بنام خدا

بهنام فرزانه

شماره دانشجویی : ۹۴۱۴۷۳۴

سوالات سمینار درس امنیت شبکه

موضوع سمینار: تشخیص نفوذ در اینترنت اشیاء

استاد مربوطه : آقای دکتر فانیان

۱. مفهوم اینترنت اشیاء و فازهای مربوط به عملیات اینترنت اشیاء را بیان کنید؟

اصطلاح اینترنت اشیاء یا IoT برای اولین بار توسط کوین اشتون، مدیر مرکز Auto-ID در MIT در سال ۱۹۹۹ ارائه شد. مفهوم اصلی اینترنت اشیاء، توسعه هوشمندی محیط و کنترل مستقل است. درواقع اینترنت اشیاء به عنوان یک زیرساخت جهانی پویا تعریف شده است با قابلیت خودپیکربندی مبتنی بر پروتکل‌های سازگار و استاندارد که در آن اشیاء فیزیکی و مجازی، هویت، خصوصیات فیزیکی و شخصیت مجازی دارند و قادر به استفاده از رابط‌های هوشمند هستند و به عنوان یک شبکه اطلاعاتی یکپارچه شده اند.

عملیات IoT شامل سه فاز متمایز است: فاز جمع‌آوری، فاز انتقال، فاز پردازش و مدیریت و بهره‌وری. در فاز جمع‌آوری هدف جمع‌آوری داده درمورد محیط فیزیکی است. این فاز اشاره به LLNها دارد. فاز انتقال به انتقال داده جمع‌آوری شده در فاز قبلی به برنامه‌های کاربردی و متعاقباً به کاربران کمک می‌کند. در فاز آخر، برنامه‌های کاربردی، داده را برای به دست آوردن اطلاعات درمورد محیط فیزیکی پردازش می‌کنند.

۲. شبکه‌های کم‌توان و پراتلاف چه نوع شبکه‌هایی هستند؟

اشیای هوشمند معمولی دارای چندین کیلوبایت حافظه، یک میکروکنترلر کوچک و منبع انرژی محدود می‌باشند اما می‌توانند شبکه‌های حسگری که به طور بالقوه متشکل از صدها هزار گره می‌باشند را تشکیل دهند. اینگونه شبکه‌ها به طور معمول به عنوان شبکه‌های کم‌توان و پراتلاف یا LLN شناخته می‌شوند و این نام برگرفته از محدودیت جدی انرژی و گسترش این شبکه‌ها در محیط‌های غیرقابل پیش‌بینی می‌باشد. تجهیزات شبکه‌های کم‌توان و پراتلاف دارای منابع محدود ازقبیل پردازشگر، حافظه، باتری و ارتباط رادیویی ناپایدار می‌باشند. اندازه کوچک، توان کم و هزینه پایین تولید تجهیزات اینگونه شبکه‌ها محدودیت منابع در آنها را موجب می‌شود.

