Facoltà di scienze
Matematiche Fisiche e Naturali

BLUETOOTH SECURITY

CORSO DI SICUREZZA SU RETI 2
A. A . 2008/09
PROF. ALFREDO DE SANTIS

GRUPPO:
SPINIELLO CARMINE [0521-000562]

OUTLINE

- Introduzione
- Protocolli
- Profili
- Sicurezza
- Vulnerabilità

Bluetooth™

OUTLINE

- Introduzione
- Protocolli
- Profili
- Sicurezza
- Vulnerabilità

Bluetooth™

Introduzione a Bluetooth

- Il Bluetooth è uno standard creato affinché una vasta gamma di prodotti possano comunicare tra loro utilizzando le onde radio a corto raggio.

Bluetooth™

Un po' di storia (1)

- Nel 1990 Ericsson avviò un progetto di ricerca con l'obiettivo di realizzare un sistema di comunicazione basato sulle onde radio

- Nel 1998 nacque il **SIG** (Special Industry Group) che aveva tra i partecipanti:

  Ericsson, Nokia, IBM, Toshiba, Intel

  L'obiettivo principale era sviluppare e promuovere una soluzione globale per le comunicazioni wireless operante nella banda ISM (Industrial Scientific Medicine band) 2.4 GHz

- Nel 1999 si aggiunsero altre 4 multinazionali:

  3COM, Motorola, Lucent, Microsoft

Bluetooth™

Un po' di storia (2)

- Nel mese di aprile del 1999 il consorzio contava ben 600 membri
- Nel mese di luglio dello stesso anno uscirono le prime specifiche tecniche del neonato Bluetooth
- Da quel momento varie versioni del Bluetooth sono state ratificate dal SIG, tutte rispondenti ai requisiti di interoperabilità, armonizzazione della banda e promozione della tecnologia

Bluetooth™

Versioni (1)

- **Bluetooth 1.0**: offriva una velocità di connessione di 1Mbps suddiviso tra dati e voce, se non fosse che soltanto circa 700Kbps vengono utilizzati per il trasferimento e come se non bastasse poteva comunicare con un solo dispositivo per volta.

- **Bluetooth 1.1**: fissati alcuni bug della versione precedente.

- **Bluetooth 1.2**: viene adottata la Adaptive Frequency Hopping per rendere la comunicazione tra dispositivi più resistente alle interferenze esterne, e Enhanced Voice Processing per migliorare la qualità audio, soprattutto in ambienti rumorosi.

Bluetooth™

Versioni (2)

- **Bluetooth 2.0 + EDR:** la velocità di trasmissione dati passa a 2.1Mbps e scendono i consumi di energia.

- **Bluetooth 2.1 + EDR:** migliorata la velocità di associazione ed i passaggi necessari. Migliora ancora il consumo di energia, che varia in base all'utilizzo che si fa.

- **Bluetooth 3.0+HS, o Bluetooth High Speed Technology:** capace di raggiungere velocità di connessione che sfiorano i 24Mbps. La specifica finale è stata pubblicata nel mese di aprile del 2009.

Bluetooth™

Caratteristiche dei dispositivi (1)

- La potenza massima di trasmissione dei dispositivi è di 100 metri
- Per avere un risparmio energetico le case produttrici limitano la potenza dei dispositivi ad una trasmissione di 10 metri
- Ogni dispositivo ha un indirizzo di 48 bit diviso in 3 parti:
  - per identificare la casa costruttrice
  - per identificare il dispositivo
  - per identificare la rete di cui fa parte “piconet”
- Ogni dispositivo ha un clock a 28 bit che scatta 3200 volte al secondo
- Sono supportati due tipi di canali :
  - Canali Sincroni
  - Canali Asincroni

Bluetooth™

Caratteristiche dei dispositivi (2)

- I Canali Sincroni

  vengono utilizzati per la trasmissione della voce offrendo una trasmissione bilaterale con velocità di trasmissione massima di 64 Kb/s

- I Canali Asincroni:

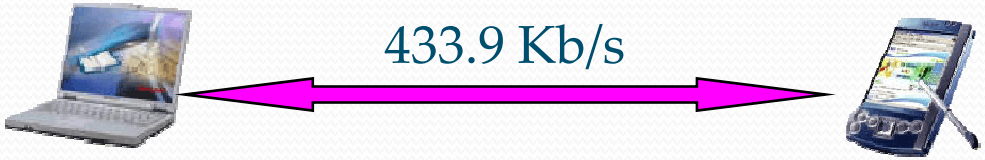
  vengono utilizzati per la trasmissione dei dati e vengono usati in 2 modalità:
  - simmetrica
  - asimmetrica

Bluetooth™

Caratteristiche dei dispositivi (3)

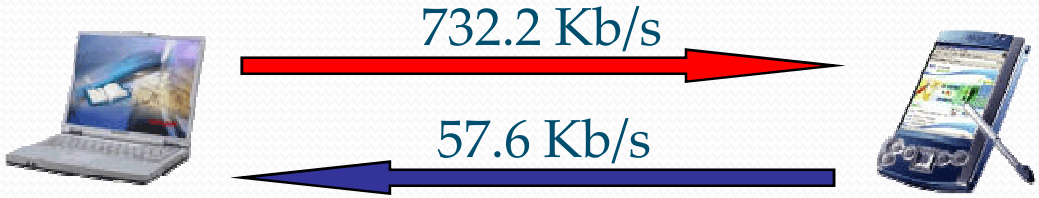
- I Canali Asincroni Simmetrici:

  si può disporre di una velocità di trasmissione simmetrica massima di 433.9 Kb/s per direzione



- I Canali Asincroni Asimmetrici:

  si può disporre di una velocità di trasmissione simmetrica massima di 732.2 Kb/s in una direzione e 57.6 Kb/s nell'altra



Bluetooth™

Bluetooth 3.0 HS

Miglioramenti rispetto le altre versioni:

- Aumento nella velocità di trasferimento e nuove funzionalità
  - 480 megabit (60 megabyte) al secondo per brevi distanze, mentre per distanze superiori ai 10 metri 100 megabit (12.5 megabyte) al secondo
  - inviare contenuti in alta definizione a computer e televisioni con Bluetooth
- Meno interferenze
  - Bluetooth 3.0 funziona nell'intervallo 6-9 GHz invece che 2,4 Ghz, come nei precedenti standard

Bluetooth™

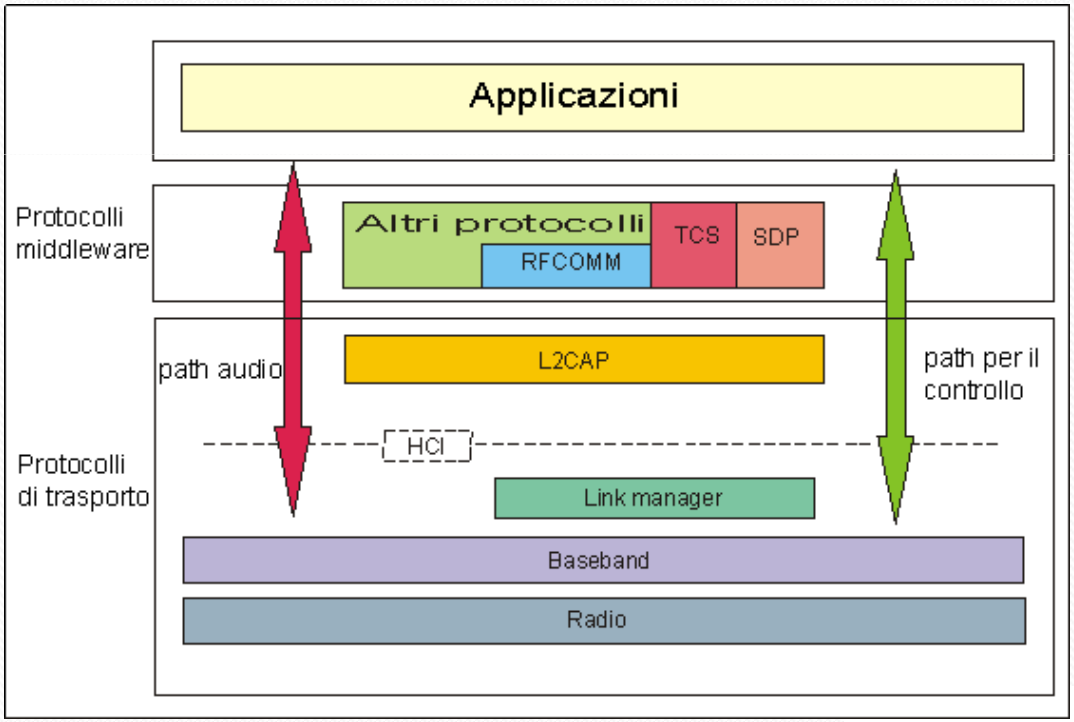
OUTLINE

- Introduzione
- Protocolli
- Profili
- Sicurezza
- Vulnerabilità

Bluetooth™

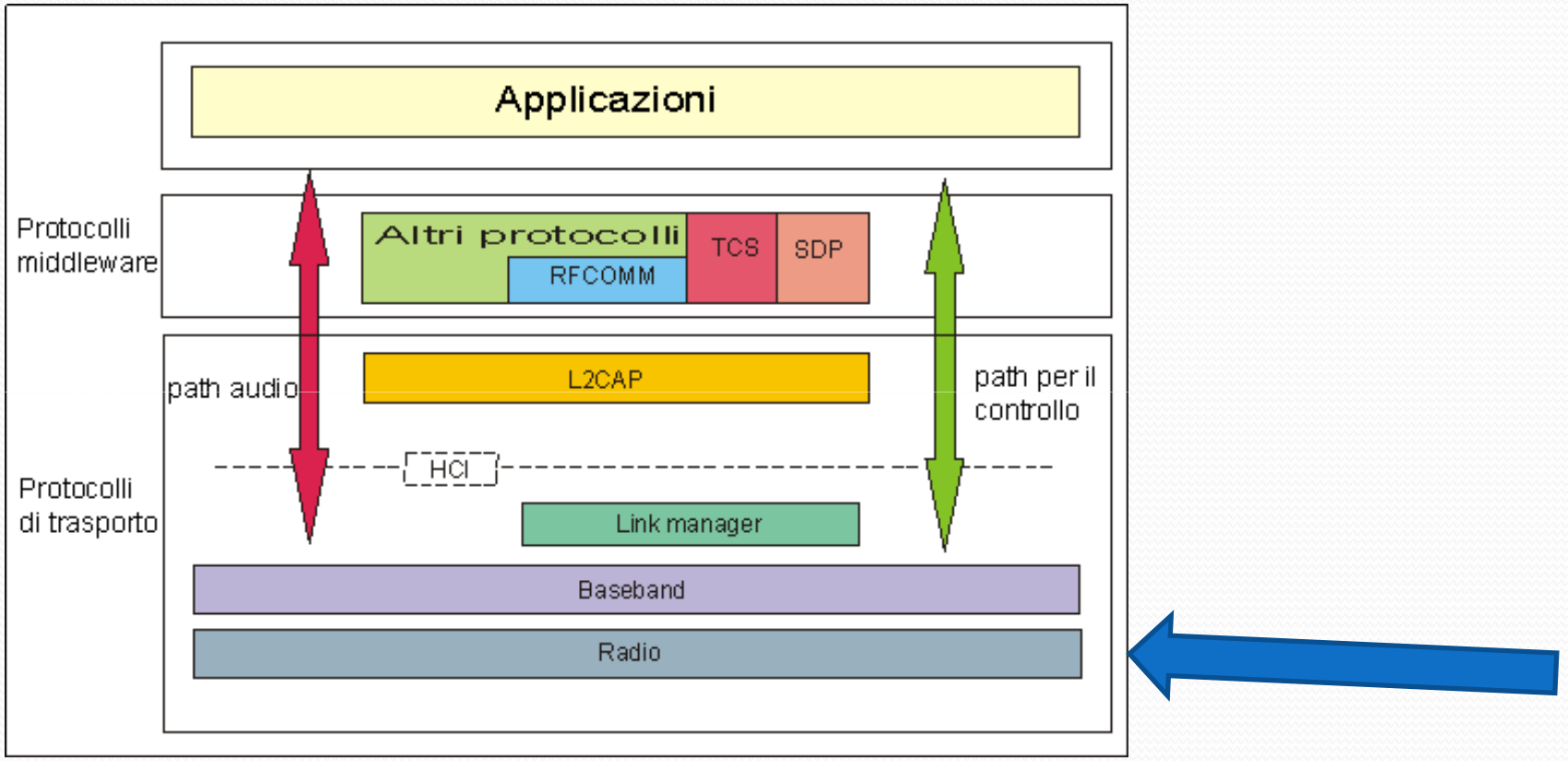
Protocolli in Bluetooth

- Lo stack dei protocolli è diviso in due parti:
  - protocolli di trasporto (basilari per lo scambio di dati)
  - protocolli middleware (protocolli intermedi per interagire con le applicazioni



