PENERAPAN EVIL TWIN DETEKTOR DALAM PENDETEKSIAN PENGGANGGU JARINGAN NIRKABEL PADA USER

Peniarsih
ppeniarsih@yahoo.co.id

Abstract

Nowadays, wireless networking facilities are provided in public places such as fast food restaurant, airports, hotels, campuses and are an attraction for users to use them. The wireless network provided uses an open authentication system and web-based authentication as the second layer used by customers to identify themselves according to the service they have before they can connect to the internet or WiFi Hotspot is a frequently used name. However, unnoticed by the user, it can be utilized by parties who are not entitled to attack and disturb. One of the attacks on wireless networks is the evil twin attack, given the ease in creating it by only duplicating the existing wireless network configuration and forcing users to move to the evil twin network because the installation tends to be closer to the victim's location. Administrator-based detection is one solution that is implemented but has a dependency on the availability of network administrators and supporting devices. To assist users in detecting disturbances, this research proposed client-based evil twin detection that utilizes Medium Access Control (MAC) address data and automatic configuration information provided by a Dynamic Host Configuration Protocol (DHCP) server on a wireless network. Shell programming on the Linux operating system is used to implement the solution.

Keywords: *Evil Twin Attack, Hotspot WiFi, WiFi Security*

1 PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di Indonesia saat ini sudah menyentuh semua kalangan, termasuk masyarakat umum, pemerintah, pendidikan dan bisnis yang mengakibatkan adanya peningkatan jumlah penggunanya (Asosiasi Penyelenggara Jasa Internet Indonesia, 2016). *Wireless Local Area Networks* (WLAN) atau jaringan nirkabel atau yang saat ini lebih dikenal dengan *Wireless Fidelity* (WiFi) merupakan koneksi internet yang paling disukai dengan alasan kecepatannya yang tinggi dan stabil menurut survei yang dilakukan (APJII, 2016).

Dan saat ini, di tempat umum seperti Bandar Udara, Hotel, Sekolah atau Kafe banyak ditemukan WiFi *Access Point*. Dimana pengguna dapat menggunakan perangkat *mobile* maupun laptopnya untuk terhubung ke internet (Hsu, Wang, Hsu, Cheng, & Hsneh, 2015).

Meski jaringan nirkabel lebih nyaman dibandingkan dengan jaringan kabel, WiFi juga tidak luput dari sasaran kejahatan, yaitu *Denial of Service*, *Spoofing and Session Hijacking* dan *Eavesdropping* (Hamid, 2003). Dengan cara-cara seperti tersebut dapat dilakukan perusakan atau pencurian data, selain itu ada yang langsung menyerang para pengguna, salah satunya ialah *Rogue Access Point* (Chabinsky, 2014).

Serangan *evil twin* merupakan teknik penyerangan pada jaringan nirkabel yang efektif dan mudah dalam hal pembuatannya. Penyerang dapat

menggunakan perangkat WiFi-nya untuk memulai serangan *evil twin*. Dan penyerang dapat menghentikan serangan kapan pun untuk mengelabui serangan yang dilakukan (Nakhila & Zou, 2016).

Evil twin adalah istilah yang digunakan untuk *Rogue Access Point* (Panch & Singh, 2010). Terdapat dua kategori solusi untuk melakukan pendeteksian serangan *evil twin*, yaitu pendeteksian berbasis administrator jaringan dan berbasis pengguna jaringan (Hsu et al., 2015; Nikbakhsh, Manaf, Zamani, & Janbeglou, 2012). Terdapat dua model penyerangan evil twin menurut (Mustafa & Xu, 2014), yaitu penyerangan dengan kartu jaringan nirkabel tunggal dan kartu jaringan nirkabel ganda.

