Сигурност Bluetooth механизама за откривање периферија рачунарских система

Јована Вучковић 2012/0086

Садржај

Bluetooth протокол

Bluetooth је протокол бежичне комуникације на фреквенцијама кратког домета (*short-range Radio Frequency RF*). Користи се за креирање бежичних личних мрежа (*Wireless Personal area networks - WPANs*) у циљу бежичног упаривања различитих типова периферија за репродукцију и унос података, са радним системом. (рад на протоколу почиње 1994, први стандард 2002)

Bluetooth протокол

Bluetooth Low Energy

Као одговор на потражњу “лаких” уређаја за комуникацију, који су више пасивни и не захтевају непрестану комуникацију, конекцију, и самим тим, користе мање енергије, изграђен је протокол за нископотрошне уређаје – Bluetooth Low Energy (BLE). (2010)

Основне одлике:

- Слање пакета оглашавања уређаја
- Конекција није обавезна током комуникације
- Одређивање удаљености уређаја
- Одређивање правца у коме се уређај налази

Bluetooth протокол

	Bluetooth Low Energy (LE)	Bluetooth Classic
Frequency Band	2.4GHz ISM Band (2.402 – 2.480 GHz Utilized)	2.4GHz ISM Band (2.402 – 2.480 GHz Utilized)
Data Transports	Asynchronous Connection-oriented Isochronous Connection-oriented Asynchronous Connectionless Synchronous Connectionless Isochronous Connectionless	Asynchronous Connection-oriented Synchronous Connection-oriented
Communication Topologies	Point-to-Point (including piconet) Broadcast Mesh	Point-to-Point (including piconet)
Positioning Features	Presence: Advertising Direction: Direction Finding (AoA/AoD) Distance: RSSI, Channel Sounding	None

Сигурност протокола Bluetooth

Протокол Bluetooth прописује 5 сигурносних модела по којима се успоставља и врши комуникација између два уређаја.

Упаривање (*Pairing*, *Bounding*) се користи да би два уређаја разменили сигурносне кључеве, и тиме започеле сигурну енкриптовану комуникацију.

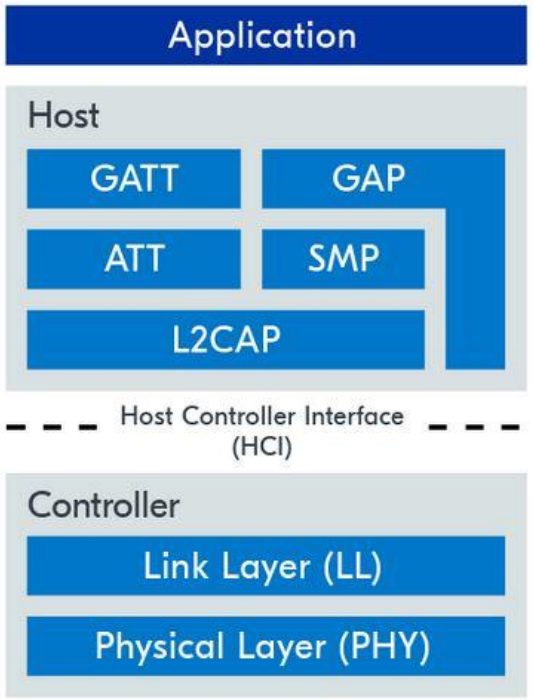
Сигурност протокола Bluetooth

Модел	Опис	Сигурносне процедуре се врше током креирања
4	Захтева се употреба аутентификованог кључа и захтева се енкриптовање пакета (безбедна веза)	Сервиса и везе (пре и после успостављања физичке везе)
3	Захтева се употреба се аутентификованог кључа	Везе (пре успостављања физичке везе)
2	Користи се неаутентификовани кључ	Сервиса (након успостављања физичке везе)
1	Сигурносни механизми се не користе	/
0	Без сигурнсоних механизама - Модел дозвољен само за Service Discovery Protocol	/

BLE?

Сигурност протокола Bluetooth

Bluetooth Low Energy

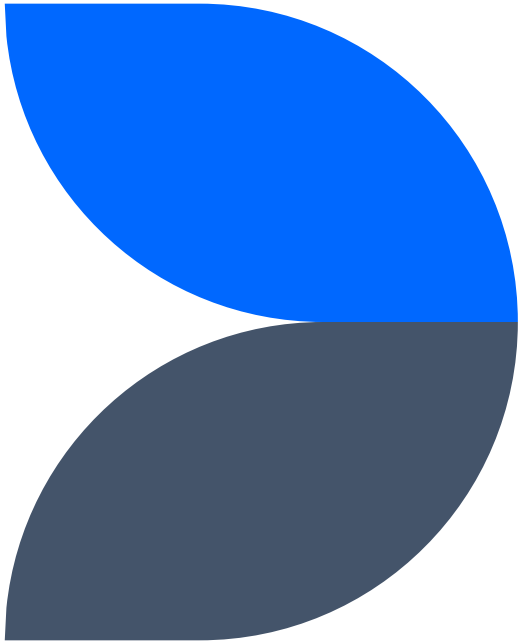


- **GAP** – *Generic Access Profile* је слој који комуницира са апликацијом и пружа подршку за откривање и повезивање уређаја
- ATT – *ATTribute Protocol* енкапсулација и одржавање података уређаја
- **SMP** – *Security Manager Protocol* за сигурносну комуникацију

Пример злоупотребе – replay напад

Сценарију злоупотребе огласних пакета, познат као *replay* напад, је ситуација у којој један уређај (нападач) долази до огласних пакета уређаја (жртве) као и остали уређаји у простору, и затим их складишти у меморију. Када је уређај-жртва постао недоступан кроз гашење *Bluetooth*-а или физичке удаљености, уређај-нападач почиње емитовање пакета уређаја жртве у простор, и тиме опонаша уређај жртву.

Демо



Закључак

Уређај који скенира радио једноставно мапирање уређаја у своју базу са паром кључевима MAC адреса + име уређаја - овај начин идентификације није довољно сигуран начин да се уређај-жртва идентификује као физички присутна у простору. Ова комуникација је рањива на replay тип напада.

Хвала на пажњи.