Bluetooth™

Protocollo Radio



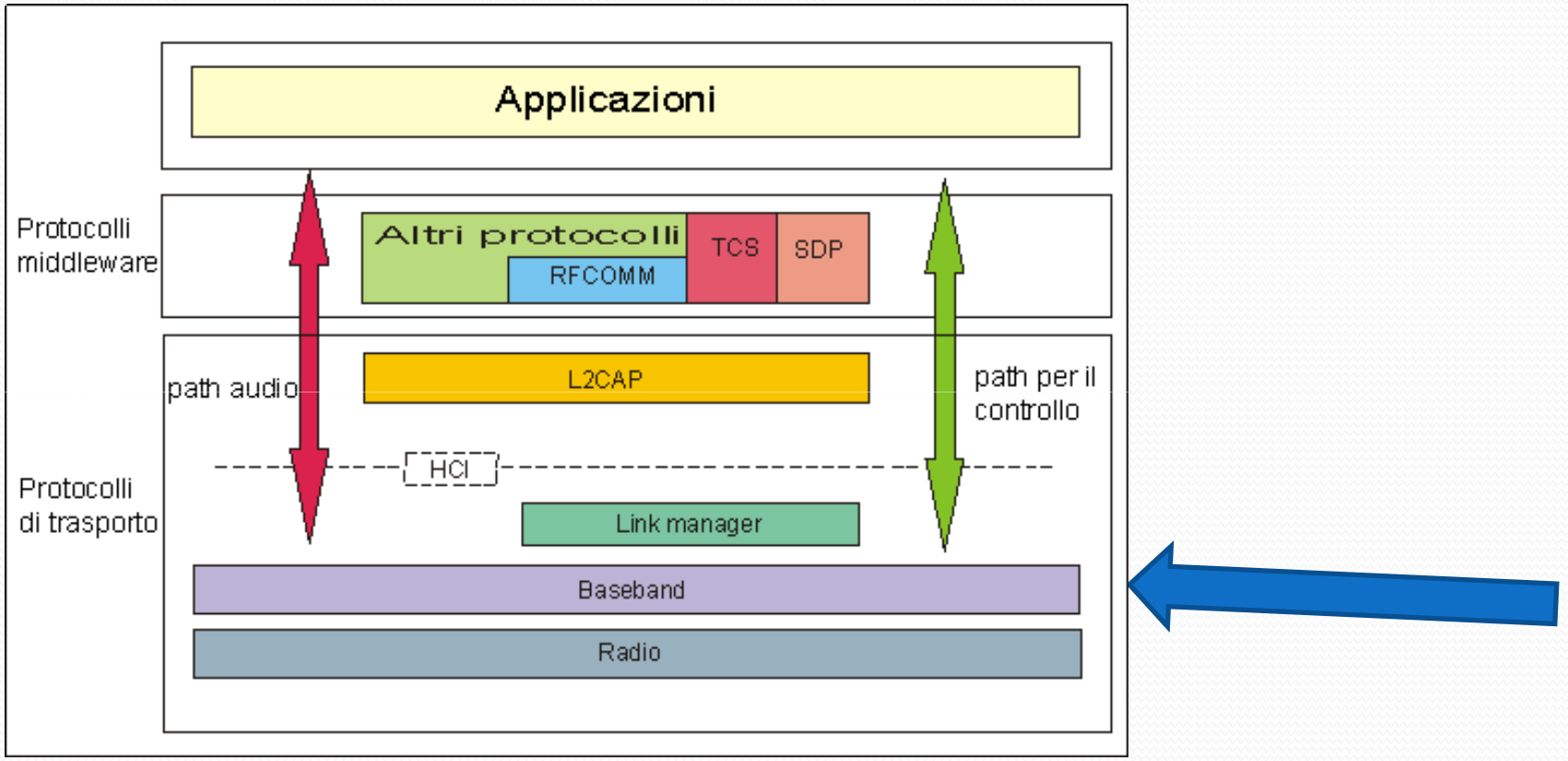
Bluetooth™

Protocollo Radio

- E' il protocollo di più basso livello e si occupa della definizione delle caratteristiche tecniche del sistema di trasmissione dei dispositivi
- Il sistema Bluetooth opera nella banda di frequenza ISM (Industrial Scientifics Medicine band), globalmente disponibile, e la modulazione di frequenza è la GFSK
- Bluetooth è un sistema FHSS operante su un insieme di *m* canali ognuno di 1 Mhz, nella maggioranza dei paesi il valore di *m* è 79
  Gli hop sono effettuati rapidamente sui possibili 79 canali nella banda, che inizia a 2.4 Ghz e termina a 2.480 Ghz

Bluetooth™

Protocollo Baseband



Protocollo Baseband

- E' il protocollo responsabile per la comunicazione dei dispositivi Bluetooth

  Tra i suoi compii fondamentali c'è:
  - la sincronizzazione dei dispositivi
  - la scelta delle frequenze di hopping
  - la correzione degli errori
  - il controllo del flusso
  - il controllo della sicurezza delle trasmissioni

Bluetooth™

Piconet

- La comunicazione Bluetooth prende luogo grazie alla creazione di una rete ad hoc chiamata *piconet*.

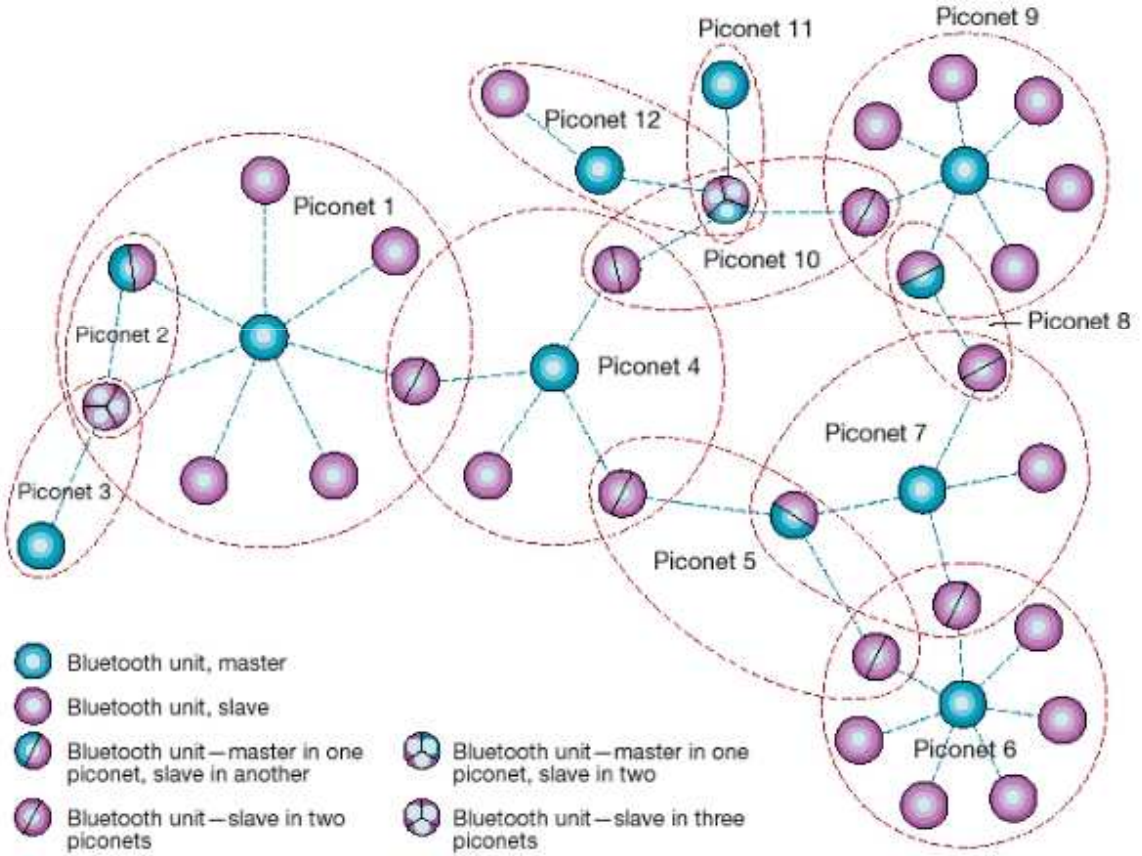
Una piconet è formata da:

- Un dispositivo Master che è il creatore della rete
- Al massimo sette dispositivi slave con cui il master comunica attivamente con indirizzo AM_ADDR
- Al più 255 dispositivi parked che possono diventare attivi su richiesta

Bluetooth™

Scatternet

- Quando un dispositivo appartiene a più reti si viene a creare una Scatternet



- Possibilità di collisioni

Bluetooth™

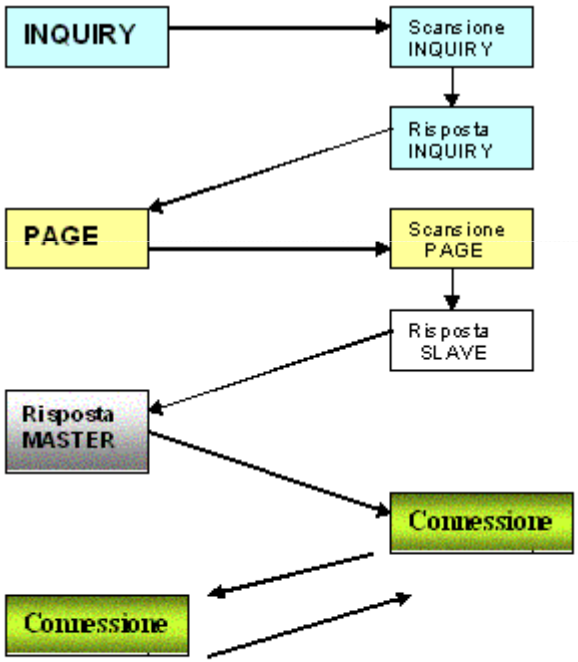
Stati di Bluetooth

- Inizialmente tutti i dispositivi si troveranno nella modalità standby

- Il Master inizia la fase di Inquiry per associare dei dispositivi alla Piconet

- Durante la fase di Page avviene la sincronizzazione tra Master e Slave e si conclude con la fase di Connessione

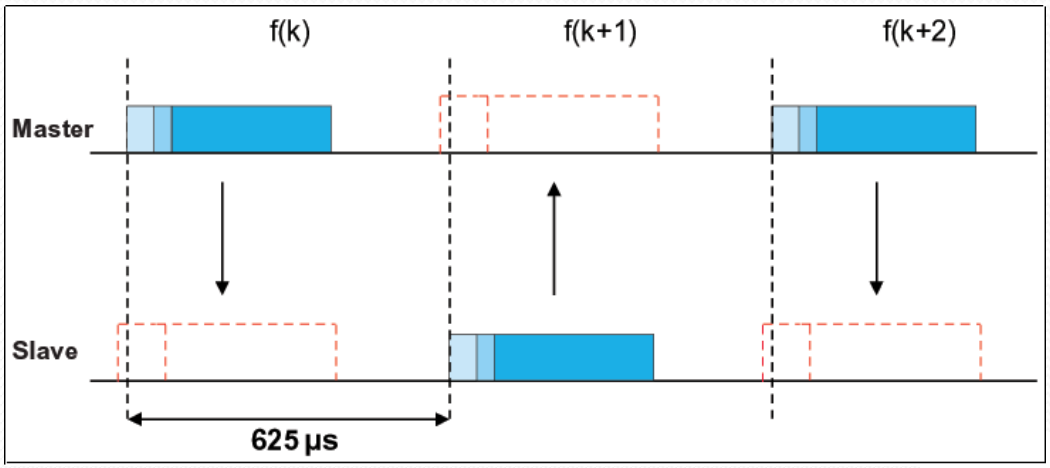
- In questa fase un dispositivo può essere in quattro modalità (active, hold, sniff e park)



Bluetooth™

Canale Fisico (1)

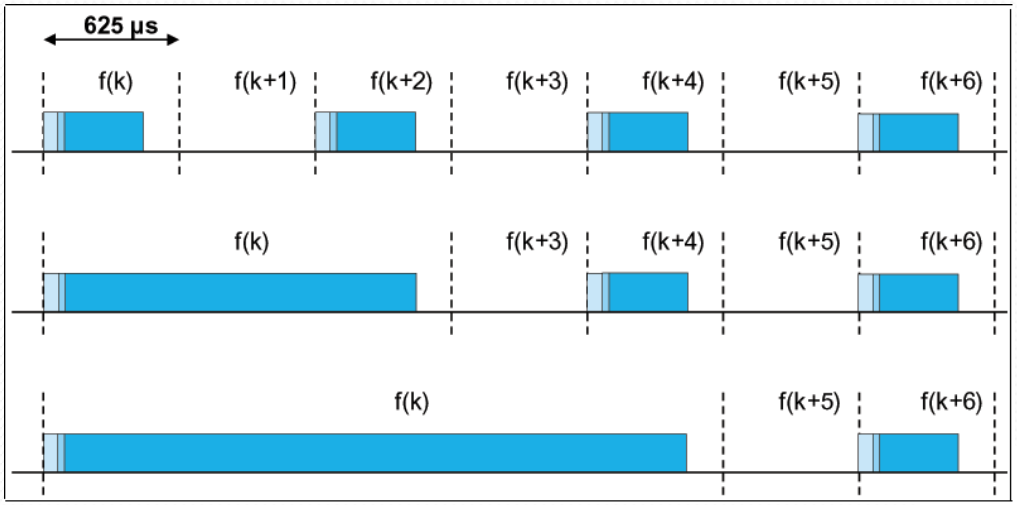
- Il Canale Fisico è diviso in Time Slot, ogni membro della Piconet esegue dei salti di frequenza
- La durata di ogni slot è di 0,625 ms
- La trasmissione avviene tramite uno schema TDD (time-division duplex):
  - Il Master trasmette negli slot con numero pari
  - Gli slave trasmettono negli slot con numero dispari



Bluetooth™

Canale Fisico (2)

- L'inizio della trasmissione di un pacchetto coincide sempre con l'inizio di uno slot
- Durante la trasmissione di un pacchetto non avvengono mai salti di frequenza.
- E' possibile trasmettere anche pacchetti multislot, che possono occupare fino a 5 slot consecutivi.

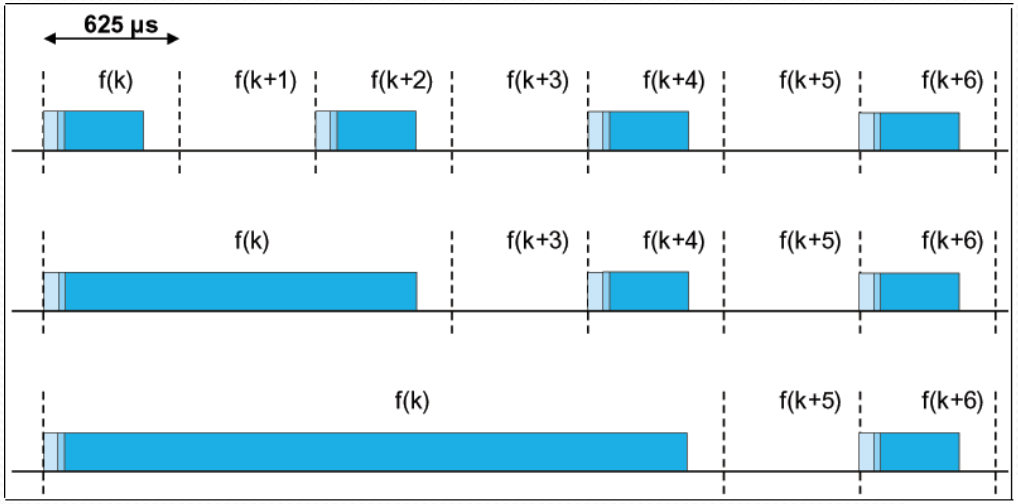


Bluetooth™

Canale Fisico (3)

