Common Attack Pattern Enumeration and Classification (CAPEC™) Schema Description Version 2.5

Schema Element Name	Description	Usage	Completeness			Abstraction		
			Hook	Stub	Complete	Meta	Standard	Detailed
Attack Pattern	This element represents an attack pattern.							
Description	This element represents a detailed description of an attack pattern. Content may include a summary and a list of steps taken by the attacker.	This element can be used to capture a range of descriptive information. Comprehensive descriptions might include attack trees, exploit graphs, etc., to more clearly elaborate this type of attack.		R	R	R	R	R
Summary	This element provides a summary description of the attack that includes the attack target and sequence of steps.			R	R	R	R	R
Attack_Execution_Flow	This element lists the steps typically performed by an attacker when executing the attack.							

Alternate_Terms	This element contains one or more alternative terms used to identify the attack pattern.							
Target_Attack_Surface	This element characterizes the locations where an attacker interacts with the target system.							
Attack _Prerequisites	This element represents a container of one or more attack prerequisites. An attack prerequisite is a condition that must exist in order for an attack of this type to succeed.				R	S	S	S
Attack_Prerequsite	An attack prerequisite is a condition that must exist in order for an attack of this type to succeed.			R	R	S	S	S
Typical_Severity	This element reflects the typical severity of an attack on a scale of {Very Low, Low, Medium, High, Very High}.	This element is used to capture an overall typical average value for this type of attack with the understanding that it will not be completely accurate for all attacks.		R	R	O	R	R

Typical_Likelihood_of_Exploit	This element represents the typical likelihood that the attack will succeed, and provides a likelihood estimate and an explanation that qualifies the estimate.	This element is used to capture an overall typical average value for this type of attack with the understanding that it will not be completely accurate for all attacks.		R	R	O	R	R
Likelihood	This element reflect the likelihood of attack success on a scale of {Very Low, Low, Medium, High, Very High}, in consideration of the attack prerequisites, targeted weakness, attack surface, skills and resources required, as well as effectiveness of likely implemented blocking solutions.			R	R	O	R	R
Explanation	This element provides qualifications or assumptions regarding the estimated likelihood.					O	R	R
Methods_of_Attack	This element represents a container of one or more methods of attack. Method of attack is enumerated list of defined vectors that identify the underlying			R	R	R	R	R

	mechanism(s) used in the attack.							
Method_of_Attack	Method of attack is enumerated list of defined vectors that identify the underlying mechanism(s) used in the attack.	This element is represented as an enumerated list to facilitate normalization and classification of attack patterns, and to help define the applicable attack surface required for this attack.		R	R	R	R	R
Examples-Instances	This element represents a container of one or more example instances. An example instance details an explanatory example or demonstrative exploit instance of this attack,	This element is used to help the reader understand the nature, context and variability of the attack in more practical and concrete terms.				O	S	R
Example-Instance	This element represents an exploit description and may also provide an external reference and/or a range of related vulnerabilities.					O	S	R
Example-Instance_Description	This element describes in detail a specific example or exploit instance of this attack pattern.	This element is used to define the context of an attack, targeted weaknesses or vulnerabilities, the				O	S	R

		sequence of attack steps, and the resulting impact of attack success or failure.						
References	This element provides a reference to external documentation detailing the individual example or exploit instance.					O	S	R
Example-Instance_Related_Vulnerabilities	This element represents a container of one or more instance related vulnerabilities. An instance-related vulnerability identifies vulnerabilities targeted by this exploit instance of the attack.					O	S	R
Example-Instance_Related_Vulnerabiltity	This element identifies specific vulnerabilities targeted by this exploit instance of the attack.	This element is used to reference industry-standard identifiers such as Common Vulnerabilities and Exposures (CVE®) numbers and/or US-CERT numbers.				O	S	R
Attacker_Skills_or_Knowledge_Required	This element represents a container of one or more attacker skill or knowledge required. Attacker skill or knowledge required describes the level of skills			R	R	S	S	R

