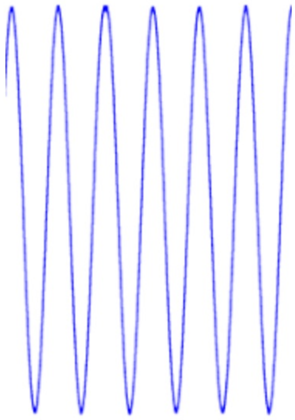
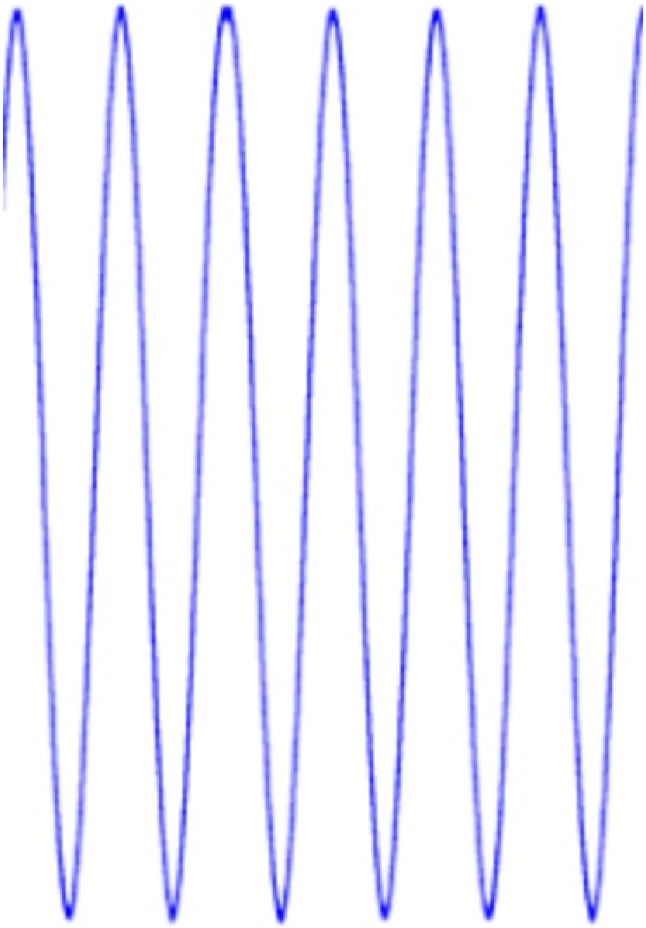


MICROCHIP AN3523 UWB Transceiver Security Considerations Application Note User Guide

Home » MICROCHIP » MICROCHIP AN3523 UWB Transceiver Security Considerations Application Note User Guide

MICROCHIP AN3523 UWB Transceiver Security Considerations Application Note User Guide



Contents

Introduction

Systems to measure distance using round-trip time-of-flight radio signals are becoming more popular in present-day automobiles equipped with Passive Entry/Passive Start (PEPS).
Once the value of the distance is measured, the proximity of the key fob to the car can be verified.
That information can be used to block a Relay Attack (RA).
However, without careful implementation, such proximity-verification methods are not enough to guard against an adversarial attack.
This document explains important security considerations and the ways they are addressed with the Microchip ATA5350 Ultra-Wide-Band (UWB) Transceiver IC.

Quick References

Reference Documentation

1. ATA5350 Datasheet
2. ATA5350 User Manual
3. Mridula Singh, Patrick Leu and Srdjan Capkun, “UWB with Pulse Reordering: Securing Ranging Against Relay and Physical Layer Attacks,” in Network and Distributed System Security Symposium (NDSS), 2020
4. Aanjhan Ranganathan and Srdjan Capkun, “Are We Really Close? Verifying Proximity in Wireless Systems,” in IEEE Security & Privacy Magazine, 2016

Acronyms/Abbreviations

Table 1-1. Acronyms/Abbreviations

Acronyms/Abbreviations	Description
BCM	Body Control Module
CAN	Controller Area Network
ED/LC	Early Detect/Late Commit
IC	Integrated Circuit
ID	Identification
IV	Initial Value
LIN	Local Interface Network
PEPS	Passive Entry/Passive Start
PR	Prover

