کتاب یادمان

شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران

شهریور ۱۳۹۸

کتاب یادمان

شانزدهمین کنفرانس بین‌المللی

انجمن رمز ایران

دانشگاه فردوسی مشهد
۶ و ۷ شهریور ۱۳۹۸

فهرست مطالب

سیاست‌های کلی نظام در بخش امنیت فضای تولید و تبادل اطلاعات (افتا)..... ۴
۱- مقدمه ۵
۲- گزارش دبیرخانه دائمی کنفرانس‌های انجمن رمز ایران ۶
۳- سخن دبیر کنفرانس..... ۱۰
۴- محورهای کنفرانس ۱۳
۵- ساختار اجرایی و دبیرخانه کنفرانس..... ۱۴
۶- کمیته علمی کنفرانس ۱۶
۷- برنامه‌های شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران ۱۸
۸- سخنرانی‌های کلیدی و مدعو..... ۲۰
۹- چکیده سخنرانی‌های کلیدی و مدعو ۲۱
۵- ساختار اجرایی و دبیرخانه کنفرانس..... ۱۴
۶- کمیته علمی کنفرانس ۱۶
۷- برنامه‌های شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران ۱۸
۸- سخنرانی‌های کلیدی و مدعو..... ۲۰
۹- چکیده سخنرانی‌های کلیدی و مدعو ۲۱
۱۰- نشست‌های ارائه مقاله ۲۵
۱۱- مقاله‌های ارائه شده شفاهی..... ۲۶
۱۲- چکیده مقاله‌های ارائه شده شفاهی..... ۳۰
۱۳- مقاله‌های ارائه شده به صورت پوستر ۴۶
۱۴- چکیده مقاله‌های ارائه شده به صورت پوستر..... ۴۸
۱۵- کارگاه‌های آموزشی..... ۶۰
۱۶- نمایشگاه تخصصی افتا..... ۶۱
۱۷- ارائه‌های علمی- کاربردی افتا..... ۶۲
۱۸- میزگرد هم‌اندیشی ۶۳
۱۹- نشست طرح مسأله..... ۶۴
۲۰- پیش رویداد کنفرانس..... ۶۵
۲۱- رویداد دهکده امنیت و رمز ۶۶
۲۲- ماراتن عمومی‌سازی امنیت و رمز ۶۷
۲۳- بیانیه پایانی کنفرانس..... ۶۸
۲۴- گزارش تصویری ۷۲
۲۵- شرح کوتاه رویداد دهکده امنیت و رمز ۹۴
۲۶- چکیدهٔ ارائه‌های علمی- کاربردی افتا..... ۹۷
۲۷- چکیدهٔ کارگاه‌های آموزشی ۱۰۲
۲۸- سابقه برگزاری کنفرانس‌های سالیانه انجمن رمز ایران ۱۰۸
برگزاری هفدهمین کنفرانس بین‌المللی انجمن رمز ایران ۱۱۵

۱- مقدمه

انجمن رمز ایران به عنوان یک تشکل علمی غیردولتی توانسته است از ابتدای تأسیس در سال ۱۳۷۹ تاکنون، منشأ خدمات ارزنده‌ای در حوزه گسترش دانش رمزشناسی و امنیت فضای تولید و تبادل اطلاعات (افتا) در کشور باشد و با مشارکت در تدوین سند افتا، ارائه پیشنهاد اولیه سیاست‌های کلی نظام در بخش افتا و توصیه‌های لازم به دولت و نهادهای قانون‌گذار در نظام جمهوری اسلامی ایران، نقش تأثیرگذار و تعیین‌کننده‌ای در تصویب اسناد و الزامات قانونی مورد نیاز این حوزه ایفا نماید و عامل بسیار مؤثری برای رشد و نوآوری صنعت افتا در کشور بوده است.

این انجمن در حال حاضر با برگزاری منظم کنفرانس‌های بین‌المللی سالیانه، انتشار مجله علمی‌پژوهشی ISeCure، انتشار مجله علمی‌ترویجی «منادی امنیت فضای تولید و تبادل اطلاعات (افتا)»، انتشار مجله علمی‌پژوهشی «رایانش و امنیت (JCS)» به صورت مشترک با دانشگاه اصفهان و مجله علمی‌پژوهشی «کد، رمز و امنیت سایبری» به زبان فارسی با همکاری دانشگاه خواجه نصیرالدین طوسی و همچنین هدایت شاخه‌های دانشجویی انجمن در بسیاری از دانشگاه‌های کشور، در زمره فعال‌ترین انجمن‌های علمی کشور به شمار می‌آید.

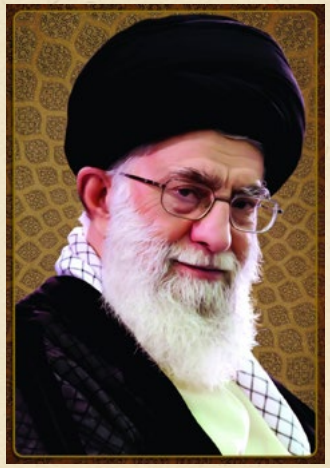
در تداوم این فعالیت‌ها، شانزدهمین دوره کنفرانس‌های بین‌المللی این انجمن به توفیق الهی در روزهای ششم و هفتم شهریور ماه ۱۳۹۸ به میزبانی گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد برگزار گردید که کتاب حاضر خلاصه‌ای از این رویداد مهم را ارائه می‌دهد.

رویکرد کلی کنفرانس‌های این انجمن به عنوان مهمترین رویداد علمی سالیانه کشور در حوزه افتا، فراهم آوردن محیطی برای تبادل نظر متخصصین و پژوهشگران حوزه افتا به منظور ارتقاء سطح دانش رمزشناسی و توسعه فناوری‌های این حوزه در کشور و ارائه راهکارهای بهبود امنیت سامانه‌های اطلاعاتی و جلوگیری از مخاطرات و تهدیدات سایبری بین‌المللی است که زیرساخت‌های حیاتی، حساس و مهم کشور را هدف قرار می‌دهند.

