Telecomunicaciones y privacidad.

Resumen.

El presente ensayo tiene como objetivo fundamental demostrar los problemas de seguridad en los cuales estamos sometidos desde tiempos previos a Snowden y que él nos informo de su existencia, como resulta mucho más procedente creer que no solo las personas pueden realizar una vigilancia, sino que son los Estados, Empresas y usuarios (en grupos) los que generan esta vigilancia. Para ello empleamos un método de "romper para reparar", en pocas palabras como violar nuestra privacidad, generar una forma de vigilancia, para luego incrementar nuestros niveles de seguridad, con el fin de intentar que esa vigilancia sea nula o mucho más complicada de realizar, este no es un enfoque técnico sino orientado a Abogados.

Introducción.

Corría el año 1955 y la empresa AT&T publica un artículo donde se explicaba como se trazan las comunicaciones telefónicas, sin publicar la frecuencia que utilizaban los tonos, esto fue debelado en 1964, con estas dos indicaciones se dejo abierta la puerta a que cualquier persona con conocimientos de electrónica pudiera comenzar a utilizar el servicio de una forma "distinta".
Este es el comienzo de una nueva forma de pensar la forma de utilizar las cosas, y fue el inicio del pensamiento Hacker, gracias a Josef Carl Engressia (Joybubbles) y John Draper (Capitán Crunch) modificaron un silvato y lo hicieron sonar a 2600hz, con ello ingresaban en el sistema de telefonía y les permitía realizar cualquier llamada telefónica de forma gratuita. Con esto comenzó a darse forma la bluebox, y el pensamiento hacker que hoy conocemos como tal, es decir la utilización de una cosa con un fin distinto.

En los días en los que vivimos Internet nos lleva a pensar muchas veces de la misma forma en que lo hicieron estas personas, para usar el concepto de "romper para reparar".

¿Que podemos romper?.

En la actualidad, Internet es una herramienta que se basa en dos protocolos, que ya todos conocemos ellos son TCP/IP el principal problema es el protocolo TCP que tiene errores desde su creación y por ello nuestras comunicaciones son más delicadas en cuanto a la privacidad y la vigilancia que nos pueden producir, tanto Estados, Empresas o Usuarios. Es necesario entender "que" podemos (y como) romper en materia de seguridad en nuestras comunicaciones para luego incrementar los niveles de nuestra propia seguridad y con ello, nuestra privacidad. Hoy con ver simples vídeos en Internet comprobamos que el conocimiento se encuentra a disposición de quien tenga la intensión de abrir cualquier sistema, conocer de programación[1], de realizar un test de penetración sobre su maquina (o su modem), y como incrementar los niveles de seguridad[2]. Claro que también puede ser utilizado en forma deshonesta y realizar dichos controles sobre objetivos no tan santos, y realizar delitos ya tipificados por el Código Penal desde el año 2008, es por esto que sostenemos que este trabajo es a nivel educativo y a los únicos fines de nuestra investigación, la propia seguridad de nuestras comunicaciones a la hora de tener una conversación privada con nuestros clientes.

1 https://rubymonk.com/ como aprender a programar Ruby, de forma autodidacta.
2 http://www.jsitech.com/linux/tips-para-mejorar-la-seguridad-en-los-servidores-linux/ aunque es sobre servidores, esta información es igual de buena para un uso normal.

Vamos a intentar vulnerar TODO, si todo lo que se nos ocurra, con los fines de demostrar que la vigilancia es algo innecesario y contrario al concepto de seguridad, que esta seguridad debe ser el objetivo del Estado, y que la vigilancia trae consecuencias negativas.

¿Que vamos a utilizar?.

Software, simples programas de computadora, de código abierto, de distribución gratuita y desarrollados por la misma comunidad que todos integramos. Algunos de ellos son: Kali Linux, Wireshark, Backtrack, Kali, etc. Y para aumentar nuestra privacidad, y por tanto disminuir la vigilancia y así aumentar nuestra seguridad: Linux, Thunderbird, TOR, Ciboulette, Riseup, Enigmail, etc.