RA	Relay Attack
RNR	Random Nonce data
SSID	Secure Session Identifier
UHF	Ultra-High Frequency
UWB	Ultra-Wideband
VR	Verifier

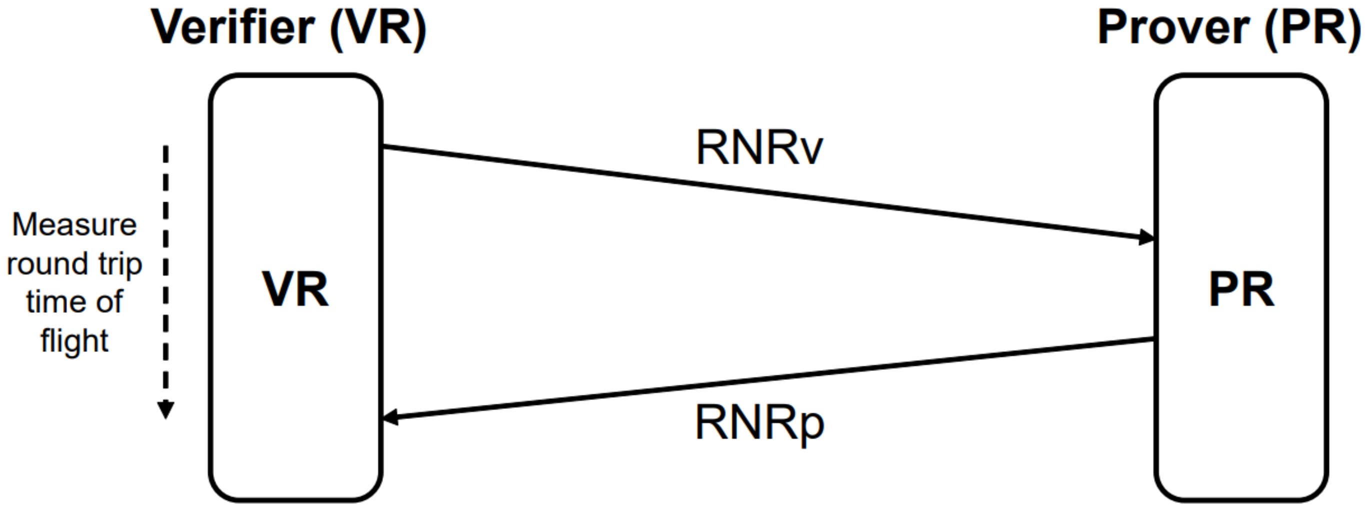
Distance Bounding

Two ATA5350 devices (for example, key fob and car) can be set up to calculate distance by measuring the time of flight of the UWB signal between them.

There are two types of devices involved in the process:

- **First device:** also known as Verifier (fob) starts the measurement
- **Second device:** also known as the Prover (car) replies to the data telegram The measured value, round-trip time-of-flight, between the devices is used to calculate distance using the following simple formula: **distance=(round trip time of flight speed of light)**

Normal Mode Distance Bounding Session (VR/PR)
The following figure illustrates an application for making distance bounding measurements with the ATA5350 UWB transceiver using the Normal mode.
Figure 2-1. Distance Bounding Measurement System



The communication and data exchange between a Verifier node and a Prover node is divided into segments and takes place in the following order:

- Verifier sends its pulse distance measurement request
- Prover receives Verifier request
- Prover waits for fixed turnaround time (16uS)
- Prover sends its pulse distance measurement response
- Verifier receives Prover response

The Normal mode VR/PR ranging session is achieved using a pulse telegram with structure shown in the following figure.

