CROZONO: Cracking the Security Perimeter with Drones & Robots

Mg. Ing. Pablo Romanos, Sheila Berta

Departamento de Investigación Tecnológica, Facultad de Ingeniería, Universidad de la Marina Mercante
Buenos Aires, Argentina
promanos@udemm.edu.ar
sberta@udemm.edu.ar

***Abstract*— This work focuses on the development of a software module and a working methodology (framework CROZONO) for automated penetration testing security perimeters from unconventional mobile devices (drones, robots, remote control prototypes, etc.) that can facilitate access to the physical environment of a wireless network.**

***Resumen*— El presente trabajo denominado CROZONO, se centra en el desarrollo de un framework que contiene diversos módulos de software que permiten la realización de pruebas de penetración automatizadas en perímetros de seguridad, desde dispositivos móviles no convencionales que podrían facilitar el acceso al medio físico de una red inalámbrica (drones, robots, prototipos teledirigidos, etc.).**

I. INTRODUCCIÓN

La tecnología Wi-Fi aprovecha la tecnología de radiofrecuencia que proporciona ventajas en comparación con otras tecnologías cableadas tradicionales. A pesar de que la tecnología inalámbrica puede proporcionar una red altamente eficiente, de fácil implementación y de bajo costo, el principal freno es el mantenimiento de su seguridad. En las topologías tradicionales por cable, el acceso físico al medio de transmisión está limitado sólo a los usuarios autorizados, sin embargo en las redes WLAN el acceso físico al medio lo tiene toda persona que esté dentro del rango del AP. Actualmente, el protocolo de seguridad WPA/WPA2 es incapaz de brindar total fiabilidad en la protección frente al acecho de los atacantes, mucho menos puede hacerlo el protocolo WEP. Al comprometer una red WiFi, un atacante puede llevar a cabo diversas técnicas que le permitirían con mayor facilidad acceder a los equipos que están en esa misma red y robar información sensible de los usuarios.

II. DESARROLLO DE CONTENIDOS

CROZONO se presenta como un framework de código abierto desarrollado en Python versión 3, que se encuentra disponible para ser empleado en plataformas de hardware libre, tales como Raspberry PI, Cubieboard y equivalentes, pudiendo ser empleado para realizar pruebas de penetración en perímetros de seguridad desde dispositivos móviles no convencionales (drones en general, quadcopters, hexacopters, octacopters, robots, prototipos teledirigidos, etc.).

Las pruebas que han sido realizadas con CROZONO se han hecho empleando distintos tipos de drones (Ej.: Phantom 3, de la firma DJI, adaptado para poder soportar una Raspberry PI) y robots (un robot llamado Axón especialmente diseñado para moverse en espacios públicos.

Arquitectura Funcional de CROZONO

CROZONO posee la capacidad de realizar ataques automatizados y dirigidos a una red o a un grupo de redes y tomar decisiones -sin requerir la interacción directa del atacante- sobre qué ataques llevar a cabo en base a parámetros preestablecidos y a la información que recopila sobre su objetivo. La meta de CROZONO es introducirse en una red y comprometer uno o varios de los equipos de la misma. Para lograrlo, incorpora diversos módulos que implementan variados ataques para WLAN y LAN, que mencionaremos en los párrafos subsiguientes.

CROZONO es un framework inteligente: ajusta la configuración de su hardware automáticamente, busca el objetivo y sabe elegirlo; lleva a cabo el ataque adecuado para crackear la red y una vez que lo ha logrado, realiza un mapeo de la misma obteniendo información de cada equipo activo y llevando adelante el ataque que haya sido previamente definido. Entre los ataques disponibles se encuentran Sniffing y MITM, MITM con Evilgrade o ataques relacionados con la ejecución de exploits mediante Metasploit. Estos ataques, una vez lanzados, desencadenan una comunicación reversa con el atacante enviándole en tiempo real -a través del acceso ganado sobre la red de la víctima- toda la información capturada y/o necesaria según el ataque que se ha llevado a cabo.

