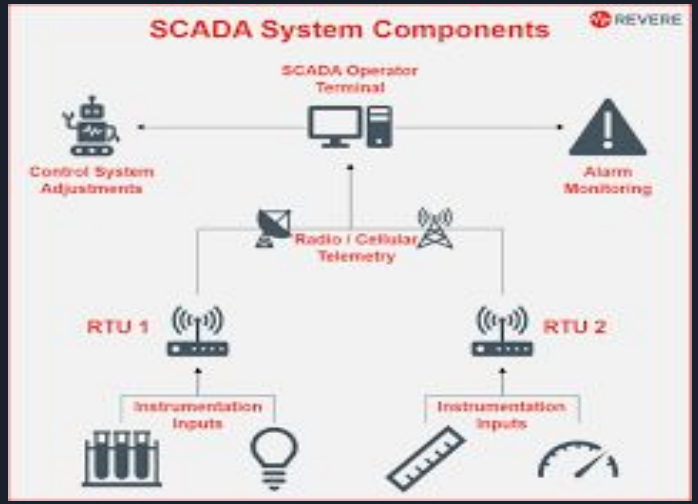
- Confidentiality
  - Online banking - encryption protocols protect your personal and financial information; also ensures that only you and the authorized bank personnel can view or manage your account
- Integrity
  - Online platforms - integrity helps maintain the accuracy of information shared on social media, forums, and online communities, preventing the spread of misinformation and maintaining trust within these communities
- Availability
  - Online services (e.g., Shein, Amazon, etc.) - ensure that their services are available to users, even during peak hours or system outages

SCADA Systems

By: Derrick Amissah

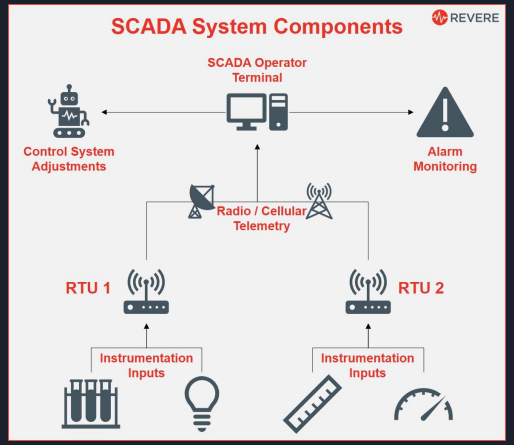
What is a SCADA System?

- A SCADA system (Supervisory Control and Data Acquisition) is a computer system that helps monitor and control things like factories, power plants, water systems, or other big machines and equipment.



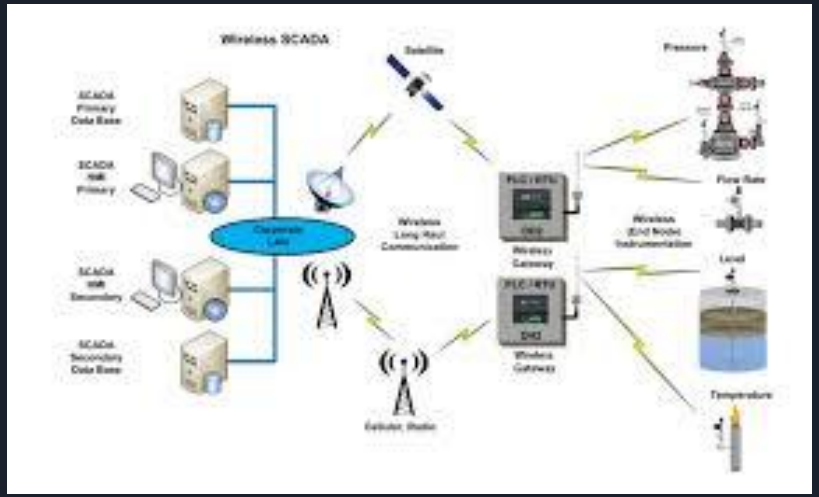
Why are SCADA Systems important?

- Helps keep big, critical things run smoothly like electricity, water, gas, and factories.
- Without SCADA, people would have to be everywhere checking and controlling machines by hand.
- SCADA lets you watch, control, and fix problems from far away, fast. If something breaks or goes wrong (like a water pump failing or power line overheating), SCADA can send alerts right away, so it can be fixed before things get out of hand.



How Is SCADA Used ?

- Used to monitor and control machines like pumps, power lines, or factory equipment, often from far away.
- Collects data through sensors, shows it on screens, and can send alerts or automatically fix problems if something goes wrong.
- Helps keep important systems running safely, efficiently, and without needing people to be everywhere in person.



Additional Information About SCADA

- They save time and money by letting machines run automatically and reducing the need for people to check things in person.
- Because they’re connected to networks, they need strong cybersecurity to protect them from hackers.

Phishing: A Common Threat

By: Seth Moore

Common threats

- What are the common threats?
  - There are many common threats, hence the name “common” threats. Some of them include, various malware, DDOS attacks, **Phishing**, and zero day exploits.
  - Phishing is the most common, and has resulted in a great amount of damages.

- How is phishing done? What is it?
  - Phishing is deception, for instance one could receive an email containing a fake bill that when paid will steal their credit card information.

