Rating: Very high = VH, High = H, Medium = M, Low = L, Very low = VL, no data = n/a

CAPEC – ATT&CK Related Patterns https://capec.mitre.org/data/definitions/658.html

Group	Attack	Skill level	Likeliness of Attack	Typical Severity	STRIDE	Target	Currently Applicable	Notes
Subvert Access Control								
	1. Accessing Functionality Not Properly Constrained by ACLs	L	H	H	T, I, E	web application	No	
16.95%	13. Subverting Environment Variable Values	L, H	VH	VH	R, I, E	OS	Yes	
	17. Using Malicious Files	L	H	VH	S, T, I, E	LAN	Yes	
	21. Expolitation of Trusted Identifiers	L	H	H	T, I, E	web application	No	
	30. Hijacking a Privileged Thread of Execution	H	L	VH	I, E	OS	Yes	
	31. Accessing/Intercepting/Modifying HTTP Cookies	L, H	H	H	S, T, I, E	web application	No	
	60. Reusing Session IDs (aka Session Replay)	L, M	H	H	S, I, E	web application	No	
	68. Subvert Code-signing Facilities	H	L	VH	E	web application	Yes	Use of an old web browser can lead to this attack
	94. Adversary in the Middle (AiTM)	M	H	VH	T, I, E	web application	No	
	114. Authentication Abuse	n/a	n/a	M	E	OS, web app, software	Yes	
	115. Authentication Bias	n/a	n/a	M	E	OS, web app, software	Yes	
	122. Privilege Abuse	L	H	M	I, E	OS, web app, LAN	Yes	
	177. Create files with the same name as files protected with a higher classification	n/a	n/a	VH	T, I, E	OS application	Yes	
	180. Exploiting Incorrectly Configured Access control Security Levels	L	H	M	T, I, E	OS, WAN, LAN	Yes	
	196. Session Credential Falsification Through Forging	M	M	M	T, I, E	web application	No	
	233. Privilege Escalation	n/a	n/a	n/a	E	OS, web application	Yes	
	480. Escaping Virtualization	n/a	L	VH	T, E	OS, web application	No	Current system does not use virtualization software
	509. Kerberoasting	M	n/a	H	I, E	OS	Yes	Windows
	555. Remote Services with Stolen Credentials	n/a	n/a	VH	E	WAN	No	System does not use RSP/RDS
	560. Use of Known Domain Credentials	L	H	H	E	OS	Yes	
	561. Windows Admin Shares with Stolen Credentials	L	n/a	n/a	E	OS	Yes	
	562. Modify Shared File	n/a	n/a	n/a	T	OS	Yes	
	593. Session Hijacking	L	H	VH	I, E	web application	No	Check with team on this one
	600. Credential Stuffing	L	H	H	E	OS, web app, OS app	Yes	
	642. Replace Binaries	n/a	n/a	H	T	OS	Yes	
	644. Use of Captured Hashes (Pass the Hash)	L	M	H	E	OS, LAN	Yes	
	645. Use of Captured Tickets (Pass the Ticket)	L, H	L	H	E	OS	Yes	
	650. Upload a Web Shell to a Web Server	n/a	n/a	H	T, I, E	WAN	No	Web server not currently utilized
	652. Use of Known Kerberos Credentials	L	M	H	S, T, I, E	OS	Yes	
	668. Key Negotiation of Bluetooth Attack (KNOB)	M	L	H	T, I, E	Bluetooth	No	Network does not use Bluetooth to communicate
Abuse Existing Functionality								
	2. Inducing Account Logout	L	H	M	D	web application	No	
9.04%	125. Flooding	n/a	H	M	D	WAN, LAN	Yes	
	130. Excessive Allocation	n/a	M	M	D	WAN, LAN	Yes	
	131. Resource Leak Exposure	n/a	M	M	D	WAN, LAN	Yes	
	227. Sustained Client Engagement	n/a	n/a	n/a	D	WAN, LAN, web app	Yes	
	464. Evercookie	n/a	n/a	M	T	browser	Yes	
	465. Transparent Proxy Abuse	M	n/a	M	I	browser	Yes	
	469. HTTP DoS	n/a	n/a	L	D	web application	No	
	482. TCP Flood	n/a	n/a	n/a	D	WAN	No	
	488. HTTP Flood	n/a	n/a	n/a	D	WAN	No	
	489. SSL Flood	n/a	n/a	n/a	D	WAN	No	
	490. Amplification	n/a	n/a	m	D	WAN	No	
	528. XML Flood	L	L	M	D	WAN	No	
	620. Drop Encryption Level	n/a	n/a	H	T	Data	Yes	Check with team on this one
	665. Exploitation of Thunderbolt Protection Flaws	H	L	VH	T, I, E	OS	Yes	
	666. BlueSmacking	L	M	M	D	Bluetooth	Yes	Check with team on this one
Manipulate System Resources								
	11. Cause Web Server Misclassification	L, M	M	H	I, E	WAN	No	
27.12%	35. Leverage Executable Code in Non-Executable Files	L	H	VH	T, E	OS, web application	Yes	Would need to be at the file-level, a malicious email attachment
	141. Cache Poisoning	M	H	H	T	WAN, web application	No	
	142. DNS Cache Poisoning	M	H	H	S, I	WAN, web application	No	
	165. File Manipulation	n/a	n/a	M	T, I	OS	Yes	
	186. Malicious Software Update	H	n/a	H	S, T	OS	Yes	supply chain risks: sustainment
	187. malicious Automated Software Update via Redirection	H	H	H	T	WAN	No	supply chain risks: sustainment
	203. Manipulate Registry Information	H	n/a	M	T, I	OS, web application	Yes	
	206. Signing malicious Code	n/a	n/a	VH	S, T, R, I, E	OS, software	Yes	supply chain risks: development and production, sustainment