	or specific knowledge needed by an attacker to execute this type of attack.							
Attacker_Skill_or_Knowledge_Required	Attacker skill or knowledge required describes the level of skills or specific knowledge needed by an attacker to execute this type of attack.			R	R	S	S	R
Skill_or_Knowledge_Level	This element reflects the level of knowledge or skill required to execute this type of attack on a scale of {Low, Medium, High}.	This element is used to represent the level with respect to a specified type of skill or knowledge, e.g., low - basic SQL knowledge, high - expert knowledge of LINUX kernel, etc.		R	R	S	S	R
Skill_or_Knowledge_Type	This element details the skill or knowledge required.			R	R	S	S	R
Resources_Required	This element describes the resources (CPU cycles, IP addresses, tools, etc.) required by an attacker to effectively execute this type of attack.					S	S	R

Probing_Techniques	This element represents a container of one or more probing techniques. A probing technique describes a method used to probe and reconnoiter a potential target to determine vulnerability and/or to prepare for this type of attack.							
Probing_Technique	A probing technique describes a method used to probe and reconnoiter a potential target to determine vulnerability and/or to prepare for this type of attack.							
Description	This element provides an explanatory description of the probing technique.							
Observables	This element specifies detailed cyber observable patterns for potential detection of the probing technique activity.							
Indicators-Warning_of_Attack	This element represents a container of one or more indicator warning of attack. Indicator warning of attack describes activities, events, conditions or behaviors that may indicate that an attack of this type is imminent, in							

	progress or has occurred.							
Indicator-Warning_of_Attack	Indicator warning of attack describes activities, events, conditions or behaviors that may indicate that an attack of this type is imminent, in progress or has occurred.							
Description	This element provides an explanatory description of the indicator warning of attack.							
Observables	This element specifies detailed cyber observable patterns for potential detection of the indicator warning of attack.							
Obfuscation_Techniques	This element represents a container of one or more obfuscation techniques. An obfuscation technique can be used to disguise the fact that an attack of this type is imminent, in progress or has occurred.							
Obfuscation_Technique	An obfuscation technique can be used to disguise the fact that an attack of this type is imminent, in progress or has occurred.							
Description	This element provides an explanatory description of							

	the obfuscation technique.							
Observables	This element specifies detailed cyber observable patterns for potential detection of the obfuscation technique.							
Solutions_and_Mitigations	This element represents a container of one or more solutions or mitigations. A solution or mitigation describes actions or approaches to prevent or mitigate the risk of this attack by improving the resilience of the target system, reduce its attack surface or to reduce the impact of the attack if it is successful.			R	R	R	R	R
Solution_or_Mitigation	A solution or mitigation describes actions or approaches to prevent or mitigate the risk of this attack by improving the resilience of the target system, reduce its attack surface or to reduce the impact of the attack if it is successful.			R	R	R	R	R

Attack_Motivation-Consequences	This element represents a container of one or more attack motivation consequences. Attack motivation consequence represents the desired technical results that could be achieved/leveraged by this attack pattern, represented as an enumerated list of defined adversary motivations/ consequences.	This element is used to identify specific technical results that could be leveraged to achieve the adversary's business or mission objective. This information is useful for aligning attack patterns to threat models and for determining which attack patterns are relevant for a given context.				R	R	R
Attack_Motivation-Consequence	Attack motivation consequence represents the desired technical results that could be achieved/ leveraged by this attack pattern, represented as an enumerated list of defined adversary motivations/ consequences.					R	R	R
Injection_Vector	This element details the mechanism and format of an input-driven attack of this type. Injection vectors take into account the grammar of an attack, the syntax accepted by the					O	S	S

	system, the position of various fields, and the ranges of data that are acceptable.							
Payload	This element describes the code, configuration or other data to be executed or otherwise activated as part of an injection-based attack of this type.					O	S	S
Activation_Zone	This element describes the area within the target software that is capable of executing or otherwise activating the payload of an injection-based attack of this type. The activation zone is where the intent of the attacker is put into action. The activation zone may be a command interpreter, some active machine code in a buffer, a client browser, a system API call, etc.					O	S	S
Payload_Activation_Impact	This element describes the impact that the activation of the attack payload for an injection-based attack of this type would typically have on the confidentiality, integrity or availability of the target software.					O	S	S