شانزدهمین دوره کنفرانس‌های سالیانه این انجمن، فرصت بسیار گرانقدری را فراهم نمود تا علاوه بر ارائه مقالات علمی‌پژوهشی در مباحث نظری و کارگاه‌های آموزشی این حوزه، به موضوعات مهم «امنیت سامانه‌های کنترل صنعتی» و «امنیت اینترنت اشیاء» در قالب محورهای علمی‌ترویجی کنفرانس پرداخته شود که جمعیت قابل توجهی از جامعه صنعتی کشور را مخاطب خود قرار داد و در کنار نمایشگاه جانبی و ارائه‌های علمی‌کاربردی اهالی صنعت افتا، با رویداد نوآورانه «دهکده امنیت و رمز» توانست گام ارزنده‌ای را در زمینه عمومی‌سازی آموزش رمزشناسی برای دانش‌آموزان و دبیران دوره متوسطه آموزش‌وپرورش بردارد که با استقبال خوب این گروه از مخاطبین کنفرانس مواجه شد.

سیاست‌های کلی نظام در بخش امنیت فضای تولید و تبادل اطلاعات (افتا)

متن کامل سیاست‌های مقام معظم رهبری به‌عنوان راهنمای دستگاه‌های اجرایی، تقنینی و نظارتی، خط مشی و جهت‌گیری نظام در بخش افتا



۱. ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای امن‌سازی ساختارهای حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات، و ارتقاء مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در کشور به منظور:

- استمرار خدمات عمومی؛
- پایداری زیرساخت‌های ملی؛
- صیانت از اسرار کشور؛
- حفظ فرهنگ و هویت اسلامی- ایرانی و ارزش‌های اخلاقی؛
- حراست از حریم خصوصی و آزادی‌های مشروع و سرمایه‌های مادی و معنوی.

۲. توسعه فناوری اطلاعات و ارتباطات با رعایت ملاحظات امنیتی.

۳. ارتقاء سطح دانش و ظرفیت‌های علمی، پژوهشی، آموزشی و صنعتی کشور برای تولید علم و فناوری مربوط به امنیت فضای اطلاعاتی و ارتباطی (افتا).

۴. تکیه بر فناوری بومی و توانمندی‌های تخصصی داخلی در توسعه زیرساخت‌های علمی و فنی امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی.

۵. پایش، پیشگیری، دفاع و ارتقاء توان بازدارندگی در مقابل هرگونه تهدید در حوزه فناوری اطلاعات و ارتباطات.

۶. تعامل مؤثر و سازنده منطقه‌ای و جهانی و همکاری و سرمایه گذاری مشترک در حوزه‌های دانش، فناوری و امور مربوط به امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی با حفظ منافع و امنیت ملی.

۷. تعیین نهاد متولی و هماهنگ‌کننده زیر نظر دولت به منظور هدایت، نظارت و تدوین استانداردهای لازم برای حفظ و توسعه امنیت فضای تولید و تبادل اطلاعات و ارتباطات و تهیه پیش‌نویس قوانین مورد نیاز.

۸. فرهنگ‌سازی، آموزش و افزایش آگاهی و مهارت‌های عمومی در حوزه افتا.

۹. رعایت موازین شرعی و مقررات قانونی مربوط به حفظ حقوق فردی و اجتماعی در اجرای این سیاست‌ها.

۲- گزارش دبیرخانه دائمی کنفرانس‌های انجمن رمز ایران

با نام و یاد خدا و سپاس بیکران به درگاه او برای توفیق در برگزاری شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران، در ابتدای کتاب خلاصه اهم فعالیت‌های دبیرخانه دائمی کنفرانس‌های این انجمن ارائه می‌شود؛ فعالیت‌هایی که از پایان کنفرانس پانزدهم تا چند ماه بعد از کنفرانس شانزدهم در دستور کار بوده‌اند.

فراخوان پاییزه و فراخوان بهاره

به منظور تداوم و استمرار فعالیت‌های پژوهشی جامعه رمزنگاری و امنیت، در فاصله بین دو کنفرانس متوالی انجمن رمز ایران، به پیشنهاد دبیرخانه دائمی کنفرانس و تصویب شورای اجرایی انجمن مقرر گردید که علاوه بر فراخوان بهاره، یک فراخوان پاییزه نیز صورت گیرد. در این فرآیند مقالاتی که با توجه به نظرات داوران امکان اصلاح و ارائه مجدد دارند توسط نویسندگان بازنگری و در فراخوان بهاره ارائه می‌شوند. بدین ترتیب نظرات داوران موجب ارتقاء و بهبود مقالات می‌شود و سطح کیفی مقالات ارتقاء می‌یابد. این فرآیند با نتایج بسیار مثبت همراه بوده است و در کنفرانس‌های بعدی نیز ادامه خواهد داشت.

کمیته علمی کنفرانس شانزدهم

کمیته علمی کنفرانس دو جلسه (خرداد و مرداد ماه) در تهران برگزار نمود. مقالات دریافت شده و پذیرفته شده (ارائه شفاهی و پوستری) به تفکیک فارسی و انگلیسی و در فراخوان‌های پاییزه و بهاره در جدول زیر مشخص شده‌اند. بر روی مقالات دریافتی در مجموع ۳۵۷ داوری (به طور متوسط ۲/۵۸ داوری به ازای هر مقاله) انجام شده است.

ردیف	عنوان	تعداد مقالات	
۱	فراخوان پاییزه	•تعداد مقاله‌های ارسالی به دبیرخانه: ۲۶ •تعداد مقاله‌های پذیرفته‌شده شفاهی: ۴ •تعداد مقاله‌های پذیرفته‌شده پوستر: ۳	• تعداد مقاله‌های ارسالی به دبیرخانه: ۱۳۸ •تعداد مقاله‌های پذیرفته‌شده شفاهی: ۲۵ (۱۸٪) (۱۶ مقاله انگلیسی و ۹ مقاله فارسی) •تعداد مقاله‌های پذیرفته‌شده پوستر: ۱۸ (۱۳٪) (۸ مقاله انگلیسی و ۱۰ مقاله فارسی)
۲	فراخوان بهاره	•تعداد مقاله‌های ارسالی به دبیرخانه: ۱۱۲ •تعداد مقاله‌های پذیرفته‌شده شفاهی: ۲۱ •تعداد مقاله‌های پذیرفته‌شده پوستر: ۱۵	

مقالات انگلیسی پذیرفته شده در کنفرانس، در تاریخ ۹۸/۱۱/۱۷ در پایگاه IEEE Xplore نمایه شده‌اند.

