فصلنامه علمی-ترویجی پدافند غیرعامل

سال سوم، شماره ۱، بهار ۱۳۹۱، (پیاپی ۹): صص ۳۷-۴۴

کانال‌های پوششی تحت شبکه؛ یکی از راه‌های اصلی نشت اطلاعات

مهدی دهقانی[۱]

محمود صالح اصفهانی[۲]

تاریخ دریافت: ۹۱/۱۲/۱۵

تاریخ پذیرش: ۹۱/۰۲/۲۵

چکیده

کانال پوششی به معنی مبادله اطلاعات در پوشش یک کانال آشکار و مجاز است به نحوی که وجود ارتباط مخفی بماند. کانال‌های پوششی تحت شبکه دارای کاربردهای زیادی برای مقاصد مجاز یا بدخواهانه هستند که محور همه آن‌ها برقراری ارتباط پنهان می‌باشد. کانال‌های پوششی شبکه‌ای به دو دسته کلی انبارشی و زمان‌بندی‌دار تقسیم می‌شوند. کانال‌های پوششی دارای سه معیار ارزیابی ظرفیت، استحکام و نامحسوسی هستند و روش‌های مقابله با آن‌ها شامل حذف کردن، محدود کردن و تشخیص کانال می‌باشد. بهره‌برداری از کانال‌های پوششی، یک راه‌کار مناسب پدافند غیرعامل برای برقراری ارتباطات امن در شبکه محسوب می‌گردد. از سوی دیگر تشخیص و مقابله با کانال‌های پوششی غیرمجاز، برای دفاع از شبکه‌ها ضروری به نظر می‌رسد. در این مقاله، کاربردها و رده‌بندی کانال‌های پوششی تشریح شده و معیارهای ارزیابی و نحوه مقابله با آن‌ها بیان می‌گردد.

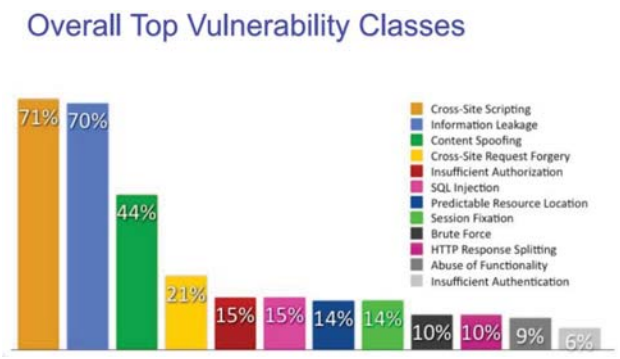
کلیدواژه‌ها: کانال پوششی، نشت اطلاعات، معیارهای ارزیابی، تحلیل ترافیک

۱- دانشجوی دکتری کامپیوتر- گرایش نرم‌افزار- دانشگاه جامع امام حسین(ع) mdehghany@ihu.ac.ir- نویسنده مسئول

۲- استادیار و عضو هیئت علمی دانشکده و پژوهشکده فناوری اطلاعات و ارتباطات - دانشگاه جامع امام حسین(ع) msaleh@ihu.ac.ir

۱- مقدمه

با توسعه شبکه‌های رایانه‌ای گسترده، برقراری و ارتقای سطح امنیت در شبکه‌ها به یک مسئله اساسی تبدیل شده است. یکی از تهدیدهای امنیتی برای شبکه‌های رایانه‌ای، نشت اطلاعات[1] محرمانه یا حساس از طریق شبکه می‌باشد. این تهدید برای سازمان‌ها به دلیل وجود دشمنان و رقبای متعدد از اهمیت حیاتی برخوردار است. آمارها نشان می‌دهد (شکل ۱) که نشت اطلاعات در رتبه‌بندی تهدیدات و حملات، دومین رتبه را به خود اختصاص داده است[۱].



شکل ۱- آمار ۱۰ آسیب‌پذیری بالا در سال ۲۰۱۰ به ترتیب احتمال رخداد

یکی از راه‌های اصلی که عمده نشت اطلاعات سازمان‌ها از طریق آن انجام می‌شود، کانال‌های پوششی می‌باشد. کانال پوششی در واقع یک ارتباط پنهان است که در پوشش یک ارتباط آشکار برقرار می‌گردد و اصل وجود ارتباط و طرفین ارتباط مخفی می‌ماند. کانال‌های پوششی منجر به نشت اطلاعات از یک کاربر با سطح دسترسی بالا به کاربر دیگر شبکه با سطح دسترسی پایین می‌گردند. مطابق معیارهای مرکز ملی امنیت رایانه امریکا[۲]، تحلیل کانال‌های پوششی جزئی از معیارهای ارزیابی برای دسته‌بندی سیستم‌های امن و احراز سطح امنیتی شده است. در این مقاله، تعاریف، کاربردها و کارهای تحقیقاتی انجام شده در زمینه کانال‌های پوششی بررسی می‌گردند و معیارهای ارزیابی و راه‌های مقابله با آن‌ها نیز بیان می‌گردند.

۲- راه‌های نشت اطلاعات

نفوذ فناوری اطلاعات در کلیه عرصه‌ها و بهره‌گیری از رایانه و شبکه‌ها، سازمان‌ها را قادر ساخته تا فرایندهای اطلاعات-محور را توسعه دهند. با رشد اتکاء به اطلاعات و فناوری اطلاعات، نگهداری و حفاظت از داده‌های حساس و محرمانه برای سازمان‌ها از اهمیت بالایی برخوردار شده است. امکان نشت اطلاعات محرمانه در یک سازمان در زمره بالاترین نگرانی‌ها محسوب می‌گردد. نشت اطلاعات محرمانه ممکن است به طرق مختلفی انجام شود. انتشار عمدی و با غرض محتوای حساس یا محرمانه به خارج سازمان را خروج داده‌ها[2] می‌نامند. جیانی و همکارانش یک رده‌بندی[3] برای راه‌های خروج اطلاعات ارائه داده‌اند[۳]. در این رده‌بندی رسانه استفاده شده برای انتقال داده‌ها، دسته‌بندی کلی راه‌های خروج اطلاعات را مشخص می‌کند.