Para lograr todo esto, CROZONO realiza en resumen, los siguientes pasos: Al iniciar prepara su hardware, lo cual implica detectar el adaptador USB WiFi conectado, cambiar su modo a monitor, cambiar la dirección MAC (falseo de MAC), entre otras configuraciones. Luego obtiene información acerca de todas las redes WiFi (AP) que están dentro de su alcance (tarea que toma aproximadamente unos 60 segundos). En base a la información recopilada, CROZONO decidirá cuál será su objetivo (a menos que se lo haya especificado antes). Para ello tendrá en cuenta por ejemplo, la cercanía con la red y la cantidad de vectores de inicialización (en adelante IVs) que ha capturado de la

misma. A partir de esto, seleccionará la red más conveniente para atacar.

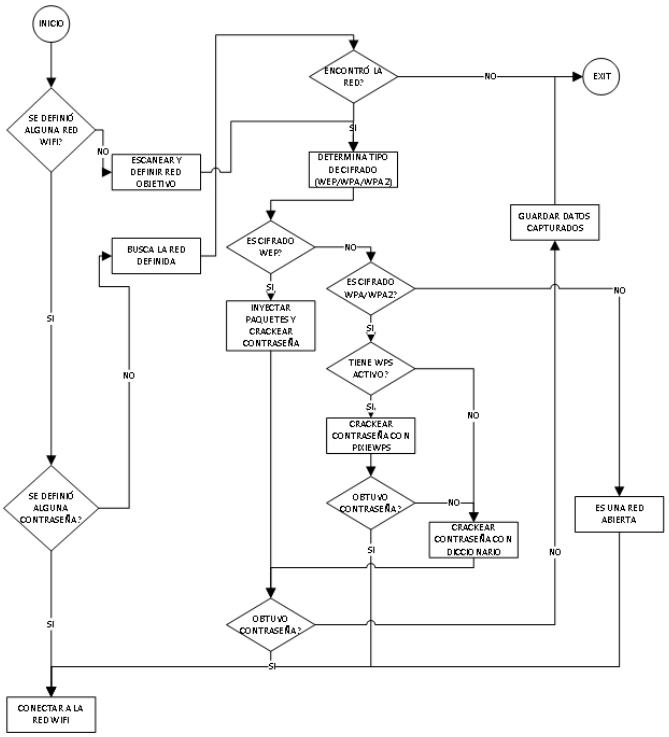
Al momento de lanzar el ataque hacia la red WiFi, CROZONO analiza la información previamente capturada sobre su objetivo y detecta su nivel de privacidad (WEP, WPA/WPA2, WPA/WPA2 con WPS) para rápidamente realizar el crackeo del AP ejecutando el ataque adecuado de acuerdo con el protocolo de seguridad empleado. El framework intentará crackear la red de la forma más ágil y rápida posible; incorporando diversos módulos de ataque y analizando cuál utilizar. Si eventualmente el ataque seleccionado por CROZONO no fuera exitoso, éste cambiará de forma automática a otro tipo de ataque, de acuerdo con el nivel de seguridad configurado en la red víctima.

En caso de que CROZONO no pudiese obtener la contraseña del punto de acceso WiFi, guardará la información capturada (por ejemplo el handshake en WPA/WPA2) y el dispositivo móvil (drone o equivalente) tendrá la opción de regresar al punto de origen, para que el atacante realice el intento de crackeo de la contraseña desde otro equipo con mayor poder de cómputo. Una vez logrado esto, será posible suministrarle a CROZONO la contraseña de la red para que el drone (o equivalente) regrese al punto en donde se encontraba y continúe con la segunda fase del ataque, esta vez dirigido a la red LAN.