Comencemos!!!.

Parte 1.

Desde 1998, ingresamos al mundo de Internet con un acceso bastante precario y fue mejorando a lo largo de los años, pero la gran cantidad de usuarios lo hacían con Sistemas Operativos privativos y esos sistemas siempre fueron (y de forma creciente) inseguros, muchos recuerdan los virus como Miguel Angel y más en nuestros tiempos LOVE. Esto es culpa del mismo SO que se encuentra diseñado de forma deficiente, y es necesario colocar un antivirus, para no correr estos riesgos (perder información, ese era el riesgo). Hoy muchos usuarios no aprendieron de estos problemas y continúan utilizando estos sistemas, dado que los SO seguros se demoraron mucho en generar un entorno gráfico "amigable" para el usuario doméstico y esto fue, es y será la mayor deuda del software libre.
Ya en el año 2001 los Estados entendieron que los Delitos Informáticos comenzaban a ser un problema y por ello se realizó el Tratado de Cibercrimen (o convenio de Budapest) donde se realizó un marco para que los Estados adecuen su normativa a este tipo de delitos.
Argentina tuvo proyectos de ley en este sentido desde 1996, pero no fue hasta 2008 que entró en vigencia la ley de delitos informáticos, que aun continúa vigente, tipificando muchas de las conductas delictivas.
Es claro que la ley de protección de datos personales (Ley 25326), el artículo 43 de la Constitución Nacional, muchas de ellas con muy buenas intenciones y malos resultados, faltos de personal, presupuesto o simplemente sin un funcionamiento claro a la hora de investigar al propio Estado.
Con esto nos vemos obligados a investigar las telecomunicaciones y sabiendo que el Derecho (más precisamente las leyes y sus aplicaciones) vienen en desventaja en relación al tiempo en el cual se aplica. Entonces son los propios usuarios quienes deben incrementar su seguridad y su privacidad en términos de telecomunicaciones en la Internet.

Parte 2.

Como anteriormente señalamos, los SO libres son tardíos en cuanto a una interfaz gráfica amigable y por ello, en los inicios son mucho más complicados de utilizar por el usuario promedio, en cuanto ese entorno gráfico se volvió de uso sencillo, estos se encuentran en un crecimiento exponencial en cuanto a cantidad de usuarios y mucho tuvo que ver el uso de celulares con SO simples y si bien no son libres, estos utilizaron un entorno gráfico muy similar a distintas distribuciones de Linux, dando lugar a que miles de usuarios pasen a la utilización de SO libres, incluso en países se está utilizando dicho software en el Estado (generando ahorro en grandes sumas por licencias y aumentando la seguridad de su país), pero ese es un análisis

para otro trabajo. Comencemos a romper.

En la actualidad, nos es impensable que una computadora no este conectada a Internet, el envío de mail, la conexión a redes sociales, transferencias bancarias, búsquedas de información, ver vídeos, etc. Pero, ¿esas cosas que habitualmente hacemos son seguras, privadas y confidenciales?.

