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 دوم سال تحصیلی ۹۴_۹۵ ارائه کرده است.

نیمسال دوم سال تحصیلی ۹۵_۹۴

۱. **جناب آقای سید امیر مرتضوی** (دانشجو دکتری الکترونیک - دانشگاه صنعتی شریف) سخنرانی تحت عنوان:

" رمزنگاری مقاوم در برابر دست‌کاری "

هدف از رمزنگاری مقاوم در برابر دست‌کاری طراحی سامانه‌های امن رمزنگاری و مقاوم در برابر دست‌کاری مهاجم است. در این نوع رمزنگاری فرض می‌شود مهاجم فعالی وجود دارد که می‌تواند بعضی از حالات درونی سامانه رمزنگاری را دست‌کاری کند. راه‌های مقابله با دست‌کاری در یک تقسیم‌بندی به دودسته؛ راه‌ها با استفاده از یک کلید و بدون کلید تقسیم می‌شود. به دلیل عدم استفاده از کلید راهکار بدون کلید بیشتر موردتوجه است. در راهکار بدون کلید برای رسیدن به امنیت از کدهای چکش ناپذیر استفاده می‌شود. کدهای چکش ناپذیر کدهای بدون کلیدی هستند که در برابر دست‌کاری مهاجم مقاوم هستند. تعاریف مختلفی از امنیت برای چکش ناپذیر وجود دارد که در این ارائه سعی می‌شود برخی از این تعاریف ارائه شود.

۲. **سرکار خانم معصومه صف خانی** (عضو هیئت‌علمی دانشکده کامپیوتر - دانشگاه شهید رجایی، تهران) سخنرانی تحت عنوان:

" امنیت در سامانه‌های RFID"

سامانه شناسایی بسامد رادیویی RFID فناوری نو و جدیدی است که از بسامدهای رادیویی برای شناسایی اشیاء استفاده می‌نماید. یکی از مهم‌ترین نگرانی‌ها در استفاده از فناوری شناسایی بسامد رادیویی امنیت است. حفظ حریم خصوصی، احراز اصالت دوطرفه، عدم امکان ردیابی، عدم امکان حمالت جعل و مقاومت در برابر دیگر حمالت فعال و غیرفعال ازجمله چالش‌هایی هستند که محققان در تلاش برای فراهم کردن آن در حوزه امنیت هستند. تا به امروز، برای حل این مسائل، پروتکل‌های امنیتی متنوعی در مقالات پیشنهاد شده است، اما، بیشتر این تلاش‌ها در برآوردن اهداف امنیتی موردنظر خود ناموفق بوده‌اند. در این سخنرانی، مشکلات امنیتی موجود در برخی پروتکل‌های شناسی بسامد رادیوی تحلیل و بررسی می‌شود. و رهنمودهایی جهت طراحی پروتکل‌های امن ارائه می‌شود. در تحلیل‌های انجام‌شده، حملات کارای مختلفی مانند حمله افشای شناسه، حمله ردیابی، حمله جعل برچسب، حمله جعل مجموعه برچسب – برچسب خوان، حمله جعل برچسب خوان و حمله اخلال درهم زمانی، به‌صورت موفق به این پروتکل‌ها اعمال شده است که دو حمله اول خاصیت محرمانگی، سه حمله میانی خاصیت یکپارچگی و حمله آخر خاصیت دسترس‌پذیری را نقض می‌کنند.

۳. **جناب آقای نصرالله پاک‌نیت** (دانش‌آموخته دکتری ریاضی - دانشگاه شهید بهشتی) سخنرانی تحت عنوان:

" طرح‌های رمزنگاری باقابلیت جستجو "

با افزایش حجم اطلاعات و داده‌ها، استفاده از فضای ابری برای اهدافی چون پشتیبان‌گیری از داده‌ها یا برون‌سپاری آن‌ها بیش از پیش موردتوجه قرارگرفته است. از طرفی، ذخیره داده‌های خام بر روی سرور نیازمند اعتماد به اشخاص ثالث بوده و امنیت مورد نیاز در بسیاری از کاربردها را تأمین نمی‌کند. از طرف دیگر، رمزگذاری داده‌ها (با استفاده از سیستم‌های رمزگذاری معمول مانند AES،RSA و ElGamal) و ذخیره داده‌های رمز شده بر روی سرور، علی‌رغم تأمین سطح امنیت موردنیاز، قابلیت جستجو بر روی داده‌ها را از بین می‌برد. رمزگذاری باقابلیت جستجو روشی است که ضمن حفظ محرمانگی داده‌ها، قابلیت جستجو بر روی‌داده‌های رمز شده را معین می‌سازد. در این ارائه، به طرح‌های رمزگذاری باقابلیت جستجو پرداخته و پس از بیان نیازمندی‌های امنیتی این طرح‌ها، نمونه‌های از آن‌ها را بررسی خواهیم کرد.

