امنیت الکترونیکی ؛ نیازها، راه‌حل‌ها، چالش‌ها

نگارندگان:

آرام حیدری[1]

a.heidari@ece.ut.ac.ir

افشین لامعی[2]

afshinLamei@yahoo.com

[1] از شرکت پردازش‌گران کردستان و دانشجوی دانشکده فنی دانشگاه تهران

[2] از شرکت آشنا نت ایمن و دانشجوی دانشکده فنی دانشگاه تهران

واژگان کلیدی:
امنیت اطلاعات، امنیت الکترونیکی، نفوذ، رمزنگاری، گواهی کلید عمومی، DS، محرمانه بودن، جامعیت، مسیریاب، شبکه، دسترسی

چکیده:

در عصر انفجار اطلاعات، داده به عنوان یک سرمایه گران‌بهای ملی مورد توجه است. در حالی که بسیاری از ساختارهای سنتی، جای خود را به فناوری‌های مدرن می دهند، مکانیزم‌های تبادل اطلاعات نیز به سرعت به سمت الکترونیکی شدن پیش می‌روند. در این میان، امنیت الکترونیکی و به عبارت دیگر امنیت شبکه، به عنوان محور مباحث فناوری اطلاعات در آمده است. خطرات و تهدیدهای موجود، لزوم دست‌یابی به دانش عمیق این رشته را در کشورمان بیش از پیش نمایان ساخته است. در حالی که فناوری الکترونیک به سرعت پیشرفت می کند، نیازها و راه حل‌های جدیدی به وجود می‌آیند.

در این مقاله، سعی شده است که قدم کوچکی برای معرفی مباحث پایه‌ای امنیت برداشته شود.

مقدمه:

امنیت الکترونیکی امروزه نه فقط به عنوان موضوعی قابل توجه برای مطالعات و تحقیقات، بلکه به صورت نیازی در کنار دیگر مباحث فناوری اطلاعات و گاه به عنوان مرکز و محور مباحث این رشته مطرح است. حوزه امنیت، حوزه‌ای بسیار حساس و دقیق است و اطلاعات به عنوان سرمایه گران‌بهای اشخاص حقیقی و حقوقی، نیازمند محافظت دقیق و قوی است.

مساله امنیت در سال‌های اخیر به صورت بسیار گسترده‌ای مورد توجه محافل علمی و به خصوص جامعه دانشگاهی قرار گرفته است.

شاید بتوان گفت که مطرح شدن بحث **معماری امنیت** در سال‌های اخیر به نحو مطلوبی توانسته است مفاهیم گسترده و گوناگون این حوزه را به صورتی مفید و منطقی دسته بندی و جایگاه و خاستگاه آنها را مشخص کند.

با توجه به نو بودن و تازگی این رشته در دنیا و همچنین گستردگی و عمق مطالب، به نظر می‌آید که تا کنون نسبت به جایگاه مسئله امنیت و نسبت آن با دیگر مباحث فناوری اطلاعات توجه کافی نشده است.

گستره مباحث و پراکندگی کارهای انجام شده تنها در زمینه امنیت اطلاعات به حدی است که متاسفانه جز در مواردی خاص، آن هم به صورت محدود، دانش ریشه ای در کشورمان وجود ندارد.

در این مقاله، کوشش شده است که مفاهیم اولیه امنیت الکترونیکی و نیازهای مطرح در این زمینه تعریف و توصیف و جایگاه آن تبیین گردد تا علاقه‌مندان به این رشته، به دیدگاهی جامع دست یابند. هچنین این مقاله، نیم نگاهی به راه‌حل‌های اساسی مرتبط با موضوعات مطرح شده دارد تا خواننده نسبت به آنچه که امروزه به عنوان فناوری‌های برتر در این زمینه شناخته شده است، دید مناسبی پیدا کند.

طی پیشرفت روز افزون فناوری الکترونیک، ابزارها و روش‌های جدیدی در خدمت تبادل اطلاعات قرار گرفته است. با وجود این که این ابزارها و روش‌های جدید، خود ملزومات و نیازمندی‌های نویی به همراه آورده‌اند، اما با نگاهی صرفا" کارکردی، هدف نهایی آنها، پاسخگویی به نیازهای سنتی است. [6][4] برای مثال، در مورد

امضای دیجیتال، در عین این که تنها طرح این مفهوم، نیازمندی‌های جدیدی را القا می کند، اما هدف اصلی از طرح مفهوم امضای دیجیتال، رسیدن به مفهوم سنتی امضا و احراز هویت، در قالب همیشگی آن است. بنابراین، به نظر می‌رسد که شناخت نیازمندی‌های فناوری الکترونیک، به ویژه بعد امنیتی آن، بدون شناخت دقیق نیازهای اولیه امنیت در تبادل اطلاعات، میسر نیست. بر این اساس، در این جا، در اولین قدم، به معرفی نیازمندی‌های اساسی سیستم‌های تبادل اطلاعات الکترونیکی پرداخته می‌شود.