	268. Audit Log Manipulation	n/a	n/a	n/a	T	OS	Yes	Currently no audit system in place for a log file
	270. Modification of Registry Run Keys	n/a	M	M	T, E	OS	Yes	
	438. Modification During Manufacture	n/a	n/a	n/a	T	hardware	Yes	supply chain risks:
	439. Manipulation During Distribution	n/a	n/a	n/a	T	hardware	Yes	supply chain risks: distribution
	440. Hardware Integrity Attack	n/a	L	H	T	hardware	Yes	supply chain risks: sustainment
	442. Infected Software	n/a	M	H	T	OS, software	Yes	supply chain risks: sustainment
	443. Malicious Logic Inserted Into Product by Authorized Developer	n/a	M	H	T	Software	Yes	supply chain risks: development and production, sustainment
	445. Malicious Logic Insertion into Product Software via Configuration Manageme	n/a	M	H	T	Software	Yes	supply chain risks: development and production, sustainment
	446. Malicious Logic Insertion into product via Inclusion of Third-Party Componer	n/a	M	H	T	Software	No	Meant for supply chain infrastructure; supply chain risks: development and production, sustainment
	457. USB Memory Attacks	n/a	L	H	T, I	OS, software	Yes	Would require insider access; supply chain risks: sustainment
	478. Modification of Windows Service Configuration	n/a	L	H	T	OS	Yes	
	481. Contradictory Destinations in Traffic Routing Schemes	M	M	H	T, I	WAN	No	
	511. Infiltration of Software Development Environment	M, H	L	H	T	OS, IDE	Yes	supply chain risks: development and production, sustainment
	516. Hardware Component Substitution During Baselining	M, H	L	H	T	hardware	Yes	supply chain risks: development and production, sustainment
	520. Counterfeit Hardware Component During Product Assembly	H	L	H	T	hardware	No	Current system does not appear to have a firewall, supply chain risks: development and production
	522. Malicious Hardware Component Replacement	H	L	H	T	hardware	No	Current system not advanced enough; supply chain risks: distribution
	523. Malicious Software Implanted	H	L	H	T	software, web application	No	Current system does not have a dedicated supply chain system, supply chain risks: distribution
	531. Hardware Component Substitution	H	L	H	T	hardware	Yes	supply chain risks: sustainment
	532. Altered Installed BIOS	H	L	H	T	OS	Yes	supply chain risks: development and production, sustainment
	537. Infiltration of Hardware Development Environment	M, H	L	H	T	hardware	No	supply chain risks: development and production, sustainment
	538. Open-Source Library Manipulation	H	L	H	T	software	Yes	If in utilized software, supply chain risks: development and production, sustainment
	539. ASIC With Malicious Functionality	H	L	H	T	software	No	supply chain risks: development and production, sustainment
	571. Block Logging to Central Repository	n/a	n/a	L	T	OS	Yes	
	572. Artificially Inflate File Sizes	n/a	H	M	T, D	OS	Yes	
	578. Disable Security Software	n/a	M	H	T	Software	Yes	
	635. Alternative Execution Due to Deceptive Filenames	n/a	n/a	H	T, I, E	web application	No	Check with team on this one
	636. Hiding Malicious Data or Code Within Files	n/a	n/a	H	T	OS	Yes	
	638. Altered Component Firmware	L, M, H	L	VH	T	OS	Yes	
	649. Adding a Space to a File Extension	n/a	L	M	T	OS, software, web app	Yes	
	655. Avoid Security Tool Identification by Adding Data	n/a	H	H	T	OS, software, web app	Yes	
	657. Malicious Automated Software Update via Spoofing	n/a	H	H	S, T	Software	Yes	supply chain risks: sustainment
	669. Alteration of a Software Update	H	M	H	T, I, E	software	Yes	supply chain risks: sustainment
	670. Software Development Tools Maliciously Altered	H	L	H	T, I, E	software, IDE	No	supply chain risks: development and production, sustainment
	671. Requirements for ASIC Functionality Maliciously Altered	H	L	H	T	hardware	No	application specific, supply chain risks: design
	672. Malicious Code Implanted During Chip Programming	M	L	H	T	hardware	Yes	supply chain risks: development and production
	673. Developer Signing Malicious Altered Software	H	M	H	T, I, E	software	Yes	supply chain risks: development and production, sustainment
	674. Design for FPGA Malicious Altered	H	L	H	T	hardware	No	supply chain risks: design
	677. Server Functionality Compromise	n/a	L	H	T	hardware	Yes	supply chain risks: sustainment
	678. System Build Data Maliciously Altered	n/a	L	H	T, I, E	software	Yes	supply chain risks: development and production, sustainment