- اگر خروج داده‌ها با انتقال دستگاه‌های فیزیکی حاوی داده‌ها به خارج سازمان باشد، این روش، خروج فیزیکی نام‌گذاری شده است.
- اگر خروج داده‌ها با بهره‌گیری از زیرساخت شبکه رایانه‌ای باشد، این روش، خروج شبکه‌ای نام‌گذاری شده است.
- اگر افراد دارای اطلاعات محرمانه سازمان، به روشی متقاعد یا فریب داده شوند تا آن‌ها را در اختیار مهاجم قرار دهند، به این روش، ادراکی[4] گفته شده است. به این روش، مهندسی اجتماعی[5] نیز گفته می‌شود.

یکی از راه‌هایی که مهاجمین برای خروج داده‌های مورد نظر از شبکه سازمان استفاده می‌نمایند، انتقال اطلاعات در پوشش ارتباطات و ترافیک مجاز است. به این نوع ارتباط، کانال پوششی گویند. مفهوم انتقال نامحسوس اطلاعات و در پوشش یک کانال ارتباطی مجاز، به طور تاریخی وجود داشته است. ظهور شبکه‌های رایانه‌ای با لایه‌ها و پروتکل‌های پیچیده، یک رسانه جدید برای عبور پوششی داده‌ها به‌وجود آورده است. لمپسن در سال ۱۹۷۳ برای اولین بار کانال پوششی در سیستم‌های رایانه‌ای را مطرح کرده است[۴].

۳- تعاریف

برای کانال پوششی تعاریف مختلفی ارائه شده است. لمپسن[۴] کانال پوششی را یک کانال ارتباطی که برای انتقال اطلاعات استفاده می‌شود، ولی به طور کلی نه برای ارسال اطلاعات طراحی شده و نه مقصود آن بوده است، می‌داند. در فرهنگ اصطلاحات وزارت دفاع امریکا[۵]، کانال پوششی یک کانال ارتباطی است که می‌تواند توسط پردازه‌ای برای ارسال اطلاعات استفاده شود به نحوی که از سیاست امنیت سیستم تجاوز نماید. از نظر گلیگور[۶]، کانال پوششی یک کانال ارتباطی انگلی است که به منظور ارسال اطلاعات بدون اجازه یا آگاهی طراح، مالک یا اپراتور کانال، از پهنای باند آن استفاده می‌کند. این تعاریف از این جهت مهم هستند که حقیقت ذاتی و منظور کانال‌های پوششی را آشکار می‌سازند، یعنی عبور از سیاست امنیت سیستم و ارسال اطلاعات بدون آنکه تشخیص داده شود.

1- Information leakage

2- data Exfilteration
3- taxonomy
4- cognitive
5- Social Engineering

۴- تفاوت رمزنگاری و کانال پوششی

تفاوت اصلی بین رمزنگاری و ارتباطات پوششی (شامل پنهان‌نگاری و کانال پوششی) آن است که در رمزنگاری محتوای پیام محافظت می‌شود و برای افراد غیرمجاز، نامفهوم و غیرقابل بازیابی است. در ارتباطات رمزنگاری‌شده، حقیقت این است که ارتباط برقرار است و هویت مبدأ و مقصد مخفی نگه‌داشته نمی‌شود؛ ولی در ارتباطات پوششی، وجود ارتباط و هویت طرف‌های ارتباط مخفی نگه‌داشته می‌شود. اطلاعات پوششی با استفاده از روش‌هایی، در رسانه و ارتباط عادی و مجاز به نحوی مخفی‌سازی می‌شوند که تا حد زیادی غیرقابل تشخیص باشند. در پنهان‌نگاری، اطلاعات پوششی در محتوای صوتی، تصویری یا متنی مخفی‌سازی می‌شود، ولی در کانال‌های پوششی از پروتکل‌های شبکه به‌عنوان حامل اطلاعات پوششی استفاده می‌گردد.

۵- کاربردهای کانال پوششی

بسیاری از گروه‌ها و افراد برای مخفی نگه‌داشتن ارتباطات خود انگیزه دارند[۷]. مجرمان، نفوذگران، جاسوسان امنیتی و صنعتی، کاربران معارض دولت‌ها و سازمان‌ها و مدیران شبکه ممکن است در جستجوی کانال‌های پوششی باشند. این‌ها ممکن است به منظورهای زیر از کانال پوششی استفاده کنند:

- *گردآوری و خروج داده‌های حساس یا محرمانه از شبکه‌های امن*: در این موارد معمولاً با نصب اسب تروا[1] روی سیستم تسخیر شده، انتقال اطلاعات از طریق کانال پوششی و دور از چشم مدیران شبکه انجام می‌گردد.
- *نصب، گسترش یا کنترل بدافزار روی سیستم‌های تسخیر شده*: بدافزارهای شبکه‌ای مثل شبکه‌های بات[2] برای ارسال دستورات و مبادله اطلاعات بین فرماندهی و عناصر شبکه از کانال‌های پوششی استفاده می‌کنند تا شناسایی نشوند.
- *امن‌سازی ارتباطات مربوط به مدیریت شبکه*: مدیران شبکه برای مخفی نگه‌داشتن ارتباطات لازم برای مدیریت شبکه از چشم نفوذگران، می‌توانند از کانال‌های پوششی استفاده کنند. احراز هویت در شبکه نیز یکی از این مصادیق است. سیستم‌های کوزه عسل[3] که در واقع سیستم‌های رایانه‌ای تله شده برای نفوذگران هستند نیز می‌توانند از کانال‌های پوششی، پنهان از دید نفوذگران برای ارسال به‌موقع داده‌های ثبت وقایع استفاده کنند.
- *عبور از دیوار آتش برای دستیابی نامحدود به اینترنت*: سازمان‌ها و شرکت‌ها ممکن است دسترسی کارکنانشان به منابع اینترنت را محدود سازند. برای عبور از این محدودیت از کانال پوششی استفاده می‌شود.
- *امن‌سازی ارتباطات*: در کشورهایی که رمزنگاری قوی داده‌ها ممنوع است، از کانال پوششی برای امن‌سازی ارتباطات استفاده می‌شود. این کار در واقع مخفی‌سازی ارتباط است و یک امنیت قوی در مقایسه با رمزنگاری به حساب نمی‌آید.
- *مبادله کلید رمزنگاری*: برای برقراری ارتباط به صورت رمز، باید کلیدهای رمزنگاری که ممکن است متقارن یا نامتقارن باشند از طریق یک کانال امن غیر از کانال ارتباطی مورد نظر انجام شود. کانال پوششی می‌تواند به عنوان یک کانال امن برای مبادله کلید رمزنگاری استفاده شود.
- *حفاظت از حقوق معنوی*: مبادله اطلاعات حساس محصولات صوتی و تصویری همانند شماره سریال می‌تواند با روش‌های کانال پوششی انجام شود[۸].
- *تعقیب ترافیک خاص*: با استفاده از روش‌های کانال پوششی، نشان‌گذاری[4] روی جریان‌های ترافیک شبکه پیاده‌سازی شده و آن‌ها را از همدیگر متمایز می‌نمایند. بدین ترتیب امکان تعقیب ترافیک خاص در شبکه‌های گمنامی و یافتن مهاجم یا مجرم فراهم می‌گردد[۹].

برقراری و استفاده از کانال‌های پوششی، یک راه‌کار مناسب پدافند غیرعامل برای ایجاد ارتباطات امن در شبکه محسوب می‌گردد. از سوی دیگر، تشخیص و مقابله با کانال‌های پوششی غیرمجاز، برای دفاع از شبکه‌ها ضروری به نظر می‌رسد. این کاربردها، مطالعه کانال‌های پوششی در شبکه را جذاب نموده است.

۶- رده‌بندی کانال پوششی

برای کانال‌های پوششی با توجه به فنون بکار رفته در هر کدام، دسته بندی‌های مختلفی ارائه شده است. جدیدترین رده‌بندی که به نظر می‌رسد رده‌بندی دقیق‌تری باشد توسط زندر ارائه شده است[۱۰]. زندر معیارهای رده‌بندی کانال‌های پوششی را به صورت زیر در نظر گرفته است:

کانال‌های انبارشی[5] *و کانال‌های زمان‌بندی‌دار*[6]: در دسته‌بندی اولیه، کانال‌های پوششی به کانال‌های انبارشی و زمان‌بندی‌دار تقسیم شده‌اند. کانال‌های انبارشی، اطلاعات پوششی را در فیلدهای رزرو یا فیلدهای استفاده نشده یا در فیلدهایی که امکان استفاده از آن‌ها بدون تأثیر در عملکرد پروتکل وجود دارد، ذخیره می‌شوند. فرستنده، داده‌های مورد نظر را در این فیلدها می‌نویسد و گیرنده، آن‌ها را از این فیلدها می‌خواند. در کانال‌های زمان‌بندی‌دار، فرستنده اطلاعات

1- trojan Horse
2- botnets
3- honeypot

4- watermarking
5- covert Storage Channel
6- covert Timing Channel

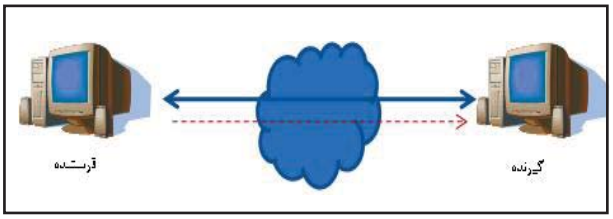
پوششی را روی زمان‌بندی ارسال بسته‌ها سوار می‌کند؛ یعنی زمان‌بندی ارسال بسته‌ها را به نحوی دستکاری می‌کند که حامل اطلاعات مورد نظر باشد. گیرنده از این نحوه دستکاری یا به بیان دیگر کدگذاری اطلاعات آگاه است و می‌تواند اطلاعات را کدگشایی کند.

انواع پوشش؛ قابل پیش‌بینی[1]*، متغیر*[2] *و تصادفی*: پوشش در واقع مشخصه ترافیک آشکار است که داده پوششی در آن کدگذاری می‌شود. پوشش قابل پیش‌بینی به معنی آن است که اساساً هیچ تغییری در پوشش داده نمی‌شود. پوشش متغیر به معنی آن است که تغییرات محدودی وجود دارد. پوشش تصادفی نیز به معنی آن است که داده پوششی شبه تصادفی است.

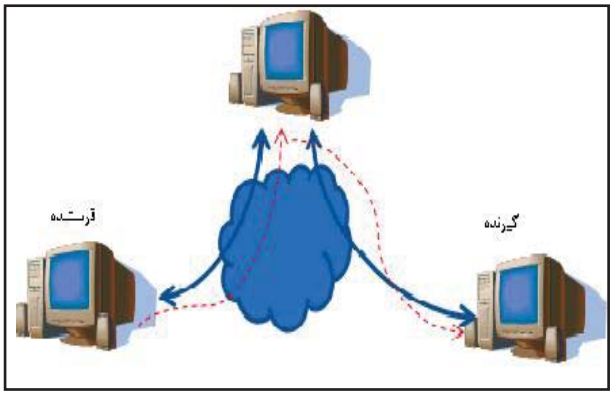
کانال نویزدار و کانال عاری از نویز: در کانال نویزدار خطای کانال وجود دارد. در حالی که در کانال عاری از نویز، هیچ خطای کانالی وجود ندارد. خطاهای احتمالی در کانال نویزدار عبارت‌اند از: جایگشت[3] به معنی جابجایی بیت‌ها با مکان ناشناخته، پاک شدگی[4] به معنی جابجایی بیت‌ها با مکان شناخته شده، حذف به معنی مفقود شدن کامل بیت‌ها و درج بیت‌ها.

