

Security Service Architecture Maturity

Security Service Architecture Maturity

Publication date 2020-11-05

Copyright © 2020

Table of Contents

1. Architecture	1
RABET-V Approach to Architecture	1
Technology Provider Components Description	1
Subsystems	1
Purpose of subsystems	1
Identifying subsystems	1
Components in Subsystem	1
Trust Zone Listing	1
Detailed Diagrams by Subsystem	2
2. Security Services	3
Scoring	3
About Scoring	3
Security Service Components	3
Point of Use Scoring	3
Raw Scores	3
Security Service Component Listing	4
Security Service Matrtix	4
Security Service Listing	5
3. Appendixes	6
Composites	6

List of Figures

1.1. Technology Provider Components Diagram	1
1.2. Components in Subsystem Diagram	1
1.3. Trust Zone Table	2
1.4. AWS Enviornment Diagram	2
2.1. Security Service Components Table	3
2.2. Authentication	3
2.3. Authorization	3
2.4. Boundary Protection	3
2.5. Data Confidentiality and Integrity	4
2.6. Injection Prevention	4
2.7. Logging and Alerting	4
2.8. Secret Management	4
2.9. Session Management	4
2.10. System Availibility	4
2.11. System Integrity	4
2.12. Security Service Matrix Diagram	5
2.13. Security Control Families	5


Chapter 1. Architecture

RABET-V Approach to Architecture

Technology Provider Components Description

The following table describes components that the technology provider has either independently produced or has provided significant value-add to. Components appearing in this table constitute the vendor’s solution space and are targets of security service protection.

Figure 1.1. Technology Provider Components Diagram

#	Name	Documentation
1	 Results Uploader	Provides results upload functionality to localities.

Subsystems

Purpose of subsystems






Many election technology products are complex “system of systems”. These smaller “subsystems” may use different technology stacks that do not interoperate at all levels. This is particularly true of software stacks, where it is understood that a library for Ruby on Rails will not work with one designed for Microsoft ASP.NET MVC.

Identifying subsystems

A subsystem is a grouping of components identified from the threat modeling exercise and other architecture artifacts. If a vendor uses different security services for the same set of users, same trust boundary, and similar use cases, the architecture may be inadequate.

Components in Subsystem

Figure 1.2. Components in Subsystem Diagram


#	Name	Used Security Services	Covered Control Families
1	 Acme Cloud Service	 AWS GuardDuty	 Logging Alerting  System Integrity
2	 Results Uploader		

Trust Zone Listing

Trust Zone Description

The following trust zones were documented during the review. A trust zone is a logical collection of systems that have similar data sensitivity and network controls.

Figure 1.3. Trust Zone Table

#	Name	Documentation
1	 Acme Cloud Service	A cloud environment for the most demanding clients.

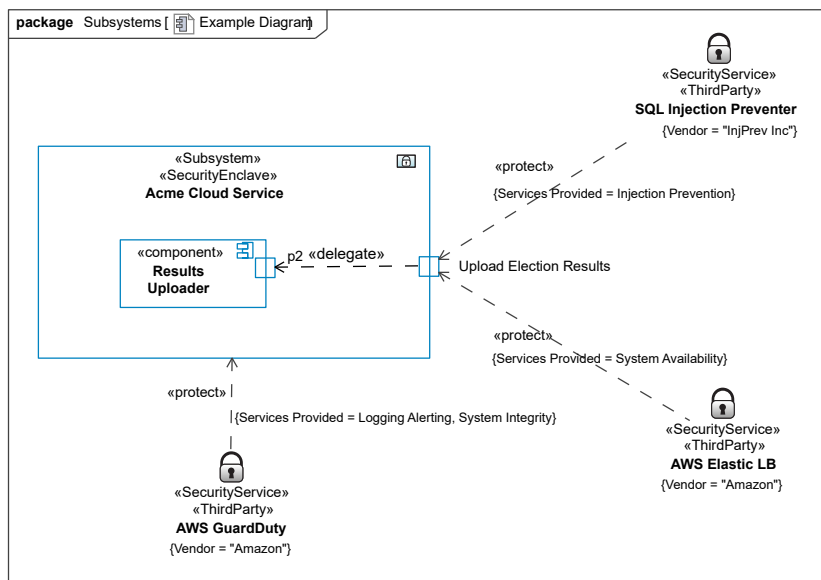
Detailed Diagrams by Subsystem

AWS Enviornment

AWS Enviornment Definition

Example AWS Diagram

Figure 1.4. AWS Enviornment Diagram



Chapter 2. Security Services

Scoring




About Scoring

Scores are given across three to four criteria. Reliability Manageability, Modularity, and Isolation. For composite services, the system modularity and software modularity scores are averaged.

Security Service Components

The following table defines ten security control families that are used throughout RABET-V to help evaluate the products in scope.

Figure 2.1. Security Service Components Table

#	△ Name	Documentation	Vendor
1	 AWS Elastic LB	Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, Lambda functions, and virtual appliances.	Amazon
2	 AWS GuardDuty	Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3.	Amazon
3	 SQL Injection Preventer	Sanitizes queries to prevent SQL Injection	InjPrev Inc

Point of Use Scoring

This following tables display the scores for each security service at their point of use, broken down by security control family.