مقاله برتر

فرآیند انتخاب مقاله برتر دارای سه مرحله است، در مرحله اول مسئولین محورها مقالات برتر محور خود را انتخاب و به دبیرخانه دائمی معرفی می‌کنند. در دبیرخانه دائمی با توجه به ضوابط از قبل تعیین شده، حداکثر دو مقاله انتخاب می‌شود. انتخاب نهایی پس از ارائه در کنفرانس توسط داوران صورت می‌گیرد. در کنفرانس شانزدهم، مقاله: GSLHA: Group-based Secure Lightweight Handover Authentication Protocol for M2M Communication به نویسندگی محمدمهدی مدیری، جواد مهاجری و محمود سلماسی‌زاده به عنوان مقاله برتر انتخاب شده است.

داور برتر

به منظور ارتقاء کیفیت کمیته علمی کنفرانس، همه ساله داوران برتر کنفرانس بر اساس معیارهای: تعداد، کیفیت و داوری به موقع مقالات، توسط مسئولین محورها به دبیر کمیته علمی و دبیرخانه دائمی معرفی می‌شوند و از بین آنها یک نفر به عنوان داور برتر انتخاب و به عضویت کمیته علمی کنفرانس پذیرفته می‌شود. در کنفرانس شانزدهم سرکار خانم دکتر معصومه صفخانی عضو هئیت علمی دانشگاه تربیت دبیر شهید رجایی به عنوان داور برتر انتخاب شدند.

رساله و پایان‌نامه برتر و شایسته تقدیر

رساله‌ها و پایان‌نامه‌هایی که موضوع آنها مرتبط با محورهای کنفرانس باشند، همه ساله طبق ضوابط موجود بررسی می‌شوند و از نویسندگان رساله و پایان‌نامه برتر و شایسته تقدیر با اهداء جایزه نقدی، تقدیر به عمل می‌آید. به این مناسبت در کنفرانس شانزدهم سه رساله و یک پایان‌نامه مورد تقدیر قرار گرفتند.

ردیف	عنوان تقدیر	عنوان رساله/ پایان‌نامه (دانشجو/ استاد راهنما)	دانشگاه محل تحصیل
۱	رساله برتر	امضاهای رقمی با حفظ حریم خصوصی (پروین رستگاری/ دکتر محمدعلی دخیل علیان)	دانشگاه صنعتی اصفهان
۲	رساله شایسته تقدیر	پیاده‌سازی کارای رمزنگاری خم بیضوی (راضیه سالاری فرد/ دکتر سیاوش بیات سرمدی)	دانشگاه صنعتی شریف
		آشکارسازی کور پردازش‌های اعمال شده بر سیگنال ویدئو از طریق تحلیل آثار عملیات (وحیده امانی پور/ دکتر شاهرخ قائم مقامی)	دانشگاه صنعتی شریف
۳	پایان‌نامه شایسته تقدیر	بهبود پروتکل‌های امنیتی در اینترنت اشیاء (مهیار شریعت/ دکتر معصومه صفخانی)	دانشگاه تربیت معلم شهید رجایی

داوران و مقالات برتر مجلات انجمن رمز ایران

همه ساله از نویسندگان مقالات برتر مجلات انجمن رمز ایران و داوران برتر آنها در مراسم اختتامیه کنفرانس‌ها تقدیر می‌شود. این مجلات عبارتند از: مجله علمی- پژوهشی ISeCure که در سال ۱۳۹۶ موفق به دریافت درجه ISI شده است و هم‌اینک در پایگاه Clarivate Analytics نمایه می‌شود، مجله علمی- پژوهشی به صورت مشترک با دانشگاه اصفهان با عنوان Jornal of Computing and Security (JSC) و مجله علمی- ترویجی «منادی افتا». در کنفرانس شانزدهم از مقالات مندرج در جدول زیر تقدیر شده است.

ردیف	عنوان تقدیر	عنوان مقاله/ نویسندگان
۱	مقاله برتر مجله ISeCure	Impossible Differential Cryptanalysis on Deoxys-BC-256 فرخ لقا معظمی، علیرضا مهرداد و هادی سلیمانی
۲	مقاله برتر مجله JCS	Provably Secure Variant of ETRU Based on Extended Ideal Lattices Over Direct Product of Dedekind Domains رضا ابراهیمی آتانی، شهاب‌الدین ابراهیمی آتانی و امیر حسنی کرباسی
۳	مقالات برتر مجله منادی افتا	• بهبود معماری امنیت سرویس‌های اساسی در محاسبات ابری • بررسی چالش‌های امنیتی و چگونگی مقابله با آنها در شبکه‌های نرم‌افزار محور • بررسی عملکرد امنیتی یکپارچه‌سازی شبکه‌های اقتضایی خودرویی با شبکه‌های نرم‌افزارمحور محمود دی‌پیر
		• ارزیابی عملکرد الگوریتم‌های شبه‌بیولوژیکی جهت حل مسأله کوله‌پشتی در قالب تابع هدف کمینه‌سازی‌شده • ارزیابی عملکرد الگوریتم‌های مختلف فرااکتشافی در کشف کلیدرمز الگوریتم رمزنگاری ویجینر • بررسی عملکرد الگوریتم‌های جستجوی فرااکتشافی و فراگیر جهت تحلیل رمز الگوریتم رمزنگاری SDES میثم مرادی

همچنین در این کنفرانس از داوران مجلات انجمن به شرح جدول زیر تقدیر به عمل آمده است:

ردیف	عنوان تقدیر	تقدیر شونده
۱	داوران برتر ISeCure	محمدعلی هادوی - محسن پورپونه
۲	داور برتر مجله JCS	حمید ملا
۳	داوران برتر مجله منادی افتا	عبدالرسول میرقدری - شهریار بیژنی

از دیگر اقدامات انجمن رمز ایران برای گسترش رویدادهای علمی حوزه رمزشناسی و افتا، همکاری برای تشکیل هیئت مؤسس «جایزه مرحوم دکتر برنجکوب» با مشارکت خانواده محترم آن مرحوم، دانشگاه صنعتی اصفهان و پارک علم و فناوری شیخ بهایی اصفهان بوده است تا از برندگان این جایزه در ایام برگزاری کنفرانس‌های سالیانه انجمن تقدیر شود. این حرکت شروع شده است و امیدواریم در سال آینده شاهد اقدامات اجرایی آن باشیم.

