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 تحصیلی ۹۴_۹۵ ارائه کرده است.

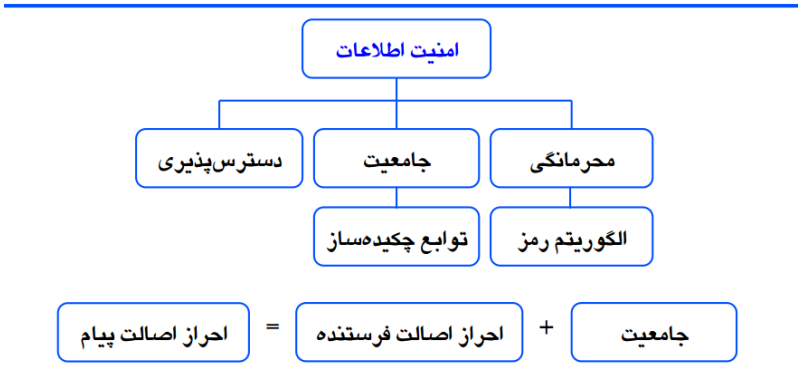
نیمسال اول سال تحصیلی ۹۵_۹۴

۱. **جناب آقای دکتر نصور باقری** (عضو هیئت‌علمی مرکز تحقیقات مخابرات ایران) سخنرانی تحت عنوان:

"مروری بر رمزنگاری احراز اصالت شده و مسابقه سزار "

برای برقراری امنیت اطلاعات و ارتباطات، ایجاب محرمانگی و احراز اصالت پیام دو هدف اصلی است .منظور از محرمانگی اطمینان از این امر است که اطلاعات تنها برای افراد مجاز قابل حصول باشد و منظور از احراز اصالت پیام فرآیندی است که در آن از جامعیت (دست‌نخوردگی)اطلاعات در طول تبادل آن، اطمینان حاصل‌شده و مبدأ (فرستنده) اطلاعات نیز احراز اصالت شود. ابزار اصلی برای به دست آوردن محرمانگی استفاده از الگوریتم‌های رمزنگاری و برای احراز اصالت پیام، استفاده از کدهای احراز اصالت پیام (MAC)است.

اما استفاده از دو الگوریتم، بار محاسباتی و هزینه بالایی را تحمیل خواهد کرد. به همین دلیل، بهتر است از الگوریتمی استفاده شود که دو شرط امنیتی مذکور را همزمان برآورده سازد. طرح‌های رمزنگاری که بتوانند این کار را انجام دهند، طرح‌های رمزگذاری احراز اصالت شده یا به‌اختصار طرح‌های AE نامیده می‌شوند. روش سنتی برای به دست آوردن یک طرح، AE ترکیب مستقیم روش‌های تولیدکننده محرمانگی احراز اصالت پیام است. اما مهم‌ترین مسئله در این روش، همان احتیاج به دو الگوریتم رمزنگاری و احراز اصالت مجزا، با کلیدهای متفاوت و نیز انجام دو سری محاسبات (دو گذر) روی پیام است. در مقابل روش سنتی، دسته دیگری از طرح‌های AE وجود دارند که برای ایجاب همزمان محرمانگی و احراز اصالت پیام از یک الگوریتم و یک کلید استفاده کرده و تنها یک سری محاسبات (یک گذر) روی پیام انجام می‌دهند. در این راستا یک مسابقه تحت عنوان CAEAR در جریان است که درواقع فراخوانی است برای طراحی AE های اختصاصی .این مسابقه در سال ۲۰۱۴شروع‌شده است و تا سال ۲۰۱۷ادامه خواهد داشت. هدف اصلی در این سخنرانی ،مرور کارهای صورت گرفته در مورد طرح‌های AE اختصاصی است و چالش‌های موجود در این حوزه، با تمرکز بر روی کاندیداهای راه‌یافته به مرحله دوم، موضوعات تحقیقاتی باز و کارهای انجام‌شده مرتبط.