تقسیم‌بندی‌های متنوعی در مورد اهداف بنیادین امنیت الکترونیکی وجود دارد، که کما بیش ناشی از برداشت‌های مختلف از موضوعی واحد است، به طوری که فصل مشترک این برداشت‌ها بسیار گسترده‌تر از وجوه تمایز آنها است.

جنبه‌های مختلف امنیت اطلاعات:

کلیه مشکلات، نیازها و راه‌حل‌های امنیتی را در سه دسته زیر می‌توان طبقه‌بندی کرد:

- **نفوذ:** هر عملی که امنیت داده‌ها را به هر شکلی زیر سوال ببرد.[2]

نفوذها، شامل تمام انواع حملاتی می‌شوند که توسط نفوذگر و به قصد انجام هر عمل غیرمجاز درباره‌ی داده‌ها انجام می‌گیرند.

نفوذها بر اساس تغییر دادن یا ندادن داده، به دو دسته فعال و غیر فعال تقسیم می‌شوند. نفوذهای فعال، تمام یا قسمتی از جریان داده را تغییر داده یا جایگزین می‌کنند. این نفوذ شامل ۴ نوع زیر است:

۱. **Masquerade**: رفتاری که بر اساس آن، نفوذگر خود را به جای فرد (یا ماشین) دیگری جا می‌زند.
۲. **Replay** : دریافت داده‌ها (در میانه راه) و فرستادن دوباره آن با هدف دست‌یابی غیر مجاز.
۳. **Modification**: ایجاد تغییر در داده‌های دریافتی غیر مجاز.
۴. **Denial of Service**: ایجاد مانع، یا جلوگیری کردن از استفاده یا مدیریت نرمال یک سرویس.

نفوذهای غیر فعال، برای گوش دادن یا monitor کردن یک جریان داده استفاده می‌شوند و تغییری در محتوای داده تبادلی انجام نمی‌دهند. معمولا این نفوذها، مقدمه انجام یک نفوذ فعال هستند.

- **مکانیزم امنیتی**: مکانیزمی که برای شناخت، پیش‌گیری یا درمان یک نفوذ امنیتی طراحی می‌شود.[2] در واقع هر مکانیزم، راه حلی برای نیازها و مشکلات امنیتی است.

مکانیزم‌های امنیت، انواع روش‌ها و روال‌های مورد استفاده برای مقابله با نفوذ و اثرات آن را بیان می کنند. **رمزنگاری**، اساسی‌ترین و مهم‌ترین این مکانیزم‌هاست که در این مقاله به آن خواهیم پرداخت.[2] از دیگر مکانیزم‌ها، می توان به امضای دیجیتال و کنترل دسترسی اشاره کرد.

- **سرویس امنیتی**: سرویسی که برای ارتقای وضعیت امنیت داده‌ها استفاده می‌شود.[2]

محقق شدن این سرویس‌ها، با استفاده از یک یا چند مکانیزم امنیتی امکان‌پذیر است. سرویس‌های امنیت را به نوعی می‌توان هدف کلی بحث امنیت اطلاعات دانست.

نظرات مختلفی درباره اهداف و اصول اولیه امنیت اطلاعات وجود دارد. البته باید در نظر داشت که نقاط اختلاف این برداشت‌ها تنها در میزان اهمیتی است که به عناصر مختلف آنها داده شده است و گرنه اساس این اصول یکسان است. مثلا، نویسنده کتاب "معماری امنیت ..." از موسسه استانداردهای RSA، **محرمانه بودن**، **جامعیت و در دسترس بودن** داده را از اهداف اولیه یک زیر ساخت امنیت اطلاعاتی می شمارد.[3]

در بعضی متون، **محرمانه بودن**، **جامعیت و سندیت** اطلاعات در این زمینه مطرح شده است.