¿Como pueden ingresar a un modem y conectarse a una red wifi con claves de seguridad?.
La respuesta es simple, depende de si la conexción es WEP, WPA o WPA2. Pero de todas formas todas son vulnerables (depende de la clave que ingreso el usuario y de la capacidad que tiene quien quiere ingresar).
Claves WEP: si bien este tipo de cifrado tiene una seguridad "igual a la de una red cableada" fue fácilmente vulnerada y ya no cuenta con el apoyo de la wifi alliance desde 2004, aun en Argentina se continúa con este sistema en todos los usuarios de empresas como Speedy.
Claves WPA: fue creado para reemplazar WEP, incluyendo una mayor seguridad en las comunicaciones de este tipo, utiliza un principio de autenticación mediante un servidor donde se guardan las credenciales y contraseñas, para que no se utilice el servidor se realiza mediante una clave precompartida, este sistema es vulnerable al realizar un ataque de recupero, reinyectando tráfico, esto es posible dado que diversos canales utilizan el modo QoS, pero también es posible utilizarlo por fuera del modo QoS. También se encuentra disponible en todos los ISP que ofrecen el servicio de Wifi en Argentina.
Claves WPA2: Claramente se utiliza este sistema para corregir los problemas de seguridad originados en sus antecesores. Tanto la versión 1 de WPA, como la denominada versión 2, se basan en la transmisión de las autenticaciones soportadas en el elemento de información correspondiente. En el caso de WPA 1, en el tag propietario de Microsoft, y en el caso de WPA2 en el tag estándar 802.11i RSN.
Durante el intercambio de información en el proceso de conexión RSN, si el cliente no soporta las autenticaciones que especifica el AP (access point, punto de acceso), será desconectado pudiendo sufrir de esta manera un ataque DoS específico a WPA.
Además, también existe la posibilidad de capturar el 4-way handshake que se intercambia durante el proceso de autenticación en una red con seguridad robusta. Las claves PSK (precompartidas) son vulnerables a ataques de diccionario (no así las empresariales, ya que el servidor RADIUS generará de manera aleatoria dichas claves), existen proyectos libres que utilizan GPU con lenguajes específicos como CUDA (NVIDIA) y Stream (AMD) para realizar ataques de fuerza bruta hasta cien veces más rápido que con computadoras ordinarias.

Uno puede pensar, que si se conectan a nuestra red Wifi, el único problema que puede existir es que nuestro servicio funcione de forma mas "lenta" que si bien no es un gran problema (para algunas personas) el principal inconveniente es sufrir un proceso legal por algún delito informático realizado desde el wifi en cuestión, pero salvando este inconveniente no existe un problema "significativo" para el propietario del servicio. No así para las empresas que ofrecen este servicio, dado que además de perder un potencial cliente, ven como un abonado tiene un consumo elevado de servicio y el mismo sufre una depreciación en cuanto a cantidad de clientes conectados a un mismo nodo, en definitiva complicaría mucho más la reducción de la cantidad de tráfico que nos va a "recortar" nuestro ISP, que un ataque real desde nuestro equipo.

Este es uno de los pocos casos en los cuales el SO no tiene ninguna incumbencia, dado que el ataque se realiza sobre el Modem o Router[3], pero si algunas Empresas tienen defectos de fabrica

3 Aunque puede utilizarse https://openwrt.org/ para cambiar el firmware de nuestro modem y con esto modificar algunos patrones.

y los accesos son mucho más accesibles de distintas formas, claro que ningún ISP cambia un Modem o Router por estos inconvenientes. Pero de todas formas dichos equipos tienen un firmware que siempre se encuentra desactualizado, es decir hace que el inicio de tu conexión y poder realizar una libre VPN se torne imposible, con ello necesitamos openwrt y además de ser código abierto y utilizar licencias del tipo GPL, se encuentra muy actualizado.
Además, en estos ultimos días se descubrio que Estados Unidos logró descifrar el código de las tarjetas Sim Card de una empresa [4]y esta misma opera en Argentina con Telecom Personal[5]

Parte 3.

Navegando en privado.

Mucho se ha dicho sobre TOR[6], quitando prestigio o diciendo que los usan "hackers para hacer cosas malas", la verdad es que para muchos nuestra privacidad es dinero y con hacer una gran campaña contra nuestra privacidad es muy buenos números para Estados y Empresas, fundamental a la hora de que nuestro cliente nos muestre algunas cosas en Internet, o la mera búsqueda de esto.