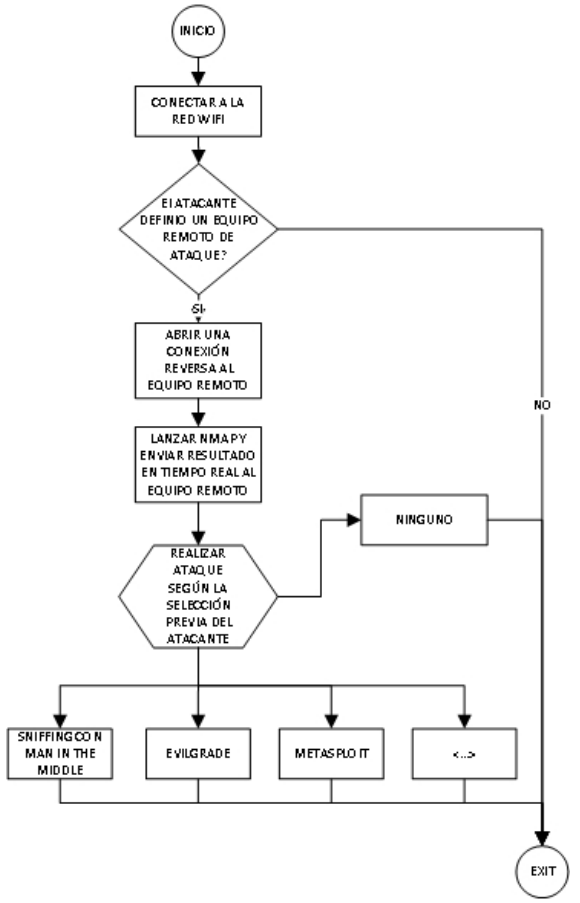
Una vez obtenida la contraseña del punto de acceso WiFi, CROZONO modifica la configuración de su hardware y se conecta a la red. He aquí el mayor peligro para la víctima dado que CROZONO realiza un mapeo de la red obteniendo los equipos activos con sus respectivos puertos abiertos y servicios; y envía esta información en tiempo real al atacante, ejecutando a la vez el ataque que se le haya definido previamente Ej.: sniffing y MITM (con envío de datos en tiempo real) o acceso a un equipo de la red mediante Evilgrade, enviando al atacante una sesión de Meterpreter o de otro agente sobre dicho equipo (haciendo una conexión reversa a través de la conexión local de internet de la víctima).

III. DIAGRAMAS DE CONTEXTO

A continuación se presentan los diagramas de flujo de datos correspondientes a la Fase I – Ataque a la red WLAN y a la Fase II – Ataque a la red LAN.



Fase I – Ataque a la red WLAN



Fase II – Ataque a la red LAN

IV. DESCRIPCIÓN

A. Estructura Modular

A continuación se listan los módulos de ataque publicados a la fecha (marzo 2016), disponibles para utilizar en las diferentes versiones de CROZONO. Los ataques de

cada módulo son llevados adelante de forma autónoma y prácticamente sin necesidad de interacción con el atacante.

1) Módulos de ataque para el perímetro WLAN (Fase I)

- Cracking WEP: Se utiliza de fondo la suite de Aircrack-ng para atacar la implementación de WEP. Mientras se capturan los IVs, se ejecuta una asociación al punto de acceso seguido de una inyección de paquetes, cuyo objetivo es generar el suficiente volumen de datos capturados para obtener la clave de manera rápida.
- Cracking WPA/WPA2: Se utiliza de fondo la suite de Aircrack-ng para desautenticar a los clientes conectados al punto de acceso WiFi, de manera que cuando se vuelven a conectar, el handshake es capturado y se procede a realizar el crackeo utilizando diccionarios.
- Cracking WPA/WPA2 con WPS: Se utiliza de fondo la herramienta Reaver en conjunto con PixieWPS para atacar aquellos puntos de acceso WiFi que tengan activo el WPS.
- Almacenamiento del handshake y/u otros datos capturados del AP, para entregar al atacante en caso de que fallen los ataques anteriormente descritos.

CROZONO utiliza los diferentes módulos de ataque de fase I por sí mismo, decidiendo de forma inteligente cuáles utilizar, según el nivel de seguridad que haya detectado sobre su objetivo.

2) Módulos de ataque para el perímetro LAN (Fase II)

- Mapeo de la red: se utiliza de fondo la herramienta NMap para realizar la detección de equipos activos, puertos abiertos y servicios ejecutándose en cada uno de ellos. El resultado es enviado al atacante en tiempo real.
- Sniffing y MITM: se utilizan de fondo las herramientas ettercap y tshark para realizar un MITM entre el Gateway y un equipo de la red víctima elegido al azar. Toda la información capturada por el sniffer se envía al atacante en tiempo real.
- MITM con Evilgrade: Se utilizan de fondo las herramientas ettercap y evilgrade. A través de un DNS Spoofing realizado con ettercap, evilgrade puede infectar un equipo de la red víctima cuando éste intente actualizar determinado software. CROZONO lo implementa permitiendo utilizar el agente que se desee (por ejemplo: troyano, meterpreter, etc.).
- Metasploit: se le permite al atacante interactuar en tiempo real con una terminal de metasploit. Esto se realiza abriendo una conexión inversa hacia el atacante, utilizando el acceso a internet de la red comprometida. La terminal de metasploit se ejecuta a través de CROZONO, lo que significa que es posible hacer pivoting y/o ejecutar exploits funcionales en redes LAN.