Figure 2-2. Normal Mode VR/PR Pulse Telegrams

Verifier

Preamble (224 pulses)	Sync (127 pulses)	SSID (512 pulses = 4 bytes)	RNRv (512 pulses = 4 bytes)

Turn Around Time

16 uS

Prover

Preamble (224 pulses)	Sync (127 pulses)	SSID (512 pulses = 4 bytes)	RNRp (512 pulses = 4 bytes)

In Normal mode, the logical values for RNRv and RNRp are mapped to pulses using a fixed 1 bit to 16-pulse spreading pattern, which is defined below:

- Logical Bit 0 = pulse pattern 1101001100101100
- Logical Bit 1 = pulse pattern 0010110011010011

For the Verifier, the 4-byte SSID and 4-byte RNRv are mapped to a 1024-pulse pattern and combined with the Preamble and Sync pulses to form a 1375-pulse telegram.
The Prover pulse telegram is also formed in a similar way.
Pulse telegrams using this fixed pattern are vulnerable to physical attacks and should not be used as a countermeasure to the PEPS Relay Attack.
To avoid this scenario, additional security measures must be implemented.
They are described in the following section.

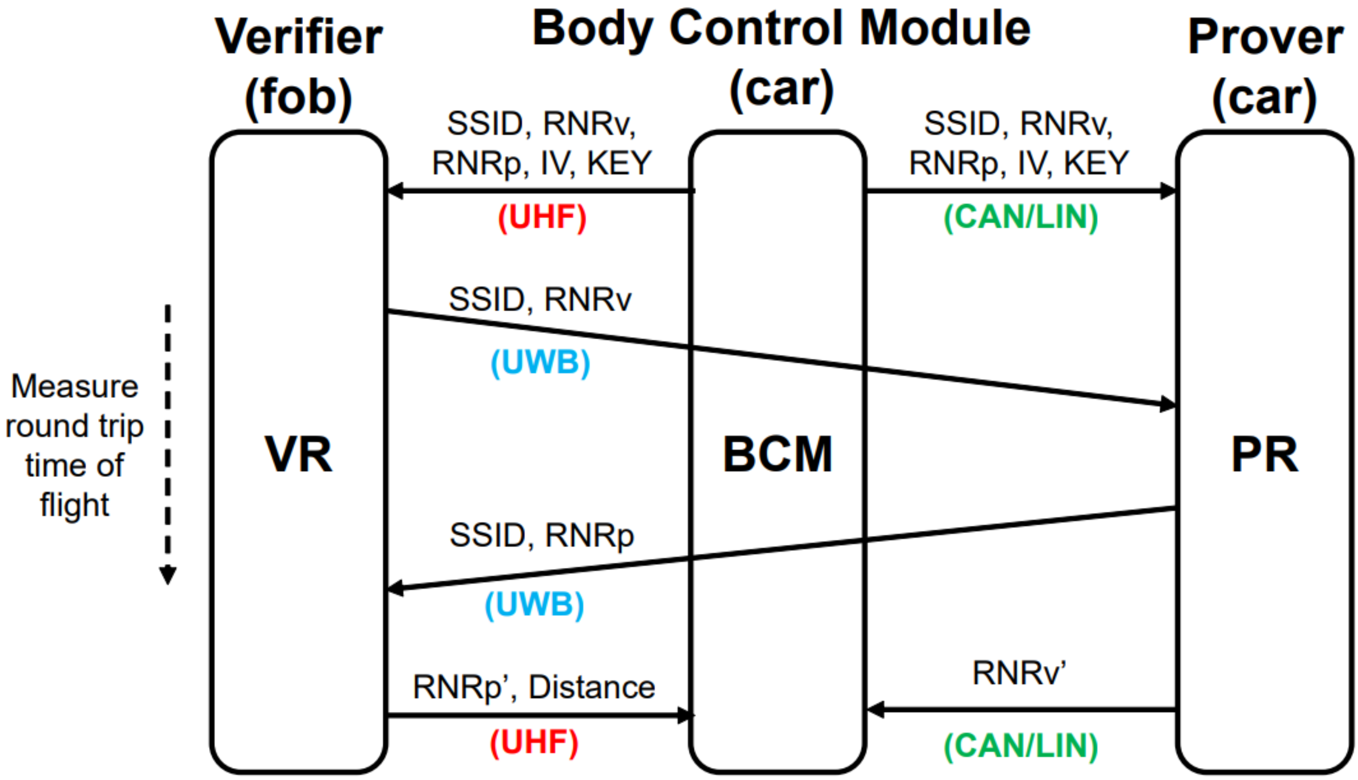
Secure Mode Distance Bounding Session (VRs/PRs)
An improved application for making distance bounding measurements with the ATA5350 UWB transceiver using the Secure mode is shown in Figure 2-3.