۳. شبکه‌های 6lowpan به چه شبکه‌هایی گفته می‌شود؟

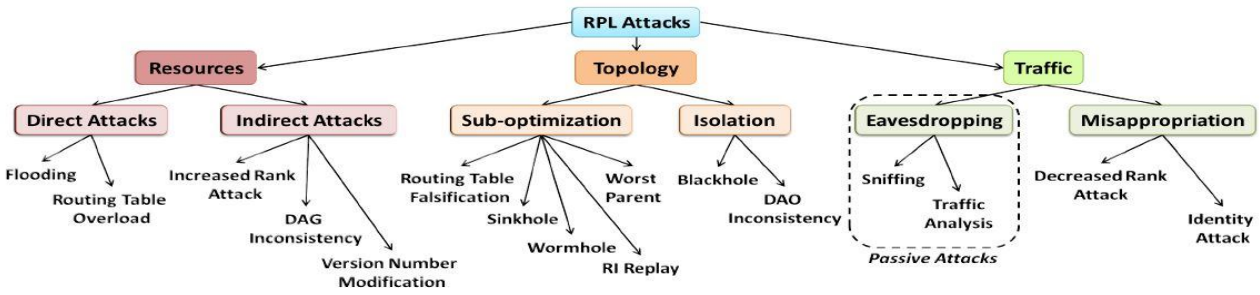
شبکه حوزه‌ی شخصی بی‌سیم کم‌توان روی IPV6 ، یک شبکه ارتباطی کم‌توان و کم‌هزینه است که دستگاه‌های بی‌سیم منبع محدود، معمولاً حسگرهای بی‌سیم یا محرک‌ها را با استفاده از IPV6 متصل می‌کند. همچنین، یک فشرده‌سازی سرآیند تعریف می‌کند و مشخص می‌کند که چطور بسته‌ها در شبکه‌های بی‌سیم مسیریابی شوند که از پروتکل IEEE 802.15.4 در لایه لینک و فیزیکی استفاده می‌کند. همچنین تکه‌تکه‌شدن داده‌گرام IPV6 را تعریف می‌کند، وقتی که اندازه داده‌گرام بیشتر از ۱۲۷ بایت باشد که حداکثر واحد انتقال IEEE 802.15.4 می‌باشد. شبکه‌های 6LOWPAN ارتباطات چندگامی یا Multihop را پشتیبانی می‌کنند که گره‌ها می‌توانند بسته‌ها را به نمایندگی از سایر گره‌ها ارسال بکنند. انرژی یکی از منابع کمیاب در شبکه‌های 6LOWPAN می‌باشد. با توجه به اتصال جهانی IP، این شبکه‌ها نسبت به بیشتر حملات موجود در برابر شبکه‌های حسگر بی‌سیم به علاوه حملات از اینترنت آسیب‌پذیر است.

۴. درمورد پروتکل مسیریابی RPL در شبکه‌های کم‌توان و پراتلاف توضیح دهید؟

RPL، پروتکل مسیریابی IPV6 برای شبکه‌های کم‌توان و پراتلاف و یک پروتکل مسیریابی استاندارد برای اینترنت اشیاء است. RPL در درجه اول در یک شبکه 6LOWPAN استفاده می‌شود. این پروتکل، یک گراف جهت‌دار بدون دور مقصدگرا (DODAG) بین گره‌ها در یک 6LOWPAN ایجاد می‌کند. همچنین، ترافیک یک‌سویه به سمت یک ریشه گراف جهت‌دار بدون دور مقصدگرا و ترافیک دوسویه بین دستگاه‌های 6LOWPAN و بین دستگاه‌ها و ریشه‌ی DODAG (معمولاً 6BR) را پشتیبانی می‌کند. RPL پروتکل فعال است و به محض شروع کار شبکه شروع به مسیریابی می‌کند. در شبکه هر گره یک سرخوشه دارد که مانند درگاه برای آن گره عمل می‌کند. اگر گره برای هدایت بسته اطلاعاتی در جدول مسیریابی خود برای آن بسته نداشته باشد، آن را به گره سرخوشه خود هدایت می‌کند. این هدایت تا جایی ادامه خواهد داشت که گره به مقصد یا به گره سینک برسد که اطلاعات مربوطه را داشته باشد. گره سرخوشه بنابراین دارای جدول مسیریابی بزرگتری خواهد بود. انتخاب مسیر یکی از فاکتورهای مهم در RPL است. بسته‌هایRPL می‌توانند بر اساس سه الگوی ترافیکی ارسال شوند: ترافیک چند نقطه‌ای به تک نقطه‌ای از برگها به سمت ریشه با مسیرهای روبه بالا- تک نقطه‌ای به چند نقطه‌ای از ریشه به سمت برگها با استفاده از مسیرهای رو پایین - نقطه به نقطه با استفاده از هر دو مسیر رو به بالا و رو به پایین. پروتکل مسیریابی RPL می‌تواند به حملات مسیریابی در برابر شبکه‌های حسگر بی‌سیم و همچنین به حملات در برابر اینترنت اشیاء آسیب‌پذیر باشد.

