#	Domain of Attack	#	Meta Attack Pattern	#	Standard Attack Pattern	#	Detailed Attack Pattern	Likelihood of Attack	Typical Severity	Skills Required
437	Supply Chain									
		116	Excavation							
				54	Query System for Information					
						95	WSDL Scanning	high	high	low
										medium
						127	Directory Indexing	high	medium	low
										high
						215	Fuzzing for application mapping	high	low	medium
						261	Fuzzing for garning other adjacent user/sensitive data	n/a	medium	n/a
						462	Cross Domain Search Timing	n/a	medium	low
				150	Collect Data from Common Resource Locations					
						143	Detect Unpublisized Web Pages	n/a	low	n/a
						144	Detect Unpublisized Web Services	n/a	low	n/a
						155	Screen Temporary Files for Sensitive Information	medium	medium	n/a
						406	Dumpster Diving	n/a	low	n/a
						637	Collect Data from Clipboard	low	low	high
						647	Collect Data from Registeries	medium	medium	low
						648	Collect Data from Screen Capture	medium	medium	low
				545	Pull Data from System Resources					
						498	Probe iOS Screenshots	n/a	n/a	n/a
						546	Incomplete Data Deletion in a Multi-Tenant Environment	low	medium	low
						634	Probe Audio and Visual Peripherals	low	high	high
						639	Probe System Files	n/a	medium	n/a
				569	Collect Data as Provided by Users					
						568	Capture Credentials via Keylogger	n/a	high	n/a
				675	Retrieve Data from Decomissioned Devices			medium	medium	high
								medium	medium	high
		154	Resource Location Spoofing							
				159	Redirect Access to Libraries					
						38	Leveraging/Manipulating Configuration File Search Paths	high	very high	low
						132	Symlink Attack	low	high	low
										high
						471	Search Order Hijacking	n/a	medium	medium
						641	DLL Side-Loading	low	high	high
				616	Establish Rogue Location					
						505	Scheme Squatting	n/a	n/a	n/a
						611	BitSquatting	low	medium	low
						615	Evil Twin Wifi Attack	n/a	low	n/a
						617	Cellular Rougue Base Station	n/a	low	low
						630	TypoSquatting	low	medium	low
						631	SoundSquatting	low	medium	low
						632	Homograph Attack via Homoglyphs	low	medium	low
						667	Bluetooth Impersonation AttackS (BIAS)	medium	high	low
						695	Repo Jacking	medium	high	low
		184	Software Integrity Attack							
				185	Malicious Software Download			n/a	very high	n/a
				186	Malicious Software Update					
						187	Malicious Automated Software Update via Redirection	high	high	n/a
						533	Malicious Manual Software Update	low	high	high
						614	Rooting SIM cards	n/a	high	medium
						657	Malicious Automated Software Update via Spoofing	high	high	n/a
				663	Exploitation of Transient Instruction Execution					
						696	Load Value Injection	low	very high	high
				669	Alternation of a Software Update			medium	high	n/a
		438	Modification During Manufacture							
				444	Development Alteration					
						206	Signing Malicious Code	n/a	very high	n/a
						443	Malicious Logic Inserted Into Product by Authorized Dealer	medium	high	n/a
						445	Malicious Logic Insertion Into Product via Configuration Management Manipulation	medium	high	n/a
						446	Malicious Logic Insertion Into Product via Inclusion of Third-Party Component	medium	high	n/a
						511	Infiltration of Software Development Environment	low	high	medium
										high
						516	Hardware Component Substitution During Baselining	low	high	medium
										high
						520	Conunterfeit Hardware Component Inserted During Product Assembly	low	high	high
						532	Altered Installed BIOS	low	high	high
						537	Infiltration of Hardware Development Environment	low	high	medium
										high
						538	Open-Source Library Manipulation	low	high	high
						539	ASIC with Malicious Functionality	low	high	high
						670	Software Development Tools Maliciously Altered	low	high	high
						672	Malicious Code Implanted During Chip Programming	low	high	medium
						673	Developer Signing Malicious Altered Software	medium	high	high
						678	System Build Data Maliciously Altered	low	high	n/a
				447	Design Alteration					
						517	Documentation Alteration to Circumvent Dial-down	low	high	high
						518	Documentation Alteration to Produce Under-performing Systems	low	high	high
						519	Documentation Alteration to Cause Errors in System Design	low	high	high
						521	Hardware Design Specifications are Altered	low	high	high
						671	Requirements for ASIC Functionality Maliciously Altered	low	high	high
						674	Design for FPGA Maliciously Altered	low	high	high
		439	Manipulation During Distribution							
				522	Malicious Hardware Component Replacement			low	high	high
				523	Malicious Software Implanted			low	high	high
				524	Rogue Integration Procedures			low	high	high
		440	Hardware Integrity Attack							
				401	Physically Hacking Hardware					
						402	Bypassing ATA Password Security	n/a	n/a	n/a
				534	Malicious Hardware Update					
						531	Hardware Component Substitution	low	high	high
						677	Server Functionality Compromise	low	high	n/a
		441	Malicious Logic Insertion							
				442	Infected Software					
						448	Embed Virus into DLL	medium	high	n/a
				452	Infected Hardware					
						452	Altered Component Firmware	low	very high	high
										medium
										low
				456	Infected Memory					
						457	USB Memory Attacks	low	high	n/a
						458	Flash Memory Attacks	n/a	n/a	n/a
		690	Metadata Spoofing					medium	high	medium