فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال اول، شماره‌ی ۴ (زمستان ۱۳۹۱): صص ۶۹ – ۹۱

کانال‌های پوششی سایبری:
پروتکل ارتباط امن در شبکه‌های پنهان

مهدی دهقانی[۱]
محمود صالح اصفهانی[۲]

تاریخ دریافت: ۱۳۹۱/۰۵/۱۲
تاریخ پذیرش: ۱۳۹۱/۰۸/۲۳

چکیده

کانال پوششی به معنی مبادله اطلاعات در پوشش یک کانال آشکار و مجاز است به نحوی که اصل وجود ارتباط مخفی بماند. کانال‌های پوششی سایبری دارای کاربردهای زیادی برای مقاصد مجاز یا بدخواهانه می‌باشد که محور همه آنها برقراری ارتباط پنهان بین منابع انسانی یا نرم‌افزاری در فضای سایبری می‌باشد. کانال‌های پوششی سایبری از پروتکل‌های شبکه‌های رایانه‌ای که در فضای سایبر برای ارتباطات مجاز برقرار است، برای سوار کردن اطلاعات پوششی و مبادله اطلاعات بین منابع استفاده می‌شود. کانال‌های پوششی دارای سه معیار ارزیابی ظرفیت، استحکام و نامحسوسی می‌باشد و روش‌های مقابله با آنها شامل حذف کردن، محدود کردن و تشخیص کانال می‌باشد. هدف این تحقیق شناخت کانال‌های پوششی در فضای سایبری به عنوان یک پروتکل ارتباطی امن بین منابع انسانی در شبکه پنهان و ارائه یک چارچوب مفهومی برای کانال پوششی می‌باشد که در این چارچوب مفهومی، تعاریف، دسته‌بندی، معیارهای ارزیابی و نحوه مقابله با کانال‌های پوششی تشریح شده و کاربردهای آنها در برقراری ارتباط امن بین منابع (انسانی یا نرم‌افزاری) در شبکه‌های پنهان تشریح می‌گردد. این تحقیق از نوع تحقیقات کاربردی می‌باشد و به روش کتابخانه‌ای با بهره‌گیری از بانک‌های اطلاعاتی پژوهشی قابل دسترسی از طریق اینترنت انجام پذیرفته است. سوال اصلی تحقیق این است که آیا کانال‌های پوششی سایبری، راه‌کار و پروتکلی مناسب برای حل مسئله ارتباط‌گیری با منابع (انسانی یا نرم‌افزاری) شبکه پنهان محسوب می‌گردد. نتایج این تحقیق نشان می‌دهد که بهره‌برداری از کانال‌های پوششی سایبری یک راه‌کار مناسب برای برقراری ارتباط امن بین منابع در شبکه پنهان محسوب می‌گردد.

کلید واژه‌ها: *فضای سایبری، کانال پوششی، ارتباط امن، معیارهای ارزیابی، مقابله، شبکه‌های پنهان*

۱- مربی و عضو هیئت‌علمی دانشکده و پژوهشکده دفاع الکترونیک و سایبری و دانشجوی دکتری کامپیوتر دانشگاه جامع امام‌حسین(ع)
۲- استادیار و عضو هیئت علمی دانشکده و پژوهشکده فناوری اطلاعات و ارتباطات ـ دانشگاه جامع امام حسین(ع)

۱- مقدمه

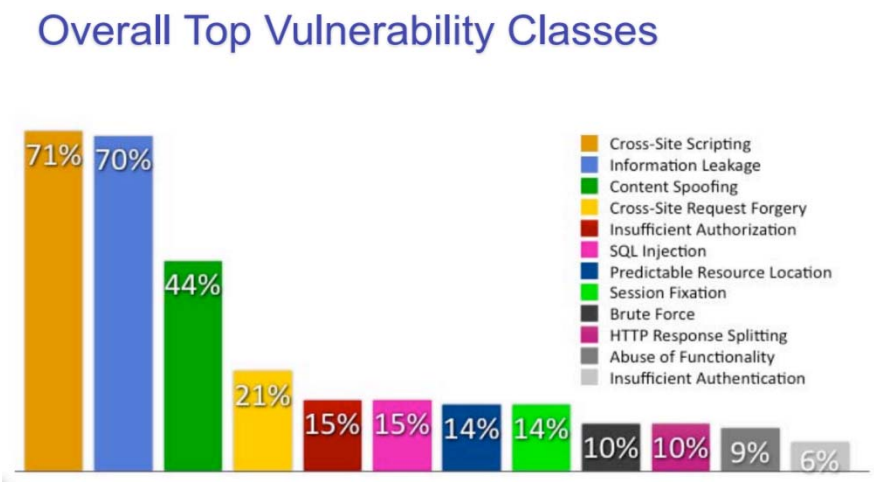
فضای سایبر به عنوان یک پدیده جدید در عصر اطلاعات، پدیده‌های متعددی را با خود به همراه آورده است که هر کدام تهدیدات و فرصت‌هایی را به دنبال دارد. از فناوری‌هایی که یکی از ارکان اصلی تشکیل دهنده فضای سایبری است، پروتکل‌های ارتباطی شبکه‌های رایانه‌ای می‌باشد که در انواع مختلف و برای کاربردهای متعدد ایجاد شده و است. پروتکل‌های ارتباطی با ویژگی‌های ساختاری، نحوه برقراری ارتباط، ظرفیت ارتباطی، سطح امنیت و کاربردهای متفاوت، دارای آسیب‌پذیری‌های متعددی نیز می‌باشد.

