Modelo de Evaluación de Canales Ocultos para Establecer una Comunicación Segura

Gunnar Wolf

Especialidad en Seguridad Informática y Tecnologías de la Información
SEPI • ESIMECU

Proyecto de especialización • 18 de mayo, 2015

Objetivo general

Desarrollo de un **modelo descriptivo** que permita **caracterizar** los distintos **canales ocultos** de comunicación, y **evaluarlos** sobre sus distintos ejes.

Esto permitirá tanto que un *administrador* pueda **compararlos** para necesidades particulares, como auxiliar para que un *desarrollador* pueda **enfocarse en los puntos** que necesita para diseñar una nueva propuesta.

Hipótesis

El desarrollo de un modelo que documente los componentes y principales interacciones para la implementación de mecanismos de comunicación sobre canal oculto contribuirá a su mejor comprensión y uso, y contribuirá a que los canales ocultos dejen de verse desde un punto de vista meramente *adversarial* para convertirse en un objeto del estudio formal.

Objetivos particulares (1)

1. Caracterizar **escenarios** de comunicación legítima empleando canales ocultos.
2. Realizar una revisión bibliográfica de las diferentes **implementaciones** de canales ocultos existentes, tanto en la literatura formal científica/académica como entre las comunidades de práctica.
    1. Explorar y contrastar los distintos **espacios de ocultamiento** empleados.
    2. Determinar la validez de un **término único** para las distintas implementaciones.
3. Examinar los **fundamentos teóricos** sobre los cuales se construyen las implementaciones abordadas.
    1. Explorar los planteamientos formales respecto al uso de **canales de comunicación**, **espacios de ocultamiento** de información, estimación de capacidad de canales y autenticación.

Objetivos particulares (2)

4. Analizar y validar la necesidad de este trabajo entre un **grupo amplio de especialistas**.
5. Integración de un modelo que permita la **descripción y comparación** de los esquemas resultantes del inciso 2.
    1. Aplicar el modelo a todos los **esquemas presentados**, retroalimentándolo de forma iterativa.
6. Desarrollo de una **propuesta de canal seguro** que ataque a los supuestos planteados en el inciso 1, considerando los aspectos obtenidos del inciso 4.
    1. Aplicar el **modelo** integrado en el inciso 5 a la propuesta desarrollada.
7. Sintetizar la aplicación del modelo a todos los esquemas presentados (incluyendo al propuesto) en una **comparativa global**.

Justificación

- Existen numerosos esquemas de administración remota de servidores sobre *canales cifrados*
  - Pueden resultar insuficientes para la respuesta a incidentes
- Propuesta: Uso de *canales ocultos* como parte de la gestión completa y proactiva de la seguridad
- Presentación de los canales ocultos desde un acercamiento no *adversarial*

Escenarios legítimos ejemplo justificando este enfoque:

- Administración desde redes públicas o poco confiables
- El administrador inter-jurisdiccional
- Gestión de un *honeypot*

Canales ocultos

- Antecedentes
  - 1970s (Lampson; Schaefer) en adelante
  - 1990s (NCSC, *Serie del Arcoíris*)
- Port knocking
  - $\approx$ 2003 (Krzywinsky) – 2006: Popularización
  - Crítica: Izquierdo Manzanares, 2005; deGraaf, 2007
  - Refinamientos
    - SPA/fwknop (Rash, 2007)
    - Comunicación oculta sobre encabezados (Kundur, 2003; Bo, 2007)
  - Web knocking (Lebelt, 2005; Bello, 2008; Briganti, 2012)

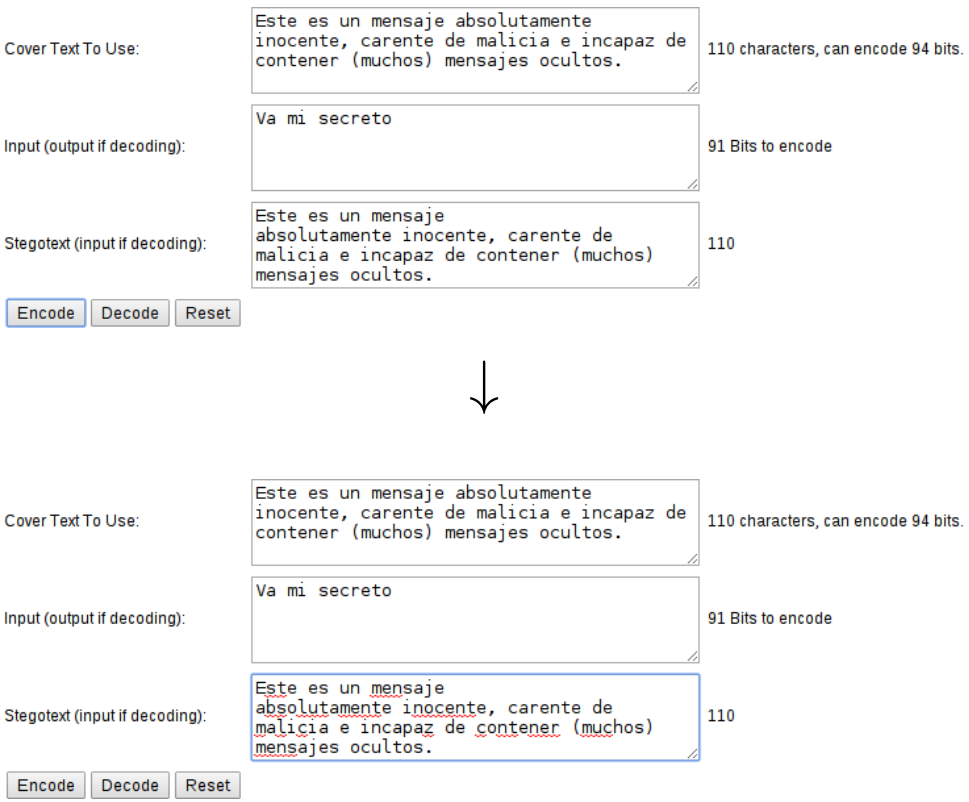
Ocultamiento esteganográfico

¿Por qué *esteganografía*?

Esteganografía sobre *objetos binarios* vs. *texto*

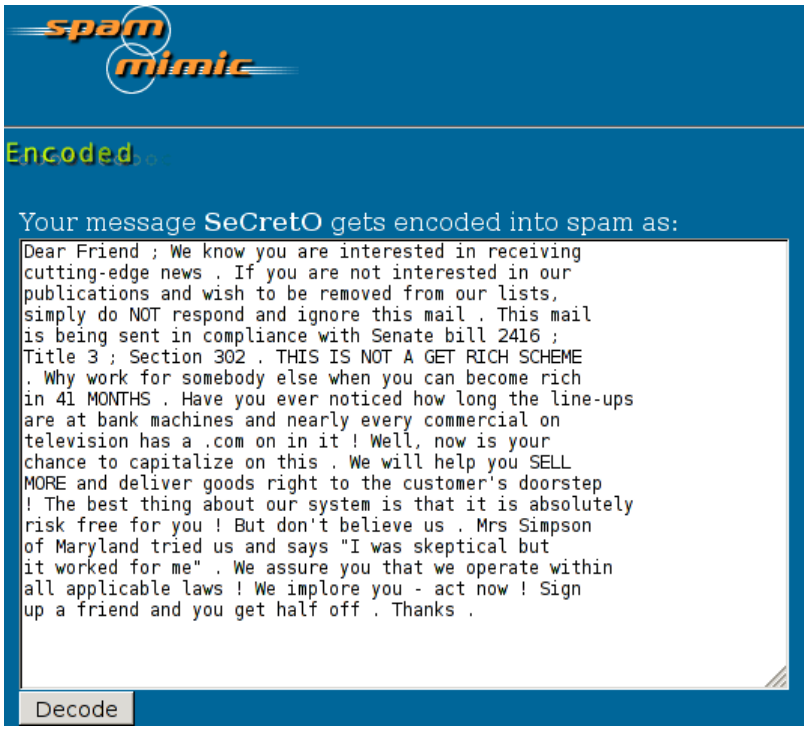
Invisibilidad vs. indetectabilidad

¿De *quién* se oculta la comunicación?