محمود سلماسی‌زاده
مسئول دبیرخانه دائمی کنفرانس‌های انجمن رمز ایران
دانشیار پژوهشکده الکترونیک، دانشکده مهندسی برق دانشگاه صنعتی شریف

۳- سخن دبیر کنفرانس

سپاس خداوند را که کتاب خود را به‌صورت عمومی و همگانی در اختیار انسان‌ها قرار داد تا چراغ راه آنان باشد و حمد بیکران تنها شایسته اوست که پیامبر اکرم حضرت محمد مصطفی و خاندان پاکش (درود خداوند بر ایشان باد) را خزانه‌داران علم، نگهداران حکمت و مترجمان وحی خود قرار داد تا دستگیر و راهنمای سالکان طریقش شوند. همچنین او را شاکریم که میزبان شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران در شهر امام رئوف و مهربانی بودیم. دانشگاه فردوسی مشهد با ۷۰ سال سابقه، سومین دانشگاه کشور از نظر قدمت و دومین دانشگاه جامع ملی است. انجمن رمز ایران با ۲۰ سال سابقه، متولی کنفرانسی بین‌المللی است که هر ساله در یکی از دانشگاه‌های معتبر ایران عزیزمان برگزار می‌شود. گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد با حدود ۳۰ عضو هیات علمی از تخصص‌های مختلف با همکاری دبیرخانه دائمی کنفرانس‌های انجمن رمز ایران، میزبان این همایش بین‌المللی است.

برنامه‌های این کنفرانس نتیجه یک سال فعالیت، تلاش و پیگیری مستمر همکاران متعددی در سطح ملی و بین‌المللی است که در قالب ۲ روز اصلی به همراه ۲ روز برای برگزاری کارگاه‌ها ارائه شد. یکی از شاخص‌های کنفرانس بین‌المللی انجمن رمز ایران حضور گسترده اساتید و صاحب‌نظران است و در این دوره نیز شاهد برگزاری دو سخنرانی کلیدی و نیز چهار سخنران مدعو همزمان با نشست ارائه مقاله‌ها بودیم. در شانزدهمین کنفرانس، همچنین برنامه‌های بدیعی ارائه شد که از جمله می‌توان از فراخوان و پذیرش مقالات در دو مرحله پاییزه و بهاره، عمومی‌سازی امنیت و رمز برای دانش‌آموزان و معلمان، برگزاری پیش رویداد برای افزایش تأثیرگذاری اجتماعی و ترویج امنیت و رمز نام برد.

در کنفرانس شانزدهم در مجموع ۱۳۸ مقاله به دبیرخانه کنفرانس ارسال شد که در فراخوان پاییزه ۲۶ مقاله و در فراخوان بهاره ۱۱۲ مقاله دریافت شد. که پس از انجام ۳۵۷ مورد داوری توسط ۹۹ عضو کمیته داوران، تعداد ۴۷ مقاله پذیرش و ۴۳ مقاله در کنفرانس ارائه شد. در بخش کارگاه‌ها نیز ۱۶ درخواست ارائه کارگاه آموزشی با موضوعات مختلف توسط سازمان‌ها و صنایع مرتبط به دبیرخانه کنفرانس ارسال شد که از این میان ۱۰ کارگاه برای ارائه در دو روز پیش از برگزاری کنفرانس انتخاب شدند و ۷ کارگاه آموزشی برگزار شد. در مجموع بیش از ۳۰۰ نفر برای شرکت در این دوره کنفرانس ثبت‌نام کرده و حضور داشتند.

دهکده امنیت و رمز با هدف آموزش و ترویج مفاهیم و اصول امنیت و رمز و نیز کشف و پرورش استعدادهای جوان در آموزش و پرورش، برای دانش‌آموزان دبیرستانی پایه نهم، دهم و یازدهم طراحی شده است. این مجموعه شامل سه رویداد نیم روزه فصلی زمستانه، بهاره و تابستانه بود که در دانشکده مهندسی دانشگاه فردوسی مشهد برگزار شد. رویداد اول همزمان با جشن چهلمین سالگرد پیروزی انقلاب اسلامی در دهه فجر ۱۳۹۷، با حضور بیش از ۱۰۰ دانش‌آموز از مدارس مختلف مشهد برگزار شد. منتخبین رویداد اول در رویداد دوم که در اواخر

بهار ۱۳۹۸ برگزار شد شرکت کردند و در رویداد آخر رقابت شرکت‌کنندگان برتر همزمان با برگزاری کنفرانس در شهریور ۱۳۹۸ بود. در هر یک از این رویدادهای نیم روزه، دو کارگاه آموزشی و ترویجی و یک مسابقه برگزار شد. کارگاه‌ها شامل تور آشنایی با مفاهیم کلی امنیت رمز و نشست‌های آموزشی الگوریتم‌های رمزنگاری، پنهان‌نگاری و پروتکل‌های امنیتی بود. در این کارگاه‌ها سعی شد با عمومی‌سازی و تصویرسازی مفاهیم علمی- فنی و بیان آن در قالب مثال‌های ساده، مهیج و کاربردی، مطالب به‌صورت قابل فهم برای دانش‌آموزان ارائه شود. منتخبین نهایی علاوه بر کسب جایزه ارزنده، امکان شرکت در کنفرانس را داشتند.