Pada umumnya, ancaman *Rogue Access Point* dapat dilakukan pendeteksian menggunakan perangkat lunak atau perangkat keras dan terdapat dua macam pendekatan, yaitu menggunakan pendekatan nirkabel dan pendekatan kabel (Beyah & Venkataraman, 2011). Dari pendekatan tersebut sebagian besar deteksi *Rogue Access Point* dilakukan dengan melibatkan peran dari administrator jaringan sehingga perlidungan secara *real time* tidak dapat diberikan ketika serangan *evil twin* terjadi (Hsu et al., 2015) dan memerlukan *deployment* atau pembangunan perangkat deteksi *Rogue Access Point* ke dalam infrastruktur jaringan yang akan dideteksi (Song, Yang, & Gu, 2010).

Pendeteksian lainnya yaitu berbasis pengguna jaringan, terdapat beberapa metode yang digunakan dalam deteksi *evil twin* berbasis pengguna jaringan seperti yang dilakukan dalam penelitian-penelitian sebelumnya, diantaranya (1) Pengecekan dan pembandingan alamat *internet protocol* (IP) yang diperoleh dari *Access Point* (Nikbakhsh et al., 2012), (2) Pendeteksian evil twin dengan menjalankan *Wireless Network Interface Card* (WNIC) pada mode monitor untuk mengamati perilaku *packet forwarding* yang terjadi (Hsu et al., 2015), (3) Pemanfaatan *Received Signal Strength Indicator* (RSSI) untuk menentukan adanya *evil twin acces point* (Tang et al., 2017), (4) Pendeteksian *evil twin* dengan membuat dua *Virtual Wireless Client* (VWC) pada *Wireless Client* yang dimiliki untuk mendeteksi dua model *gateway* yang digunakan oleh *evil twin* secara bersamaan (Nakhila, Amjad, Dondyk, & Zou, 2018).

Dalam penelitian ini, diusulkan penerapan pendeteksian serangan *evil twin* pada sisi pengguna jaringan nirkabel di area publik dengan melakukan pengamatan dan pembandingan data alamat *medium access control* (MAC) yang digunakan oleh *access point* yang target dan konfigurasi otomatis yang didapatkan dari *server dynamic host configuration protocol* (DHCP) yang dikembangkan menggunakan bahasa pemrograman Shell pada sistem operasi Linux.

Dari penelitian ini diharapkan dapat membantu pengguna yang memanfaatkan jaringan nirkabel dengan sistem otentikasi terbuka dan otentikasi berbasis web sebagai lapisan keduanya, khususnya yang menggunakan sistem operasi Linux dalam melakukan pendeteksian serangan *evil twin*.

2 METODE YANG DIUSULKAN

Metode yang diusulkan dan digunakan dalam penelitian ini adalah pengamatan perilaku penyedia layanan jaringan nirkabel. Terdapat tiga hal yang dilakukan pengamatan dalam penelitian ini, yaitu:

a. Pengamatan terhadap tipe keamanan yang diterapkan pada jaringan nirkabel hotspot
b. Arsitektur yang digunakan pada infrastruktur jaringan nirkabel, dan
c. Pengamatan terhadap layanan yang diberikan setelah perangkat keras pengguna terhubung dengan jaringan nirkabel.

Pengamatan tipe keamanan dan arsitektur jaringan nirkabel yang digunakan dilakukan dengan pemindaian menggunakan aplikasi bernama inSSIDer yang dijalankan pada sistem operasi Windows. Tipe keamanan yang digunakan oleh penyedia layanan jaringan nirkabel di ruang publik atau *Hotspot* WiFi adalah tipe otentikasi terbuka dengan tambahan keamanan otentikasi berbasis web, menurut (Gast, 2005). Tampilan otentikasi berbasis web ini seperti yang terlihat pada Gambar 1.

Pada Gambar 2, diperlihatkan hasil pengamatan yang telah disaring berdasarkan tipe keamanan yang digunakan oleh penyedia jaringan nirkabel yaitu tipe keamanan dengan otentikasi terbuka yang terlihat dengan simbol gembok terbuka yang dilakukan pada area publik sebuah perusahaan. Pada pengamatan ini dapat dilihat bahwa jaringan nirkabel tersebut hanya menggunakan satu perangkat yang digunakan sebagai AP. Arsitektur seperti ini disebut juga arsitektur jaringan nirkabel dengan AP tunggal.