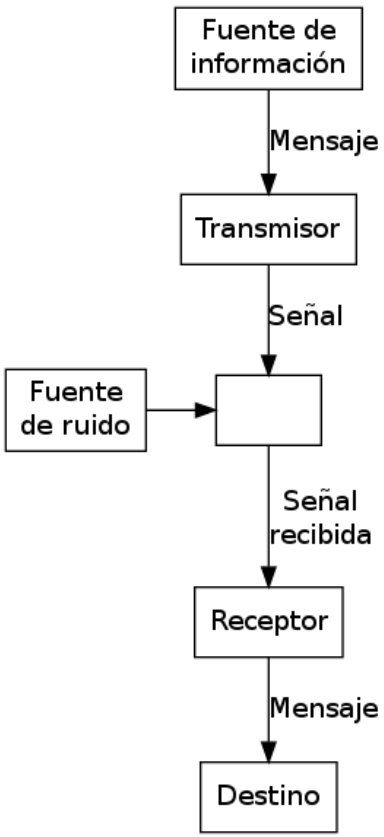
Esteganografía por homoglifos: *Invisible*, pero *trivialmente detectable* (Crenshaw, 2012)

Funciones mímica

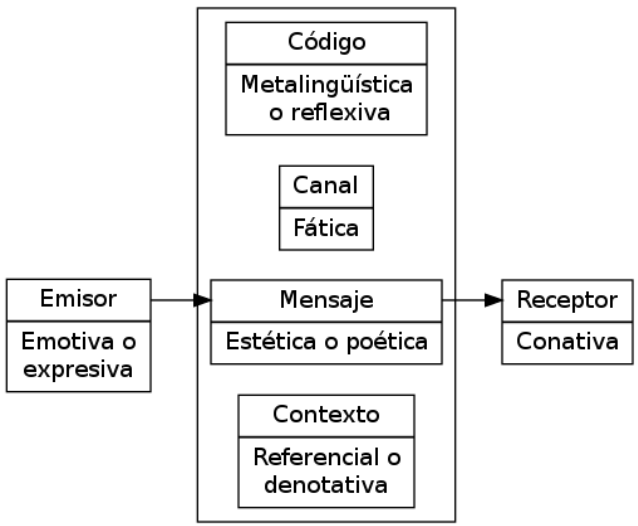


SpamMimic (McKellar 2000-2014), basado en las ideas presentadas por Wayner (1991; 1999; 2009)

Sistema de comunicaciones



Sistema de comunicaciones (Shannon, 1948)



Factores fundamentales de la comunicación (Hébert, 2011)

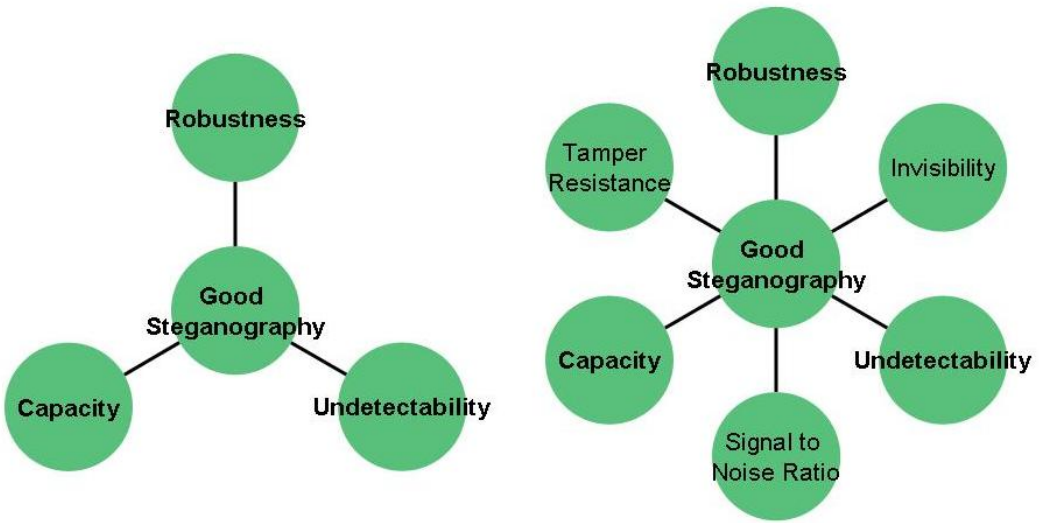
Ocultamiento de información, canales subliminales: ¿Por qué canal oculto?

- Estudio de *canales ocultos* desde $\approx$ 1970s (Lampson, 1973)
- Enfoque mayormente *adversarial*
  - *Sistemas en los que el acceso directo está prohibido por política* (Cabuk, 2006)
- Imposibilidad de aislar y evitar *por completo* los canales ocultos (Handel, 1996)
- Canales subliminales: Definición rígida (Simmons, 1983 y 1985): Mensaje escondido en la firma de un mensaje cubierta enviado en claro.

¿Qué constituye *violación administrativa*?
¿Y qué *acceso legítimo*?

Capacidad del canal

- Restricción de espacio de comunicación por la naturaleza oculta
- Clasificación de canales (Wang, 2005)
  - Canal (espacial/temporal) basado en (valores/transiciones)
- Ocultamiento máximo: Entropía disponible en el canal



Atributos / tensiones de la *buena esteganografía* (Codr, 2009)

Autenticación

Contraseñas más frecuentemente utilizadas (Burnett, 2011). El esquema usuario/contraseña se tiene como débil ya desde (Morris y Thompson, 1979)

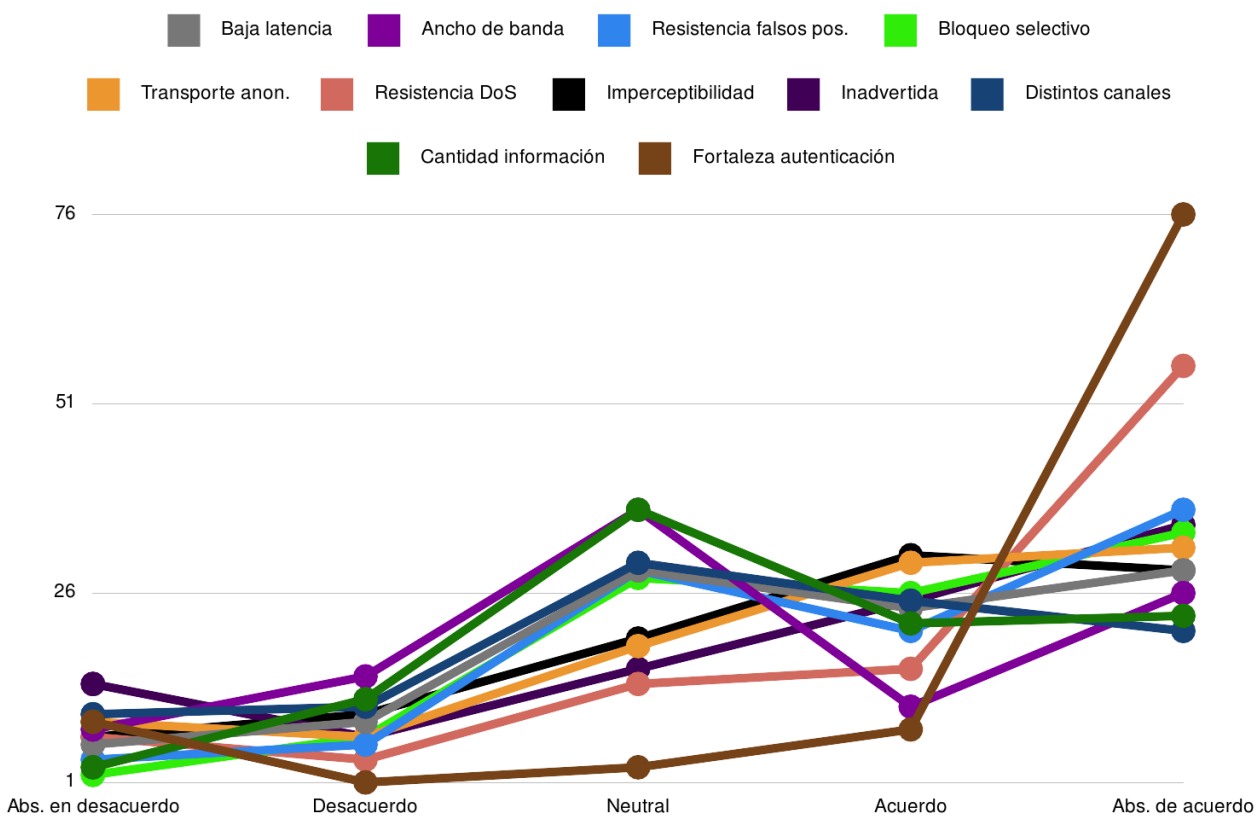
- Fortaleza de la autenticación
  - Espacio de entropía → mínimo absoluto, 72 bits (Smart, 2012)
- Enfrentando los ataques de reproducción
  - *Sal* (Morris y Thompson, 1979), *Nonces* (Rogaway, 2004)

Aplicación de encuesta

- *Encuesta sobre las necesidades para la implementación de un canal oculto*
  - Participación abierta, anónima
  - Busca validar ante un grupo de expertos las hipótesis presentadas
- Aplicada a:
  - Administradores de sistemas (UNAM, Chile)
  - Activistas de privacidad y anonimato
  - Usuarios de Debian hispanoparlantes
  - Círculo social del autor
- 97 respuestas completas contabilizadas

