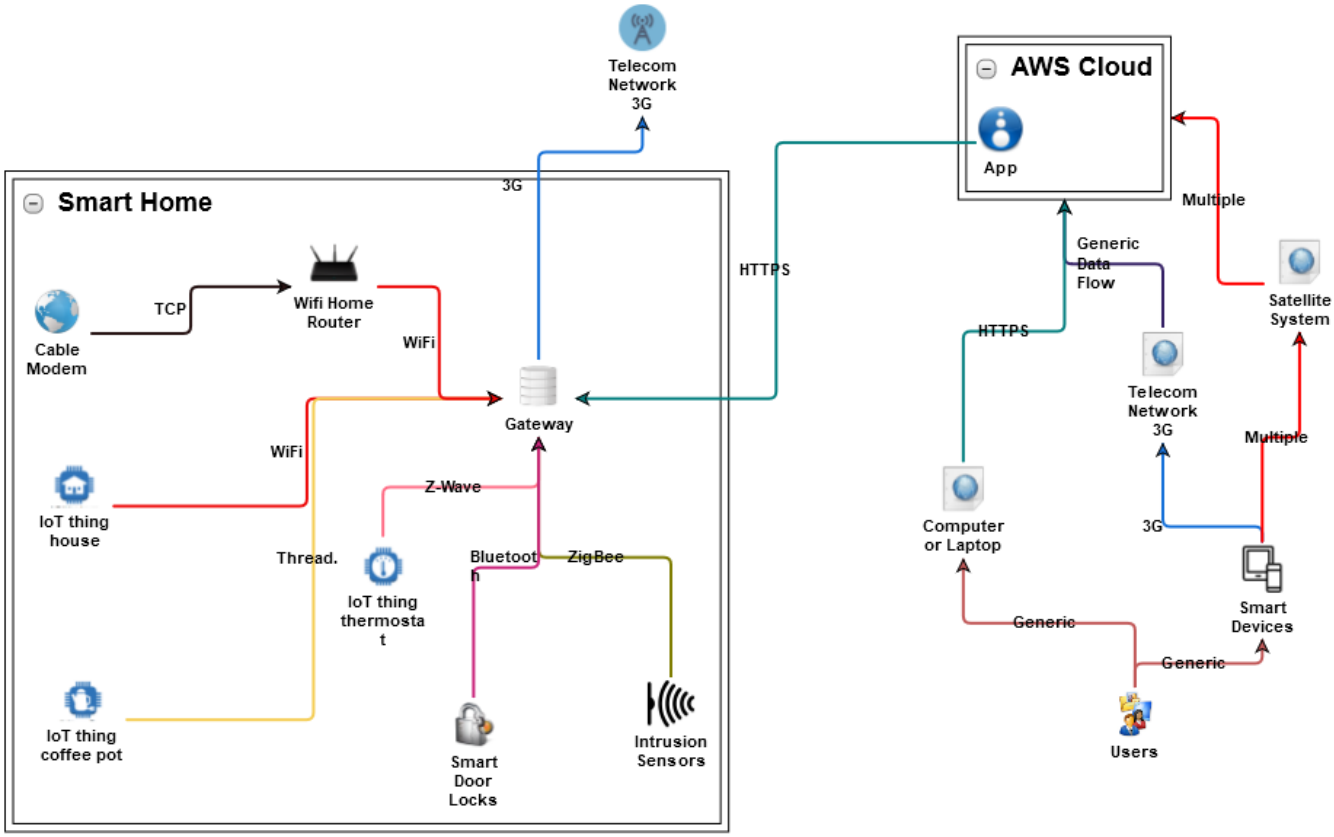
Smart Home - 2

04/10/2018

Threat Model



Description

Threats

Threat	Source	Risk	Status	Date Created
Man in the Middle Attack	Gateway	Very High	Open	03/31/2018
Mobile Phone: Camera and or Mic Hijack	Smart Devices	Very Low	Open	03/31/2018
Mobile Phone: Insecure Communications	Smart Devices	Very	Open	03/31/2018