The Onion Routers mucho más conocido como TOR, es un sistema de comunicaciones en Internet, el cual nos permite modificar nuestra dirección IP y con ello generar una conexión segura y privada, para que no puedan generar un rastreo de nuestra navegación, de quien la utiliza y desde donde. TOR propone un enrutamiento del tipo "cebolla" es decir por capas, con lo cual hace imposible descubrir la IP de quien se encuentra navegando, claramente hay que tener configurado de forma correcta (cancelar cookies, deshabilitar todos los plugins java, etc) el navegador dado que muchas personas creen tenerlo configurado de forma correcta y no es así.
Según declaraciones de Snowden la agencia de seguridad de Estados Unidos habría roto la seguridad de dicho sistema, consiguiendo mediante una inyección de paquetes detectar un %80 de los datos traficados por dicha red, en cuanto se informó de este inconveniente se cambio el sistema y se colocó una libre VPN haciendo imposible el rastreo de ningún paquete.
En este caso es el único que utilizamos el concepto inverso de lo que veníamos demostrando (romper para reparar) dado que en sus inicios TOR fue creado con el fin de proteger las comunicaciones de la armada naval de Estados Unidos y luego por falta de financiamiento recae en TOR Project desde 2005, en marzo de 2011 TOR fue premiado por la Free Software Foundation[7] y se encuentra utilizándose para aquellos países que vulneran la libertad de expresión y diversas cuestiones políticas en Internet, como vemos tiene finalidades muy distintas a la mala prensa que contiene el servicio que brinda.

Parte 4.

El correo electrónico.

Actualmente se cree (en el campo del derecho) que el correo electrónico es igual que una carta ordinaria, y no es cierto, más bien es como el envío de una postal sin sobre, es decir que el sobre protege de una forma la privacidad del correo y en el correo electrónico no existe un "sobre" sino que circula desprotegido de tal elemento.

---

4 La Emprea es Gemalto http://infomed66.blogspot.com.ar/2015/02/nsa-robo-millones-de-sim-card-claves-de.html
5 http://tecnoportaleconomico.blogspot.com.ar/2011/10/gemalto-y-personal-argentina.html por ejemplo en el acceso a Facebook de sus clientes.
6 https://www.torproject.org/
7 https://www.fsf.org/

Existen varias formar de vulnerar la seguridad de los correos, pero siempre es necesario instalar en la PC a atacar un Keylogger o una aplicación, para obtener la dirección y la contraseña, podemos instalar en la PC un software como keylogger Doublas 2,0 y aguardar a que cualquier persona ingrese desde esa PC (es claro que todo lo que escriba va a ser guardado en una carpeta oculta) se debe tener el antivirus (si utilizan SO privativos) deshabilitado.
Podemos realizar ataques con Kali Linux para obtener dichas contraseñas, con ingenieria social, es una forma de obtener cualquier tipo de contraseñas, desde un ataque remoto.
Pero existe un problema adicional a la privacidad y seguridad de los usuarios, y es que el servicio de correo electrónico se encuentra en permanente vigilancia de los prestadores más comunes (como Gmail), para brindar publicidad o para (a pedido de la justicia en nuestro país) obtener todos los correos de determinado usuario.
Entonces ¿como nos protegemos?, recordemos que vamos a proteger la privacidad y la vigilancia, entonces existen varias formas.
Cifrar el contenido del mensaje[8], es decir utilizar un software de cifrado para ello necesitamos distintas claves (una publica y una privada), en el cual el mensaje (en este caso nuestro mail) no va a ser observado por la empresa que brinda el servicio, y de ningún otro usuario que no tenga dicha clave publica.
Otra forma es utilizar servicios de correo electrónico que garantisen la seguridad de nuestros mensajes y nuestra privacidad (como ser Riseup[9]) estos servicios no solo tienen cifrada la comunicación de nuestro mail (desde origen hasta destino) sino que los servidores utilizados se encuentran cifrados, con ello se protegen de ataques externos y de cualquier solicitud judicial que quiera obtener dicha información.
Lo ideal es tener un servicio de correo electrónico para usos generales, y un servicio que resguarde nuestras comunicaciones para obtener una privacidad de las cosas que queremos que sean privadas, por ejemplo la comunicación entre abogado y cliente.

Parte 5.

Redes sociales.