در این مقاله، برای آشنایی بیشتر، اکثر قریب به اتفاق این اهداف یا سرویس‌ها به صورت زیر مطرح می‌شود:

۱. **محرمانه بودن**: تمام داده‌های ارسالی، فقط و فقط توسط کاربر مجاز، قابل دسترسی باشد.

۲. **جامعیت**: ارسال داده و هرگونه تغییر داده‌های دریافتی (در مسیر بین مبدا و مقصد) توسط کاربر مجاز انجام شده باشد.
۳. **تصدیق هویت**: هویت طرفین هر ارتباط، صحیح و مستند باشد.
۴. **سندیت**: عمل ارسال و دریافت و نیز محتوای داده نه توسط فرستنده و نه توسط گیرنده قابل انکار نباشد.
۵. **کنترل دسترسی**: توانایی محدود کردن و کنترل دست‌یابی به ماشین‌ها و نیز داده‌ها.
۶. **در دسترس بودن**: پیش‌گیری از محدود شدن یا از دست رفتن منابع داده‌ای، به ویژه در سیستم‌های توزیع شده مثل شبکه.

چه خطراتی این اهداف را تهدید می‌کند؟

بدون شک، نقش انکار ناپذیر نفوذگرها امروزه به عنوان بزرگ‌ترین عامل تهدیدکننده امنیت اطلاعات مطرح است. سال‌هاست که نفوذگرها، همگام با پیشرفت فناوری، روش‌های خود را به روز کرده اند. نقاط ضعف فراوان پروتکل‌ها و برنامه‌های کاربردی، اشتباهات کاربران و مدیران شبکه ها و ... به علاوه زیرکی و پشتکار مثال زدنی نفوذگرها، راه را برای خطرات همه جانبه امنیتی باز گذاشته است.

همان طور که در قسمت معرفی انواع نفوذ گفته شد، حملات غیر فعال، ساده‌ترین و حداقل کاری است که نفوذگر در مقابل جریان سالم تبادل داده انجام می‌دهد. به همین دلیل، اغلب فعالیت‌های تحقیقاتی از سال‌های دور تا کنون، بر این پایه استوار بوده که به نوعی اطمینان در صحت و سندیت داده‌ایجاد شود. روش‌های مختلف رمزنگاری و تصدیق هویت، راه‌حل‌هایی هستند که به طور عمیق مورد توجه قرار داشته‌اند.

- **حملات محتوایی**:

این حملات، متوجه محتوای داده ارسالی هستند. در ساده ترین حالت، نفوذگر سعی می‌کند که از محتوای داده ارسالی آگاه شود، به عنوان مثال، با زیر نظر گرفتن

ترافیک شبکه به صورت غیر مجاز. در نوع پیچیده‌تر، تلاش نفوذگر بر ایجاد تغییر دلخواه در محتوای داده‌ها استوار است.

رمزنگاری، راه حل سنتی:

رمزنگاری عبارت است از ایجاد تغییری در شکل داده، به وسیله یک کلید و به صورت برگشت پذیر. دو نوع اصلی رمز نگاری عبارت است از روش متقارن و روش نامتقارن. در روش متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌شود. در حالی که در روش نامتقارن، دو کلید وجود دارد، یک کلید عمومی که به صورت عمومی منتشر می‌شود و یک کلید خصوصی که فقط در اختیار صاحب جفت کلید است. این دو کلید به صورت مکمل یکدیگر عمل می‌کنند، یعنی داده‌ای که با یکی از آن دو رمز شده باشد، فقط و فقط به وسیله دیگری قابل رمزگشایی است. با کمک این ویژگی بسیار مهم، می‌توان محرمانه بودن، سندیت و جامعیت داده‌ها را تضمین کرد. اولا"، داده‌ای که با کلید عمومی گیرنده، رمز شده باشد، فقط با کلید خصوصی متناظر (که تنها در اختیار گیرنده است) قابل رمزگشایی است. بنابراین، در صورتی که نفوذگر به اطلاعات رمز شده دست یابد، مادامی که کلید خصوصی متناظر با کلید رمز کننده را در اختیار نداشته باشد، به داده اصلی دست پیدا نمی‌کند.

ثانیا"، اگر فرستنده، داده‌ای را با کلید خصوصی خود رمز کند، هر کس که کلید عمومی او را در اختیار داشته باشد، می‌تواند آن را رمزگشایی کند. این ویژگی، به دریافت کننده اطمینان می‌دهد که داده دقیقا" از طرف صاحب کلید عمومی فرستاده شده است. این، مفهوم عام امضای دیجیتال است که امروزه به گستردگی در تبادلات الکترونیکی کمک می کند.