Inject Unexpected Items								
	19. Embedding Scripts within Scripts	L, M	H	H	T, E	web application	No	
7.91%	251. Local Code Inclusion	n/a	n/a	M	T	web application	No	
	542. Targeted Malware	n/a	n/a	n/a	T, I, E	OS	Yes	
	550. Install New Service	n/a	n/a	n/a	T, E	OS	Yes	
	551. Modify Existing Service	n/a	n/a	n/a	T	OS	Yes	
	552. Install Rootkit	n/a	M	H	T, E	OS	Yes	
	556. Replace File Extension Handlers	n/a	n/a	n/a	T, I	OS, software	Yes	
	558. Replace Trusted Executable	n/a	L	H	T, E	OS	Yes	
	564. Run Software at Logon	n/a	n/a	n/a	T, E	OS	Yes	
	579. Replace Winlogon Helper DLL	n/a	n/a	n/a	T	OS	Yes	
	640. Inclusion of Code in Existing Process	H	L	H	T, E	OS	Yes	
	660. Root/Jailbreak Detection Evasion via Hooking	M, H	M	VH	T, I, E	mobile	Yes	Could spread to PCs?
	662. Adversary in the Browser (AiTB)	M	H	VH	T, I, E	mobile	Yes	Could spread to PCs?
	698. Install Malicious Extension	M	M	H	S, T, I, E	software	Yes	If software can have 3rd party plugins
Manipulate Timing and State								
0.56%	25. Forced Deadlock	M	L	H	D	software	Yes	
Collect & Analyze Information								
	31. Accessing/Intercepting/Modifying HTTP Cookies	L, H	H	H	S, T, I	web application, WAN	No	
22.60%	37. Retrieve Embedded Sensitive Data	M	H	VH	I	software, hardware	Yes	
	57. Utilizing REST's Trust in the System Resource to Obtain Sensitive Data	L	M	VH	I, E	web application	No	
	65. Sniff Application Code	M	L	H	I	software, LAN, WAN	Yes	Network sniffing
	127. Directory Indexing	L, H	H	M	I	OS, software	Yes	
	150. Collect Data from Common Resource Locations	n/a	n/a	M	I	OS	Yes	
	158. Sniffing Network Traffic	L	n/a	M	I	WAN, LAN?	Yes	Check with team on this one
	169. Footprinting	L	H	VL	I	OS, WAN, LAN, software	Yes	
	191. Read Sensitive constants within an Executable	n/a	n/a	L	I	software, web application	Yes	Can get a hard-code password
	204. Lifting Sensitive Data Embedded in Cache	n/a	n/a	M	I	browser	Yes	
	292. Host Discovery	n/a	n/a	L	I	WAN, LAN	Yes	
	295. Timestamp Request	n/a	n/a	L	I	OS, WAN, LAN?	Yes	
	300. Port Scanning	n/a	n/a	L	I	WAN, LAN	Yes	
	309. Network Topology Mapping	n/a	n/a	L	I	WAN, LAN	Yes	
	312. Active OS Fingerprinting	n/a	M	L	I	OS	Yes	
	313. Passive OS Fingerprinting	n/a	H	L	I	OS	Yes	
	383. Harvesting Information via API Event Monitoring	n/a	n/a	L	T, I	OS, web application	Yes	Check with team on this one
	407. Pretexting	L	M	L	S, I	Personnel	Yes	
	497. File Discovery	n/a	H	VL	I	OS, WAN, LAN, web app	Yes	
	541. Application Fingerprinting	n/a	n/a	L	I	web application	No	
	545. Pull Data from System Resources	n/a	n/a	n/a	I, E	OS	Yes	