		Low		
Mobile Phone: Session Hijacking	Smart Devices	Very Low	Open	03/31/2018
Mobile Phone: Sensitive Data Leakage	Smart Devices	Very Low	Open	03/31/2018
Mobile Phone: Browser SSL Vulnerability	Smart Devices	Very Low	Open	03/31/2018
Failed Wakeup Alarm	Smart Home	Medium	Open	03/31/2018
Family Needs	Smart Home	High	Open	03/31/2018
Man in the Middle Attack	WiFi	Very High	Open	03/31/2018
Wi-Fi Jamming	WiFi	High	Open	03/31/2018
WiFi MAC Address Tracking	WiFi	Very High	Open	03/31/2018
WiFi SSID Tracking	WiFi	Very High	Open	03/31/2018
Content Spoofing	3G	Medium	Open	03/31/2018
Sniffing Attacks	3G	Medium	Open	03/31/2018
Action Spoofing	3G	Very High	Open	03/31/2018
Denial of Service through Resource Depletion	3G	Medium	Open	03/31/2018
Privilege Abuse	3G	Very High	Open	03/31/2018
Resource Location Spoofing	3G	Very High	Open	03/31/2018
Sniffing Network Traffic	3G	Very High	Open	03/31/2018
Intent Spoof	3G	Very High	Open	03/31/2018
Cellular Traffic Intercept	3G	Very High	Open	03/31/2018
Denial of Service	3G	Very High	Open	03/31/2018
Flooding	Thread.	Medium	Open	03/31/2018
Sniffing Attacks	Thread.	Medium	Open	03/31/2018
Denial of Service through Resource Depletion	Thread.	Medium	Open	03/31/2018
Scanning for Vulnerable Software	Thread.	Low	Open	03/31/2018
Malicious Logic Inserted Into Product	Thread.	Very High	Open	03/31/2018
Malicious Logic Inserted Into Product Software	Thread.	Very High	Open	03/31/2018
Malicious Logic Insertion into Product Memory	Thread.	High	Open	03/31/2018
Man in the Middle Attack	Thread.	Very High	Open	03/31/2018

Signature Spoofing by Key Theft	Thread.	Very High	Open	03/31/2018
Add Malicious File to Shared Webroot	Thread.	Very High	Open	03/31/2018
Communication Channel Manipulation	Thread.	Very High	Open	03/31/2018
Intent Spoof	Thread.	Very High	Open	03/31/2018
Jamming	Thread.	Very High	Open	03/31/2018
Denial of Service	Thread.	Very High	Open	03/31/2018
TCP SYN Scan	TCP	Low	Open	03/31/2018
TCP Window Scan	TCP	Low	Open	03/31/2018
TCP RPC Scan	TCP	Low	Open	03/31/2018
TCP Sequence Number Probe	TCP	Low	Open	03/31/2018
TCP ISN Greatest Common Divisor Probe	TCP	Low	Open	03/31/2018
TCP ISN Counter Rate Probe	TCP	Low	Open	03/31/2018
TCP ISN Sequence Predictability Probe	TCP	Low	Open	03/31/2018
TCP Congestion Control Flag Probe	TCP	Low	Open	03/31/2018
TCP Initial Window Size Probe	TCP	Low	Open	03/31/2018
Sniffing Attacks	Z-Wave	Medium	Open	03/31/2018
Sniff Application Code	Z-Wave	High	Open	03/31/2018
Man in the Middle Attack	Z-Wave	Very High	Open	03/31/2018
Signature Spoofing by Key Theft	Z-Wave	Very High	Open	03/31/2018
Signature Spoofing by Key Recreation	Z-Wave	Very High	Open	03/31/2018
Add Malicious File to Shared Webroot	Z-Wave	Very High	Open	03/31/2018
Intent Spoof	Z-Wave	Very High	Open	03/31/2018
Exploiting Incorrectly Configured SSL	HTTPS	Very High	Open	03/31/2018
Sniffing Attacks	ZigBee	Medium	Open	03/31/2018
Man in the Middle Attack	ZigBee	Very High	Open	03/31/2018
Add Malicious File to Shared Webroot	ZigBee	Very High	Open	03/31/2018
Shared Technology Issues	ZigBee	Very High	Open	03/31/2018
Man in the Middle Attack	Bluetooth	Very High	Open	03/31/2018

Dictionary-based Password Attack	App	High	Open	03/31/2018
Password Brute Forcing	App	High	Open	03/31/2018
Password Recovery Exploitation	App	High	Open	03/31/2018
Exploit Common or default Usernames and Passwords	App	High	Open	03/31/2018
Clickjacking	App	Very High	Open	03/31/2018
HTTP Response Splitting	App	High	Open	03/31/2018
Cross Site Request Forgery	App	Very High	Open	03/31/2018
SQL Injection	App	High	Open	03/31/2018
Blind SQL Injection	App	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	App	High	Open	03/31/2018
Persistent Cross Site Scripting - WASC	App	High	Open	03/31/2018
Accessing, Intercepting, Modifying HTTP Cookies	App	High	Open	03/31/2018
Session Hijacking	App	Very High	Open	03/31/2018
Session Credential Falsification through Forging	App	Medium	Open	03/31/2018
Reusing Session IDs aka Session Replay	App	High	Open	03/31/2018
Session Fixation	App	High	Open	03/31/2018
Weak Identity, Credential and Access Management	AWS Cloud	Very High	Open	03/31/2018
Denial of Service	AWS Cloud	Very High	Open	03/31/2018
Confidential Data Exposure	AWS Cloud	Very High	Open	03/31/2018
Malicious Insiders	AWS Cloud	Very High	Open	03/31/2018
Account Hijacking	AWS Cloud	Very High	Open	03/31/2018
Insecure Communication	AWS Cloud	Very High	Open	03/31/2018
Permanent Data Loss	AWS Cloud	Very High	Open	03/31/2018
Sensitive Data Exposure	AWS Cloud	Very High	Open	03/31/2018
Code Injection	AWS Cloud	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	AWS Cloud	High	Open	03/31/2018
File Manipulation	Computer or Laptop	Medium	Open	03/21/2018
Accessing, Modifying or Executing Executable Files	Computer or Laptop	Very High	Open	03/21/2018
Create files with the same name as files protected with a higher classification	Computer or Laptop	Very High	Open	03/21/2018