۴. **جناب آقای محمد سبزی نژاد** (دانش‌آموخته دکتری ریاضی - دانشگاه خوارزمی) سخنرانی تحت عنوان:

"روش‌های پروتکل‌های رمزنگاری"

روش‌های متنوع برای ساخت پروتکل‌های رمزنگاری پیشنهاد شده و متناسب با نوع کاربرد طرح‌های زیادی ارائه‌شده است. بااین‌وجود، بیشتر پروتکل‌های طراحی‌شده به‌نوعی نشان داده‌شده که آسیب‌پذیر هستند. این امر لزوم ارزیابی امنیتی دقیق و کارآمد پروتکل‌های رمزنگاری را نشان می‌دهد. دو رویکرد کلی برای ارزیابی امنیتی پروتکل‌های رمزنگاری وجود دارد:۱) رویکرد مبتنی بر پیچیدگی محاسباتی ۲) رویکرد مبتنی بر امنیت کامپیوتری. رویکرد مبتنی بر پیچیدگی محاسباتی، امنیت پروتکل به یک مسئله سخت کاهیده می‌شود به این صورت که شکست پروتکل با حل یک مسئله سخت معادل‌سازی می‌شود. مزیت اصلی این رویکرد این است که جزئیات اولیه‌های رمزنگاری مورداستفاده در پروتکل مورد ارزیابی قرار می‌گیرد، اما نقطه‌ضعف این رویکرد پیچیدگی ارزیابی و درک سخت اثبات امنیتی آن است. علاوه بر این امکان بروز خطا در ارزیابی‌های مبتنی بر پیچیدگی محاسباتی وجود دارد زیرا توسط انسان و به‌صورت دستی صورت می‌پذیرد. در رویکرد مبتنی بر امنیت کامپیوتری از روش‌های فرمال یا سمبلیک برای ارزیابی امنیت پروتکل استفاده می‌شود. مهم‌ترین مزیت این رویکرد این است که با استفاده از ماشین و به‌صورت خودکار قابل انجام است. اما نقطه‌ضعف این رویکرد این است که اولیه‌های رمزنگاری مورداستفاده در پروتکل به‌صورت جعبه سیاه در نظر گرفته می‌شود. به‌عبارت‌دیگر جزئیات اولیه‌های رمزنگاری در ارزیابی امنیتی بررسی نمی‌شود. بااین‌وجود به دلیل اجرای خودکار و مبتنی بر ماشین می‌توان شرایط زیادی را در مورد پروتکل بررسی نمود.

۵. **جناب آقای محمد اهدایی** (دانش‌آموخته دکتری - دانشگاه خواجه نصیر - شرکت امن افزار) سخنرانی تحت عنوان:

" رمزنگاری و امنیت اطلاعات، از دانشگاه تا صنعت"

در دانشگاه با برخی از مبانی و مفاهیم امنیت اطلاعات آشنا شده‌ایم: رمزنگاری متقارن، رمزنگاری نامتقارن، امضای دیجیتال، گواهی الکترونیکی، مراکز صدور گواهی و ده‌ها مورد دیگر، از اصطلاحاتی است که در دروس رمزنگاری به ما معرفی می‌شوند. اما این مفاهیم در دنیای امروز ما چه کاربردی دارد؟ دنیای آینده ما چگونه است و رمزنگاری چرا و چگونه باید در فناوری‌های نوین نقش ایفا کند؟ در این ارائه برخی از حوزه‌های مهم رمزنگاری و امنیت در جهان امروز مورد

بحث قرار می‌گیرد و به نمونه‌های واقعی، خصوصاً پیاده‌سازی‌های آن در کشور، اشاره خواهد شد. پس‌ازآن، چند مورد از فناوری‌های ۲۰۲۰و ۲۰۳۰دنیا معرفی می‌شود و خواهیم دید که رمزنگاری و امنیت اطلاعات در آن‌ها چگونه خواهد بود.