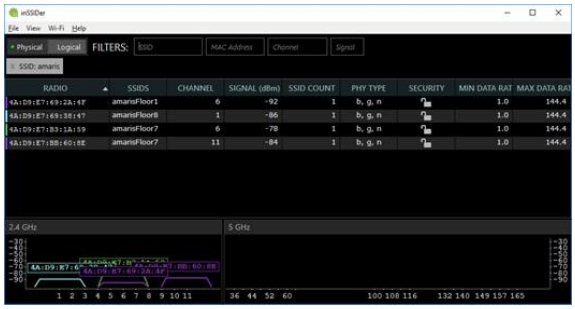
Gambar 1. Tampilan Otentikasi Tambahan Berbasis Web

Gambar 2. Tampilan Hasil Pengamatan pada Perusahaan

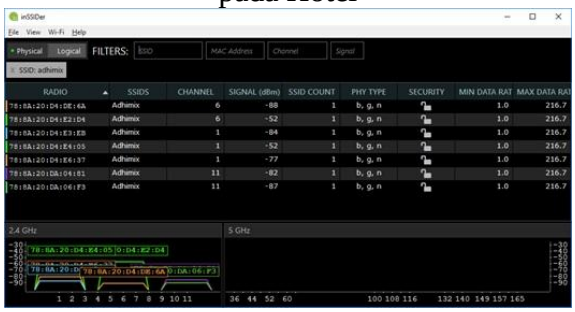
Selain arsitektur jaringan nirkabel dengan AP tunggal juga terdapat arsitektur jaringan nirkabel dengan multi AP yang digunakan dengan tujuan untuk memperluas area cakupan layanan jaringan nirkabel yang dibangun. Arsitektur multi AP ini dapat ditemukan pada bangunan bertingkat atau yang memiliki area yang luas seperti Hotel, Apartemen, Perkantoran dengan skala besar, Bandar Udara. Pada Gambar 3 dan Gambar 4, diperlihatkan hasil pengamatan pada area publik sebuah hotel dan gedung perkantoran.

Dari pengamatan yang dilakukan pada jaringan nirkabel yang menggunakan aristektur multi AP pada implementasinya memiliki ciri-ciri sebagai berikut:

a. Menggunakan perangkat keras AP dari pabrikan yang sama. Hal ini dapat diketahui dengan melihat alamat MAC perangkat dimana enam angka pertama dari alamat MAC perangkat merupakan identifikasi pabrikan dari perangkat keras
b. Ada dua tipe cara penamaan SSID, yaitu menggunakan satu nama SSID untuk semua AP atau menggunakan nama SSID yang berbeda-beda. Dengan penggunaan penamaan SSID yang sama, akan memberikan kemudahan kepada pengguna dalam hal perpindahan dari satu AP ke AP yang lainnya (*roaming*). Namun untuk penggunaan nama yang berbeda, seperti yang diimplementasikan di hotel, hal ini lebih untuk privasi dan tidak ada kebutuhan untuk melakukan *roaming*