Description	This element provides an explanatory description of the payload activation impact.							
Observables	This element specifies detailed cyber observable patterns for potential detection of the payload activation impact.							
Related_Weaknesses	This element represents a container of one or more related weaknesses. Related weaknesses refer to software weaknesses potentially targeted for exploit by this attack pattern.	This element is used to reference industry standard Common Weakness Enumeration (CWE™) data, including weaknesses that are exploited by the attack as well as weaknesses whose presence increases the likelihood or impact of the attack.	R	R	R	S	R	R
Related_Weakness	Related weaknesses refer to software weaknesses potentially targeted for exploit by this attack pattern.		R	R	R	S	R	R

CWE_ID	The element contains the Common Weakness Enumeration (CWE™) ID of the exploited software weakness.		R	R	R	S	R	R
Weakness_Relationship_Type	This element describes the nature of the relationship between the attack pattern and the software weakness, represented as the enumerated list {Targeted, Secondary}.	This element is used to indicate whether the weakness is targeted or secondary. If the attack is designed to exploit the weakness, then that weakness is Targeted. A weakness whose presence may increase the likelihood of the attack succeeding or the impact of the attack if it does succeed is Secondary.	R	R	R	S	R	R
Related_Vulnerabilities	This element represents a container of one or more related vulnerabilities. A related vulnerability refers to a specific instance vulnerability targeted for exploit by this attack pattern.	This element is used to identify specific vulnerabilities by their industry-standard Common Vulnerabilities and Exposures (CVE®) numbers and/or				S	R	R

		US-CERT numbers. As vulnerabilities are much more specific and localized than weaknesses, it is uncommon that an attack pattern would target a specific vulnerability. This would most likely occur if the attack pattern were targeting vulnerabilities in the underlying platform, framework, or software library.						
Related_Vulnerability	This element represents a specific instance vulnerability targeted for exploit by this attack pattern.					S	R	R
Vulnerability_ID	The element contains the Common Vulnerabilities and Exposures (CVE®) or US-CERT number identifying the vulnerability.					S	R	R
Vulnerability_Description	This element contains a short textual description of the specific related vulnerability taken from the					S	R	R

	industry standard vulnerability listing.							
Related_Attack_Patterns	This element represents a container of one or more related attack patterns. A related attack pattern refers to an attack pattern that is dependent on or applied in conjunction with this attack pattern.			R	R	S	S	S
Related_Attack_Pattern	A related attack pattern refers to an attack pattern that is dependent on or applied in conjunction with this attack pattern.			R		S	S	S
Relevant_Security_Requirements	This element represents a container of one or more relevant security requirements. A relevant security requirement is a general security requirement that is relevant to this type of attack.					S	S	S
Relevant_Security_Requirement	A relevant security requirement is a general security requirement that is relevant to this type of attack.					S	S	S

Relevant_Design_Patterns	This element represents a container of one or more relevant design patterns. Relevant design patterns include both recommended design patterns, which increase the software's resistance or resilience to this type of attack, and non-recommended design patterns, which could leave the system especially susceptible to this type of attack.					S	S	S
Recommended_Design_Patterns	This element represents a container of one or more recommended design patterns. A recommended design pattern increases the software's resistance or resilience to this type of attack.							
Recommended_Design_Pattern	A design pattern that is likely to increase the software’s resistance or resiliency to this type of attack.							
Non-Recommended_Design_Patterns	This element represents a container of one or more non-recommended design patterns. A non-recommended design can decrease a sofware's							

	resistance or resilience to this type of attack, leaving the system more susceptible.							
Non-Recommended_Design_Pattern	A non-recommended design can decrease a sofware's resistance or resilience to this type of attack, leaving the system more susceptible.							
Relevant_Security_Patterns	This element represents a container of one or more relevant security patterns. A relevant security pattern provides resistance or resilience to this type of attack.					S	S	S
Relevant_Security_Pattern	A relevant security pattern provides resistance or resilience to this type of attack.					S	S	S
Related_Security_Principles	This element represents a container of one or more related security principles. A principle is defined as a rule or standard for good behavior. A related security principle is a security rule or practice that impedes this attack pattern.	Usage defined in NIST Special Publication 800-27 Rev A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.				S	S	S