	568. Capture Credentials via Keylogger	n/a	n/a	H	I, E	OS	Yes	
	569. Collect Data as Provided by Users	n/a	n/a	n/a	I	OS, web application	Yes	
	573. Process Footprinting	n/a	L	L	I	OS, software, web app	Yes	
	574. Services Footprinting	n/a	L	L	I	OS, software, web app	Yes	
	575. Account Footprinting	n/a	L	L	I	OS, software, web app	Yes	
	576. Group Permission Footprinting	n/a	L	L	I	OS, software, web app	Yes	
	577. Owner Footprinting	n/a	L	L	I	OS, software, web app	Yes	
	580. System Footprinting	L	L	L	I	OS, software, web app	Yes	
	581. Security Software Footprinting	n/a	n/a	n/a	I	OS, software, web app	Yes	
	609. Cellular Traffic Intercept	M	n/a	L	I	mobile	No	
	634. Probe Audio and Video Peripherals	H	L	H	I	mobile, OS, hardware	No	Computers not used for A/V communication
	637. Collect Data from Clipboard	H	L	L	I	OS	Yes	
	639. Probe System Files	n/a	n/a	M	I	OS, software, web app	Yes	
	643. Identify Shared Files/Directories on System	L	M	M	I	OS, LAN	Yes	
	646. Peripheral Footprinting	M	L	M	I	OS, LAN	Yes	
	647. Collect Data from Registries	L	M	M	I	OS	Yes	
	651. Eavesdropping	n/a	n/a	M	I	Personnel	Yes	Employee training may be the solution here.
	675. Retrieve Data from Decommissioned Devices	M, H	M	M	I	Hardware, OS, software	No	Supply chain risks: disposal, No decommissioned devices mentioned
	694. System Location Discovery	L	H	VL	I	OS	Yes	
Engage in Deceptive Interactions								
	38. Leveraging/Manipulating Configuration File Search	L	H	VH	T, E	OS	Yes	
11.86%	98 Phishing	M	H	VH	S, I	Personnel	Yes	
	132. Symlink Attack	L, H	L	H	T, I, E	OS	Yes	
	148. Content Spoofing	n/a	M	M	S, T, I	web application	No	
	159. Redirect Access to Libraries	L, M, H	H	VH	T, E	OS, web application	Yes	
	163. Spear Phishing	M	H	H	S, I	Personnel	Yes	
	383: Harvesting Information via API Event Monitoring	n/a	n/a	L	T, I	OS, web application	Yes	
	407. Pretexting	L	M	L	S, I	Personnel	Yes	
	471. Search Order Hijacking	M	n/a	M	T,	OS, web application	Yes	
	473. Signature Spoof	H	n/a	n/a	S, T,	OS, cryptography	No	OS does not appear to be dependent on a cryptographic signature-based verification system, check with team on this one
	474. Signature Spoofing by Key Theft	L, H	M	H	S, T,	Personnel, cryptography	No	OS does not appear to be dependent on a cryptographic signature-based system
	479. Malicious Root Certificate	n/a	L	L	T	OS, browser, web applica	Yes	
	485. Signature Spoofing by Key Recreation	H	L	H	S, T,	Personnel, cryptography	No	Os does not appear to be dependent on a cryptographic signature-based system
