ioXt 2020 Smart Speaker Profile

Version 2.00

Document C-20-06-10
Date 4/9/21
Document Status: Released
Abstract
Keywords

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

1 Notice of Use and Disclosure

Copyright © ioXt Alliance, Inc. (2018 – 2021). All rights Reserved. This information within this document is the property of the ioXt Alliance and its use and disclosure are restricted.

Elements of ioXt Alliance documentation, specifications, and test plans may be subject to third party property rights, including without limitation copyrights and patents. The ioXt Alliance is not responsible and shall not be held responsible in any manner for identifying or failing to identify any or all such third-party intellectual property rights.

This document and information contained herein are provided on a “AS IS” basis.

THE IOXT ALLIANCE DISCLAIMS ALL WARRANTIES EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OF THIRD-PARTIES, OR ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR USE, TITLE, NON INFRINGEMENT, OR GUARANTEE OF PRODUCT SECURITY. IN NO EVENT WILL THE IOXT ALLIANCE BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OF DATA, INTERRUPTION OF BUSINESS, OR FOR ANY OTHER DIRECT, INDIRECT, SPECIAL OR EXEMPLARY, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, IN CONTRACT OR IN TORT, IN CONNECTION WITH THIS DOCUMENT OR THE INFORMATION CONTAINED HEREIN.

The above notice must be included in all copies of this document.

2 Document Version Information

Version	Date	Author	Description
0.1	3/19/20	Brad Ree (ioXt)	Initial Draft
0.12	3/21/20	Brad Ree (ioXt)	1. Updated threats in all sections. 2. Added Device definition
0.13	3/22/20	Kevin Haw (ioXt)	1. Fill out threat model content. 2. "Definitions" section – Add definitions for scopes (single device, local network, fleet). 3. Fixed minor spelling and punctuation errors throughout document.
0.14	3/24/20	Brad Ree (ioXt)	1. Finished threat assessment through compromised device certificate in production phase.
0.15	3/25/20	Brad Ree(ioXt)	1. Filled out content from Ankur
0.16	3/29/20	Bridgette Roberts (ioXt)	1. Formatting Updates
0.17	4/6/20	Brad Ree (ioXt)	1. Inserted blank colored charts for threat model.
0.18	4/7/20	Bridgette Roberts (ioXt)	1. Merged comments from Amit Agrawal- section 7.5, Matt Reyes- section 7.4, 7.7
0.19	4/8/20	Brad Ree (ioXt)	1. Updated 7.4.1 and 7.5.3
0.20	4/10/20	Bridgette Roberts (ioXt)	1. Merged comments from Matt Reyes, Changed device definition (6.1 and 6.2) 2. Changed 7.4, 7.7 Likelihood Medium to Likelihood Moderate 3. Updated various 7.7 Threat Countermeasures
0.21	4/12/20	Bridgette Roberts (ioXt)	1. Merged comments from Amit Agrawal for all section 7.5 threats
0.22	4/13/20	Matt Reyes (ioXt)	1. Modified Threat Evaluation (7.1) to match rest of document 2. Formatted Device Definition (6.1 and 6.2) 3. Corrected Severity Calculation on multiple threats in 7.4 4. Added comments in 7.5
0.23	4/14/20	Matt Reyes (ioXt)	1. Took Ankur and Amit's updates from meeting

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

0.24	4/14/20	Matt Reyes (ioXt)	1. Split up Normal Operation Threats (7.6) into Physical (7.6), Network (7.7) and Functional Attacks (7.8) 2. Fix Formatting 3. Rename *Disposal* to *Reverse Logistics*
0.25	4/17/20	Bridgette Roberts (ioXt)	1. Merged comments from Matt Reyes on evaluation for 7.6 Normal Operation -Physical Attacks
0.26	4/19/20	Bridgette Roberts (ioXt)	1. Merged updates from Amit Agrawal on section 7.5 cleaning up severity levels and threat scenarios. 2. Section 7.7 for network-based attacks.
0.27	4/20/20	Matt Reyes (ioXt)	1. Formatting Updates to 7.4, 7.6
0.28	4/22/20	Matt Reyes (ioXt)	1. Merge updates from Amit Agrawal (7.7) and Ankur Chakraborty (7.8, 7.10) 2. Create Threat Overview Table (7.11)
0.29	4/22/20	Matt Reyes (ioXt)	1. Update Test Cases (8.7) to match Countermeasures 2. Update Threat Model Definitions (7.3)
0.30	4/29/20	Matt Reyes (ioXt)	1. WIP for Comment Resolution
0.31	5/4/20	Matt Reyes (ioXt)	1. Update Test Cases to match those in the library. 2. Format the Threat Model Overview 3. Add the Profile Overview Section 4. Add definitions 5. Added updates from Amit Agrawal & Ankur Chakraborty
0.32	5/4/20	Matt Reyes (ioXt)	1. Filled in Definitions for Impact & Likelihood by Ankur Chakraborty
0.33	5/6/20	Matt Reyes (ioXt)	1. Updated Test cases to match version 2.0 of Test Case Library 2. Formatting clean up. 3. Removed Placeholders.
0.34	5/6/20	Matt Reyes (ioXt)	1. Added Countermeasure chart to Overview (0) 2. Updated SI Countermeasure to 0 to match version 2.0 of Test Case Library

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

0.35	5/10/20	Matt Reyes (ioXt)	1. Modified Test Plan (7) to only include additional test cases not defined in the ioXt 2020 Base Profile.
0.36	5/15/20	Matt Reyes (ioXt)	1. Modified Test Plan to include Levels 2. Indicated the highest severity covered by each test case
0.37	5/19/20	Matt Reyes (ioXt)	1. Changed wording on 7.9
0.38	5/20/20	Matt Reyes (ioXt)	1. Fixed Typo in 8.4.1, Updated 0, Changed CM for 0, Removed SD107
0.39	5/21/20	Matt Reyes (ioXt)	1. Comments from NCC resolved.
0.40	5/21/20	Matt Reyes (ioXt)	1. Harmonize Test Plan with the test case numbering found in Test Case Library 2.08. 2. Comments from NCC resolved
0.41	5/25/20	Matt Reyes (ioXt)	1. Add threats 7.3.10, 7.6.12. 2. Add Levels 5.1
0.42	5/28/20	Matt Reyes (ioXt)	1. Comment Resolution by Compliance WG 2. Clarify Level Overview Table
0.43	5/29/20	Matt Reyes (ioXt)	1. Put threats in Appendix and after Test Plan.
0.44	5/29/20	Matt Reyes (ioXt)	1. Table of Contents Updated
0.45	6/1/20	Matt Reyes (ioXt)	1. Level Overview Table includes all test cases 2. CM for 8.5.4 3. Threat 8.4.7 was incorrectly formatted
0.46	6/9/20	Matt Reyes (ioXt)	1. Remove SI105 from Required Test Cases. 2. VS5 & VS6 Required for Certification Minimum. 3. Change Level Overview Table colors.
0.47	6/10/20	Matt Reyes (ioXt)	1. Update Participants & Document Number
0.48	6/11/20	Matt Reyes (ioXt)	1. SI104 Title Changed
1.00	6/25/20	Matt Reyes (ioXt)	1. Profile Released
2.0	4/4/21	Brad Ree (ioXt)	1. Updated anti-rollback requirements

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

Table of Contents

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

3 Introductions

3.1 Purpose

This document provides the specifications required to certify a device such that the manufacturer may use the ioXt Compliance mark. This specification defines which devices may be certified under the profile, along with the test plan which must be met. The test cases are defined in the ioXt Test Case Library Version 5.0 document.

The Smart Speaker profile shall define the devices which may be certified using the profile, a threat model, and test plan.

ioXt approved labs must be explicitly approved to execute this profile and shall be governed with the ioXt Lab Agreement.

3.2 Acronyms and Abbreviations

Acronym	Definition
VDP	Vulnerability Disclosure Program or Vulnerability Reporting Pledge
AA	Automatically Applied Update Pledge
SE	Security Expiration Date Pledge
VS	Verified Software Pledge
UP	No Universal Password Pledge
PC	Proven Cryptography Pledge
SI	Secured Interface Pledge
CM	Countermeasure

3.3 Definitions

Term	Definition
Threat Modelling	Threat modelling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value.
Likelihood: Physical Access	The attacker has unrestricted physical access to the device.
Likelihood: Proximity Access	The attacker is within radio range. The attacker may be able to see the device, but not touch the device. The attacker may be on the same network.
Likelihood: Remote Access	The attacker is remote to the network and device. The attacker does not have access to the cloud service, or the internet routing network.
Likelihood: Easy	Does not require compromised device. Easily repeatable with methodology
Likelihood: Moderate	Requires non-trivial effort/expense per victim or requires a compromised device

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

Likelihood: Difficult	Requires intimate knowledge of or access to the victim or non-trivial effort or expense
Impact: Low sensitivity data or Denial of Service	Some data is compromised but no sensitive data or control has been compromised.
Impact: Limited sensitive data or control	Some functions of the device are compromised by the threat agent.
Impact: Complete compromise	All functions of the device are compromised by the threat agent.
Impact: Single Device	Only a single device is compromised by some degree.
Impact: Local Network	The local network of the end user has been compromised. The individual device of the end user may also be compromised.
Impact: Complete Fleet	All fielded devices of the given type are subject to compromise. The attack can be scaled for the entire fleet.