۵. حملات روی پروتکل مسیریابی RPL به چند دسته تقسیم می‌شوند؟

حملات روی RPL به سه دسته تقسیم میشود: دسته اول، حملات اتلاف منابع شبکه(انرژی، حافظه و توان) را پوشش میدهد .این حملات به طور خاص به چنین شبکه‌های محدودی آسیب میرسانند، به این دلیل که آنها تا حد زیادی طول عمر دستگاه‌ها و درنتیجه طول عمر RPL را کاهش می‌دهند .دسته دوم، شامل حملات با هدف توپولوژی شبکه RPL است و عملکرد عادی شبکه را مختل می‌کنند. دسته سوم، مربوط به حملات در مقابل ترافیک شبکه هستند. در شکل زیر دسته‌بندی حملات علیه RPL با جزئیات آمده است.



۶. علی‌رغم بلوغ فناوری سیستم تشخیص نفوذ برای شبکه‌های سنتی، چرا راه حل‌های فعلی برای سیستم‌های اینترنت اشیاء کافی نیستند، توضیح دهید؟

به دلیل ویژگی‌های خاص IoT که توسعه سیستم تشخیص نفوذ را تحت تاثیر قرار می‌دهد، راه‌حل‌های فعلی برای سیستم‌های IoT ناکافی هستند. در ابتدا، ظرفیت حافظه و پردازش نودهای شبکه که میزبان عامل‌های سیستم تشخیص نفوذ هستند، یک مسئله مهم است. شبکه‌های IoT از نودهای با منبع محدود تشکیل می‌شوند. بنابراین پیدا کردن نودها با توانایی پشتیبانی از عامل‌های سیستم تشخیص نفوذ در سیستم‌های IoT سخت‌تر است. دوم، ویژگی‌های عملی مرتبط با معماری شبکه است. در شبکه‌های سنتی، سیستم‌های انتهایی مستقیماً به نودهای خاص مثل سوییچ و روتر متصل هستند که مسئول انتقال بسته‌ها به مقصد هستند اما شبکه‌های IoT معمولاً به صورت multihop هستند و نودهای عادی ممکن است به صورت همزمان بسته‌ها را انتقال دهند و به عنوان سیستم انتهایی عمل کنند. ویژگی آخر مرتبط با پروتکل‌های شبکه است. شبکه‌های IoT پروتکل‌هایی استفاده می‌کنند که در شبکه‌های سنتی قرار نگرفته‌اند، مثل IEEE 802.15.4، Lowpan، RPL و Coap.

۷. از نیازمندی‌های سیستم تشخیص نفوذ در اینترنت اشیاء چند مورد را نام ببرید؟

اجرای سریعتر-حافظه مورد استفاده کوچکتر-کاهش محاسبات-داشتن تنوعی از داده یادگیری-نیازمندی‌های کم ادغام داده.

۸. دسته‌بندی سیستم تشخیص نفوذ در اینترنت اشیاء را براساس متد تشخیص شرح دهید؟

دسته‌بندی براساس متد تشخیص به صورت مبتنی بر امضاء، مبتنی بر ناهنجاری، مبتنی بر مشخصات و ترکیبی است.