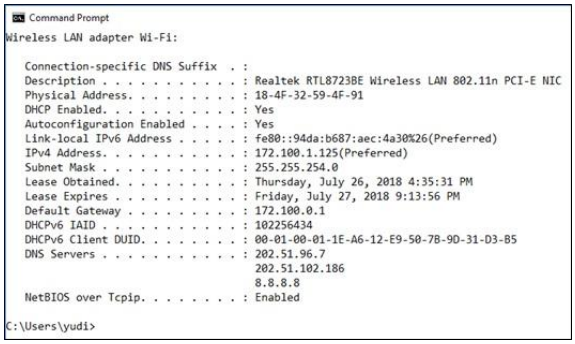


Gambar 3. Tampilan Hasil Pengamatan pada Hotel



Gambar 4. Tampilan Hasil Pengamatan pada Gedung Perkantoran

Sedangkan untuk pengamatan terhadap layanan yang diberikan setelah terhubung dengan jaringan nirkabel dapat dilakukan pengecekan dengan menggunakan *command prompt* pada Windows dengan perintah *ipconfig*. Adapun tampilannya terlihat pada Gambar 5, dimana alokasi konfigurasi tersebut memiliki waktu sewa yang mengindikasikan bahwa pengguna dengan perangkat keras yang sama akan mendapatkan alokasi yang sama selama masa sewanya masih berlaku. Alokasi konfigurasi disediakan oleh sebuah *server* DHCP seperti yang disampaikan (Mustafa & Xu, 2014) bahwa setiap pengguna jaringan nirkabel perlu melakukan konfigurasi kartu jaringan nirkabelnya untuk dapat melakukan koneksi ke internet atau *server*. Dan kebanyakan jaringan nirkabel memiliki paling tidak satu buah *server* DHCP untuk melayani konfigurasi jaringan otomatis pengguna jaringan.



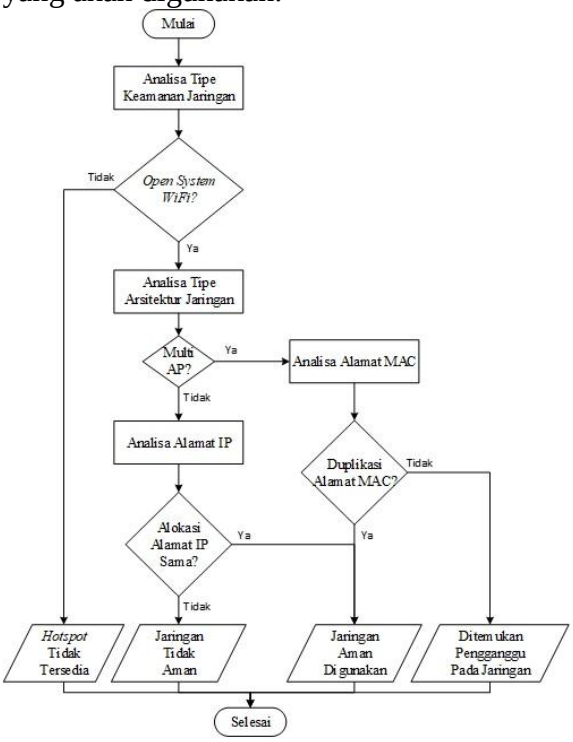
Gambar 5. Tampilan Konfigurasi Otomatis yang Didapatkan

Dari hasil pengamatan yang sudah dilakukan, alur proses usulan metode pendeteksian gangguan jaringan nirkabel yang disebabkan serangan *evil twin* dapat dilihat pada Gambar 6. Dimana proses diawali dengan analisa terhadap tipe keamanan yang digunakan pada jaringan nirkabel. Proses akan berhenti jika tidak ditemukan jaringan nirkabel yang menggunakan otentikasi terbuka.

Jika ditemukan adanya jaringan nirkabel dengan otentikasi terbuka maka akan dilajutkan dengan analisa arsitektur jaringan nirkabel yang digunakan. Dalam hal arsitektur AP tunggal yang ditemukan, maka proses akan dilanjutkan dengan analisa konfigurasi yang didapatkan dari penyedia layanan berupa alamat IP. Setiap AP akan memberikan alokasi alamat IP yang berbeda jika tidak menggunakan satu server DHCP yang sama sehingga proses akan mendeteksi dan memberikan peringatan kepada pengguna bahwa jaringan nirkabel yang akan digunakan memiliki potensi digandakan oleh pihak yang tidak bertanggung jawab. Namun apabila hasil analisa menunjukkan adanya kesamaan alokasi alamat IP, maka proses akan memberikan informasi bahwa jaringan nirkabel yang tersedia dapat digunakan.

