
بسم الله الرحمن الرحیم

سمینار

عنوان

مطالعه و ارزیابی روش های ایجاد امنیت در سیستم‌های نهفته

نگارنده:

چکیده

سیستم‌های نهفته، کامپیوترهای کوچکی هستند که عضوی از سیستم یا ماشین بزرگ‌تر بوده و وظیفه یا کار خاصی را انجام می‌دهند. این سیستم‌ها معمولا برنامه‌های محدودی را اجرا می‌کنند که غالبا از نوع کنترلی هستند، به همین دلیل امنیت در این سیستم‌ها به یکی از مهمترین چالش‌ها تبدیل شده است. کشف حمله یکی از چالش‌های امنیتی این نوع سیستم‌هاست. با توجه به اینکه سیستم‌های کشف حمله نرم‌افزاری دارای تاخیر در کشف حمله هستند و حمله را پس از وقوع کشف می‌کنند، گزینه‌ی مناسبی برای سیستم‌های نهفته نیستند. در سیستم نهفته با توجه به کاربردهای این سیستم لازم است حمله در لحظه‌ی وقوع کشف شود. از جمله بهترین راه کارهای دفاع در برابر حمله، کشف حمله‌ی سخت افزاری است که با کمترین تاخیر و قبل از اجرای کد مخرب، آن را کشف می‌کند. در این سمینار مروری بر انواع روش‌های ایجاد امنیت و کشف حمله در سیستم‌های نهفته خواهیم داشت و پس از آن با تمرکز بر روی روش‌های سخت‌افزاری و نرم افزاری، انواع روش‌های ارائه شده را بررسی و مزایا و کاستی‌های آنها را برخواهیم شمرد و با ارزیابی روش‌ها در پارامترهای متفاوت که دارای اهمیت هستند، نحوه‌ی عملکرد آنها را مقایسه خواهیم کرد.

کلید واژه : سیستم های نهفته، امنیت، حملات.

فهرست مطالب

عنوان **صفحه**

فصل ۳- روش‌های ایجاد امنیت در سیستم‌های نهفته

فهرست شکل‌ها

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

فصل اول

مقدمه

۱–۱– مقدمه

سیستم‌های نهفته که متشکل از اجزای مختلف می‌باشد، از جمله کارت‌های هوشمند، روترها و تلفن‌های هوشمند. علاوه بر این، سیستم‌های نهفته یکی از عناصر کلیدی اینترنت اشیاء را تشکیل می‌دهد. پیشرفت‌های فن آوری اثرات مختلفی تولید کرده است، از جمله افزایش قدرت و عملکرد سیستم‌های نهفته. از این رو، توانایی‌ها و خدمات آنها نیز مطرح شده است، و در نتیجه، استفاده از آنها به طور قابل توجهی افزایش یافته است. همراه با تکامل عملکرد، مصرف انرژی و اندازه، سیستم‌های نهفته از یک محیط‌های جدا شده وارد حوزه‌های درون ارتباطاتی شده اند. اگر چه تکامل و پیشرفت قابل اتصال سبب بزرگ شدن تعداد خدمات ممکن شده است، ولیکن درعین حال، ریسک حمله به این نوع سیستم‌ها را نیز افزایش داده است. امنیت سیستم یک معیار طراحی به طور فزاینده مهم برای بسیاری از سیستم‌های جاسازی شده است. این سیستم‌ها اغلب قابل حمل و راحت تر از سیستم‌های دسکتاپ و سرور محاسبات سنتی مورد حمله واقع می‌شوند. الزامات کلیدی برای امنیت سیستم شامل دفاع در برابر حملات فیزیکی و پشتیبانی بسیار سبک وزن از نظر مساحت و مصرف انرژی است. رویکرد سیستم‌های نهفته برای اهداف مختلفی استفاده می‌شود، به طور عمده برای ضبط، ذخیره سازی، دستکاری و دسترسی به داده‌هایی با ماهیت حساس. بعنوان مثال سیستم‌های ماشین. حمله کننده‌ها می‌توانند اهداف مختلفی برای تهدید سیستم‌های نهفته داشته باشند، از جمع آوری داده‌ها حساس گرفته تا به خطر انداختن حریم خصوصی و اخلال در خدمات توسط حمله‌های محروم‌سازی از سرویس (DoS) و سوء استفاده از امنیت و قابلیت اعتماد آنها. عواقب مخرب یک حمله موفقیت آمیز می‌تواند زیان‌های فیزیکی و اقتصادی باشد، و در نتیجه حفظ حریم خصوصی و امنیت لازم و ضروری می‌باشد. به طور سنتی، فرآیند طراحی سیستم‌های نهفته در کاهش هزینه، اندازه و مصرف انرژی و در عین حال، افزایش عملکرد و قدرت متمرکز شده است. طبق روال معمول، در طول فرایند طراحی؛ امنیت، حفظ حریم خصوصی و اعتماد کنار گذاشته می‌شوند و شامل یک ویژگی افزودنی محسوب می‌شود. علاوه بر این، و نه به عنوان یک گروه، این ویژگی‌ها به صورت جداگانه تجزیه و تحلیل و اجرا شداند که باعث کاهش بهره‌وری آنها شده است. اگر چه این روش هزینه طراحی و توسعه را کاهش می‌دهد، ولیکن کیفیت معیارهای کاربردی را قربانی می‌کند و سبب می‌شود سیستم‌های نهفته آسیب پذیر تر گردد. در این سمینار مروری بر انواع روش‌های ایجاد امنیت و کشف حمله در سیستم‌های نهفته خواهیم داشت و پس از آن با تمرکز بر روی روش‌های سخت‌افزاری و نرم افزاری، انواع روش‌های ارائه شده را بررسی و مزایا و کاستی‌های آنها را برخواهیم شمرد و با ارزیابی روش‌ها در پارامترهای متفاوت که دارای اهمیت هستند، نحوه‌ی عملکرد آنها را مقایسه خواهیم کرد.