Impact	**Definition**
Low	Impact of the threat is limited to local network or single device and low-limited sensitive data
Medium	Impact of the threat can be limited to requiring local network or complete fleet
High	Impact of the threat is wide and can lead to complete compromise

Likelihood	**Definition**
Low	The threat is difficult to execute and may need to be in radio proximity or physical access
Medium	The threat is difficult to moderate to execute and can be done through physical access to remote access
High	The threat is moderate to easy to execute and can be done via proximity or remote access

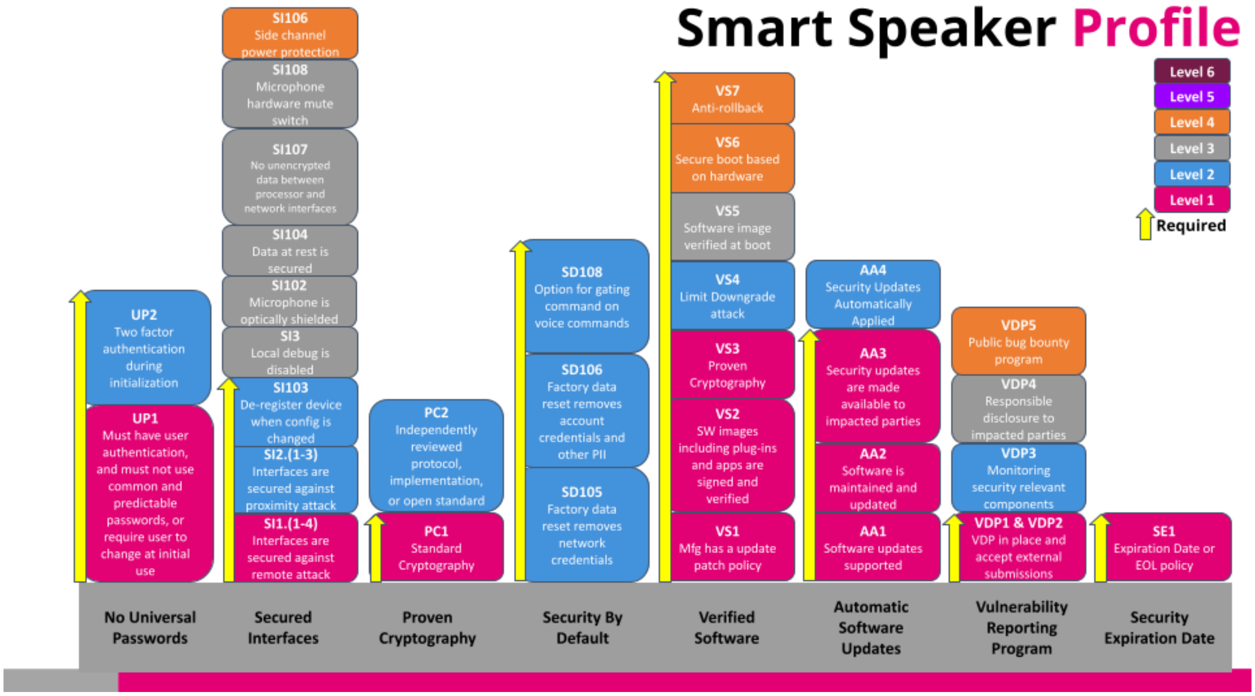
3.4 References

Application Threat Modeling. (n.d.). Retrieved from owasp.org: https://owasp.org/www-community/Application_Threat_Modeling

ioXt 2020 Base Profile. (n.d.). Retrieved from https://ioxtalliancemembers.org/wg/Compliance_wg/document/135

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

4 Profile Overview



Smart Speaker Profile
Level 6
Level 5
Level 4
Level 3
Level 2
Level 1
Required
UP2 Two factor authentication during initialization
UP1 Must have user authentication, and must not use common and predictable passwords, or require user to change at initial use
No Universal Passwords
SI106 Side channel power protection
SI108 Microphone hardware mute switch
SI107 No unencrypted data between processor and network interfaces
SI104 Data at rest is secured
SI102 Microphone is optically shielded
SI3 Local debug is disabled
SI103 De-register device when config is changed
SI2.(1-3) Interfaces are secured against proximity attack
SI1.(1-4) Interfaces are secured against remote attack
Secured Interfaces
PC2 Independently reviewed protocol, implementation, or open standard
PC1 Standard Cryptography
Proven Cryptography
SD108 Option for gating command on voice commands
SD106 Factory data reset removes account credentials and other PII
SD105 Factory data reset removes network credentials
Security By Default
VS7 Anti-rollback
VS6 Secure boot based on hardware
VS5 Software image verified at boot
VS4 Limit Downgrade attack
VS3 Proven Cryptography
VS2 SW images including plug-ins and apps are signed and verified
VS1 Mfg has a update patch policy
Verified Software
AA4 Security Updates Automatically Applied
AA3 Security updates are made available to impacted parties
AA2 Software is maintained and updated
AA1 Software updates supported
Automatic Software Updates
VDP5 Public bug bounty program
VDP4 Responsible disclosure to impacted parties
VDP3 Monitoring security relevant components
VDP1 & VDP2 VDP in place and accept external submissions
Vulnerability Reporting Program
SE1 Expiration Date or EOL policy
Security Expiration Date

4.1 Profile Methodology

This profile contains a Device Definition that specifies which devices are covered.
The process of threat modeling has been followed to identify potential threats against the device. Known threats have been included in Appendix A: Threat Model. Once all potentially known threats have been identified, the severity of each threat was evaluated. Countermeasures to those threats with High or Medium severity were defined and helped determine the Test Plan.

5 Device Definition

5.1 Devices which are in scope

5.1.1 Device MUST include the following:

1. The device MUST have an interface which allows it to be connected to an IP Network.
2. The device MUST include a speaker.
3. The device MUST support audio streaming services from at least one source.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

4. The device MUST include both a physical device and a cloud service in which the device is logically connected through an IP Network.

5.1.2 Device MAY include the following

1. The device MAY include a microphone in which voice commands are received.
2. The device MAY include communications interfaces such as Wi-Fi, BLE, IEEE 802.15.4 and Ethernet.

6 Test Plan

This section defines tests required to address the threats defined in Section 7. Devices covered under the Smart Speaker Profile must pass the tests below in addition to those defined in the ioXt 2020 Base Profile[1].

6.1 Automatic Security Updates

6.1.1 Test Cases

Yardstick ID	Yardstick Name	Test Case #	Test Case Name	Highest Threat Severity
AA4	Security Updates applied automatically, when device usage allows	AA4	Security Updates applied automatically, when device usage allows	Medium

6.1.2 Profile Security Levels

Security Level	Test Cases Required to Pass	Notes
1	ioXt 2020 Base	Certification Minimum
2	AA4	

6.2 Security Expiration Date

6.2.1 Test Cases

There are no additional test cases defined for Security Expiration Date

6.2.2 Profile Security Levels

Security Level	Test Cases Required to Pass	Notes
1	ioXt 2020 Base	Certification Minimum

6.3 Vulnerability Reporting Program

6.3.1 Test Cases

There are no additional test cases defined for Vulnerability Reporting Program

6.3.2 Profile Security Levels

Security Level	Test Cases Required to Pass	Notes

[1] The ioXt 2020 Base Profile can be found at https://ioxtalliancemembers.org/wg/Compliance_wg/document/135

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

1	ioXt 2020 Base	Certification Minimum

6.4 Verified Software

6.4.1 Test Cases

Yardstick ID	Yardstick Name	Test Case #	Test Case Name	Highest Threat Severity
VS4	Limit Downgrade Attack	VS4	Limit Downgrade Attack	
VS5	Software images verified at boot time	VS5	Software images verified at boot time	Medium (NOTE: ioXt recommends this to be included in the Certification Minimum)
VS6	Secure boot based on hardware root of trust	VS6	Secure boot based on hardware root of trust	Medium (NOTE: ioXt recommends this to be included in the Certification Minimum)
VS7	Anti-rollback	VS7	Anti-rollback	

6.4.2 Profile Security Levels

Security Level	Test Cases Required to Pass	Notes
1	ioXt 2020 Base	
2	VS4	
3	VS5	
4	VS6	
4	VS7	Certification Minimum

6.5 No Universal Passwords

6.5.1 Test Cases

Yardstick ID	Yardstick Name	Test Case #	Test Case Name	Highest Threat Severity
UP2	Availability of two factor authentication for devices which have a user facing interface during initialization and management	UP2.1	Availability of two factor authentication for devices which have a user facing interface during initialization	High
		UP2.2	Availability of two factor authentication for devices which have a user facing interface during management	High

6.5.2 Profile Security Levels

Security Level	Test Cases Required to Pass	Notes

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

1	ioXt 2020 Base	
2	UP2.1, UP2.2	Certification Minimum

6.6 Proven Cryptography

6.6.1 Test Cases

There are no additional test cases defined for Proven Cryptography

6.6.2 Profile Security Levels

Security Level	Test Cases Required to Pass	Notes
1	ioXt 2020 Base	Certification Minimum