۲. **جناب آقای دکتر رضا ابراهیمی آتانی** (دانشکده مهندسی کامپیوتر،دانشگاه گیلان، رشت، ایران) عضو هیئت‌علمی -سخنرانی تحت عنوان:

"مقدمه‌ای بر توابع کپی ناپذیر فیزیکی "

با افزایش روزافزون ارتباطات و نقش غیرقابل‌انکار آن در توسعه جوامع بشری، امنیت و محرمانگی اطلاعات به یکی از مهم‌ترین نیازهای سیستم‌های ارتباطی کنونی دنیا تبدیل‌شده است. از طرف دیگر افزایش کاربردهای رمزنگاری در ادواتی نظیر کارت‌های اعتباری، تلفن‌های همراه، شبکه‌های بی‌سیم، اینترنت اشیاء و کنترل‌کننده‌های از راه دور باعث گردیده تا نیازهای دیگری نیز علاوه بر سرعت و امنیت بالا مطرح گردند. با توسعه حملات سخت‌افزاری و افزایش تعداد سازندگان بسترهای پردازشی ،توان مهاجمین برای مشاهده و دست‌کاری تراشه‌ها افزایش چشم‌گیری پیدا کرده است. روش‌های دست‌کاری فیزیکی این امکان را فراهم آورده است که اطلاعات رمز شدهٔ دیجیتال از مدارات مجتمع استخراج شود و با در دست داشتن یک کپی تقلبی از اطلاعات رمز شده بتوان سیستم جدیدی را پیکربندی نمود. متأسفانه سرقت IP منجر به ضررهای جبران‌ناپذیری مالی و امنیتی در شرکت‌های طراحی و ساخت پردازنده‌های خاص منظوره رمزنگار گردیده است. یکی از تکنیک‌های مؤثر برای حفاظت از رمزها در برابر حملات فیزیکی و ایجاد احراز اصالت برای سخت‌افزار، استفاده از توابعی بانام توابع کپی ناپذیر فیزیکی (PUFs) است. این توابع به‌منظور جلوگیری از ایجاد هرگونه کپی‌برداری و تکثیر سخت‌افزاری و حفاظت از IP بر روی بسترهای FPGAوASIC طراحی گردیده است و نقش احراز اصالت سخت‌افزاری آن مشابه کارکرد اثرانگشت در روش‌های بیومتریک است. به‌عبارت‌دیگر تشخیص دست‌کاری سخت‌افزاری به‌منظور ایجاد محیطی امن برای ذخیرهٔ داده‌ها ایجادشده‌اند و با بهره‌گیری از خواص ذاتی تصادفی که در حین فرآیند ساخت اتفاق میافتند و قابل‌کنترل نیستند، امنیت سیستم‌های اطلاعاتی و سخت‌افزاری را بالابرده‌اند. در این سخنرانی ابتدا مروری روی حملات سخت‌افزاری و حملات روی سیستم‌های تعبیه‌شده ارائه می‌گردد. در ادامه ضمن تمرکز روی توابع کپی ناپذیر فیزیکی دسته‌بندی جامعی از این توابع و کاربردهای متنوع آن‌ها ارائه می‌گردد. سپس ضمن بررسی حملات اعمال‌شده روی PUFها آسیب‌پذیری‌های این توابع ارائه می‌گردد.در انتها نیز سعی خواهد شد موضوعات باز این حوزه به‌طور مختصر ارائه شود تا پیشنهادهایی جهت ادامه پژوهش در این زمینه تحقیقاتی ارائه گردد.

در این سخنرانی فهرست مطالب به‌صورت زیر بوده است:

- ✓ سخت‌افزارهای رمزنگاری و سیستم‌های تعبیه‌شده
- ✓ مروری کوتاه روی حملات سخت‌افزاری
- ✓ مقدمه‌ای بر توابع کپی ناپذیر فیزیکی و کاربردها
- ✓ آشنایی با ساختار چند تابع کپی ناپذیر فیزیکی
- ✓ مروری بر مشخصات PUF ها
- ✓ مروری بر موضوعات پژوهشی روز PUF ها
- ✓ جمع‌بندی بحث

۳. **جناب آقای سیاوش احمدی** (دانشگاه مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران) دانشجوی دکتری سخنرانی تحت عنوان:

" معرفی شبکه Torو مروری بر ضعف‌ها و حملات آن "