	504. Task Impersonation	L	M	H	S, I, E	OS	Yes	
	543. Counterfeit Websites	n/a	n/a	H	S, T, I	Personnel, web applicatio	Yes	
	616. Establish Rogue Location	L	M	M	T, I	Personnel, web applicatio	Yes	
	633. Token Impersonation	n/a	n/a	M	T	web application	No	Not possible on transaction software?
	641. DLL Side-Loading	H	L	H	T	OS	Yes	
	654. Credential Prompt Impersonation	L	M	H	S, I, E	OS, software	Yes	Can be used on an email server
	695. Repo Jacking	L	M	H	T, I, E	OS, software	No	Required: owner changed/deleted account recently
	697. DHCP Spoofing	M	L	H	S, T, I	LAN	Yes	Network: local
Employ Probabilistic Techniques								
	49. Password Brute Forcing	L	M	H	I, E	OS, software, web app	Yes	
2.82%	55. Rainbow Table Password Cracking	L	M	M	I, E	database	No	
	70. Try Common or Default Usernames and Passwords	L	M	H	I, E	OS, software, web app	Yes	
	112. Brute Force	L	n/a	H	I, E	OS, software, web app	Yes	Not likely, though possible
	565. Password Spraying	L	H	H	I, E	OS, software, web app	Yes	Not likely, though possible
Manipulate Data Structures								
0.56%	267. Leverage Alternate Encoding	L, M	H	H	T, I, E	web application	No	
Other								
0.56%	691. Spoof Open-Source Software Metadata	M	M	H	S, T, R, I, E	software	Yes	Depends on what software is used on device
100.00%		0	0	20	23	web application		
		38	35	75	97	29.94%	128	-- Yes
		32	36	36	36	OS	49	-- No
		47	45	23	95	49.15%		
		0	0	3	14	WAN	72.32%	
		79	59	20	64	14.69%	27.68%	
						LAN		
						10.73%		
						Software		
		0%	0%	12%	12%	23.73%		
		17%	18%	37%	51%	Hardware		
		14%	20%	21%	2%	8.47%		
		24%	26%	16%	55%	Personnel		
		0%	0%	2%	5%	4.52%		
		50%	35%	13%	35%	Database		
						1.13%		
						Mobile		
						2.26%		
						Other		
						5.65%		
Security Practices	Very Good =3, Somewhat = 2, Not at All = 1 Don't know = 0							
Security awareness and Training								
Not at all		1		3		Hardware		
Not at all		1		2		5%		
Not at all		1		2		Personnel		
Not at all		1		3	2.5	5%		
Somewhat		2	1.2			Database		
Security Strategy								
		1		3		Mobile		
		1		3		2%		
		1		2	2.666666666667	Other		
		1	1			4%		
Security Management								
		2		3				
		1		3				
		1		3				
		1		3				
		1		3				
		1		3				
		1		2	2.857142857143			
		1	1.125					
Security Policies and Regulations		1						
		1		3				
		1		3				
		2		3				
		2	1.4	3				
Collaborative Security Management		2		3				
		1		3				
		1		2				
		1		2	2.75			
		1	1.2					
Contigency Planning/Disaster Recover		1						
		1		3				
		1		3				
		1		3				
		1	1	2	2.75			
Physical Access Control		1						
		3		2				
		2		3				
		2		3				
		2	2	2	2.5			
Monitoring and Auditing Physical Sec		1						
		1		3				
		1		3				
		1	1	3	3			
System and Network Management		1		3				
		1		2				
		1		3				
		1		3				
		1		3				
		1		3				
		2		2				
		1		3				
		1		3	2.777777777778			
		1	1.1					
Monitoring and Auditing IT Sec		1		3				
		1		3	3			
		1	1					
Authentications and Authorization		1		3				
		1		3	3			
		1						
		1	1	3				
				3	3			
Vulnerability Management		1						
		1		3				
		1		3	3			
