Bluetooth **Shared Items**   Bluetooth **Logo**   Bluetooth Share **App**   **Android** Bluetooth Share   Sharing   **Windows Phone**   ›

Bluetooth Secure Simple Pairing Using NFC Part 1
NFC FORUM 10 YEARS
2014 NFC World Congress
September 24, 2014 | Marseille, France

Bluetooth Low Energy Security and Pairing Overview
NFC FORUM 10

Bluetooth Security Mechanisms
Hochschule der Medien
Computer Science and Media
Mobile Security
Marvin Hoffmann (B.Sc.)
contact@marvin.hoffmann.de   08 April 2011

Bluetooth® Secure Simple Pairing / LE OOB Pairing Using NFC: Record Types
NFC FORUM 10
16
21
185+
2500+
6000+
- Mime types
  - One Mime type defined for the NDEF record type name for Bluetooth BR/EDR configuration data record: application/vnd.bluetooth.ep.oob
  - One Mime type defined for the NDEF record type name for Bluetooth LE configuration data record: application/vnd.bluetooth.le.oob
  - Mime types defined by Internet Assigned Numbers Authority (IANA)
    - http://www.iana.org/assignments/media-types/media-types.xhtml#application
  - May define both BR/EDR and LE in same handover message, then need two carrier data configuration records with different record type name
  (MIME = Multipurpose Internet Mail Extensions)

Bluetooth LE Technology: Security Manager Profile Overview
NFC FORUM 10
16
21
185+
2500+
6000+
SM Overview
- Security Manager Protocol
  - Handles pairing and bonding
  - Security parameter negotiation
  - Encryption key generation and distribution

BLUETOOTH PENTESTING
Nikhil Raj (n1k5_b0t)
http://facebook.com/krazzy2hack
krazzy2hack

Explore more searches like ~~secure bluetooth~~ pair and share

Read, Write, Pair, Share
Read Pair Share

Pair Work: Listen, draw, write (2)
Pair and Write

Turn and TALK
Pair and Talk

Think Pair
Directions:
1. With a partner, discuss the question given.
2. Be prepared to share.
1. Why is lesson planning important for the teacher and learner?
2. What things/ sections should a lesson plan have?
3. What things are the most difficult when lesson planning? Why?
Directions for Think Pair Sh...

Mix-Pair-Sha
Mix Pair Sh...

Message Composition
Handover Carrier Record
NFC FORUM 10
16
The carrier data reference can point to an NDEF record containing
- a Handover Carrier Record
- or a Carrier Configuration Record

Bluetooth® Secure Simple Pairing Using NFC: AD and EIR Data
NFC FORUM 10
The format used in the Bluetooth configuration data record is the Extended Inquiry Response (EIR) data format for Bluetooth BR/EDR and the Advertising and Scan Response Data (AD) format for Bluetooth LE.
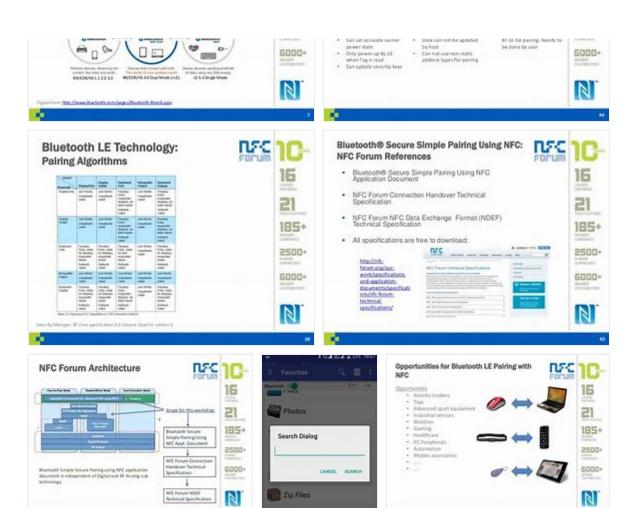
💬 Feedback

Handover Carrier Record is used when a carrier is proposed
When no configuration data is to be provided

