EXPUNEREA LA ATACURI A REȚELELOR WIRELESS

Maria CERNEI

Universitatea Tehnică a Moldovei

Abstract: *Noi posibilităţi de atac asupra infrastructurii interne a unei reţele de calculatoare au apărut odată cu utilizarea tot mai frecventă a reţelelor fără fir. Sistemele fără fir oferă beneficiul mobilităţii utilizatorilor şi o desfăşurare flexibilă a unei reţele într-o anumită arie. Ca orice tehnologie relativ nouă, reţelele fără fir reprezintă un mediu de comunicaţie susceptibil la ameninţări ce ţin atât de acţiuni din exteriorul mediului cât şi din interiorul lui, ce poate duce ulterior la diverse probleme şi breşe de securitate.*

Cuvinte cheie: *Wi-Fi, puncte de acces, protocol, securitate, smishing, grayware, EMI.*

Introducere

Reţelele wireless nu beneficiază de securitate fizică incorporată precum reţelele cu fir, deci sunt mai predispuse atacurilor. Odată obţinut accesul în reţea, un intrus poate folosi cu uşurinţă resursele din cadrul acesteia. O serie de atacuri specifice reţelelor fără fir, pot avea loc, aşa ca: atacuri la protocoalele de protecţie wireless, instalarea punctelor de acces neautorizate, interferenţe electromagnetice, mesaje sms care pot cauza furtul credenţialelor sau descărcarea programelor maliţioase în dispozitivele mobile ale victimei.

Dispozitivele mobile, smartphone-uri şi tabletele, trebuie să îndeplinească anumite cerinţe de securitate considerate de bază: confidenţialitate, integritate şi disponibilitate. Pentru a atinge aceste obiective trebuie intensiv de analizat majoritatea ameninţărilor la care acestea sunt susceptibile.

1. Atacuri ale protocoalelor de securitate: WEP, WPA, and WPA2

Wired Equivalent Privacy (WEP) este un protocol de securitate care a încercat să furnizeze o reţea locală fără fir (WLAN) cu acelaşi nivel de securitate ca o reţea LAN cu fir. Deoarece măsurile de securitate fizică ajută la protejarea unei LAN cu fir, WEP urmăreşte să asigure o protecţie similară pentru datele transmise prin WLAN cu criptare. Adică datele transmise sunt criptate.

WEP foloseşte o cheie pentru criptare. Nu există nicio prevedere pentru managementul cheilor cu WEP, astfel încât numărul de persoane care împărtăşesc cheia va creşte în mod constant. Deoarece toţi utilizatorii utilizează aceeaşi cheie, criminalul are acces la o cantitate mare de trafic pentru atacuri analitice.

WEP are, de asemenea, mai multe probleme cu vectorul iniţial (IV) al algoritmului RC4, care este una dintre componentele sistemului criptografic:

1. Este un câmp de 24 biţi, care este prea mic.
2. Este un text clar, ceea ce înseamnă că este uşor de citit.
3. Este static, astfel încât fluxurile cheie identice se vor repeta într-o reţea ocupată.

Wi-Fi Protected Access (WPA) şi apoi WPA2 au fost emise ca protocoale îmbunătăţite pentru a înlocui WEP. WPA2 nu are aceleaşi probleme, deoarece la fiecare sesiune stabilită are loc emiterea unei noi chei de criptare, prin implementarea algoritmului AES şi astfel dispare pericolul ca un atacator să poată recupera cheia prin observarea traficului. WPA2 este susceptibil totuşi la atac, deoarece criminalii cibernetici pot analiza pachetele dintre punctul de acces şi un utilizator legitim. Cyber criminalii utilizează un sniffer de pachete şi apoi execută atacuri offline bazate pe fraza de acces (passphrase).

2. Puncte de acces Rogue

Un punct de acces rogue este un punct de acces wireless instalat într-o reţea securizată fără cunoştinţa administratorului de sistem. Dispozitivele fără fir neautorizate pot fi ascunse în interior sau ataşate la un computer sau altă componentă a sistemului, sau pot fi ataşate direct la un port de reţea, sau la un dispozitiv de reţea, cum ar fi un switch sau un router.

