Tampering

- CAPEC-624: Hardware Fault Injection
  - CAPEC-625: Mobile Device Fault Injection
- CAPEC-594: Traffic Injection
  - CAPEC-596: TCP RST Injection
  - CAPEC-595: Connection Reset
- CAPEC-548: Contaminate Resources
- CAPEC-441: Malicious Logic Insertion
  - CAPEC-448: Embed Virus into DLL
  - CAPEC-442: Infected Software
  - CAPEC-638: Altered Component Firmware
  - CAPEC-452: Infected Hardware
  - CAPEC-457: USB Memory Attacks
  - CAPEC-456: Infected Memory
  - CAPEC-458: Flash Memory Attacks
- CAPEC-439: Manipulation During Distribution
  - CAPEC-522: Malicious Hardware Component Replacement
  - CAPEC-523: Malicious Software Implanted
  - CAPEC-524: Rogue Integration Procedures
- CAPEC-440: Hardware Integrity Attack
  - CAPEC-402: Bypassing ATA Password Security
  - CAPEC-401: Physically Hacking Hardware
  - CAPEC-530: Provide Counterfeit Component
  - CAPEC-531: Hardware Component Substitution
  - CAPEC-535: Malicious Gray Market Hardware
  - CAPEC-534: Malicious Hardware Update
  - CAPEC-677: Server Functionality Compromise
- CAPEC-444: Development Alteration
  - CAPEC-206: Signing Malicious Code
  - CAPEC-443: Malicious Logic Inserted into Product Software by Authorized Developer
  - CAPEC-445: Malicious Logic Insertion into Product Software via Configuration Management Manipulation
  - CAPEC-446: Malicious Logic Insertion into Product Software via 3rd Party Component Dependency
  - CAPEC-511: Infiltration of Software Development Environment
  - CAPEC-516: Hardware Component Substitution During Baselining
  - CAPEC-520: Counterfeit Hardware Component Inserted During Product Assembly
  - CAPEC-532: Altered Installed BIOS
  - CAPEC-537: Infiltration of Hardware Development Environment
  - CAPEC-538: Open-Source Library Manipulation
  - CAPEC-539: ASIC with Malicious Functionality
  - CAPEC-670: Software Development Tools Maliciously Altered
  - CAPEC-672: Malicious Code Implanted During Chip Programming
  - CAPEC-673: Developer Signing Maliciously Altered Software
  - CAPEC-678: System Build Data Maliciously Altered
- CAPEC-438: Modification During Manufacture
- CAPEC-447: Design Alteration
  - CAPEC-517: Documentation Alteration to Circumvent Dial-down
  - CAPEC-518: Documentation Alteration to Produce Under-Performing Systems
  - CAPEC-519: Documentation Alteration to Cause Errors in System Design
  - CAPEC-521: Hardware Design Specifications are Altered
  - CAPEC-671: Requirements for ASIC Functionality Maliciously Altered
  - CAPEC-674: Design for FPGA Maliciously Altered
- CAPEC-185: Malicious Software Download
  - CAPEC-187: Malicious Automated Software Update via Redirection
  - CAPEC-533: Malicious Manual Software Update
  - CAPEC-614: Rooting SIM Cards
  - CAPEC-657: Malicious Automated Software Update via Spoofing
  - CAPEC-186: Malicious Software Update
- CAPEC-184: Software Integrity Attack
  - CAPEC-663: Exploitation of Transient Instruction Execution
  - CAPEC-669: Alteration of a Software Update
- CAPEC-481: Contradictory Destinations inTraffic Routing Schemes
- CAPEC-166: Force the System to Reset Values
- CAPEC-51: Poison Web Service Registry
- CAPEC-142: DNS Cache Poisoning
- CAPEC-141: Cache Poisoning
- CAPEC-93: Log Injection-Tampering-Forging
- CAPEC-81: Web Logs Tampering
- CAPEC-268: Audit Log Manipulation
- CAPEC-571: Block Logging to Central Repository
- CAPEC-161: Infrastructure Manipulation
- CAPEC-123: Buffer Manipulation
  - CAPEC-100: Overflow Buffers
    - CAPEC-10: Buffer Overflow via Environment Variables
    - CAPEC-14: Client-side Injection-induced Buffer Overflow
    - CAPEC-24: Filter Failure through Buffer Overflow
    - CAPEC-256: SOAP Array Overflow
    - CAPEC-42: MIME Conversion
    - CAPEC-44: Overflow Binary Resource File