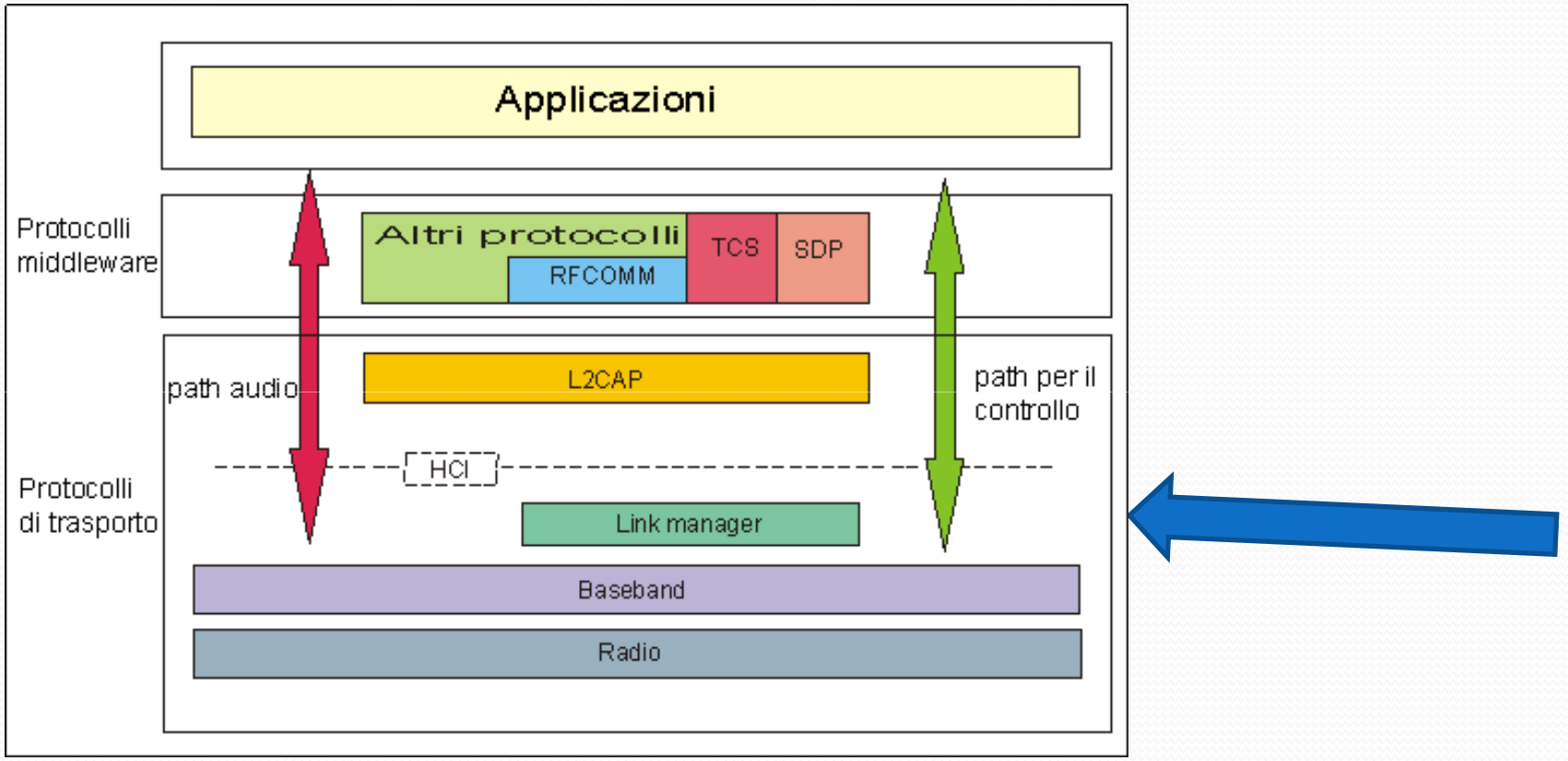
- Durante la trasmissione di un di pacchetto multislot non avvengono salti di frequenza

- Alla fine della trasmissione di un pacchetto multislot si parte con la frequenza che si sarebbe usata, se fossero stati trasmessi solo pacchetti di dimensione pari ad uno slot.



Bluetooth™

Protocollo Link Manager



Protocollo Link Manager (1)

- E' il protocollo responsabile dell'impostazione e del mantenimento del collegamento Bluetooth, ha come maggiori funzionalità la gestione dell'energia e della sicurezza

- Un dispositivo può trovarsi in 4 diverse modalità operative:

  - **Active Mode:** in questa modalità l'unità Bluetooth partecipa attivamente all'interno della piconet

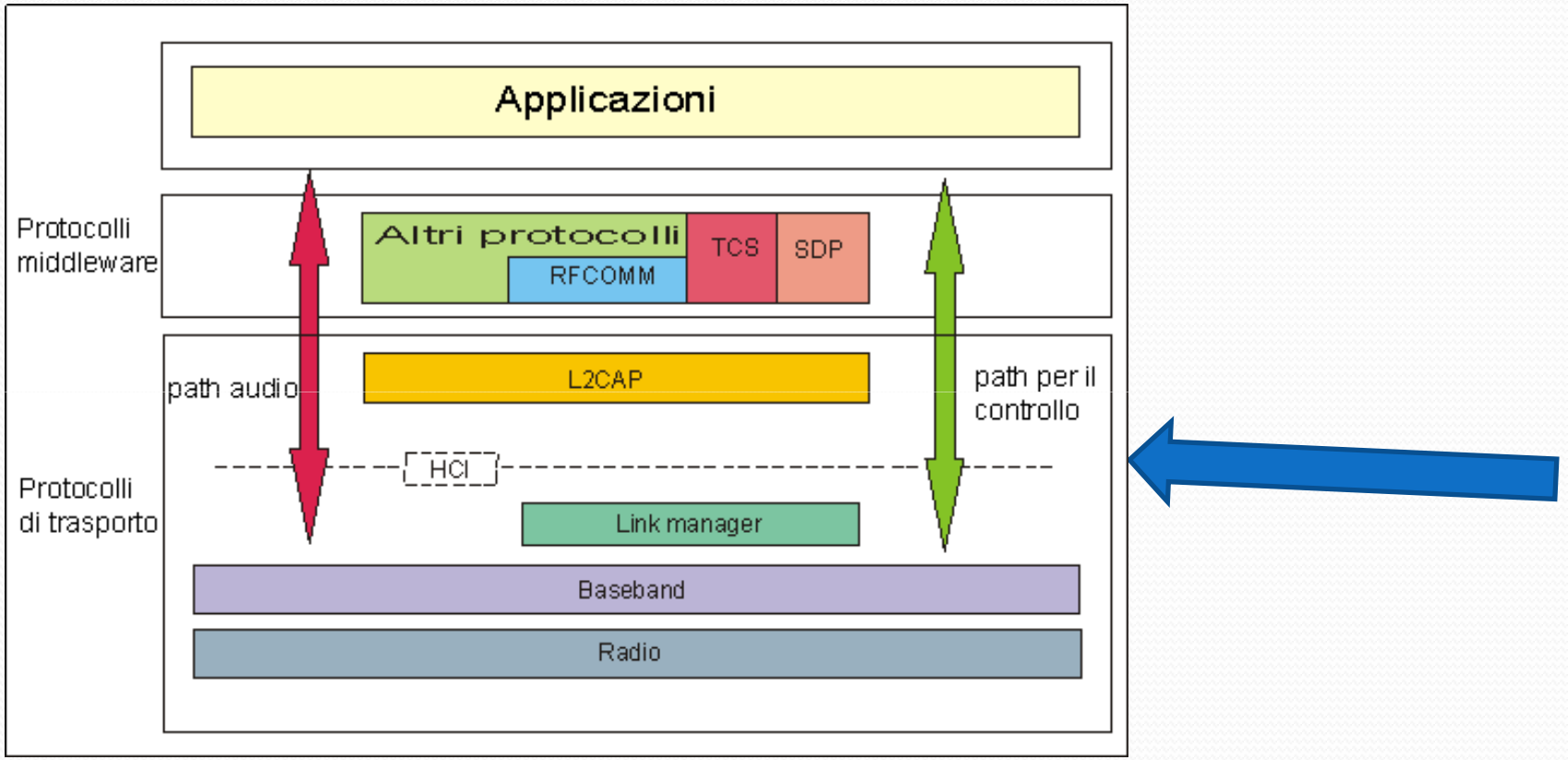
  - **Sniff Mode:** modalità a basso consumo, viene ridotta l'attività di listening, il Master invia allo slave un comando di sniff, dicendogli di ascoltare la trasmissione solo in determinati intervalli

Bluetooth™

Protocollo Link Manager (2)

- **Hold Mode:** non viene supportata la comunicazione Asincrona
- **Park Mode:** lo slave non è più tra i sette attivi ma resta comunque sincronizzato al canale risparmiando molta energia

Protocollo Host Controller Interface



Bluetooth™

Host Controller Interface

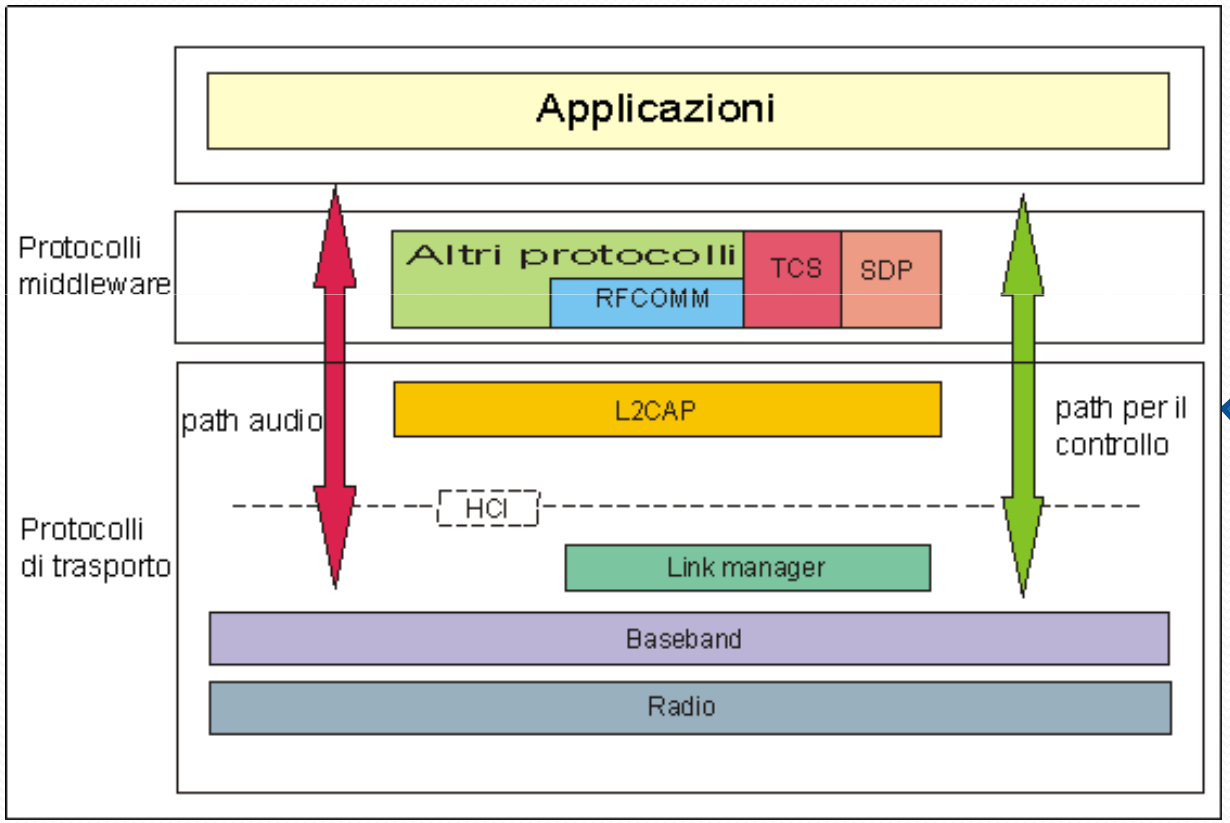
L'host controller interface è un'interfaccia standardizzata

Attraverso l'HCI i protocolli di più alto livello possono:

- inviare dati agli altri dispositivi e ricevere informazioni dalle altre unità presenti nella piconet.
- ordinare allo strato baseband di creare un link ad uno specifico dispositivo
- eseguire richieste di autenticazione
- richiedere l'attivazione della modalità a basso consumo energetico
- passare una chiave per il link

Bluetooth™

Protocollo Logical Link Control & Application



Bluetooth™

Logical Link Control & Application

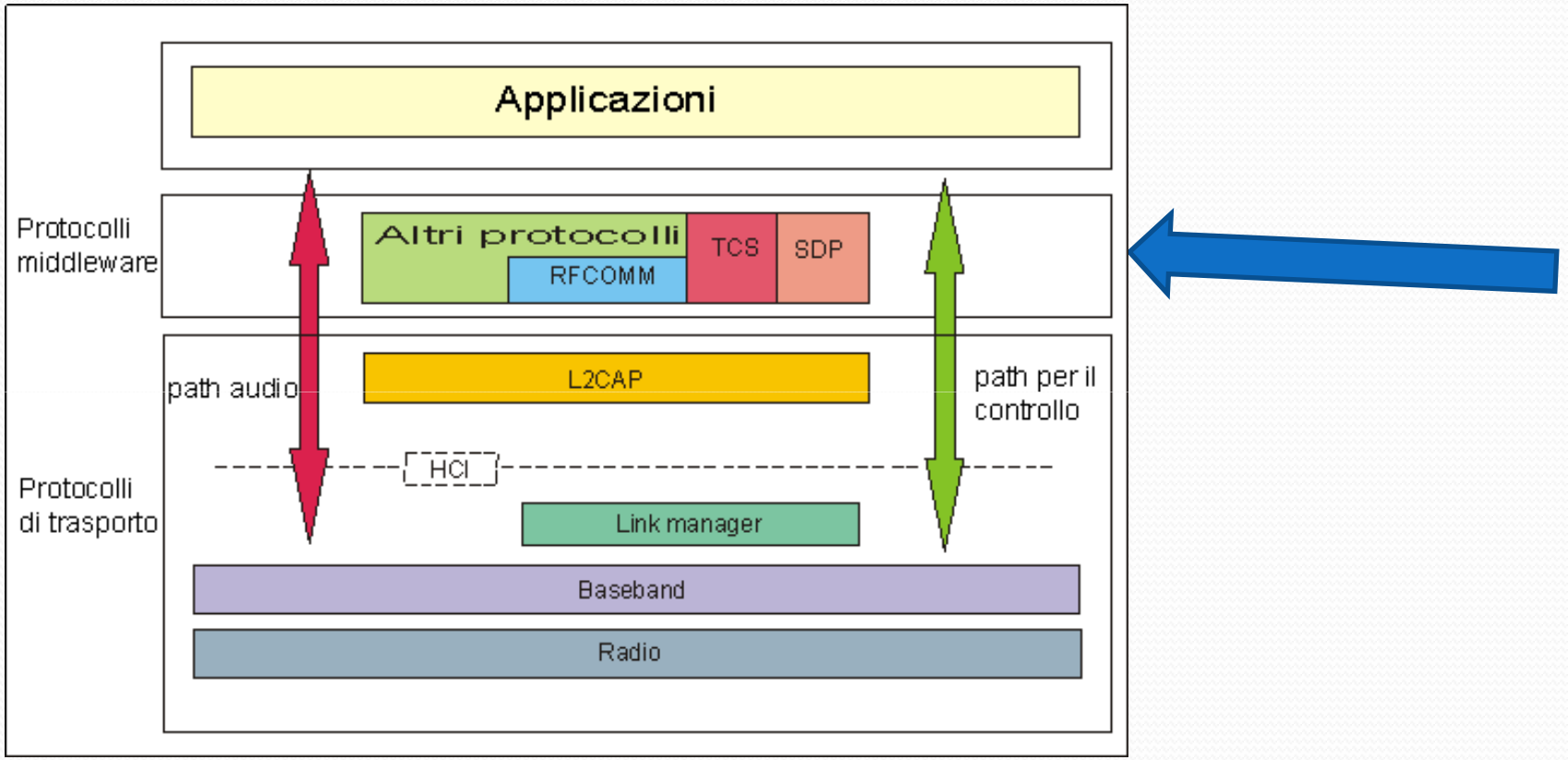
L2CAP fornisce per la trasmissione dei dati sia un servizio orientato alla connessione che uno non connesso.