گواهی‌های x.509 :[5]

کلید عمومی، نمایانگر هویت الکترونیکی صاحب آن است، بر این اساس، باید برای اثبات مالکیت آن، از سند خاصی که " گواهی دیجیتال " نامیده می‌شود، استفاده کرد. فرمت و شکل این گواهی‌های دیجیتال، توسط IETF در استاندارد X.509 مشخص

شده است. در این گواهی، اطلاعات لازم برای اثبات هویت صاحب کلید عمومی، به این کلید متصل (bind) می‌شود. برنامه‌های کاربردی، از این اطلاعات برای برقراری رابطه اطمینان (Trust Relationship) استفاده می‌کنند.

مدیریت گواهی‌های کلید عمومی، اعم از تولید، انتشار و ابطال آنها از بزرگ‌ترین چالش‌های فراروی فناوری امنیت است. به طوری که برای این منظور، PKI یا زیرساخت کلید عمومی به عنوان راه حل جامع پیشنهاد شده است. PKI عبارت است از یک زیرساخت یا framework، شامل نیروی انسانی، تجهیزات سخت افزاری و نرم افزاری (به خصوص در زمینه شبکه) و پروتکل‌های ارتباطی و مدیریتی که امکان استفاده از گواهی‌های کلید عمومی و مدیریت آنها را در امور مربوط به رمزنگاری فراهم می‌کند. یکی از مشکلات عمده این راه حل، هزینه سرسام آور آن، به خصوص در کاربردهای بزرگ است. به طوری که امروز جز در کاربردهای کوچک و متوسط، از آن استفاده نمی‌شود. از کاربردهای امروزین این زیرساخت، می‌توان به پروتوکل SSL که برای امن کردن اتصالات وب، FTP و ... به کار می‌رود، اشاره کرد.

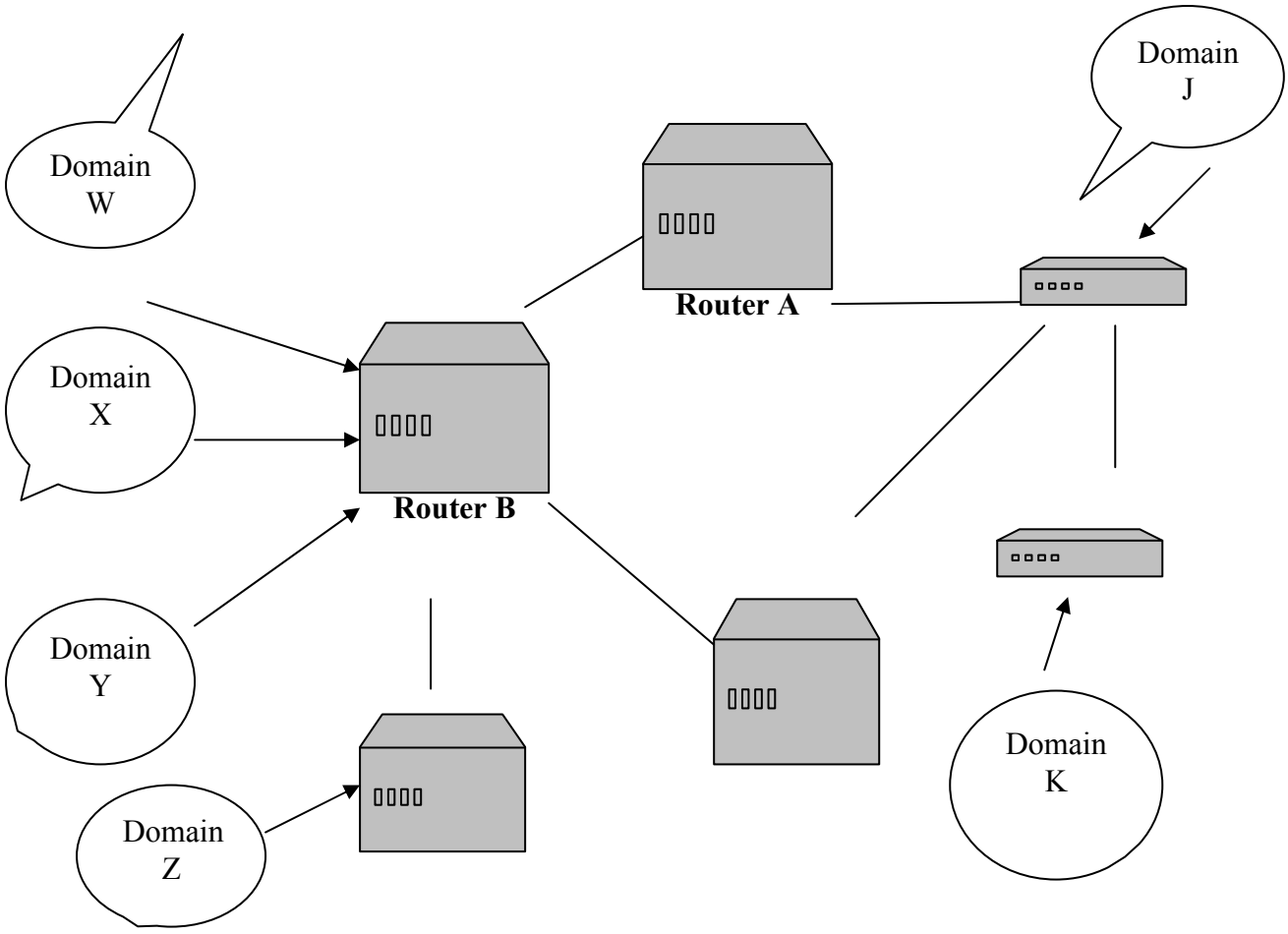
همان طور که بیان شد، رمزنگاری با وجود برخی مشکلات و نارسایی‌های تئوریک و عملی، راه‌حل مناسب و مطلوبی برای محافظت از محتوای داده‌هاست. اما باید توجه داشت که بستر تبادل اطلاعات الکترونیکی، ابزارهایی هستند که هر گونه خلل در آنها، می‌تواند اهداف بنیادی امنیت را به خطر اندازد. این ابزارها، به خصوص شامل تمام تجهیزات شبکه‌ها هستند. بنابراین، توجه به مسایل ابزارهای زیرساختی شبکه، بسیار حساس و با اهمیت است و باید بیش از پیش مورد توجه قرار گیرد.