Ketika proses iterasi menemukan arsitektur multi AP pada layanan jaringan nirkabel dimana terdapat lebih dari dua AP yang menggunakan SSID yang sama, kemudian akan dilanjutkan dengan analisa

terhadap enam angka pertama dari alamat MAC yang digunakan oleh setiap AP yang terpasang. Jika dari hasil analisa didapatkan alamat MAC yang sama maka proses akan dihentikan dengan memberikan informasi bahwa jaringan nirkabel yang tersedia dapat digunakan dengan aman. Namun apabila alamat MAC yang dianalisa terdapat ketidakcocokan maka proses akan memberikan informasi adanya potensi serangan evil twin pada jaringan nirkabel yang akan digunakan.



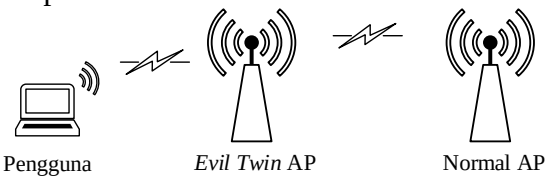
Gambar 6. Diagram Alir Proses Usulan *Evil Twin* Detektor

3 HASIL EKSPERIMEN

Sebagai pembuktian metode dari penelitian yang dilakukan, pada bagian ini akan dilakukan eksperimen sebagai penerapan dari usulan *evil twin* detektor (ET Detektor). Adapun ilustrasi dari arsitektur jaringan yang digunakan dalam eksperimen seperti terlihat pada Gambar 7.

Eksperimen yang dilakukan dalam penelitian ini memiliki cakupan dan batasan, sebagai berikut:

a. Untuk normal AP dibangun dengan menggunakan jaringan nirkabel buatan dengan arsitektur AP tunggal tanpa terkoneksi ke internet
b. *Evil twin* AP dibuat dengan menggunakan dua kartu jaringan nirkabel, satu kartu jaringan menggunakan yang tertanam pada perangkat keras sedangkan satu lagi menggunakan kartu jaringan tambahan yang menggunakan antarmuka *universal serial bus* (USB)
c. Evil twin AP yang digunakan tidak menerapkan arsitektur *wireless distribution system* (WDS), sehingga sistem konfigurasi jaringan otomatis akan disediakan oleh kedua AP, baik *evil twin* AP maupun normal AP
d. Dalam melakukan aplikasi pendeteksian, ET Detektor dibuat dengan menggunakan bahasa pemrograman Shell yang dijalankan pada sistem operasi Linux



Gambar 7. Arsitektur Eksperimen Penelitian

Adapun perangkat yang digunakan dalam eksperimen ini seperti terlihat pada Tabel 1.

Tabel 1. Spesifikasi Perangkat Eksperimen

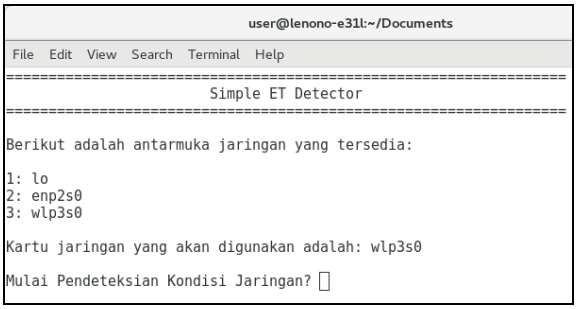
Parameter	Deskripsi
1. Pengguna	
a. Kartu Jaringan Nirkabel	Realtek ® RTL8111
b. Sistem Operasi	RHEL ® 7.4
c. Perangkat Lunak	Terminal
2. Normal AP	
a. Kartu Jaringan Nirkabel	802.11b/g/n
b. Sistem Operasi	RouterOS
3. *Evil Twin* AP	

Parameter	Deskripsi
a. Kartu Jaringan Nirkabel	a. 802.11n (*Embed*) b. Edimax (Eksternal)
b. Sistem Operasi	Kali Linux

Persiapan perangkat dari eksperimen penelitian ini dapat disampaikan sebagai berikut.