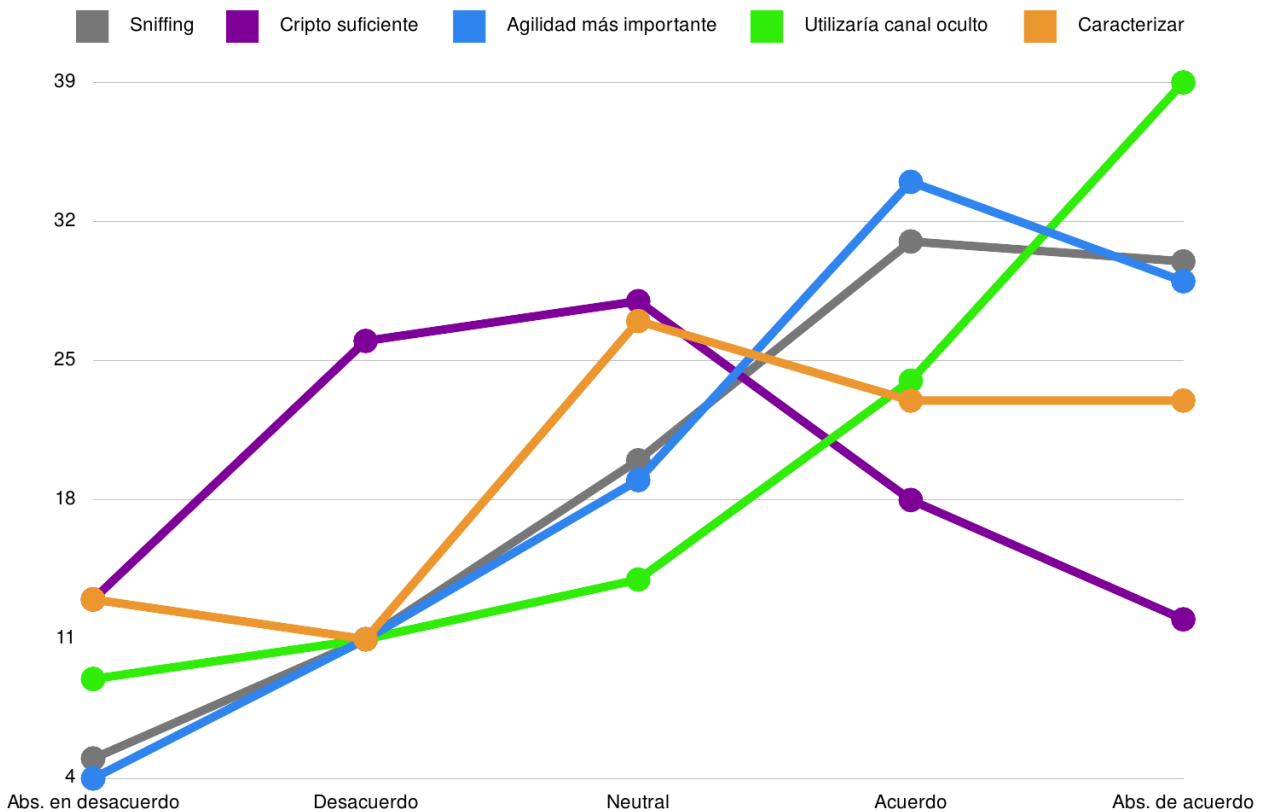
Requisitos para la comunicación

¿Qué tan importante le parece cada uno de los siguientes aspectos para la creación de un canal seguro?



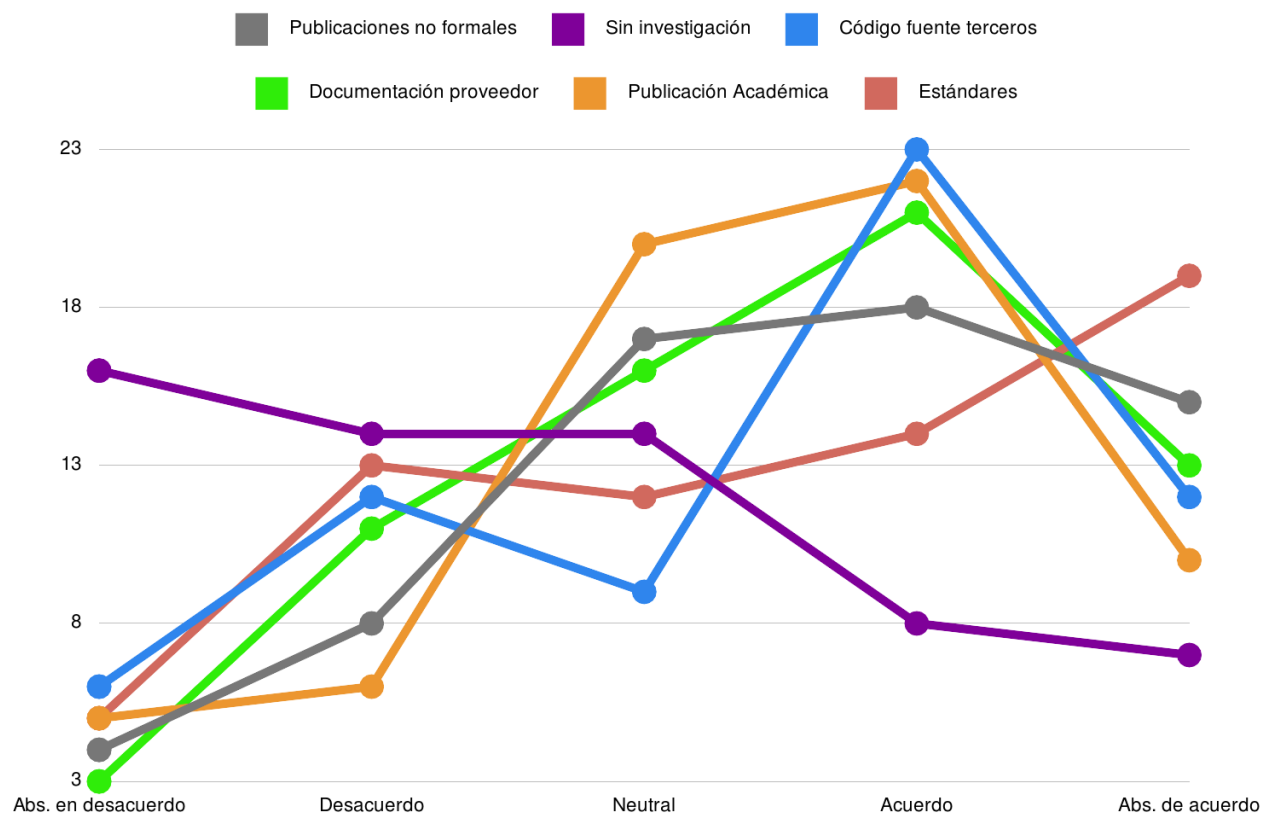
Relevancia del trabajo

¿Qué tan de acuerdo está con las siguientes afirmaciones, en el contexto de la utilidad para la realización de su trabajo diario u otras actividades cotidianas?



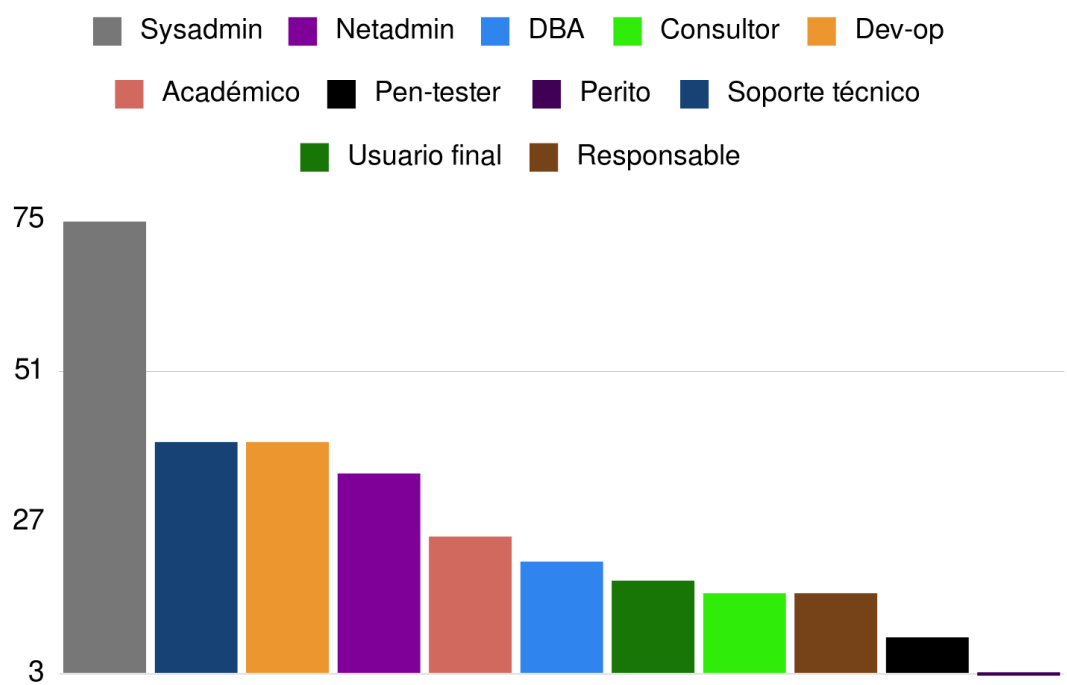
Fuentes de información

Al desarrollar o implementar una solución relativa a seguridad informática (...) ¿Qué tan frecuente es que consulte los siguientes tipos de documentos?