کانال‌های منفعل[5]*، نیمه‌منفعل و فعال*: در کانال منفعل، فرستنده از ترافیک موجود کاربران ناآگاه به عنوان پوشش استفاده می‌کند. در کانال‌های نیمه‌منفعل، فرستنده ترافیک آشکار را به‌وسیله نرم‌افزارهای کاربردی واقعی تولید می‌کند و کنترل محدودی روی ترافیک آشکار (پوششی) دارد. در کانال‌های فعال، فرستنده خودش ترافیک آشکار را تولید و ارسال می‌کند. بنابراین روی ترافیک کنترل کامل دارد.

کانال مستقیم و کانال غیرمستقیم: در کانال‌های مستقیم، ترافیک آشکار که حاوی داده‌های پوششی است مستقیماً بین فرستنده و گیرنده پوششی جریان می‌یابد(شکل۲). در کانال‌های غیرمستقیم، دو جریان ترافیک آشکار که داده‌های پوششی را حمل می‌کنند وجود دارد. اولی بین فرستنده و یک میزبان ناآگاه میانی و دومی بین میزبان میانی و گیرنده برقرار است (شکل ۳).



شکل ۲- کانال پوششی مستقیم



شکل ۳- کانال پوششی غیرمستقیم

۶-۱- کانال‌های انبارشی عاری از نویز مستقیم

اغلب کانال‌های پوششی موجود، در این دسته قرار دارند. زیرا امکان وجود این کانال‌ها زیاد است. در این کانال‌ها، داده‌های پوششی در فیلدها جاسازی می‌شوند و یا در فرایند عملکرد پروتکل کدگذاری می‌شوند یا از ابهام معنایی موجود در پروتکل‌ها بهره‌برداری می‌نمایند. اگرچه پیاده‌سازی این کانال‌ها ساده است و به دلیل فقدان نویز، کاراً هستند، ولی رفتار ناهنجارشان به سادگی قابل تشخیص است و با تنظیمات بهینه‌سازی[6] پروتکل، این کانال‌ها حذف می‌شوند. به‌طور اجمال، چند روش ذخیره‌سازی داده‌های پوششی در این کانال‌ها به شرح زیر می‌باشد:

- ذخیره‌سازی در فیلدهای رزرو یا استفاده نشده در سرآیند فریم یا بسته در پروتکل‌های IP و TCP
- ذخیره‌سازی در بخش گسترش[7] سرآیند پروتکل‌های IPV6
- ذخیره‌سازی در بخش لایه‌گذاری[8] فریم یا بسته در پروتکل‌های IP و TCP
- ذخیره‌سازی یا سوارکردن اطلاعات روی فیلد مهرزمانی[9]
- سوار کردن اطلاعات روی فیلدهای آدرس در لایه پیوند داده‌ها و لایه IP
- ذخیره اطلاعات در فیلد طول فریم‌های لایه پیوند داده‌ها
- استفاده از فیلد مجموع مقابله‌ای[10] برای انتقال پیام در سرآیند IP یا در بسته‌های UDP
- ارسال فریم‌ها یا بسته‌های به ظاهر خراب در شبکه‌های بی‌سیم که در واقع حاوی داده‌های پوششی هستند ولی مجموع مقابله‌ای آن‌ها به غلط تنظیم شده است.

1- predictable
2- variable
3- substitution
4- erasures
5- passive

6- normalisation
7- header extensions
8- padding
9- timestamp
10- checksum

- تونل‌سازی[1] با پروتکل‌هایی که معمولاً مسدود نمی‌شوند مثل HTTP یا DNS و قرار دادن بسته‌های IP حاوی داده های پوششی در آن‌ها
- ذخیره‌سازی داده‌ها در فیلدهای Fragment offset
- استفاده از فیلد شماره توالی اولیه در پروتکل TCP
- ذخیره‌سازی داده‌ها در فیلد MAC در پروتکل SSH

و بسیاری روش‌های مشابه که ذکر آن‌ها از حوصله این مقاله خارج است.

۶-۲- کانال‌های انبارشی دارای نویز مستقیم

کانال‌های انبارشی دارای نویز به همان روش مشابه کانال‌های عاری از نویز از فیلدهای مشخص یا ابهامات معنایی استفاده می‌کنند. اما فیلدهای داده که به عنوان پوشش استفاده می‌شوند در مسیر بین فرستنده و گیرنده در معرض تغییرات هستند. این تغییرات ممکن است خطاهای روی کانال باشد که به عنوان نویز شناخته می‌شود. نویز ظرفیت را کاهش می‌دهد، اما به طور بالقوه نامحسوسی را بهبود می‌بخشد. در مقایسه با کانال‌های انبارشی عاری از نویز مستقیم، تعداد کمی کانال انبارشی دارای نویز وجود دارد.

در این دسته کانال‌ها، چند کار با استفاده از فیلد TTL در سرآیند Ipv4 و فیلد مشابه آن، فیلد HopLimit در Ipv6 انجام شده است. چون فیلدهای مذکور توسط گره‌های شبکه در مسیر بین فرستنده و گیرنده تغییر می‌یابند و بسته‌ها نیز می‌توانند از مسیرهای مختلف در شبکه عبور کنند، این کانال دارای نویز است.