Le sue funzionalità più importanti sono:

- Multiplexing
- Segmentazione dei pacchetti prodotti dagli strati superiori
- Riassemblaggio dei segmenti inviati da un altro dispositivo

Bluetooth™

Protocolli Middleware



Bluetooth™

Protocolli Middleware

- RFCOMM emula una porta seriale su Bluetooth facendo modo che tutti i dispositivi progettati per funzionare tramite un interfaccia seriale possono funzionare su Link Bluetooth
- TCS serve per trovare informazioni di altri membri appartenenti al gruppo
- SDP serve per scoprire i servizi offerti dagli altri dispositivi
- IrDA serve a far funzionare applicazioni realizzate per gli Infrarossi su dispositivi Bluetooth senza alcuna modifica

Bluetooth™

OUTLINE

- Introduzione
- Protocolli
- Profili
- Sicurezza
- Vulnerabilità

Bluetooth™

Profili Bluetooth (1)

I profili sono stati sviluppati per promuovere l'interoperabilità tra le varie implementazioni dello stack di protocolli Bluetooth.

Due dispositivi Bluetooth possono ottenere una funzionalità comune solo se entrambi i dispositivi supportano profili identici.

Ci sono 4 differenti profili:

- General
- Telephony
- Network
- Serial and Object exchange

Bluetooth™

Profili Bluetooth (2)

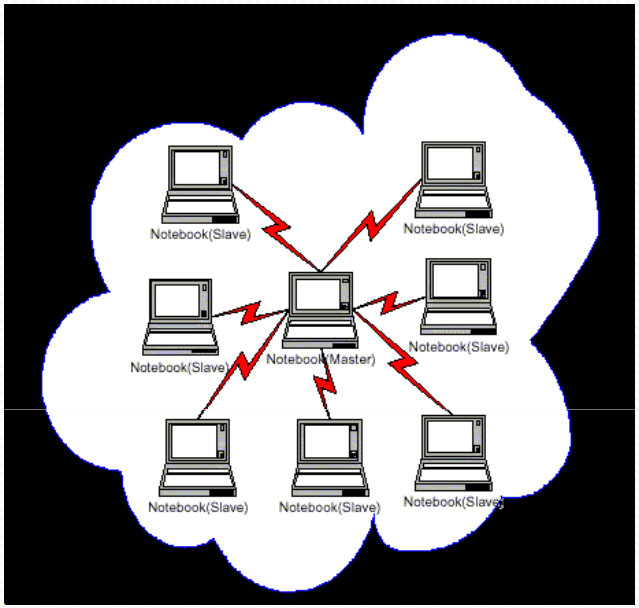
- **General:** fornisce un mezzo per effettuare delle connessioni tra Master e Slave, utilizza il SDP per scoprire i servizi offerti dagli altri utenti

- **Telephony:** tramite il quale possiamo utilizzare Bluetooth nelle comunicazioni vocali, tra telefoni e telefoni oppure tra auricolari e telefoni o portatili

Bluetooth™

Profili Bluetooth (3)

- **Network:** il profilo LAN Access abilita i dispositivi Bluetooth sia a connettersi ad una LAN attraverso APs che a formare una piccola LAN wireless tra di loro



- **Serial and object exchange profiles:** il profilo che simula una porta seriale per applicazioni che richiedono una porta seriale

Bluetooth™

OUTLINE

- Introduzione
- Protocolli
- Profili
- Sicurezza
- Vulnerabilità

Bluetooth™

Sicurezza in Bluetooth(1)

Lo standard Bluetooth specifica 3 servizi base di sicurezza:

- **Autenticazione:** serve a verificare l'identità dei dispositivi con i quali comunicare
- **Riservatezza:** garantisce che i dati non siano intercettati da dispositivi non autorizzati
- **Autorizzazione:** permette il controllo delle risorse assicurando che un dispositivo è autorizzato ad usare un servizio prima di accedervi

Bluetooth™

Sicurezza in Bluetooth(2)

La specifica Bluetooth prevede tre livelli di sicurezza che devono essere implementati nei dispositivi:

- **Mode 1:** nessuna sicurezza, non c'è nessun controllo sulle autenticazioni e nessuna cifratura dei dati
- **Mode 2:** procedure di protezione a livello di servizio/applicazione, è possibile far associare nuovi dispositivi e consentire l'accesso a tutti i servizi o solo in parte
- **Mode 3:** procedura di protezione a livello di dispositivo; usando questa modalità è possibile far comunicare due o più dispositivi solo se questi sono stati già associati e quindi sono considerati "fidati"

Bluetooth™

Sicurezza in Bluetooth(3)

La sicurezza è garantita per mezzo di 4 entità:

- un indirizzo pubblico, BD_ADDR, unico per ciascun dispositivo (48 bit)
- due chiavi segrete:
  - chiave per l'autenticazione (autentication key 128 bit)
  - chiave privata per la cifratura (encryption key da 8 a 128 bit)
- numeri casuali differenti per ogni nuova transazione (128 bit)
  - non-repeating
  - randomly generated

La generazione di chiavi sicure la si ottiene tramite l'utilizzo degli algoritmi:

- E0, E1, E21, E22, E3

Bluetooth™

Sicurezza in Bluetooth: fase1

La sicurezza è garantita dall'esecuzione di vari passi divisibili in 3 fasi.

Fase 1

A

B

Prima accensione del dispositivo

Prima accensione del dispositivo

Chiave associata al dispositivo

Generazione unit key

Generazione unit key

Bluetooth™

Sicurezza in Bluetooth: fase2

Fase 2

A   B

Primo Handshake

Generazione initialization key (K_{init})

↓

Autenticazione (usando K_{init})

↓

Scambio link key

link key
=
chiave associata ad un link
tra due dispositivi

Bluetooth™

Sicurezza in Bluetooth: fase3

Fase 3

A   B

Handshake successivi

Autenticazione (usando la link key K_{AB})

↓

Generazione encryption key

↓

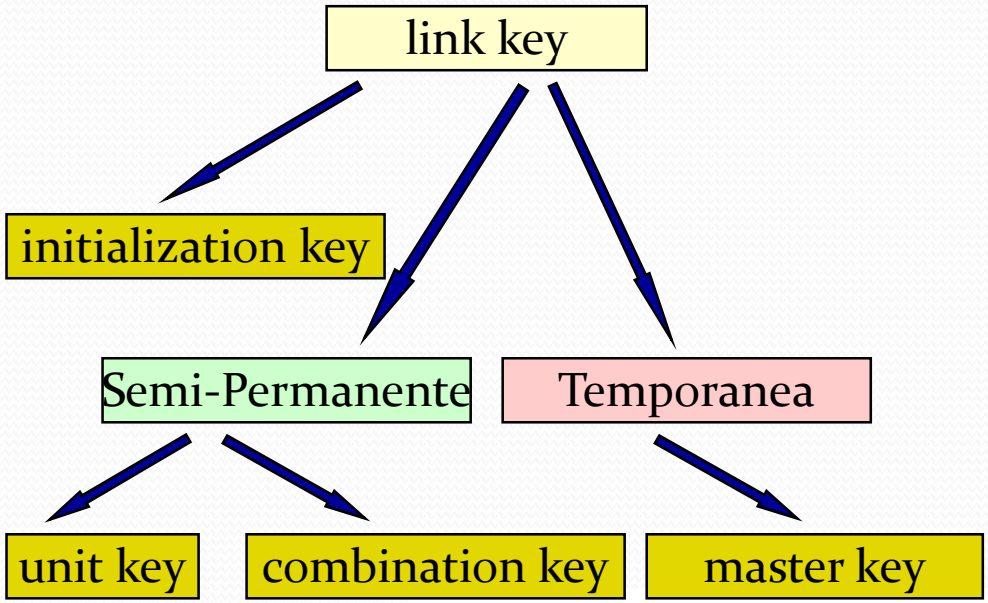
Comunicazioni cifrate

Bluetooth™

Tipi di Link Key (1)

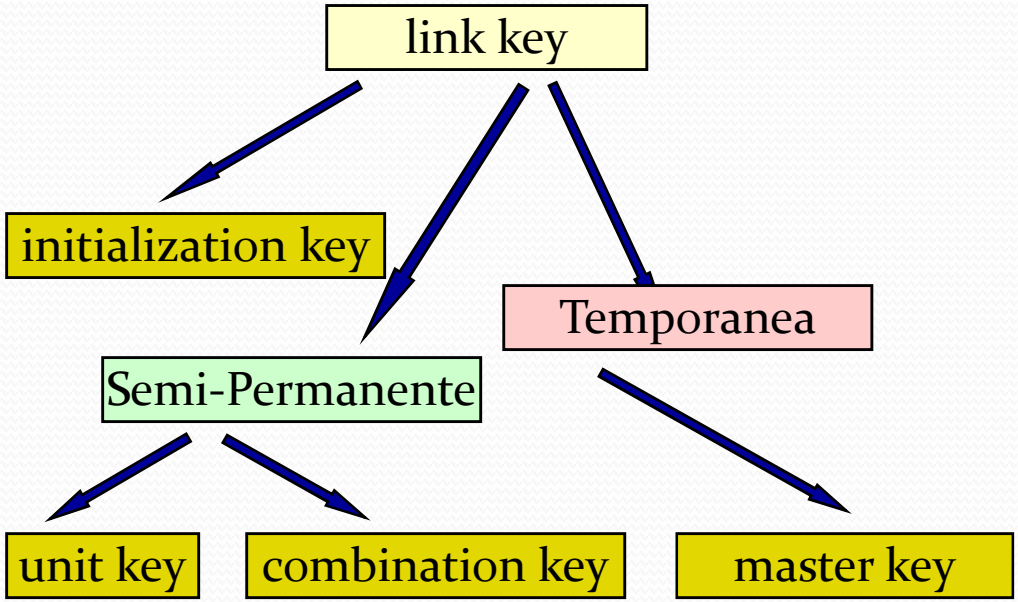
Una link key è una chiave associata ad un link esistente tra due dispositivi, può essere:

- Una initialization key, creata in fase di inizializzazione
- Una link key semi-permanente
- Una link key temporanea



Bluetooth™

Tipi di Link Key (2)

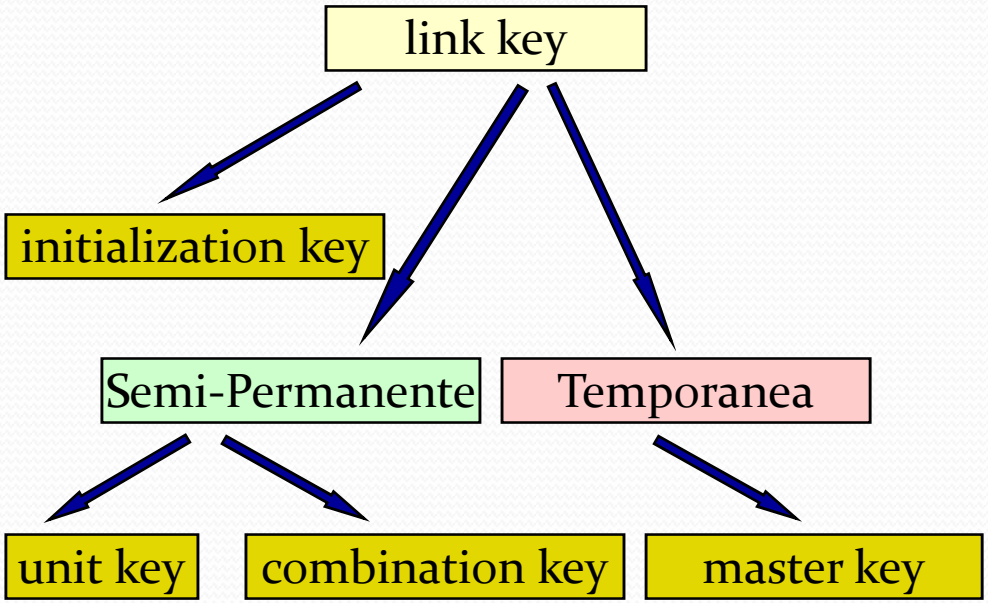


1. Una initialization key, K_{init}, è creata quando due dispositivi entrano in contatto per la prima volta

2. Una unit key, K_A, è generata da un dispositivo nell'istante in cui è acceso per la prima volta

Bluetooth™

Tipi di Link Key (3)



3. Una combination key, K_{AB}, è ottenuta da informazioni prodotte da una coppia di dispositivi, A e B

4. Una master key, K_{master}, è usata dal dispositivo master quando vuole trasmettere contemporaneamente a più dispositivi slave

Bluetooth™

Fase 1

A

B

Prima accensione del dispositivo

Prima accensione del dispositivo

Chiave associata al dispositivo

Generazione unit key

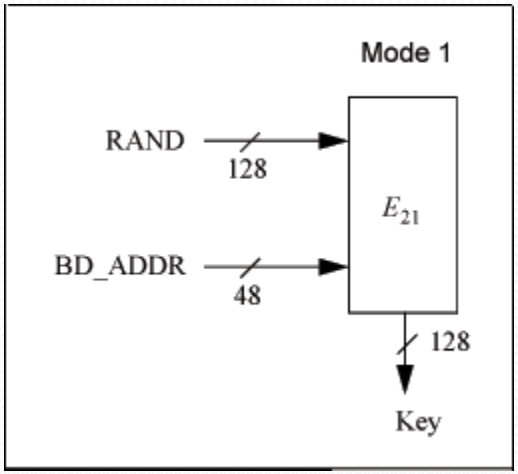
Generazione unit key

Generazione della Unit Key

Una Unit Key viene generata tramite l'algoritmo E21 quando un dispositivo si avvia per la prima volta

L' algoritmo E21 prende in input:

- BD_ADDR (indirizzo Bluetooth del dispositivo)
- RAND (numero casuale di 128 bit)



Bluetooth™

Fase 2

A

B

Primo Handshake

Generazione initialization key (K_{init})

↓

Autenticazione (usando K_{init})

↓

Scambio link key

link key
=
chiave associata ad un link tra due dispositivi

Bluetooth™

Generazione della Initialization Key (1)

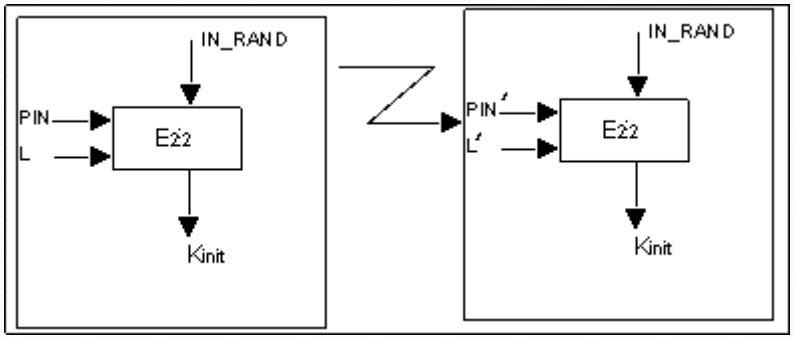
Una Initialization Key viene generata tramite l'algoritmo E22 quando due dispositivi entrano in contatto per la prima volta, uno dei due il Richiedente (B) prova a raggiungere il Verificatore (A)

Il Richiedente deve dimostrare al Verificatore di essere un dispositivo autorizzato ovvero di condividere lo stesso PIN

Il PIN è un **P**ersonal **I**dentification **N**umber, nei dispositivi Bluetooth può variare tra 1 e 16 bytes. Le tipiche 4 cifre spesso usate per i codici PIN sono sufficienti per una situazione a basso rischio, mentre per avere un alto livello di sicurezza può deve essere usato un PIN più lungo.

