VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
ELEKTRONIKOS FAKULTETAS
KOMPIUTERIŲ INŽINERIJOS KATEDRA

Informacijos saugos namų darbai
„ „Bluetooth“ saugumas ir jo spragos“

Parengė: Šarūnas Venclovas EPKf-09
Tikrino: Doc. Eimantas Garšva

Vilnius, 2013

Turinys

1. „Bluetooth“ istorija.

Taikant vis populiarėjančią belaidę „Bluetooth“ technologiją, galima greitai ir paprastai sujungti nešiojamuosius įtaisus ar nedideliu atstumu prisijungti prie interneto. Toks ryšys tinkamas spausdintuvams, nešiojamiesiems kompiuteriams, klaviatūroms, pelėms, delniniams ir automobiliniams kompiuteriams, tačiau net 60 proc. visų „Bluetooth“ įtaisų sudaro mobilieji telefonai.

„Bluetooth“ dažniausiai padeda sinchronizuoti mobiliojo telefono ar delninio kompiuterio adresų knygelę, kalendorių su staliniu kompiuteriu, prijungti spausdintuvą, pelę ar klaviatūrą prie stalinio kompiuterio, persiųsti paveikslėlius ar melodijas iš vieno telefono į kitą. Prognozuojama, kad 2008 m. pasaulyje bus beveik milijardas įtaisų, kuriuose veiks „Bluetooth“. Tačiau dėl šios technologijos gali kilti saugumo ir privatumo problemų.

„Bluetooth“ idėja gimė 1994 m., kai, ieškodami universalaus būdo belaidžiu būdu sujungti mobiliuosius telefonus, kompiuterius ir kitus nedideliu atstumu nutolusius įtaisus, „Ericsson“ mokslininkai atliko išsamius tyrimus. Vėliau jų studija tapo šiuolaikinės „Bluetooth“ technologijos, kurią tobulina 1998 m. rugsėjį „Ericsson“, IBM, „Intel“, „Nokia“ ir „Toshiba“ korporacijų įkurta specialiųjų interesų grupė SIG („Bluetooth Special Interest Group“), pagrindu. 1998 m. gruodį prie SIG prisidėjo kompanijos 3Com, „Lucent Technologies“, „Microsoft“ ir „Motorola“.

Šiuo metu „Bluetooth“ veikia mažos galios siųstuvams nelicencijuojamu (taigi ir nemokamu) ISM (Industrial, Scientific, and Medical) 2,45 GHz dažniu, leidžiančiu belaidžiu būdu sujungti įtaisus, nutolusius nuo 10 iki 100 metrų atstumu. Duomenų mainų sparta gali siekti iki 723,2 Kbps (iki 2,1 Mbps pagal „Bluetooth 2.0“ standartą). Be to, kiekvienas įtaisas vienu metu gali palaikyti ryšį su septyniais kitais, sudarydamas mini tinklą (piconet). „Bluetooth“ taip pat leidžia sujungti keletą mini tinklų į didesnį „scatternet“. Tokiu atveju vienas „Bluetooth“ įtaisas veiktų kaip mini tinklų jungiamoji grandis (bridge).

Saugumui užtikrinti „Bluetooth“ numatytos duomenų kodavimo, įtaiso identifikavimo, paslaugos kokybės valdymo (QoS) ir kito priemonės, tačiau „Bluetooth“ technologija vis dar yra pažeidžiama.

1 pav. „Bluetooth“ prisijungimo galimybės

2. „Bluetooth“ saugumo ypatybės.

Pagrindinis Bluetooth saugumo mechanizmas – galimybė pasirinkti įtaiso veikimo režimą. Įvedus radimo (discoverable) režimą, įtaisą leidžiama „matyti“ kitiems, o slaptasis (non-discoverable) šią galimybę panaikina. Įtaisui dirbant radimo režimu, įsilaužėlis savo asmeniniu kompiuteriu gali nesunkiai atsisiųsti svetimus duomenis: adresų knygelę, darbotvarkę ir pan. Įjungus slaptąjį režimą, paieškos sistema įtaiso neranda ir jis į sąrašą neįtraukiamas, tačiau vartotojai, žinantys „paslėpto“ įtaiso MAC adresą, gali prie jo prisijungti. Taip gali nutikti įtaisams anksčiau užmezgus ryšio seansą (paired).

