سمینارهای پژوهشکده

پژوهشکده فضای مجازی سلسله سخنرانی‌هایی با موضوعات مربوط به هر یک از سه گروه پژوهشی خود(گروه پژوهشی امنیت شبکه و رمزنگاری، گروه پژوهشی فناوری انتقال محتوا و گروه پژوهشی مدیریت و حقوق فضای مجازی) برگزار می‌کند. در این شماره از نشریه خانم دکتر فرخ لقا معظمی- عضو هیئت‌علمی گروه رمز و امنیت پژوهشکده - گزارش مختصری از سمینارهای برگزارشده در نیمسال اول سال تحصیلی۹۶_۹۵ ارائه کرده است.

نیمسال اول سال تحصیلی ۹۶_۹۵

۱. **جناب آقای جواد علیزاده** (دانش‌آموخته دکتری - دانشگاه امام حسین) سخنرانی تحت عنوان:

" تحلیل تفاضلی و خطی رمزهای متقارن با استفاده از برنامه‌ریزی خطی"

برای بررسی امنیت یک الگوریتم، مقاومت آن در برابر تحلیل‌های شناخته‌شده مانند تحلیل‌های خطی و تفاضلی موردمطالعه و بررسی قرار می‌گیرد. برای این کار می‌توان از اثبات‌های ریاضی استفاده کرد و یا با روش‌های عملی نشان داد که نمی‌توان حمله تفاضلی یا خطی موفقیت‌آمیز روی رمز موردنظر اعمال کرد روش‌های تحلیل خودکار رمزهای متقارن که اخیراً موردتوجه بیشتری قرارگرفته‌اند، در مقایسه با روش‌های قبلی، از سرعت عمل و دقت بیشتری برخوردار هستند. یکی از این روش‌ها، استفاده از روش برنامه‌ریزی خطی (MILP) است که به‌طور رسمی در سال ۲۰۱۱توسط Mouha مطرح شد و سپس برای بررسی امنیت الگوریتم‌ها و ساختارهای جدید مورداستفاده قرار گرفت. در این سمینار تحلیل رمزهای متقارن با استفاده از برنامه‌ریزی خطی مورد بحث قرارگرفته و دستاوردها و نیز برخی چالش‌های این حوزه معرفی می‌شود.

۲. **سرکار خانم معصومه کوچک شوشتری** (دانش‌آموخته دکتری الکترونیک - دانشگاه خواجه نصیر) سخنرانی تحت عنوان:

" تحلیل رمزنگاری سیستم‌های رمزنگاری کلید عمومی کدمبنا"

رمزنگاری کد مبنا یکی از انواع رمزنگاری پسا کوانتوم است که به‌عنوان جایگزین مناسب برای سیستم‌های رمز مبتنی بر نظریه اعداد شناخته می‌شود. سیستم رمزنگاری مک الیس به‌عنوان اولین سیستم رمزنگاری کلید عمومی کد مبنا، از کدهای باینری گویا استفاده می‌کند. مشکل اصلی این سیستم، طول کلید عمومی بزرگ آن است. برای رفع این نقص، استفاده از کدهای ساختاریافته پیشنهادشده است. به‌کارگیری هر کد جدید، چالش‌های جدید را برای سیستم رمز کلید عمومی ایجاد می‌کند. در این ارائه، ابتدا معرفی کوتاهی از سیستم‌های رمزنگاری کلید عموماً کدمبنا و انواع امن آن خواهیم داشت و سپس حملات اصلی به سیستم‌های رمز کلید عمومی کدمبنا معرفی می‌شود. در انتها نیز برخی حملات جدید معرفی می‌شوند.

۳. **سرکار خانم شیوا ابراهیمی** (دانش‌آموخته ارشد - مرکز تحقیقات مخابرات ایران) سخنرانی تحت عنوان:

" تحلیل رمزنگاری سیستم‌های رمزنگاری کلید عمومی کدمبنا"

بسیاری از برنامه‌های اندروید برای انتقال اطلاعات حساس به‌طور امن از پروتکل SSL/TSL استفاده می‌کنند. از آنجایی‌که توسعه‌دهندگان استانداردهای اعتبارسنجی گواهی SSL رعایت نمی‌کنند، مشکلات امنیتی را در برنامه‌های اندروید به وجود می‌آورند. این مشکلات امنیتی موجب آسیب پذیری برنامه‌های اندروید در مقابل حملات مردمیانی می‌شوند. بنابراین امنیت ارتباطات SSL در مقابل حملات مردمیانی بستگی به اعتبارسنجی درست گواهی SSL در زمان ثبت ارتباط دارد. در این ارائه سعی می‌شود پروسه اعتبارسنجی گواهی SSL در اندروید، انواع آسیب‌پذیری‌ها SSL و ریشه آن‌ها شرح داده شود. سپس با

استفاده از تجزیه‌وتحلیل ایستا روی برنامه‌های اندروید و حملات مردمیانی، نقاط آسیب‌پذیری محتمل بررسی می‌شوند. درنهایت راه حل‌هایی برای کاهش مشکلات امنیتی SSL در برنامه‌های موبایل ارائه می‌گردد.

۴. **جناب آقای فرید دریابار** (دانش‌آموخته ارشد - مرکز تحقیقات مخابرات ایران) سخنرانی تحت عنوان:

" جرم‌شناسی در سامانه هوشمند تلفن همراه"

در سال‌های اخیر، شاهد تغییر سریع استفاده از تکنولوژی کامپیوترهای رومیزی به سامانه‌های هوشمند همراه بوده‌ایم. محبوبیت سامانه‌های هوشمند همراه به دلیل نزدیک شدن کارایی آن‌ها به کامپیوترهای شخصی و همچنین حمل آسان، به‌عنوان ابزاری پرکاربرد و چندمنظوره در سطوح مختلف جامعه نفوذ پیداکرده و مدام در حال افزایش است. سامانه‌های هوشمند همراه به دلیل چندمنظوره بودن برای انجام امور شخصی به اطلاعات حساس کاربران دسترسی دارند. از طرفی پیشرفت این سامانه‌ها به مجرمان کمک می‌کند تا با سوءاستفاده از این تکنولوژی به‌راحتی بتوانند در زمینه‌های مختلف جرم مانند حملات سایبری، سرقت هویت، دزدی، تجارت غیرقانونی، تروریسم سایبری و غیره فعالیت کنند. بنابراین، نیاز به جرم‌یابی دیجیتال در سامانه‌های هوشمند همراه بسیار احساس می‌شود. کارشناسان و بازرسان جرم‌یابی وظیفه شناسایی یک جرم، جمع‌آوری شواهد و اثبات جرم را در سامانه‌های هوشمند دیجیتال به عهده دارند. در این سخنرانی به‌طور کامل مبحث جرم‌شناسی دیجیتال در سامانه‌های هوشمند بر اساس چارچوب‌های استاندارد بررسی می‌شود و ابزارهای جرم‌یابی در هر مرحله ارائه می‌شود. سپس، یک نمونه جرم‌شناسی دیجیتال بر روی سامانه‌های هوشمند اندروید به‌صورت عملی و بر اساس یک سناریوی جرم واقعی ارائه می‌شود. درنهایت نمونه گزارش جرم‌شناسی دیجیتال برای ارائه در دادگاه بر اساس سناریوی تعریف‌شده، تهیه می‌شود. بطورخلاصه فازهای مهم جرم‌یابی سامانه‌های هوشمند همراه شامل حفاظت، شناسایی و جمع‌آوری، بررسی و تجزیه تحلیل و درنهایت آماده‌سازی گزارشی از مدارک و شواهد است.