با توسعه فضای سایبر، برقراری و ارتقای سطح امنیت در آن به یک مسئله اساسی تبدیل شده است. یکی از تهدیدهای امنیتی برای فضای سایبر، نشت اطلاعات[1] محرمانه یا حساس از طریق پروتکل‌های شبکه می‌باشد. این تهدید برای سازمان‌ها به دلیل وجود دشمنان و رقبای متعدد از اهمیت حیاتی برخوردار است. آمارها نشان می‌دهد (شکل۱) که نشت اطلاعات در رتبه‌بندی تهدیدات و حملات، دومین رتبه را به خود اختصاص داده است (W.Security,2010) یکی از راه‌های اصلی که عمده نشت اطلاعات سازمان‌ها در فضای سایبری 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 می‌گردد. مطابق معیارهای مرکز ملی امنیت رایانه امریکا (Gligor,1993)، تحلیل کانال‌های پوششی جزئی از معیارهای ارزیابی برای دسته‌بندی سامانه‌های امن و احراز سطح امنیتی شده است.

چون اصولاً کانال پوششی برای برقرای ارتباط پنهان استفاده می‌گردد، می‌تواند با دید فرصت نیز مورد بهره‌برداری قرار گیرد. با توجه به کاربردهای متعدد کانال‌های پوششی می‌توان از آنها برای ارتباط‌گیری با منابع انسانی در شبکه پنهان نیز استفاده کرد. برای مخفی ماندن ارتباط و طرفین ارتباط در حالی که شبکه ارتباطی کاملاً تحت نظارت است، از کانال پوششی می‌توان برای برقراری ارتباط بین منابع انسانی در شبکه پنهان استفاده نمود.

در این مقاله یک چارچوب مفهومی برای شناخت و مطالعه کانال پوششی سایبری ارائه می‌شود. تعاریف، کاربردها و کارهای تحقیقاتی انجام شده در زمینه کانال‌های پوششی بررسی می‌گردد و معیارهای ارزیابی و راه‌های مقابله با آن نیز در این چارچوب بیان می‌گردد.

1. Information leakage



شکل۱ ــ آمار ۱۰ آسیب‌پذیری بالا در سال ۲۰۱۰ به ترتیب احتمال رخداد

۲- بیان مسئله، اهمیت و ضرورت آن و سوالات تحقیق

شبکه پنهان عبارت است از شبکه‌ای منسجم، امن، پایدار و پنهان از دید دشمن بین منابع اطلاعاتی. مدیریت منابع پنهان دارای دو دسته فعالیت منبع‌گیری و منبع‌گردانی می‌باشد. منبع‌گیری شامل فعالیت‌های نشان‌گذاری، تحقیق، آماده‌سازی، ارزیابی و توجیه و دعوت به همکاری است. منبع‌گردانی شامل فعالیت‌های ارتباط‌گیری، آموزش، واگذاری ماموریت، پشتیبانی منابع و کنترل و حفاظت منابع است. یکی از فعالیت‌های مهم و ضروری در منبع‌گردانی، برقراری ارتباط از طریق کانالی با سرعت مناسب، امنیت، پایداری و نامحسوسی قابل قبول است.

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 فضای سایبر با لایه‌ها و پروتکل‌های پیچیده، یک رسانه جدید برای عبور پوششی داده‌ها به وجود آورده است.

مسئله این تحقیق این است که برای ایجاد ارتباط امن بین منابع انسانی در شبکه پنهان در فضای سایبری، چه راه‌کارها و پروتکل‌های ارتباطی وجود دارد. این راه‌کارها به چه میزان کاربردی

بوده ، نیازهای واقعی ارتباطی در شبکه پنهان را برآورده می‌نماید. پروتکل‌های ارتباطی با ظرفیت مناسب و امنیت قابل قبول که قابلیت عبور از موانع دفاعی شبکه‌های رایانه‌ای را دارد کدام است. سوال اصلی این تحقیق آن است که آیا کانال‌های پوششی سایبری راه‌کار و پروتکلی مناسب برای حل مسئله ارتباط‌گیری با منابع (انسانی یا نرم‌افزاری) شبکه پنهان محسوب می‌گردد. لذا دیگر سوالات تحقیق بدین شرح است:

ـ کانال پوششی چیست؟

ـ فناوری‌ها و انواع آن کدام است؟

ـ راه‌های مقابله با آن چیست؟

ـ کاربرد آن در ارتباط‌گیری با منابع انسانی در شبکه پنهان چگونه است؟

ـ چارچوب مفهومی شناخت و مطالعه کانال‌های پوششی چیست؟

۳- اهداف و روش تحقیق

هدف اصلی این تحقیق شناخت کانال‌های پوششی سایبری و ارائه چارچوبی برای مطالعه آن می‌باشد. این تحقیق از نوع کاربردی است. گردآوری منابع و مطالعات اولیه تحقیق به روش کتابخانه‌ای با بهره‌گیری از بانک‌های اطلاعاتی قابل دسترسی از طریق اینترنت انجام می‌پذیرد و اطلاعات جمع‌آوری شده به روش‌های گوناگون استدلال مورد تجزیه و تحلیل قرار می‌گیرد. سپس با بهره‌گیری از الگوهای موجود چارچوب کاری مفهومی در کاربردهای دیگر، یک چارچوب مفهومی برای شناخت و مطالعه کانال پوششی پیشنهاد می‌گردد.

در این تحقیق محدودیت‌های زیر وجود دارد:

ـ محدودیت دسترسی به بانک‌های اطلاعاتی و منابع تحقیقاتی مورد نیاز

۴- چارچوب مفهومی کانال‌های پوششی

چارچوب مفهومی[1] مجموعه نظریاتی است که به اندازه کافی مورد قبول واقع شده تا برای تحقیق تحت یک انتظام خاص به‌عنوان اصول راهنما به خدمت گرفته شود (www.wikipedia.org). چارچوب مفهومی کانال‌های پوششی را می‌توان در شش بخش تعریف نمود:

1. conceptual framework

تعریف: شامل تعریف علمی کانال‌های پوششی و الگوی مفهومی و عناصر تشکیل دهنده آن

دسته‌بندی: شامل معرفی ویژگی‌های متمایز کننده رفتار کانال‌های پوششی و معرفی دسته‌بندی‌های موجود برای آنها. از این طریق می‌توان برای پاسخ‌گویی نیاز کاربردی، نسبت به انتخاب ویژگی‌های کانال مورد نظر اقدام نمود.

