Security Architecture and System Design

Ryan Coon

CYB-690

Dr. Kim Ford

September 24, 2025

Part 1:

RC Cybersecurity will deploy a range of hardware and software devices critical to its operations, including secure servers, firewalls, intrusion detection/prevention systems (IDPS), endpoint protection software on all workstations and mobile devices, secure routers and switches, and potentially IoT devices for operational monitoring. Sensitive data types to be stored will encompass customer Personally Identifiable Information (PII), financial records, proprietary intellectual property, employee data, and operational logs.

Technical requirements for compliance will align with industry best practices and regulatory mandates, such as GDPR, CCPA, and NIST guidelines. This involves ensuring all network devices, servers, and endpoints meet stringent security configurations. Externally, cloud services and partner integrations will be assessed for their security posture and compliance certifications. Internally, systems architecture will be designed with a layered security approach, often referred to as 'defense in depth'(Legit Security, n.d.).

Security controls and services will be strategically positioned throughout the architecture. Network security will be managed by firewalls and IDPS at the perimeter and within internal network segments. Endpoint security will be enforced via robust antivirus, anti-malware, and endpoint detection and response (EDR) solutions. Data security will be paramount, with encryption applied to data at rest or in databases and storage systems and in transit using TLS/SSL for all network communications. Access restriction will be implemented through the principle of least privilege, ensuring users and systems only have access to the resources necessary for their function(Computer Security Division, I. T. L., 2022). This will be managed via Role-Based Access Control (RBAC).

Authentication will be multi-factor (MFA) for all access points, especially for privileged accounts and remote access. Storage encryption will utilize strong cryptographic algorithms to protect sensitive data, even in the event of a physical breach. Automated data security policies will be deployed to enforce data retention, deletion, and classification rules, reducing manual error and ensuring consistent application(Naka, 2023). Procedures will detail incident response, vulnerability management, and regular security audits. Technical responsibilities will be clearly defined for system administrators, network engineers, and security analysts, covering patch management, configuration hardening, and continuous monitoring.

Effective security program management involves establishing a clear security strategy, implementing robust policies and procedures, conducting regular risk assessments, and fostering a security-aware culture. This includes developing an incident response plan, managing security awareness training, and ensuring continuous monitoring of security events.

Assessing the effectiveness of the security program will be achieved through a combination of metrics, including vulnerability scan results, penetration testing outcomes, the number and severity of security incidents, compliance audit findings, and the results of regular security control testing(CISA, 2023). Key Performance Indicators (KPIs) related to threat detection and response times will also be tracked to gauge program efficacy.

Part 2:

The primary design goals for RC Cybersecurity's security architecture are to ensure the Confidentiality, Integrity, and Availability (CIA) of its systems and data, alongside maintaining operational resilience and adaptability. Key considerations include minimizing the attack surface through secure configurations, implementing a defense-in-depth strategy with multiple layers of security controls, and adhering to the principle of least privilege for all access.

Threat modeling is a cornerstone of this design, employing methodologies like STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) to systematically identify potential threats and vulnerabilities(Kelly & Sastre, 2023). This proactive approach allows RC Cybersecurity to anticipate attacker methodologies and build defenses accordingly, informing the overall security architecture.

The high-level security architecture will feature a layered defense. This includes perimeter security with firewalls and Intrusion Detection/Prevention Systems (IDPS), network segmentation to isolate critical assets, robust endpoint security on all devices, and secure application development practices. Identity and Access Management (IAM) with Multi-Factor Authentication (MFA) will enforce strict access controls. Data will be encrypted at rest and in transit, with Data Loss Prevention (DLP) measures in place. Continuous monitoring via a Security Information and Event Management (SIEM) system will provide visibility and facilitate rapid incident response.

Security baselining establishes minimum security standards for all systems and devices, ensuring consistency and hardening against common exploits. This involves defining secure configurations for operating systems, network devices, and applications. The data design focuses on data classification, minimization, and implementing appropriate security controls based on sensitivity, including encryption and strict access logging.

The human-machine interface (HMI), particularly for operational systems, will be designed for intuitive use and clear presentation of security status, minimizing the potential for human error. Operational scenarios will define how users interact with systems during normal business operations, as well as during security incidents or disaster recovery events, ensuring security protocols are integrated into every workflow.