Bluetooth™

Generazione della Initialization Key (2)



Viene prima di tutto generata una initialization key in entrambi i dispositivi, sulla base di questo PIN, e poi è avviata la fase di autenticazione in cui A accerta che B condivide con se una stessa link key, che in questa fase coincide con l'initialization key appena generata.

Autenticazione(1)

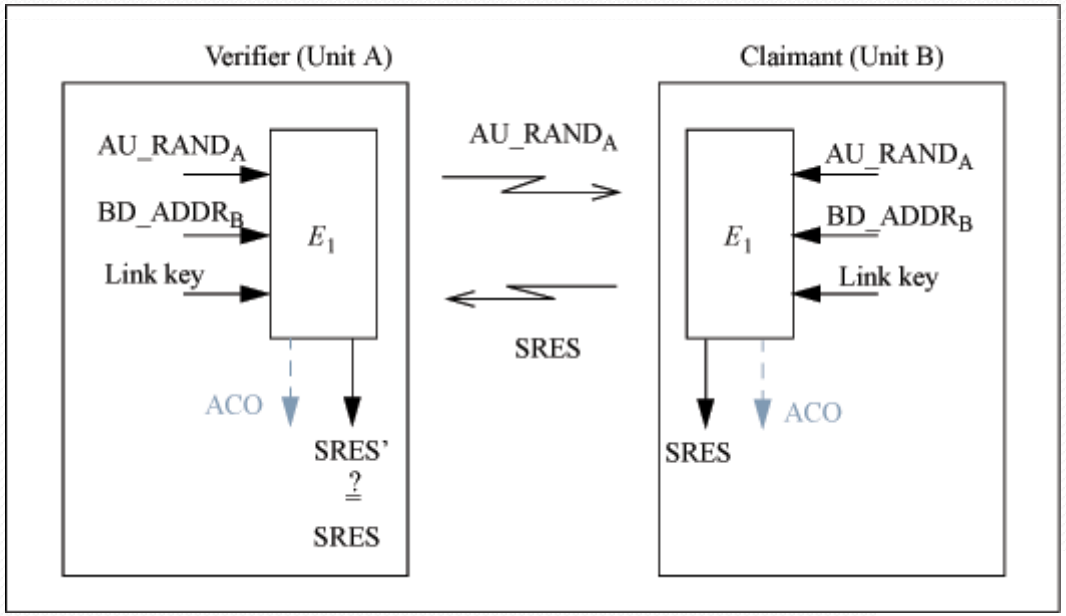
Viene usata la link key K_{AB} decisa dai due dispositivi

Il processo di autenticazione si basa su uno schema di challenge-response in cui un dispositivo verificatore accerta che uno richiedente condivida con se una certa chiave segreta

Autenticazione(2)

Entrambi i dispositivi basano l'autenticazione sull'algoritmo E1, che ritorna come risultato i valori SRES e ACO (Authenticated Ciphering Offset) prendendo in input:

- un numero casuale AU_RAND_A prodotto dal dispositivo verificatore A;
- l'indirizzo Bluetooth del dispositivo B, che richiede di essere autenticato;
- l'attuale link key.



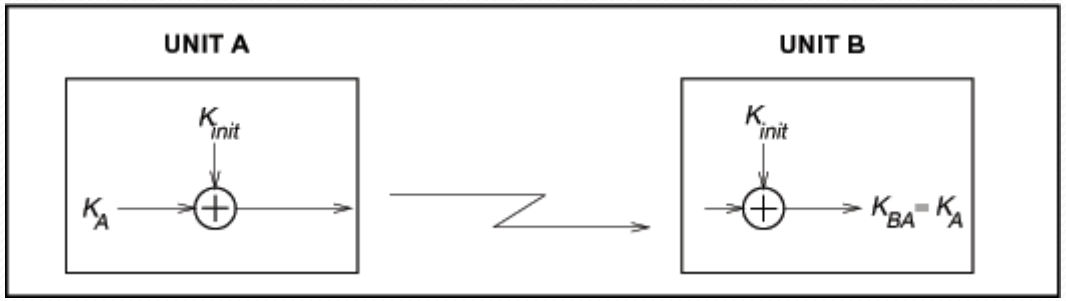
Bluetooth™

Scambio della Link Key(1)

La chiave associata al link tra due dispositivi dipende dal grado di sicurezza richiesto e dalle capacità di memoria dei dispositivi, può essere:

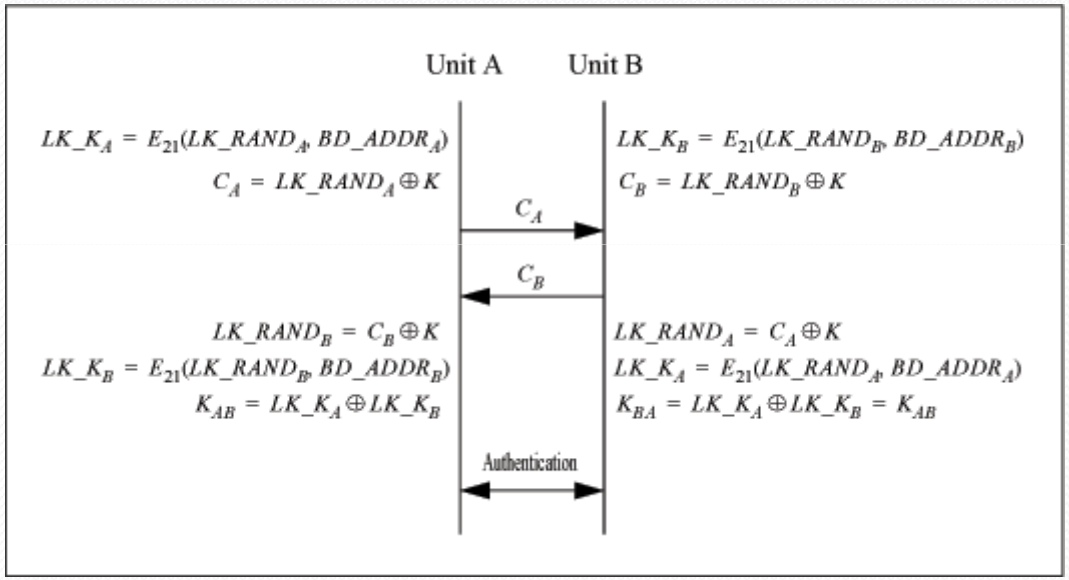
- La Unit Key di uno di essi;
- Una Combination Key ottenuta da informazioni prodotte da entrambi i dispositivi

Esempio di 2 dispositivi che usano la Unit Key del dispositivo A:



Scambio della Link Key(2)

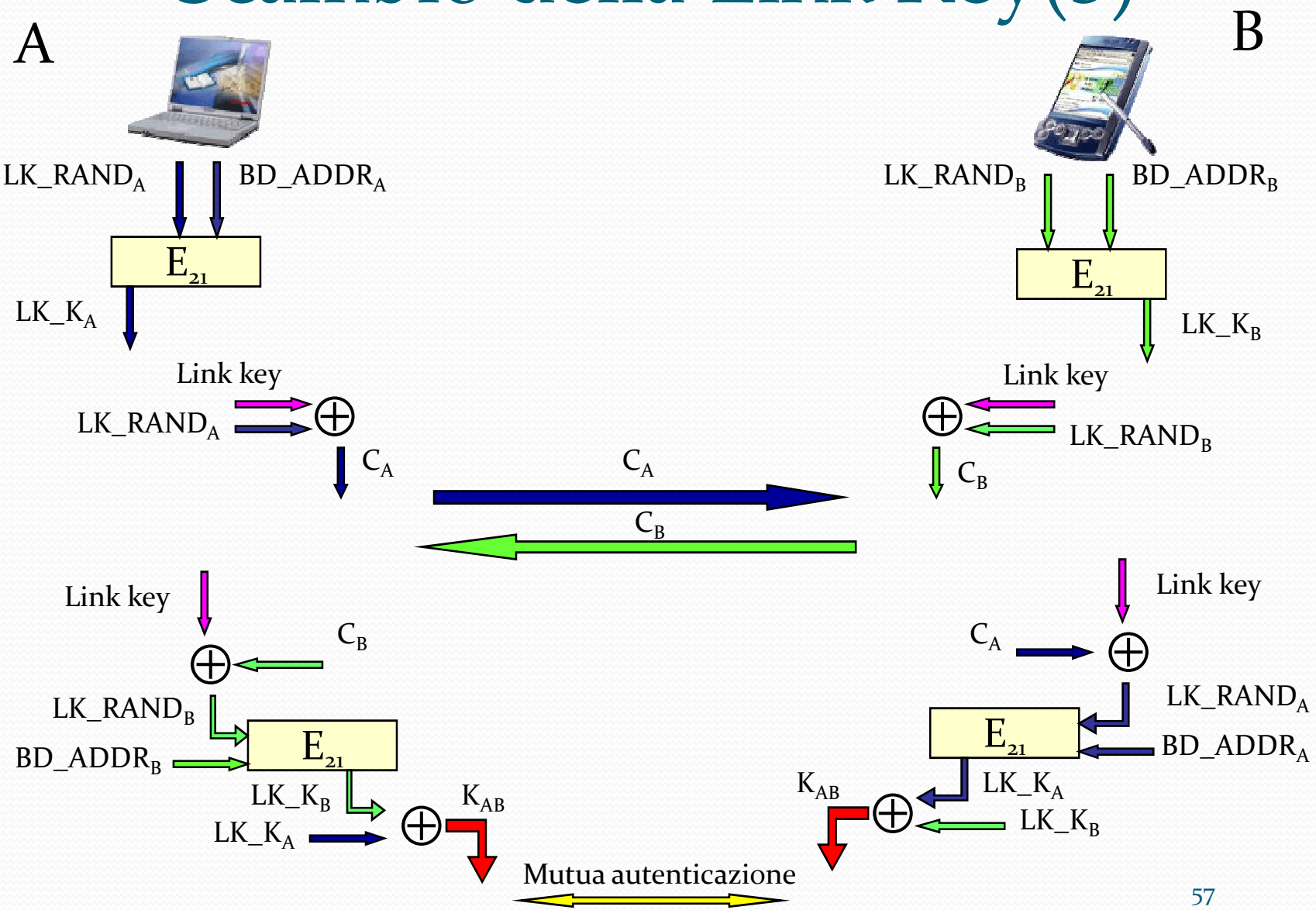
Esempio di generazione di una Combination Key:



Entrambi i dispositivi basano l'autenticazione sull'algoritmo E21

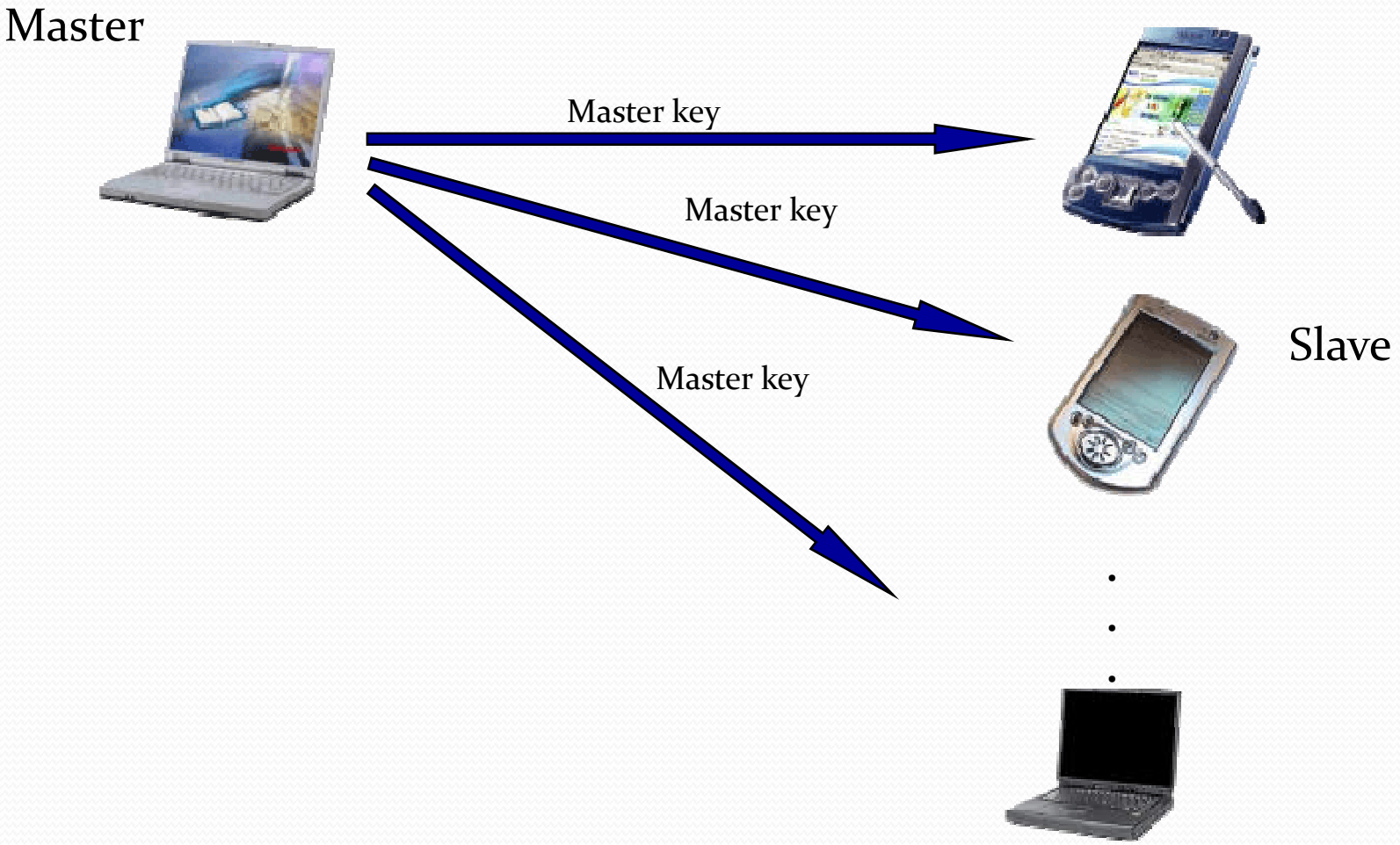
Bluetooth™

Scambio della Link Key(3)