This system enhancements include the addition of:

- Random data packet for message authentication (RNRv and RNRp)
- Random data packet pulse re-ordering/scrambling (IV, KEY)

Before starting a distance measurement session, the SSID, RNRv, RNRp, IV and KEY values must be transferred from the Body Control Module (BCM) to the Verifier over an encrypted link (for example PEPS UHF channel) to the Prover(s) over a secure CAN or LIN communication channel.
Upon completion of the distance measurement session, the Verifier sends the calculated distance information to the BCM over an encrypted UHF link (for example, PEPS channel)

Figure 2-3. Secure Distance Bounding Measurement System

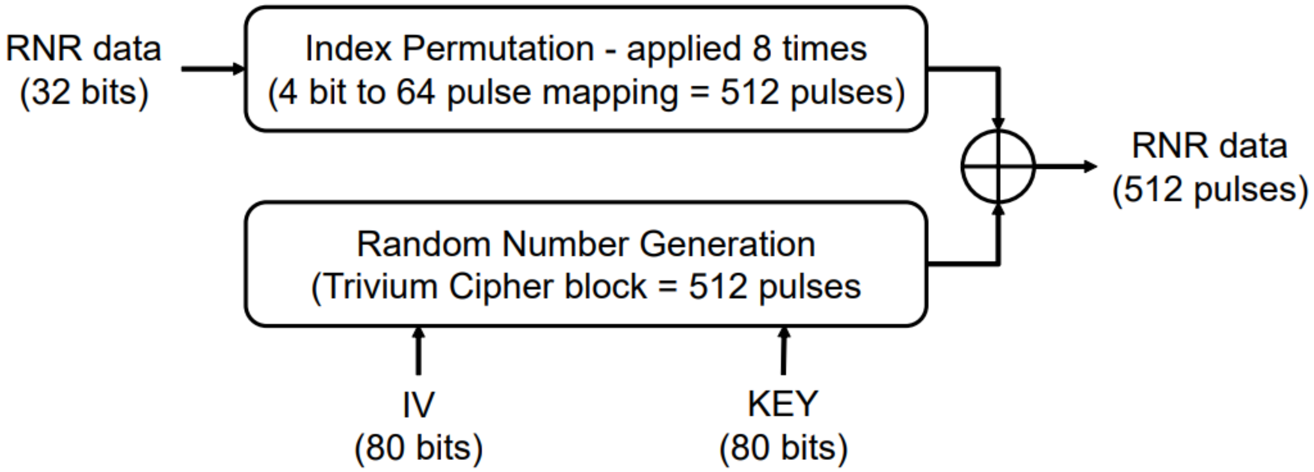


Secure Session Identifier (SSID)
The SSID information provided by the BCM is amended to the UWB pulse telegram. If SSID checking is enabled,

only pulse telegrams with valid SSID values are accepted.
The session is immediately ended if SSID does not match.
See the user manual for the corresponding Configuration bit in register A19.

Random Data Packet for Verifier and Prover (RNRv and RNRp)
The RNRv and RNRp values provided by the BCM are used for checking the authenticity of the received UWB pulse telegram.
The Prover reports its received value from the Verifier, RNRv', to the BCM over the secure CAN or LIN communication channel at the end of the distance measurement session.
If the BCM determines that RNRv ≠ RNRv', the distance measurement is considered invalid.
In a similar way, the Verifier reports its received value from the Prover, RNRp', to the BCM over an encrypted UHF link (for example, PEPS channel) at the end of the distance measurement session.
If the BCM determines that RNRp ≠ RNRp', the distance measurement is considered invalid.