Force Use of Corrupted Files	Computer or Laptop	Medium	Open	03/21/2018
Leveraging or Manipulating Configuration File Search Paths	Computer or Laptop	Very High	Open	03/21/2018
User-Controlled Filename	Computer or Laptop	High	Open	03/21/2018
Manipulating Web Input to File System Calls	Computer or Laptop	Very High	Open	03/21/2018
Bluejacking	Computer or Laptop	Very High	Open	03/21/2018
Bluesnarfing	Computer or Laptop	Very High	Open	03/21/2018
Bluebugging	Computer or Laptop	Very High	Open	03/21/2018
Man in the Middle Attack	Computer or Laptop	Very High	Open	03/21/2018
Wi-Fi Jamming	Computer or Laptop	High	Open	03/21/2018
WiFi MAC Address Tracking	Computer or Laptop	Very High	Open	03/21/2018
WiFi SSID Tracking	Computer or Laptop	Very High	Open	03/21/2018
Physical Theft	Computer or Laptop	Very High	Open	03/21/2018
Jamming	Computer or Laptop	Very High	Open	03/21/2018
File Manipulation	Computer or Laptop	Medium	Open	03/21/2018
Accessing, Modifying or Executing Executable Files	Computer or Laptop	Very High	Open	03/21/2018
Create files with the same name as files protected with a higher classification	Computer or Laptop	Very High	Open	03/21/2018
Manipulating Web Input to File System Calls	Computer or Laptop	Very High	Open	03/21/2018
Email Injection	Computer or Laptop	Medium	Open	03/21/2018
DNS Cache Poisoning	Computer or Laptop	Very High	Open	03/21/2018
Phishing	Computer or Laptop	Very High	Open	03/21/2018
Targeted Malware	Computer or Laptop	Very High	Open	03/21/2018
SPAM	Computer or Laptop	Medium	Open	03/21/2018
Overflow Buffers	Computer or Laptop	Very High	Open	03/21/2018

Man in the Middle Attack	Computer or Laptop	Very High	Open	03/21/2018
File Manipulation	Computer or Laptop	Medium	Open	03/21/2018
Accessing, Modifying or Executing Executable Files	Computer or Laptop	Very High	Open	03/21/2018
Create files with the same name as files protected with a higher classification	Computer or Laptop	Very High	Open	03/21/2018
Manipulating Web Input to File System Calls	Computer or Laptop	Very High	Open	03/21/2018
Identity Spoofing - Impersonation	Computer or Laptop	Medium	Open	03/21/2018
Man in the Middle Attack	Computer or Laptop	Very High	Open	03/21/2018
Targeted Malware	Computer or Laptop	Very High	Open	03/21/2018
Account Footprinting	Computer or Laptop	Very High	Open	03/21/2018
Malware Propagation via USB Stick	Computer or Laptop	Very High	Open	03/21/2018
DEPRECATED: Malware Propagation via USB U3 Autorun	Computer or Laptop	Very High	Open	03/21/2018
DEPRECATED: Malware Propagation via Infected Peripheral Device	Computer or Laptop	Very High	Open	03/21/2018
USB Memory Attacks	Computer or Laptop	High	Open	03/21/2018
Exploiting Incorrectly Configured SSL	Computer or Laptop	Very High	Open	03/21/2018
Email Injection	Computer or Laptop	Medium	Open	03/21/2018
IMAP or SMTP Command Injection	Computer or Laptop	Medium	Open	03/21/2018
IMAP or SMTP Command Injection	Computer or Laptop	Medium	Open	03/21/2018
TCP SYN Scan	Computer or Laptop	Low	Open	03/21/2018
TCP Window Scan	Computer or Laptop	Low	Open	03/21/2018
TCP RPC Scan	Computer or Laptop	Low	Open	03/21/2018
TCP Sequence Number Probe	Computer or Laptop	Low	Open	03/21/2018
TCP ISN Greatest Common Divisor Probe	Computer or Laptop	Low	Open	03/21/2018
TCP ISN Counter Rate Probe	Computer or Laptop	Low	Open	03/21/2018
TCP ISN Sequence Predictability Probe	Computer or	Low	Open	03/21/2018