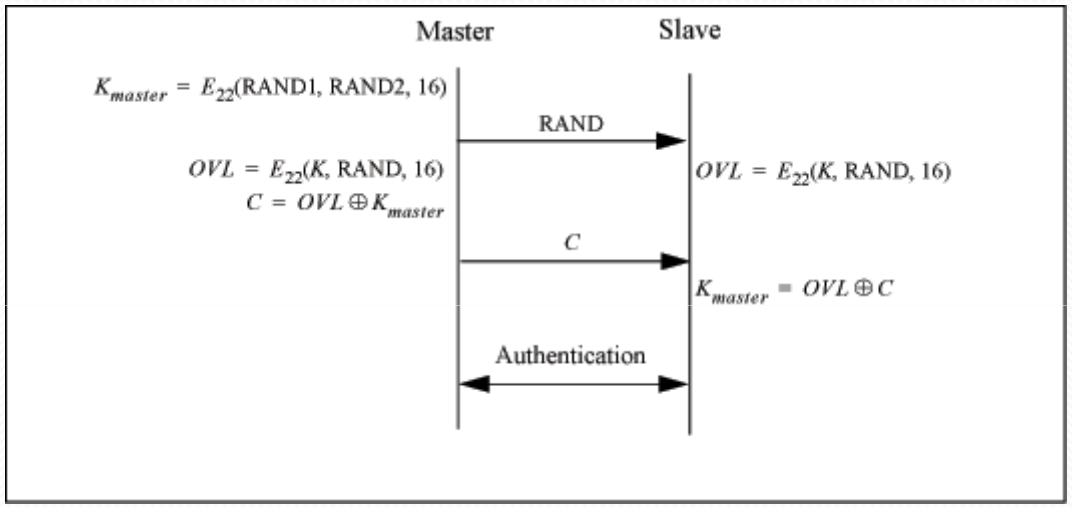
Generazione Master Key(1)

Una Master Key è creata dal dispositivo Master in caso di trasmissione della stessa informazione a più dispositivi slave



Generazione Master Key(2)

Esempio di generazione di una Master Key:

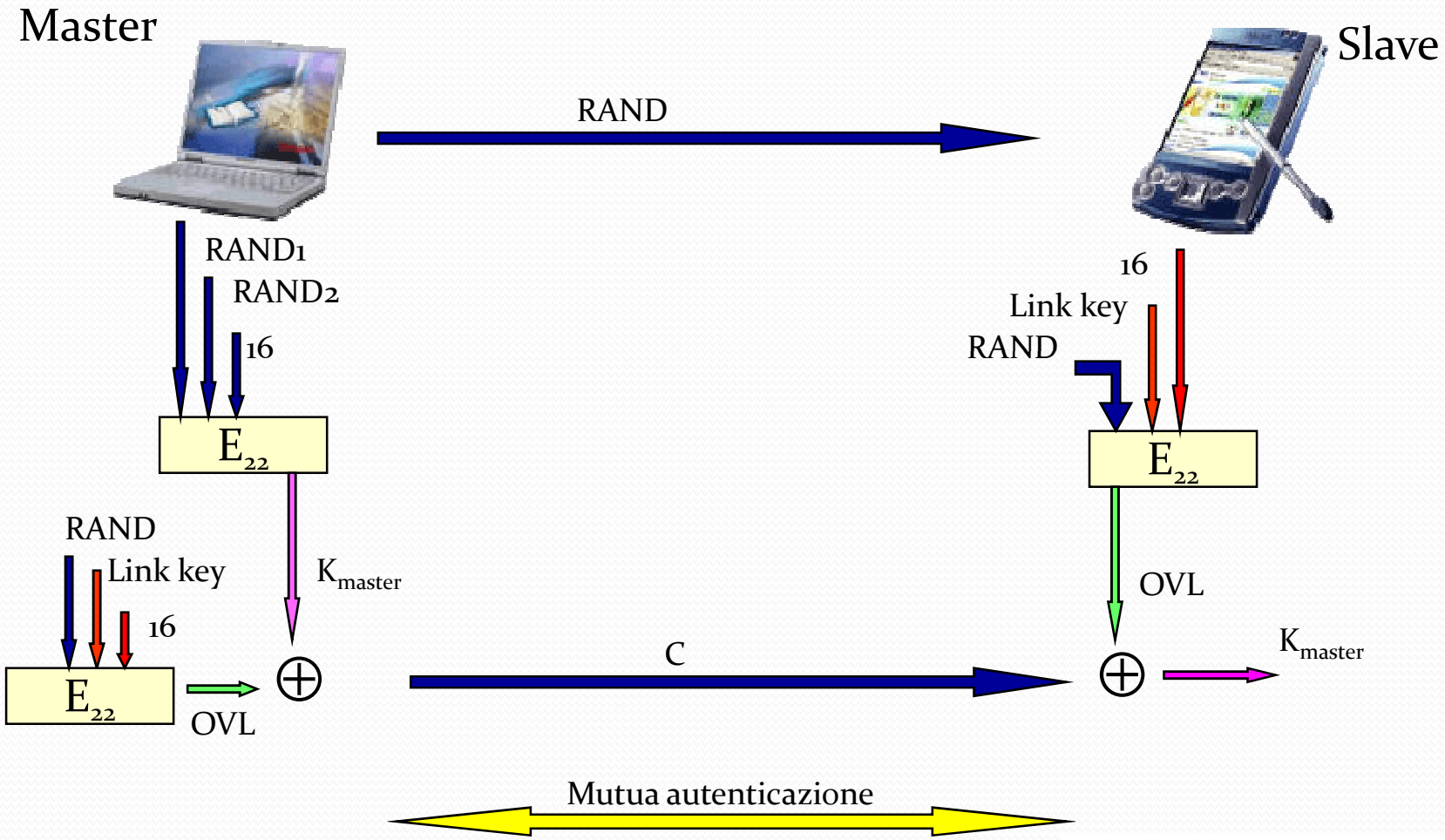


Entrambi i dispositivi basano l'autenticazione sull'algoritmo E22

Utilizzando l'algoritmo E_{22} con la corrente link key e RAND come input, sia il master che lo slave calcolano un valore, detto overlay, OVL, a 128 bit

Bluetooth™

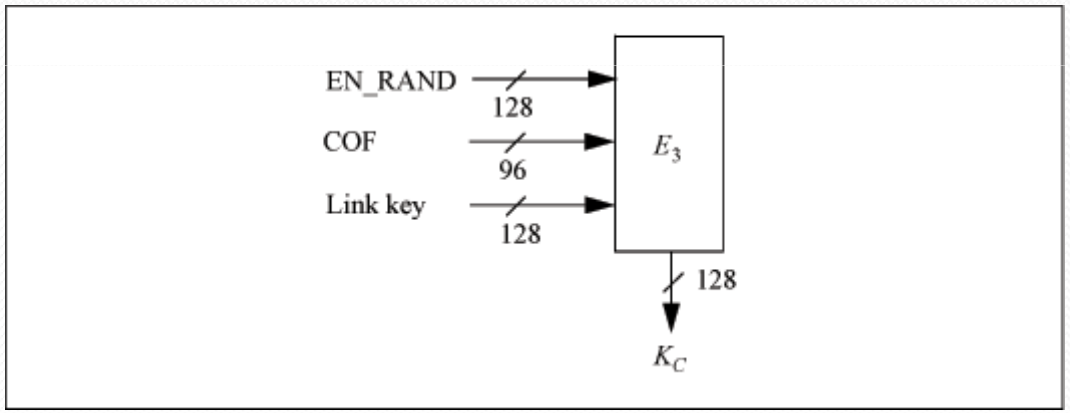
Generazione Master Key(3)



Encryption(1)

In Bluetooth, le informazioni utente sono protette cifrando prima della trasmissione il campo payload dei pacchetti, ovvero il campo che contiene le vere e proprie informazioni da trasmettere.

Come prima cosa viene creata una Encryption Key utilizzando l'algoritmo E3

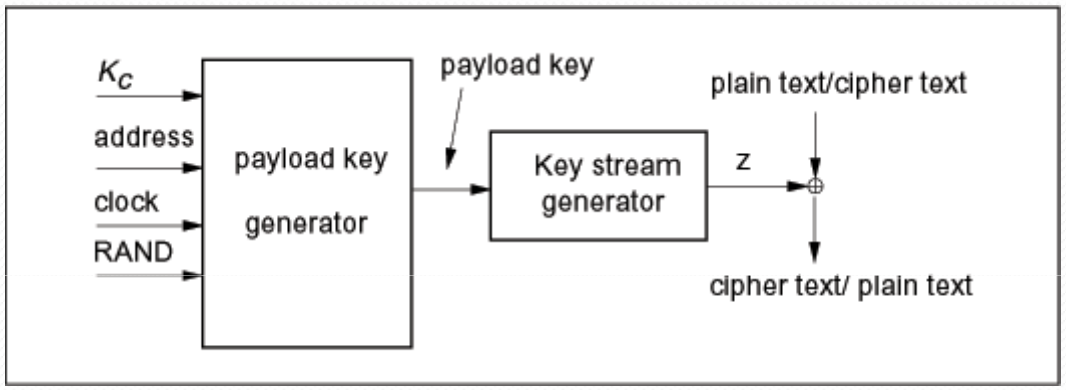


dove COF = { BD_ADDR U BD_ADDR se la link key è master key
ACO altrimenti

Bluetooth™

Encryption(2)

La cifratura è ottenuta per mezzo dello Stream Cipher E0, che viene nuovamente sincronizzato per ogni nuovo payload trasmesso.



Lo Stream Cipher consiste sostanzialmente di 3 parti:

- La prima esegue l'inizializzazione, ovvero genera la chiave per il payload (tramite l'algoritmo E0)
- La seconda genera i bit del key stream
- La terza esegue la cifratura o la decifratura delle informazioni trasmesse come XOR bit a bit tra ogni bit del testo in chiaro/cifrato e ogni bit generato dal key stream generator

Bluetooth™

OUTLINE

- Introduzione
- Protocolli
- Profili
- Sicurezza
- Vulnerabilità

Attacchi(1)

Esistono varie tipologie di attacchi:

- **Attacchi contro il protocollo:**
  Aggressione contro gli elementi deboli del protocollo
  Gravità: Media
  Tipologie: Attacco a E22, Spoofing, BlueDump, DOS

- **Attacchi contro le funzionalità di discovery:**
  Identificazione dei dispositivi, abuso delle informazioni di discovery
  Gravità: bassa
  Tipologie: Bluejacking, Discovery Mode Abuse, Blueprinting

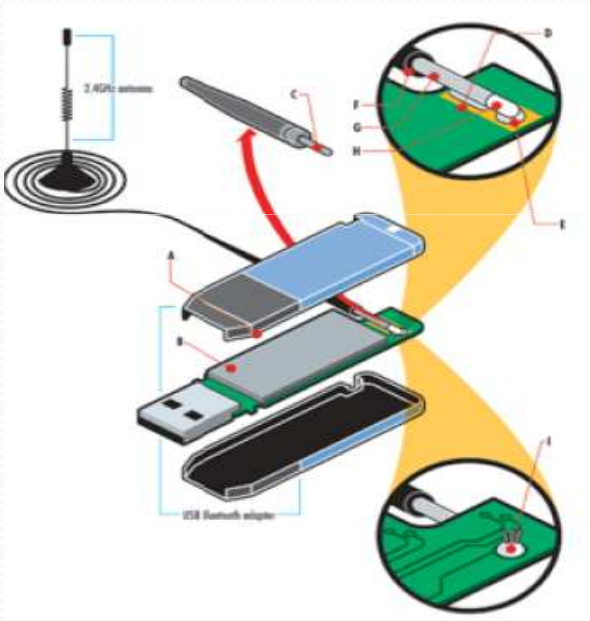
Bluetooth™

Attacchi(2)

- **Attacchi contro i servizi offerti dai dispositivi**
  Abuso dei servizi e prelievo di informazioni
  Gravità: alta
  Tipologie: BlueSnarf, HELOMoto, Bluebug, BlueBump, Bluesmack, CarWhisperer

Attacchi(3)

Questi attacchi si possono fare esclusivamente a causa delle lacune nell'implementazione dello Standard, si corrono rischi nonostante questa tecnologia ha un range di utilizzo limitato

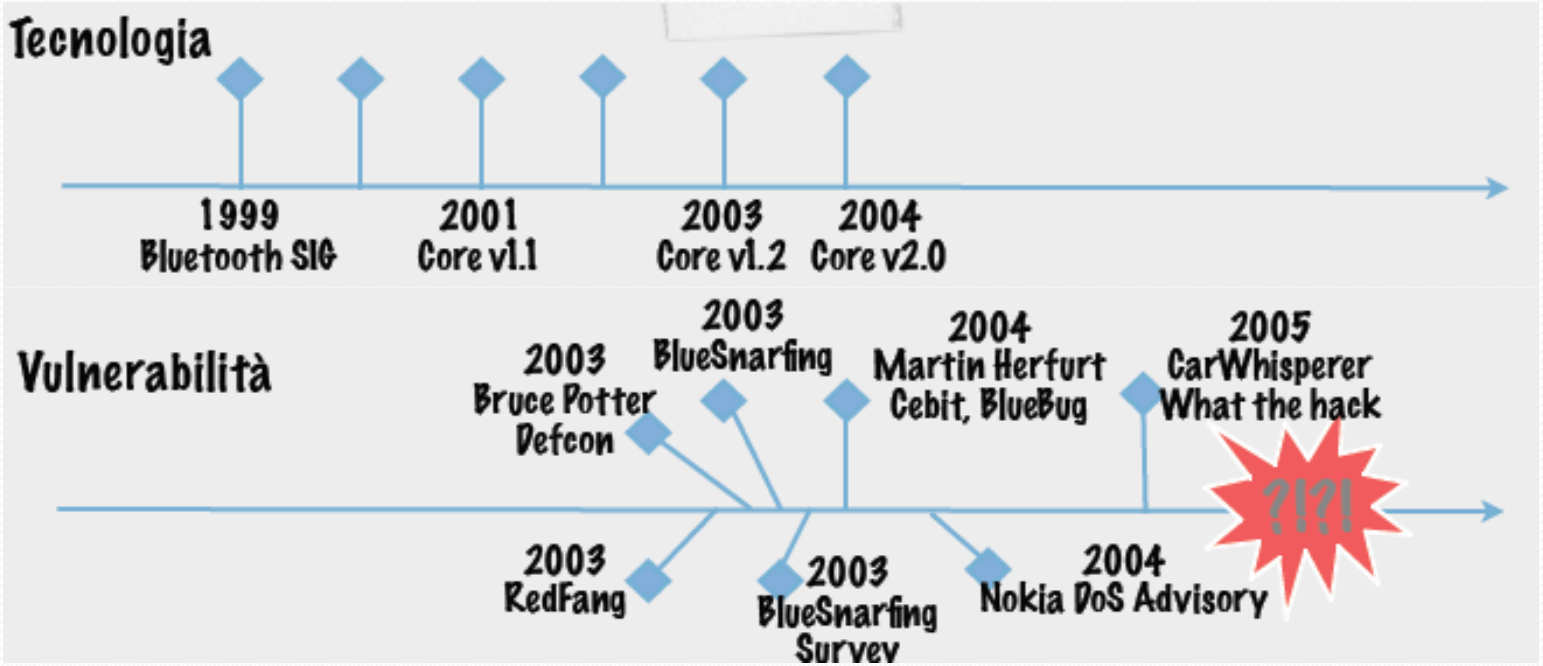


Si possono raggiungere distanze di 1,78 Km costo 14 euro
http://www.ikkisof t.com/security.html

Bluetooth™

Attacchi(4)

Evoluzione nel tempo dello standard Bluetooth e degli attacchi a esso rivolti:



Ne vedremo alcuni....