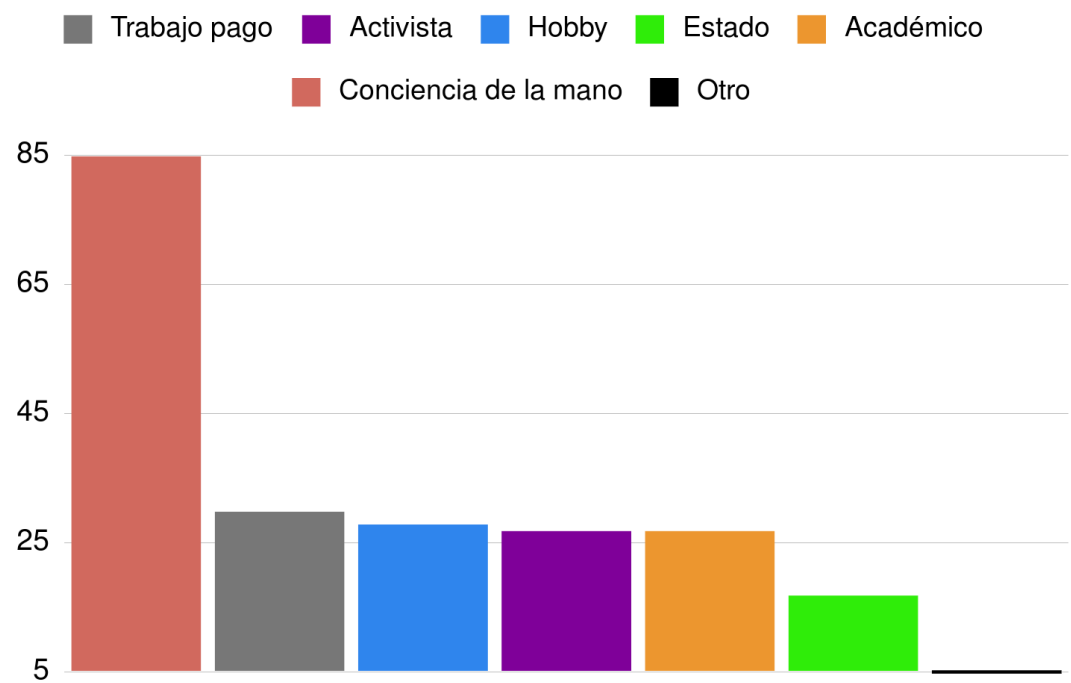
Datos demográficos

¿Cuál o cuáles de las siguientes opciones describen mejor su área de especialización laboral?



Identificación personal

Indique si siente pertenencia con alguno (o varios) de los grupos presentados a continuación, o a alguno no contemplado.



1. Naturaleza del canal

- Canal visible (Nominativo)
- Técnica de ocultamiento (N)
  - Fortaleza del ocultamiento (Discretizado)
  - Vector para el ocultamiento (N)
- Mecanismo de corrección de errores (D)
  - Resistencia al ruido (D)
- Dúplex (D)
- Longevidad (N)
- Capacidad (D)

2. Establecimiento y codificación

- Inicialización (D)
  - Acuse de establecimiento (D)
  - Autenticación (D)
- Codificación y envío de datos (N)
- Costo computacional (D)

3. Reconocimiento y decodificación

- Identificación de mensaje oculto (D)
  - Evento disparador (D)
  - Autenticación (D)
- Decodificación del mensaje (N)
  - Codificación de respuestas (N)
- Costo computacional (D)

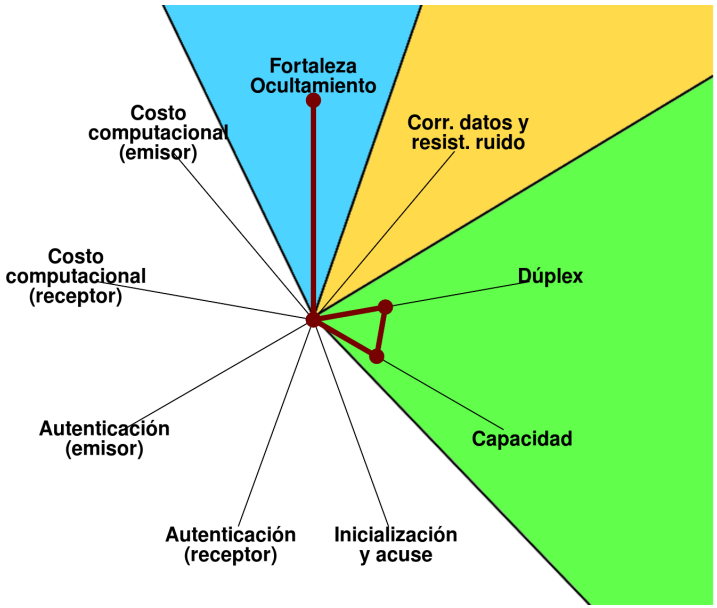
El problema del confinamiento

Given a procedure open (file, error) which does **goto** error if the file is already open, the following procedures will perform this simulation:

procedure *settrue* (file); **begin** loop 1: open (file, loop 1) **end**;
procedure *setfalse* (file); **begin** close (file) **end**;
Boolean procedure *value* (file); **begin** *value* := **true**;
open (file, loop 2); *value* := **false**; close (file); loop 2: **end**

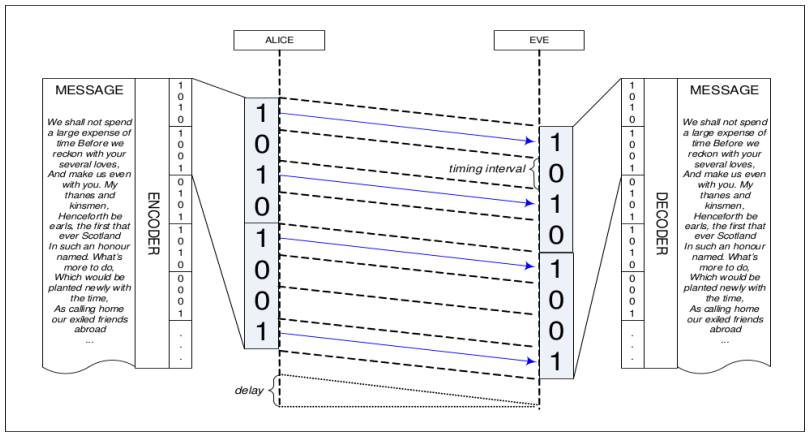
Using these procedures and three files called data, sendclock, and receiveclock, a service can send a stream of bits to another concurrently running program. Referencing the files as though they were variables of this rather odd kind, then, we can describe the sequence of events for transmitting a single bit:

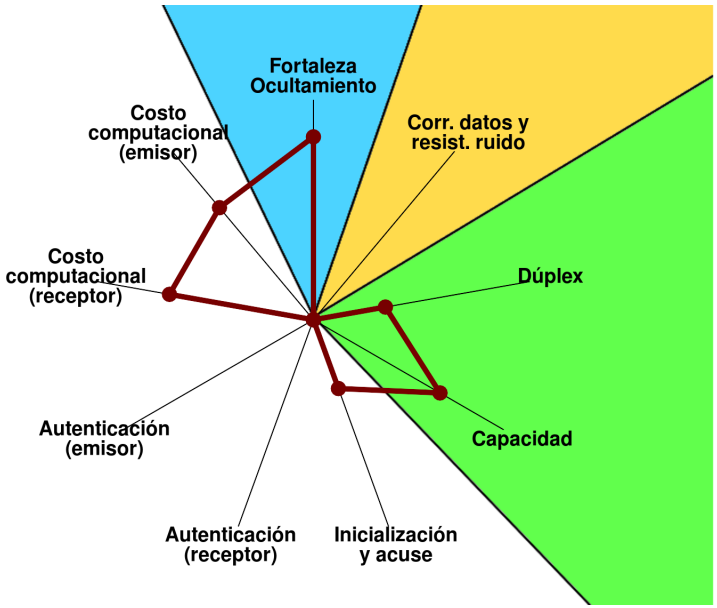
sender: data := bit being sent; sendclock := **true**
receiver: wait for sendclock = **true**; received bit := data;
receive clock := **true**;
sender: wait for receive clock = **true**; sendclock := **false**;
receiver: wait for sendclock = **false**; receiveclock := **false**;
sender: wait for receiveclock = **false**;