- حملات ساختاری :

این نوع حمله متوجه زیرساخت شبکه از قبیل مسیریاب‌ها، سرویس دهنده‌ها و ... است. یک نکته بسیار مهم این است که ساختار و شیوه حملات یاد شده به شکلی است که حمله کننده را به شدت از دیدها پنهان و شناخت حمله را بسیار مشکل می‌کند.[1]

در شکل زیر، نفوذگر قصد حمله به شبکه Z را که شامل چند سرویس دهنده پرترافیک است، دارد. فرض کنید که اتصال بین مسیریاب‌های A و B دارای هزینه

۱۰۰۰ باشد. نفوذگر A با تلاش خود موفق به دستیابی به مسیریاب A و تغییر این هزینه به عددی بسیار بزرگ مثل ۱۰۰۰ می‌شود. این عمل باعث می‌شود که مسیریاب B، کلیه بسته‌های به مقصد J و K را از طریق مسیریاب C بفرستد. بر این اساس، مسیریاب C در بر اثر ترافیک بسیار بالا، به اصطلاح Congest شده و از کار باز می‌ماند. این به معنای وقوع یک نفوذ از نوع DoS علیه شبکه های W، X، Y و Z است. همان طور که در این مثال ساده نشان داده شد، این نوع نفوذ، نه تنها ردپای قابل توجهی از نفوذگر به جا نمی‌گذارد، بلکه به شدت دیرتشخیص است.[1]



نمونه‌های نفوذهای زیرساختی بسیار گسترده و از نظر مشخصات متنوع است. بنابراین خوب است که تقسیم بندی مناسبی از آنها ارایه شود.

حملات زیر ساختی، به ۴ دسته عمده تقسیم می‌شوند:

۱. نفوذهای DNS

سیستم DNS یک دایرکتوری سراسری (جهانی) و توزیع شده است که نام ماشین/دامنه را به IP مربوطه ترجمه می‌کند.[1] در زمان نگارش این مقاله یعنی خردادماه ۱۳۸۲، تعداد ۱۴ سرویس دهنده دامنه سطح بالا(TLD) (مانند com.، org.، edu. و...) وجود داشته است. www.icann.org

