THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Doctor of Engineering – Cybersecurity Analytics

Cohort: DC7

SEAS 8405: Cybersecurity Architecture

November 9, 2024

HOMEWORK – 1

SUBMITTED BY

Viswanath S CHIRRAVURI

G34657239

viswanath.chirravuri@gwu.edu

(Under the guidance of Professor John P Sahlin)

Attached Files:
File CISA-Cybersecurity-Advisory-Committee_DRAFT-Recommendations_20241011.pdf

Watch the video of Dir. Easterly's Opening Statement before Congress on the Cyber Threat from China: https://youtu.be/kWFihTC2pOs?si=VqK5hBRssmW1W2jQ

Review the CISA Draft Report on Building Resilience for Critical Infrastructure (also available in Electronic Reserves)

Describe how the architecture context of a system drives cybersecurity architecture decisions about the design of a system.

Describe how you would balance the need for security and the need to execute a business goal with the constraints of the architecture context / operational environment of a system. What tradeoffs would you consider?

How did Dir. Easterly's comments change your view of this issue?

Compare Dir. Easterly's comments and the CISA Draft Report findings compare to the concept of Boehm's curve with respect to cybersecurity. Is Shift Left cybersecurity dead? Explain your answer.

Q. Describe how the architecture context of a system drives cybersecurity architecture decisions about the design of a system.

The system's setup, or "architecture," strongly outlines the choices made for its cybersecurity. This means that how a system is built, what it depends on, and the types of risks it faces all decide the kind of security it needs. For example, as stated in the document, many critical systems like electricity grids or transportation networks might face threats from foreign countries. Because of this, they need security solutions that are specific to their needs, not just one-size-fits-all methods. If a system relies a lot on outside services or is connected to many other networks, the security has to cover all these areas and make sure it can still work even if it's attacked.

Also, understanding the system's role and its connections to other services helps in deciding what security measures are most important. Some systems are so critical that if they stop operations (for whatever reason), it could affect the whole country. So, the security has to ensure these key services keep running smoothly, even during major incidents. CISA, a U.S. agency, works with public and private sector managers to plan for these situations and makes sure there are backup plans and strong protections in place.

Lastly, the architecture also guides how prepared the system is for tough situations. For instance, they may even plan for ways to keep running manually if digital systems fail. This approach helps avoid big breakdowns and ensures that systems can keep working no matter what happens. So, good cybersecurity design is about more than stopping attacks, it's about creating a setup that's strong, flexible, and ready for anything.

Q. Describe how you would balance the need for security and the need to execute a business goal with the constraints of the architecture context / operational environment of a system. What tradeoffs would you consider?

Balancing security needs with business goals in a constrained operational environment involves a careful evaluation of trade-offs that optimize security without impacting critical functions. Based on insights from the CISA Cybersecurity Advisory Committee's recommendations, here are the key considerations:

- **Risk Mitigation vs. Business Continuity**: Effective security measures should protect against threats while preserving operational continuity. This means prioritizing resilience over perfect security, especially for critical infrastructure where downtime has significant impacts. CISA recommends resilience planning and quick-implement measures to mitigate impact while maintaining essential functions.
- **Threat Detection and Living Off the Land**: Given constraints, traditional threat detection may not be suitable, especially against nation-state actors. CISA's focus is on both threat intelligence and sector-specific risk mitigation. An approach that includes "living off the land" detection, or using native functions to detect threats, can be less resource-intensive and more adaptive.
- **Sector-Specific Threat Modeling**: Different sectors have unique technology environments and risk profiles, which impacts how security measures can be balanced with business goals. CISA advises using tailored strategies and conducting sector-specific exercises to build resilience and ensure defenses are appropriate to the operational environment without overburdening systems.
- **Automated Controls**: In resource-limited environments, automated threat response reduce the need for constant monitoring and manual updates. This approach, advised for systems with shared dependencies, allows efficient use of resources while maintaining security.
- **Tradeoffs in Speed and Security Investment**: Investing in resilience measures, like enhanced defense and rapid threat detection, should be balanced with cost and implementation time. CISA's recommendation to focus on quick-to-implement security measures helps ensure systems remain functional without heavy upfront investments in complex security architectures.