کاربردها: کاربردهای متنوع کانال‌های پوششی معرفی می‌گردد و جایگاه کانال مورد مطالعه مشخص می‌شود.

چرخه حیات: فرآیند برپایی کانال پوششی بین فرستنده و گیرنده و تبادل اطلاعات و در نهایت خاتمه ارتباط تعریف می‌شود.

معیارهای ارزیابی کارآیی: معیارهای موثر در کارآیی کانال پوششی معرفی و مطالعه می‌شود.

روش‌های مقابله: از دیدگاه امنیت شبکه، باید با کانال‌های پوششی مقابله نمود. در این بخش راه‌های مقابله با کانال‌های پوششی مطالعه می‌شود.

این چارچوب طریقه خاصی را برای انجام تحقیق معرفی می‌نماید و نحوه استفاده از تحقیقات مشابه و ایده‌های دیگران را نشان می‌دهد. چارچوب‌کاری، همانند یک نقشه راه دقیق علامت‌گذاری شده است و هر بخش از آن به عنوان یک مرحله از تحقیق محسوب می‌گردد. برای به دست آوردن یک شناخت کامل و تحقیق در زمینه کانال پوششی باید هر شش مرحله را مد نظر قرار داد. در ادامه مقاله در مورد هر بخش به طور مبسوط بحث می‌شود.

۵- تعریف و الگوی مفهومی

برای فرایند پنهان‌سازی اطلاعات در پروتکل‌های شبکه از عبارات مختلفی استفاده شده است. در حالی که محققین مختلفی از آن به عنوان کانال‌های پوششی یاد می‌کنند، برخی دیگر از عبارت پنهان‌نگاری[1] و یا پنهان‌سازی اطلاعات[2] استفاده کرده‌اند.

در این مقاله، هنگامی که به پنهان‌سازی اطلاعات در پروتکل‌های شبکه ارجاع می‌شود از عبارت *کانال پوششی* استفاده شده، از اطلاعاتی که از طریق کانال پوششی انتقال می‌یابد تحت عنوان *اطلاعات پوششی* یاد می‌شود. هنگامی که از پنهان‌سازی اطلاعات در محتوا(فایل تصویر، صوت یا متن) سخن به میان می‌آید، از عبارت پنهان‌نگاری (که از حیث لفظی به معنای *نوشتن*

1. steganography
2. information hiding

پوششی می‌باشد)، و از عبارت پنهان*سازی اطلاعات* به عنوان عبارتی کلی به جای هر دو آنها، استفاده می‌گردد.

۵-۱- تعاریف

برای کانال پوششی تعاریف مختلفی ارائه شده است.

ـ لمپسن (B. Lampson,1973:613-615) 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.

ـ در فرهنگ اصطلاحات وزارت دفاع امریکا (U. S. DoD,1985)، کانال پوششی یک کانال ارتباطی است که می‌تواند توسط پردازه‌ای برای ارسال اطلاعات استفاده شود به نحوی که از سیاست امنیت تشکیلات تجاوز نماید.

ـ از نظر گلیگور (G. V.D.,1993)، 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 است که حقیقت ذاتی و منظور کانال‌های پوششی را آشکار می‌سازد، یعنی عبور از سیاست امنیت تشکیلات و ارسال اطلاعات به صورت پنهان بدون آن که تشخیص داده شود. نگارنده این مقاله، تعریف گیلگور را مناسب‌تر تشخیص می‌دهد.

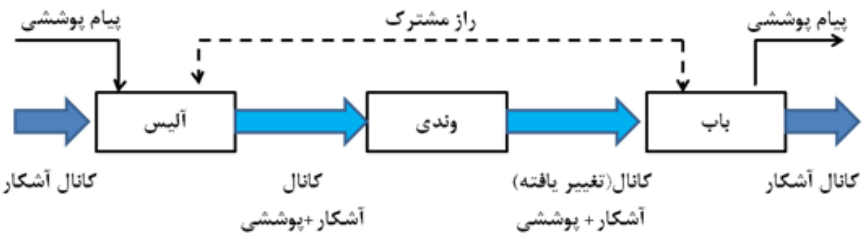
۵-۲- تفاوت رمزنگاری و کانال پوششی

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 رمزنگاری شده، ارتباط برقرار است و هویت مبداء و مقصد مخفی نگه داشته نمی‌شود. ولی در ارتباطات پوششی، وجود ارتباط و هویت طرف‌های ارتباط مخفی نگهداشته می شود. اطلاعات پوششی با استفاده از روش‌هایی، در رسانه و ارتباط عادی و مجاز به نحوی مخفی سازی می‌شود که تا حد زیادی غیرقابل تشخیص باشد. در پنهان‌نگاری، اطلاعات پوششی در محتوای صوتی، تصویری یا متنی مخفی‌سازی می‌شود، ولی در کانال‌های پوششی از پروتکل‌های شبکه به عنوان حامل اطلاعات پوششی استفاده می‌گردد.

۵-۳- الگوی مفهومی کانال پوششی

مسئله زندانی یک مدل مفهومی عملی برای ارتباطات کانال پوششی است (G. J. Simmons, 1983, 51–67) صورت مسئله از این قرار است که دو نفر به نام‌های آلیس و باب به زندان افتاده ، قصد فرار دارند. برای توافق بر سر برنامه فرار آنها نیاز به ارتباط دارند ولی نگهبانی به نام وندی بر تمامی پیام‌های آنها نظارت می‌نماید. اگر نگهبان هر نشانه‌ای از پیام‌های مشکوک بیابد، آن دو را به زندان انفرادی می‌اندازد و فرار آنها را غیرممکن می‌سازد. آلیس و باب باید پیام‌های معمولی و بی‌ضرری را مبادله نمایند که حاوی اطلاعات پنهانی باشد و وندی متوجه آن نشود.

