Security Requirements (Requirements Phase):

- Focus: Security requirements center on defining the specific security goals and constraints that the software must meet. They address the "what" of security – what level of protection is needed, what types of threats and vulnerabilities must be mitigated, and what security controls are necessary.
- Key Activities:
    - Risk Assessment: Analyzing potential threats and vulnerabilities to the software, along with their potential impact.
    - Security Objectives: Defining the desired security outcomes, such as confidentiality, integrity, availability, and non-repudiation.
    - Regulatory Compliance: Identifying and incorporating relevant security standards and regulations (e.g., HIPAA, GDPR) into the requirements.
    - Threat Modeling: Creating a model that identifies potential threats, attack vectors, and vulnerabilities to guide the design and implementation of security controls.
- Output: A documented set of security requirements that will serve as a guide throughout the development process. These requirements are often expressed as high-level statements, such as "The system must protect sensitive data from unauthorized access" or "The system must be resilient to denial-of-service attacks."

Design Requirements (Design Phase):

- Focus: Design requirements elaborate on the security requirements, detailing the specific technical solutions and strategies that will be implemented to achieve the desired security outcomes. They address the "how" of security – how the system will be designed and built to meet the security requirements.

- Key Activities:
    - Secure Architecture Design: Creating a high-level system architecture that incorporates security principles like defense in depth, least privilege, and secure defaults.
    - Component Design: Designing individual components of the system (e.g., authentication module, data access layer) with security in mind.
    - Security Controls Selection: Choosing specific security controls (e.g., encryption, firewalls, intrusion detection systems) to address identified threats and vulnerabilities.
    - Data Flow Analysis: Mapping how data will flow through the system to identify potential security risks and design appropriate data protection mechanisms.
- Output: Detailed design specifications, diagrams, and models that outline the technical implementation of the security requirements. These design requirements often include specific details about algorithms, protocols, data structures, and security controls.

Key Differences:

Feature	Security Requirements (Requirements Phase)	Design Requirements (Design Phase)
Focus	What level of security is needed? What threats need to be mitigated?	How will the security requirements be implemented in the system design?
Output	High-level security objectives and constraints	Detailed technical specifications for security controls and mechanisms
Activities	Risk assessment, threat modeling, regulatory compliance	Secure architecture design, component design, security controls selection, data flow analysis
Examples	"The system must protect sensitive data from unauthorized access." "The system must be resilient to DDoS attacks."	"Use AES-256 encryption for data at rest." "Implement a web application firewall to protect against web attacks."

Relationship:

Security requirements and design requirements are closely intertwined. Security requirements provide the foundation for the design process, while design requirements translate those security goals into concrete technical solutions. Design requirements must be traceable back to the security requirements to ensure that the design effectively addresses the identified security risks.