6.7 Secured Interfaces

6.7.1 Test Cases

Yardstick ID	Yardstick Name	Test Case #	Test Case Name	Highest Threat Severity
SI2	Interfaces are secured against proximity attack	SI2.1	Proximity Attack: Unused Services are disabled	High
		SI2.2	Proximity Attack: Authentication	High
		SI2.3	Proximity Attack: Secured Communications	High
SI3	Interfaces are secured against local attack	SI3.1	Local Attack: Debug ports are disabled	Medium
		SI101	Proximity Attack: Denial of Service Mitigation	Low
		SI102	Microphone shall be optically shielded	Medium
		SI103	De-register device when device configuration is changed (network configuration).	High
		SI104	Securing Data at Rest	Medium
		SI106	Local Attack: Side Channel Power Protection	Medium (NOTE: ioXt recommends this as a higher level of Security due to the complexity in testing)
		SI107	Local Attack: No unencrypted data	Medium

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

			between processor and network interfaces	
		SI108	Microphone shall have the ability to be muted by hardware switch	Medium (NOTE: ioXt recommends this to be included in the Certification Minimum)

6.7.2 Profile Security Levels

Security Level	Test Cases Required to Pass	Notes
1	ioXt 2020 Base	
2	SI2.1, SI2.2, SI2.3, SI103	Certification Minimum
3	SI3.1, SI102, SI104, SI107, SI108	
4	SI106	

6.8 Security by Default

6.8.1 Test Cases

Yardstick ID	Yardstick Name	Test Case #	Test Case Name	Notes
SD1	Security by Default	SD105	Factory Data Reset removes Wi-Fi or any network credentials	High
		SD106	Factory Data Reset removes account token and credentials	High
		SD108	Have option for gating commands on user voice recognition	High

6.8.2 Profile Security Levels

Security Level	Test Cases Required to Pass	Notes
1	None	ioXt Base Profile does not specify test cases for level 1
2	SD105, SD106, SD108	Certification Minimum

6.9 Profile Specific

This profile does not have any profile specific test cases that fall outside the ioXt Yardstick. However, there are further test cases in multiple ioXt Pledge items, such as Security by Default.

ioXt alliance

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7 Appendix A: Threat Model

7.1 Threat Evaluation

7.1.1 Likelihood (Difficulty x Access)

Difficulty ↓ Access →	Physical Access	Proximity Access	Remote Access
Difficult	Low	Medium	Medium
Moderate	Low	Medium	High
Easy	Medium	High	High

7.1.2 Impact (Scope x Data access/control)

Scope ↓ Data Access/Control →	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device	Low	Medium	Medium
Local Network	Low	Medium	High
Complete Fleet	Medium	High	High

7.1.3 Severity (Likelihood x Impact)

Likelihood↓Impact→	Low	Medium	High
Low	Low	Medium	Medium
Medium	Low	Medium	High
High	Medium	High	High

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.2 Supply Chain

7.2.1 Leaked Firmware Obtained from Supply Chain

Threat Description	Device firmware leaked from the factory
Threat Agent	Factory or programming location employee
Resulting Impact	Firmware may be used to create counterfeit devices or analyzed for vulnerabilities.

7.2.1.1 Threat Evaluation

7.2.1.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Moderate	X		
Easy			

7.2.1.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network			
Complete Fleet		X	

7.2.1.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			X
Medium			
High			

7.2.1.2 Countermeasure

ioXt Pledge	Secured Interfaces, Verified Software
Yardstick	SI3, VS6
Test Case	SI104, VS6
Comment	Even if a firmware image gets loaded onto counterfeit hardware, the HW Root of Trust should be present to validate the image.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.2.2 Modified Firmware Inserted in Supply Chain

Threat Description	Firmware modified by attacker and injected into device in factory.
Threat Agent	Factory or programming location employee
Resulting Impact	Infected/compromised devices inserted into trusted supply chain.

7.2.2.1 Threat Evaluation

7.2.2.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	X	🟨	🟨
Moderate	🟩	🟨	🟥
Easy	🟨	🟥	🟥

7.2.2.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	🟩	🟨	🟨
Local Network	🟩	🟨	🟥
Complete Fleet	🟨	🟥	X

7.2.2.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low	🟩	🟨	X
Medium	🟩	🟨	🟥
High	🟨	🟥	🟥

7.2.2.2 Countermeasure

ioXt Pledge	Verified Software
Yardstick	VS2, VS5, VS6
Test Case	
Comments	Required to implement VS6 as the impact is high if malware is inserted at the factory.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.2.3 Modified Bootloader Inserted in Supply Chain

Threat Description	Bootloader modified by attacker injected into device in factory
Threat Agent	Factory or programming location employee
Resulting Impact	Infected/compromised devices inserted into trusted supply chain. This threat is similar to the Modified Firmware Inserted in Supply Chain threat in which the attacker has access to the signing keys or the developer's software libraries.

7.2.3.1 Threat Evaluation

7.2.3.1.1 Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult	X		
Medium			
Easy			

7.2.3.1.2 Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			
Local Network			
Complete Fleet			X

7.2.3.1.3 Severity

Likelihood↓Impact→	Low	Medium	High
Low			X
Medium			
High			

7.2.3.2 Countermeasure

ioXt Pledge	Verified Software
Yardstick	VS2, VS6
Test Case	VS2, VS6
Comment	It is critical that a hardware root of trust used for any device which has high impact or may be manufactured by multiple suppliers. The hardware root key should be programmed in a separate location than the device application code.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.2.4 Counterfeit Device

Threat Description	Counterfeit/unauthorized devices made in factory
Threat Agent	Factory employees/management
Resulting Impact	Lost profit from missed sales of authentic products, risk of infected/compromised devices in market if proper manufacturing/quality procedures not followed. This threat assumes the attacker gained control of the firmware and has made a clone of a single device's image.

7.2.4.1 Threat Evaluation

7.2.4.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	**X**		
Medium			
Easy			

7.2.4.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network			
Complete Fleet		**X**	

7.2.4.1.2.1 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium			
High	**X**		

7.2.4.2 Countermeasure

ioXt Pledge	Verified Software
Yardstick	VS2, VS6
Test Case	VS2, VS6
Comment	A cloned device would require a cloned hardware key in the processor. Also, cloned hardware would not be able to modify the code running on the device.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.2.5 Debug Access in Product Development or Manufacturing

Threat Description	Use of debug interfaces (JTAG, serial debug ports, remote software debuggers) in a trusted environment.
Threat Agent	Factory programming location employee
Resulting Impact	Access to all assets in product by unauthorized actors.

7.2.5.1 Threat Evaluation

7.2.5.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium	**X**		
Easy			

7.2.5.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network			
Complete Fleet		**X**	

7.2.5.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			**X**
Medium			
High			

7.2.5.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI3
Test Case	SI3.1
Comment	The secure boot keys are not accessible from the debug ports. Further, unsigned code will not execute.

7.2.6 Compromised Firmware Signing Key

Threat Description	Firmware signing key is compromised, which allows the attack to load malicious code onto the device.
Threat Agent	Product development.
Resulting Impact	The attacker may inject malicious code into the device.

7.2.6.1 Threat Evaluation

7.2.6.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	**X**		
Medium			
Easy			

7.2.6.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network			
Complete Fleet			**X**

7.2.6.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium			
High	**X**		

7.2.6.2 Countermeasure

ioXt Pledge	None.
Yardstick	
Test Case	
Summary	The device manufacturer must manage their software development process.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.2.7 Compromised Device Certificate

Threat Description	The private key of the device certificate has been leaked in the factory.
Threat Agent	Product development, factory or programming location employee.
Resulting Impact	Key can be used to break encryption of trusted communications or perform following man-in-the-middle attacks. If certificate is unique to device, only that device is compromised.

7.2.7.1 Threat Evaluation

7.2.7.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	**X**		
Medium			
Easy			

7.2.7.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network			
Complete Fleet			**X**

7.2.7.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			**X**
Medium			
High			

7.2.7.2 Countermeasure

ioXt Pledge	Verified Software, Secured Interfaces
Yardstick	VS6, SI3
Test Case	VS6, SI3.1
Comment	Device certificates must be unique to the device to prevent complete fleet attacks.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.2.8 QR codes used for provisioning via BLE or SoftAP mode leaked

Threat Description	The QR code containing the BLE Configuration or SoftAP SSID and passphrase are leaked from the factory
Threat Agent	Product development, factory or programming location employee.
Resulting Impact	Pairing information is leaked.

7.2.8.1 Threat Evaluation

7.2.8.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium	**X**		
Easy			

7.2.8.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	**X**		
Local Network			
Complete Fleet			

7.2.8.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low	**X**		
Medium			
High			

7.2.8.2 Countermeasure

ioXt Pledge	No Universal Passwords
Yardstick	UP1
Test Case	UP1

7.3 Provisioning

7.3.1 Passive Monitoring with Compromised Symmetric Key

Threat Description	After an encryption key has been leaked, third party monitors network traffic to eavesdrop on communications.
Threat Agent	Eavesdropper in Wi-Fi range
Resulting Impact	Sensitive data, possibly including user data, user passwords, or other encryption keys, exposed.