CROZONO configura el módulo de ataque de fase II de forma automática, ahorrando tiempo sumamente útil en el caso de utilizar drones que posean una autonomía de batería limitada.

B. Parametrización

Como se expresó anteriormente, CROZONO posee la capacidad de decidir por sí mismo la red que le conviene atacar y los módulos que empleará para ganar el acceso a la misma. Sin embargo, a través de diversos parámetros es posible indicarle a CROZONO una red específica a penetrar, y ampliar su alcance definiendo los ataques a llevar a cabo para el perímetro LAN una vez realizada con éxito la fase I.

A continuación se describen algunos ejemplos de parámetros:

```
./crozono.py –d <IP_ATACANTE>
```

La ejecución de CROZONO utilizando sólo el parámetro –d implica que el framework tome el control absoluto y decida qué red atacar y de qué forma hacerlo. Una vez que logre acceder a la red, recopilará información de los equipos activos dentro de la misma y enviará el resultado en tiempo real al atacante a través de una conexión inversa hacia la IP identificada mediante el parámetro –d.

```
./crozono.py   -e testAP -d <IP_ATACANTE>
```

El parámetro –e permite indicarle a CROZONO el ESSID a atacar. Al momento de iniciar la fase I, buscará la red especificada y en caso de encontrarla, avanzará sobre el crackeo de la misma. A partir de este punto, procederá a realizar el mapeo de la red y enviará la información en tiempo real al atacante.

```
./crozono.py –e testAP –k <contraseña> -d
<IP_ATACANTE>
```

Si el atacante conoce los datos de acceso a la red podrá indicarlos, de manera que CROZONO al iniciar la fase I, busque esa red y se conecte a ella mediante la contraseña especificada con el parámetro –k. Una vez dentro de la red, procederá a realizar el mapeo de la red y enviará la información en tiempo real al atacante.

```
./crozono.py –e testAP –k <contraseña> –a
evilgrade –d <IP_ATACANTE>

./crozono.py –a evilgrade –d <IP_ATACANTE>
```

El parámetro –a permite especificar un ataque que se llevará a cabo una vez que CROZONO penetre la red. Para el ejemplo anterior: –a evilgrade, se llevará a cabo un MITM, junto con la ejecución de evilgrade; lo que permitiría eventualmente comprometer algún equipo dentro de la red, infectando la misma con el agente que se desee (por ejemplo un meterpreter o un troyano). Toda la información capturada es enviada al atacante en tiempo real.

```
./crozono.py –a metasploit –d <IP_ATACANTE>
```

El valor “metasploit” junto al parámetro –a, permite indicar a CROZONO que una vez que gane acceso y recopile información relevante de la red, ejecute una terminal de Metasploit a merced del atacante. De esta manera el atacante podrá lanzar exploits funcionales en redes LAN como por ejemplo: ms08_067, comprometiendo los equipos de la red interna.

```
./crozono.py –a sniffing-mitm –d
<IP_ATACANTE>
```

Mediante el valor “Sniffing-mitm” al parámetro –a, se le indica a CROZONO que se desea ejecutar un ataque de Sniffing junto a MITM dentro de la red, una vez que se haya ganado el acceso a través de los módulos de ataque de fase I.

Toda la información capturada es enviada al atacante en tiempo real.

C. Características Exclusivas

En la actualidad, diversos grupos de hackers/especialistas han intentado utilizar drones y/o dispositivos teledirigidos para llevar cabo ataques informáticos a diferentes infraestructuras. En algunos casos ciertos grupos han creado su propio dispositivo móvil no convencional con el hardware necesario para lanzar ataques. En otros casos han montado un hardware libre sobre drones de fabricantes conocidos. Estas iniciativas tienen como denominador común facilitarle al atacante una terminal de comandos remota a través de una conexión mobile (GPRS o superior) sobre el hardware anexado al drone, de manera que pueda ejecutar manualmente algunos ataques.