هدف از نفوذهای DNS، هرگونه اخلال در سیستم خدمات DNS است. از آنجا که DNS یکی از حیاتی‌ترین سرویس‌های شبکه‌های اطلاع رسانی است که با تمام سرویس دهنده‌ها، اتصالات، کاربران و ... مرتبط است این نوع نفوذ ساختاری، پتانسیل بسیار بالایی برای تاثیر گذاشتن بر بخش عظیمی از شبکه‌های اطلاع‌رسانی را دارد.[1]

برخی از مهم‌ترین اثرات این نفوذ عبارت‌اند از:

- اثر Denial of Service، از طریق ارسال پاسخ‌های منفی مبنی بر موجود نبودن آدرس مورد نظر، یا redirect کردن درخواست به آدرسی غیر از آنچه که سرویس گیرنده خواسته است.
- اثر Masquerade، به این معنا که نفوذگر، درخواست را ابتدا به آدرسی Redirect کرده و سپس خود به عنوان موجود مورد اطمینان، وارد ارتباط شده و به تبادل داده با سرویس گیرنده می پردازد. مثلا، کاربر به جای سایت یاهو، به سایت شخصی نفوذگر هدایت می‌شود، در حالی که صفحه وب یاهو در برابرش قرار دارد و به ارسال نام کاربر و کلمه عبور خود به سمت نفوذگر می پردازد!

یکی از راه حل‌های ارایه شده برای امن تر کردن سرویس DNS، پروتکل DNSSEC است که توسط IETF پیشنهاد شده است. پروتکل DNSSEC نوعی ساز و کار تصدیق هویت را براساس مفهوم امضای دیجیتال، برای سرویس DNS پیشنهاد می‌کند. [1]

۲. نفوذهای دستکاری Routing Table

طراحان پروتکل‌های مسیریابی، از ابتدا اهمیت لازم را به مساله امنیت نداده اند.[1] به همین خاطر، مسیریاب‌ها همواره از مشکل سازترین ابزارها در شبکه بوده‌اند.
مسیریاب‌های شبکه هدف اولیه این نفوذ هستند که غالبا وظایف خود را با کمک Routing Table های خود انجام می‌دهند. نفوذگر تلاش می‌کند که با اعمال تغییر یا خرابکاری در Routing Table، مسیریاب را به اشتباه انداخته و قسمت بزرگی از backbone شبکه (نه فقط یک ماشین) را از کار بیاندازد.

اثرات این نفوذ به اختصار عبارت‌ند از:

- مسیریابی غیر بهینه که باعث هدر رفتن زمان به خصوص برای برنامه‌های Real Time می‌شود.[1]
- تراکم ترافیک و به عبارت دیگر Congest شدن یک یا چند مسیریاب.
- ایجاد زیر شبکه‌های مصنوعی و ناخواسته، به طوری که باعث دسترسی نداشتن بعضی host ها به یکدیگر شود.
- ایجاد دور در چند مسیریاب بر اثر تبادل بسته های update غلط.

اثرات و نتایج دستکاری Routing Table، بسیار گسترده است که در بالا فقط به چند مورد مهم‌تر اشاره شد. طبیعت وظایف یک مسیریاب طوری‌ست که در صورت مورد حمله قرار گرفتن، می‌تواند به مشکل بسیار بزرگی برای تبادل صحیح اطلاعات تبدیل گردد و به عبارت دیگر، نفوذ یاد شده، پتانسیل بسیار بالایی برای تبدیل شدن به یک نفوذ DoS کشنده را داراست.[1]
راه‌حل‌های مختلفی برای حالات مختلف این حمله پیشنهاد شده است. از جمله می‌توان به استفاده از امضای دیجیتال در بسته های update اشاره کرد که البته مستلزم وجود یک PKI در شبکه یاد شده است. از دیگر راه‌حل‌ها می‌توان به افزودن اطلاعات تکمیلی مثل بسته‌های acknowledgement و sequence number اشاره کرد.

۳. نفوذهای مبتنی بر بدرفتاری بسته‌ها

در این نوع از حملات، نفوذگر با اعمال تغییر در بسته‌های داده، باعث ایجاد اثری نامتعارف یا خرابی می‌شود.[1] بر این اساس، این نوع حمله، درست در زمان تبادل بسته‌های اطلاعات، انجام می‌شود.