شکل۲ الگوی مفهومی کانال پوششی بین آلیس و باب را نشان می‌دهد. آنها یک کانال آشکار که در ظاهر بی‌ضرر و معمولی است برقرار می‌نمایند که حاوی یک کانال پوششی پنهان است. آلیس و باب یک راز را به اشتراک می‌گذارند که برای کدگذاری و کدگشایی کانال پوششی و پیام‌های مخفی استفاده می‌شود. در برخی کاربردها ممکن است فرستنده و گیرنده یک نفر باشند. مثلاً نفوذگری که اطلاعات محرمانه را از سازمان خارج می‌کند، در دو طرف ارتباط همان نفوذگر قرار دارد. وندی شبکه را مدیریت می‌کند و برای یافتن کانال پوششی بر شبکه نظارت می‌کند یا ترافیک عبوری را برای حذف یا قطع کانال‌های پوششی تغییر می‌دهد.



شکل۲ ــ الگوی مفهومی کانال پوششی

۶- دسته‌بندی کانال‌های پوششی

از دیدگاه کاربردی می‌توان کانال‌های پوششی سایبری را به دو دسته کانال بین منابع انسانی و کانال بین منابع هوشمند نرم‌افزاری تقسیم نمود. موضوع این تحقیق کانال‌های پوششی سایبری بین منابع انسانی است. در این دسته، کانال پوششی بین دو نقطه فرستنده و گیرنده برقرار

می‌گردد و منابع انسانی توسط یک نرم‌افزار کاربردی از این کانال ارتباطی استفاده می‌نمایند. برای ارتقای سطح امنیت ارتباط، می‌توان امکان رمزنگاری و رمزگشایی اطلاعات را نیز در این نرم‌افزارهای کاربردی پیش‌بینی نمود.

برای کانال‌های پوششی با توجه به فنون به کار رفته در هر کدام، دسته‌بندی‌های دیگری نیز ارائه شده است. جدیدترین آنها که به نظر می‌رسد دسته‌بندی دقیق‌تری باشد توسط زندر ارائه شده است (S. Zander,2010). زندر معیارهای دسته‌بندی کانال‌های پوششی را به‌صورت زیر در نظر گرفته است:

کانال‌های انبارشی۱ و کانال‌های زمان بندی‌دار۲: در دسته‌بندی اولیه، کانال‌های پوششی به کانال‌های انبارشی و زمانبندی‌دار تقسیم شده است. کانال‌های انبارشی، اطلاعات پوششی را در فیلدهای رزرو یا فیلدهای استفاده نشده یا در فیلدهایی که امکان استفاده از آنها بدون تاثیر در عملکرد پروتکل وجود دارد،ذخیره می‌شود. فرستنده داده‌های مورد نظر را در این فیلدها می نویسد و گیرنده آنها را از این فیلدها می‌خواند. در کانال‌های زمان بندی‌دار، فرستنده اطلاعات پوششی را روی زمان بندی ارسال بسته‌ها سوار می‌کند. یعنی زمان بندی 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.

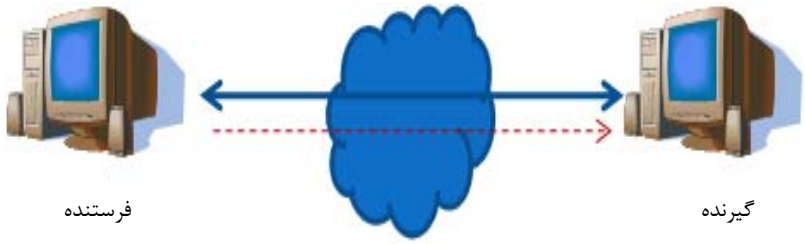
انواع پوشش؛ قابل پیش‌بینی[3]، متغیر[4] و تصادفی: پوشش در واقع مشخصه ترافیک آشکار است که داده پوششی در آن کدگذاری می‌شود. پوشش قابل پیش‌بینی به معنی آن است که اساساً هیچ تغییری در پوشش داده نمی‌شود. پوشش متغیر به معنی آن است که تغییرات محدودی وجود دارد. پوشش تصادفی نیز به معنی آن است که داده پوششی شبه 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 عبارتند از: جایگشت[5] به معنی جابجایی بیت‌ها با مکان ناشناخته، پاک شدگی[6] به معنی جابجایی بیت‌ها با مکان شناخته شده، حذف به معنی مفقود شدن کامل بیت‌ها و درج بیت‌ها.

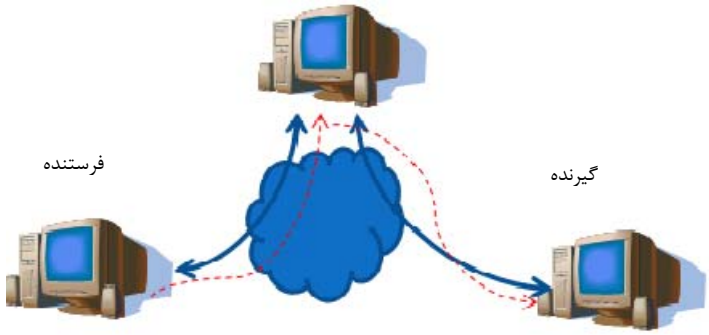
1. covert storage channel
2. covert timing channel
3. predictable
4. variable
5. substitution
6. erasures

کانال‌های منفعل[1]**، نیمه‌منفعل و فعال:** در کانال منفعل، فرستنده از ترافیک موجود کاربران ناآگاه به عنوان پوشش استفاده می‌کند. در کانال‌های نیمه‌منفعل، فرستنده ترافیک آشکار را بوسیله 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(شکل۳). 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(شکل۴).