Como vimos en la Parte 4 cualquier ataque externo puede darnos la contraseña del usuario, es por esto que no se recomienda la utilización de casi ninguna red social (o mantener su uso conociendo las distintas vulnerabilidades que conlleva), si bien casi todas las personas utilizan redes sociales para distintos fines (recreativos, venta de productos, publicidad) muy pocos ven los riesgos que tienen frente a la vigilancia y privacidad de sus datos. No solo nunca se encuentra inscripta la base de datos, sino que todos los datos ingresados no son de pertenencia de quien los sube, sino de la red social (esto es un problema). Informar que nuestros datos (sean fotos, publicaciones o archivos) son de uso propietario por parte de las empresas es el modelo de negocio (dado que hasta borran los metadatos[10]) que es el de trasmitir publicidad directa en función a los gustos (o visitas) de quien usa dicha red social.
Además las empresas se encuentran en permanente observación por distintos organismo, que pueden ser muy buenos en materia de delitos, pero algunos no son de este tipo y brindan un espionaje muy real a sus usuarios.

---

8 https://enigmail.net/home/index.php es un servicio adicional al Thunderbird y cifra nuestros correos antes de ser enviados a cualquier servidor.

9 https://help.riseup.net/es una buena aclaración es que para obtener una cuenta hay dos formas, una es solicitar la cuenta indicando el motivo por el cual se requiere este tipo de correo (casi nunca responden), la otra es soliicitar dos códigos (una a cada usuario diferente) y poder abrir nuestra cuenta nueva.

10 Para saber que es un metadato y que redes sociales las eliminan recomiendo http://netting.wordpress.com/2013/09/02/imagenes-a-por-los-metadato/

Existe una red social en base a TOR realizada en Buenos Aires y su nombre es Ciboulette[11] *dado que opera con la misma lógica que TOR es 100% privada si realizamos la configuración correcta y manejamos los proxys de forma correcta. Esta es la única red social completamente segura para el usuario.*

Parte 6.

Protección de nuestra PC.

Como anteriormente dijimos, utilizar software libre es una de las opciones más seguras en relación a virus y malware debemos aumentar el nivel de nuestra seguridad, dado que los dispositivos que utilizamos son de muy buena utilidad para vulnerar la privacidad y generar un nivel de vigilancia optimo. Casi todas las Notebook, Netbook poseen cámaras de video o webcam y casi ninguna de ellas tiene su lente cerrada, y este es un objetivo más habitual de lo que pensamos tanto por delincuentes como por parte de investigaciones que pueda utilizar cualquier servicio del Estado (el nuestro o cualquier otro) para poder observar quien se encuentra frente a estos dispositivos (un ejemplo básico es utilizando Cammy, pero existen otras formas). La única forma se estar seguros es tapando el objetivo de la cámara.
Si nuestros datos pueden ser vulnerados, ingresando a nuestra PC, como me protejo?.
Entonces podemos cifrar nuestro Disco Rígido, esto se puede realizar al instalar el Sistema Operativo (un Ubuntu, por ejemplo), pero si no le realizamos en ese momento podemos utilizar Truecrypt (pero desde hace unos meses presenta problemas de seguridad), recomendamos utilizar LUKS[12] *(en caso de utilizar Sistemas Operativos Libres) o AxCrypt (en Sistemas Operativos Privativos). LUKS es posible su utilización en dispositivos de almacenamiento externos. Si interesa saber como es el funcionamiento de GPG, solo hay que visitar su web https://www.gnupg.org/ donde explican de forma muy completa su desarrollo.*
Si tenemos archivos cifrados y deseamos enviarlo a cualquier servicio de "nube", entonces ciframos nuestros archivos y los subimos, destacamos que algunos servicios de "nube" se encuentran brindando información a distintos Estados, por ello en caso de necesitar este tipo de servicios recomendamos utilizar Owncloud[13]

Si bien existen muchas otras formas de vulnerar la privacidad de las personas, sean por el Estado o por delincuentes, existen formas de protegernos y esta es la finalidad de este trabajo, el mismo presenta las ventajas de utilizar software libre. Lo importante de nuestra privacidad (además de ser nuestra), es mantener la confidencialidad entre Abogado y cliente.

Autor: Rodrigo Iglesias.

11 http://wiki.hackcoop.com.ar/Ciboulette
12 https://code.google.com/p/cryptsetup/
13 http://owncloud.org/