Pulse Scrambling (IV, KEY)
Pulse scrambling is implemented to provide a way to secure the distance measurement against all physical layer distance shortening attacks[3].
In order to scramble the UWB pulse telegram, the Secure Mode re-orders and randomizes the RNRv and RNRp data fields of the pulse telegram.
Pulse re-ordering is achieved by replacing the fixed pulse spreading pattern used in Normal Mode with a permuted pattern from an indexed Look-up Table loaded ahead of the distance measurement session.
Randomization of the pulses is accomplished by applying an exclusive OR operation between the reordered pulses and a random number from the Trivium block cipher.
These operations are shown graphically in the following figure.
It is noteworthy to mention that pulse Re-ordering and Randomization only applies to the RNR data field.
The Preamble, Sync and SSID are not scrambled.
Figure 2-4. Pulse Reordering Process



Types of Adversarial Distance Bounding Attacks

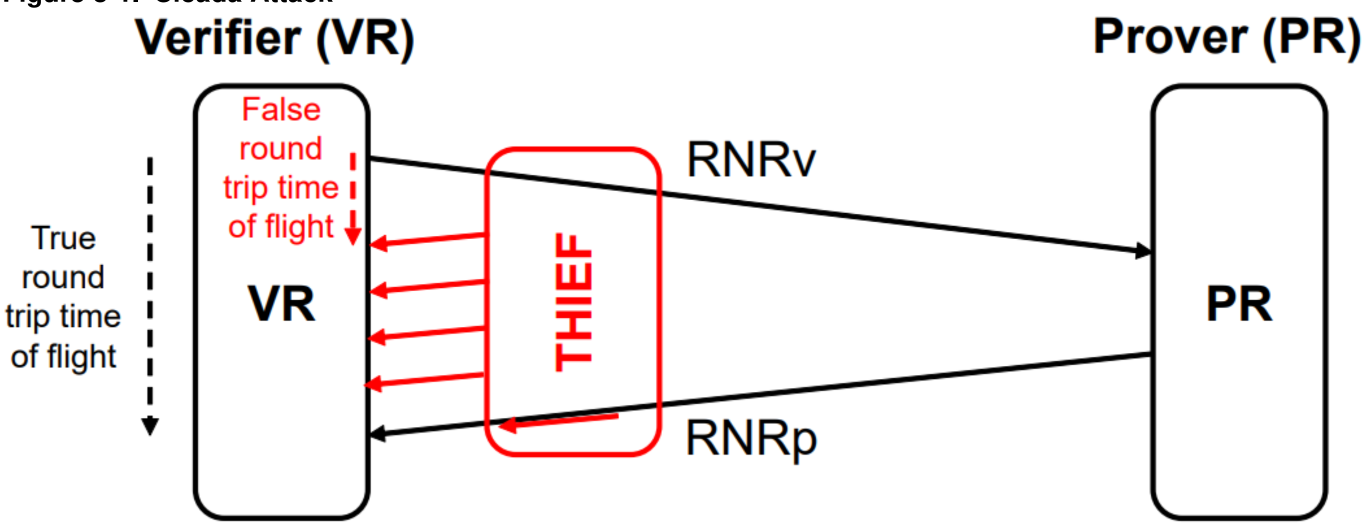
Without proper design considerations, Proximity Verification or Distance Bounding systems can be vulnerable to distance-modifying attacks.
These attacks can make use of the weaknesses in the data layer and/or the physical layer to manipulate the measured distance.
Data-layer attacks can be prevented by including strong encryption and this method is already in practice on PEPS systems in present-day automobiles.
Physical-layer attacks are of significant concern because there is a possibility of executing the attack independent of data-layer encryption and also the attacks make use of data obtained through eavesdropping and by playing (composed or modified) or replaying radio signals to manipulate distance measurements[4].
The context for this document is performing Proximity Verification of the key fob in the PEPS system, so this document only focuses on those threats capable of causing the system to report a distance that is less than actual.