ACF	CRF
CARRIER_TYPE_LENGTH	
CARRIER_TYPE	
CARRIER_DATA	

→ Additional carrier information, length set by NDEF definition

Value	Carrier Type Format
0x0	NFC Forum well-known type [NFC RTD]
0x1	Media-type as defined in RFC 2046 [RFC 2046]
0x2	Absolute URI as defined in RFC 3986 [RFC 3986]
0x4	NFC Forum external type [NFC RTD]

---

1. The EIR and AD formats are described in Bluetooth Core specification
2. The different EIR and AD types are described in the Bluetooth Core specification Supplement
3. EIR and AD data types values can be found in Bluetooth Assigned numbers

Examples of EIR and AD types are
- Local name
- Security keys
- Manufacturer data
- Appearance

EIR and AD data types are defined by Bluetooth SIG

---

5. Recommendations

- pairing process at secure place
- choose strong PIN
- turn off completely when not in use
- at least hide your phone

Bluetooth® Secure Simple Pairing Using NFC: Objectives

- Application document:
  - The document is administered by the NFC Forum
  - The document is jointly developed and approved by the NFC-Forum and the Bluetooth Special Interest Group (SIG)
- What is described in the document:
  - The application document only describes the Bluetooth specific content in the "carrier configuration record" pointed to by the alternative carrier record described in the connection handover specification.
  - Connection handover message composition is described in the Connection Handover specification and the NDEF structure is defined in the NFC Forum NDEF specification.
  - Bluetooth data types and pairing process are described in Bluetooth specifications

---

Summary:

Security Mode of Bluetooth

- **Security Mode 1:** No-Secure Mode, (There won't be any authentication or encryption in this mode. Bluetooth device can easily be connected with the other devices).
- **Security Mode 2:** Service level security mode, (The management of the access control and interfaces with other protocols and device users is handled by the centralized security manager, it includes Authentication, Configuration and Authorization).
- **Security Mode 3:** Link-level security mode, (This is a built in security mechanism that offers the authentication (unidirectional or mutual) and encryption based on the secret key shared by the pair of devices).

SRM UNIVERSITY

Bluetooth® Secure Simple Pairing Using NFC: Mandatory and Optional Configuration Data

- Mandatory data types
  - Some data types are defined as mandatory
  - Bluetooth BR/EDR mandatory data
    - Bluetooth device address
  - Bluetooth LE mandatory data
    - LE Bluetooth device address
    - LE Role
- Optional data types
  - All other EIR or AD types may be included in the carrier configuration record
  - The receiver of the EIR or AD types may use or may ignore any of the optional data types

---

Bluetooth Technology: Essentials

- Standard for Personal Area Network based on Ericsson research
- Short range, low power
- Frequency hopping spread spectrum (FHSS)
- 2.4 GHz ISM band
- Bluetooth Special Interest Group formed in 1998
- 20,000+ SIG member companies
- **Billions** of products shipped

http://www.bluetooth.com/Pages/History-of-Bluetooth.aspx
http://www.bluetooth.com/Pages/Board-of-Directors.aspx

---

share

Partner Share

Black and Share

SHARE LIGHT

Light and Share

Load and Share

Think and S

Bluetooth Technology: Terminology

Term	Introduced	Means
BR	1.1 (2002)	Basic Rate (1 Mbit/s)
EDR	2.0 (2004)	Enhanced Data Rate (2 and 3 Mbit/s)
HS	3.0 (2009)	High Speed (Alternate MAC/PHY)
LE	4.0 (2010)	Low Energy (1 Mbit/s ultra low power)
Bluetooth Smart	4.0	Single mode, LE-only radio
Bluetooth Smart Ready	4.0	Dual mode, BR/EDR and LE dual radio

---

Dynamically Programmable Tags

Dynamically programmable Tags | Tags with field detect | Tags with no interface to host

Flexible solution:
- Can update non-static addresses

Can be made power efficient:
- Only power up BL-LE when tag enters NFC field

Cheap solution:
- Major drawback: can not inform host to power up

- Can set accurate carrier power state
- Only power up BL-LE when Tag is read
- Can update security keys

- Data can not be updated by host
- Can not use non-static address types for pairing