	Laptop			
TCP Congestion Control Flag Probe	Computer or Laptop	Low	Open	03/21/2018
TCP Initial Window Size Probe	Computer or Laptop	Low	Open	03/21/2018
Man in the Middle Attack	Computer or Laptop	Very High	Open	03/21/2018
Wi-Fi Jamming	Computer or Laptop	High	Open	03/21/2018
WiFi MAC Address Tracking	Computer or Laptop	Very High	Open	03/21/2018
WiFi SSID Tracking	Computer or Laptop	Very High	Open	03/21/2018
Sensitive Data Exposure	Computer or Laptop	Very High	Open	03/21/2018
Dictionary-based Password Attack	Computer or Laptop	High	Open	03/21/2018
Password Brute Forcing	Computer or Laptop	High	Open	03/21/2018
Password Recovery Exploitation	Computer or Laptop	High	Open	03/21/2018
Exploit Common or default Usernames and Passwords	Computer or Laptop	High	Open	03/21/2018
Cross Site Request Forgery	Computer or Laptop	Very High	Open	03/21/2018
Reflected Cross Site Scripting - WASC	Computer or Laptop	High	Open	03/21/2018
Email Injection	Computer or Laptop	Medium	Open	03/21/2018
IMAP or SMTP Command Injection	Computer or Laptop	Medium	Open	03/21/2018
Leveraging or Manipulating Configuration File Search Paths	Computer or Laptop	Very High	Open	03/21/2018
Manipulating Writeable Configuration Files	Computer or Laptop	Very High	Open	03/21/2018
Overflow Buffers	Computer or Laptop	Very High	Open	03/21/2018
Verify - Insecure Configuration	Computer or Laptop	Very High	Open	03/21/2018
DNS Cache Poisoning	Computer or Laptop	Very High	Open	03/21/2018
Redirect Access to Libraries	Computer or Laptop	Very High	Open	03/21/2018
Accessing, Modifying or Executing Executable Files	Computer or Laptop	Very High	Open	03/21/2018
Code Inclusion	Computer or Laptop	Very High	Open	03/21/2018

Malicious Software Download	Computer or Laptop	Very High	Open	03/21/2018
File System Function Injection, Content Based	Computer or Laptop	Very High	Open	03/21/2018
Hijacking a Privileged Thread of Execution	Computer or Laptop	Very High	Open	03/21/2018
Overflow Binary Resource File	Computer or Laptop	Very High	Open	03/21/2018
Malicious Logic Inserted Into Product	Computer or Laptop	Very High	Open	03/21/2018
Malicious Logic Inserted Into Product Software by Authorized Developer	Computer or Laptop	Very High	Open	03/21/2018
Malicious Logic Insertion into Product Software via Externally Manipulated Component	Computer or Laptop	Very High	Open	03/21/2018
Malicious Logic Insertion into Product Software via Configuration Management Manipulation	Computer or Laptop	Very High	Open	03/21/2018
Malicious Logic Insertion into Product Software via Inclusion of 3rd Party Component Dependency	Computer or Laptop	Very High	Open	03/21/2018
Malicious Logic Insertion into Product Software during Update	Computer or Laptop	Very High	Open	03/21/2018
Malware Infection into Product Software	Computer or Laptop	Very High	Open	03/21/2018
Malware Propagation via USB Stick	Computer or Laptop	Very High	Open	03/21/2018
Privilege Abuse	Computer or Laptop	Very High	Open	03/21/2018
Buffer Manipulation	Computer or Laptop	Very High	Open	03/21/2018
Overread Buffers	Computer or Laptop	Very High	Open	03/21/2018
Privilege Escalation	Computer or Laptop	Very High	Open	03/21/2018
Malware-Directed Internal Reconnaissance	Computer or Laptop	Very High	Open	03/21/2018
Targeted Malware	Computer or Laptop	Very High	Open	03/21/2018
Install Rootkit	Computer or Laptop	Very High	Open	03/21/2018
Malware Infection into Product Software	Computer or Laptop	Very High	Open	03/21/2018
Man in the Middle Attack	Computer or Laptop	Very High	Open	03/21/2018
Dictionary-based Password Attack	Computer or Laptop	High	Open	03/21/2018
Password Brute Forcing	Computer or Laptop	High	Open	03/21/2018
Password Recovery Exploitation	Computer or	High	Open	03/21/2018