The most common methods of mounting a physical-layer, distance-reducing attack are:

- Cicada Attack – Exploits the deterministic signaling of both preamble and data payload
- Preamble Injection – Exploits the deterministic structure of the preamble
- Early Detect/Late Commit Attack – Exploits the long symbol lengths

Cicada Attack
If the time-of-flight measurement system uses pre-defined data packets for ranging, there is a possibility for the attacker to generate a malicious acknowledgment signal even before the authentic Prover receives its authentic ranging signal.
The Cicada Attack takes advantage of systems having this physical layer weakness by continuously transmitting a malicious acknowledgment (Prover) signal with a greater power compared to the authentic Prover[4].
This causes the authentic Verifier to receive the thief's malicious acknowledgment signal sooner than the authentic acknowledgment signal.
This tricks the system into calculating an incorrect and shortened distance (see the following figure).
Normal mode must be avoided as it makes the user vulnerable to the Cicada attack.
Instead, the Secure mode must be selected.
It replaces pre-defined data packets with uniquely derived data packets and blocks this type of attack.

Figure 3-1. Cicada Attack

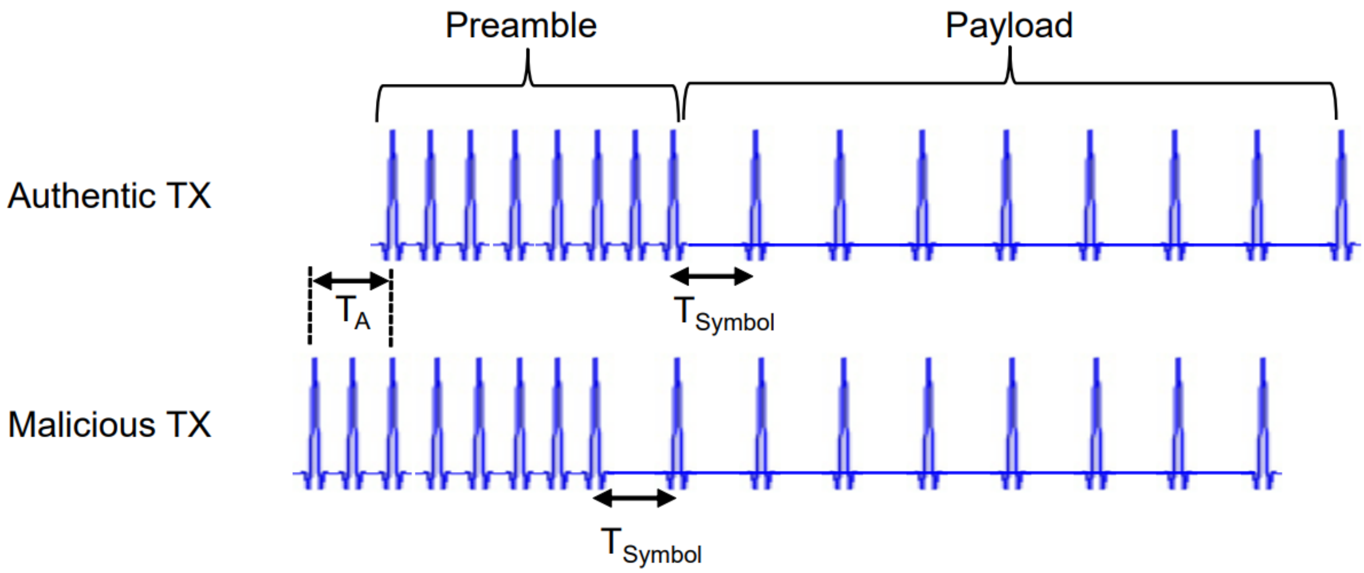


Preamble Injection
In this type of attack, the thief attempts to do the following:

- Leverage its knowledge of the preamble's structure (which is known to the public)
- Guess values for the secure data payload (refer to Section 2.2.3 Pulse Scrambling (IV, KEY))
- Advance the full transmission (Preamble + Data Payload) by an amount, TA, sooner than the authentic Prover will reply.

Refer the following figure for details.