Bluetooth™

Attacco a E22

Si cerca di scoprire il PIN del dispositivo vittima tramite un attacco BRUTE FORCE

Questo elemento è il “segreto condiviso” dell’algoritmo, ma spesso si tratta solamente di quattro cifre decimali

Un attacco “brute-force” può essere fattibile in due modalità:

- Attacco offline: Serve un registratore frequenziale
  ($ costoso $)
- Attacco online: nel caso di dispositivi con pin assegnato

Bluetooth™

Equivalente del Phishing in ambito Web

Durante la fase di Discovery di altri apparecchi viene scambiato il nome identificativo dei device, un intruso può sfruttare questa informazione per mandare messaggi del tipo:

- " Problemi alla Rete, digita 1234 per associare il telefono alla cella"
- " Vodafone ti regala una suoneria …. digita 1234 per proseguire "

L' utente inesperto potrebbe essere tratto in inganno, facendo diventare Trusted dispositivo sconosciuto che quindi acquisirebbe tutti i privilegi necessari a compromettere i dati e le comunicazioni

Bluetooth™

Bluejacking

Per questo tipo di attacco sono stati sviluppati una serie di software appositi (Freejack, BlueJackX, Meeting)

Bluetooth™

Discovery Mode Abuse (1)

Un dispositivo Bluetooth può selezionare vari modi di funzionamento:

- Acceso (Visibile)
- Acceso (Nascosto)
- Spento

Quando un dispositivo è nascosto non fa nient'altro che scartare tutte le richieste di Inquiry inviate in Broadcast da altri dispositivi che vogliono conoscere la presenza di soggetti con cui comunicare

Bluetooth™

Discovery Mode Abuse (2)

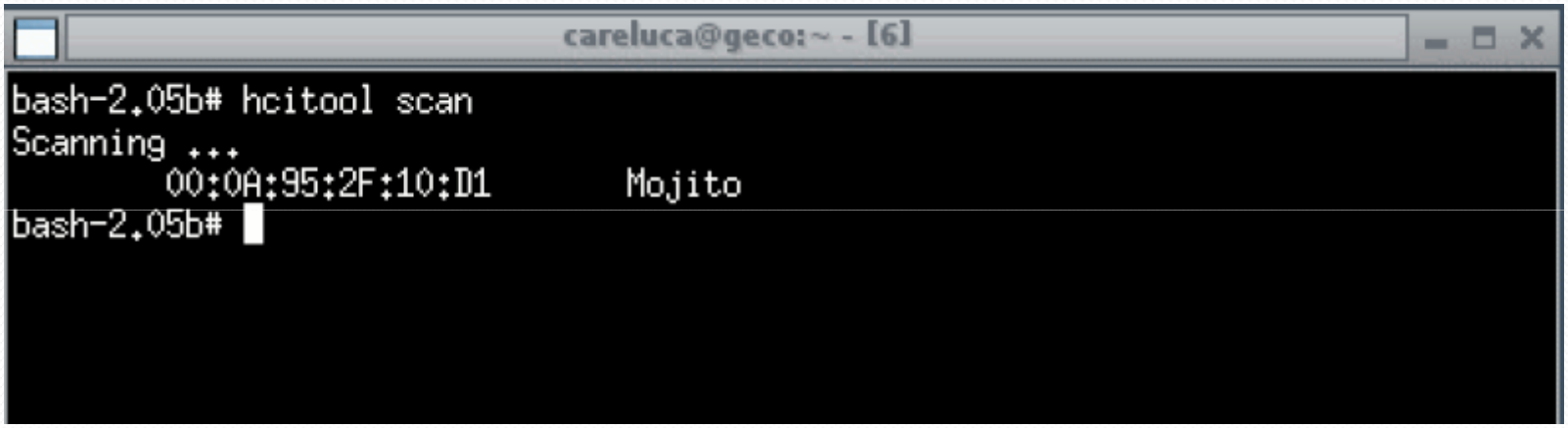
Un dispositivo nascosto non disabilita i suoi servizi, in questo modo alcuni apparecchi possono comunque interrogare il singolo dispositivo,
che risponde normalmente alle richieste

@Stake ha realizzato un software RedFang in grado di scoprire i dispositivi nascosti, inoltre tramite un meccanismo di brute-forcing può scoprire anche B_ADDR del dispositivo,
(24 bit del costruttore e 24 identificano il dispositivo) in circa un' ora

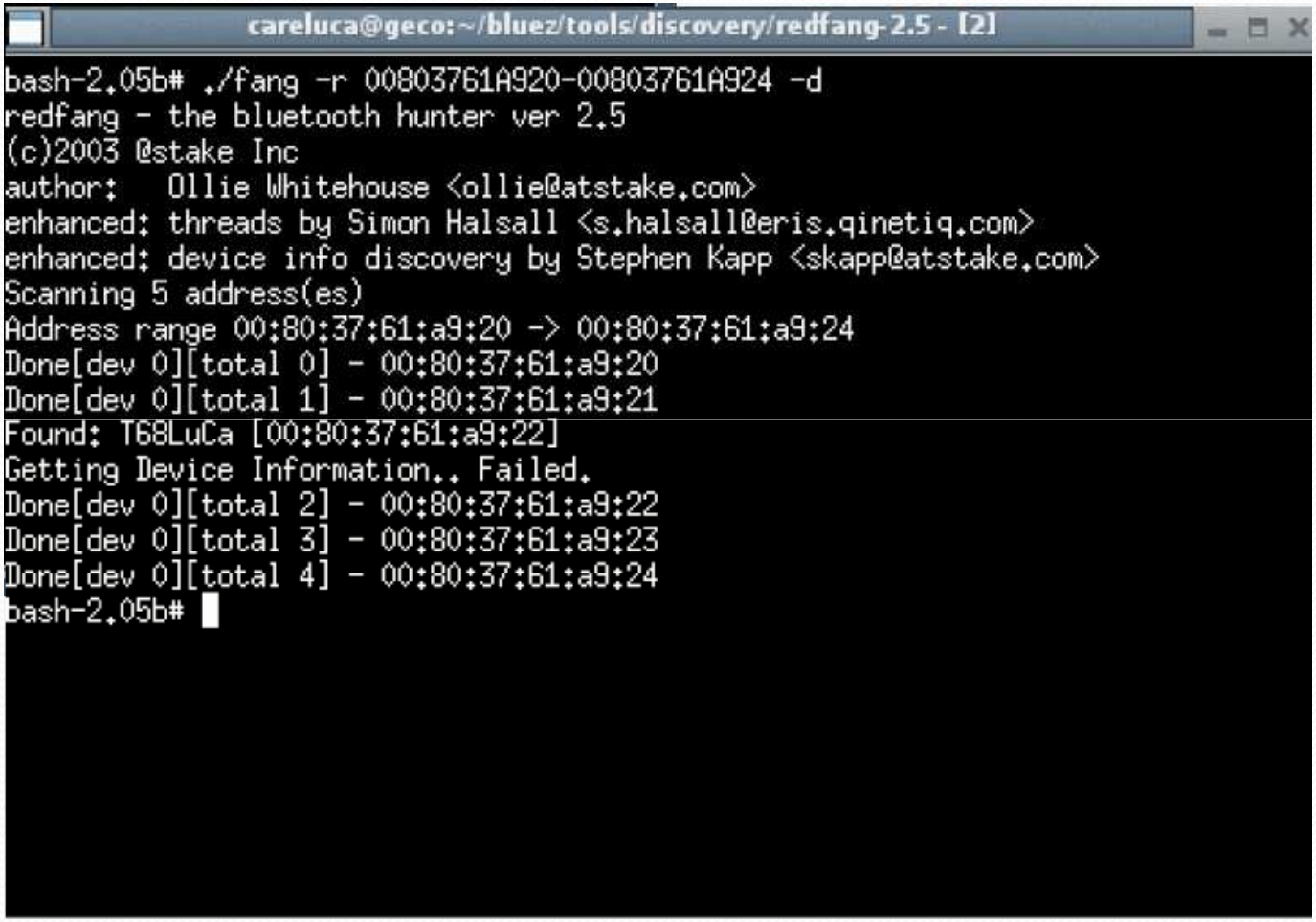
Bluetooth™

Discovery Mode Abuse Esempio(1)

RedFang:



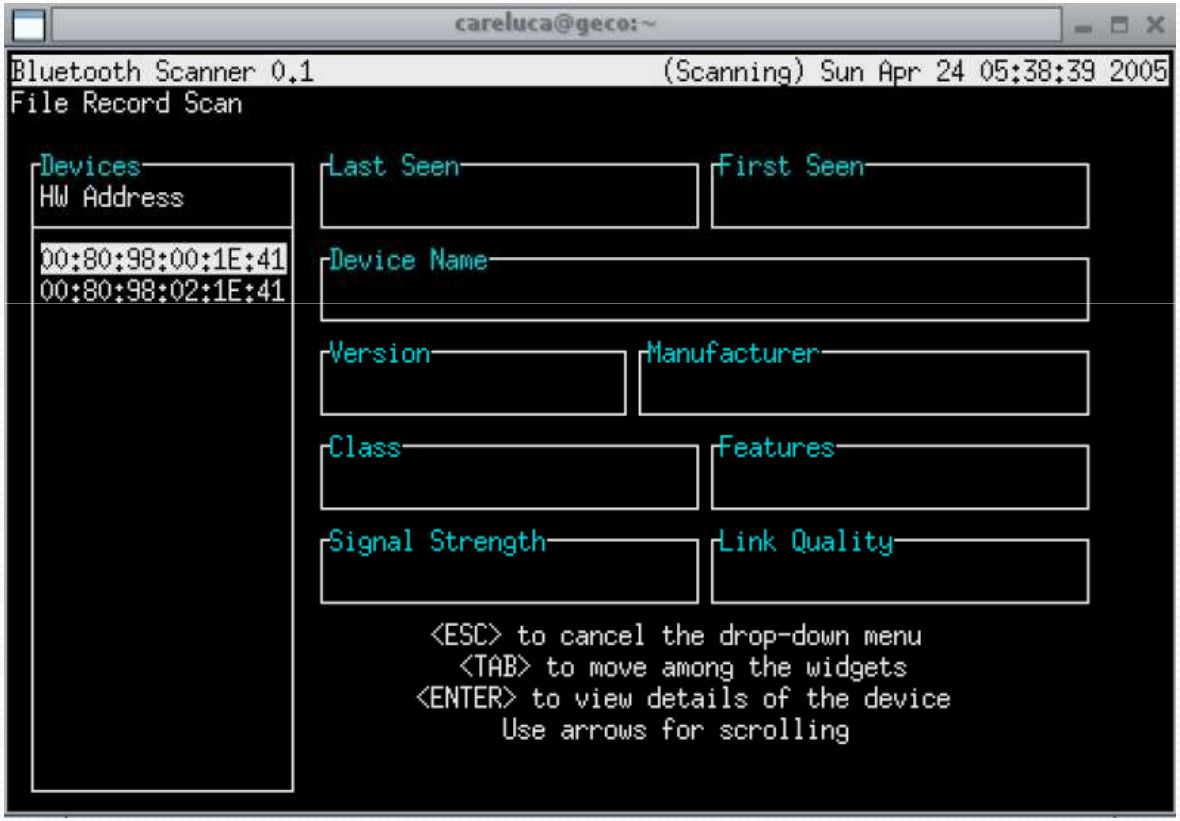
Discovery Mode Abuse Esempio(2)



Bluetooth™

Discovery Mode Abuse Esempio(3)

BluSniff:



Bluetooth™

- In molti cellulari è spesso implementato il servizio OBEX Push, che serve a scambiarsi il biglietto da visita

- Non in tutti i dispositivi è implementato in maniera ottima questo servizio, infatti è permesso anche l'OBEX Get, ovvero la richiesta di un file

- Conoscendo la presenza di qualche oggetto sul dispositivo è possibile scaricarla senza autenticazione, la necessità di conoscere un path è sorvolata dal fatto che in molti apparecchi le informazioni sono mantenute in file disposti dal sistema

- Ci sono molti dispositivi esposti a questo rischio: Ericsson T68, Sony Ericsson T68m, T68i, T610, Z1010, Z600, R520m, Nokia 6310, 7650, 8910 e molti altri