7.3.1.1 Threat Evaluation

7.3.1.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	🟩	🟨	🟨
Medium	🟩	X	🟥
Easy	🟨	🟥	🟥

7.3.1.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	🟩	🟨	🟨
Local Network	🟩	X	🟥
Complete Fleet	🟨	🟥	🟥

7.3.1.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low	🟩	🟨	🟨
Medium	🟩	X	🟥
High	🟨	🟥	🟥

7.3.1.2 Countermeasure

ioXt Pledge	Proven Cryptography, Automatic Updates, Vulnerability Disclosure Program, Verified Software
Yardstick	PC1, AA3, AA4, VDP4, VS3
Test Case	PC1, AA3, AA4, VDP4, VS3

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.3.2 Blocking Device Provisioning

Threat Description	Attacker uses carrier wave jamming or other RF-based data interruption technique to prevent communication between target device and cloud services during provisioning.
Threat Agent	Attacker in close proximity or Wi-Fi range.
Resulting Impact	Device cannot be provisioned, denying user of functionality.

7.3.2.1 Threat Evaluation

7.3.2.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	🟩	🟨	🟨
Medium	🟩	🟨 **X**	🟥
Easy	🟨	🟥	🟥

7.3.2.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	🟩	🟨	🟨
Local Network	🟩 **X**	🟨	🟥
Complete Fleet	🟨	🟥	🟥

7.3.2.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low	🟩	🟨	🟨
Medium	🟩 **X**	🟨	🟥
High	🟨	🟥	🟥

7.3.2.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI2, SI3
Test Case	SI101, SI2.3

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.3.3 Replay Attack During Provisioning

Threat Description	Attacker records encrypted traffic during valid device provisioning and replays it while target device is provisioning to mimic the provisioning (cloud) services.
Threat Agent	Attacker in proximity or Wi-Fi range.
Resulting Impact	Target device believes attacker's endpoint is trusted cloud service, which can then be used to compromise device or data.

7.3.3.1 Threat Evaluation

7.3.3.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		X	
Easy			

7.3.3.1.2 Impact

	Low sensitivity data	**High sensitivity data/control**	**Complete compromise of the device**
Single Device			
Local Network			
Complete Fleet		X	

7.3.3.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium			X
High			

7.3.3.2 Countermeasure

ioXt Pledge	Secured Interfaces, No Universal Passwords
Yardstick	SI2 - Interfaces secured against proximity attack UP2 - Two factor authentication
Test Case	SI2.2, SI2.3, UP2.1

7.3.4 Passive monitoring of Wi-Fi configuration through Bluetooth configuration

Threat Description	Attacker monitors provisioning of device by intercepting Bluetooth communications between device and device user uses to provision (usually a phone or tablet).
Threat Agent	Attacker in Bluetooth range.
Resulting Impact	Sensitive data, possibly including user passwords or other encryption keys, exposed.

7.3.4.1 Threat Evaluation

7.3.4.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		**X**	
Easy			

7.3.4.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			**X**
Local Network			
Complete Fleet	**NA**	**NA**	**NA**

7.3.4.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		**X**	
High			

7.3.4.2 Countermeasure

ioXt Pledge	Secured Interfaces, No Universal Passwords
Yardstick	SI2 - Interfaces secured against proximity attack UP2 - Two factor authentication
Test Case	SI2.2, SI2.3, UP2.1

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.3.5 Passive monitoring of Wi-Fi configuration while device is SoftAP

Threat Description	Attacker monitors provisioning of device by intercepting Wi-Fi communications between device and device user uses to provision (usually a phone or tablet).
Threat Agent	Attacker in Wi-Fi range.
Resulting Impact	Sensitive data, possibly including user passwords or other encryption keys, exposed.

7.3.5.1 Threat Evaluation

7.3.5.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	🟩	🟨	🟨
Medium	🟩	🟨 X	🟥
Easy	🟨	🟥	🟥

7.3.5.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	🟩	🟨	🟨
Local Network	🟩	🟨	🟥 X
Complete Fleet	🟨	🟥	🟥

7.3.5.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low	🟩	🟨	🟨
Medium	🟩	🟨	🟥 X
High	🟨	🟥	🟥

7.3.5.2 Countermeasure

ioXt Pledge	Secured Interfaces, No Universal Passwords
Yardstick	SI2 - Interfaces secured against proximity attack
Test Case	SI2.2, UP2.1

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.3.6 Passive monitoring of Mobile Device when setting up cloud account

Threat Description	Attacker monitors connection between device and Cloud while setting up an account.
Threat Agent	Attacker in proximity or Wi-Fi range.
Resulting Impact	Sensitive data, possibly including user passwords or other encryption keys, exposed.

7.3.6.1 Threat Evaluation

7.3.6.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		**X**	
Easy			

7.3.6.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network		**X**	
Complete Fleet			

7.3.6.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		**X**	
High			

7.3.6.2 Countermeasure

ioXt Pledge	Secured Interfaces, No Universal Passwords
Yardstick	SI2 - Interfaces secured against proximity attack UP2 - Two factor authentication
Test Case	SI2.2, SI2.3, UP2.1

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.3.7 Re-provision from user account to attackers account

Threat Description	Attacker forces deprovisioning of device through factory reset, legitimate re-provisioning mechanism, or existing vulnerability.
Threat Agent	Attacker with physical access to machine (factory reset) or in proximity or remote access.
Resulting Impact	Complete compromise of device. If factory reset or other memory wipe technique not used for attack, sensitive user data may also be exposed.

7.3.7.1 Threat Evaluation

7.3.7.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			**X**
Medium		**X**	
Easy	**X**		

7.3.7.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			**X**
Local Network			**X**
Complete Fleet			

7.3.7.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium			**X**
High			

7.3.7.2 Countermeasure

ioXt Pledge	No Universal Passwords, Secured Interfaces
Yardstick	UP2 – Two factor authentication SI1 – Interfaces are secured against remote attack SI2 – Interfaces are secured against proximity attack
Test Case	UP2.1, SI1.3, SI2.2, SI103

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.3.8 Key Negotiation of Bluetooth attack during configuration of Wi-Fi credentials

Threat Description	Attacker exploits vulnerability in Bluetooth implementation to monitor encrypted traffic during provisioning[2].
Threat Agent	Attacker in Bluetooth range.
Resulting Impact	Sensitive data, possibly including user passwords or other encryption keys, exposed.

7.3.8.1 Threat Evaluation

7.3.8.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		**X**	
Easy			

7.3.8.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device		**X**	
Local Network			
Complete Fleet			

7.3.8.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		**X**	
High			

7.3.8.2 Countermeasure

ioXt Pledge	Proven Cryptography; Secured Interfaces
Yardstick	PC1 – Proven Cryptography SI2 – Interfaces are secured against proximity attack
Test Case	PC1, SI2.2, SI2.3

[2] For an example of this exploit, see The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR, Antonioli, Tippenhauer and Rasmussen, USENIX Security Symposium, August 2019. The corresponding CVE is CVE-2019-9506 (https://nvd.nist.gov/vuln/detail/CVE-2019-9506).

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.3.9 Power interruption during provisioning

Threat Description	Power interruption either halts attempted provisioning or leaves device in indeterminate , vulnerable provisioning state (e.g. no password, using expired certificates, unable to accept new provisioning).
Threat Agent	Unreliable power source, attacker with access to device power.
Resulting Impact	Device maybe in unusable and/or insecure state.

7.3.9.1 Threat Evaluation

7.3.9.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium	**X**		
Easy			

7.3.9.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			**X**
Local Network			
Complete Fleet			

7.3.9.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			**X**
Medium			
High			

7.3.9.2 Countermeasure

ioXt Pledge	None.
Yardstick	
Test Case	
Notes	This threat would leave some implementations in an indeterminate state. Creating requirements on how to solve this would not be security related.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.3.10 Predictable Device IDs Exploited

Threat Description	Attacker iterates through device IDs to assign unpurchased devices to attackers account, such that a new user's device would automatically connect to the attacker's account.
Threat Agent	Remote Attacker
Resulting Impact	Devices connected to the attacker’s account which would give control of the device to the attacker.

7.3.10.1 Threat Evaluation

7.3.10.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	🟩	🟨	🟨
Medium	🟩	🟨	🟥
Easy	🟨	🟥	X

7.3.10.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	🟩	🟨	🟨
Local Network	🟩	🟨	🟥
Complete Fleet	🟨	X	🟥

7.3.10.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low	🟩	🟨	🟨
Medium	🟩	🟨	🟥
High	🟨	🟥	X

7.3.10.2 Countermeasure

ioXt Pledge	No Universal Passwords
Yardstick	UP1
Test Case	UP1

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.4 Normal Operation – Physical Attacks

7.4.1 Attacker reads flash memory for security parameters or sensitive user data

Threat Description	Attacker attempts to extract security parameters or sensitive user data from the flash memory in the device.
Threat Agent	Attacker with physical access to device.
Resulting Impact	Compromise of sensitive user or security data (e.g. encryption keys).