3. „Bluetooth“ adreso nustatymai.

Bluetooth įtaisas identifikuojamas pagal įprastą 48 bitų MAC adresą. Pirmieji 3 baitai rodo įtaiso gamintoją, o likusius tris gamintojas pasirenka savo nuožiūra. Pavyzdžiui, Sony Ericsson P900 mobiliojo telefono adresas gali būti 00:0A:D9:EB:66:C7. Tai reikštų, kad visų P900 telefonų adresai turi prasidėti (00:0A:D9). Remiantis MAC adreso aprašu, trys likę telefono aparato adreso baitai turėtų skirtis, tačiau taip yra ne visada.
Teoriškai, įjungus slaptąjį režimą, prie įtaiso prisijungti negalima. Tačiau iš tikrųjų tokius įtaisus rasti įmanoma. Jau yra sukurta programų, iš eilės skaitančių visus galimus MAC adresus ir pranešančių, kokiais adresais sulaukta atsakymo. Tačiau tokios programos dar nepraktiškos, nes vienam Bluetooth adresui patikrinti sugaištama nuo trijų iki dešimties sekundžių. Sony Ericsson telefonams skirti 3 baitai = 24 bitai, taigi iš viso reikėtų patikrinti 224 = 16 777 216 adresų. Jei vienas adresas nuskaitomas vidutiniškai per šešias sekundes, visiems Sony Ericsson adresams patikrinti reikėtų daugiau nei trejų metų! Tačiau adresų skaičių galima sumažinti.

Dažnai naujuose telefonuose būna įrengtas mėlynas šviesos indikatorius, kuris, veikiant Bluetooth sistemai, pradeda mirksėti. Pastebėjęs telefoną su mirksinčiu mėlynu šviesos indikatoriumi ir neradęs jo įprastomis paieškos priemonėmis (discover), įsilaužėlis gali suprasti, kad įtaisas veikia slaptuoju režimu. Matydamas patį telefono aparatą, piktavalis gali atpažinti jo gamintoją bei modelį.

4. Adresų erdvės peržiūra

Žinant telefono gamintoją, adresų erdvė sumažėja, nes pirmieji 3 MAC adreso baitai jau yra žinomi. Be to, pastebėta, kad tokio pat modelio telefonams dažnai suteikiami panašūs adresai, pavyzdžiui, daugumos Sony Ericsson P900 mobiliųjų telefonų adresai skaičiais 00:0A:D9:E. Taigi galimų variantų skaičius sumažėja nuo 16 milijonų iki 1 048 576. Taip pat pastebėta, kad P900 modelio telefonų adreso ketvirtas baitas labai dažnai yra E7 – EE, taigi lieka tik 524 288 variantai. Vienam adresui patikrinti sugaišus šešias sekundes, visą erdvę būtų galima „perbėgti“ per 36 dienas. Tačiau tai vis tiek nepraktiška.

Dar labiau procesą būtų galima paspartinti sumažinus adreso patikrinimo trukmę arba keletą adresų pradėjus tikrinti vienu metu. Naudojant 8 Bluetooth antenas, paieškos trukmę galima sumažinti nuo 36 dienų iki pus penktos dienos. Nors tai vis dar per daug, tačiau nereikėtų pamiršti, kad Bluetooth adresai pradėti skaityti dar gana neseniai, o ateityje galbūt atsiras kur kas efektyvesnių jų tikrinimo būdų.

5. Adreso aptikimas perduodant duomenis

Bluetooth adresus galima sužinoti dviem įtaisams besikeičiant duomenimis, net ir vartotojams įjungus duomenų šifravimo režimą. Tai įmanoma, nes dabartinis Bluetooth standartas nenumato MAC adreso šifravimo. Tiesa, dažnių keitimas (1600 kartų per sekundę) suteikia šiokią tokią apsaugą, tačiau keitimo dėsnis yra pseudoatsitiktinis. Teoriškai įsilaužėlis, naudodamasis tam tikra įranga, gali prisitaikyti prie vartotojų dažnių keitimo modelio. Kadangi šis modelis yra toks pats visame mini tinkle, piktadarys gali tuo bematant pasinaudoti. Jau dabar prekiaujama įranga, leidžiančia realiu laiku išanalizuoti perduodamus Bluetooth duomenų srautus. Tiesa, jos kaina dar labai didelė.