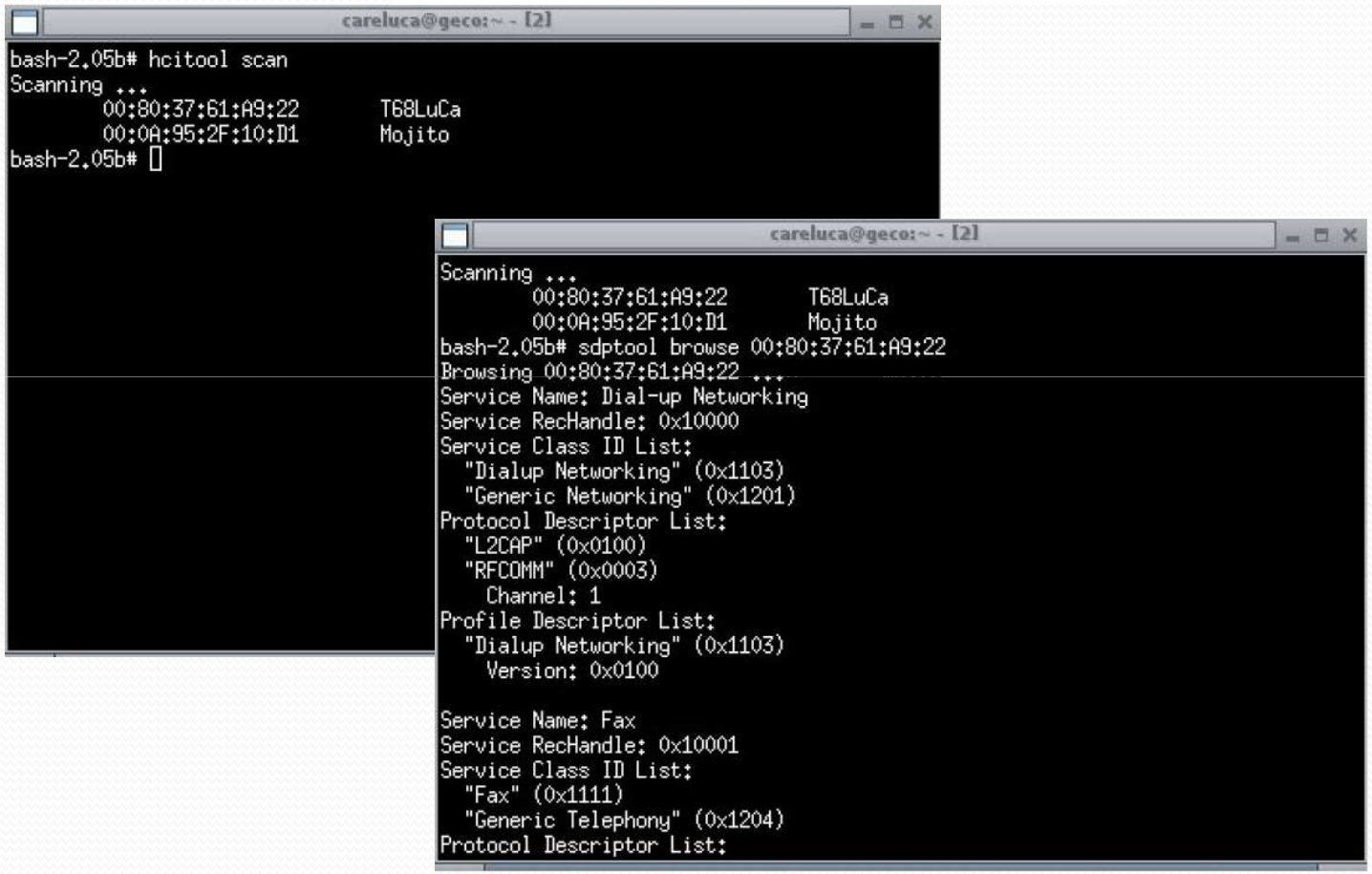
Bluetooth™

Ci sono molte varianti di BlueSnaff, tra queste le più conosciute sono:

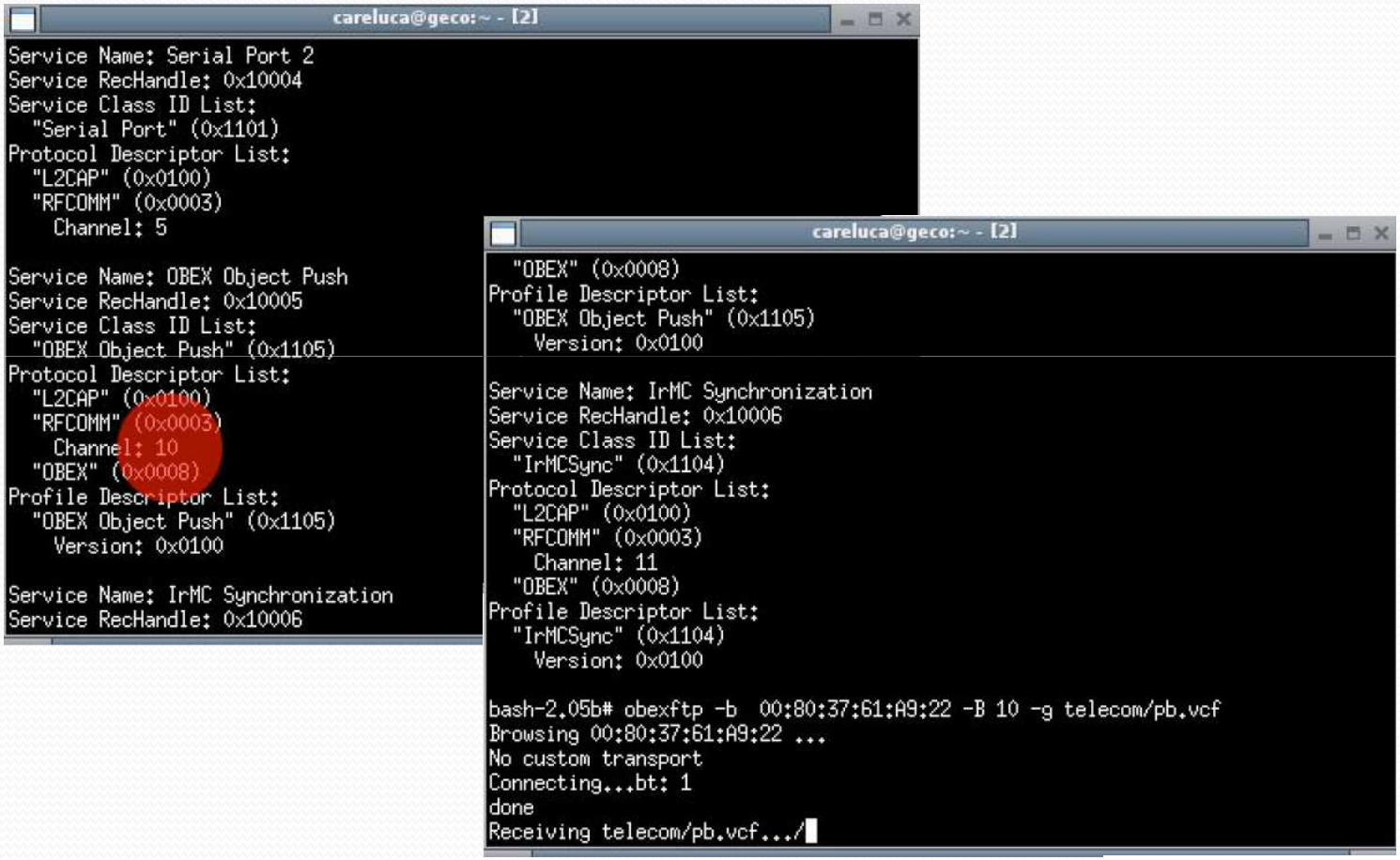
- **BlueSnaf++** che permette oltre al download dei file anche un accesso completo al filesystem dei dispositivi vittima

- **HeloMoto** è la versione per i dispositivi Motorola, e offre all' aggressore il pieno accesso ai comandi AT (ASCII Terminal) del dispositivo, dando cosi un pieno controllo:
  - Invio di chiamate
  - Invio, Lettura e Cancellazione di SMS
  - Lettura e Scrittura della rubrica
  - Modifica dei parametri di configurazione

Bluetooth™


BlueSnarf™
careluca@geco:~ - [2]
bash-2.05b# hcitool scan
Scanning ...
00:80:37:61:A9:22 T68LuCa
00:0A:95:2F:10:D1 Mojito
bash-2.05b#
careluca@geco:~ - [2]
Scanning ...
00:80:37:61:A9:22 T68LuCa
00:0A:95:2F:10:D1 Mojito
bash-2.05b# sdptool browse 00:80:37:61:A9:22
Browsing 00:80:37:61:A9:22 ...
Service Name: Dial-up Networking
Service RecHandle: 0x10000
Service Class ID List:
"Dialup Networking" (0x1103)
"Generic Networking" (0x1201)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 1
Profile Descriptor List:
"Dialup Networking" (0x1103)
Version: 0x0100
Service Name: Fax
Service RecHandle: 0x10001
Service Class ID List:
"Fax" (0x1111)
"Generic Telephony" (0x1204)
Protocol Descriptor List:

Bluetooth™


careluca@geco:~ - [2]
Service Name: Serial Port 2
Service RecHandle: 0x10004
Service Class ID List:
"Serial Port" (0x1101)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 5
Service Name: OBEX Object Push
Service RecHandle: 0x10005
Service Class ID List:
"OBEX Object Push" (0x1105)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 10
"OBEX" (0x0008)
Profile Descriptor List:
"OBEX Object Push" (0x1105)
Version: 0x0100
Service Name: IrMC Synchronization
Service RecHandle: 0x10006
careluca@geco:~ - [2]
"OBEX" (0x0008)
Profile Descriptor List:
"OBEX Object Push" (0x1105)
Version: 0x0100
Service Name: IrMC Synchronization
Service RecHandle: 0x10006
Service Class ID List:
"IrMCSync" (0x1104)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 11
"OBEX" (0x0008)
Profile Descriptor List:
"IrMCSync" (0x1104)
Version: 0x0100
bash-2.05b# obexftp -b 00:80:37:61:A9:22 -B 10 -g telecom/pb.vcf
Browsing 00:80:37:61:A9:22 ...
No custom transport
Connecting...bt: 1
done
Receiving telecom/pb.vcf.../

- Vulnerabilità presente in alcuni cellulari che permette un pieno accesso ai comandi AT del dispositivo

- Il Bluebug, obbliga il cellulare a telefonare a un numero indicato dal pirata. Ne può nascere quindi un business illegale: magari il numero è ad alto costo e, come con i dialer, chi lo gestisce è d'accordo con il pirata per spartirsi i ricavi

- Il problema è dovuto a causa di un'implementazione errata dello stack Bluetooth, durante la fase di costruzione vengono abilitati sui prototipi dei canali di comunicazione per effettuare dei test, ma poi non vengono rimossi in fase di produzione

Bluetooth™

- BlueSmack è un tipico attacco DOS (Denial of Service) che permette di far diventare instabile un sistema operativo sino a fargli generare delle eccezioni critiche

- E' la rivisitazione del classico Ping of Death che affliggeva Windows 95

- Si incrementa oltre misura la dimensione di un pacchetto echo request (L2CAP ping) che verrà poi spedito verso il dispositivo vittima

- Alcuni apparecchi, oltre ad un certa dimensione del pacchetto, ricevono il dato, ma generano degli errori che fanno bloccare completamente il sistema operativo (esempio Compaq IPAQ con sistema operativo Windows Mobile in cui se il numero dei byte del pacchetto ricevuto è superiore a 600 mostrano un messaggio di errore \con un conseguente blocco del sistema)

Bluetooth™

- Esistono in circolazioni programmi che permettono di scovare queste vulnerabilità

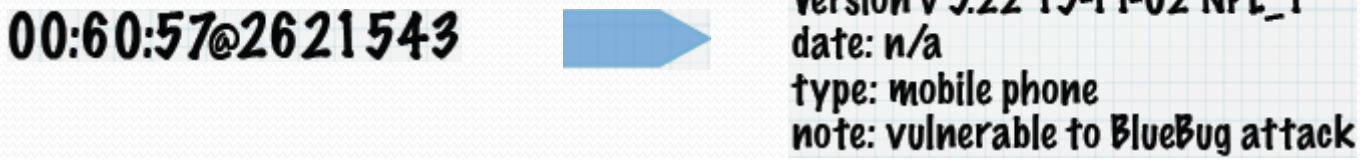
- Uno di questi è chiamato BloooverII e nella sua ultima release permette di provare molte delle vulnerabilità mostrate (BlueSnarf, BlueBug ma anche HELOMoto e Malformed Objects) in maniera veloce tramite una semplice interfaccia utente

- Il software è disponibile per tutte le piattaforme che supportano Java Micro Edition (MIDP 2.0) e le Bluetooth API (JSR-82); per questa caratteristica si presta perfettamente ad essere installato su dispositivi cellulari di ultima generazione

Bluetooth™

Blueprinting™

- E' un metodo per avere informazioni tecniche sul dispositivo, in maniera remota
- Attraverso la creazione di un database di "impronte" è possibile conoscere le caratteristiche tecniche dei dispositivi e le eventuali vulnerabilità



Bluetooth™

Il Progetto BlueBag(1)

- Nato nel 2005 e terminato nel 2007 da un gruppo di ricercatori del Politecnico di Milano

- Aveva come scopo comprendere la reale diffusione della tecnologia, determinare il reale rischio di fronte ad un possibile attacco, in particolare sono state studiate alcune caratteristiche dei dispositivi:

    - Il loro numero all'interno di un area
    - Il loro range di trasmissione
    - Il tempo di esposizione
    - Azioni e Reazioni di una potenziale vittima di attacco
    - Limitazioni Ambientali
    - Limitazioni Tecnologiche

Bluetooth™

Il Progetto BlueBag(2)

Per rispondere a queste domande è stato realizzato il primo survey italiano dei dispositivi Bluetooth avvalendosi di un particolare strumento realizzato ad hoc: la *BlueBag*

Bluetooth™

Il Progetto BlueBag(3)

- La BlueBag è basata su un sistema mini-ITX al fine di ridurre al minimo i consumi avendo comunque una discreta potenza computazionale
- La BlueBag utilizza il dongle modificato con l'antenna per rilevare i dispositivi a distanza maggiore (intorno ai 150 metri)
- A livello software, la BlueBag utilizza un sistema GNU/Linux Gentoo con kernel 2.6 e lo stack protocollare BlueZ, l'implementazione più nota e diffusa per Linux
- In maniera automatica il software della BlueBag cerca di associare anche la precisa tipologia e il particolare modello dell'apparecchio; (BluePrinting)

Bluetooth™

Il Progetto BlueBag(4)

La BlueBag ricerca tutti i dispositivi presenti nell'ambiente e cerca di effettuare il trasferimento di un file grazie al servizio OBEX PUSH, valutandone il tasso di successo, in questo modo è possibile determinare empiricamente il numero di potenziali vittime da Bluetooth malware. Risultati:

In meno di 24 ore totali di scansione nella città di Milano e in svariati luoghi, la BlueBag ha identificato 1405 dispositivi con una distribuzione del 93% per i telefoni cellulari, 3% notebook, 2% pda, 2% antenne GPS e altro

Dalle misurazioni effettuate tramite l'OBEX Pusher è stato inoltre possibile stimare il tasso medio di successo, valutando al 7.5% il numero delle persone che senza conoscere la sorgente ed il contenuto del trasferimento hanno accettato di buon grado un file potenzialmente dannoso

Bluetooth™

Il Progetto BlueBag(4)

Il tempo medio di visibilità dei dispositivi che può essere letto come il tempo utile ad un eventuale aggressore per portare a termine un attacco:

- 12.3 secondi per il centro commerciale
- 10.1 sec. per il campus universitario
- 23.1 sec. per l'aeroporto
- 14.4 sec. per gli uffici generali di una banca

Tempi ridotti ma decisamente sufficienti per portare a compimento un attacco

Bluetooth™

Conclusioni (1)

Bluetooth, inteso come standard è sicuro, i problemi sono a livello applicativo e di implementazione!

Soluzioni preventive:

- Scegliere codici PIN non banali e lunghi (dove possibile!)
- Usare almeno il dispositivo in modalità nascosta, per allungare i tempi di un'eventuale aggressione
- Effettuare l'operazione di pairing in ambienti protetti
- Evitare di utilizzare bluetooth per applicazioni critiche

Bluetooth™

Conclusioni (2)

Soluzione tecniche auspicate:

- Fornire autenticazione ai livelli più alti del protocollo
- Maggior impegno e sinergia tra Bluetooth SIG e case produttrici

Grazie per l'attenzione!!!!!!