7.4.1.1 Threat Evaluation

7.4.1.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium	X		
Easy			

7.4.1.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device		X	
Local Network			
Complete Fleet			

7.4.1.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low		X	
Medium			
High			

7.4.1.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI3
Test Case	SI104

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.4.2 Attacker monitors external flash to steal certificate

Threat Description	Attacker makes electrical connection to internal flash component within device and extracts a certificate, which may be used to break encrypted traffic or perform following man-in-the-middle attack.
Threat Agent	Attacker with physical access to device who has disassembled unit.
Resulting Impact	Compromise of sensitive user data. Further device and data compromise depending on success of a following man-in-the-middle attack. If certificate is unique to device, only that device is compromised. If common to all devices, entire fleet is compromised.

7.4.2.1 Threat Evaluation

7.4.2.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	**X**	🟨	🟨
Medium	🟩	🟨	🟥
Easy	🟨	🟥	🟥

7.4.2.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	🟩	**X**	🟨
Local Network	🟩	🟨	🟥
Complete Fleet	🟨	🟥	🟥

7.4.2.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low	🟩	🟨	🟨
Medium	**X**	🟨	🟥
High	🟨	🟥	🟥

7.4.2.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI3
Test Case	SI104

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.4.3 Attacker monitors external DRAM to steal certificate

Threat Description	Attacker makes electrical connection to internal DRAM component within device and extracts a certificate, which may be used to break encrypted traffic or perform following man-in-the-middle attack.
Threat Agent	Attacker with physical access to device who has disassembled unit.
Resulting Impact	Compromise of sensitive user data. Further device and data compromise depending on success of a following man-in-the-middle attack. If certificate is unique to device, only that device is compromised. If common to all devices, entire fleet is compromised.

7.4.3.1 Threat Evaluation

7.4.3.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	**X**		
Medium			
Easy			

7.4.3.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device		**X**	
Local Network			
Complete Fleet			

7.4.3.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low		**X**	
Medium			
High			

7.4.3.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI3
Test Case	SI104

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.4.4 Attacker monitors external DRAM to steal session key

Threat Description	Attacker makes electrical connection to internal DRAM component within device and extracts a session key. Key may be used to break encrypted traffic or perform following man-in-the-middle attack.
Threat Agent	Attacker with physical access to device who has disassembled unit.
Resulting Impact	Compromise of sensitive user data. Further device and data compromise depending on success of a following man-in-the-middle attack. Vulnerability ends when session key rotation period expires.

7.4.4.1 Threat Evaluation

7.4.4.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	**X**		
Medium			
Easy			

7.4.4.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device		**X**	
Local Network			
Complete Fleet			

7.4.4.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low		**X**	
Medium			
High			

7.4.4.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI3
Test Case	SI104

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.4.5 Attacker performs side channel attack

Threat Description	Attacker monitors power supply consumption for device and extracts a session key. Key may be used to break encrypted traffic or perform following man-in-the-middle attack. Attacker can also perform glitching and fault injection.
Threat Agent	Attacker with physical access to device who has disassembled unit.
Resulting Impact	Compromise of sensitive user data. Further device and data compromise depending on success of a following man-in-the-middle attack. Vulnerability ends when session key rotation period expires.

7.4.5.1 Threat Evaluation

7.4.5.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	🟩 **X**	🟨	🟨
Medium	🟩	🟨	🟥
Easy	🟨	🟥	🟥

7.4.5.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	🟩	🟨 **X**	🟨
Local Network	🟩	🟨	🟥
Complete Fleet	🟨	🟥	🟥

7.4.5.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low	🟩	🟨 **X**	🟨
Medium	🟩	🟨	🟥
High	🟨	🟥	🟥

7.4.5.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI3
Test Case	SI106

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.4.6 Attacker attempts to control processor through Debug Interfaces

Threat Description	The attacker connects to the JTAG, SWD, UART, BDM or other Debug Interfaces and attempts to bypass secure boot, extract keys, read sensitive memory, etc.
Threat Agent	Attacker with physical access to device who has disassembled unit.
Resulting Impact	Complete device compromise. If recovered certificate is common to all devices, entire fleet is compromised.

7.4.6.1 Threat Evaluation

7.4.6.1.1 Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult	X		
Medium			
Easy			

7.4.6.1.2 Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			
Local Network			
Complete Fleet			X

7.4.6.1.3 Severity

Likelihood↓Impact→	Low	Medium	High
Low			X
Medium			
High			

7.4.6.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI3
Test Case	SI3.1, SI104

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.4.7 Attacker reprograms the device with a completely new image

Threat Description	The attacker reprograms the devices such that it is running a completely new, invalid image.
Threat Agent	Attacker with physical access to device
Resulting Impact	Complete device compromise. Device may be used for man-in-the-middle attack to gain further sensitive user information.

7.4.7.1 Threat Evaluation

7.4.7.1.1 Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult	X		
Medium			
Easy			

7.4.7.1.2 Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			X
Local Network			
Complete Fleet			

7.4.7.1.3 Severity

Likelihood↓Impact→	Low	Medium	High
Low		X	
Medium			
High			

7.4.7.2 Countermeasure

ioXt Pledge	Verified Software
Yardstick	VS5, VS6
Test Case	VS5, VS6

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.4.8 Attacker monitors external radio interface to steal sensitive data

Threat Description	Attacker makes electrical connection to external radio interface component within device and extracts a session key. Key may be used to break encrypted traffic or perform following man-in-the-middle attack
Threat Agent	Attacker with physical access to device who has disassembled unit.
Resulting Impact	Compromise of sensitive user data. Further device and data compromise depending on success of a following man-in-the-middle attack. Vulnerability ends when session key rotation period expires.

7.4.8.1 Threat Evaluation

7.4.8.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	**X**		
Medium			
Easy			

7.4.8.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device		**X**	
Local Network			
Complete Fleet			

7.4.8.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low		**X**	
Medium			
High			

7.4.8.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI3
Test Case	SI104, SI107

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.5 Normal Operation - Network-based Attacks

7.5.1 Constant Carrier Message Jamming

Threat Description	Attacker uses constant RF carrier to jam RF communication.
Threat Agent	Attacker outside network but in RF transmitter range.
Resulting Impact	Critical messages may be dropped to and from device.

7.5.1.1 Threat Evaluation

7.5.1.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		X	
Easy			

7.5.1.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network	X		
Complete Fleet			

7.5.1.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium	X		
High			

7.5.1.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI2 – Interfaces are secured against proximity attack
Test Case	SI101

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.5.2 Message Protocol Jamming

Threat Description	Attacker injects signals over some or all of a message in transit to render one or message checksums or CRCs illegal.
Threat Agent	Attacker outside network but in RF transmitter range.
Resulting Impact	Critical messages may be dropped/rejected to and from device.

7.5.2.1 Threat Evaluation

7.5.2.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		X	
Easy			

7.5.2.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network	X		
Complete Fleet			

7.5.2.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium	X		
High			

7.5.2.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI2 – Interfaces are secured against proximity attack
Test Case	SI101

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.5.3 Network Flood

Threat Description	Valid device floods network with messages.
Threat Agent	Device or firmware defect.
Resulting Impact	Localized network congestion or failure.

7.5.3.1 Threat Evaluation

7.5.3.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			**X**
Medium		**X**	
Easy			

7.5.3.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network		**X**	
Complete Fleet			

7.5.3.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		**X**	
High			

7.5.3.2 Countermeasure

ioXt Pledge	Secured Interfaces, Automatic Security Updates, Verified Software
Yardstick	SI2 – Interfaces are secured against proximity attack AA3 – Security updates made available to impacted parties VS5 – Software images verified at boot time
Test Case	AA3, VS5

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.5.4 Compromised DNS record

Threat Description	Attacker uses “DNS Hijacking” to change the DNS records hosted by third parties to point to a different server than the one the manufacturer intended, thus rerouting traffic from the device to a different address.
Threat Agent	Attacker who has compromised DNS entries for the manufacturer’s intended domain.
Resulting Impact	Traffic to and from cloud server completely rerouted, potentially exposing sensitive user data and/or compromising device.

7.5.4.1 Threat Evaluation

7.5.4.1.1 Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult	🟩	🟨	🟨
Medium	🟩	🟨	🟥 X
Easy	🟨	🟥	🟥

7.5.4.1.2 Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device	🟩	🟨	🟨
Local Network	🟩	🟨	🟥
Complete Fleet	🟨	🟥 X	🟥

7.5.4.1.3 Severity

Likelihood↓Impact→	Low	Medium	High
Low	🟩	🟨	🟨
Medium	🟩	🟨	🟥
High	🟨	🟥	🟥 X

7.5.4.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI1
Test Case	SI1.3, SI1.4

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.5.5 Message Exploit

Threat Description	Attacker crafts message to exploit vulnerability in target device firmware.
Threat Agent	Attacker inside network or attacker outside network but within RF transmitter range.
Resulting Impact	Denial of service from device or device compromise.