    - CAPEC-45: Buffer Overflow via Symbolic Links
    - CAPEC-46: Overflow Variables and Tags
    - CAPEC-47: Buffer Overflow via Parameter Expansion
    - CAPEC-67: String Format Overflow in syslog()
    - CAPEC-8: Buffer Overflow in an API Call
    - CAPEC-9: Buffer Overflow in Local Command-Line Utilities
  - CAPEC-540: Overread Buffers
- CAPEC-124: Shared Resource Manipulation
  - CAPEC-26: Leveraging Race Conditions
  - CAPEC-27: Leveraging Race Conditions via Symbolic Links
  - CAPEC-29: Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions
- CAPEC-129: Pointer Manipulation
- CAPEC-272: Protocol Manipulation
  - CAPEC-90: Reflection Attack in Authentication Protocol
  - CAPEC-220: Client-Server Protocol Manipulation
    - CAPEC-5: Blue Boxing
    - CAPEC-33: HTTP Request Smuggling
    - CAPEC-34: HTTP Response Splitting
    - CAPEC-105: HTTP Request Splitting
    - CAPEC-273: HTTP Response Smuggling
    - CAPEC-274: HTTP Verb Tampering
  - CAPEC-276: Inter-Component Protocol Manipulation
    - CAPEC-665: Exploitation of Thunderbolt Protection Flaws
  - CAPEC-277: Data Interchange Protocol Manipulation
  - CAPEC-278: Web Services Protocol Manipulation
    - CAPEC-201: Serialized Data External Linking
    - CAPEC-221: Data Serialization External Entities Blowup
    - CAPEC-279: SOAP Manipulation
- CAPEC-153: Input Data Manipulation
  - CAPEC-126: Path Traversal
    - CAPEC-139: Relative Path Traversal
    - CAPEC-597: Absolute Path Traversal
    - CAPEC-76: Manipulating Web Input to File System Calls
  - CAPEC-128: Integer Attacks
    - CAPEC-92: Forced Integer Overflow
  - CAPEC-267: Leverage Alternate Encoding
    - CAPEC-120: Double Encoding
    - CAPEC-3: Using Leading 'Ghost' Character Sequences to Bypass Input Filters
    - CAPEC-4: Using Alternative IP Address Encodings
    - CAPEC-43: Exploiting Multiple Input Interpretation Layers
    - CAPEC-52: Embedding NULL Bytes
    - CAPEC-53: Postfix, Null Terminate, and Backslash
    - CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
    - CAPEC-71: Using Unicode Encoding to Bypass Validation Logic
    - CAPEC-72: URL Encoding
    - CAPEC-78: Using Escaped Slashes in Alternate Encoding
    - CAPEC-79: Using Slashes in Alternate Encoding
    - CAPEC-80: Using UTF-8 Encoding to Bypass Validation Logic
  - CAPEC-28: Fuzzing
  - CAPEC-33: HTTP Request Smuggling
  - CAPEC-34: HTTP Response Splitting
  - CAPEC-105: HTTP Request Splitting
  - CAPEC-165: File Manipulation
    - CAPEC-73: User Controlled Filename
    - CAPEC-572: Artificially Inflate File Sizes
      - CAPEC-655: Avoid Security Tool Identification by Adding Data
    - CAPEC-635: Alternative Execution Due to Deceptive Filenames
      - CAPEC-649: Adding a Space to a File Extension
    - CAPEC-636: Hiding Malicious Data or Code within Files
      - CAPEC-168: Windows ::DATA Alternate Data Stream
  - CAPEC-74: Manipulating State
    - CAPEC-140: Bypassing of Intermediate Forms in Multiple-Form Sets
    - CAPEC-663: Exploitation of TransientInstruction Execution
  - CAPEC-75: Manipulating Writeable Configuration Files
  - CAPEC-113: Interface Manipulation
    - CAPEC-133: Try All Common Switches
    - CAPEC-160: Exploit Script-Based APIs
  - CAPEC-176: Configuration/Environment Manipulation
    - CAPEC-75: Manipulating Writeable Configuration Files
    - CAPEC-203: Manipulate Registry Information
      - CAPEC-51: Poison Web Service Registry
      - CAPEC-270: Modification of Registry Run Keys
      - CAPEC-478: Modification of Windows Service Configuration
    - CAPEC-271: Schema Poisoning
      - CAPEC-146: XML Schema Poisoning
    - CAPEC-536: Data Injection During Configuration
    - CAPEC-578: Disable Security Software