Why is knowing about phishing important?

- Phishing has resulted in over a billion dollars of damages last year alone is projected to increase.
- According to the FBI has constantly been the most prevalent cyber threat out there.
- Phishing may not just steal money too, it has the capability to plant malware places, steal SSN and much more. Most of the time Phishing can be the precursor to most common threats.

Other things to know about phishing

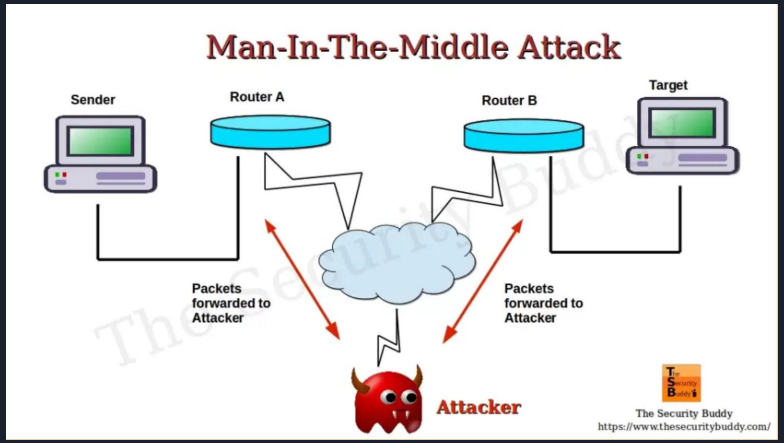
- Phishing is the most common and costly issue in cybersecurity, but you can take steps to defend against it.
  - Always make sure to use antivirus software and keep it constantly updated
  - Never reply to ANY email asking for information about yourself
  - Be wary of fear based claims “Your account will be suspended”, and “You have a bill”
  - Only ever open email attachments if you are expecting them and know what they are

Man in the Middle

By: Duchess Rodgers

What is “Man in the Middle?”

- A cyber-attack where an attacker intercepts and manipulates communication between two parties, making it appear as if the parties are communicating directly with each other
- The attacker inserts themselves into the conversation, eavesdropping, stealing information, or even altering messages without the knowledge of either party.



Why is it Important?

- Compromises the confidentiality, integrity, and authenticity of communications
- Leads to theft of personal information, financial data, login credentials, and other sensitive information
- Results in financial loss, identity theft, and damage to reputations

How it is Used

- **Wi-FI Eavesdropping**
  - An attacker sets up a rogue Wi-Fi hotspot and tricks users into connecting to it
  - Once connected, the attacker can intercept all data transmitted over the network
- **IP Spoofing**
  - The attacker masks their IP address to appear as a trusted source, intercepting communications between the victim and the intended recipient
- **DNS Spoofing**
  - The attacker alters DNS records to redirect the victim to a malicious website that looks like legitimate one.

Examples

- Public Wi-Fi
  - attacker sets up a free Wi-Fi network in a public place
  - users connect to this network and the attacker steals their data and sensitive information
- Email Hijacking
  - attacker intercepts email communications between two parties like a business and a client
  - attacker can alter emails to redirect payments to his/her account

Additional Information

- To protect against MitM attacks, use secure communication channels such as HTTPS
- Avoid using public networks/WiFi (especially for sensitive transactions)
- Using VPNs (virtual private networks) can encrypt your data and reduce the risk of an attack/theft
- Verify the authenticity of websites
- Avoid clicking on suspicious links or downloading unknown files

Philosophical Approach

Q: Are we adequately thinking through the long-term impact of technologies being developed today (the short arm of predictive knowledge)?

A: Our ability to predict the future impact of technology is limited. It can be difficult to anticipate every possible outcome; this is why incident responses and recovery is essential.

We are better at recovering from cyber-attacks, thanks to better threat intelligence sharing and response teams. However, we underestimate the risks of interconnected systems. For example, AI-generated content can be used in phishing or deep fake-driven social engineering attacks.

Notebook LM PODCAST

https://notebooklm.google.com/notebook/a88dbecd-285d-46d4-b29f-ad96455128b3?_gl=1*4edk85*_ga*MjA2NTAyNzQ5LjE3NDU0MzA3NDg.*_ga_W0LDH41ZCB*MTc0NTQzMDc0Ny4xLjAuMTc0NTQzMDc0Ny42MC4wLjA.&original_referer=https:%2F%2Fnotebooklm.google%23&pli=1

References

- FBI’s IC3 Report: Losses from Cybercrime Surpass $12.5 Billion—a New Record | Proofpoint UK. (2024, March 18). Proofpoint. https://www.proofpoint.com/uk/blog/email-and-cloud-threats/fbis-ic3-report-losses-cybercrime-surpass-125-billion-new-record
- imperva. (2019). What is MITM (Man in the Middle) Attack. Imperva. https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/
- Irwin, L. (2023, February 14). What Is the CIA Triad and Why Is It Important? IT Governance UK Blog. https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important
- Phishing 101: Tips to Protect Yourself. (n.d.). Retrieved April 16, 2025, from https://www.it.miami.edu/wda/it/UMIT_Security_Phishing_101_Tips.pdf