7.5.5.1 Threat Evaluation

7.5.5.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	🟩	🟨 **X**	🟨
Medium	🟩	🟨	🟥
Easy	🟨	🟥	🟥

7.5.5.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	🟩	🟨 **X**	🟨
Local Network	🟩	🟨	🟥
Complete Fleet	🟨	🟥	🟥

7.5.5.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low	🟩	🟨	🟨
Medium	🟩	🟨 **X**	🟥
High	🟨	🟥	🟥

7.5.5.2 Countermeasure

ioXt Pledge	Secured Interfaces, Automatic Security Updates, Vulnerability Reporting Program
Yardstick	SI2 – Interfaces are secured against proximity attack AA2 – Software is Maintained and Updated AA3 – Security updates made available to impacted parties
Test Case	SI2.2, SI2.3, AA2, AA3

7.5.6 Compromised router gateway address

Threat Description	Gateway address in device is corrupted.
Threat Agent	Configuration error or attacker exploiting vulnerability causing configuration error.
Resulting Impact	Device is unable to access the Internet outside the local network.

7.5.6.1 Threat Evaluation

7.5.6.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		X	
Easy			

7.5.6.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network	X		
Complete Fleet			

7.5.6.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium	X		
High			

7.5.6.2 Countermeasure

ioXt Pledge	Secured Interface, Verified Software
Yardstick	SI2 – Interfaces are secured against proximity attack VS2 – Software images including plug-ins and apps are signed and verified VS5 – Software images verified at boot time
Test Case	SI2.2, SI2.3, VS2, VS5

7.5.7 Replay attack on messages from device towards cloud

Threat Description	Attacker records traffic from device to cloud service and then replays traffic at a later time. Attacker attempts to deceive cloud service into believing attacker's device is the target device.
Threat Agent	Attacker in network path between device and cloud.
Resulting Impact	Compromise of sensitive user data. May fool cloud service into believing that security updates have been applied to device when they have not.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.5.7.1 Threat Evaluation

7.5.7.1.1 Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			X
Medium		X	
Easy			

7.5.7.1.2 Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device		X	
Local Network			
Complete Fleet			

7.5.7.1.3 Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium		X	
High			

7.5.7.2 Countermeasure

ioXt Pledge	Secured Interface, Proven Cryptography
Yardstick	SI1 – Interfaces are secured against remote attack SI2 – Interfaces are secured against proximity attack PC1 – Standard Cryptography
Test Case	SI1.1, SI1.2, SI1.4, SI2.1, SI2.3, PC1

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.5.8 Unauthorized Device Deprovisioning

Threat Description	Attacker causes device to de-register or de-provision over network by exploiting vulnerability or masquerading as cloud service.
Threat Agent	Attacker inside network.
Resulting Impact	Target device may be configured to deny service or prevent reporting of critical events.

7.5.8.1 Threat Evaluation

7.5.8.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult		**X**	
Medium			
Easy			

7.5.8.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			**X**
Local Network			
Complete Fleet			

7.5.8.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			**X**
Medium			
High			

7.5.8.2 Countermeasure

ioXt Pledge	No Universal Passwords Secured Interfaces
Yardstick	UP2 – Two factor authentication SI2 - Interfaces secured against proximity attack
Test Case	SI2.2, SI2.3, UP2, SI103

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.5.9 Replay attack on messages from cloud to device

Threat Description	Attacker records traffic from cloud service to device and then replays traffic at a later time. Attacker attempts to deceive device into believing attacker's device is cloud service.
Threat Agent	Attacker in network path between device and cloud.
Resulting Impact	Compromise of sensitive user data. Compromise of device.

7.5.9.1 Threat Evaluation

7.5.9.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			**X**
Medium		**X**	
Easy			

7.5.9.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			**X**
Local Network			**X**
Complete Fleet			**X**

7.5.9.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium			**X**
High			

7.5.9.2 Countermeasure

ioXt Pledge	Secured Interfaces, Proven Cryptography
Yardstick	SI1 – Interfaces are secured against remote attack PC1 – Standard Cryptography
Test Case	SI1.1, SI1.2, SI1.4, PC1

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.5.10 Compromised session key

Threat Description	Attacker compromises the session key between device and cloud service, which may be used to break encrypted traffic or perform following man-in-the-middle attack .
Threat Agent	Attacker in network path between device and cloud.
Resulting Impact	Compromise of sensitive user data. Further device and data compromise depending on success of a following man-in-the-middle attack. Vulnerability ends when session key rotation period expires.

7.5.10.1 Threat Evaluation

7.5.10.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			**X**
Medium		**X**	
Easy			

7.5.10.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device		**X**	
Local Network		**X**	
Complete Fleet		**X**	

7.5.10.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium			**X**
High			

7.5.10.2 Countermeasure

ioXt Pledge	Secured Interfaces, Proven Cryptography
Yardstick	SI1 – Interfaces are secured against remote attack PC1 – Standard Cryptography
Test Case	SI1.1, SI1.2, SI1.4, PC1

7.5.11 Local man in the middle attack during voice command to cloud

Threat Description	Attacker intercepts traffic between device and cloud over local network while a voice command is being issued.
Threat Agent	Attacker in network path between device and cloud.
Resulting Impact	Attacker can deny service to device, preventing it from performing requested command. Attacker can inject their own command.

7.5.11.1 Threat Evaluation

7.5.11.1.1 Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			X
Medium		X	
Easy			

7.5.11.1.2 Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			X
Local Network			X
Complete Fleet			

7.5.11.1.3 Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium			X
High			

7.5.11.2 Countermeasure

ioXt Pledge	Secured Interfaces, Proven Cryptography
Yardstick	SI1 – Interfaces are secured against remote attack SI2 – Interfaces are secured against proximity attack PC1 – Standard Cryptography
Test Case	SI1.1, SI1.2, SI1.4, SI2.2, SI2.3, PC1

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.5.12 Local man in the middle attack during audio stream from cloud to device

Threat Description	Attacker intercepts traffic between device and cloud over local network while audio is being streamed.
Threat Agent	Attacker in network path between device and cloud.
Resulting Impact	Attacker can deny service to device, preventing it from performing streaming requested audio.

7.5.12.1 Threat Evaluation

7.5.12.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		**X**	
Easy			

7.5.12.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network		**X**	
Complete Fleet			

7.5.12.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		**X**	
High			

7.5.12.2 Countermeasure

ioXt Pledge	Secured Interfaces, Proven Cryptography
Yardstick	SI2 – Interfaces are secured against proximity attack PC1 – Standard Cryptography
Test Case	SI2.2, SI2.3, PC1

7.5.13 Local man in the middle attack during notifications sent from cloud to device

Threat Description	Attacker intercepts traffic between device and cloud over local network while cloud is issuing notifications to device.
Threat Agent	Attacker in network path between device and cloud.
Resulting Impact	Attacker can stop notifications from being received by device or inject own notices. This can be used to prevent notifications of important events such as alarms or to postpone device form requesting security upgrades.

7.5.13.1 Threat Evaluation

7.5.13.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		**X**	
Easy			

7.5.13.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network		**X**	
Complete Fleet			

7.5.13.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		**X**	
High			

7.5.13.1.4 Countermeasure

ioXt Pledge	Secured Interfaces, Proven Cryptography
Yardstick	SI2 – Interfaces are secured against proximity attack PC1 – Standard Cryptography
Test Case	SI2.2, SI2.3, PC1

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.5.14 Attacker uses brute force attack to steal session key

Threat Description	Attacker monitors encrypted traffic and then performs brute force cryptographic attack to extract a session key. Key may be used to break encrypted traffic or perform following man-in-the-middle attack.
Threat Agent	Attacker in network path between device and cloud.
Resulting Impact	Compromise of sensitive user data. Further device and data compromise depending on success of a following man-in-the-middle attack. Vulnerability ends when session key rotation period expires.

7.5.14.1 Threat Evaluation

7.5.14.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult		**X**	
Medium	**X**		
Easy			

7.5.14.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device		**X**	
Local Network		**X**	
Complete Fleet			

7.5.14.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium	**X**		
High			

7.5.14.2 Countermeasure

ioXt Pledge	Secured Interfaces, Proven Cryptography
Yardstick	SI2 – Interfaces are secured against proximity attack SI3 – Interfaces are secured against physical attack PC1 – Standard Cryptography
Test Case	SI2.2, SI2.3, SI3.1, PC1

7.5.15 Attacker monitor’s Wi-Fi radio interface to steal network SSID and passphrase

Threat Description	Attacker passively monitors Wi-Fi traffic during connection and reconnection to extract network SSID and passphrase. Unless Wi-Fi access point was set up without encryption, a following cryptographic attack must be made to exploit captured traffic.
Threat Agent	Attacker in Wi-Fi range of device.
Resulting Impact	User’s local network SSID and passphrase compromised.

7.5.15.1 Threat Evaluation

7.5.15.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult		**X**	
Medium			
Easy			

7.5.15.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network		**X**	
Complete Fleet			

7.5.15.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		**X**	
High			

7.5.15.2 Countermeasure

ioXt Pledge	Secured Interfaces, Proven Cryptography
Yardstick	SI2 – Interfaces are secured against proximity attack PC1 – Standard Cryptography
Test Case	SI2.2, SI2.3, PC1

7.6 Normal Operation - Functional Attacks

7.6.1 Attacker pairs smart speaker to their device

Threat Description	Attacker pairs with device over phone, tablet, or other device controlled by attacker.
Threat Agent	Attacker in physical proximity to device.
Resulting Impact	Attacker can control device and may be able to retrieve sensitive user data.