	Laptop			
Exploit Common or default Usernames and Passwords	Computer or Laptop	High	Open	03/21/2018
Cross Site Request Forgery	Computer or Laptop	Very High	Open	03/21/2018
Reflected Cross Site Scripting - WASC	Computer or Laptop	High	Open	03/21/2018
iOS: Data Storage	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Weak Server Side Controls	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Insufficient Transport Layer Protection	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Client Side Injection	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Poor Authorization and Authentication	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Improper Session Handling	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Security Decisions via Untrusted Inputs	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Side Channel Data Leakage	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Broken Encryption	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Sensitive Information Disclosure	Telecom Network 3G	Very High	Open	03/19/2018
Probe iOS Screenshots	Telecom Network 3G	Very High	Open	03/19/2018
Altered Installed BIOS	Telecom Network 3G	Very High	Open	03/19/2018
Physical Theft	Telecom Network 3G	Very High	Open	03/19/2018
Session Hijacking	Telecom Network 3G	Very High	Open	03/19/2018
Denial of Service through Resource Depletion	Telecom Network 3G	Medium	Open	03/19/2018
Protocol Manipulation	Telecom Network 3G	Medium	Open	03/19/2018
TCP SYN Scan	Telecom Network 3G	Low	Open	03/19/2018
TCP ACK Ping	Telecom Network 3G	Low	Open	03/19/2018
TCP SYN Ping	Telecom Network 3G	Low	Open	03/19/2018
TCP Connect Scan	Telecom Network 3G	Low	Open	03/19/2018

TCP ACK Scan	Telecom Network 3G	Low	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network 3G	High	Open	03/19/2018
WS: XML Denial of Service	Telecom Network 3G	Very High	Open	03/19/2018
Gather Information	Telecom Network 3G	Very High	Open	03/19/2018
HTTP DoS	Telecom Network 3G	Very High	Open	03/19/2018
ICMP Fragmentation	Telecom Network 3G	Very High	Open	03/19/2018
Unauthorized Use of Device Resources	Telecom Network 3G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 3G	Very High	Open	03/19/2018
Eavesdropping	Telecom Network 3G	Very High	Open	03/19/2018
Reusing Session IDs aka Session Replay	Telecom Network 3G	High	Open	03/19/2018
Weak Identity, Credential and Access Management	Telecom Network 3G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 3G	Very High	Open	03/19/2018
Sensitive Data Exposure	Telecom Network 3G	Very High	Open	03/19/2018
Code Injection	Telecom Network 3G	High	Open	03/19/2018
Reflected Cross Site Scripting - WASC	Telecom Network 3G	High	Open	03/19/2018
Encryption Brute Forcing	Telecom Network 3G	Low	Open	03/19/2018
Cross Site Request Forgery	Telecom Network 3G	Very High	Open	03/19/2018
Overflow Buffers	Telecom Network 3G	Very High	Open	03/19/2018
Sensitive Data Exposure	Telecom Network 3G	Very High	Open	03/19/2018
Weak Identity, Credential and Access Management	Telecom Network 3G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 3G	Very High	Open	03/19/2018
Code Injection	Telecom Network 3G	High	Open	03/19/2018
Reflected Cross Site Scripting - WASC	Telecom Network 3G	High	Open	03/19/2018

Dictionary-based Password Attack	Telecom Network 3G	High	Open	03/19/2018
Password Brute Forcing	Telecom Network 3G	High	Open	03/19/2018
Password Recovery Exploitation	Telecom Network 3G	High	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network 3G	High	Open	03/19/2018
Encryption Brute Forcing	Telecom Network 3G	Low	Open	03/19/2018
Cross Site Request Forgery	Telecom Network 3G	Very High	Open	03/19/2018
Overflow Buffers	Telecom Network 3G	Very High	Open	03/19/2018
Overflow Buffers	Telecom Network 3G	Very High	Open	03/19/2018
Cross Site Request Forgery	Telecom Network 3G	Very High	Open	03/19/2018
Dictionary-based Password Attack	Telecom Network 3G	High	Open	03/19/2018
Password Brute Forcing	Telecom Network 3G	High	Open	03/19/2018
Password Recovery Exploitation	Telecom Network 3G	High	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network 3G	High	Open	03/19/2018
Encryption Brute Forcing	Telecom Network 3G	Low	Open	03/19/2018
Weak Identity, Credential and Access Management	Telecom Network 3G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 3G	Very High	Open	03/19/2018
Sensitive Data Exposure	Telecom Network 3G	Very High	Open	03/19/2018
Code Injection	Telecom Network 3G	High	Open	03/19/2018
Reflected Cross Site Scripting - WASC	Telecom Network 3G	High	Open	03/19/2018
Authentication Bypass	Telecom Network 3G	Medium	Open	03/19/2018
Sniff Application Code	Telecom Network 3G	High	Open	03/19/2018
Exploiting Incorrectly Configured SSL	Telecom Network 3G	Very High	Open	03/19/2018
Data Interception Attacks	Telecom Network 3G	Medium	Open	03/19/2018
Fake the Source of Data	Telecom Network 3G	Medium	Open	03/19/2018

