WINC1500 Software

Release Notes

VERSION :	**19.5.4**
DATE :	**OCT 4, 2017**

Abstract

This document presents an overview of the WINC1500 firmware release version 19.5.4, and corresponding driver.

1 Introduction

This document describes the WINC1500 version 19.5.4 release package.

The release package contains all the necessary components (binaries and tools) required to make use of the latest features including tools, and firmware binaries.

1.1 Firmware readiness

Microchip Technology Inc. considers version 19.5.4 firmware to be suitable for production release.

2 Changes since the last release (version 19.5.3)

2.1 New Features

- WLAN:
  - Protect against WPA2 key re-installation attack
- Network Stack:
  - Use well known public NTP pools to obtain time

2.2 Issues Fixed

  - Interoperability issues involving ARRIS TG862G/CT (Xfinity XFI) routers
  - Ensure m2m_wifi_set_tx_power() API works as expected in all cases

2.3 Release Comparison

Features in 19.5.3	Changes in 19.5.4
Wi-Fi STA	
• IEEE 802.11 b/g/n. • OPEN, WEP security. • WPA Personal Security (WPA1/WPA2). • WPA Enterprise Security (WPA1/WPA2) supporting EAP-TTLS/MS-Chapv2.0 authentication with RADIUS server.	• Protect against key re-installation attacks forcing NONCE re-use. • Fix m2m_wifi_set_tx_power() to work in all cases • Fix interopability issues with ARRIS TG862G/CT (Xfinity XFI) access point
Wi-Fi Hotspot	
• Only ONE associated station is supported. After a connection is established with a station, further connections are rejected. • OPEN and WEP, WPA2 security modes. • The device cannot work as a station in this mode (STA/AP Concurrency is not supported).	No change.
Wi-Fi Direct	
• Wi-Fi direct client is not supported.	No change
WPS	
The WINC1500 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods.	No change
TCP/IP Stack	
The WINC1500 has a TCP/IP Stack running in firmware side. It supports TCP and UDP full socket operations (client/server). The maximum number of supported sockets is currently configured to 11 divided as: • 7 TCP sockets (client or server). • 4 UDP sockets (client or server).	No change

Features in 19.5.3	Changes in 19.5.4
Transport Layer Security	
• Support TLS v1.2. • Client and server modes. • Mutual authentication. • X509 certificate revocation scheme. • Add SHA384 and SHA512 support in X509 certificates processing. • Integration with ATECC508 (Add ECDSA/ECHE support). • Certificate revocation check API. • Disable Support of DH groups larger than 2048 bits. • Supported cipher suites are: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (requires ECC508) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (requires ATECC508)	No change
Networking Protocols	
DHCPv4 (client/server) DNS Resolver IGMPv1, v2. SNTP	Use NTP server pools instead of specific servers.

Features in 19.5.3	**Changes in 19.5.4**
Power saving Modes	
• M2M_PS_MANUAL • M2M_PS_AUTOMATIC • M2M_PS_H_AUTOMATIC • M2M_PS_DEEP_AUTOMATIC	No change
Device Over-The-Air (OTA) upgrade	
• Built-in OTA upgrade available. • Backwards compatible as far as 19.4.4, with the exception of: - Wi-Fi Direct (removed in 19.5.3) - Monitor mode (removed in 19.5.2)	No change
Wi-Fi credentials provisioning via built-in HTTP server	
Built-in HTTP/HTTPS (TLS server mode) provisioning using AP mode (Open, WEP or WPA2 secured).	No change.
Ethernet Mode (TCP/IP Bypass)	
Allow WINC1500 to in WLAN MAC only mode and let the host to send/receive Ethernet frames.	No change.
ATE Test Mode	
Embedded ATE test mode for production line testing driven from the host MCU.	No change.

3 Release summary

3.1 Auditing information

Master Development Ticket	:	`projects/W1500/`versions/34844
Wi-Fi:		
Release Repository	:	`Wifi_M2M`
Source Branch	:	`/branches/trunk_19.5.x`
Subversion Revision	:	**`r15567`**

3.2 Version information

WINC Firmware version	:	19.5.4
Host Driver version	:	19.5.4
Minimum driver version	:	19.3.0

Please note that the SVN revision advertised in the firmware serial trace will be **15567**.

```
(20)NMI M2M SW  VERSION 19.5.4 SVNREV 15567
(30)NMI MIN DRV VERSION 19.3.0
(30)Firmware SVN URL branches/trunk_19.5.x
(30)Built at Oct  4 2017      14:59:09
```

3.3 Released components

The release contains documentation, sources and binaries.