7.6.1.1 Threat Evaluation

7.6.1.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	🟩	🟨	🟨
Medium	🟩	🟨	🟥
Easy	🟨	🟥 **X**	🟥

7.6.1.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	🟩	🟨	🟨 **X**
Local Network	🟩	🟨	🟥
Complete Fleet	🟨	🟥	🟥

7.6.1.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low	🟩	🟨	🟨
Medium	🟩	🟨	🟥
High	🟨	🟥 **X**	🟥

7.6.1.2 Countermeasure

ioXt Pledge	Secure by Default
Yardstick	SD1
Test Case	SD105, SD106

7.6.2 Nonverbal attack on microphone to issue non-critical commands to home devices (such as turn off light)

Threat Description	Attacker uses laser[3] or subsonic[4] techniques to issue audio commands to the device that cannot be heard with human hearing. Any users present will hear audio responses/confirmations from device. Attacker uses this exploit to issue non-critical commands.
Threat Agent	Attacker with line of sight on device, possibly through windows.
Resulting Impact	Attacker issues non-critical commands to device.

7.6.2.1 Threat Evaluation

7.6.2.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult		**X**	
Medium			
Easy			

7.6.2.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device		**X**	
Local Network			
Complete Fleet			

7.6.2.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		**X**	
High			

7.6.2.2 Countermeasure

ioXt Pledge	Secured Interfaces

[3] For an example of this attack, see Light Commands: Laser-Based Audio InjectionAttacks on Voice-Controllable Systems, Sugawara, Cyr, Rampazzi, November 2019.

[4] For an example of this attack, see DolphinAttack: Inaudible Voice Commands, Zhang, Yan, and Ji, CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, October 2017, pages 103–117.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

Yardstick	SI3
Test Case	SI102

7.6.3 Nonverbal attack on microphone to adjust account settings

Threat Description	Attacker uses laser or subsonic techniques to issue audio commands to the device that cannot be heard with human hearing. Any users present will hear audio responses/confirmations from device. Attacker uses this exploit to adjust account settings.
Threat Agent	Attacker with line of sight on device, possibly through windows.
Resulting Impact	Possible change of account security settings, making compromise of sensitive user data or device compromise easier.

7.6.3.1 Threat Evaluation

7.6.3.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult		**X**	
Medium			
Easy			

7.6.3.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			**X**
Local Network			
Complete Fleet			

7.6.3.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		**X**	
High			

7.6.3.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI3
Test Case	SI102

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.6.4 Nonverbal attack on microphone to issue critical commands to home devices (such as unlock door)

Threat Description	Attacker uses laser or subsonic techniques to issue audio commands to the device that cannot be heard with human hearing. Any users present will hear audio responses/confirmations from device. Attacker uses this exploit to issue critical commands.
Threat Agent	Attacker with line of sight on device, possibly through windows.
Resulting Impact	Possible compromise of sensitive user data or user physical security. Possible complete compromise of device.

7.6.4.1 Threat Evaluation

7.6.4.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult		X	
Medium			
Easy			

7.6.4.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			X
Local Network			
Complete Fleet			

7.6.4.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		X	
High			

7.6.4.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI3
Test Case	SI102

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.6.5 Attacker uses his voice to issue non-critical commands to home devices

Threat Description	Attacker uses voice to issue audio commands to the device that can be detected with human hearing. Any users present will hear audio responses/confirmations from device. Attacker uses this exploit to issue non-critical commands.
Threat Agent	Attacker in close physical proximity of device.
Resulting Impact	Attacker issues non-critical commands to device.

7.6.5.1 Threat Evaluation

7.6.5.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		**X**	
Easy			

7.6.5.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	**X**		
Local Network			
Complete Fleet			

7.6.5.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium	**X**		
High			

7.6.5.2 Countermeasure

ioXt Pledge	None, Low Severity Issue.
Yardstick	
Test Case	

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.6.6 Attacker uses his voice to adjust account settings

Threat Description	Attacker uses voice to issue audio commands to the device that can be detected with human hearing. Any users present will hear audio responses/confirmations from device. Attacker uses this exploit to adjust device account settings.
Threat Agent	Attacker in close physical proximity of device.
Resulting Impact	Possible change of account security settings, making compromise of sensitive user data or device compromise easier.

7.6.6.1 Threat Evaluation

7.6.6.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		**X**	
Easy			

7.6.6.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			**X**
Local Network			
Complete Fleet			

7.6.6.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		**X**	
High			

7.6.6.2 Countermeasure

ioXt Pledge	Secure by Default, Universal Passwords
Yardstick	UP2, SD1
Test Case	UP2.2, SD108

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.6.7 Attacker uses his voice to issue critical commands to home devices

Threat Description	Attacker uses voice to issue audio commands to the device that can be detected with human hearing. Any users present will hear audio responses/confirmations from device. Attacker uses this exploit to issue critical commands.
Threat Agent	Attacker in close physical proximity of device.
Resulting Impact	Possible compromise of sensitive user data or user physical security. Possible complete compromise of device.

7.6.7.1 Threat Evaluation

7.6.7.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		X	
Easy			

7.6.7.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			X
Local Network			
Complete Fleet			

7.6.7.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		X	
High			

7.6.7.2 Countermeasure

ioXt Pledge	Secure by Default
Yardstick	SD1
Test Case	SD106

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.6.8 Attacker uses recording of user's voice to issue non-critical commands to home devices

Threat Description	Attacker uses recording of user's voice to issue audio commands to the device that can be detected with human hearing. Any users present will hear audio responses/confirmations from device. Attacker uses this exploit to issue non-critical commands.
Threat Agent	Attacker or attacker device in close physical proximity of device.
Resulting Impact	Attacker issues non-critical commands to device.

7.6.8.1 Threat Evaluation

7.6.8.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium			
Easy		**X**	

7.6.8.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	**X**		
Local Network			
Complete Fleet			

7.6.8.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium			
High	**X**		

7.6.8.2 Countermeasure

ioXt Pledge	NOTE: Medium Severity, Recommend no Countermeasure.
Yardstick	
Test Case	

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.6.9 Attacker uses recording of user’s voice to adjust account settings

Threat Description	Attacker uses recording of user’s voice to issue audio commands to the device that can be detected with human hearing. Any users present will hear audio responses/confirmations from device. Attacker uses this exploit to issue non-critical commands.
Threat Agent	Attacker or attacker device in close physical proximity of device.
Resulting Impact	Possible change of account security settings, making compromise of sensitive user data or device compromise easier.

7.6.9.1 Threat Evaluation

7.6.9.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium			
Easy		**X**	

7.6.9.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			**X**
Local Network			
Complete Fleet			

7.6.9.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium			
High		**X**	

7.6.9.2 Countermeasure

ioXt Pledge	No Universal Passwords
Yardstick	UP2
Test Case	UP2.2

7.6.10 Attacker uses recording of user’s voice to issue critical commands to home devices

Threat Description	Attacker uses recording of user’s voice to issue audio commands to the device that can be detected with human hearing. Any users present will hear audio responses/confirmations from device. Attacker uses this exploit to issue critical commands.
Threat Agent	Attacker or attacker device in close physical proximity of device.
Resulting Impact	Possible compromise of sensitive user data or user physical security. Possible complete compromise of device.

7.6.10.1 Threat Evaluation

7.6.10.1.1 Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult	🟩	🟨	🟨
Medium	🟩	🟨	🟥
Easy	🟨	X	🟥

7.6.10.1.2 Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device	🟩	🟨	X
Local Network	🟩	🟨	🟥
Complete Fleet	🟨	🟥	🟥

7.6.10.1.3 Severity

Likelihood↓Impact→	Low	Medium	High
Low	🟩	🟨	🟨
Medium	🟩	🟨	🟥
High	🟨	X	🟥

7.6.10.2 Countermeasure

ioXt Pledge	Secure by Default
Yardstick	SD1
Test Case	SD108

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.7 Device Upgrade

7.7.1 Image Rollback

Threat Description	The attacker has compromised the cloud upgrade service and attempts to roll back the version of code running on the device.
Threat Agent	Firmware error or attacker inside network.
Resulting Impact	Security patches may be lost.

7.7.1.1 Threat Evaluation

7.7.1.1.1 Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult	🟩	🟨	🟨 X
Moderate	🟩	🟨	🟥
Easy	🟨	🟥	🟥

7.7.1.1.2 Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device	🟩	🟨	🟨
Local Network	🟩	🟨	🟥
Complete Fleet	🟨	🟥	🟥 X

7.7.1.1.3 Severity

Likelihood↓Impact→	Low	Medium	High
Low	🟩	🟨	🟨
Medium	🟩	🟨	🟥 X
High	🟨	🟥	🟥

7.7.1.2 Countermeasure

ioXt Pledge	Verified Software
Yardstick	VS2, VS3, VS5, VS6
Test Case	VS2, VS3, VS5, VS6

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.7.2 Firmware Update Service is spoofed and invalid image sent to the device

Threat Description	Cloud service is spoofed, device receives update from that a malicious update service .
Threat Agent	Man in the middle with poisoned DNS records
Resulting Impact	Device received compromised firmware - may be used to attack other devices.