User-Controlled Filename	Telecom Network 3G	High	Open	03/19/2018
Manipulating User State	Telecom Network 3G	High	Open	03/19/2018
Email Injection	Telecom Network 3G	Medium	Open	03/19/2018
IMAP or SMTP Command Injection	Telecom Network 3G	Medium	Open	03/19/2018
Content Spoofing	Telecom Network 3G	Medium	Open	03/20/2018
Action Spoofing	Telecom Network 3G	Very High	Open	03/20/2018
Resource Location Spoofing	Telecom Network 3G	Very High	Open	03/20/2018
Intent Spoof	Telecom Network 3G	Very High	Open	03/20/2018
Denial of Service through Resource Depletion	Telecom Network 3G	Medium	Open	03/20/2018
Denial of Service	Telecom Network 3G	Very High	Open	03/20/2018
Sniffing Attacks	Telecom Network 3G	Medium	Open	03/20/2018
Sniffing Network Traffic	Telecom Network 3G	Very High	Open	03/20/2018
Privilege Abuse	Telecom Network 3G	Very High	Open	03/20/2018
Cellular Traffic Intercept	Telecom Network 3G	Very High	Open	03/20/2018
SQL Injection	Telecom Network 3G	High	Open	03/20/2018
SQL Injection	Telecom Network 3G	High	Open	03/20/2018
SQL Injection	Telecom Network 3G	High	Open	03/20/2018
Blind SQL Injection	Telecom Network 3G	High	Open	03/20/2018
Blind SQL Injection	Telecom Network 3G	High	Open	03/20/2018
Blind SQL Injection	Telecom Network 3G	High	Open	03/20/2018
Persistent Cross Site Scripting - WASC	Telecom Network 3G	High	Open	03/20/2018
Persistent Cross Site Scripting - WASC	Telecom Network 3G	High	Open	03/20/2018
Persistent Cross Site Scripting - WASC	Telecom Network 3G	High	Open	03/20/2018

HTTP Response Splitting	Telecom Network 3G	High	Open	03/27/2018
HTTP Response Splitting	Telecom Network 3G	High	Open	03/27/2018
HTTP Response Splitting	Telecom Network 3G	High	Open	03/27/2018
Clickjacking	Telecom Network 3G	Very High	Open	03/27/2018
Clickjacking	Telecom Network 3G	Very High	Open	03/27/2018
Clickjacking	Telecom Network 3G	Very High	Open	03/27/2018
CVE-2015-0726	Telecom Network 3G	Very High	Open	03/19/2018
CVE-2016-6375	Telecom Network 3G	Very High	Open	03/19/2018
CVE-2015-0726	Telecom Network 3G	Very High	Open	03/19/2018
CVE-2016-6375	Telecom Network 3G	Very High	Open	03/19/2018
CVE-2005-0356	Telecom Network 3G	Very High	Open	03/19/2018
CVE-2005-4499	Telecom Network 3G	Very High	Open	03/19/2018
CVE-2006-4098	Telecom Network 3G	Very High	Open	03/19/2018
Jamming	Satellite System	Very High	Open	03/20/2018
Denial of Service	Satellite System	Very High	Open	03/20/2018
Eavesdropping	Satellite System	Very High	Open	03/20/2018
Hijacking	Satellite System	Very High	Open	03/20/2018
Protocol Manipulation	Satellite System	Medium	Open	03/20/2018
Lifting Data Embedded in Client Distributions	Satellite System	Very High	Open	03/20/2018
Password Recovery Exploitation	Satellite System	High	Open	03/20/2018
Manipulate Resources	Satellite System	Very High	Open	03/20/2018
Jamming	Satellite System	Very High	Open	03/20/2018
TCP SYN Scan	Satellite System	Low	Open	03/21/2018
TCP Window Scan	Satellite System	Low	Open	03/21/2018
TCP RPC Scan	Satellite System	Low	Open	03/21/2018