۶-۳- کانال‌های انبارشی غیرمستقیم

کانال‌های انبارشی غیرمستقیم، فرستنده و گیرنده را قادر می‌سازند تا داده‌های پوششی کدگذاری شده در فیلدهای پروتکل را از طریق گره میانی ناآگاه مبادله نمایند. این امر، نامحسوسی را افزایش می‌دهد؛ زیرا یک نگهبان، جریان مستقیم اطلاعات بین فرستنده و گیرنده را نمی‌بیند. ولی پیاده‌سازی کانال‌های غیرمستقیم سخت‌تر است و ظرفیت کمتری نسبت به کانال‌های مستقیم دارند.

چند نمونه کار انجام شده در این دسته بدین شرح است. فرستنده، بسته SYN با آدرس مبدأ جعلی که همان آدرس گیرنده مورد نظر است را با ISN حاوی داده‌های پوششی برای یک میزبان ناآگاه می‌فرستد. میزبان واسط ناآگاه، SYN/ACK یا SYN/RST را با شماره توالی برابر ISN+1 به آدرس گیرنده مورد نظر می‌فرستد. گیرنده مقدار ISN دریافتی را یکی کم کرده و اطلاعات پوششی را به دست می‌آورد. مشابه کار ذکر شده، روی پروتکل ICMP و با بسته های Echo Request و Echo Replies انجام شده که داده‌های پوششی در بار مفید این بسته‌ها حمل می‌شود.

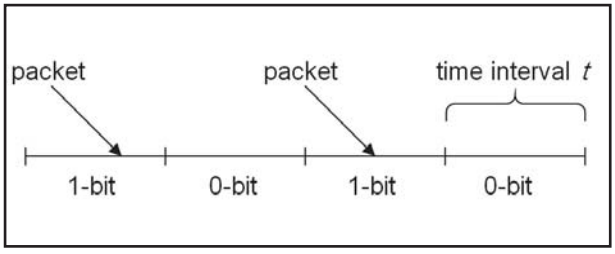
1- tunneling

۶-۴- کانال‌های زمان‌بندی‌دار مستقیم

کانال‌های زمان‌بندی‌دار پوششی کانال‌هایی هستند که داده‌های پوششی را در زمان‌بندی فریم‌ها، بسته‌ها یا پیام‌هایی که مستقیماً بین فرستنده و گیرنده مبادله می‌شوند کدگذاری می‌نمایند. کانال‌های زمان‌بندی‌دار به دلیل عدم دقت زمان‌بندی در فرستنده و گیرنده و لغزش زمانی[2] شبکه، همیشه دارای نویز هستند. ظرفیت کانال‌های زمان‌بندی‌دار اغلب کمتر از کانال‌های انبارشی عاری از نویز است، اما در عوض، تشخیص و حذف آن‌ها سخت‌تر است. برخی روش‌هایی که این دسته کانال‌ها را پیاده‌سازی کرده‌اند به شرح زیر است:

نرخ بسته[3]: در این روش، اطلاعات پوششی با تغییر نرخ ارسال بسته کدگذاری می‌گردند. فرستنده، نرخ ارسال بسته‌ها در هر دوره زمانی[4] را بین دو نرخ یا چندین نرخ تغییر می‌دهد (شکل۴). گیرنده با اندازه‌گیری نرخ بسته‌ها در هر دوره زمانی، اطلاعات پوششی را کدگشایی می‌کند. مثلاً در ساده‌ترین شکل این روش، ارسال بسته در یک دوره زمانی به منزله "یک" و عدم ارسال بسته در یک دوره زمانی به منزله "صفر" تلقی می‌گردد. در این روش، فرستنده و گیرنده یک ساز و کار همگامی[5] برای دوره‌های زمانی نیاز دارند.

زمان‌های بین‌بسته‌ها[6]: در این روش، اطلاعات پوششی در زمان‌های(فواصل) بین‌بسته‌های متوالی، کدگذاری یا سوار می‌شوند (شکل ۵). فواصل زمانی بین‌بسته‌های متوالی می‌توانند به صورت دودویی یعنی صرفاً دو مقدار t_0 و t_1 برای نمایش مقادیر "صفر" و "یک" در نظر گرفته شود، یا مقادیر فواصل زمانی $t_1,t_2,\ldots,t_n$ در نظر گرفته شده و کدگذاری خاصی برای سوار کردن داده‌های پوششی روی این n مقدار مختلف طراحی و اجرا نمود.



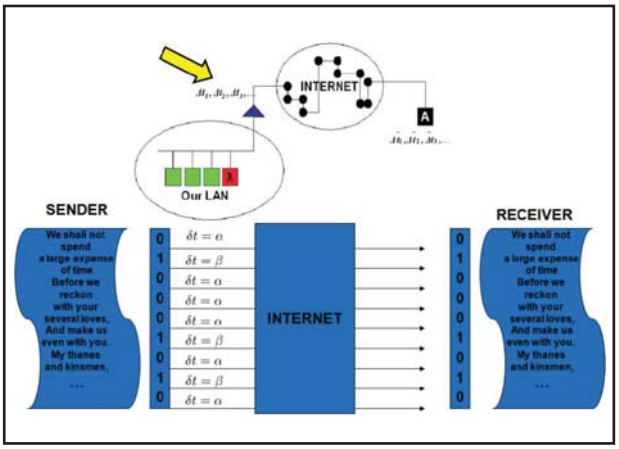
شکل ۴- کانال زمانبندی‌دار پوششی مبتنی بر نرخ بسته

۲-Jitter: تغییرات در زمان‌بندی بین بسته‌های رسیده است که می‌تواند به علت ازدحام شبکه، راندگی زمان‌بندی، یا تغییرات مسیر بسته‌ها به‌وجود آید.

3- packet rate
4- time interval
5- synchronisation
6- inter-packet times

زمان‌بندی توالی پیام[1]: در این روش یکی از ویژگی‌های عملیاتی پروتکل برای سوارکردن داده‌های پوششی مورد استفاده قرار می‌گیرد. مثلاً ارسال تاییدیه[2] به ازای هر فریم یا به ازای هر دو فریم می‌تواند به عنوان یک کدگذاری داده‌های پوششی استفاده شود. در طرحی دیگر بر مبنای وب، برای سوار کردن داده‌های پوششی، ایجاد تأخیر در پاسخ‌دهی توسط سرویس‌دهنده وب به منزله "یک" و پاسخ دهی فوری سرویس‌دهنده وب به منزله "صفر" در نظر گرفته شده است.