شکل۳ ـ کانال پوششی مستقیم



شکل۴ ـ کانال پوششی غیرمستقیم

1. passive

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 یا در فرایند عملکرد پروتکل کدگذاری می‌شوند یا از ابهام معنایی موجود در پروتکل‌ها بهره‌برداری می‌نماید. اگرچه پیاده‌سازی این کانال‌ها ساده است و به دلیل فقدان نویز، کارآ هستند، ولی رفتار ناهنجارشان به سادگی قابل تشخیص است و با تنظیمات بهینه‌سازی[1] پروتکل، این کانال‌ها حذف می‌شوند.

به‌طور اجمالی، 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[2] سرآیند پروتکل‌های IPV6
- ذخیره‌سازی در بخش لایه‌گذاری[3] فریم یا بسته در پروتکل‌های IP و TCP
- ذخیره‌سازی یا سوارکردن اطلاعات روی فیلد مهرزمانی[4]
- سوارکردن 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[5] 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 می‌باشد ولی مجموع مقابله‌ای آن‌ها به غلط تنظیم شده است.
- تونل‌سازی[6] با پروتکل‌هایی که معمولاً مسدود نمی‌شود مثل HTTP یا DNS و قرار دادن بسته‌های IP حاوی داده‌های 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.

1. normalisation
2. header extensions
3. padding
4. timestamp
5. checksum
6. tunneling

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 می‌کند. اما فیلدهای داده که به عنوان پوشش استفاده می‌شود در مسیر بین فرستنده و گیرنده در معرض تغییرات است. 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 می‌یابد و بسته‌ها نیز می‌تواند از مسیرهای مختلف در شبکه عبور کند، این کانال دارای نویز است.

۶-۳- کانال‌های انبارشی غیرمستقیم

کانال‌های انبارشی غیرمستقیم، فرستنده و گیرنده را قادر می‌سازد تا داده‌های پوششی کدگذاری شده در فیلدهای پروتکل را از طریق گره میانی ناآگاه مبادله نماید. 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 دارد.

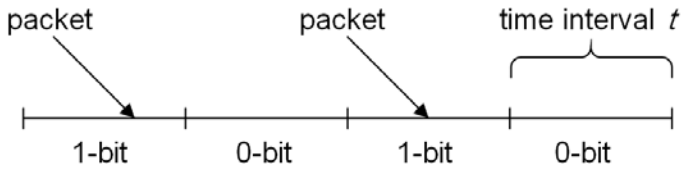
چند نمونه کار انجام شده در این دسته بدین شرح است: فرستنده، بسته SYN با آدرس مبداء جعلی که همان آدرس گیرنده مورد نظر است را با ISN حاوی داده‌های پوششی برای یک میزبان ناآگاه می‌فرستد. میزبان واسط ناآگاه، SYN/ACK یا SYN/RST را با شماره توالی برابر ISN+1 به آدرس گیرنده مورد نظر می‌فرستد. گیرنده مقدار ISN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

۶-۴- کانال‌های زمان بندی‌دار مستقیم

کانال‌های زمان بندی‌دار پوششی کانال‌هایی است که داده‌های پوششی را در زمان بندی فریم‌ها، بسته‌ها یا پیام‌هایی که مستقیماً بین فرستنده و گیرنده مبادله می‌شود کدگذاری می‌نماید. کانال‌های زمان بندی‌دار به دلیل عدم دقت زمان بندی در فرستنده و گیرنده و لغزش زمانی[۱] شبکه، همیشه دارای نویز می‌باشد. 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 کرده است به شرح زیر می‌باشد :

نرخ بسته[۲]: در این روش، اطلاعات پوششی با تغییر نرخ ارسال بسته کدگذاری می‌گردد. فرستنده، نرخ ارسال بسته‌ها در هر دوره زمانی[۳] را بین دو نرخ یا چندین نرخ تغییر می‌دهد (شکل۵). 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[۴] برای دوره‌های زمانی نیاز دارند.

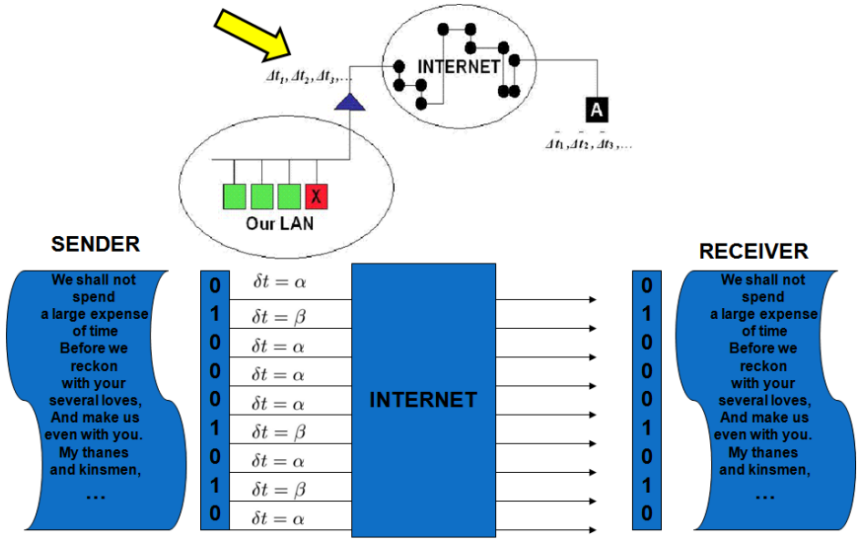
زمان‌های بین‌بسته‌ها[۵]: در این روش، اطلاعات پوششی در زمان‌های(فواصل) بین‌بسته‌های متوالی کدگذاری یا سوار می‌شود (شکل۶). فواصل زمانی بین‌بسته‌های متوالی می‌تواند به صورت دودویی یعنی صرفاً دو مقدار t_0 و t_1 برای نمایش مقادیر "صفر" و "یک" در نظر گرفته شود، یا مقادیر فواصل زمانی $t_1,t_2,\ldots,t_n$ در نظر گرفته شده ، کدگذاری خاصی برای سوار کردن داده‌های پوششی روی این n مقدار مختلف طراحی و اجرا نمود.