TCP Sequence Number Probe	Satellite System	Low	Open	03/21/2018
TCP ISN Greatest Common Divisor Probe	Satellite System	Low	Open	03/21/2018
TCP ISN Counter Rate Probe	Satellite System	Low	Open	03/21/2018
TCP ISN Sequence Predictability Probe	Satellite System	Low	Open	03/21/2018
TCP Congestion Control Flag Probe	Satellite System	Low	Open	03/21/2018
TCP Initial Window Size Probe	Satellite System	Low	Open	03/21/2018
Man in the Middle Attack	Satellite System	Very High	Open	03/21/2018
Exploiting Incorrectly Configured SSL	Satellite System	Very High	Open	03/21/2018
Media Access Control - MAC Attack	Satellite System	Very High	Open	03/21/2018
Double Encapsulation VLAN Hopping Attack	Satellite System	Very High	Open	03/21/2018
Address Resolution Protocol - ARP Attacks	Satellite System	Very High	Open	03/21/2018
Spanning Tree Attack	Satellite System	Very High	Open	03/21/2018
VLAN Trunking Protocol - VTP attack	Satellite System	Very High	Open	03/21/2018
Cisco Discovery Protocol - CDP Attacks	Satellite System	Very High	Open	03/21/2018
Private VLAN - PVLAN Attack	Satellite System	Very High	Open	03/21/2018
Basic VLAN Hopping attack	Satellite System	Very High	Open	03/21/2018
VMPS and or VQP attack	Satellite System	Very High	Open	03/21/2018
Session Hijacking	Satellite System	Very High	Open	03/21/2018
Session Credential Falsification through Forging	Satellite System	Medium	Open	03/21/2018
Exploitation of Trusted Credentials	Satellite System	High	Open	03/21/2018
WS: Insufficient Authentication	Satellite System	Very High	Open	03/21/2018
Exploitation of Authentication	Satellite System	Very High	Open	03/21/2018
Privilege Escalation	Satellite System	Very High	Open	03/21/2018
Lack of confidentiality	Satellite System	Very High	Open	03/21/2018
Sensitive Data Exposure	Satellite System	Very High	Open	03/21/2018
Malware Propagation via USB Stick	Satellite System	Very High	Open	03/21/2018
DEPRECATED: Malware Propagation via USB U3 Autorun	Satellite System	Very	Open	03/21/2018

		High		
DEPRECATED: Malware Propagation via Infected Peripheral Device	Satellite System	Very High	Open	03/21/2018
USB Memory Attacks	Satellite System	High	Open	03/21/2018
Content Spoofing	Satellite System	Medium	Open	03/21/2018
Sniffing Attacks	Satellite System	Medium	Open	03/21/2018
Action Spoofing	Satellite System	Very High	Open	03/21/2018
Denial of Service through Resource Depletion	Satellite System	Medium	Open	03/21/2018
Privilege Abuse	Satellite System	Very High	Open	03/21/2018
Resource Location Spoofing	Satellite System	Very High	Open	03/21/2018
Sniffing Network Traffic	Satellite System	Very High	Open	03/21/2018
Intent Spoof	Satellite System	Very High	Open	03/21/2018
Cellular Traffic Intercept	Satellite System	Very High	Open	03/21/2018
Denial of Service	Satellite System	Very High	Open	03/21/2018
Exploitation of Authorization	Satellite System	Medium	Open	03/21/2018
Identity Spoofing - Impersonation	Satellite System	Medium	Open	03/21/2018
Sniffing Attacks	Satellite System	Medium	Open	03/21/2018
Exploitation of Authentication	Satellite System	Very High	Open	03/21/2018
Denial of Service	Satellite System	Very High	Open	03/21/2018
SQL Injection	Satellite System	High	Open	03/21/2018
Blind SQL Injection	Satellite System	High	Open	03/21/2018
Sensitive Data Exposure	Satellite System	Very High	Open	03/21/2018
HTTP DoS	Satellite System	Very High	Open	03/21/2018
Weak Identity, Credential and Access Management	Satellite System	Very High	Open	03/21/2018
DDOS	Satellite System	Very High	Open	03/21/2018
Session Hijacking	Satellite System	Very High	Open	03/21/2018
Denial of Service through Resource Depletion	Satellite System	Medium	Open	03/21/2018
Protocol Manipulation	Satellite System	Medium	Open	03/21/2018
TCP SYN Scan	Satellite System	Low	Open	03/21/2018
TCP ACK Ping	Satellite System	Low	Open	03/21/2018

TCP SYN Ping	Satellite System	Low	Open	03/21/2018
TCP Connect Scan	Satellite System	Low	Open	03/21/2018
TCP ACK Scan	Satellite System	Low	Open	03/21/2018
Exploit Common or default Usernames and Passwords	Satellite System	High	Open	03/21/2018
WS: XML Denial of Service	Satellite System	Very High	Open	03/21/2018
Gather Information	Satellite System	Very High	Open	03/21/2018
HTTP DoS	Satellite System	Very High	Open	03/21/2018
ICMP Fragmentation	Satellite System	Very High	Open	03/21/2018
Unauthorized Use of Device Resources	Satellite System	Very High	Open	03/21/2018
Denial of Service	Satellite System	Very High	Open	03/21/2018
Eavesdropping	Satellite System	Very High	Open	03/21/2018
Reusing Session IDs aka Session Replay	Satellite System	High	Open	03/21/2018
File Manipulation	Satellite System	Medium	Open	03/21/2018
Accessing, Modifying or Executing Executable Files	Satellite System	Very High	Open	03/21/2018
Create files with the same name as files protected with a higher classification	Satellite System	Very High	Open	03/21/2018
Force Use of Corrupted Files	Satellite System	Medium	Open	03/21/2018
Leveraging or Manipulating Configuration File Search Paths	Satellite System	Very High	Open	03/21/2018
User-Controlled Filename	Satellite System	High	Open	03/21/2018
Manipulating Web Input to File System Calls	Satellite System	Very High	Open	03/21/2018
Identity Spoofing - Impersonation	Satellite System	Medium	Open	03/21/2018
Man in the Middle Attack	Satellite System	Very High	Open	03/21/2018
Targeted Malware	Satellite System	Very High	Open	03/21/2018
Account Footprinting	Satellite System	Very High	Open	03/21/2018
Wi-Fi Jamming	Satellite System	High	Open	03/21/2018
WiFi MAC Address Tracking	Satellite System	Very High	Open	03/21/2018
WiFi SSID Tracking	Satellite System	Very High	Open	03/21/2018
Malware Propagation via USB Stick	Satellite System	Very	Open	03/21/2018