Canal visible	Técnica ocultamiento	Vector ocultamiento	Longitud	Codificación y envío	Decodificación y respuesta
Bloqueos en acceso a archivos en el sistema operativo	Canal espacial basado en transiciones	Conativo	Sesión	Señalizado por acceso a tres archivos con bloqueo exclusivo	Señalizado por acceso a tres archivos

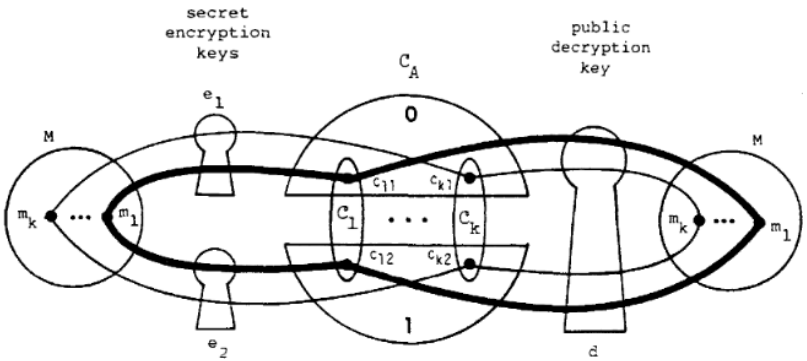
COS sobre IP por almacenamiento

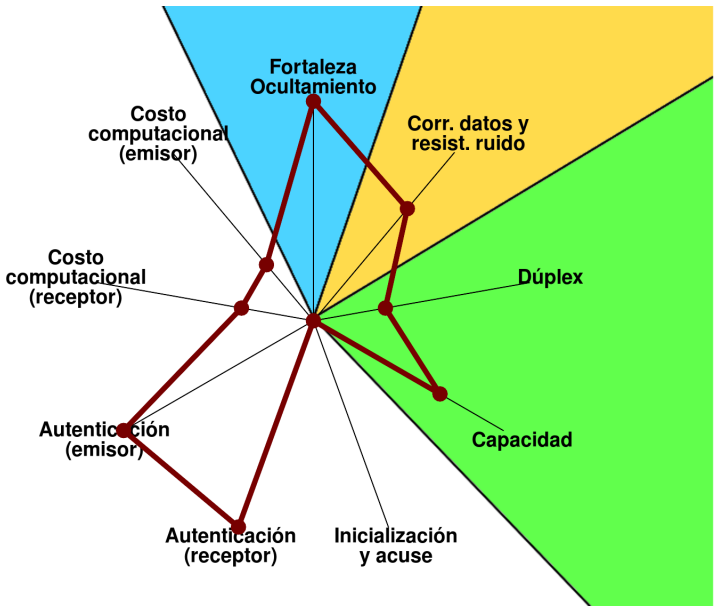




Canal visible	Técnica ocultamiento	Vector oculta-miento	Longitud	Codificación y envío	Decodificación y respuesta
Conexiones IP arbitrarias entre los participantes	Canal temporal basado en valores	Estética	Sesión	Mensaje paquetizado, codificado con el algoritmo elegido, enviando (1) o no (0) mensajes en el tiempo τ establecido	Recibir un número dado de paquetes, verificar integridad. Se entrega a capa superior.

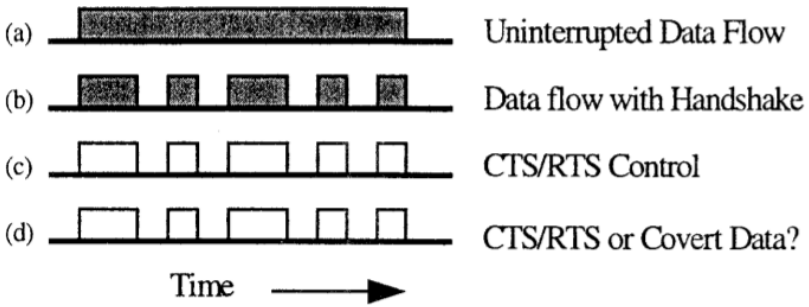
El canal subliminal y las firmas digitales

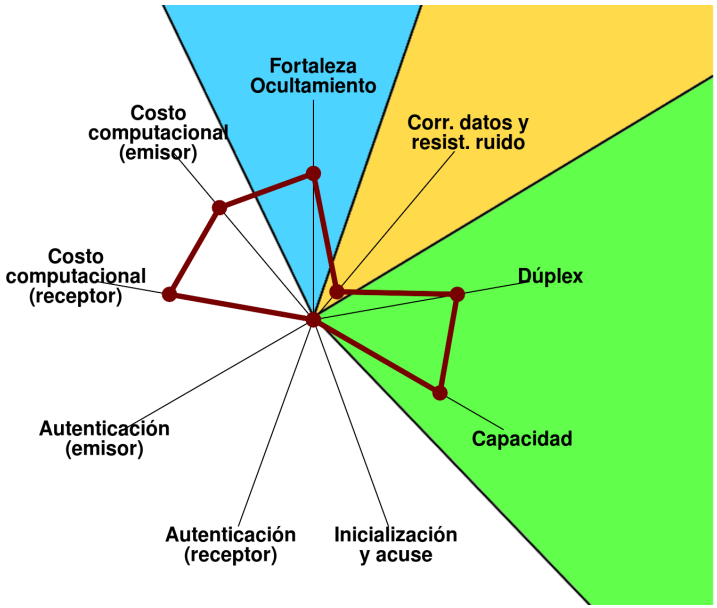




Canal visible	Técnica ocultamiento	Vector ocultamiento	Longitud	Codificación y envío	Decodificación y respuesta
Comunicación abierta y firmada (comprobable por terceros)	Esteganografía	Fática	Señalización	El firmado del mensaje se altera entre dos *sub-llaves* relacionadas para señalizar 1 o 0.	Conociendo *u* y con un mensaje recibido, la sub-llave elegida indica un bit.

Capa 1 OSI: Disciplina serial





Canal visible	Técnica ocultamiento	Vector ocultamiento	Longitud	Codificación y envío	Decodificación y respuesta
Canal serial punto a punto	Canal temporal basado en valores	Estética	Sesión	Basado en la modulación de un flujo de datos sobre el tiempo, permitiendo (1) o deteniendo (0) el flujo.	*Receptor* envía datos irrelevantes; el *emisor* los modula con CTS/RTS, a intervalos determinados. Respuesta codificada por el mismo proceso.

Capa 4 OSI: Manipulación del paquete TCP

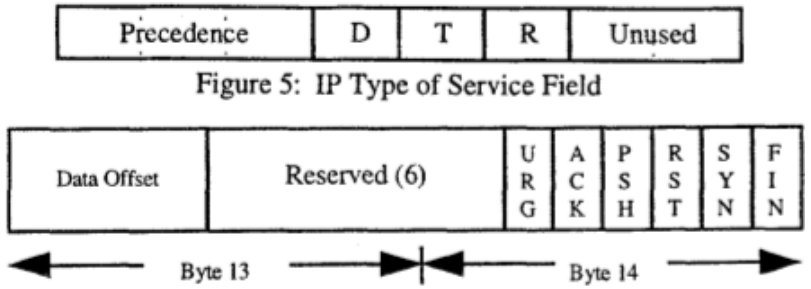
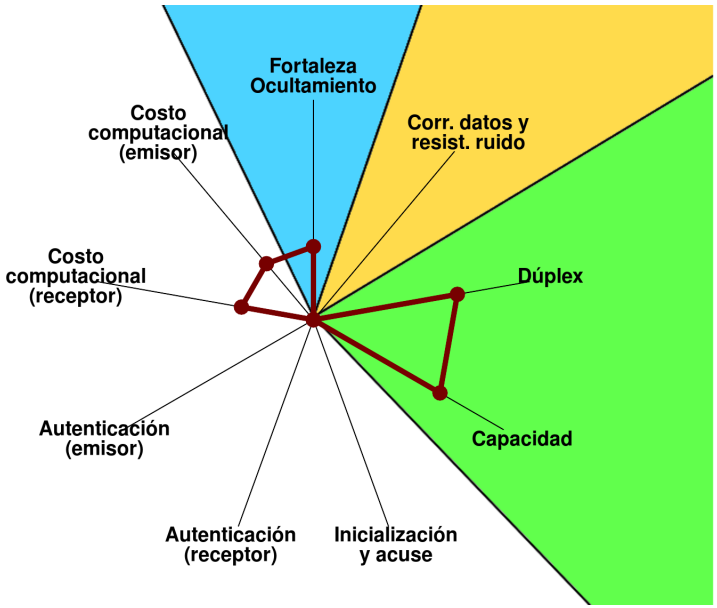