**A diagram of a computer network

AI-generated content may be incorrect.**

The importance of secure software cannot be overstated, as vulnerabilities can lead to data breaches, financial losses, reputational damage, and disruption of services. Secure software protects sensitive data, maintains customer trust, and ensures compliance with regulations.

To achieve secure software, RC Cybersecurity will adopt rigorous programming practices. These include:

* Input Validation - Ensuring all data received from users or external systems is checked for correctness and malicious intent before being processed.
* Output Encoding - Properly encoding data before it's displayed or transmitted to prevent cross-site scripting (XSS) attacks.
* Secure Error Handling - Avoiding the disclosure of sensitive system information in error messages.
* Authentication and Authorization - Implementing strong mechanisms to verify user identities and control access to resources.
* Cryptography - Utilizing robust encryption algorithms for data at rest and in transit.
* Memory Management - Preventing vulnerabilities like buffer overflows through careful memory handling.

Development processes will integrate security throughout the Software Development Lifecycle (SDLC), often referred to as DevSecOps. This means security is not an afterthought but a continuous consideration:

* Threat Modeling - Identifying potential threats and vulnerabilities during the design phase.
* Secure Code Reviews - Having developers review each other's code specifically for security flaws.
* Static Application Security Testing (SAST) - Analyzing source code to find vulnerabilities before execution.
* Dynamic Application Security Testing (DAST) - Testing the running application for vulnerabilities.
* Software Composition Analysis (SCA) - Identifying and managing security risks in open-source components.
* Penetration Testing - Simulating real-world attacks to uncover exploitable weaknesses.

Methodologies that lead to secure software include:

* Secure Software Development Lifecycle (SSDLC) - A framework that embeds security activities into each phase of the traditional SDLC.
* DevSecOps - An approach that integrates security practices into DevOps workflows, automating security checks and deployments.
* OWASP (Open Web Application Security Project) Guidelines - Following best practices and guidelines from OWASP, such as the OWASP Top 10, which lists the most critical web application security risks.

References:

CISA. (2023). *TLP:CLEAR Continuous Diagnostics and Mitigation Program Technical Capabilities Volume Two: Requirements Catalog*. https://www.cisa.gov/sites/default/files/2023-08/CDM\_Tech%20Volume2\_v2.5.pdf

Computer Security Division, I. T. L. (2022a, March 3). *Access CPRT - Cybersecurity and Privacy Reference Tool | CSRC | CSRC*. CSRC | NIST. https://csrc.nist.gov/projects/cprt/catalog#/cprt/home

Computer Security Division, I. T. L. (2022b, May 9). *Hardware Security | CSRC | CSRC*. CSRC | NIST. https://csrc.nist.gov/projects/hardware-security

Dataguard. (2025). *Cyber security compliance 101 — All you need to know*. Dataguard.com. https://www.dataguard.com/cyber-security/compliance

Dijk, V. van. (2024, November 13). *A Complete Guide to Threat Modeling for Security Experts, Architects and developers*. Security Scientist. https://www.securityscientist.net/blog/a-complete-guide-to-threat-modeling-for-security-exports-architects-and-developers

Kelly, J., & Sastre, D. (2023, February 20). *Security by design: Security principles and threat modeling*. Www.redhat.com. https://www.redhat.com/en/blog/security-design-security-principles-and-threat-modeling

Legit Security. (n.d.). *Learn About Secure Software Development & Best Practices*. Www.legitsecurity.com. https://www.legitsecurity.com/secure-software-development-best-practices

Murison, N. (2024, March 20). *Understanding the 3 Phases of Cybersecurity Architecture | Ardoq*. Www.ardoq.com. https://www.ardoq.com/blog/cybersecurity-architecture

Naka. (2023, February 25). *Recommended Design for a Secure Network Architecture*. Medium. https://medium.com/@nakah\_/recommended-design-for-a-secure-network-architecture-15612e17ece4

Schulz, S. (2023, June 6). *Security Architecture Diagrams: A Quick Overview & Example*. GoGet Secure. https://gogetsecure.com/security-architecture-diagram

SentinelOne. (2025, August 11). *What Is Cyber Security Architecture?* SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-architecture

Team, H. (2024, March 28). *Secure Software Development: Best Practices, Frameworks, and Resources*. Hyperproof. https://hyperproof.io/resource/secure-software-development-best-practices