		High		
DEPRECATED: Malware Propagation via USB U3 Autorun	Satellite System	Very High	Open	03/21/2018
DEPRECATED: Malware Propagation via Infected Peripheral Device	Satellite System	Very High	Open	03/21/2018
USB Memory Attacks	Satellite System	High	Open	03/21/2018
Malicious Software Download	Satellite System	Very High	Open	03/21/2018
Content Spoofing	Satellite System	Medium	Open	03/21/2018
Protocol Manipulation	Satellite System	Medium	Open	03/21/2018
Physical Theft	Satellite System	Very High	Open	03/21/2018
Sensitive Data Exposure	Satellite System	Very High	Open	03/21/2018
Brute Force	Satellite System	High	Open	03/21/2018
Password Brute Forcing	Satellite System	High	Open	03/21/2018
Reusing Session IDs aka Session Replay	Satellite System	High	Open	03/21/2018
Denial of Service	Satellite System	Very High	Open	03/21/2018
Verify - Spoofed packet injection	Satellite System	Very High	Open	03/21/2018
SQL Injection	Satellite System	High	Open	03/21/2018
Blind SQL Injection	Satellite System	High	Open	03/21/2018
Session Hijacking	Satellite System	Very High	Open	03/21/2018
Denial of Service through Resource Depletion	Satellite System	Medium	Open	03/21/2018
TCP SYN Scan	Satellite System	Low	Open	03/21/2018
TCP ACK Ping	Satellite System	Low	Open	03/21/2018
TCP SYN Ping	Satellite System	Low	Open	03/21/2018
TCP Connect Scan	Satellite System	Low	Open	03/21/2018
TCP ACK Scan	Satellite System	Low	Open	03/21/2018
Exploit Common or default Usernames and Passwords	Satellite System	High	Open	03/21/2018
WS: XML Denial of Service	Satellite System	Very High	Open	03/21/2018
Gather Information	Satellite System	Very High	Open	03/21/2018
HTTP DoS	Satellite System	Very High	Open	03/21/2018
ICMP Fragmentation	Satellite System	Very High	Open	03/21/2018
Unauthorized Use of Device Resources	Satellite System	Very High	Open	03/21/2018
Eavesdropping	Satellite System	Very	Open	03/21/2018

		High		
Reusing Session IDs aka Session Replay	Satellite System	High	Open	03/21/2018
Encryption Brute Forcing	Satellite System	Low	Open	03/21/2018
Cross Site Request Forgery	Satellite System	Very High	Open	03/21/2018
SQL Injection	Satellite System	High	Open	03/21/2018
Blind SQL Injection	Satellite System	High	Open	03/21/2018
Reflected Cross Site Scripting - WASC	Satellite System	High	Open	03/21/2018
Persistent Cross Site Scripting - WASC	Satellite System	High	Open	03/21/2018
Accessing, Intercepting, Modifying HTTP Cookies	Satellite System	High	Open	03/21/2018
Email Injection	Satellite System	Medium	Open	03/21/2018
IMAP or SMTP Command Injection	Satellite System	Medium	Open	03/21/2018
File Manipulation	Satellite System	Medium	Open	03/21/2018
Accessing, Modifying or Executing Executable Files	Satellite System	Very High	Open	03/21/2018
Create files with the same name as files protected with a higher classification	Satellite System	Very High	Open	03/21/2018
Manipulating Writeable Configuration Files	Satellite System	Very High	Open	03/21/2018
Manipulating Web Input to File System Calls	Satellite System	Very High	Open	03/21/2018
Malware Infection into Product Software	Satellite System	Very High	Open	03/21/2018
Session Hijacking	Satellite System	Very High	Open	03/21/2018
Session Credential Falsification through Forging	Satellite System	Medium	Open	03/21/2018
Reusing Session IDs aka Session Replay	Satellite System	High	Open	03/21/2018
Session Fixation	Satellite System	High	Open	03/21/2018
HTTP Response Splitting	Satellite System	High	Open	03/27/2018
Clickjacking	Satellite System	Very High	Open	03/27/2018