گم شدن بسته‌ها[3]: در این روش، از ویژگی‌های ارسال مجدد بسته‌های مفقود شده بهره‌گیری می‌شود. مثلاً گیرنده برای یک بسته که به طور صحیح رسیده است تاییدیه نمی‌دهد. فرستنده قبل از ارسال مجدد بسته، به جای داده‌های کاربر، داده‌های پوششی را در آن جاسازی می‌کند.



شکل ۵- کانال زمانبندی‌دار پوششی مبتنی بر فواصل زمانی بین بسته‌ها

بازترتیب بسته‌ها[4]: در این روش، یک مجموعه از n بسته متوالی در نظر گرفته می‌شود که می‌توانند به n! حالت مرتب شوند. لذا ترتیب ارسال بسته‌ها، مبنای کدگذاری داده‌های پوششی در نظر گرفته می‌شود. در این روش حداکثر تعداد $\log_2 n!$ بیت می‌تواند ارسال شود.

تصادم فریم‌ها[5]: در این روش به هنگام تصادم فریم‌ها در پروتکل CSMA/CD در اترنت، با انتخاب مقدار تأخیر عقب‌نشینی[6] که صفر باشد یا حداکثر، داده‌های پوششی کدگذاری می‌شود. در این مثال یک کانال پوششی یک بیت بر فریم ایجاد می‌گردد.

۶-۵- کانال‌های زمان‌بندی‌دار غیرمستقیم

کانال‌های زمان‌بندی‌دار غیرمستقیم نیز از زمان‌بندی بسته‌ها و پیام‌ها برای ارسال داده‌های پوششی استفاده می‌کنند. ولی ارتباط بین فرستنده و گیرنده به طور مستقیم برقرار نمی‌شود. بدین جهت نامحسوسی این کانال‌ها بهبود می‌یابد. پیاده‌سازی این کانال‌ها سخت‌تر است و در این دسته تعداد کمی طرح ارائه و پیاده‌سازی شده است. ظرفیت این کانال‌ها نیز معمولاً کمتر از ظرفیت کانال‌های زمان‌بندی‌دار مستقیم است.

۶-۶- کانال‌های طول بسته[7] پوششی

به دلیل ناپایداری زیاد زمان ارسال بسته‌ها و تغییرات کیفیت ارتباطات شبکه، کانال‌های زمان‌بندی‌دار فلج می‌شوند. از این‌رو استفاده از طول بسته‌ها برای سوار کردن داده‌های پوششی، مد نظر برخی محققین قرار گرفته است[۱۱]. در این روش، عدد طول بسته‌ها به عنوان یک مجموعه نماد[8] در نظر گرفته می‌شود. مثلاً طول بسته‌ها اگر ۴۰۰ تا ۵۲۷ بایت باشد، هر کدام به یکی از نمادها در جدول کد ASCII منتسب می‌شوند. حال ارسال هر بسته با طول مشخص به منزله ارسال آن نماد در نظر گرفته شده و گیرنده با کدگشایی طول بستهٔ رسیده، به نماد مربوطه که همان داده پوششی است دست می‌یابد.

۷- معیارهای ارزیابی کانال‌های پوششی

برای ارزیابی کانال‌های پوششی، سه معیار اصلی وجود دارد[۱۰]. این معیارها مشابه معیارهای ارزیابی سیستم‌های پنهان‌نگاری می‌باشند.

ظرفیت: حداکثر نرخ ارسال بدون خطا از کانال پوششی را ظرفیت یا پهنای باند کانال می‌نامند. ظرفیت معمولاً با واحد بیت بر ثانیه اندازه‌گیری می‌شود. اما ظرفیت کانال‌های پوششی شبکه به صورت بیت بر بسته نیز بیان می‌گردد که در این‌جا منظور از بسته، همان بسته‌های کانال آشکار/حامل است.

استحکام: استحکام بیانگر میزان دشواری حذف کانال پوششی یا محدود کردن ظرفیت کانال توسط نویز می‌باشد.

نامحسوسی: نامحسوسی نشانگر میزان دشواری تشخیص کانال پوششی است که با مقایسه مشخصه‌های ترافیک کانال پوششی با ترافیک مجاز انجام می‌گردد.

ظرفیت، نامحسوسی و استحکام، به عنوان معیارهای ارزیابی اهداف متضادی هستند. معمولاً حداکثر کردن هم‌زمان هر سه معیار غیرممکن است و کاربران باید برای هر وضعیت خاصی، سبک سنگین کنند که کدام بهترین است. مثلاً ارسال داده‌های کمتر، موجب بهبودی نامحسوسی کانال می‌شود و افزایش افزونگی داده‌ها استحکام کانال را بهبود می‌بخشد. اما هردوی این‌ها، یعنی ارسال کمتر داده‌ها و افزایش افزونگی داده‌ها، ظرفیت کانال را کاهش می‌دهند. از سوی

1- message sequence timing
2- acknowledge
3- facket loss
4- reordering
5- frame collisions
6- back-off

7- packet length
8- symbol

دیگر، استحکام می‌تواند به سادگی با افزایش دامنه سیگنال افزایش داده شود، اما این امر نامحسوسی را کاهش می‌دهد.