Figure 3-2. Preamble Injection Attack

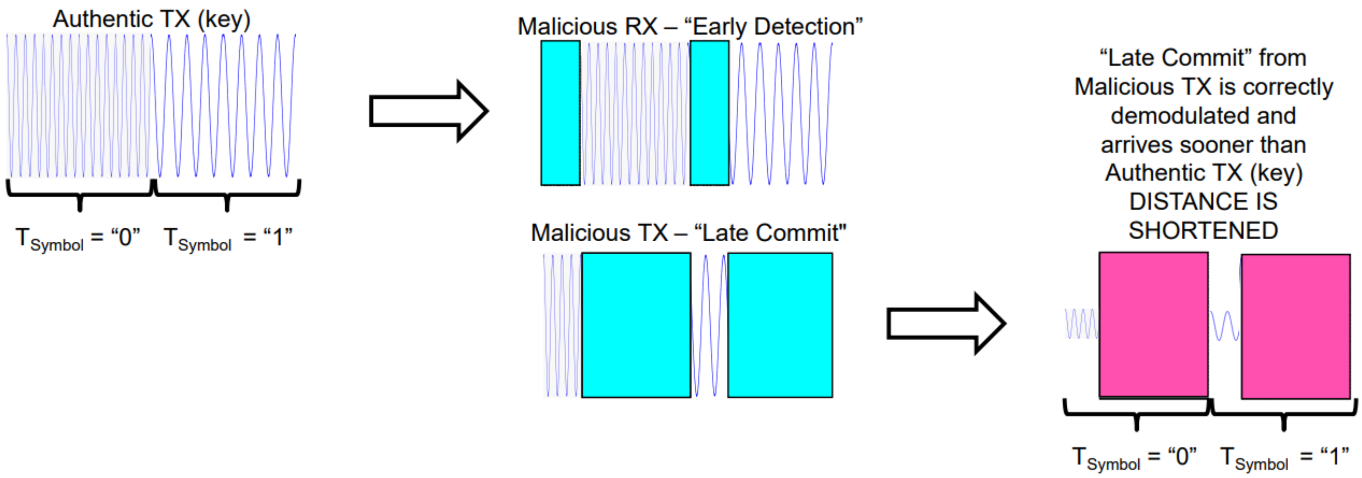


By design, the ATA5350 device uses the preamble's RF characteristics to create a precise sampling profile for the detection of subsequent pulses.
If the preamble that is injected TA sooner than the authentic reply leads to the wrong sample time point, the rest of the secure data payload will not be received correctly, and the attack will be blocked.

Early Detect/Late Commit Attack

Another physical layer characteristic that can be exploited to manipulate distance measurement is the way in which data is encoded.
Due to the nature of UWB radio, logical data bits are encoded using a sequence of pulses which was discussed previously in Section 2.1 Normal Mode Distance Bounding Session (VR/PR).
These sequences of pulses form a symbol and are used by UWB radios to improve sensitivity & robustness.
In fact, UWB radios are capable of correctly determining the transmitted symbol, even if some of the individual symbol pulses are missing.
Consequently, UWB radio systems are vulnerable to the Early Detect/Late Commit (ED/LC) attack.
The principle behind the ED/LC attack is to advance the acknowledge data packet by predicting the symbol pattern after only receiving the first portion of it.
The attack is completed by transmitting a malicious acknowledge data packet sooner than the authentic Prover (see the following figure).

Figure 3-3. Early Detect/Late Commit Attack



The Secure mode effectively blocks all ED/LC attacks and is recommended to avoid this type of distance-reducing attack.
This is achieved by replacing the fixed-pulse patterns (Normal mode) with re-ordered pulse patterns (Secure mode) that are unknown to the attacker.
The information required to properly re-order the pulse patterns are known to both the Verifier and Prover before the start of each ranging session, but not to the attacker.
The entire pulse reordering process is explained in Section 2.2.3 Pulse Scrambling (IV, KEY) and shown graphically in Figure 2-4.

Importance of Protocol

To ensure the authenticity of both the Verifier and Prover messages, a Challenge-Response protocol is required. One of the primary vulnerabilities of the IEEE® 802.15.4a/f standard is that it does not have provisions for an authenticated acknowledgment, and without this capability, the time-of-flight measurement systems are at risk from both physic allayer attacks and simple message-replay attacks[4].
The ATA5350 has this capability, which is explained in Section 2.2.2 Random Data Packet for Verifier and Prover (RNRv and RNRp) and represented in Figure 2-3.

