Group Assignment 6.1: Blueprint for Modern Component Architecture

Jacob Harrison

Joshua A. Wortz

Stephanie Wright

University of San Diego

CSOL-520

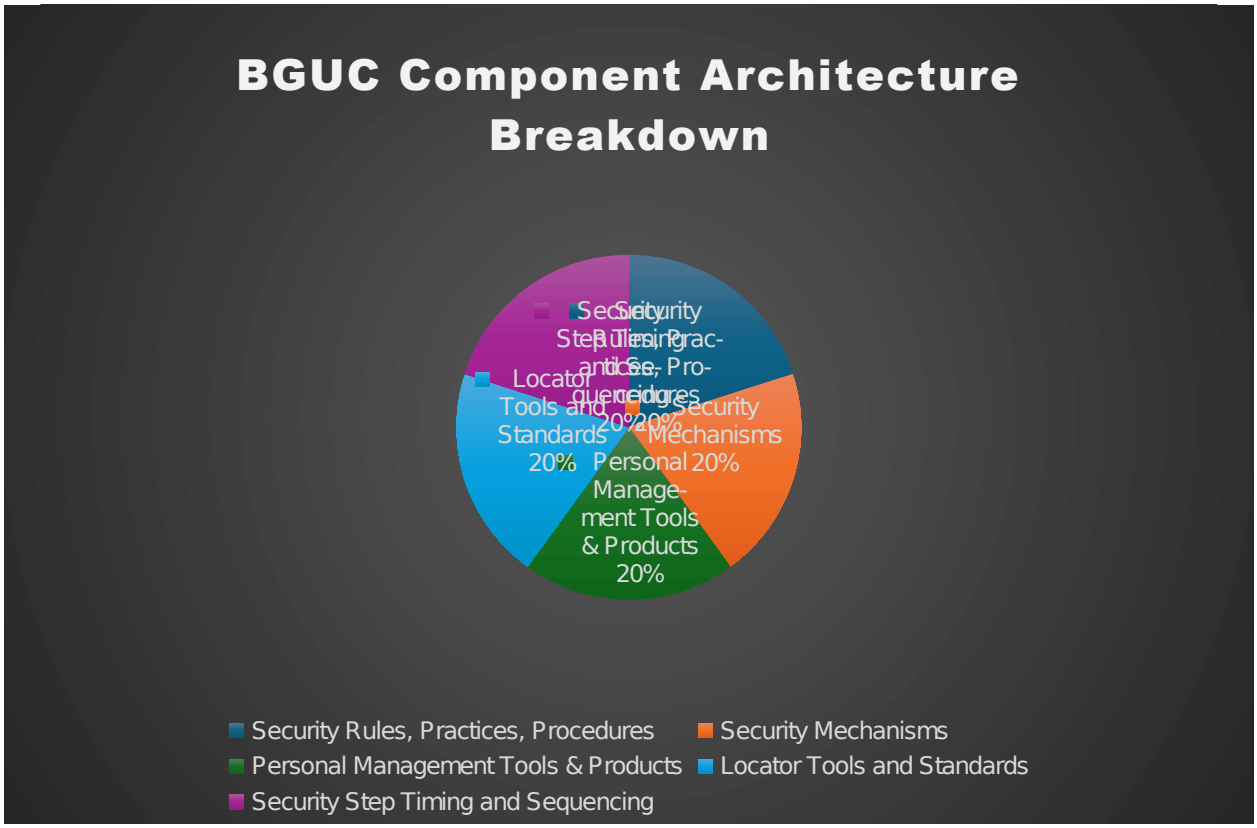
Melanie Thomas, M.S.

April 7, 2025

Blueprint for Modern Component Architecture

Component Architecture Analysis: BGUC Business Scenario

This paper continues the architectural analysis of the Bene Gesserit Urgent Care Offices (BGUC) by detailing the component security architecture. Built upon previous work, including the physical business model, this analysis reflects the technician's or tradesman's view of the system, similar to the role of various specialists during a building's construction. The focus includes data models, security practices, technical mechanisms, personal management tools and products, locator tools and standards, as well as security step sequencing and timing. All these elements are essential for establishing a secure and interoperable healthcare information system (Sherwood, Clark, & Lynas, 2009).



Business Data Model

The BGUC business data model captures and organizes critical organizational data. It encompasses various components essential for the organization's operation. Patient records are a vital component and include personally identifiable information (PII), medical histories, treatment plans, electronic prescriptions, and insurance details. Operational data involves staff schedules, facility information, inventory levels, and details about clinic operations. Billing and insurance data relate to claims processing, payment histories, and communications with payers. Integration logs record system activities and audit trails from electronic health records (EHRs), pharmacies, and insurance providers. Standardization using models such as HL7 and FHIR is vital for ensuring interoperability between internal systems and external partners (Health Level Seven International, n.d.). These standards facilitate accurate, secure, and efficient exchange of information, reduce errors, and support regulatory compliance and advanced data analytics.

Security Rules, Practices, and Procedures

Robust security practices and formal procedures are necessary to safeguard BGUC’s sensitive health and business data. Access control policies, such as role-based access control (RBAC) and attribute-based access control (ABAC), are employed to restrict data access based on specific user roles and attributes. Data handling guidelines define clear procedures for collecting, storing, transmitting, and disposing of sensitive data in compliance with HIPAA and local regulations (U.S. Department of Health and Human Services, 2013). An incident response plan provides a structured and rehearsed approach for identifying, containing, mitigating, and recovering from security breaches. Security awareness training is conducted regularly to educate staff members about various threats, including phishing, ransomware, and social engineering. Finally, audit and compliance monitoring is conducted through scheduled reviews and automated

tools to detect policy breaches or system misconfigurations. Together, these rules and procedures create a risk-aware organizational culture and help maintain the integrity and trustworthiness of the system (NIST, 2018).