۸- مقابله با کانال‌های پوششی

کانال‌های پوششی به دو دلیل عمده به‌وجود می‌آیند: یکی کم دقتی‌های حین طراحی و دیگری ضعف‌های ذاتی که در طراحی سیستم وجود دارد[۱۲]. کانال‌های پوششی که به دلیل کم دقتی‌های حین طراحی به‌وجود می‌آیند را می‌توان پس از کشف، اصلاح نمود؛ ولی کانال‌های پوششی ناشی از ضعف‌های ذاتی سیستم را جز با طراحی مجدد نمی‌توان حذف کرد. راه‌های مقابله با کانال‌های پوششی به سه دسته کلی زیر تقسیم می‌شوند:

۸-۱- حذف[1] کانال

در مرحله طراحی باید وجود هرگونه کانال پوششی مورد تحلیل قرار گرفته و حدالمقدور حذف شوند. زیرا حتی کانال‌های با ظرفیت پایین نیز ممکن است مورد بهره‌برداری واقع شوند. ولی حذف کامل همه کانال‌های پوششی منجر به ناکارآمد شدن سیستم‌ها می‌شود و شاید صرفاً با جایگزینی رویه‌های دستی با رویه‌های خودکار بتوان کانال‌های پوششی را به طور کامل حذف کرد. علاوه برآن، در شبکه‌های رایانه‌ای به طور ذاتی امکان بهره‌گیری از عناصر پیام آشکار برای سوارکردن داده‌های پوششی وجود دارد. بنابراین محققین عقیده دارند که نمی‌توان کانال‌های پوششی را به طور کامل حذف کرد. این مطلب توسط استانداردهای امنیتی نیز تأیید شده است. به طور مثال، کتاب نارنجی TCSEC کانال‌های پوششی با ظرفیت کمتر از یک ثانیه را قابل قبول دانسته است[۱۳].

۸-۲- محدودکردن[2] ظرفیت کانال

اگر کانال را نتوان حذف کرد، باید ظرفیت آن را کاهش داد. مقدار قابل قبول ظرفیت، به مقدار نشت اطلاعاتی که بحران‌ساز می‌شود بستگی دارد. مثلاً اگر ظرفیت کانال آن‌قدر پایین باشد که قبل از آن‌که کاربرد اطلاعات محرمانه منقضی شود نتواند نشت داده شود، چنین کانالی قابل تحمل است. محدود کردن ظرفیت کانال به معنای آهسته کردن فرآیندهای سیستم یا ایجاد نویز است که هر دو، کارآیی سیستم را محدود می‌کنند.

۸-۳- تشخیص[3] کانال

تشخیص کانال پوششی، برای یافتن هرگونه کانال محتمل باید انجام شود. تشخیص کانال‌های پوششی شبکه با نظارت و بازبینی عمیق ترافیک شبکه و به صورت منفعل انجام می‌گردد. اغلب روش‌های تشخیص بر اساس تشخیص رفتار ناهنجار پایه‌گذاری شده‌اند. فرض بر این است که سیستم تشخیص، رفتار طبیعی پروتکل و میزبان‌ها را می‌شناسد و قادر است رفتار ناهنجاری که توسط کانال‌های پوششی بروز می‌کند را تشخیص دهد. به همین دلیل تشخیص کانال‌هایی که رفتارشان بیشتر شبیه رفتار عادی پروتکل شبکه باشد سخت‌تر می‌شود.

تشخیص کانال‌های انبارشی: در برخی از روش‌ها از فضاهای رزرو شده یا استفاده نشده سرآیند یا لایه‌گذاری با مقادیر خاص، برای ایجاد کانال پوششی استفاده می‌کنند. این‌ها چون در واقع از پروتکل به طور غیراستاندارد استفاده می‌نمایند به سادگی قابل تشخیص هستند. برخی روش‌ها که از بیت‌هایی که سابقاً استفاده نمی‌شدند بهره می‌گیرند، ولی اکنون به دلیل استفاده از آن بیت‌ها در پروتکل‌ها، غیرعملی شده‌اند؛ یا برخی پیام‌های تعریف شده یا گسترش‌های سرآیند در پروتکل‌ها عملاً دیگر استفاده نمی‌شوند. از این‌رو استفاده از آن‌ها برای کانال پوششی مشکوک خواهد بود (مثلاً کنترل جریان مبتنی بر ICMP یا گسترش سرآیند مهر زمانی IP).

برخی کانال‌های پوششی که قبلاً توصیف شدند، از این قابلیت که در پروتکل‌ها برخی فیلدهای سرآیند می‌توانند دارای مقادیر دلخواه باشند بهره‌برداری می‌نمایند. در این کانال‌ها، توزیع این مقادیر، از توزیع واقعی که توسط سیستم عامل ایجاد می‌گردد متفاوت می‌شود و به سادگی قابل تشخیص می‌باشد.

تشخیص کانال‌های زمان‌بندی‌دار: درکانال‌های پوششی که براساس تغییر نرخ بسته کار می‌کنند، تشخیص کانال نیز با بازبینی تغییر نرخ‌های ترافیک در طی زمان انجام می‌گردد. گذشتن نرخ ترافیک از یک آستانه خاص نشان‌دهنده وجود کانال پوششی است. برای تشخیص کانال‌های پوششی زمان‌بندی‌دار از آزمون‌های خاص روی زمان‌بندی ترافیک شبکه استفاده می‌شود که این آزمون‌ها به دو دسته کلی تقسیم می‌شوند[۱۴]: آزمون‌های شکل[4] و آزمون‌های قاعده‌مندی[5]. شکل ترافیک با آمارهای مرتبه اول مثل میانگین، واریانس و توزیع، توصیف می‌گردد. قاعده‌مندی ترافیک توسط آمارهای مرتبه دوم یا بالاتر مثل همبستگی داده‌ها توصیف می‌شود. در این‌جا قاعده‌مندی در حوزه زمان منظور است، مثل قاعده‌مندی فرآیند در طول زمان.

همان‌طور که مشاهده می‌شود روش‌های تشخیص کانال‌های پوششی مبتنی بر تحلیل آماری ترافیک شبکه و تشخیص ناهنجاری رفتاری پایه‌گذاری شده‌اند.