شکل۵ ــ کانال زمان‌بندی‌دار پوششی مبتنی بر نرخ بسته

۱- Jitter: تغییرات در زمان بندی بین بسته‌های رسیده است که می‌تواند به علت ازدحام شبکه، راندگی زمان بندی، یا تغییرات مسیر بسته‌ها به وجود آید.

2. packet rate
3. time interval
4. synchronisation
5. inter-packet times



شکل ۶ ـ کانال زمان‌بندی‌دار پوششی مبتنی بر فواصل زمانی بین بسته‌ها

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.

گم‌شدن 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.

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

1. message sequence timing
2. acknowledge
3. facket loss
4. reordering

تصادم فریم‌ها[1]: در این روش به هنگام تصادم فریم‌ها در پروتکل CSMA/CD در اینترنت، با انتخاب مقدار تأخیر عقب نشینی[2] که صفر باشد یا حداکثر، داده‌های پوششی کدگذاری می‌شود. در این مثال یک کانال پوششی یک بیت بر فریم ایجاد می‌گردد.

۶-۵- کانال‌های زمان بندی‌دار غیرمستقیم

کانال‌های زمان بندی‌دار غیرمستقیم نیز از زمان بندی بسته‌ها و پیام‌ها برای ارسال داده‌های پوششی استفاده می‌کند. 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 پیاده سازی شده است. ظرفیت این کانال‌ها نیز معمولاً کمتر از ظرفیت کانال‌های زمان بندی‌دار مستقیم است.

۶-۶- کانال‌های طول بسته[3] پوششی

به دلیل ناپایداری زیاد زمان ارسال بسته‌ها و تغییرات کیفیت ارتباطات شبکه، کانال‌های زمان بندی‌دار فلج می‌شود. از این‌رو استفاده از طول بسته‌ها برای سوار کردن داده‌های پوششی، مد نظر برخی محققین قرار گرفته است (D. J. Dye,2011). در این روش، عدد طول بسته‌ها به عنوان یک مجموعه نماد[4] در نظر گرفته می‌شود. مثلاً طول بسته‌ها اگر ۴۰۰ تا ۵۲۷ بایت باشد، هر کدام به یکی از نمادها در جدول کد ASCII منتسب می‌شود. حال ارسال هر بسته با طول مشخص به منزله ارسال آن نماد در نظر گرفته شده ، گیرنده با کدگشایی طول بسته‌ی رسیده، به نماد مربوطه که همان داده پوششی است دست می‌یابد.

۷- کاربردهای کانال پوششی

بسیاری از گروه‌ها و افراد برای مخفی نگهداشتن ارتباطات خود انگیزه دارند (E. Couture,2010). مجرمان، نفوذگران، معارضین دولت‌ها و سازمان‌ها، مدیران شبکه و عوامل سرویس‌های اطلاعاتی ممکن است در جستجوی کانال‌های پوششی باشند. این‌ها ممکن است به منظورهای زیر از کانال پوششی استفاده کنند:

1. frame collisions
2. back-off
3. packet length
4. symbol

ـ **گردآوری و خروج داده‌های حساس یا محرمانه از شبکه‌های امن:** در این موارد معمولاً با نصب اسب تروا[1] روی سامانه تسخیر شده، انتقال اطلاعات از طریق کانال پوششی و دور از چشم مدیران شبکه انجام می‌گردد.

ـ **نصب، گسترش یا کنترل بدافزار روی سامانه‌های تسخیر شده:** بدافزارهای شبکه‌ای مثل شبکه‌های بات۲ برای ارسال دستورات و مبادله اطلاعات بین فرماندهی و عوامل شبکه از کانال های پوششی استفاده می‌کند تا شناسایی نشود.

ـ **ارتباط‌گیری با منابع شبکه پنهان:** برای مخفی ماندن ارتباط و طرفین ارتباط در حالی که شبکه ارتباطی کاملاً تحت نظارت است، از کانال پوششی می‌توان برای برقراری ارتباط بین منابع شبکه پنهان استفاده نمود.

ـ **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.

ـ **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. سامانه‌های کوزه عسل۳ که در واقع سامانه‌های رایانه‌ای تله شده برای نفوذگران است نیز می‌تواند از کانال‌های پوششی، پنهان از نفوذگران برای ارسال به موقع داده‌های ثبت وقایع استفاده کند.

ـ **عبور از دیوارآتش 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.

ـ **مبادله کلید رمزنگاری:** برای برقراری ارتباط به صورت رمز، باید کلیدهای رمزنگاری که ممکن است متقارن یا نامتقارن باشد 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.

ـ **حفاظت از حقوق معنوی:** مبادله اطلاعات حساس محصولات صوتی و تصویری همانند شماره سریال می‌تواند با روش‌های کانال پوششی انجام شود (P. Peng, et al.,2006).

1. trojan horse
2. botnets
3. honeypot

ـ **تعقیب ترافیک خاص:** با استفاده از روش‌های کانال پوششی، نشان‌گذاری[1] روی جریان‌های ترافیک شبکه پیاده‌سازی شده، آنها را از همدیگر متمایز می‌نماید. بدین ترتیب امکان تعقیب ترافیک خاص در شبکه‌های گمنام و یافتن مهاجم یا مجرم فراهم می‌گردد (X. Y. Wang, et al.,2005).