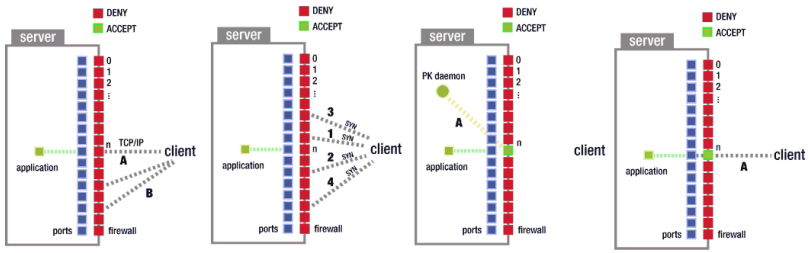
Figure 5: IP Type of Service Field

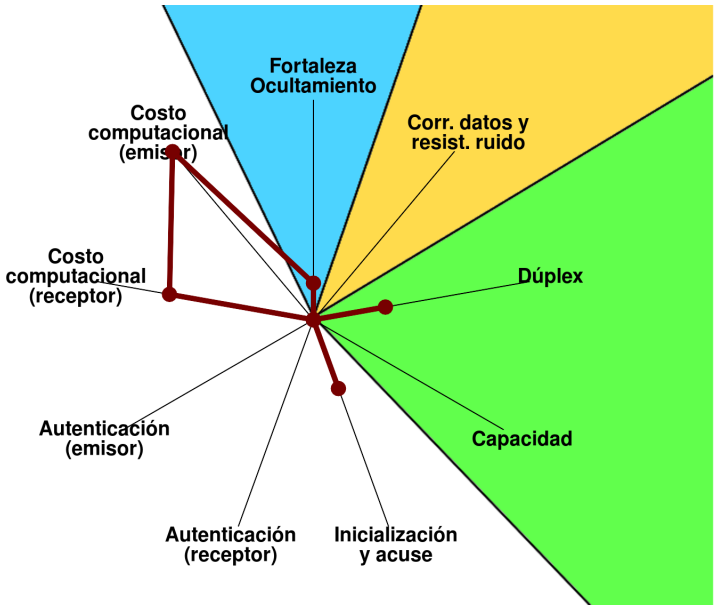
Figure 6: Reserved bytes in TCP Packet Header



Canal visible	Técnica ocultamiento	Vector oculta-miento	Longitud	Codificación y envío	Decodificación y respuesta
Conexión TCP/IP cualquiera	Esteganografía	Fática	Sesión	Cada byte se descompone en sus bits. Dos bits se codifican en el encabezado IP, seis en el TCP. Requiere privilegios de administrador.	Interfaz en modo *promiscuo*; registra paquetes con campos *reservados* en uso. Requiere privilegios de admin. Resp. codif. por el mismo proceso.

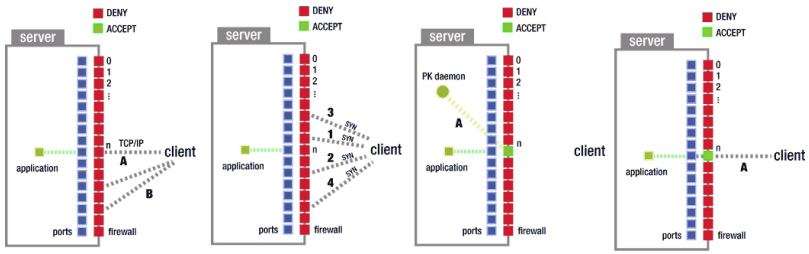
Port knocking: Puerto único, mapeo fijo

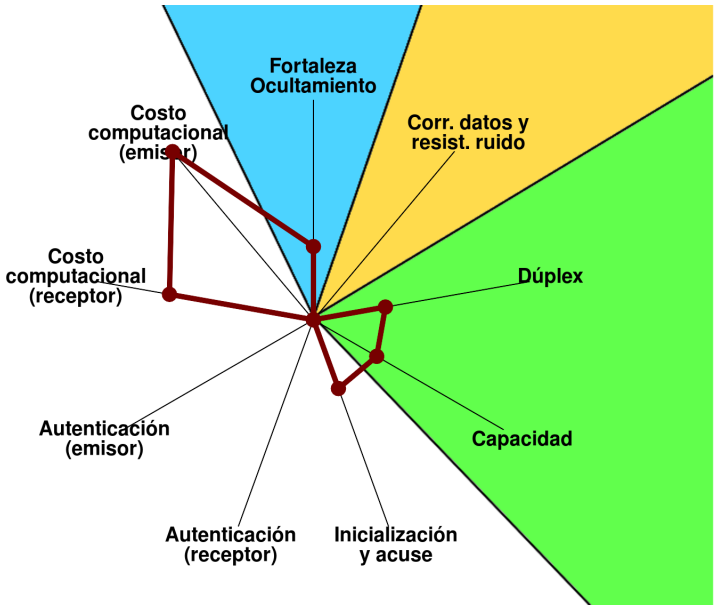




Canal visible	Técnica ocultamiento	Vector ocultamiento	Longitud	Codificación y envío	Decodificación y respuesta
Tráfico normal de red	Esteganografía	Conativa	Señalización	Intentos de conexión (`SYN`) a puertos TCP cerrados en secuencia predeterminada	Identificar la secuencia de paquetes con `SYN` de entre las configuraciones

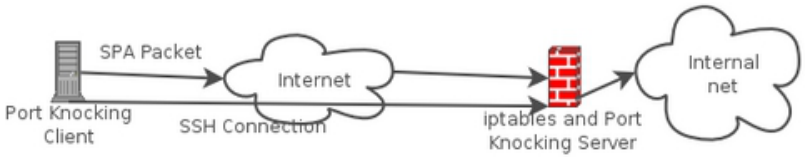
Port knocking: Puertos múltiples, mapeo dinámico

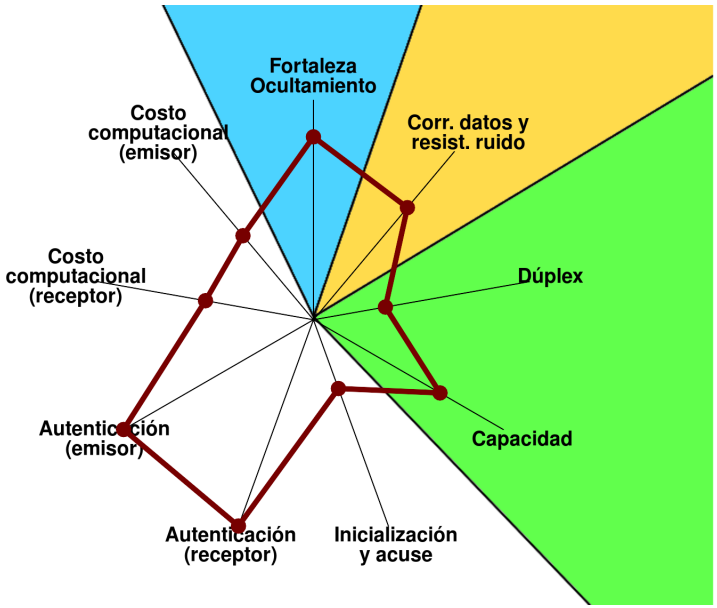




Canal visible	Técnica ocultamiento	Vector ocultamiento	Longitud	Codificación y envío	Decodificación y respuesta
Tráfico normal de red	Esteganografía	Conativa	Señalización	Encabezado fijo, seguido de una serie de *golpes* que codifican acorde a la configuración el puerto a abrir.	Detección de secuencia de paqutes `SYN` (encabezado, puerto, verificación, finalización) en la bitácora del firewall.

Autenticación por un solo paquete: fwknop



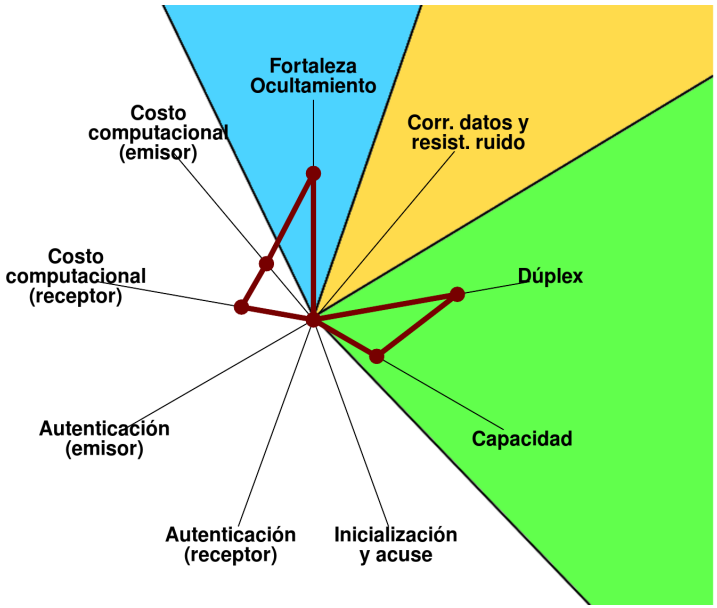


Canal visible	Técnica ocultamiento	Vector ocultamiento	Longitud	Codificación y envío	Decodificación y respuesta
Tráfico normal de red	Esteganografía, criptografía	Referencial	Señalización	Cadena de texto que incluye *token*, nombre de usuario, *timestamp*, acción deseada y otros datos, cifrados y validados por hash.	