با ورود به عصر اطلاعات و گسترش روزافزون ارتباطات، شبکه‌های مختلفی برای تسهیل روابط و انتقال داده‌های اشخاص ایجاد شدند که ازجمله معروف‌ترین آن‌ها، شبکه جهانی اینترنت است. با گسترده‌تر شدن این شبکه‌ها و عدم امنیت کانال ارتباطی در آن‌ها، امنیت داده‌های ارسالی نیز بیش‌ازپیش موردتوجه قرار گرفت. نیاز برای محرمانه نگه‌داشتن اطلاعات ارسالی از قبیل اطلاعات بانکی، نامه‌های اداری و داده‌های حساس نظام، استفاده از رمزنگاری را در هنگام جابه‌جایی داده‌ها مرسوم کرد. همچنین جهت حفظ اعتبار اطلاعات ارسال‌شده، الگوریتم‌های احراز اصالت ارائه شدند تا از تغییر اطلاعات توسط دشمنان در حین ارسال جلوگیری کنند. با مرور زمان، رفته‌رفته ویژگی‌هایی مانند تازگی پیام،دسترسی‌پذیری، انکارناپذیری و مقاومت در برابر حملات مختلف نیز موردتوجه قرار گرفت. ضمن این موارد، یکی از مهم‌ترین ویژگی‌هایی که نیاز به آن در حین ارتباط امن در شبکه‌ها احساس شد، حفظ گمنامی است که ایده ایجاد آن اولین بار توسط چام مطرح شد. در صورت عدم گمنامی، ضمن اینکه محرمانگی و احراز اصالت داده‌ها حفظ می‌شود، اما مهاجم می‌تواند طرفین ارتباط را بشناسد. به‌عنوان‌مثال در هنگام استفاده یک کاربر از اینترنت، مهاجم می‌تواند تشخیص دهد که شخص هدف خود، از چه سرویسی در اینترنت استفاده می‌کند و یا به چه سروری در آن متصل است. در تعریف حریم خصوصی افراد و ایجاد یک ارتباط امن، نشت این اطلاعات به مهاجم قابل‌قبول نیست و بنابراین استفاده از روشی برای ایجاد یک ارتباط گمنام لازم به نظر می‌رسد.

۴. **سرکار خانم دکتر هدی جنتی** (پژوهشگاه دانش‌های بنیادی(IPM)، تهران، ایران) پژوهشگر پسادکتری، سخنرانی تحت عنوان:

"All-or-Nothing Approach to Protect a Distance Bounding Protocol against Terrorist Fraud Attack"

این بحث معرفی روش" همه‌یاهیچ" است برای پیشنهاد یک پروتکل جدید درزمینهٔ فاصله محدوده با سطح امنیت بالاتر است که می‌تواند از تقلب‌های تروریستی که در این فاصله ممکن است اجرا شوند، جلوگیری نماید.

مطالب ارائه‌شده در این سخنرانی به شرح زیر بوده است:

- سیستم‌های RFID و حمله Relay (امدادی)
- چگونه از سیستم‌های RFID در مقابل حمله Relay محافظت کنیم.
- روش همه یا هیچ بر اساس مسافت پروتکل محدوده.

۵. **جناب آقای وحید جهاندیده** (دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران) دانشجوی دکتری، سخنرانی تحت عنوان:

" نقش تصادفی بودن در رمزنگاری "

در این سخنرانی به عدم امکان استخراج قطعی منابع تصادفی ناقص بر اساس مدل‌های موجود پرداخته خواهد شد. اگر استخراجی موجود باشد به‌عنوان یک‌رشته تصادفی ناقص ورودی پذیرفته می‌شود و به‌عنوان یک‌رشته کوچک‌تر تولید می‌شود. بطوریکه این رشته دارای یک توزیع غیرقابل تشخیص از یک‌رشته تصادفی دقیقاً در همان اندازه است.

مطالب ارائه‌شده در این سخنرانی به شرح زیر بوده است:

- جایگاه منابع تصادفی در رمزنگاری
- مدل‌سازی منابع تصادفی
- منابع آنتروپی
- فاصله آماری و تمایز ناپذیری محاسباتی
- بازی استخراج پذیری منابع
- غیرممکن بودن رمزنگاری با منابع آنتروپی
- ممکن بودن امضا با منابع آنتروپی
- ممکن بودن شبیه‌سازی با منابع آنتروپی
- استخراج پذیری منابع آنتروپی با هسته‌ی تصادفی
- جمع‌بندی و نتیجه‌گیری