در حالت مبتنی بر امضا، الگوهای نفوذ از پیش ساخته شده (امضاء) به صورت قانون نگهداری می‌شوند .به طوری که هر الگو انواع متفاوتی از یک نفوذ خاص را در بر گرفته و در صورت بروز چنین الگویی در سیستم، وقوع نفوذ اعلام می‌شود. در این روش ها، معمولاً تشخیص دهنده دارای پایگاه داده ای از امضاء ها یا الگوهای حمله است و سعی می‌کند با بررسی ترافیک شبکه، الگوهای مشابه با آنچه را که در پایگاه داده خود نگهداری می‌کند، بیابد .این دسته از روش‌ها تنها قادر به تشخیص نفوذهای شناخته شده می‌باشند و در صورت بروز حملات جدید در سطح شبکه، نمی‌توانند آن‌ها را شناسایی کنند و مدیر شبکه باید همواره الگوی حملات جدید را به سیستم تشخیص نفوذ اضافه کند. از مزایای این روش دقت در تشخیص نفوذهایی است که الگوی آنها عیناً به سیستم داده شده است.

در حالت مبتنی بر ناهنجاری، یک نما از رفتار عادی ایجاد می‌شود. یک ناهنجاری ممکن است نشان دهنده یک نفوذ باشد. برای ایجاد نماهای رفتار عادی از رویکردهایی از قبیل شبکه‌های عصبی، تکنیک های یادگیری ماشین و حتی سیستم های ایمنی زیستی استفاده می شود که ممکن است برای نودهای ظرفیت پایین شبکه‌های IoT خیلی سنگین باشد. بنابراین رویکردهای مبتنی بر ناهنجاری برای شبکه‌های IoT باید این خصوصیات را به حساب بیاورند. برای تشخیص رفتار غیرعادی، باید رفتارهای عادی را شناسایی کرده و الگوها و قواعد خاصی برای آن ها پیدا کرد. رفتارهایی که از این الگوها پیروی

می کنند، عادی بوده و رویدادهایی که انحرافی بیش از حد معمول آماری از این الگوها دارند، به عنوان رفتار غیرعادی تشخیص داده می شود .نفوذهای غیرعادی برای تشخیص بسیار سخت هستند، چون هیچگونه الگوی ثابتی برای نظارت وجود ندارد. معمولاً رویدادی که بسیار بیشتر یا کمتر از دو استاندارد انحراف از آمار عادی به وقوع می پیوندد، غیرعادی فرض می شود.

در حالت مبتنی بر مشخصات، یک کارشناس باید به طور manually و دستی قوانین هر مشخصات را تعریف کند. نفوذ زمانی تشخیص داده می‌شود که رفتار شبکه از تعاریف مشخصات منحرف شوند. در این حالت نیاز به فاز آموزشی نیست و فوراً پس از تنظیم مشخصات می‌توانند شروع کنند. با این حال ممکن است مشخصات دستی تعریف‌شده ممکن است با محیط‌های سازگار نباشد و مستعد خطا و مصرف زمان باشد.

در حالت ترکیبی، ترکیبی از حالت‌های فوق استفاده می‌شود.

۹. دسته‌بندی سیستم تشخیص نفوذ در اینترنت اشیاء را براساس معماری سیستم تشخیص شرح دهید؟

دسته‌بندی براساس معماری سیستم تشخیص به صورت Stand-Alone ، Distributed & Cooperative ، Hierarchical و Mobile Agent است.

Stand-Alone : هر نود ناظر اطلاعات را جمع‌آوری کرده و تشخیص نفوذ را خودش انجام می‌دهد. نود ناظر ممکن است متمرکز یا توزیع‌شده باشد. در معماری با نود ناظر متمرکز، هر نود شبکه به عنوان یک نود ناظر عمل می‌کند.در معماری با نود نود ناظر توزیع‌شده، هر نود ناظر ناحیه خاصی از شبکه را نظارت می‌کند و هر نود حسگر باید داخل ناحیه حداقل یک نود ناظر باشد. هر نود ناظر تشخیص نفوذ مستقلی دارد.

Distributed & Cooperative : عامل‌های سیستم تشخیص نفوذ روی هر نود ناظر اجرا می‌شوند. کل نودهای ناظر در روال تشخیص نفوذ همکاری دارند. عامل سیستم تشخیص نفوذ رفتار نودهای همسایه‌اش را نظارت می‌کند اما داده تبادل یافته و هشدارها با نود ناظر دیگری از کل شبکه، در تصمیم‌گیری کلی شرکت دارند. چنین سیستمی، کارایی تشخیص را بهبود می‌بخشد. این معماری مناسب زیرساخت شبکه با یک DODAG است.