Esteganografía práctica en Internet

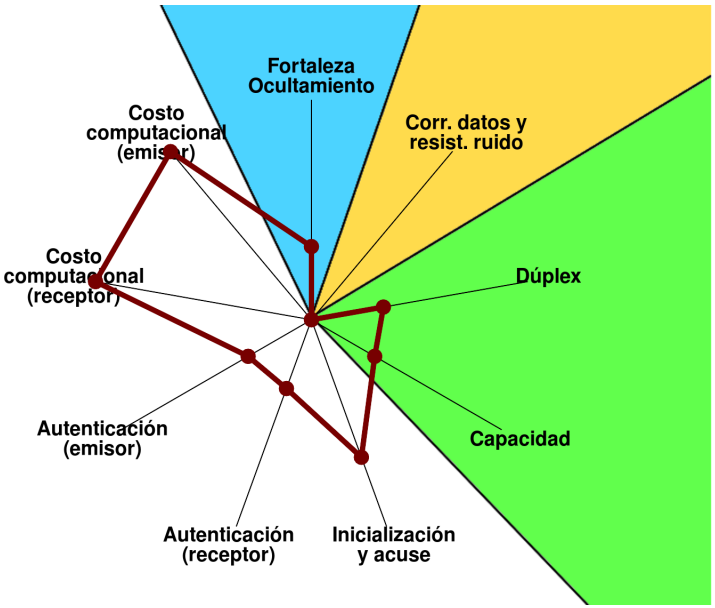
ID field	Flags	Frag.Offset	Total Length
XXX..XX	010	000...0	472

ID field	Flags	Frag.Offset	Total Length
XXX..XX	000	000...0	472



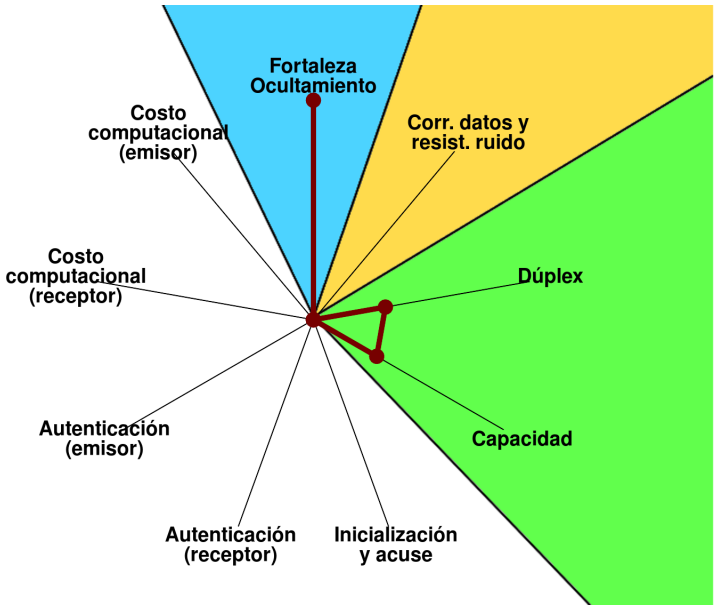
Canal visible	Técnica ocultamiento	Vector oculta-miento	Longitud	Codificación y envío	Decodificación y respuesta
Una conexión TCP/IP cualquiera	Esteganografía	Fática	Sesión	Bits enviados secuencialmente, empleando el campo DNF de TCP en paquetes cortos.	Captura de paqs. en crudo; busca paqs. chicos de la conexión portadora, obtiene bandera DNF de cada uno, arma el mensaje bit a bit.

Webknocking: Golpea diferente



Canal visible	Técnica ocultamiento	Vector oculta-miento	Longitud	Codificación y envío	Decodificación y respuesta
Solicitudes Web (HTTP o HTTPS)	Esteganografía	Conativa	Señalización	No hay envío posterior, la solicitud va codificada en los parámetros `GET` o `POST` de la solicitud a la página *maestra*.	No hay envío posterior, la solicitud se codifica en los parámetros `GET` o `POST` de la solicitud a la página *maestra*.

Escondiendose entre el spam



Canal visible	Técnica ocultamiento	Vector ocultamiento	Longitud	Codificación y envío	Decodificación y respuesta
Correo electrónico no solicitado	Esteganografía (función mímica)	Emotiva, conativa, referencial, fática	Señalización	Separado en bloques, cada uno se pasa por un *parser inverso* que entrega la cadena que representa al árbol de parseo en cuestión.	Mensaje entregado al *parser* bloque a bloque; éste construye un árbol de parseo, obtiene su representación numérica, que es el mensaje oculto.

Comunicación oculta entre servidores HTTP

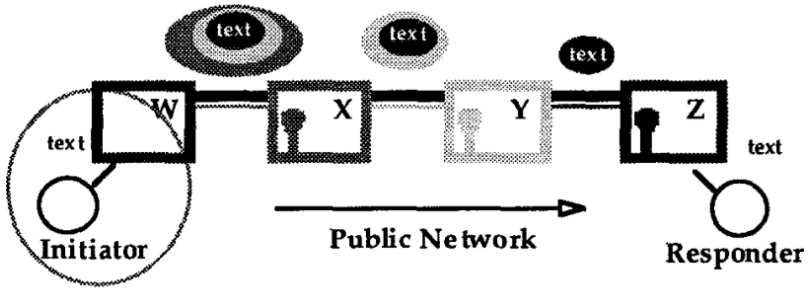


Figure 6: Moving Data Forward

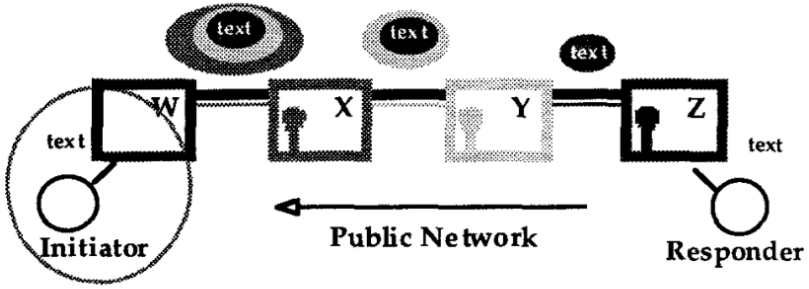
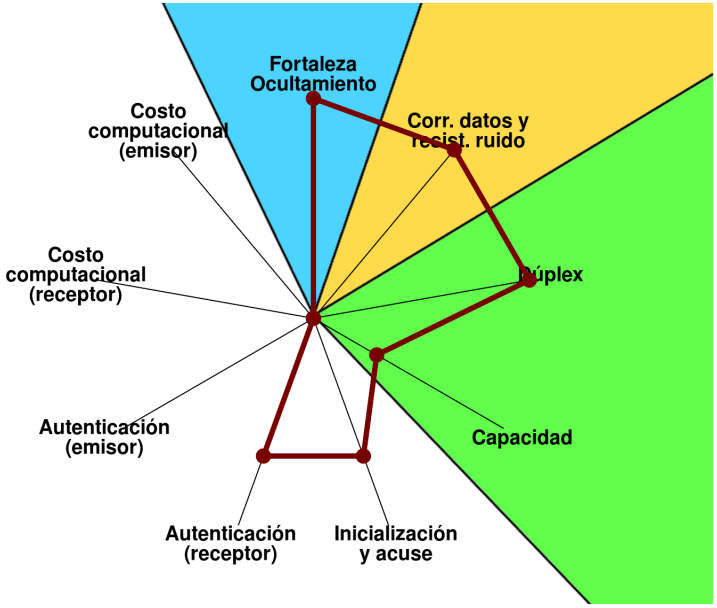
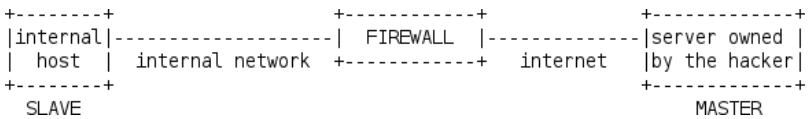


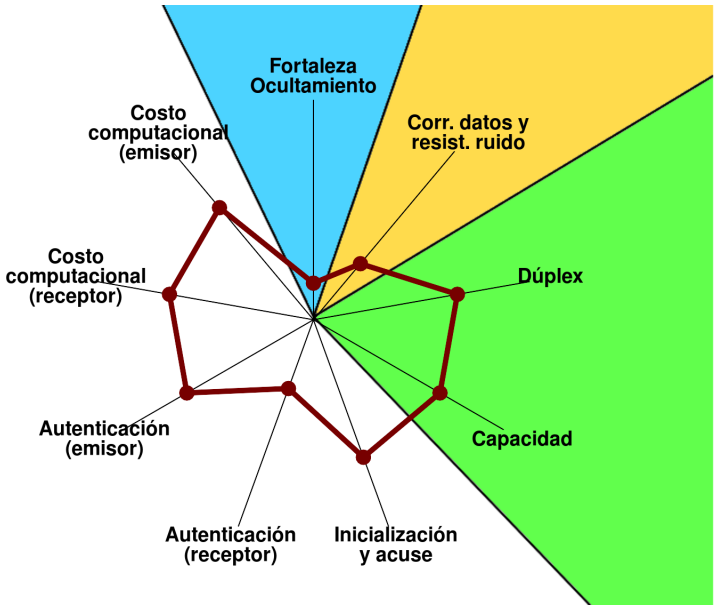
Figure 7: Moving Data Backward



Canal visible	Técnica ocultamiento	Vector ocultamiento	Longitud	Codificación y envío	Decodificación y respuesta
Comunicación estándar HTTP	Esteganografía	Referencial, Señalización conativa		Secuencia aleatoria por mensaje. Ruta entre servidores, sobre parámetros y *cookies* de solic. Web de terceros (clientes).	No especifica mecanismo de decodificación (sólo su espacio). Para la respuesta, emplea el mismo esquema.