7.7.2.1 Threat Evaluation

7.7.2.1.1 Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			X
Medium			
Easy			

7.7.2.1.2 Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			
Local Network			
Complete Fleet			X

7.7.2.1.3 Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium			X
High			

7.7.2.2 Countermeasure

ioXt Pledge	Verified Software
Yardstick	VS2, VS5
Test Case	VS2, VS5

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.7.3 Attacker attempts to modify the bootloader to bypass secured image

Threat Description	The attacker modifies the bootloader image on the device with the goal of loading a corrupt image.
Threat Agent	Malware with limited security privileges.
Resulting Impact	Malware has increased security privileges, completely compromising device.

7.7.3.1 Threat Evaluation

7.7.3.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	**X**		
Medium			
Easy			

7.7.3.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			**X**
Local Network			
Complete Fleet			

7.7.3.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low		**X**	
Medium			
High			

7.7.3.2 Countermeasure

ioXt Pledge	Verified Software
Yardstick	VS2, VS6
Test Case	VS2, VS6

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.7.4 Update Blocked

Threat Description	Denial of service attack prevents upgrade of target device.
Threat Agent	Attacker inside network or attacker outside network but within RF transmitter range.
Resulting Impact	Security patches could be blocked.

7.7.4.1 Threat Evaluation

7.7.4.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		**X**	
Easy			

7.7.4.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network	**X**		
Complete Fleet			

7.7.4.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium	**X**		
High			

7.7.4.2 Countermeasure

ioXt Pledge	Secured Interfaces
Yardstick	SI2
Test Case	SI101

7.8 Reverse Logistics

7.8.1 Obsolete Device Reused

Threat Description	Device marked for destruction due to end of life or known defect reused.
Threat Agent	Installer, end user, or return agent
Resulting Impact	Obsolete or devices with known security defects may reenter the device ecosystem.

7.8.1.1 Threat Evaluation

7.8.1.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium	**X**		
Easy			

7.8.1.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			**X**
Local Network			
Complete Fleet			

7.8.1.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low		**X**	
Medium			
High			

7.8.1.2 Countermeasure

ioXt Pledge	Automatic Updates, Security Expiration Date
Yardstick	AA4, SE1
Test Case	AA4, SE1.1

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.8.2 Device Sensitive Information Recovered from Discarded Device

Threat Description	Security information such as encryption keys are extracted from a discarded device.
Threat Agent	Installer, end user, return agent, or attacker retrieving device from trash.
Resulting Impact	Information may be used in future attacks.

7.8.2.1 Threat Evaluation

7.8.2.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult	🟩	🟨	🟨
Medium	🟩	🟨	🟥
Easy	🟨 **X**	🟥	🟥

7.8.2.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	🟩	🟨	🟨 **X**
Local Network	🟩	🟨	🟥
Complete Fleet	🟨	🟥	🟥

7.8.2.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low	🟩	🟨	🟨
Medium	🟩	🟨 **X**	🟥
High	🟨	🟥	🟥

7.8.2.2 Countermeasure

ioXt Pledge	Security by Default
Yardstick	SD1
Test Case	SD105, SD106

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.8.3 Device Image Recovered from Discarded Device or Online

Threat Description	Device firmware is extracted from a discarded device or retrieved from a firmware update server.
Threat Agent	Installer, end user, return agent, or attacker retrieving device from trash or from a firmware update server
Resulting Impact	Firmware may be used to create counterfeit devices or analyzed for vulnerabilities.

7.8.3.1 Threat Evaluation

7.8.3.1.1 Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult	🟩	🟨	🟨
Medium	🟩	🟨	🟥
Easy	🟨 X	🟥	🟥

7.8.3.1.2 Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device	🟩 X	🟨	🟨
Local Network	🟩	🟨	🟥
Complete Fleet	🟨	🟥	🟥

7.8.3.1.3 Severity

Likelihood↓Impact→	Low	Medium	High
Low	🟩	🟨	🟨
Medium	🟩 X	🟨	🟥
High	🟨	🟥	🟥

7.8.3.2 Countermeasure

ioXt Pledge	NOTE: Low Severity, no countermeasure recommended.
Yardstick	
Test Case	

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.8.4 Attacker reads flash memory in to read User Data from Discarded Device

Threat Description	The attacker reads the flash memory of a discarded device with the goal of reading user data.
Threat Agent	Installer, end user, return agent, or attacker retrieving device from trash.
Resulting Impact	Compromise of user data.

7.8.4.1 Threat Evaluation

7.8.4.1.1 Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium			
Easy	**X**		

7.8.4.1.2 Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			**X**
Local Network			
Complete Fleet			

7.8.4.1.3 Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium		**X**	
High			

7.8.4.2 Countermeasure

ioXt Pledge	Security by Default
Yardstick	SD1
Test Case	SD105, SD106

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

7.9 Overview

This section categorizes the threats in the model based on severity. Each one is a clickable reference to each threat's details.

7.9.1 High Severity Threats

Section	Title	CM Available
8.3.3	Replay Attack During Provisioning	Y
8.3.5	Passive monitoring of Wi-Fi configuration while device is SoftAP	Y
8.3.7	Re-provision from user account to attackers account	Y
8.3.9	Power interruption during provisioning	Y
8.5.3	Network Flood	Y
8.5.4	Compromised DNS record	Y
8.5.8	Unauthorized Device Deprovisioning	Y
8.5.9	Replay attack on messages from cloud to device	Y
8.5.10	Compromised session key	Y
8.5.11	Local man in the middle attack during voice command to cloud	Y
8.6.1	Attacker pairs smart speaker to their device	Y
8.6.9	Attacker uses recording of user's voice to adjust account settings	Y
8.6.10	Attacker uses recording of user's voice to issue critical commands to home devices	Y
8.7.1	Image Rollback	Y
8.7.2	Firmware Update Service is spoofed and invalid image sent to the device	Y

7.9.2 Medium Severity Threats

Section	Title	CM Available
8.2.1	Leaked Firmware Obtained from Supply Chain	Y
8.2.2	Modified Firmware Inserted in Supply Chain	Y
8.2.3	Modified Bootloader Inserted in Supply Chain	Y
8.2.4	Counterfeit Device	Y
8.2.5	Debug Access in Product Development or Manufacturing	Y
8.2.6	Compromised Firmware Signing Key *NOTE: The private key must be guarded, however a countermeasure against a rogue developer is out of scope for this profile.*	N
8.2.7	Compromised Device Certificate	Y
8.3.1	Passive Monitoring with Compromised Symmetric Key	Y
8.3.4	Passive monitoring of Wi-Fi configuration through Bluetooth configuration	Y

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

8.3.6	Passive monitoring of Mobile Device when setting up cloud account	Y
8.3.8	Key Negotiation of Bluetooth attack during configuration of Wi-Fi credentials	Y
8.3.9	Power interruption during provisioning	
8.4.3	Attacker monitors external DRAM to steal certificate	Y
8.4.4	Attacker monitors external DRAM to steal session key	Y
8.4.5	Attacker performs side channel attack	Y
8.4.6	Attacker attempts to control processor through Debug Interfaces	Y
8.4.7	Attacker reprograms the device with a completely new image	Y
8.4.8	Attacker monitors external radio interface to steal sensitive dataAttacker monitors external radio interface to steal sensitive data	Y
8.5.5	Message ExploitMessage Exploit	Y
8.5.7	Replay attack on messages from device towards cloud	Y
8.5.12	Local man in the middle attack during audio stream from cloud to device	Y
8.5.13	Local man in the middle attack during notifications sent from cloud to device	Y
8.5.15	Attacker monitor’s Wi-Fi radio interface to steal network SSID and passphrase	Y
8.6.2	Nonverbal attack on microphone to issue non-critical commands to home devices (such as turn off light)	Y
8.6.3	Nonverbal attack on microphone to adjust account settings	Y
8.6.4	Nonverbal attack on microphone to issue critical commands to home devices (such as unlock door)	Y
8.6.6	Attacker uses his voice to adjust account settings	Y
8.6.7	Attacker uses his voice to issue critical commands to home devices	Y
8.6.8	Attacker uses recording of user’s voice to issue non-critical commands to home devices *NOTE: Defining a CM is out of scope.*	N
8.7.3	Attacker attempts to modify the bootloader to bypass secured image	Y
8.8.1	Obsolete Device Reused	Y
8.8.2	Device Sensitive Information Recovered from Discarded Device	Y

This document is confidential and contains proprietary information and intellectual property of ioXt Alliance, Inc. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of ioXt Alliance, Inc.

8.8.4	Attacker reads flash memory in to read User Data from Discarded Device	Y

7.9.3 Low Severity Threats

Section	Title	CM Available
8.2.8	QR codes used for provisioning via BLE or SoftAP mode leaked	Y
8.3.2	Blocking Device Provisioning	Y
8.4.2	Attacker monitors external flash to steal certificate	Y
8.5.1	Constant Carrier Message Jamming	Y
8.5.2	Message Protocol Jamming	Y
8.5.6	Compromised router gateway address	Y
8.5.14	Attacker uses brute force attack to steal session key	Y
8.6.5	Attacker uses his voice to issue non-critical commands to home devices	N
8.7.4	Update Blocked	Y
8.8.3	Device Image Recovered from Discarded Device or Online	N