Gana dažnai žmonės patys perjungia savo mobiliuosius telefonus radimo režimu. Norint sujungti įtaisus tarpusavyje, bent vienas jų neturi būti slaptas. Be to, daugelis vartotojų šį režimą dažnai pamiršta išjungti ir tokiu būdu palengvina darbą įsilaužėliui. Šis bematant sužino telefono MAC adresą. Kadangi kiekvieno įtaiso adresas yra unikalus ir vartotojas jo keisti negali, įsilaužėliui pakanka jį

sužinoti tik vieną kartą. Vėliau, net jei telefonas perjungtas slaptuoju režimu, piratas gali prie jo prisijungti. Aparato savininkas negali uždrausti to daryti ir net nepastebi užmegzto ryšio, nes šiuolaikiniai nešiojamieji įtaisai visada priima prašymą užmegzti ryšį L2CAP (Logical Link Control and Adaptation Layer Protocol) vartotojo apie tai neinformuodami.

6. „Bluetooth“ įrenginių sujungimas ir saugumas

Norėdami sujungti du įtaisus Bluetooth sąsaja, vartotojai paprastai turi įvesti tą patį PIN kodą. Teisingai jį įvedus, įtaisai sugeneruoja skaitmeninį susijungimo raktą. Šis raktas gali būti saugomas įtaiso atmintinėje, kad nereikėtų jo pakartotinai įvesti.

Tačiau iš tiesų viskas gali pakrypti į kitą pusę. Kai kurie gamintojai ne visada paiso standarto reikalavimų, tad įsilaužėliai gali atsisiųsti telefonų knygelę, paskambinti ar išsiųsti žinutę iš aukos mobiliojo telefono. Tokios saugumo spragos paliktos net kai kuriuose Nokia ir Sony Ericsson telefonuose.

Kadangi dauguma telefonų neišsaugo SMS žinučių, išsiųstų Bluetooth AT komandomis, vartotojas net nepastebi, kad iš jo telefono siunčiamos žinutės. Jas jis galėtų pastebėti tik įjungęs operatoriaus žinučių patvirtinimo paslaugą. Dar blogiau, jei kas nors sugalvoja paskambinti iš aukos mobiliojo telefono per Bluetooth: visos pokalbių išklotinės rodo aukos telefono numerį. Kadangi šiuolaikiniai telefonai nepalieka įrašų apie Bluetooth darbą, neįmanoma įrodyti, kad skambino ne telefono savininkas. Situaciją komplikuoja tai, kad minėtomis spragomis labai nesunku pasinaudoti. Taigi bet kuris vartotojas, bent šiek tiek susipažinęs su Bluetooth ir Linux operacine sistema, gali nesunkiai tai padaryti, turėdamas tik nešiojamąjį kompiuterį. Pavyzdžiui, norint „pavogti“ adresų knygelę iš „Sony Ericsson T610“ mobiliojo telefono, pakanka įvykdyti vos dvi komandas: Čia hcitool ir obexftp yra standartinės Linux Bluetooth paketo komandos. Ši spraga aptikta ne tik T610, bet ir kituose telefonuose: Nokia 6310, 6310i, 8910, 8910i, Sony Ericsson T68, T68i, R520m, T610, Z600.

Gamintojai jau pasiūlė programinės įrangos pataisas, tačiau daugelis vartotojų net nepagalvoja, kad telefono programinę įrangą reikėtų atnaujinti. Taigi pažeidžiamus įtaisus rasti nesunku, ypač – didesnėse žmonių susibūrimo vietose. Faktas, kad aparatuose paliekamos tokios spragos, rodo, jog gamintojai vis dar atsainiai žiūri į saugumo problemas. Jei situacija nepasikeis, ateityje pažeidžiamų įtaisų tik daugės.