Hierarchical : مناسب برای شبکه حسگر خوشه‌بندی شده با ساختار سلسله مراتبی است. شامل چندین DODAG (با نود سینک مشترک) است. هر خوشه، عامل سیستم تشخیص نفوذ سرخوشه دارد و عامل‌های محلی داخل خوشه هستند (مثل Stand-Alone) و عامل‌های سیستم تشخیص نفوذ سرخوشه متصل هستند و در فرآیند تشخیص نفوذ همکاری می‌کنند.

Mobile Agent : چندین عامل‌های موبایل را برای انجام فرآیند تشخیص نفوذ به طور همکارانه به کار می‌گیرد. تحرک عامل‌های سیستم تشخیص نفوذ ممکن است کارایی سیستم تشخیص نفوذ را بهبود بخشد. عامل‌های موبایل به عنوان یک

سگمنت برنامه خودکنترلی، یک کد قابل اجرای خاص است که از یک نود به نود دیگری حرکت می‌کند. در این مهاجرت عامل، که به معنی حرکت یک عامل از یک نود به دیگری است، علاوه بر انتقال داده، محاسبات نیز انجام می‌شود.

۱۰. دسته‌بندی سیستم تشخیص نفوذ در اینترنت اشیاء را براساس استراتژی قرارگیری سیستم تشخیص شرح دهید؟

دسته‌بندی براساس قرارگیری سیستم تشخیص به صورت توزیع شده، متمرکز، ترکیبی است.

در حالت توزیع شده، سیستم تشخیص نفوذ در هر شی فیزیکی از LLN قرار می‌گیرد. سیستم تشخیص نفوذ مستقرشده در هر نود باید بهینه شود و منابع محدود هستند. در این استراتژی، نودها ممکن است مسئول نظارت همسایگان باشند. نودهایی که همسایه‌های خود را نظارت می‌کنند به عنوان watchdog در نظر گرفته می‌شوند.

در حالت متمرکز، سیستم تشخیص نفوذ در یک مولفه متمرکز برای مثال در روتر مرزی یا یک میزبان اختصاصی قرار می‌گیرد. همه داده‌های گره‌های LLN جمع‌آوری و از طریق روتر مرزی به اینترنت متصل می‌شوند . همچنین درخواست‌های کاربران اینترنت به گره‌های LLN می‌فرستند. بنابراین سیستم تشخیص قرار گرفته در روتر مرزی می‌تواند همه ترافیک تبادل‌یافته بین LLN و اینترنت را آنالیز کند. با این حال آنالیز ترافیک که از روتر مرزی می‌گذرد برای تشخیص حملات شامل نودهای داخل LLN کافی نیستند و باید سیستم تشخیصی طراحی شود که بتواند ترافیک تبادل یافته بین گره‌های LLN را نظارت کند.

در حالت ترکیبی، رویکرد اول، شبکه را داخل خوشه‌ها یا نواحی سازماندهی می‌کند و فقط گره اصلی هر خوشه میزبان یک نمونه سیستم تشخیص نفوذ می‌باشد. بنابراین این نود مسئول نظارت گره‌های دیگر خوشه است. رویکرد دوم، ماژول‌های سیستم تشخیص نفوذ در روتر مرزی و در نودهای دیگر شبکه قرار گرفته‌اند. تفاوت اصلی این رویکرد با اولی در حضور یک مولفه مرکزی است.ماژول سیستم تشخیص نفوذ در روتر مرزی مسئول وظایفی است که متقاضی ظرفیت منبع بیشتر است درحالی که ماژول‌های سیستم تشخیص نفوذ در نودهای عادی معمولاً سبک هستند.