Security Mechanisms

The technical tools and platforms that enforce BGUC's security policies are essential to building a resilient infrastructure. Encryption using AES-256 is employed to secure data at rest, while TLS 1.3 protects data in transit. Multi-factor authentication (MFA) is enforced for all privileged access and remote connections to prevent unauthorized access. Endpoint protection mechanisms such as anti-malware software, host-based firewalls, and application safe listing are implemented for both client and server devices. Intrusion detection and prevention systems (IDPS) are used to monitor and block malicious activity based on real-time analysis (NIST, 2018). SIEM tools collect logs centrally, helping to detect threats and respond to incidents proactively. Routine scanning and automated patch deployment ensure that vulnerabilities are addressed promptly, minimizing the risk of exploitation. These mechanisms operate within the SABSA Component Security Architecture layer, contributing to enterprise resilience, data confidentiality, and business continuity (Sherwood et al., 2009).

The BGUC component architecture defines the data structures, procedural policies, and technical defenses required for a secure and functional healthcare IT environment. By adhering to industry standards and security best practices, the organization can facilitate seamless integration and maintain high levels of trust and regulatory compliance (Sherwood et al., 2009).

Personnel Management Tools and Products

In the personnel management tools and products layer, the system begins with identity management. This component handles user profiles, personal information, and credentials. It integrates with external identity providers to enable secure authentication and authorization processes. The authentication mechanism ensures access security through various methods, including passwords, biometrics, and two-factor authentication. All of these methods are linked to an authorization service, which grants access to resources based on the user's identity (Sherwood, Clark, & Lynas, 2009).

Job description management is another key component that creates and maintains detailed job descriptions, including roles, responsibilities, and required qualifications. These descriptions are linked to the role management services, which define user roles within the system, such as Admin, HR, Manager, and Employee. Each role is assigned specific permissions that determine which actions users can take within the system.

The function mapping service associates' roles with specific functions within the system. For example, an Admin role may be granted access to configuration tools, while an employee role is limited to viewing personal information. Additionally, the action permissions system defines the types of actions users can perform, such as creating, reading, updating, or deleting records. Finally, the access control list (ACL) management system provides fine-grained control over resource access. Administrators can define permissions based on user roles, ensuring that only authorized individuals can access sensitive data (Sherwood, Clark, & Lynas, 2009).

Locator Tools and Standards

The locator tools and standards layer are responsible for managing processes, nodes, addresses, and communication protocols. The workflow engine is central to this layer, as it

ensures that processes, such as employee onboarding or performance evaluations, are completed in the correct sequence. The process scheduler manages the timing of HR-related tasks, such as contract renewals and performance reviews, ensuring these tasks are conducted as needed.

The node management service identifies and tracks the computing nodes within the system, including servers and client devices. Each node is assigned a unique identifier, and the system monitors its status to ensure it is operational. The node communication interface facilitates secure data exchanges between these nodes. Alongside this, the address management system allocates and manages IP addresses, ensuring that networked devices are properly located and accessed.

The DNS/service discovery service is critical for resolving domain names to IP addresses, enabling communication between distributed services across the system. The system also employs various communication protocols, including HTTP, HTTPS, and RESTful APIs, to oversee requests and responses between components. These protocols ensure secure data transmission. The protocol handlers interpret and manage the communication, ensuring that data is routed correctly and securely.

Security Step Timing and Sequencing

The security step timing and sequencing layer governs the scheduling of security-related events within the system. The event scheduler is responsible for determining when specific actions should be triggered, such as password expirations or access reviews. The task timing control service ensures that these actions occur at the correct intervals, allowing administrators to configure times for events such as regular security audits.

The global system clock is essential for maintaining synchronization across all components of the system, ensuring that accurate timestamps are applied to logs and security events. The clock sync service ensures consistent time synchronization across all nodes in the system, making certain that logs and actions are properly timestamped.

The security event timers regulate when specific security actions should occur, such as when tokens should expire or when sessions should time out after a period of inactivity. The timeout management service allows administrators to define session limits and specify the maximum time allowed for operations. The security interrupts service manages critical security events, such as unauthorized access attempts, triggering appropriate responses like locking accounts or notifying security personnel (GeeksforGeeks, 2024).

Finally, the system includes an emergency shutdown/lockdown procedure. This procedure is activated in response to serious security breaches, allowing the system to take immediate action to mitigate risks. The BGUC component architecture integrates these components into a unified and secure system. The personnel management layer governs user roles, permissions, and job descriptions, while the locator and communication layer ensure proper management of nodes, addresses, and protocols. The security layer oversees the timing and sequencing of security events, ensuring the system remains secure and compliant with timing policies. Together, these components provide a robust architecture capable of efficiently managing personnel, resources, and security.

References:

GeeksforGeeks. (2024). *Component-Based Architecture - System Design***.** **https://www.geeksforgeeks.org/component-based-architecture-system-design/**

Health Level Seven International. (n.d.). *FHIR Overview.* **https://www.hl7.org/fhir/overview.html**

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity***,** Version 1.1**.** **https://www.nist.gov/cyberframework**

U.S. Department of Health and Human Services. (2013)**.** *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. https://www.hhs.gov/hipaa

Sherwood, J., Clark, A., & Lynas, D. (2009*). Enterprise Security Architecture: A Business-Driven Approach (SABSA White Paper).* The SABSA Institute.