پیش رویداد کنفرانس با حضور کمیته اجرایی کنفرانس و مشارکت مرکز منطقه‌ای شمال شرق شهید فهمیده و حضور بیش از ۵۰ مدعو از مدیران و کارشناسان بیش از ۳۰ سازمان دولتی و شرکت‌های بخش خصوصی در اول مرداد ۱۳۹۸ با هدف افزایش تأثیرگذاری اجتماعی و هم‌اندیشی و هم‌افزایی صنعت و دانشگاه در جهت توسعه و ارتقای امنیت صنایع مرتبط با فناوری‌های نوین اطلاعاتی و ارتباطی و ترویج مفاهیم و اصول امنیت و رمز در راستای برنامه‌های اصلی و جانبی کنفرانس شانزدهم انجمن رمز ایران برگزار شد که یکی از نتایج این هم‌اندیشی، پیشنهاد برگزاری میزگرد و نشست در حاشیه کنفرانس است. در میزگرد هم‌اندیشی «مسائل مدیریتی، سیاست‌گذاری و قانون‌گذاری در امنیت زیرساخت‌های حیاتی کشور»، تلاش شد فضای فکری و حاکمیتی را به محیط عملیاتی صنایع و سازمان‌ها نزدیک کنیم، به‌طوری‌که محیط و برنامه‌های شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران، فرصت مناسبی برای ارتباط کارشناسان و مدیران صنایع با تصمیم‌سازان دولتی و جامعه دانشگاهی و پژوهش‌گران باشد. نشست طرح مسأله «امنیت سامانه‌های کنترل صنعتی و اینترنت اشیاء»، نیز فرصتی برای شناسایی چالش‌های پیش رو و تعریف مسائل فنی و علمی مرتبط را با مشارکت اساتید، پژوهش‌گران دانشگاهی، مدیران، کارشناسان صنایع، نمایندگان سازمان‌ها و ذی‌نفعان فراهم نمود.

معتقدیم این کنفرانس فرصت مناسبی برای ارائه آخرین یافته‌های علمی، پژوهشی و فناوری اندیشمندان و متخصصان در حوزه امنیت فضای تبادل اطلاعات بوده و تأثیر آن بر توسعه راهکارهای بهبود امنیت زیرساخت‌های حیاتی، حساس و مهم کشور و نیز توسعه امن اینترنت اشیاء در ارتقای رفاه عمومی، چشمگیر بود. همچنین فرصت مناسبی برای برقراری تعامل علمی در این حوزه با کشورهای همسایه فراهم ساخته و با تقویت دیپلماسی علمی موجب افزایش جایگاه علمی و فنی ایران اسلامی عزیز در دنیا شد. البته برگزاری شایسته این کنفرانس نیز مانند هر کار بزرگی تنها در سایه توجه و عنایت حضرت حق میسر شد و مرهون مشارکت جمعی و همگانی و نیز بهره‌مندی از خردجمعی است. بنابراین برخود لازم می‌دانم از تلاش‌های مستمر کمیته علمی و اجرایی در دانشگاه فردوسی مشهد مخصوصاً خانم دکتر امین طوسی، آقای دکتر حسینی سنو و آقای مهندس طیرانی راد و نیز اعضای کمیته علمی مرکزی و شورای اجرایی انجمن رمز ایران مخصوصاً آقای دکتر سلماسی زاده، آقای مهندس رستمی و آقای مهندس حبیبی و نیز حمایت‌های مادی و معنوی مسئولین محترم انجمن رمز ایران، دانشگاه فردوسی مشهد و دانشکده مهندسی و مخصوصاً آقای دکتر عارف، آقای دکتر کافی و آقای دکتر پوررضا تشکر و قدردانی نمایم.

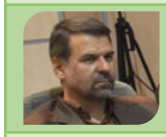
عباس قائمی بافقی

دانشیار گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد و دبیر کنفرانس

۴- محورهای کنفرانس

ردیف	عنوان محور	مسئولان محور
۱	مبانی رمزشناسی	دکتر ترانه اقلیدس (دانشگاه صنعتی شریف) دکتر محمدرضا هوشمند اصل (دانشگاه یزد)
۲	پیاده‌سازی الگوریتم‌های رمزنگاری و حملات مرتبط	دکتر بیژن علیزاده (دانشگاه تهران)
۳	امنیت شبکه	دکتر مرتضی امینی (دانشگاه صنعتی شریف)
۴	پروتکل‌های امنیتی	مهندس جواد مهاجری (دانشگاه صنعتی شریف)
۵	امنیت رایانش	دکتر عباس قائمی بافقی (دانشگاه فردوسی مشهد)
۶	مهندسی امنیت و امنیت خدمات الکترونیکی	دکتر محمدحسام تدین (مرکز تحقیقات مخابرات ایران)
۷	نهان‌سازی اطلاعات	دکتر محمدعلی اخایی (دانشگاه تهران) دکتر شاهرخ قائم مقامی (دانشگاه صنعتی شریف)
۸	جرم‌یابی در فضای مجازی	دکتر رضا ابراهیمی آتانی (دانشگاه گیلان)
۹	علمی - ترویجی: امنیت سامانه‌های کنترل صنعتی	دکتر محمود سلماسی زاده (دانشگاه صنعتی شریف)
۱۰	علمی - ترویجی: امنیت اینترنت اشیاء	دکتر محمدحسین یغمایی مقدم (دانشگاه فردوسی مشهد)

۵- ساختار اجرایی و دبیرخانه کنفرانس

رئیس کنفرانس		**دکتر محمد کافی** رئیس دانشگاه فردوسی مشهد
دبیر کنفرانس		**دکتر عباس قائمی بافقی** گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد
دبیر کمیته علمی		**دکتر هاله امین‌طوسی** گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد
دبیر کمیته اجرائی		**دکتر سیدامین حسینی سنو** گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد
مسئول کمیته دبیرخانه		**مهندس احسان طیرانی راد** مرکز فناوری اطلاعات و ارتباطات دانشگاه فردوسی مشهد
مدیر اجرایی		**مهندس مهدی مولودیان** دانشکده مهندسی دانشگاه فردوسی مشهد

