Information Disclosure

- CAPEC-410: Information Elicitation
  - CAPEC-407: Pretexting
    - CAPEC-383: Harvesting Information via API Event Monitoring
    - CAPEC-412: Pretexting via Customer Service
    - CAPEC-413: Pretexting via Tech Support
    - CAPEC-414: Pretexting via Delivery Person
    - CAPEC-415: Pretexting via Phone
- CAPEC-188: Reverse Engineering
  - CAPEC-167: White Box Reverse Engineering
    - CAPEC-37: Retrieve Embedded Sensitive Information
    - CAPEC-190: Reverse Engineer an Executable to Expose Assumed Hidden Functionality
    - CAPEC-191: Read Sensitive Constants Within an Executable
    - CAPEC-204: Lifting Sensitive Data Embedded in Cache
  - CAPEC-189: Black Box Reverse Engineering
    - CAPEC-621: Analysis of Packet Timing and Sizes
    - CAPEC-622: Electromagnetic Side-Channel Attack
    - CAPEC-623: Compromising Emanations Attack
- CAPEC-192: Protocol Analysis
  - CAPEC-97: Cryptanalysis
    - CAPEC-463: Padding Oracle Crypto Attack
    - CAPEC-608: Cryptanalysis of Cellular Encryption
- CAPEC-11: Cause Web Server Misclassification
- CAPEC-224: Fingerprinting
  - CAPEC-312: Active OS Fingerprinting
    - CAPEC-317: IP ID Sequencing Probe
    - CAPEC-318: IP 'ID' Echoed Byte-Order Probe
    - CAPEC-319: IP (DF) 'Don't Fragment Bit' Echoing Probe
    - CAPEC-320: TCP Timestamp Probe
    - CAPEC-321: TCP Sequence Number Probe
    - CAPEC-322: TCP (ISN) Greatest Common Divisor Probe
    - CAPEC-323: TCP (ISN) Counter Rate Probe
    - CAPEC-324: TCP (ISN) Sequence Predictability Probe
    - CAPEC-325: TCP Congestion Control Flag (ECN) Probe
    - CAPEC-326: TCP Initial Window Size Probe
    - CAPEC-327: TCP Options Probe
    - CAPEC-328: TCP 'RST' Flag Checksum Probe
    - CAPEC-329: ICMP Error Message Quoting Probe
    - CAPEC-330: ICMP Error Message Echoing Integrity Probe
    - CAPEC-331: ICMP IP Total Length Field Probe
    - CAPEC-332: ICMP IP 'ID' Field Error Message Probe
  - CAPEC-313: Passive OS Fingerprinting
  - CAPEC-541: Application Fingerprinting
    - CAPEC-170: Web Application Fingerprinting
    - CAPEC-310: Scanning for Vulnerable Software
    - CAPEC-472: Browser Fingerprinting
- CAPEC-129: Pointer Manipulation
- CAPEC-212: Functionality Misuse
  - CAPEC-48: Passing Local Filenames to Functions That Expect a URL
  - CAPEC-111: JSON Hijacking (aka JavaScript Hijacking)
  - CAPEC-620: Drop Encryption Level
    - CAPEC-606: Weakening of Cellular Encryption
- CAPEC-216: Communication Channel Manipulation
  - CAPEC-12: Choosing Message Identifier
  - CAPEC-217: Exploiting Incorrectly Configured SSL
- CAPEC-554: Functionality Bypass
  - CAPEC-179: Calling Micro-Services Directly
  - CAPEC-464: Evercookie
  - CAPEC-465: Transparent Proxy Abuse
- CAPEC-117: Interception
  - CAPEC-157: Sniffing Attacks
    - CAPEC-57: Utilising REST's Trust in the System Resources to Obtain Sensitive Data
    - CAPEC-65: Sniff Application Code
    - CAPEC-158: Sniffing Network Traffic
    - CAPEC-609: Cellular Traffic Intercept
  - CAPEC-499: Android Intent Intercept
    - CAPEC-501: Android Activity Hijack
  - CAPEC-651: Eavesdropping
    - CAPEC-508: Shoulder Surfing
    - CAPEC-634: Probe Audio and Video Peripherals
- CAPEC-116: Excavation
  - CAPEC-54: Query System for Information
    - CAPEC-127: Directory Indexing
    - CAPEC-95: WSDL Scanning
    - CAPEC-215: Fuzzing for Application Mapping
    - CAPEC-261: Fuzzing for Garnering Other Adjacent user/sensitive data
    - CAPEC-462: Cross-Domain Search Timing
  - CAPEC:150: Collect Data From Common Resource Locations
    - CAPEC-143: Detect Unpublicised Web Pages
    - CAPEC-144: Detect Unpublicised Web Services
    - CAPEC-155: Screen Temporary Files for Sensitive Information
    - CAPEC-406: Dumpster Diving
    - CAPEC-637: Collect Data from Clipboard
    - CAPEC-647: Collect Data from Registries
    - CAPEC-648: Collect Data from Screen Capture
  - CAPEC-545: Pull Data From System Resources
    - CAPEC-498: Probe iOS Screenshots
    - CAPEC-546: Incomplete Data Deletion in a Multi-Tenant Environment
    - CAPEC-634: Probe Audio and Video Peripherals
    - CAPEC-639: Probe System Files
  - CAPEC-569: Collect Data as Provided by Users
    - CAPEC-568: Capture Credentials via Keylogger
  - CAPEC-675: Retrieve Data from Decommissioned Devices
- CAPEC-169: Footprinting
  - CAPEC-292: Host Discovery
    - CAPEC-285: ICMP Echo Request Ping
    - CAPEC-294: ICMP Address Mask Request
    - CAPEC-295: Timestamp Request
    - CAPEC-296: ICMP Information Request
    - CAPEC-297: TCP ACK Ping
    - CAPEC-298: UDP Ping
    - CAPEC-299: TCP SYN Ping
    - CAPEC-612: WiFi MAC Address Tracking
    - CAPEC-613: WiFi SSID Tracking
    - CAPEC-618: Cellular Broadcast Message Request
    - CAPEC-619: Signal Strength Tracking
  - CAPEC-300: Port Scanning
    - CAPEC-287: TCP SYN Scan
    - CAPEC-301: TCP Connect Scan
    - CAPEC-302: TCP FIN Scan
    - CAPEC-303: TCP Xmas Scan
    - CAPEC-304: TCP Null Scan
    - CAPEC-305: TCP ACK Scan
    - CAPEC-306: TCP Window Scan
    - CAPEC-307: TCP RPC Scan
    - CAPEC-308: UDP Scan
  - CAPEC-309: Network Topology Mapping
    - CAPEC-290: Enumerate Mail Exchange Records
    - CAPEC-291: DNS Zone Transfers
    - CAPEC-293: Traceroute Route Enumeration
    - CAPEC-643: Identify Shared Files/ Directories on System
  - CAPEC-497: File Discovery
    - CAPEC-149: Explore for Predictable Temporary File Names
  - CAPEC-529: Malware-Directed Internal Reconnaissance
  - CAPEC-573: Process Footprinting
  - CAPEC-574: Services Footprinting
  - CAPEC-575: Account Footprinting
  - CAPEC-576: Group Permission Footprinting
  - CAPEC-577: Owner Footprinting
  - CAPEC-580: System Footprinting
    - CAPEC-85: AJAX Footprinting
    - CAPEC-581: Security Software Footprinting
  - CAPEC-646: Peripheral Footprinting