CROZONO posee numerosas diferencias sobre éstos inventos. La primera de ellas es que el foco de la solución está en el software y no en el hardware. Tal afirmación implica que CROZONO es independiente del hardware donde se ejecuta, convirtiéndolo en una solución portable, capaz de ser implementada en cualquier tipo de drone y robot (conocido o no, ya inventado o del futuro).

Además, tal como se ha comentado anteriormente, CROZONO es totalmente automático; posee la capacidad de decidir por sí mismo los módulos de ataque que ejecutará. No necesita interacción con el atacante, por lo que no es necesario que sea controlado por una conexión mobile (GPRS o superior), logrando que su alcance llegue hasta lugares donde tal tecnología no esté disponible.

Otra de las ventajas de los ataques automatizados es que permiten que el ataque se lleve a cabo de una forma más rápida que si el atacante tuviera que hacerlo a mano mediante una terminal de comandos. Esto implica una gran ventaja cuando se implementa en drones o robots que tienen una baja autonomía de batería.

CROZONO pretende convertirse en la primera elección de los especialistas en seguridad, a la hora de utilizar dispositivos móviles no convencionales para realizar pruebas de penetración.

V. REFERENCIAS

A. Bibliografía Consultada

[1] Pranav S. Ambavkar, Pranit U. Patil, Prof. Pamu Kumar Swamy (2012). Exploitation of WPA Authentication. Engineering (IOSRJEN) Vol. 2 Issue 2, Feb.2012, pp. 320-324.

[2] Zhendong Wu, Mengru Cai, Siyu Liang, Jianwu Zhang. (2014). An Approach for Prevention of MitM Attack Based on Rogue AP in Wireless Network. By IFSA Publishing, S.L.

[3] Aaron L.-F. Han. Derek F. Wong. Lidia S. Chao. Password Cracking and Countermeasures in Computer Security: A Survey. University of Macau, Macau SAR. ILLC, University of Amsterdam, Science Park 107, 1098 XG Amsterdam.

[4] Gounaris Georgios. (2014) WiFi security and testbed implementation for WEP/ WPA cracking demonstration. Kingston University London

[5] Johnny Cache, Vincent Liu. Hacking Exposed Wireless: Wireless Security Secrets & Solutions 1st Edition. Mc. Graw-Hill.

[6] Stuart McClure, Joel Scambray, George Kurtz. Hacking Exposed: Network Security Secrets and Solutions, Sixth Edition. Mc. Graw-Hill.

[7] Sheila Berta. (2013) WEB Hacking. Claves para desarrolladores y administradores de sitios. Ed. Users.

[8] Rodney Beede. Ryan Kroiss. Arpit Sud. (2011). Distributed WPA Cracking. University of Colorado.

B. Congresos y Conferencias

CROZONO ha sido aceptado para ser presentado en diversos congresos y conferencias, tanto en el ámbito de la seguridad informática, como en el de la tecnología y la innovación:

[1] Ekoparty Security Conference | 11 Back To Root | 21, 22 y 23 de Octubre de 2015 | Buenos Aires.
https://www.ekoparty.org/charla.php?id=34

[2] JATIC 2015 | Jornadas Argentinas de Tecnología, Innovación y Creatividad | 4, 5 y 6 de noviembre de 2015 | Mar del Plata | Buenos Aires.
http://jatic2015.ucaecemdp.edu.ar/trabajos_aceptados.php

[3] ISSA (Information Systems Security Association) Argentina | 10 de diciembre de 2015 | Buenos Aires.
https://www.facebook.com/issaarba/

[4] OWASP Latam Tour 2016 | 22 de abril de 2016 | Buenos Aires.
https://www.owasp.org/index.php/LatamTour2016

Próximos eventos a ser presentado:

[1] XI ENAI | Encuentro Nacional de Auditores Internos | 21 y 22 de abril de 2016
http://www.enai2016.com/

C. Publicación en Revistas de Divulgación Científicas

CROZONO surge como trabajo de investigación dentro del ámbito académico. A pesar del poco tiempo que lleva como proyecto ya cuenta con algunas publicaciones en revistas de tecnología aplicada y divulgación científica:

[1] JATIC 2015 | Jornadas Argentinas de Tecnología, Innovación y Creatividad | 4, 5 y 6 de noviembre de 2015 | Mar del Plata | Buenos Aires | Libro de Actas: ISBN 978-987-23963-2-9
http://www.jatic2015.ucaecemdp.edu.ar/Libro_de_Actas_JATIC_2015.pdf

[2] Revista Atenea – Universidad de la Marina Mercante - Marzo 2016 – Publicación en papel: ISSN 1668-348X

D. Notas en Medios de Comunicación

Algunas de las notas realizadas en diferentes medios de comunicación sobre el Proyecto CROZONO:

http://next.clarin.com/innovacion/escenario-participacion-termina-Buenos-Aires_0_1454254848.html

http://next.clarin.com/prueban-desde-drone-se-puede-hackear-red-Wi-Fi_0_1453654646.html

http://www.welivesecurity.com/la-es/2015/10/23/drones-usados-para-pruebas-de-penetracion/

http://www.telam.com.ar/notas/201510/125117-expertos-probaron-la-vulnerabilidad-de-las-redes-wifi-con-un-software-que-se-maneja-a-traves-de-un-dron.html

http://www.elladodelmal.com/2016/03/crozono-uso-de-drones-y-robots-en-tests.html

http://www.eldia.com/revista-domingo/demuestran-a-traves-de-un-dron-que-en-las-redes-wifi-puede-pasar-cualquier-cosa-95152

Presentación de CROZONO en programas de televisión y eventos de tecnología:

https://www.youtube.com/watch?v=EbDWMCPp1Ao

https://www.youtube.com/watch?v=4_LuCJOusoE

https://vimeo.com/album/3682874/video/147894742

E. Organizaciones que Apoyan al Proyecto

Instituciones educativas, así como organizaciones públicas y privadas, algunas de ellas de reconocimiento internacional, han depositado su confianza al prestarse para realizar pruebas y evaluaciones de seguridad con CROZONO.

I. UNIVERSIDADES E INSTITUCIONES EDUCATIVAS

[1] UdeMM | Universidad de la Marina Mercante. Ref.: Ing. Diego Caputo. Decano Facultad de Ingeniería.
http://www.udemm.edu.ar/

[2] UAI | Universidad Abierta Interamericana. Ref.: Ing. Luis Franchi. Vicerrector de Extensión Universitaria.
http://www.uai.edu.ar/

[3] Escuela Da Vinci | Escuela de Arte Multimedial. Ref.: Ing. Alejandro Martínez Casas. Director de Estudios.
https://www.davinci.edu.ar/

II. ORGANIZACIONES PÚBLICAS Y PRIVADAS

[1] Policía Metropolitana de Buenos Aires | Ministerio de Seguridad. Área Delitos Informáticos. Ref.: Comisionado Carlos Gabriel Rojas. Director de Delitos Informáticos.
http://www.metropolitana.gob.ar/

[2] Axion Energy | Área IT. Ref.: Pablo Giancarli. Regional TIC Manager.
http://www.axionenergy.com/

[3] OSDE | Organización de Servicios Directos Empresarios. Área Seguridad Informática. Ref.: Hernán Layño. CIO.
https://www.osde.com.ar

F. REFERENCIAS DE APLICACIÓN Y USO DE CROZONO

A continuación se evidencian algunas de las aplicaciones de CROZONO a partir de su uso en dispositivos móviles no convencionales (drones y robots).

CROZONO, Raspberry PI y Drone DJI Phantom 3

Pruebas realizadas con Drone DJI Phantom 3 (1)

Pruebas realizadas con Drone DJI Phantom 3 (2)

Pruebas realizadas con Robot Axón (1)

Pruebas realizadas con Robot Axón (2)

Equipamiento para la realización de pruebas

G. CONSIDERACIONES FINALES

El uso no autorizado de CROZONO como herramienta de ataque, constituye un delito según la ley argentina (cfr. Art 153 Código Penal modificado por la ley 26.388). A esto se suma la nueva legislación provisional sobre el uso de dispositivos no tripulados de la ANAC - Res. 527/2015; la Disposición 20/2015 de la DNPDP sobre recolección de información personal mediante el uso de VANTs (vehículos aéreos no tripulados) y lo establecido en la ley de Inteligencia Nacional 25.520 Titulo VI.