تیم دانشجویی از آزمایشگاه امنیت داده‌ها و ارتباطات
و شاخه دانشجویی انجمن رمز ایران در دانشگاه فردوسی مشهد

مهندس مسعود خسروی فارمد، مهندس علی احمدیان رمکی، مهندس زهرانخعی، مهندس فاطمه چارلنک بختیاری، مهندس فاطمه سادات ترابی، مهندس مهدی نیکوقدم، سید محمدرضا ایازی، امیرعلی ابراهیمی، سجاد ایرانمنش، امیر دوانلو، مارال فراشاهی، زهرا رضوی‌پور، حمید نجفی، نگین فرهنگ، مریم محمودی قرایی، زهرا کیانی، مجید عسگری، شهلا وزیری، علی عاملی و مهندس نسترن صفوی (دانشگاه صنعتی امیرکبیر)

با سپاس ویژه از همکاران
مرکز فناوری اطلاعات و ارتباطات، مرکز آموزش‌های الکترونیکی و دانشکده مهندسی دانشگاه فردوسی مشهد

دکتر حمیدرضا پوررضا، دکتر رضا لطفی، دکتر مهدی پورافشاری، مهندس داوود شکری، مهندس شهره مرجانی، مهندس طاهره خواجه‌نژاد، مهندس زهره زکی‌زاده، مهندس علیرضا گیوان، خانم فهیمه علی‌اکبری، مهندس کیارش مجتهدین یزدی، آقای الیاس نیازی، آقای علیرضا اکبری، آقای حسن سلیمانی، آقای سیدمهدی مجیدی، آقای سجاد نیازی، آقای سیدمهدی ابطحی

و با تشکر از مساعی همکاران مرکز منطقه‌ای شمال شرق شهید فهمیده مهندس جعفر زارع، مهندس محمدرضا کشمیری، مهندس نوید انوری‌پور، مهندس مسعود داوری و مهندس امیرمحمد محمدزاده

۶- کمیته علمی کنفرانس

ردیف	نام و نام خانوادگی	دانشگاه
۱	دکتر رضا ابراهیمی آتانی	دانشگاه گیلان
۲	دکتر زهرا احمدیان	دانشگاه شهید بهشتی
۳	دکتر محمود احمدیان عطاری	دانشگاه صنعتی خواجه نصیرالدین طوسی
۴	دکتر محمدعلی اخایی	دانشگاه تهران
۵	دکتر محسن اسدی	دانشگاه فردوسی مشهد
۶	دکتر زیبا اسلامی	دانشگاه شهید بهشتی
۷	دکتر ترانه اقلیدس	دانشگاه صنعتی شریف
۸	دکتر هاله امین‌طوسی	دانشگاه فردوسی مشهد
۹	دکتر مرتضی امینی	دانشگاه صنعتی شریف
۱۰	دکتر نصور باقری	دانشگاه تربیت دبیر شهید رجایی
۱۱	دکتر سیاوش بیات سرمدی	دانشگاه صنعتی شریف
۱۲	دکتر علی پاینده	دانشگاه صنعتی مالک‌اشتر
۱۳	دکتر محمدحسام تدین	پژوهشگاه ارتباطات و فناوری اطلاعات
۱۴	دکتر بهروز ترک لادانی	دانشگاه اصفهان
۱۵	دکتر علی جهانیان	دانشگاه شهید بهشتی
۱۶	دکتر سیدامین حسینی سنو	دانشگاه فردوسی مشهد
۱۷	دکتر صادق دری نوگورانی	دانشگاه تربیت مدرس
۱۸	دکتر محمود سلماسی‌زاده	دانشگاه صنعتی شریف
۱۹	دکتر مهران سلیمان فلاح	دانشگاه صنعتی امیرکبیر
۲۰	دکتر هادی سلیمانی	دانشگاه شهید بهشتی
۲۱	دکتر محمدرضا عارف	دانشگاه صنعتی شریف
۲۲	دکتر محمد عبدالهی ازگمی	دانشگاه علم و صنعت ایران
۲۳	دکتر بیژن علیزاده	دانشگاه تهران
۲۴	دکتر شاهرخ قائم‌مقامی	دانشگاه صنعتی شریف
۲۵	دکتر عباس قائمی بافقی	دانشگاه فردوسی مشهد

ردیف	نام و نام خانوادگی	دانشگاه
۲۶	دکتر محسن کاهانی	دانشگاه فردوسی مشهد
۲۷	دکتر علیرضا کشاورز حداد	دانشگاه شیراز
۲۸	دکتر فرید محمد مالک قائینی	دانشگاه یزد
۲۹	دکتر حمید ملا	دانشگاه اصفهان
۳۰	مهندس جواد مهاجری	دانشگاه صنعتی شریف
۳۱	دکتر عبدالرسول میرقدری	دانشگاه امام حسین (ع)
۳۲	دکتر مهتاب میرمحسنی	دانشگاه صنعتی شریف
۳۳	دکتر عابدین واحدیان مظلوم	دانشگاه فردوسی مشهد
۳۴	دکتر محمودرضا هاشمی	دانشگاه تهران
۳۵	دکتر محمدرضا هوشمند اصل	دانشگاه یزد
۳۶	دکتر محمدحسین یغمایی مقدم	دانشگاه فردوسی مشهد
۳۷	**Dr. Amir Moradi**	Ruhr-Universitaet Bochum
۳۸	**Prof. Josef Pieprzyk**	Mcquarie University
۳۹	**Prof. Joachim Posegga**	University of Passau