		1	1					
Encryption		1						
		1		3				
		1	1	2	2.5			
Security Architecture Design		1						
		1		2				
		1	1	2	2			
Incident Management		1						
		1		2				
		1		3	2.5			
		1	1					
Total Average		1.2			2.7			

Attack	Likeliness of Attack	Typical Severity	STRIDE	Attack Target	Likeliness of Attack	Typical Severity	Skill Level
Skill Level	Very High	Very High	Spoofing	web application	29.94%	Yes	72%
High	High	High	Tampering	OS	49.15%	No	28%
Medium	Medium	Medium	Information Disclosure	WAN	14.69%		
Low	Low	Low	Denial of Service	LAN	10.73%		
Very Low	Very Low	Very Low	Elevation of Privilege	Software	23.73%		
n/a	n/a	n/a		Hardware	8.47%		
				Personnel	4.52%		
				Database	1.13%		
				Mobile	2.26%		
				Other	5.65%		

Attack Focus	Attack Target		Attack Type		Likeliness of Attack		Typical Severity		Skill Level	
Abuse Existing Functionality	9.04%	web application	29.94%	Spoofing	12.99%	Very High	0.00%	Very High	11.30%	Very High	0.00%
Collect & Analyze Information	22.60%	OS	49.15%	Tampering	54.80%	High	19.77%	High	42.37%	High	21.47%
Employ Probabilistic Techniques	2.82%	WAN	14.69%	Repudiation	1.69%	Medium	20.34%	Medium	20.34%	Medium	18.08%
Engage in Deceptive Interactions	11.86%	LAN	10.73%	Information Disclosure	53.67%	Low	25.42%	Low	12.99%	Low	26.55%
Inject Unexpected Items	7.91%	Software	23.73%	Denial of Service	7.91%	Very Low	0.00%	Very Low	1.69%	Very Low	0.00%
Manipulate Data Structures	0.56%	Hardware	8.47%	Elevation of Privilege	36.16%	No data	33.33%	No data	11.30%	No data	44.63%
Manipulate System Resources	27.12%	Personnel	4.52%								
Manipulate Timing and State	0.56%	Database	1.13%								
Modify Shared File	0.56%	Mobile	2.26%								
Other	5.65%										

Digitized						
Warehouse inventory	high	34	102	146		
	medium	20	40			
	low	4	4			
Transaction/Tax info	high	4	12	82		
	medium	23	46			
	low	24	24			
Customer Info	high	16	48	110		
	medium	19	38			
	low	24	24			
Supplier Info	high	12	36	87		
	medium	19	38			
	low	13	13			
Employee Info	high	3	9	94		
	medium	40	80			
	low	5	5			

Current	Attack Type	Likeliness of Attack		Typical Severity		Skill Level	
Attack Focus	Spoofing	11.72%	Very High	0.00%	Very High	11.72%	Very High 0.00%
Abuse Existing Functionality 7.03%	Tampering	50.78%	High	17.97%	High	36.72%	High 17.19%
Collect & Analyze Information 26.56%	Repudiation	1.56%	Medium	19.53%	Medium	21.09%	Medium 14.06%
Engage in Deceptive Interactions 11.72%	Information Disclosure	55.47%	Low	25.78%	Low	15.63%	Low 24.22%
Inject Unexpected Items 9.38%	Denial of Service	5.47%	Very Low	0.00%	Very Low	2.34%	Very Low 0.00%
Manipulate Data Structures 0.00%	Elevation of Privilege	35.16%	No data	35.16%	No data	12.50%	No data 50.00%
Personnel 5.47%							
Manipulate System Resources 25.78%							
Manipulate Timing and State 0.78%							
Database 0.78%							
Subvert Access Control 14.84%							
Mobile 1.56%							
Other 3.91%							

Ghant chart – shows implementation
missing: online marketing
online payment sec standards HIPAA, etc.
Logistic/Supply Chain
Staff Training – upscale staff