ایجاد و استفاده از کانال‌های پوششی یک راه‌کار مناسب برای ایجاد ارتباطات پنهان در شبکه منابع 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 سایبری را جذاب نموده است.

۸- چرخه حیات کانال پوششی

طرح‌ریزی، برپایی کانال پوششی، برقراری ارتباط پنهان و در نهایت خاتمه ارتباط و برچیدن کانال شامل یک مجموعه اقدامات به شرح زیر است. چون این اقدامات برای برپایی هر کانال پوششی با ترتیب و توالی ذکر شده باید انجام پذیرد. آن را چرخه حیات کانال پوششی نام‌گذاری کرده اند.

۱- تعیین کاربرد کانال مورد نظر و ویژگی‌های آن بر اساس کاربرد. در این مرحله باید ویژگی‌های کانال چنانچه در بند ۶ این مقاله بیان شد، دقیقاً مشخص شود. در ضمن باید پروتکل ارتباطی مناسب برای ایجاد کانال شناسایی و انتخاب گردد.

۲- طراحی کتابچه کدگذاری مشترک با کارآیی مناسب

۳- تعریف سازوکار همگامی طرفین در شروع، توقف موقت و خاتمه ارتباط

۴- در اختیار گرفتن کانال آشکار: سامانه فرستنده و گیرنده کانال آشکار یا نقاط میانی در مسیر ترافیک آشکار باید در اختیار گرفته شود.

۵- مبادله کتابچه کدگذاری و اطلاعات همگامی

۶- برپایی کانال پوششی و تبادل اطلاعات پنهان بین طرفین

1. watermarking

۹- معیارهای ارزیابی کارآیی کانال پوششی

برای ارزیابی کارآیی کانال‌های پوششی سه معیار اصلی وجود دارد (S. Zander,2010). این معیارها مشابه معیارهای ارزیابی سامانه‌های پنهان‌نگاری می‌باشد.

ظرفیت: حداکثر نرخ ارسال بدون خطا از کانال پوششی را ظرفیت یا پهنای باند کانال می‌نامند. ظرفیت معمولاً با واحد بیت بر ثانیه اندازه گیری 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 می‌باشد. 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 می‌دهد. از سوی دیگر، استحکام می‌تواند به سادگی با افزایش دامنه سیگنال افزایش داده شود، اما این امر نامحسوسی را کاهش می‌دهد.

۱۰- مقابله با کانال‌های پوششی

کانال‌های پوششی به دو دلیل عمده به وجود می‌آید: یکی کم دقتی‌های حین طراحی و دیگری ضعف‌های ذاتی که در طراحی سامانه وجود دارد (S. Zander, et al.,2007: 44-57). کانال‌های پوششی که به دلیل کم دقتی‌های حین طراحی به وجود می‌آید را می‌توان پس از کشف، اصلاح نمود. ولی کانال‌های پوششی ناشی از ضعف‌های ذاتی سامانه را جز با طراحی مجدد نمی‌توان حذف کرد. راه‌های مقابله با کانال‌های پوششی به سه دسته کلی زیر تقسیم می‌شود:

۱۰-۱- حذف[1] کانال

در مرحله طراحی باید وجود هرگونه کانال پوششی مورد تحلیل قرارگرفته ، حدالمقدور حذف شود. زیرا حتی کانال‌های با ظرفیت پایین نیز ممکن است مورد بهره‌برداری واقع شود. ولی حذف کامل همه‌ی کانال‌های پوششی منجر به ناکارآمد شدن سامانه ها 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 (U. S. DoD,1985).

۱۰-۲- 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 سامانه یا ایجاد نویز است که هردو، کارآیی سامانه را محدود می‌کند.

۱۰-۳- 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 شده است. فرض بر این است که سامانه 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.

1. elimination
2. limitation
3. detection

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 می‌شود. این‌ها چون در واقع از پروتکل به طور غیراستاندارد استفاده می‌نماید به سادگی قابل تشخیص می‌باشد. برخی روش‌ها که از بیت‌هایی که سابقاً استفاده نمی‌شده بهره می‌گیرد، اکنون به دلیل استفاده از آن بیت‌ها در پروتکل‌ها، غیرعملی شده است. یا برخی پیام‌های تعریف شده یا گسترش‌های سرآیند در پروتکل‌ها عملاً دیگر استفاده نمی‌شود. 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 شده، از این قابلیت که در پروتکل‌ها برخی فیلدهای سرآیندکه می‌تواند دارای مقادیر دلخواه باشد بهره‌برداری می‌گردد. 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 می‌کند، 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 زمان بندی‌دار از آزمون‌های خاص روی زمان بندی ترافیک شبکه استفاده می‌شود که این آزمون‌ها به دو دسته کلی تقسیم می‌شود (S. Gianvecchio and H. Wang,2010): آزمون‌های شکل۱ و آزمون‌های قاعده‌مندی۲. 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 شده است.

1. shape tests
2. regularity tests

نتیجه‌گیری و پیشنهاد

یکی از مباحث مهم مدیریت منابع در شبکه پنهان، ارتباط‌گیری با منابع انسانی با استفاده از کانالی امن، پایدار و نامحسوس است. پنهان‌سازی اطلاعات یک راه‌کار فنی قابل توجه برای پاسخ‌گویی این نیاز محسوب می‌گردد. پنهان‌سازی اطلاعات شامل دو شاخه کلی پنهان‌نگاری اطلاعات در محتوای پوشه های تصویری، صوتی یا متنی، و کانال‌های پوششی سایبری می‌باشد.