۷- برنامه‌های شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران

تاریخ	عنوان برنامه	زمان	
روز چهارشنبه مورخ ۱۳۹۸/۶/۶	پذیرش	۸	۸:۳۰
	مراسم آغازین کنفرانس	۸:۳۰	۹:۳۰
	سخنرانی کلیدی: دکتر محمدرضا پاکروان، دانشگاه صنعتی شریف	۹:۳۰	۱۰:۳۰
	پذیرایی و بازدید از نمایشگاه	۱۰:۳۰	۱۱
	سخنرانی کلیدی: دکتر ترانه اقلیدس، دانشگاه صنعتی شریف	۱۱	۱۲
	اقامه نماز و صرف ناهار	۱۲:۰۰	۱۳:۳۰
	مجمع عمومی انجمن رمز ایران	۱۳:۳۰	۱۴:۳۰
	نشست ۱: امنیت اینترنت اشیاء و سامانه‌های صنعتی، جرم‌یابی سخنرانی مدعو: دکتر حسین قرائی، پژوهشگاه ارتباطات و فناوری اطلاعات	۱۴:۳۰	۱۶
	نشست ۲: پروتکل‌های امنیتی ۱	۱۴:۳۰	۱۶
	پذیرایی و بازدید از نمایشگاه	۱۶	۱۶:۳۰
	نشست ۳: امنیت شبکه سخنرانی مدعو: مهندس مرتضی نوفرستی، دانشگاه صنعتی شریف	۱۶:۳۰	۱۸
	نشست ۴: پروتکل‌های امنیتی ۲	۱۶:۳۰	۱۸
	میزگرد «مسائل مدیریتی، قانون‌گذاری و سیاست‌گذاری در امنیت زیرساخت‌های حیاتی کشور»	۱۸	۱۹:۳۰

تاریخ	عنوان برنامه	زمان	
روز پنج‌شنبه مورخ ۹۸/۶/۷	نشست ۵: مبانی رمزنگاری، پیاده‌سازی الگوریتم‌ها و پروتکل‌های رمزنگاری و حملات مرتبط سخنران مدعو: دکتر راضیه سالاری فرد، دانشگاه صنعتی شریف	۸:۳۰	۱۰
	نشست ۶: نهان‌سازی اطلاعات	۸:۳۰	۱۰
	مسابقه و ارزیابی ماراتن عمومی‌سازی امنیت و رمز	۸:۳۰	۱۰
	پذیرایی و بازدید از نمایشگاه	۱۰	۱۰:۳۰
	نشست ارائه‌های پوستری	۱۰:۳۰	۱۲:۳۰
	نشست طرح مسأله «امنیت سامانه‌های کنترل صنعتی و اینترنت اشیاء»	۱۰:۳۰	۱۲:۳۰
	رویداد شاخه‌های دانشجویی انجمن رمز ایران (گردهم‌آیی سالانه شاخه‌های دانشجویی)	۱۰:۳۰	۱۲:۳۰
	اقامه نماز و صرف ناهار	۱۲:۳۰	۱۴
	نشست ۷: مبانی رمزنگاری سخنرانی مدعو: دکتر محمدعلی ارومیه‌چی‌ها، پژوهشگاه خواجه نصیر طوسی	۱۴	۱۵:۳۰
	نشست ۸: امنیت رایانش	۱۴	۱۵:۳۰
	پذیرایی	۱۵:۳۰	۱۶
	مراسم پایانی کنفرانس و تقدیر از برگزیدگان	۱۶	۱۷:۳۰

۸- سخنرانی‌های کلیدی و مدعو

عنوان	ارائه‌دهنده	دانشگاه	نوع
درس‌ها و تجربه‌هایی از توسعه توانمندی‌های ملی در حوزه سیستم‌های مخابرات نوری	 دکتر محمدرضا پاکروان	دانشگاه صنعتی شریف	سخنرانی کلیدی
رمزنگاری در عصر کوانتوم	 دکتر ترانه اقلیدس	دانشگاه صنعتی شریف	سخنرانی کلیدی
امنیت شهر هوشمند	 دکتر حسین فرائی گرکانی	پژوهشگاه ارتباطات و فناوری اطلاعات	سخنرانی مدعو
شکار تهدیدات در شبکه‌های با پهنای باند بالا	 مهندس مرتضی نوفرستی	دانشگاه صنعتی شریف	سخنرانی مدعو
معماری کارا و سریع ضرب نقطه‌ای روی خم ۲۵۵۱۹	 دکتر راضیه سالاری‌فرد	دانشگاه صنعتی شریف	سخنرانی مدعو
روند پژوهش‌های دانش رمزنگاری در سطح بین‌الملل	 دکتر محمدعلی اروميه‌چی‌ها	پژوهشگاه خواجه نصیرالدین طوسی	سخنرانی مدعو

۹- چکیده سخنرانی‌های کلیدی و مدعو

درس‌ها و تجربه‌هایی از توسعه توانمندی‌های ملی در حوزه سیستم‌های مخابرات نوری

دکتر محمدرضا پاکروان

چکیده: مخابرات نوری، یکی از مهمترین زیرساخت‌های توسعه ارتباطات در سه دهه گذشته بوده است. دانش و فناوری این حوزه، نقشی مهم در گسترش شبکه‌های مخابراتی و توسعه اینترنت و سرویس‌های مبتنی بر آن داشته است. دستاوردهای صنعتی مخابرات نوری، این امکان را فراهم ساخته که شبکه‌های مخابراتی با ظرفیتی زیاد و در پهنه جغرافیایی وسیع و گسترده‌ای ایجاد شوند و دسترسی به تلفن، موبایل و اینترنت در کشورهای مختلف جهان از جمله ایران توسعه بیابد. دسترسی پر سرعت به اطلاعات و محتوای چندرسانه‌ای که یکی از محورهای مهم توسعه‌یافتگی کشورها محسوب می‌شود، با گسترش و رشد زیرساخت‌های مخابرات نوری امکان‌پذیر شده است. روند رشد دانش و فناوری در این حوزه بسیار سریع بوده و اثرگذاری آن در صنعت مخابرات بسیار بنیادی است. از همین رو، توسعه دانش و فناوری‌های مرتبط با مخابرات نوری در اولویت بالایی برای کشورهای صنعتی و پیشرفته قلمداد می‌شود و سرمایه‌گذاری‌ها و پیشرفت‌های آنان در این حوزه به خوبی مشهود است. در کشور ما نیز، در دو دهه گذشته فعالیت‌های خوب و مؤثری در این زمینه صورت گرفته است و نتایج خوبی در صنعت مخابرات ما به دست آمده است. در این جلسه، مروری بر تلاش‌های صورت گرفته در توسعه توانمندی‌های ملی در این عرصه خواهیم داشت و نتایج و تجارب حاصله را مورد بررسی قرار خواهیم داد.