یکی از مشکلات اساسی در شبکه‌های موجود، آن است که پروتکل TCP IP فرض می‌کند که همه آن طور که انتظار می‌رود رفتار می‌کنند و هیچ کس کاری بر خلاف استاندارد آن انجام نمی‌دهد. به همین دلیل، یک نفوذگر می‌تواند به عنوان مثال، با ایجاد ترکیبی غیر متعارف از مقادیر flag های یک بسته TCP، باعث وقوع حالتی شود که در پیاده سازی پروتکل پیش بینی نشده است، چرا که پروتکل فرض کرده است که این ترکیب نامتعارف، ایجاد نخواهد شد. بر این اساس، نفوذگر با استفاده از این نقطه ضعف و نیز دیگر ویژگی‌های شبکه، بسته را طوری تغییر می‌دهد که خرابکاری به بار آید.

بعضی از اثرات این نفوذ عبارت‌اند از:

- مسیریابی اشتباه و تراکم ترافیک و congest شدن قسمتی از شبکه.
- کاهش بازده شبکه.
- DoS، به وسیله هدایت غیرمستقیم بسته‌های فراوان (به عنوان مثال، درخواست TCP Connection) به یک سرویس دهنده و ایجاد Load کشنده در آن.

برای شناخت نفوذ بالا، راه‌حل‌های چندی پیشنهاد می‌شود، از جمله ایجاد یک سیستم Intrusion Detection یا IDS، که یکی از راه‌حل‌های جدید و به شدت مورد توجه متخصصان امنیت است. اساس کار IDS، ابتدا شناخت نفوذ از درون شبکه (نه از gateway آن) و در مراحل پیشرفت‌تر، انجام اموری برای پیش‌گیری از نفوذ است. البته IDS ها همه روزه در حال پیشرفت‌اند و توانایی‌های آنها افزون می‌شود.[3]

یکی دیگر از راه‌حل‌ها، استفاده از یکی از قابلیت‌های پروتکل IPsec است که در ایجاد شبکه‌های خصوصی مجازی (VPN) کاربرد دارد.[1]

۴. نفوذهای DoS

این نوع حمله، به راحتی قابل انجام و به سختی قابل شناسایی است. هدفش آن است که یک سرویس دهنده، برای مدتی (مثلا چند ساعت) از سرویس دهی مناسب به کاربران باز ماند.

این نوع حمله، عموما" در انواع عادی و توزیع شده طبقه‌بندی می‌شود. در نوع عادی، معمولا" از نرم‌افزارهای خاصی برای تولید و ارسال بسته‌ها به ماشین هدف، استفاده می‌شود. این نوع حمله، معمولا با IP Spoofing (تغییر غیرمجاز IP نفوذگر) همراه است تا دیرتر شناخته شود.[1]

در نوع توزیع شده، از چندین ماشین مختلف و گاه تا ۱۰۰۰ ماشین (!!) برای حمله به یک ماشین هدف، استفاده می‌شود. اثر حمله توزیع شده، می‌تواند بسیار شدیدتر از نوع عادی باشد. بسیاری از خصوصیت‌های پروتکل‌هایی همچون TCP، UDP و ICMP می‌تواند در خدمت حملات DoS قرار گیرد.

دیواره‌های آتش و IDها در شناخت و جلوگیری از اغلب انواع حملات DoS به کار می‌روند. این سیستم‌ها، برای هر حمله قواعدی را به عنوان نشانه در نظر داشته و در صورت یافتن آنها، از ادامه جریان بسته‌ها جلوگیری می‌کنند.

نقش ابزارهای امنیتی:

سخت افزارها و نرم افزارها، امروزه به عنوان بستر و ساز و کار امنیت در شبکه‌های کامپیوتری مطرح هستند. از آنجا که راه‌حل‌ها، همگی مبتنی بر مجموعه‌ای از سیستم‌های سخت‌افزاری و نرم‌افزاری هستند، لازم است که به صورت اجمالی به مهم‌ترین و پرکاربردترین این سیستم‌ها پرداخته شود.

اما پیش از آن بیان یک نکته‌ی بسیار مهم در این جا ضروری است. باید توجه داشت که امور مدیریتی در زمینه امنیت، کم اهمیت تر از امور فنی نیستند. هر کاربر، باید در حد نیاز، آموزش دیده و مسئولیت بپذیرد. در این زمینه، سیاست‌های امنیتی یا Security Policy ها، نقش اساسی ایفا می کنند. این سیاست‌ها، مجموعه رفتارها، اعمال و مسئولیت‌های هر کاربر را مشخص می کنند.[6][4]

علاوه بر این، تمام بایدها و نبایدها، و جزییات راه‌حل‌های امنیتی، باید برای برآورده ساختن سیاست‌های امنیتی به کار روند.
با عنایت به نقش محوری سیاست‌های امنیتی، در این جا، مروری بر مهم‌ترین ابزارهای امنیت امروزی می‌شود.