7. Įtaiso vardo falsifikavimas

Jungiant įtaisus tarpusavyje (pairing), pastebima dar viena saugumo spraga. Prieš juos sujungiant, ekrane pateikiamas tik įtaiso vardas – jo adreso nematyti. Vardą gali pakeisti bet kuris vartotojas, todėl visiškai nesunku vienam įtaisui „apsimesti“ kitu. Jei egzistuoja Bluetooth interneto prieigos taškas, įsilaužėlis gali aktyvuoti savo įtaisą tuo pačiu vardu ir PIN kodu, kuris taip pat užtikrina interneto ryšį toje pačioje vietoje. Skirtumas tik tas, kad visa vartotojo asmeninė informacija (taip pat ir slaptažodžiai), siunčiama šiuo įtaisu, patenka į įsilaužėlio rankas.

Kitaip falsifikuoti vardą būtų galima per kai kuriose šalyse veikiančius Bluetooth „kioskus“, leidžiančius vartotojams už tam tikrą mokestį Bluetooth sąsaja atsisiųsti į savo telefonus žaidimus, melodijas, paveikslėlius ir pan. Priskyrę savo įtaisui „kiosko“ vardą ir PIN kodą, gali į vartotojo mobilųjį įtaisą siųsti virusus ar kitas programas, padedančias lengviau pasiekti telefone esančią informaciją.

Taigi dėl netobulo standarto ir atsainaus gamintojų požiūrio į saugumą Bluetooth technologija nėra visiškai saugi. Tačiau nors egzistuoja nemažai būdų, kaip pasinaudoti Bluetooth saugumo

spragomis, kai kurie asmenys gali pamanyti, jog ryšys veikia nedideliu atstumu, todėl dažnai galima vizualiai nustatyti įsilaužėlį. Kartais įsilaužėliai naudojasi kryptinėmis Bluetooth antenomis ir stiprintuvais, didinančiais Bluetooth veikimo spindulį iki kilometro. Todėl geriausia apsauga – atnaujinti telefono programinę įrangą ir jungti Bluetooth tik tada, kai to tikrai reikia.

8. “ Bluetooth“ atakų rūšys

- BlueSnarf. Tai jungimasis prie kai kurių Bluetooth įtaisų modelių be jų savininko leidimo (t. y. įtaisas neprašo patvirtinti leidimo prisijungti ir net nerodo, kad perduodami duomenys). Tokiu būdu prisijungus galima pasiekti paprastai draudžiamas telefono atmintinės vietas: telefonų knygelę, kalendorių ir darbotvarkę, telefono IMEI (International Mobile Equipment Identity) numerį ir pan. Paprastai taip atakuojami radimo režimu veikiantys telefonai, tačiau, sužinojus MAC adresą tam skirtomis programomis (bluesniff, btscanner, redfang ir kt.), gali būti atakuojami ir slaptojo režimo telefonai.
- Backdoor. Šios atakos esmė – pasibaigus normaliam ryšio seansui (pairing) Bluetooth sąsaja ir aukai ištrynus įsilaužėlio įtaisą iš sujungimų sąrašo (paired device list), ryšys tęsiamas, o įsilaužėlis gali naudotis vidiniais telefono ištekliais. Jis gali ne tik pradėti siųsti duomenis, bet ir prisijungti vidiniu aukos telefono modemu prie interneto, pasitelkęs WAP ar GPRS. Be to, jei ši ataka sėkminga, įmanoma ir Bluesnarf ataka, net jei ji anksčiau šio telefono nepaveikė. Apsisaugoti nuo Backdoor atakos galima tik visiškai ištrynus įtaisą iš sujungimų sąrašo, o tai padaryti pavyksta tik atkūrus telefono pradines nuostatas. Tačiau tai padarius, dingsta visa vartotojo asmeninė informacija.
- BlueBug. Šios atakos metu Bluetooth sąsaja sukuriamas nuoseklusis ryšys tarp įsilaužėlio ir aukos įtaisų. Piratas gali naudotis telefono AT komandomis, taigi – visiškai kontroliuoti telefoną: prisijungti prie interneto ir perduoti duomenis, skaityti bei siųsti SMS, tvarkyti kontaktus, peradresuoti skambučius ar net skambinti pasirinktu numeriu. Vadinasi, jis gali perimti atkeliaujančius aukos skambučius ir nukreipti mokamais numeriais. Apsisaugoti nuo šios ir BlueSnarf atakų (bent jau kol kas) galima tik išjungus Bluetooth.
- Bluejacking. Tai socialinė ataka. Jos tikslas – priversti vartotoją sujungti (pairing) savo telefoną su įsilaužėlio įtaisu. Bluejacking ataka vykdoma masinėse žmonių susibūrimo vietose, parinkus žmones dominantį įtaiso vardą (Bluetooth standartas leidžia pasirinkti iki 248 simbolių įtaisų vardus). Tarkim, įsilaužėlis savo įtaisui parenka vardą PIN1234 ir pradeda jungtis su jam matomais vartotojų telefonais. Vartotojas, pastebėjęs tokį užrašą ekrane, gali surinkti PIN kodą 1234 ir patvirtinti ryšį tarp įtaisų, tokiu būdu užtikrindamas įsilaužėliui visišką savo telefono kontrolę. Bandymai žmonių susibūrimo vietose (konferencijose, technologijų parodose ar net didelėse parduotuvėse) parodė, kad į kvietimą užmegzti ryšį atsako vidutiniškai 3 iš 10 kvietimą gavusių žmonių.