Raw Scores

Figure 2.2. Authentication

#	Client	Actual Protected	Protected Subsystem	Reliability	Manageability	Modularity	Isolation
---	--------	------------------	---------------------	-------------	---------------	------------	-----------

Figure 2.3. Authorization

#	Client	Actual Protected	Protected Subsystem	Reliability	Manageability	Modularity	Isolation
---	--------	------------------	---------------------	-------------	---------------	------------	-----------

Figure 2.4. Boundary Protection

#	Client	Actual Protected	Protected Subsystem	Reliability	Manageability	Modularity	Isolation
---	--------	------------------	---------------------	-------------	---------------	------------	-----------

Figure 2.5. Data Confidentiality and Integrity

#	Client	Actual Protected	Protected Subsystem	Reliability	Manageability	Modularity	Isolation
---	--------	------------------	---------------------	-------------	---------------	------------	-----------

Figure 2.6. Injection Prevention





#	Client	Actual Protected	Protected Subsystem	Reliability	Manageability	Modularity	Isolation
1	 SQL Injection Preventer	 Results Uploader	 Acme Cloud Service	 2	2	2	2

Figure 2.7. Logging and Alerting




#	Client	Actual Protected	Protected Subsystem	Reliability	Manageability	Modularity	Isolation
1	 AWS GuardDuty		 Acme Cloud Service	 3	2	3	2

Figure 2.8. Secret Management

#	Client	Actual Protected	Protected Subsystem	Reliability	Manageability	Modularity	Isolation
---	--------	------------------	---------------------	-------------	---------------	------------	-----------

Figure 2.9. Session Management

#	Client	Actual Protected	Protected Subsystem	Reliability	Manageability	Modularity	Isolation
---	--------	------------------	---------------------	-------------	---------------	------------	-----------

Figure 2.10. System Availability








#	Client	Actual Protected	Protected Subsystem	Reliability	Manageability	Modularity	Isolation
1	 AWS Elastic LB	 Results Uploader	 Acme Cloud Service	 3	2	3	2

Figure 2.11. System Integrity

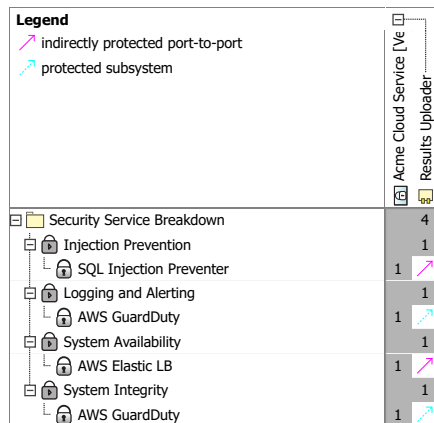
#	Client	Actual Protected	Protected Subsystem	Reliability	Manageability	Modularity	Isolation
1	 AWS GuardDuty		 Acme Cloud Service	 3	2	3	2

Security Service Component Listing

This table shows the score for the reliability measure of the security service. Other measures are contained in Raw Scores section.

Security Service Matrtix











The following matrix describes all the security services used in the product, organized by security control family (rows) and components (columns). Because a single security service may provide mitigations in more than one control family, the same service may appear more than once. The columns are organized by trust zone, then component. The colors in the matrix are used by the RABET-V Team to validate the output, and may be removed in a future iteration.

Figure 2.12. Security Service Matrix Diagram

Security Service Listing

The following diagram shows the identified security services, and the components they protect. The security services are listed as columns under a security control family (e.g. Boundary Protection). If a security service component enforces controls in more than one control family, it will appear under multiple headings. Note: Indirectly protected components are treated the same as directly protected ones.

Figure 2.13. Security Control Families

#	Name	Documentation
1	 Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [NIST FIPS 200]
2	 Authorization	The right or a permission that is granted to a system entity to access a system resource. [NIST SP 800-82 Rev. 2]
3	 Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g. gateways, routers, firewalls, guards, encrypted tunnels). [NIST SP 800-53 Rev. 4]
4	 Data Confidentiality and Integrity	Assurance that the data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. [Adapted from NIST SP 800-33]
5	 Injection Prevention	The sanitization of data input and output (possibly by rejecting unacceptable inputs or outputs) to ensure malicious executable code is not executed.
6	 Logging Alerting	The systemic management and monitoring of the events—the discrete interactions that happen within and between systems, applications, and users—occurring within an organization's systems and networks. [Adapted from NIST SP 800-92]
7	 Secret Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g. passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction. [NIST CNSSI 4009-2015]
8	 System Availability	The property that data or information is accessible and usable upon demand by an authorized person. [NIST SP 800-66 Rev. 1]
9	 System Integrity	The activities based around protecting the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. [NIST SP 800-27 Rev. A]
10	 User Session Management	The act of establishing, protecting, and, when necessary, demolishing the persistent interaction between a subscriber and an end point. [Adapted from NIST SP 1800-17b]

Chapter 3. Appendixes

Composites