Overall, a balanced approach should maintain essential functions, adopt sector-specific risk models, and use automation where feasible to support both security and operational needs.

Q. How did Dir. Easterly's comments change your view of this issue?

The United States faces a serious and escalating threat from Chinese cyber actors, specifically Volt Typhoon, which targets critical infrastructure to exploit vulnerabilities in legacy systems. This activity is particularly alarming because it seeks to infiltrate deep into essential sectors like energy, telecommunications, water facilities, and transportation, aiming to enable destructive attacks during crises or major events. Such attacks could endanger American lives and create widespread panic. This threat is real. CISA has already detected and prevented intrusions across various critical infrastructure sectors, representing only a fraction of attempted attacks. To counter this, CISA collaborates with government and industry partners to identify and mitigate Chinese cyber threats, pushing essential threat intelligence directly to infrastructure owners and operators. Additionally, CISA leverages subject matter experts to assist businesses in strengthening security and resilience. However, these measures alone are insufficient to fully address the scale of the threat.

Legacy systems in U.S. infrastructure are particularly vulnerable, and every incident must be reported to CISA or the FBI to ensure a coordinated response. Strengthening relationships with CISA for threat intelligence is crucial, and businesses must double down on their current protection mechanisms while preparing for attack recovery and backup operations to safeguard the nation's critical systems.

Q. Compare Dir. Easterly's comments and the CISA Draft Report findings compare to the concept of Boehm's curve with respect to cybersecurity. Is Shift Left cybersecurity dead? Explain your answer.

Dr. Easterly's comments and the CISA Draft Report findings reveal a strong focus on reactive resilience strategies over early-stage prevention, which contrasts with the proactive principles of Boehm's curve and the "shift left" approach in cybersecurity. Boehm's curve demonstrates that addressing security vulnerabilities earlier in the software development lifecycle (during design and coding) is far more cost-effective than fixing them later in deployment. This is the foundation of the "shift left" approach, which prioritizes embedding security early to prevent more costly and complex issues down the line.

However, both Dr. Easterly's comments and the CISA report emphasize mitigating and responding to ongoing threats, especially those targeting legacy systems in critical infrastructure, where "shift left" may be difficult to implement due to system age, resource constraints, and operational demands. CISA's work largely centers on detecting, containing, and recovering from active threats, especially as Chinese cyber actors like Volt Typhoon exploit known vulnerabilities in outdated infrastructure. This reactive stance highlights that while shift-left principles may be ideal, they face serious challenges in practice, particularly in large, critical infrastructures bound by legacy technology and complex dependencies that complicate proactive security enhancements.

In this context, shift left cybersecurity is not necessarily "dead," but it is hampered by structural challenges in certain domains, such as critical infrastructure, where legacy systems are common, upgrades are costly, and disruptions pose high societal risks. The need to "shift right" with a focus on resilience, threat detection, and rapid incident response becomes a necessary adaptation. Ultimately, while shift left remains an ideal goal, sectors reliant on older technology and facing advanced threats may find it more practical to balance shift-left aspirations with robust reactive defenses to handle vulnerabilities that cannot be feasibly addressed earlier in the lifecycle.

References

1. Cybersecurity and Infrastructure Security Agency. (2024, October 11). *CISA Cybersecurity Advisory Committee draft recommendations. CyberScoop*. Retrieved from https://cyberscoop.com/wp-content/uploads/sites/3/2024/10/CISA-Cybersecurity-Advisory-Committee_DRAFT-Recommendations_20241011.pdf

2. Cybersecurity and Infrastructure Security Agency. (n.d.). *Cybersecurity and Infrastructure Security Agency*. U.S. Department of Homeland Security. Retrieved November 9, 2024, from https://www.cisa.gov/

3. Opening Statement by CISA Director Jen Easterly. (2024, January 31). *CISA Director Jen Easterly gave her opening statement before the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party*. [Video]. YouTube. https://www.youtube.com/watch?v=kWFihTC2pOs

***** END OF DOCUMENT *****