9. Išvados

"Bluetooth" suteikia galimybę sukurti mažojo nuotolio Ad hoc ryšių tinklų viešų ir privačių tinklų. "Bluetooth" prietaisai kelia naujų pavojų, viešųjų ar privačiųjų aplinkoje nuo belaidžiai tinklai nei tradicinių laidiniais tinklais. Ši rizika yra identifikuojami visais "Bluetooth" prietaiso sluoksnių.

Identifikavimo, autentiškumo, konfidencialumo ir leidimo yra keturi informacijos saugumo sistemos, kuri turi būti atliekama siekiant apsaugoti duomenis, ir "Bluetooth" prietaisai. Jis taip pat yra priklausoma nuo saugumo režimą, prietaisas sukonfigūruotas veikti. Šie informacijos apsaugos sistemos aptarnavo bevielio ryšio ir operacinė sistema, programos ir vartotojų sluoksniai yra atsakingas už savo informavimo vertybinių popierių. Yra nemažai spragų, kurios gali būti naudojamos užpuolikai įgyti prieigą prie įrenginio. Galutinis vartotojas turi žinoti, naudojant "Bluetooth" prietaisus, taip pat organizacija turėtų suprasti saugumo sąvokas ir konfigūracijų šiai rizikai sumažinti riziką

Literatūros sąrašas

1. www.nkm.lt
2. http://electronics.howstuffworks.com
3. Žurnalas "Ryšių technikos naujienos" – http://www.rtn.lt
4. www.kompiuterija.lt/
5. www.bluetooth.com/
6. www.elektronika.lt/straipsniai/rysiai/1608/bluetooth-sistemos-saugumas/

Į K. Scarfone and J. Padgette, Guide to Bluetooth Security, NIST Special Publication 800-121, 2008.

Į F. Tvrz and M. Coetzee (2010). Information security of a bluetooth-enabled handheld device. Germany: Lambert academic publishing AG & Co. KG. 20-26, 72-86.

Į John D. Padgette. 2009. Bluetooth security in the DOD. In Proceedings of the 28th IEEE conference on Military communications (MILCOM'09). IEEE Press, Piscataway, NJ, USA, 2425-2430.

Į Alfred Loo. 2009. Technical opinion: Security threats of smart phones and Bluetooth. Commun. ACM 52, 3 (March 2009), 150-152. DOI=10.1145/1467247.1467282 http://doi.acm.org/10.1145/1467247.1467282

Į Y. Shaked and A.Wool Cracking the Bluetooth PIN. In Proceedings of 3rd USENIX/ACM Conference of Mobile Systems, Applications and Services (MOBISYS), June 2005.

Į Keijo MJ Haataja. 2008. New efficient intrusion detection and prevention system for Bluetooth networks. In Proceedings of the 1st international conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications (MOBILWARE '08). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, , Article 16 , 6 pages.

Į TJ O'Connor and Ben Sangster. 2010. honeyM: a framework for implementing virtual honeyclients for mobile devices. In Proceedings of the third ACM conference on Wireless network security (WiSec '10). ACM, New York, NY, USA, 129-138. DOI=10.1145/1741866.1741888 http://doi.acm.org/10.1145/1741866.1741888