Un punct de acces rogue ar putea fi un mic punct de acces wireless conectat la un firewall sau switch sau într-un conector de reţea etc. Poate fi de asemenea şi un dispozitiv mobil ataşat la un dispozitiv USB care creează o conexiune wireless, punct de acces sau chiar un card wireless conectat la un server. Deoarece ele sunt instalate în spatele firewall - ului unei organizaţii, punctele de acces rogue pot fi letale pentru securitate.

Iată trei pericole principale ale unui punct de acces rogue:

1. Cineva autentificat neautorizat poate accesa reţeaua.

2. Punctul de acces nu este monitorizat sau gestionat de administratorul de sistem.

3. Punctul de acces nu respectă procedurile de securitate ale altor puncte de acces wireless din aceeaşi reţea.

Dar, totuşi cum reuşesc atacatorii, de fapt, să instaleze puncte de acces rogue? Hackerii folosesc puncte de acces rogue ca o modalitate simplă de a obţine acces în sistemele de afaceri şi pentru a captura datele sensibile şi credenţialele. O modalitate des implementată de către hackeri este de a utiliza punctele de acces rogue prin aşa numitul evil twin. Evil twins sunt puncte de acces wireless configurate să pară identice cu reţeaua fără fir adevărată a unei companii. De ce? Pentru a atrage utilizatorii autorizaţi să se conecteze la reţeaua falsificată. Dacă punctul de acces fără fir are acelaşi nume şi un identificator unic de 32 de cifre (SSID) dar şi o adresă MAC, atunci dispozitivele angajaţilor se pot conecta automat la acesta. Dacă un evil twin are succes, un atacator se poate conecta cu uşurinţă la laptopul utilizatorului pentru a fura credenţialele de autentificare şi pentru a accesa reţeaua folosind un nume autorizat.

3. RF Jamming

Semnalele wireless sunt susceptibile la interferenţe electromagnetice (EMI), interferenţe radio-frecvente (RFI) şi pot fi chiar susceptibile la lovituri de trăsnet sau la zgomotul luminilor fluorescente. Semnalele wireless sunt, de asemenea, susceptibile la bruiaj deliberat. Blocarea de radiofrecvenţă (RF) întrerupe transmiterea unei staţii radio sau de satelit, astfel încât semnalul să nu ajungă la postul de recepţie.

Frecvenţa, modularea şi puterea blocatorului RF trebuie să fie egale cu cea a dispozitivului pe care criminalul doreşte să îl perturbeze pentru a bloca cu succes semnalul wireless.

Fiecare sistem inteligent de securitate DIY trebuie sa aibă activată detecţia blocajelor RF Honeywell. Dacă ceva sau cineva încearcă să blocheze dispozitivele fără fir, va fi afişat un semnal de eroare.

4. Grayware şi Smishing

Grayware-ul devine o problemă în domeniul securităţii mobile, odată cu cu popularitatea smartphone-urilor. Software-ul Gray include aplicaţii care se comportă într-o manieră enervantă sau nedorită. Este posibil ca software-ul Grayware să nu prezinte malware identificabil în interiorul acestuia, dar poate totuşi să reprezinte un risc pentru utilizator. De exemplu, programul Grayware poate urmări locaţia utilizatorului. Autorii de produse grayware, de obicei, păstrează legitimitatea prin includerea capabilităţilor unei aplicaţii într-o amprentă redusă a acordului de licenţă software. Utilizatorii instalează multe aplicaţii mobile fără a lua în considerare cu adevărat capacităţile lor.

SMiShing este utilizarea tehnicii de phishing prin SMS. Utilizează serviciul de mesaje scurte (SMS) pentru a trimite mesaje text false. Criminalii îi înşală pe utilizatori să viziteze un site web sau să sune un număr de telefon. Astfel, victimele pot furniza apoi informaţii sensibile, cum ar fi informaţii despre cărţile de credit. Vizitarea unui site web ar putea duce la descărcarea, fără acordul utilizatorului, a unui program malware care infectează dispozitivul.

Bibliografie

1. Richard A. Stanley, *Wireless LAN Risks and Vulnerabilities ,"*ISACA Journal, Volume 2, 2002.
2. David B. Jacobs, " Wireless security protocols - How WPA and WPA2 work", March 2008.
3. https://searchnetworking.techtarget.com/Rogue-access-points-Preventing-detecting-and-handling-best-practices.
4. https://www.cybrary.it/0p3n/wifi-and-its-security/.
5. https://www.alarmnewengland.com/blog/rf-jamming.
6. *https://www.comparitech.com/blog/information-security/smishing/.*