BT-LE for pairing. Needs to be done by user

Bluetooth LE Technology: Pairing Algorithms

Security Manager: BT Core specification 4.0 Volume 3 part H section 2

Bluetooth® Secure Simple Pairing Using NFC: NFC Forum References

- Bluetooth® Secure Simple Pairing Using NFC Application Document
- NFC Forum Connection Handover Technical Specification
- NFC Forum NFC Data Exchange Format (NDEF) Technical Specification
- All specifications are free to download:

http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-forum-technical-specifications/

NFC Forum Architecture

Bluetooth Secure Simple Pairing Using NFC Appl. Document

NFC Forum Connection Handover Technical Specification

NFC Forum NDEF Technical Specification

Bluetooth Simple Secure Pairing using NFC application document is independent of Digital and RF Analog sub technology.

Favorites

Photos

Search Dialog

CANCEL   SEARCH

Zip Files

Apps

Opportunities for Bluetooth LE Pairing with NFC

Opportunities
- Activity trackers
- Toys
- Advanced sport equipment
- Industrial sensors
- Watches
- Gaming
- Healthcare
- PC Peripherals
- Automation
- Mobile accessories
- ...

Cracking the Bluetooth Pairing PIN

- Attacker can eavesdrop the whole communication of pairing of two Bluetooth devices A & B and collect essential information for cracking PIN.
- Local eavesdropping is possible but eavesdropping the another piconet requires a dedicated hardware device.
- Frequency Hopping can be a bottleneck in sniffing; only master knows the sequence of frequencies to be hopped.
- The entire process can dissected into three parts :
  - Based on PIN assumption, calculate a hypothesis on K_{init}
  - Calculate a hypothesis on K_{AB}
  - Verify our assumption via challenge-response from Mutual Authentication

krazzy2hack

Bluetooth Security

By

Mohammed A. Ahmed
Amjad M. Musleh
Asmat K. Marouf

Advisors
Dr. Ashraf S. H. Mahmoud
Dr. Marwan H. Abu-Amara

Connection Handover White Paper Just Announced!

- Informative guide for developers
- Hands on tips for using Connection Handover
- Free download:
- http://nfc-forum.org/connection-handover/

Connection Handover User Experience Recommendations

The Pairing Process with the Use of NFC: Static Handover

Case: A user purchases a headset and wants to use it with his telephone

The telephone contains a BT device and an NFC engine

The user does the tap

The headset contains a BT device and an NFC Tag

The telephone will start reading the NFC Tag with NFC technology.
NDEF message on Tag will contain a
Bluetooth carrier configuration data record that contains
Bluetooth address = Headset Device address
Generic access profile = Headset
Local name = "Cool Headset"

Bluetooth Technology: Revision History

- Significant specification revisions:
  - Bluetooth 1.1 (2002): 1 Mb/s, first widely implemented version
  - Bluetooth 2.0 + EDR (2004): Adds 2Mb/s and 3Mb/s data rates
  - Bluetooth 2.1 + EDR (2007): Secure Simple Pairing
  - Bluetooth 3.0 + HS (2009): Adds alternate PHY (802.11 initially)

➤ Bluetooth 4.0 + HS (2010): EDR, HS and low energy

Bluetooth Simple Secure Pairing Using NFC Application Document:

Version 1.0 ➡ Bluetooth 2.1 SSP

Version 1.1 ➡ Bluetooth 2.1 for BR/EDR with SSP
+ Bluetooth 4.0 Out of Band pairing for LE

Bluetooth 4.1 (December 2013):

https://www.bluetooth.org/en-us/specification/adopted-specifications

---

Updated Bluetooth Secure Simple Pairing with NFC Announced today!

- Application Document guides developers in building solutions that seamlessly combine Bluetooth and NFC
- Updated to include Bluetooth® Smart devices
- Product of formal liaison with Bluetooth SIG signed last November
- Free download:
http://nfc-forum.org/our-work/specifications-and-application-documents/application-documents/

Bluetooth Secure Simple Pairing Using NFC

---

4. Authentication (Contd.)

SRM UNIVERSITY

Favorites   BlueTooth Admin

Send Contacts

Attacking the pairing key : Calculate K_{init}