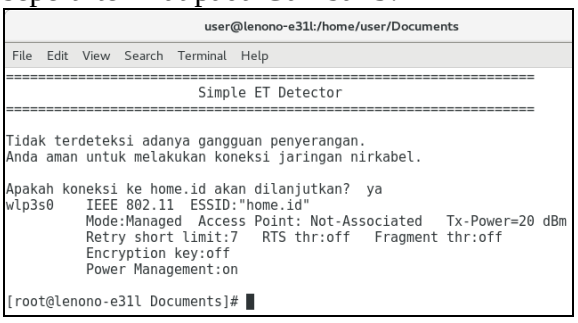
a. Normal AP
   Pada perangkat yang digunakan sebagai normal AP, akan dilakukan pengaturan dan konfigurasi untuk dapat memancarkan dan menyediakan layanan jaringan nirkabel *hotspot* dengan nama SSID home.id dengan sistem otentikasi yang digunakan adalah terbuka dengan tambahan otentikasi berbasis web.
b. *Evil Twin* AP
   Evil twin yang digunakan dalam penarapan ini menggunakan model dua kartu jaringan nirkabel. Dimana satu kartu jaringan nirkabel yang tertanam pada perangkat akan terhubung ke layanan jaringan nirkabel yang disediakan oleh normal AP. Sedangkan sisanya yang merupakan kartu jaringan nirkabel tambahan akan digunakan sebagai pemberi layanan jaringan nirkabel palsu ke komputer target yang akan memancarkan SSID dengan nama yang sama dengan normal AP, yaitu home.id.
c. Pengguna
   Merupakan simulasi dari perangkat pengguna yang nantinya terhubung dengan layanan hotspot dari home.id. Sebelum melakukan koneksi ke jaringan, akan dilakukan pengecekan kondisi menggunakan ET detektor yang sudah disiapkan.

Skenario pelaksanaan eksperimen dilakukan dalam dua tahap yaitu tanpa adanya evil twin AP dan setelah evil twin AP diaktifkan. Setelah persiapan infrastruktur eksperimen selesai dilakukan, aplikasi ET detektor dijalankan pada perangkat pengguna dengan tampilan awal seperti terlihat pada Gambar 8, dimana aplikasi akan melakukan pemindaian terhadap ketersediaan kartu jaringan nirkabel.



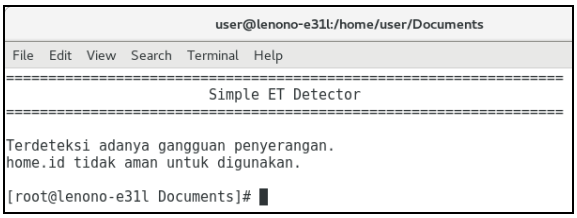
Gambar 8. Tampilan Awal Aplikasi ET Detektor

Tahap berikutnya setelah ditemukan kartu jaringan nirkabel yang akan digunakan, pengguna memberikan konfirmasi untuk memulai proses pendeteksian. Pada skenario pertama, dimana hanya normal AP yang aktif akan dihasilkan pendeteksian dengan tampilan seperti terlihat pada Gambar 9.



Gambar 9. Tampilan Pendeteksian Tanpa Ada Gangguan

Pada skenario kedua, yaitu setelah *evil twin* AP diaktifkan. Tampilan aplikasi akan terlihat pada Gambar 10, dimana terdapat notifikasi adanya indikasi gangguan terhadap jaringan nirkabel yang tersedia. Hal ini terjadi karena normal AP dan *evil twin* AP menggunakan perangkat dari pabrikan yang berbeda dan masing-masing AP menyediakan *server* DHCP sehingga alamat yang didapatkan oleh pengguna tidak memiliki kesamaan.



