دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

اطلاعیه دفاع

| | | |
|---|---|---|
| **نام دانشجو:**<br>**زینب پورجعفری** | | **نام استاد راهنما:**<br>**دکتر علی جهانیان** |
| **مقطع: کارشناسی ارشد** | **رشته:مهندسی کامپیوتر** | **گرایش: معماری سیستم‌های کامپیوتری** |
| **نوع دفاع:**<br>• **دفاع پروپوزال** □<br>• **دفاع پایان نامه** ☑<br>• **دفاع رساله دکترا** □ | | **تاریخ: ۱۴۰۲.۱۰.۱۰**<br>**ساعت: ۱۲:۰۰ الی ۱۴**<br>**مکان: اتاق ۱۱۷** |

**عنوان: ارتقاء حمله کانال‌جانبی از راه دور بدون نیاز به اطلاعات موقعیت پودمان قربانی**

| | |
|---|---|
| **داوران خارجی: آقای دکتر مصطفی ارسالی صالحی نسب** | **داوران داخلی: دکتر راضیه سالاری‌فرد** |


**چکیده: در دنیای دیجیتال امروز با گسترش نیاز به پردازش سریع داده‌ها، آرایه‌های دروازه‌ای برنامه‌پذیر میدانی به علت انعطاف‌پذیری و بازدهی بالا، یک انتخاب مناسب برای شتاب‌دهی پردازش‌های مختلف محسوب می‌شوند. ویژگی‌های خاص این فناوری موجب شده تا این تراشه‌ها به‌عنوان میزبان محاسبات و شتاب‌دهنده در سامانه‌های ابری استفاده شوند، به‌گونه‌ای که در سرویس‌دهنده‌های رایانش ابری، کاربران می‌توانند در کنار واحد پردازشی، قسمتی از منابع این نوع تراشه‌ها را نیز اجاره کنند. هرچند اشتراک‌گذاری منابع مزیت‌هایی همچون افزایش انعطاف و کارآمدی سامانه را به دنبال دارد، اما این امر می‌تواند باعث ایجاد ناامنی‌هایی مانند انواع حملات کانال‌جانبی شود.**

**پژوهش‌های اخیر نشان‌داده که در حملات کانال‌جانبی توان، لزوماً نیاز به دسترسی فیزیکی به تراشه وجود ندارد و مهاجمان می‌توانند با درج یک حسگر دیجیتال در تراشه‌ای که بین چند کاربر به‌صورت مشترک مورداستفاده قرار گرفته است، اطلاعات کانال‌جانبی سایر کاربران را جمع‌آوری کنند و برای دستیابی به اطلاعات حساس و امنیتی پودمان قربانی استفاده کنند.**

**در این پایان‌نامه باتوجه به حساسیت این نوع حملات، با مطالعه کارهای گذشته و انجام آزمایش‌های متنوع، به تجزیه‌وتحلیل دقیق نحوه انتشار اطلاعات کانال‌جانبی توان مصرفی در شبکه توزیع توان پرداخته شده و تحلیل‌های دقیق و مفصلی در مورد رابطه قدرت حملات با موقعیت فیزیکی ارائه شده که دید عمیقی نسبت به این نوع حمله ایجاد می‌کند و راهکارهایی برای بهبود حملات در شرایطی که مهاجم اطلاع دقیقی از موقعیت پودمان‌های قربانی دارد، ارائه شده است. ما با بررسی فیلترهای موجود، روش پیش‌پردازشی متشکل از چند رویکرد را ارائه نموده‌ایم که مهاجم در هر موقعیتی نسبت به پودمان قربانی، با حداکثر $۵\times۱۰^{۴}$ بتواند کلید رمزنگاری را به دست بیاورد. نتایج مقایسه با روش‌های قبلی نشان می‌دهد روش ارائه شده می‌تواند تعداد ردپاهای مصرف توان را تا ۹۰ درصد کاهش دهد. نتایج گویای آن است که با اِعمال روش‌های ارائه شده، کارایی حمله در این روش نسبت به سایر روش‌ها بهبود قابل‌توجهی داشته است.**