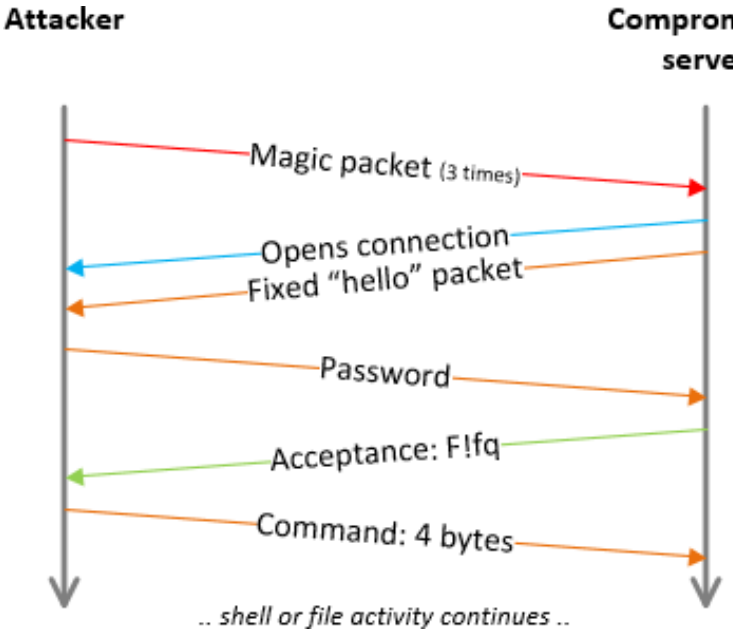
Puertas traseras para atravesar firewalls

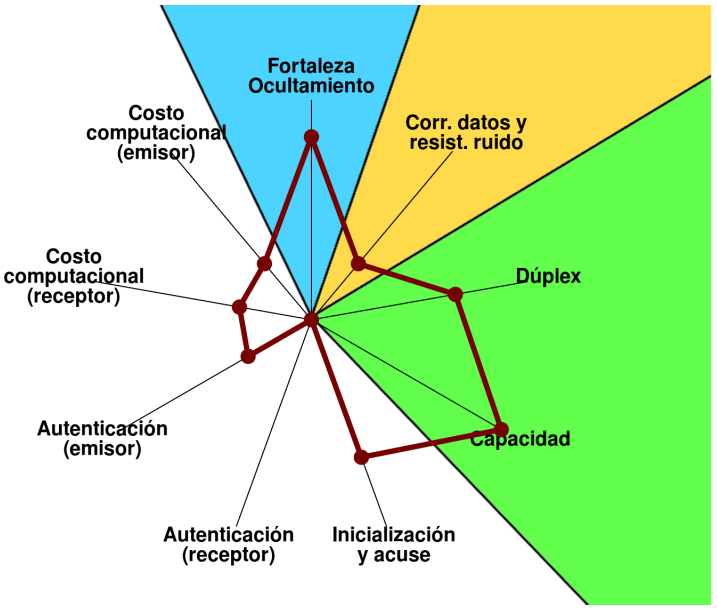




Canal visible	Técnica ocultamiento	Vector oculta-miento	Longitud	Codificación y envío	Decodificación y respuesta
Solicitud sobre conexión HTTP	Esteganografía	Referencial	Señalización	Codificación de la solicitud como Base64, enviado como parámetro HTTP	

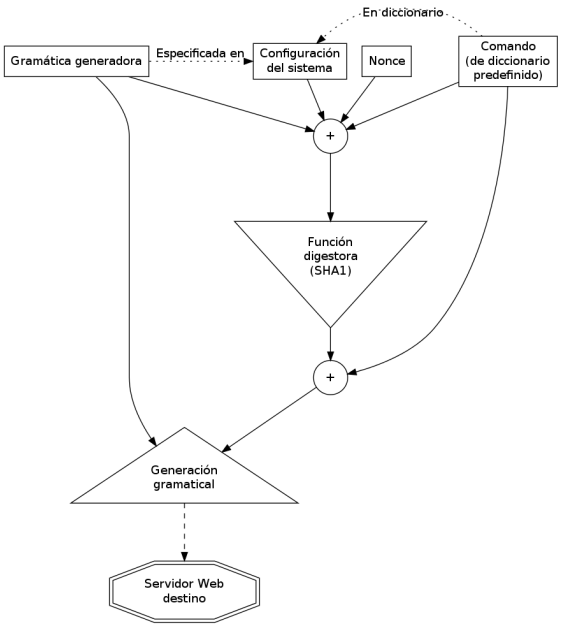
El ataque a Freenode

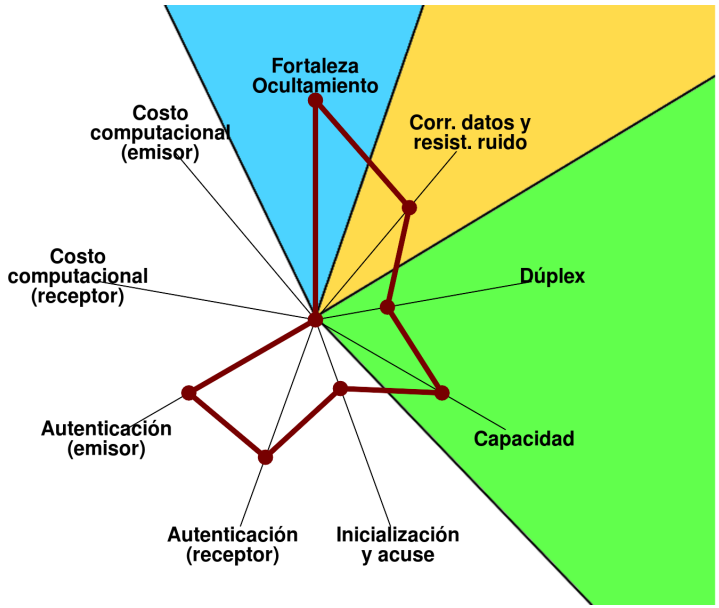




Canal visible	Técnica ocultamiento	Vector ocultamiento	Longitud	Codificación y envío	Decodificación y respuesta
Conexiones TCP/IP estándar	Esteganografía	Conativa, fática	Sesión	Comunicación por llave compartida, RC4. Define varios comandos de 4 bytes preestableciendo acciones a realizar.	Cifrado por MD4.

Implementación propuesta: *HttpSteg*





Canal visible	Técnica ocultamiento	Vector ocultamiento	Longitud	Codificación y envío	Decodificación y respuesta
Solicitudes Web (HTTP o HTTPS)	Esteganografía (función mímica)	Emotiva, fática, conativa, referencial	Señalización	El hash y comando se procesan por un *parser inverso* que entrega la cadena que representa al árbol de parseo.	Mensaje entregado al *parser*, arma un árbol de parseo, obtiene su rep. numérica, que es el msj. oculto.

Conclusiones generales

- El estudio y desarrollo de los canales ocultos amerita mayor atención en la literatura académica
  - Área con muchas implementaciones (formales e informales)
  - Clara justificación, en lo técnico y en lo social
- Se busca hacer las siguientes contribuciones con el modelo:
  - Facilitar a los administradores de sistemas la comparación de implementaciones de canales ocultos
  - Presentar de forma clara y sistematizada los principales puntos a considerar por investigadores y desarrolladores

Trabajo a futuro

- Hay espacio para análisis más profundo y desarrollos derivados
- El tema no es novedoso, pero su *tratamiento* sí — Y cada vez más necesario
- Continuar con la implementación de *HttpSteg*
- Extender al modelo, de meramente descriptivo a indicativo por prioridad de aplicación