Related_Security_Principles	A related security principle is a security rule or practice that impedes this attack pattern.					S	S	S
Related_Guidelines	This element represents a container of one or more related guidelines. A related guideline represents a security guideline that is relevant to identifying or mitigating this type of attack.	It would be helpful to provide a usage reference. However links to security principle and guideline documentation on the BSI site appear to be broken. NIST Special Publication 800-27 Rev A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A uses the terms principle and guideline interchangeably.				S	S	S
Related_Guidelines	A related guideline represents a security guideline that is relevant to identifying or mitigating this type of attack.					S	S	S
Purposes	This element represents a container of one or more	This element is used to capture						

	purposes. Purpose refers to the intended purpose behind the attack pattern relative to an enumerated list of attack objectives.	pattern composibility and assist with normalization and classification of attack patterns within the CAPEC catalog.						
Purpose	Purpose refers to the intended purpose behind the attack pattern relative to an enumerated list of attack objectives.	This element is represented as an enumerated list to facilitate normalization and classification of attack patterns.						
CIA_Impact	This element characterizes the typical relative impact of this pattern on the confidentiality, integrity, and availability of the targeted software.							
Confidentiality_Impact	This element describes the typical impact of this pattern on the confidentiality characteristics of the targeted software and related data.							
Integrity_Impact	This element describes the typical impact of this pattern on the integrity characteristics of the targeted software and							

	related data.							
Availability_Impact	This element describes the typical impact of this pattern on the availability characteristics of the targeted software and related data.							
Technical _Context	This element characterizes the technical context where this pattern is applicable.							
Architectural_Paradigms	This element represents a container of one or more architectural paradigms in which this attack pattern is possible and relevant. Architectural paradigm characterizes the target using an enumerated list of paradigms utilized by the target.							
Architectural_Paradigm	Architectural paradigm characterizes the target using an enumerated list of supported paradigms in which this attack pattern is possible and relevant.	This element is represented as an enumerated list to facilitate normalization and classification of attack patterns.						
Frameworks	This element represents a container of one or more frameworks in which this attack pattern is possible and relevant. Frameworks							

	characterizes the target using an enumerated list of frameworks utilized by the target.							
Framework	Framework characterizes the target using an enumerated list of supported frameworks in which this attack pattern is possible and relevant.	This element is represented as an enumerated list to facilitate normalization and classification of attack patterns.						
Platforms	This element represents a container of one or more platforms in which this attack pattern is possible and relevant. Platforms characterizes the target using an enumerated list of platforms utilized by the target.							
Platform	Platform characterizes the target using an enumerated list of supported platforms in which this attack pattern is possible and relevant.	This element is represented as an enumerated list to facilitate normalization and classification of attack patterns.						
Languages	This element represents a container of one or more languages in which this attack pattern is possible and relevant. Languages characterizes the target							

	using an enumerated list of languages utilized by the target.							
Language	Language characterizes the target using an enumerated list of implementation languages in which this attack pattern is possible and relevant.	This element is represented as an enumerated list to facilitate normalization and classification of attack patterns.						
Keywords	This element represents a container of one or more keywords. Keywords correspond to text strings used to tag and search CAPEC catalog data.							
Keyword	Keyword corresponds to text strings used to tag and search CAPEC catalog data.							
References	This element represents a container of one or more references. Reference represents a documentary resource used to develop the definition of this attack pattern.			R	R	S	S	S
Reference	Reference represents a documentary resource used to develop the definition of this attack pattern.			R	R	S	S	S