3.3.1 Documentation overview

The Application manuals, Release notes and Software API guides can be found in the `doc/` folder of the release package.

Release Notes:

This document

Software APIs:

WINC1500_IoT_SW_APIs.chm

3.3.2 Binaries and programming scripts

The main WINC1500 firmware binary is located in the `firmware` directory and named `m2m_aio_3a0.bin`. This can be flashed to a WINC device using, for example, a serial bridge application available from ASF.

An OTA image is provided in the `ota_firmware` directory named `m2m_ota_3a0.bin`.

3.3.3 Sources

Source code for the host driver can be found under the `src/host_drv` directory.

Source code for the tools, including crypto_lib, can be found under the `src/Tools` directory.

4 Test Information

Please refer to ticket W1500-83 for full details.

Testing was performed against the release candidate 19.5.4 against the following configuration(s):

H/W Version	:	WINC1510 Xplained module
Host MCU	:	ATSAMD21-Xplained

The following testing was performed in both open air and shielded environments;

1. General functionality including:
    1. HTTP Provisioning
    2. Station Mode
    3. AP Mode
    4. IP (TCP and UDP client and server)
    5. HTTP POST/GET
    6. WPS (PIN and PushButton methods)
    7. Over-The-Air (OTA) update functionality and robustness (with and without TLS)
2. TLS functionality including:
    1. RSA ciphersuites:
        - i. TLS_RSA_WITH_AES_128_CBC_SHA
        - ii. TLS_RSA_WITH_AES_128_CBC_SHA256
        - iii. TLS_RSA_WITH_AES_128_GCM_SHA256
        - iii. TLS_DHE_RSA_WITH_AES_128_CBC_SHA
        - iv. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
        - v. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
        - vi. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
        - vii. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

        Testing uses a 1024-bit server certificate, with a chain of 7 certificates of varying key lengths (1024,2048 and 4096 bit) leading to a 2048-bit root certificate.
    2. ECDSA ciphersuites:
        - i. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
        - ii. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

        Testing uses a NIST standard ECC P256 prime curve server certificate with two chains, one leading back to an ECC root certificate and the other leading to an RSA root certificate.
    3. Client authentication
3. Performance under interference
4. TCP/IP stack robustness testing
    1. Using an internal implementation of IPerf.
    2. Verification of multi socket functionality

5 Known Issues

ID	Description
W1500-101	**(Applies only when using Host Driver version 19.4.4.)** When responding to a WPS request, the channel number of the discovered AP is reported differently by different firmware revisions. Thus a subsequent channel-specific connect request may fail. **Workaround:** Either: 1. Upgrade Host Driver to 19.4.5 or later. 2. Ignore the WPS-reported channel number. Connect using M2M_WIFI_CH_ALL instead.
W1500-103	**(Applies only when using Host Driver version 19.4.x.)** If the application requests power save mode PS_AUTOMATIC or PS_H_AUTOMATIC, then the WINC1500 becomes unresponsive. **Workaround:** Either: 1. Upgrade Host Driver to 19.5.0 or later. 2. Avoid using power save modes PS_AUTOMATIC or PS_H_AUTOMATIC. Use PS_DEEP_AUTOMATIC instead.

6 Terms and Definitions

Term	Definition
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BLE	Bluetooth Low Energy
BSS	Basic Service Set
CBC	Cyclic Block Chaining
DHE	Diffie-Hellman Ephemeral
DNS	Domain Name Server
DTIM	Directed Traffic Indication Map
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read Only Memory
ESD	Electrostatic Discharge
ESS	Extended Service Set (infrastructure network)
GAP	Generic Access Profile
HTTP	Hypertext Transfer Protocol
IBSS	Independent BSS (ad-hoc network)
IEEE	Institute of Electronic and Electrical Engineers
MIB	Management Information Base
MQTT	Message Queuing Telemetry Transport
NDIS	Network Driver Interface Specification
OTA	Over The Air update
PCI	Peripheral Component Interconnect
PMK	Pair-wise Master Key
PSK	Pre-shared Key
RSA	Rivest-Shamir-Adleman (public key cryptosystem)
RSN	Robust Security Network
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface
SSID	Service Set Identifier
RSSI	Receive Strength Signal Indicator
TIM	Traffic Indication Map
TLS	Transport Layer Security
WEP	Wired Equivalent Privacy
WINC	Wireless Network Controller
WLAN	Wireless Local Area Network
WMM™	Wi-Fi Multimedia
WMM-PS™	Wi-Fi Multimedia Power Save
WPA™	Wi-Fi Protected Access
WPA2™	Wi-Fi Protected Access 2 (same as IEEE 802.11i)