Conclusion

The ATA5350 Impulse Radio UWB Radio was designed with security in mind.
By selecting the Secure mode, which supports pulse re-ordering and message authentication (supporting a Challenge-Response protocol), the user can be assured that the resulting distance measurement is virtually immune from malicious attacks.

Document Revision History

Revision	Date	Section	Description
A	06/2020	Document	Initial Revision

The Microchip Website

Microchip provides online support via our website at: www.microchip.com/.
This website is used to make files and information easily available to customers.

Some of the content available includes:

- **Product Support:** Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support:** Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip:** Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.
To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support.
Local sales offices are also available to help customers.
A listing of sales offices and locations is included in this document.
Technical support is available through the website at: www.microchip.com/support

Product Identification System

To order or obtain information, e.g., on pricing or delivery, refer to the factory or the listed sales office.

PIS_TABLE - Variable missing PIS_EXAMPLE - Variable missing PIS_NOTES - Variable missing

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature.
  All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets.
  Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code.
  Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving.
We at Microchip are committed to continuously improving the code protection features of our products.
Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act.
If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use.
No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, Any Rate, AVR, AVR logo, AVR Freaks, Bes Time, Bit Cloud, chip KIT, chip KIT logo, Crypto Memory, Crypto RF, dsPIC, Flash Flex, flex PWR, HELDO, IGLOO, Jukebox,
Kee Loq, Kleer, LAN Check, Link MD, maX Stylus, maX Touch, Media LB, mega AVR, Micro semi, Micro semi logo, MOST,
MOST logo, MPLAB, Opto Lyzer, Packe Time, PIC, pico Power, PICSTART, PIC32 logo, Polar Fire, Prochip Designer,
Q Touch, SAM-BA, Sen Genuity, Spy NIC, SST, SST Logo, Super Flash, Symmetrical, Sync Server, Tachyon, Temp Trackr, Time Source, tiny AVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology
Incorporated in the U.S.A. and other countries.

APT, Clock Works, The Embedded Control Solutions Company, Ether Synch, Flash Tec, Hyper Speed Control, Hyper Light Load, Intel limos, Libero, motor Bench, m Touch, Power mite 3, Precision Edge, Pro ASIC, Pro ASIC Plus,
Pro ASIC Plus logo, Quiet-Wire, Smart Fusion, Sync World, Temux, Time Cesium, Time Hub, Time Pictra, Time Provider,
Vite, Win Path, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, Any In, Any Out, Blue Sky, Body Com, Code Guard, Crypto Authentication, Crypto Automotive, Crypto Companion, Crypto Controller, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Ether GREEN, In-Circuit Serial Programming, ICSP, INIC net, Inter-Chip Connectivity, Jitter Blocker, Kleer Net, Kleer Net logo, mem Brain, Mindi, MiFi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, Multi TRAK, Net Detach, Omniscient Code Generation, PICDEM, PICDEM. net, PIC kit, PIC tail, Power Smart, Pure Silicon, Q Matrix, REAL ICE, Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, Super Switcher, Super Switcher II, Total Endurance, TSHARC, USB Check, Vari Sense, View Span, Wiper Lock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Seem com are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.
All other trademarks mentioned herein are property of their respective companies.

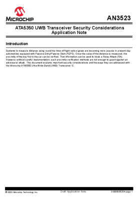
ISBN: 978-1-5224-6300-9

AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big. LITTLE, Cordio, Core Link, Core Sight, Cortex, Design Start, Dynamo, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, Real View, Secur Core, Socrates, Thumb, Trust Zone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, µVision, Versatile are trademarks or registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

Quality Management System

For information regarding Microchip’s Quality Management Systems, please visit:
www.microchip.com/quality.
Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support: www.microchip.com/support
Web Address: www.microchip.com

Documents / Resources

	MICROCHIP AN3523 UWB Transceiver Security Considerations Application Note [pdf] User Guide AN3523 UWB Transceiver Security Considerations Application Note, AN3523, UWB Transceiver Security Considerations Application Note, Considerations Application Note

References

- Empowering Innovation | Microchip Technology
- Empowering Innovation | Microchip Technology
- Product Change Notification | Microchip Technology
- Quality | Microchip Technology
- Microchip Lightning Support