۱. دیواره آتش

دیواره آتش یا firewall، اساسا" سیستمی است نرم افزاری، که بر اساس قواعدی موسوم به rule، ترافیک یک شبکه را کنترل می‌کند. ایده کلی آن است که تمام ورود و خروج بسته‌ها، از یک نقطه به نام gateway (به صورت منطقی یا فیزیکی) صورت گیرد و در آنجا کنترل ورود و خروج بسته‌ها بر اساس تطابق آنها با rule ها انجام شود.

مهم‌ترین انواع دیواره‌های آتش عبارت‌اند از:

- Packet filter: نرم‌افزاری که تنها بر اساس header یک بسته، در مورد قبول (Accept) یا رد (Drop) آن تصمیم می‌گیرد. این نوع دیواره آتش، ارزان و البته نسبت به انواع دیگر، ساده و ضعیف است.
- Application Proxy: نرم‌افزاری که به جای درخواست دهنده یک سرویس، به ارسال درخواست و دریافت پاسخ می پردازد. این نرم‌افزارها، از لحاظ امنیتی قابل قبول، اما محدود به applicationهای خاصی هستند.
- Stateful Inspection: نرم افزاری که علاوه بر موارد قبلی، به ارتباط بسته‌ها با یکدیگر، به عبارتی نوع Connection هر بسته و بسته‌های پیش و پس از آن می پردازد. هر بسته، دارای یک state است که در تمام طول عمر آن نگهداری می‌شود و بر اساس مقدار state می‌توان بسته را رد یا قبول کرد. این نوع نرم‌افزار، بسیار قوی و در عین حال دارای load بسیار بالایی است. امروزه عملا" دیواره آتشی که از این قابلیت پشتیبانی نکند، مفید نخواهد بود.

۲. **سیستم تشخیص نفوذ (IDS)**

همان طور که پیش‌تر اشاره شد، این سیستم بـر اسـاس داده واردشـده، در درون شبکه (و نه gateway آن) به بررسی فعالیت‌های کاربران و ماشین‌هـا می پردازد. هدف اولیه IDS بازرسی ترافیک است و نه فیلتر کردن آن. [2]

۳. **ظرف عسل (Honey pot)**

یکی از ایده‌های جدید و جالب مطرح، استفاده از سیستمی است که نفوذگر را به سمت خود بکشاند. در این سیستم، یک یا چند ماشین، به صـورت واقعـی یا مجازی شبکه‌ای را تشکیل می‌دهند که از نقاط ضعف امنیتی پر است. ایـن امر به راهبر شبکه اجازه می‌دهد که اولا" کسانی را که علاقه به نفوذ دارنـد، و ثانیا" نوع نفوذهای مورد علاقه آنها را شناسایی کند.

نتیجه گیری:

امنیت، به عنوان محور مباحث فناوری اطلاعات، امروزه به شدت مورد توجه است. پراکندگی و پیچیدگی موضوعات در این زمینه به حـدی‌سـت کـه امـر آموزش آن را بسیار حساس و پیچیده کرده است. امروز باید درکـشورمان به امر آموزش و پژوهش آکادمیک ایـن رشـته توجـه ویـژه شـود. همچنـین زمینه‌های خودکفایی تکنولوژیک هم باید مد نظر قرار گیرد.

دانش امنیت اطلاعات بسیار حساس و با ارزش اسـت. بـا وجـود تهدیـدهای مختلف در زمینه امنیت اطلاعات، راه برای کارهـای پژوهـشی و صـنعتی در این زمینه بسیار هموار است.

منابع:

[1] Anirban Chakrabarti and G. Manimaran, "**Internet Infrastructure Security: A Taxonomy**", IEEE Network, November/December 2002

[2] "**Cryptography and Network Security Principles & Practices"**, William Stallings, Third Edition, 2002.

[3] "**Security Architecture, Design, Deployment & Operations**", Christopher M.King, Curitis E.Dalton, RSA Press.

[4] "**Addressing New Security and Privacy Challenges**", Anup K.Ghosh, IEE IT Professional, May/June 2002

[5] RFC 2510. "**Certificate Management Protocol**", IETF standard RFCs.

[6] "**Opening Eyes: Building Company-Wide IT Security Awareness**", Mark McGovern, IEEE IT Professional, May/June 2002