کانال‌های پوششی سایبری به دو دسته کلی انبارشی و زمان بندی‌دار تقسیم می‌شود. کانال‌های زمان بندی‌دار پوششی سه تفاوت عمده با کانال‌های انبارشی پوششی دارد. به دلیل عدم دقت زمان بندی ارسال و دریافت بسته‌ها در فرستنده و گیرنده، و لغزش زمانی شبکه که اصولاً به دلیل ناپایداری تأخیرات صف‌بندی بسته‌ها در سوئیچ‌ها و مسیریاب‌ها به وجود می‌آید، کانال‌های زمان بندی‌دار پوششی همیشه دارای نویز می‌باشد. علاوه بر آن، ظرفیت کانال‌های زمان بندی‌دار اغلب کمتر از کانال‌های انبارشی عاری از نویز است. ولی تشخیص و حذف کانال‌های زمان بندی‌دار به مراتب سخت‌تر از کانال‌های انبارشی است.

علی‌رغم تعدد و تنوع تحقیقات انجام شده در زمینه کانال‌های انبارشی، این دسته کانال‌ها به سادگی حذف می‌گردد و عملاً قابل استفاده نیست. در زمینه کانال‌های زمان بندی‌دار هنوز جای تحقیقات زیادی وجود دارد. در کارهای انجام شده، هنوز کانال زمان بندی‌دار با ظرفیت بالا ابداع نشده است و این امر کاربرد آن را محدود می‌سازد.

در این مقاله کانال‌های پوششی سایبری برای ایجاد ارتباط امن و نامحسوس در شبکه پنهان پیشنهاد شد و یک چارچوب برای شناخت و مطالعه کانال‌های پوششی ارائه گردید. برای ارتقای سطح امنیت کانال، می‌توان قبل از ارسال روی اطلاعات پوششی رمزنگاری نیز انجام داد. در این مقاله ضمن ارائه چارچوب مطالعه، تعاریف، دسته‌بندی، کاربردها، چرخه حیات، معیارهای ارزیابی و روش‌های مقابله با کانال‌های پوششی نیز تشریح گردید.

باتوجه به کاربرد کانال‌های پوششی برای ارتباط‌گیری با منابع انسانی در شبکه پنهان و نیز کاربرد آن در عملیات سایبری و علاوه بر آن، از دیدگاه امنیت و پدافند غیرعامل شبکه‌ها، ضرورت تشخیص و مقابله با کانال‌های پوششی غیرمجاز، توجه محققین به این موضوع ضروری به‌نظر می‌رسد.

لذا پیشنهاد می‌گردد به منظور توسعه دانش، فناوری و کاربردهای کانال‌های پوششی، پروژه‌های تحقیقاتی در سطوح کاربردی و حتی بنیادی در حوزه کانال‌های پوششی سایبری در

مراکز تحقیقاتی تعریف و اجرا گردد و در دانشگاه‌ها نیز پروژه‌های دانشجویی در سطوح دکتری، کارشناسی ارشد و کارشناسی تعریف و اجرا گردد. 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 به کار بندد. با توجه به این که کانال‌های انبارشی به سادگی شناسایی یا حذف می‌گردد، آنها از دیدگاه کاربردی عملاً قابل استفاده نمی باشد. از این‌رو بر تمرکز تحقیقات در زمینه کانال‌های زمان بندی‌دار پوششی تاکید می‌گردد. با توجه به محدودیت پهنای باند کانال‌های زمان بندی‌دار پوششی که تاکنون ابداع شده است، در حال حاضر طراحی و ساخت یک شبکه پیام کوتاه با بهره‌گیری از کانال‌های زمان بندی‌دار پوششی برای ارتباط بین منابع انسانی در شبکه پنهان پیشنهاد می‌گردد.

مراجع

W. Security (2010), "WhiteHat Website Security Statistic Report ",

V. Gligor (1993), "A Guide to Understanding Covert Channel Analysis of Trusted Systems," National Computer Security Center, Fort George G. Meade, Maryland, U.S.A., Technical Report NCSC-TG-030 in NSA/NCSC Rainbow Series,

V. H. B. A. Giani, G. V. Cybenko (2006), "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, vol. V, April.

Available: www. wikipedia. org

B. Lampson (1973), "A note on the confinement problem," Communication of the ACM, vol. 16(10) pp. 613–615 ,

U. S. DoD (1985), "Trusted computer system evaluation criteria, TCSEC," DoD / National Computer Security Center, WashingtonDec..

G. V.D. (1993), "A Guide to Understanding Covert Channel Analysis of Trusted Systems," Number NCSC-TG-030 in NSA/NCSC Rainbow Series, November.

G. J. Simmons (1983), "The Prisoners' Problem and the Subliminal Channel," in Proceedings of Advances in Cryptology (CRYPTO), pp. 51–67.

S. Zander (2010), "Performance of Selected Noisy Covert Channels and Their Countermeasures in IP Networks," Doctor of Philosophy, Centre for Advanced Internet Architectures Faculty of Information and Communication Technologies, Swinburne University of Technology, Melbourne

D. J. Dye (2011), "Bandwidth and detection of packet length covert channels," Master of science in computer science, Naval postgraduate school.,

E. Couture (2010), "Covert Channels," The SANS Institute.,

P. Peng, et al. (2006), "On the Secrecy of Timing-Based Active Watermarking Trace-Back Techniques," In Proceedings of IEEE Symposium on Security and Privacy.,

X. Y. Wang, et al. (2005), "Tracking Anonymous Peer-to-Peer VoIP Calls on the Internet," in Proceedings of ACM Conference on Computer Communications Security (CCS), November

S. Zander, et al. (2007), "A Survey of Covert Channels and Countermeasures in Computer Network Protocols," IEEE Communications Surveys & Tutorials vol. 9, pp. 44-57.,

U. S. DoD (1985), "Trusted computer system evaluation criteria, TCSEC "The Orange Book"," DoD / National Computer Security Center, Washington.

S. Gianvecchio and H. Wang (2010), "An Entropy-Based Approach to Detecting Covert Timing Channels.",