1- elimination
2- limitation
3- detection
4- shape tests
5- regularity tests

۹- نتیجه‌گیری

کانال‌های پوششی به دو دسته کلی انبارشی و زمان‌بندی‌دار تقسیم می‌شوند. کانال‌های زمان‌بندی‌دار پوششی سه تفاوت عمده با کانال‌های انبارشی پوششی دارند. به‌دلیل عدم دقت زمان‌بندی ارسال و دریافت بسته‌ها در فرستنده و گیرنده، و لغزش زمانی شبکه که اصولاً به‌دلیل ناپایداری تأخیرات صف‌بندی بسته‌ها در سوئیچ‌ها و مسیریاب‌ها به‌وجود می‌آید، کانال‌های زمان‌بندی‌دار پوششی همیشه دارای نویز هستند. علاوه بر آن، ظرفیت کانال‌های زمان‌بندی‌دار اغلب کمتر از کانال‌های انبارشی عاری از نویز است. ولی تشخیص و حذف کانال‌های زمان‌بندی‌دار به مراتب سخت‌تر از کانال‌های انبارشی است. علی‌رغم تعدد و تنوع تحقیقات انجام شده در زمینه کانال‌های انبارشی، این دسته کانال‌ها به‌سادگی حذف می‌گردند و عملاً قابل استفاده نیستند. در زمینه کانال‌های زمان‌بندی‌دار هنوز جای تحقیقات زیادی وجود دارد. در کارهای انجام شده، هنوز کانال زمان‌بندی‌دار با ظرفیت بالا ابداع نشده است و این امر کاربرد آن‌ها را محدود می‌سازد. در کانال‌های ابداع شده تا کنون، صرفاً روی یکی از عناصر مثل نرخ، فاصله زمانی یا طول بسته‌ها کار شده است. تحقیقات جدید می‌تواند ترکیب این عناصر را برای بهبود معیارهای ظرفیت، استحکام و نامحسوسی کانال به‌کار بندد.

با توجه به کاربردهای زیاد کانال‌های پوششی جهت برقراری ارتباطات امن در پدافند غیرعامل شبکه‌ها و ضرورت تشخیص و مقابله با کانال‌های پوششی غیرمجاز برای دفاع از شبکه‌ها، توجه محققین به این موضوع ضروری به نظر می‌رسد.

مراجع

1. WhiteHat Security, WhiteHat Website Security Statistic Report. (**2010**).
2. Gligor, V., A Guide to Understanding Covert Channel Analysis of Trusted Systems. (**1993**), National Computer Security Center: Fort George G. Meade, Maryland, U.S.A.
3. A. Giani, V.H.B., G .V. Cybenko, Data Exfiltration and Covert Channels. In Proceedings of the SPIE Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense, (**2006**).
4. Lampson, B., A note on the confinement problem. Communication of the ACM, (**1973**). 16(10) p. 613–615.
5. DoD, U.S., Trusted computer system evaluation criteria, TCSEC, in Technical Report, DOD 5200.28-STD. (**1985**), DoD / National Computer Security Center: Washington.
6. V.D., G., A Guide to Understanding Covert Channel Analysis of Trusted Systems. Number NCSC-TG-030 in NSA/NCSC Rainbow Series, (**1993**).
7. Couture, E., Covert Channels. The SANS Institute, (**2010**).
8. Peng, P., P. Ning, and D.S. Reeves, On the Secrecy of Timing-Based Active Watermarking Trace-Back Techniques. In Proceedings of IEEE Symposium on Security and Privacy, (**2006**).
9. Wang, X.Y., S. Chen, and S. Jajodia. Tracking Anonymous Peer-to-Peer VoIP Calls on the Internet. in Proceedings of ACM Conference on Computer Communications Security (CCS). (**2005**).
10. Zander, S., Performance of Selected Noisy Covert Channels and Their Countermeasures in IP Networks, in Centre for Advanced Internet Architectures Faculty of Information and Communication Technologies. (**2010**), Swinburne University of Technology: Melbourne.
11. Dye, D.J., Bandwidth and detection of packet length covert channels. (**2011**), Naval postgraduate school. p. 90.
12. Zander, S., G. Armitage, and P. Branch, A Survey of Covert Channels and Countermeasures in Computer Network Protocols. IEEE Communications Surveys & Tutorials (**2007**). 9(3): p. 44-57.
13. DoD, U.S., Trusted computer system evaluation criteria, TCSEC "The Orange Book", in Technical Report, DOD 5200.28-STD. (**1985**), DoD / National Computer Security Center :Washington.
14. Gianvecchio, S. and H. Wang, An Entropy-Based Approach to Detecting Covert Timing Channels. (**2010**).

Network Covert Channels: An Information Leakage Flow

M. Dehghani[1]

M. Saleh Esfahani[2]

Abstract

Covert channel means communicating information through covering of open and authorized channel in a manner that the existence of the channel is rendered hidden. Network covert channels have many malicious and authorized applications which intend to hide communication. Network covert channels are divided into two categories called Covert Storage and Covert Timing channels. Covert channels have three performance evaluation criteria; capacity, robustness and stealth. Covert channel countermeasure methods are elimination, limitation and detection of channel.
Use of covert channel is an appropriate solution for secure communication in networks for passive defense applications. On the other hand, detection and countering unauthorized covert channels is necessary to defend networks. This paper describes applications and taxonomy of covert channels and presents performance evaluation criteria and countermeasure methods.

Key Words: *Covert Channel, Information Leakage, Performance Evaluation Criteria, Traffic Analysis*

1- PhD Candidate of Computer, Software Discipline, Imam Hossein Comprehensive University (Pbh)- Writer in Charge (Email: mdehghany@ihu.ac.ir)
2- Assistant Professor and Academic Member of the Faculty and Research Center of Computer ICT (Email: msaleh@ihu.ac.ir)