Gambar 10. Tampilan Pendeteksian Setelah *Evil Twin* AP Aktif

4 KESIMPULAN

Serangan *Evil Twin* merupakan salah satu jenis pengganggu pada jaringan nirkabel yang mudah dalam membuatnya, yaitu hanya cukup menyamakan kondisi dan konfigurasi dari jaringan nirkabel yang ada dan memaksa pengguna untuk menggunakannya dengan memasangnya dekat dengan pengguna. ET Detektor yang dibuat dalam penelitian ini menggunakan bahasa pemrograman Shell pada sistem operasi Linux, efektif membantu pengguna dalam melakukan pendeteksian terhadap kondisi jaringan nirkabel yang akan digunakan.

REFERENSI

APJII. (2016). *Konklusi survey ekosistem dna (device, network & apps)*. Diambil dari https://www.apjii.or.id/survei2017

Asosiasi Penyelenggara Jasa Internet Indonesia. (2016). *Infografis Penetrasi & Perilaku Pengguna Internet Indonesia Survey 2016*. Diambil dari www.APJII.or.id

Beyah, R., & Venkataraman, A. (2011). Rogue-access-point detection: Challenges, solutions, and future directions. *IEEE Security and Privacy*, *9*(5), 56–61. https://doi.org/10.1109/MSP.2011.75

Chabinsky, S. (2014). Wireless is Not Worry-Less. *BNP Media*, *51*(10), 28. Diambil dari https://e-resources.perpusnas.go.id:2171/docview/1611001295?accountid=25704

Gast, M. (2005). *802.11 Wireless Networks: The Definitive Guide*. (M. Loukides, Ed.) (2nd ed.). O'Reilly. Diambil dari http://books.google.com/books?id=9rHnRzzMHLIC&pgis=1

Hamid, R. A. (2003). Wireless LAN : Security Issues and Solutions. Diambil dari https://www.sans.org/reading-room/whitepapers/wireless/wireless-lan-security-issues-solutions-1009

Hsu, F.-H., Wang, C.-S., Hsu, Y.-L., Cheng, Y.-P., & Hsneh, Y.-H. (2015). A client-side detection mechanism for evil twins. *Computers & Electrical Engineering*, *000*, 1–10. https://doi.org/10.1016/j.compeleceng.2015.10.010

Mustafa, H., & Xu, W. (2014). CETAD: Detecting evil twin access point attacks in wireless hotspots. In *2014 IEEE Conference on Communications and Network Security, CNS 2014*. https://doi.org/10.1109/CNS.2014.6997491

Nakhila, O., Amjad, M. F., Dondyk, E., & Zou, C. (2018). Gateway independent user-side wi-fi Evil Twin Attack detection using virtual wireless clients. *Computers and Security*, *74*, 41–54. https://doi.org/10.1016/j.cose.2017.12.009

Nakhila, O., & Zou, C. (2016). User-side Wi-Fi evil twin attack detection using random wireless channel monitoring. *Proceedings - IEEE Military Communications Conference MILCOM*, 1243–1248. https://doi.org/10.1109/MILCOM.2016.7795501

Nikbakhsh, S., Manaf, A. B. A., Zamani, M., & Janbeglou, M. (2012). A novel approach for rogue access point detection on the client-side. In *Proceedings - 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2012* (hal. 684–687). IEEE. https://doi.org/10.1109/WAINA.2012.

108
Panch, A., & Singh, S. K. (2010). A novel approach for evil twin or rogue AP mitigation in wireless environment. *International Journal of Security and its Applications*, *4*(4), 33–38.
Song, Y., Yang, C., & Gu, G. (2010). Who is peeping at your passwords at starbucks? - To catch an evil twin access point. In *Proceedings of the International Conference on Dependable Systems and Networks* (hal. 323–332). IEEE. https://doi.org/10.1109/DSN.2010.5544302
Tang, Z., Zhao, Y., Yang, L., Qi, S., Fang, D., Chen, X., … Wang, Z. (2017). Exploiting Wireless Received Signal Strength Indicators to Detect Evil-Twin Attacks in Smart Homes. *Mobile Information Systems, 2017*. https://doi.org/10.1155/2017/1248578