رمزنگاری در عصر کوانتوم

دکتر ترانه اقلیدس

چکیده: در طی سه دهه گذشته، رمزنگاری نامتقارن به بخش جدایی‌ناپذیر از زیرساخت مخابرات رقمی تبدیل شده است. رمزنگاری نامتقارن نقش مهمی در امنیت شبکه‌های تلفن همراه، محاسبات ابری، شبکه‌های اجتماعی، پرداخت الکترونیکی و غیره ایفا می‌کند. دست‌یابی به ارتباطات امن در شبکه‌ها یکی از مهم‌ترین مسائل در فناوری اطلاعات بوده است. این به دلیل توسعه و بهره‌برداری از انواع شبکه‌های مخابراتی در دوران کنونی است. از سوی دیگر، پیشرفت در رایانه‌های کوانتومی، مفروضات امنیتی را، که رمزنگاری‌های کلید عمومی موجود برآن استوار است، تهدید می‌کند.

در این سخنرانی تحولات اخیر در رمزنگاری پساکوانتومی به‌اختصار بیان می‌شود. معیارهای طراحی و الزامات امنیتی، که توسط مؤسسه ملی استاندارد و فناوری آمریکا به طور خاص تعیین شده است، بیان می‌شود. علاوه بر این، عواملی که باید در هنگام بررسی الگوریتم‌های رمزنگاری کلید عمومی و مقایسه آنها مورد توجه قرار گیرد، ارائه می‌شود.

امنیت شهر هوشمند

دکتر حسین قرائی گرکانی

چکیده: امنیت و حریم خصوصی همواره یکی از چالش‌های اساسی در طراحی و توسعه سیستم‌ها می‌باشد که شهرهای هوشمند نیز از این قاعده مستثنی نمی‌باشند. در شهرهای هوشمند به‌علت استفاده از طیف وسیعی از سیستم‌ها و فناوری‌های هوشمند، ویژگی‌های خاص، درگیری با داده‌های مردم، ایجاد امنیت و حفظ حریم خصوصی افراد بسیار پیچیده‌تر خواهد بود. برای تأمین امنیت در شهرهای هوشمند، معماری‌ها و رویکردهای متفاوتی پیشنهاد شده که در آنها از فناوری‌های بروزی نظیر رمزنگاری، یادگیرین ماشین، داده‌کاوی و ... استفاده شده است تا بتوان ایجاد امنیت را به صورت بهینه تضمین نمود. همچنین تأمین حریم خصوصی در شهرهای هوشمند بر مشارکت افراد در شهر هوشمند و شبکه‌های اجتماعی تأثیر می‌گذارد و موجب ارتقاء سطح خدمات می‌شود. هر چند بعلت گسترده و پیچیده بودن موضوع امنیت در شهرهای هوشمند، هنوز یک معماری و رویکرد کلی و جامع که بتواند تمامی ابعاد و اجزاء شهر هوشمند را از حیث تأمین امنیت و حریم خصوصی پشتیبانی و حمایت کند، معرفی نشده است؛ اما کارهای تحقیقاتی وسیعی انجام شده و در حال انجام می‌باشد. این سخنرانی با مروری بر تحقیقات انجام شده در زمینه چالش‌های امنیتی، نیازمندی‌های امنیتی و تهدیدات و حریم خصوصی شهر هوشمند، سعی بر آگاه‌سازی جامعه امنیتی کشور و حوزه‌های تصمیم‌گیر در عصر تحول دیجیتال دارد.

شکار تهدیدات در شبکه‌های با پهنای باند بالا

مهندس مرتضی نوفرستی

چکیده: تعداد حملات سایبری و اثرات مخرب آن‌ها روز به روز در حال افزایش است. سؤال مهم این است که چرا با وجود هزینه‌های فراوان و تلاش مدیران شبکه‌ها همچنان حملات با نرخ

بالایی اتفاق می‌افتند. روش‌های محافظت از شبکه‌ها، همانند گذشته شامل مواردی مانند خرید بهترین دیوار آتش موجود در بازار، نصب وصله، و بهنگام‌سازی سامانه‌ی تشخیص و جلوگیری از نفوذ می‌باشند. جالب اینجاست که مدیران شبکه‌ها انتظار افزایش امنیت از طریق اعمال روش‌های قدیمی در شبکه‌های بزرگ و پیچیده‌ی امروزی را دارند.

شکار تهدیدات در فضای سایبری یک رویکرد فعالانه برای بررسی اتفاق‌های ویژه در شبکه است. به جای اینکه منتظر یک حادثه برای رسیدگی باشیم، فرض می‌کنیم مهاجمین از موانع دفاعی ما عبور و در شبکه رخنه کرده‌اند. در فرآیند شکار تهدید، فرضیاتی بر مبنای دانش شبکه تعریف و راستی‌آزمایی می‌شوند. کمبود دانش از محیط و عدم توانایی تشخیص دقیق رویدادها، فرآیند شکار تهدید در شبکه‌های بزرگ را مشکل‌تر کرده است.

در این ارائه، سعی خواهیم کرد فرآیند شکار تهدید و چالش‌های انجام آن در شبکه‌های واقعی را تشریح کنیم. همچنین، فرصت‌های تحقیقاتی برای ارائه راه‌حل‌های هوشمندانه و راهکارهای مقیاس‌پذیر در جهت تشخیص فعالانه حملات در شبکه‌های با پهنای باند بالا را معرفی خواهیم کرد.

معماری کارا و سریع ضرب نقطه‌ای روی خم ۲۵۵۱۹

دکتر راضیه سالاری فرد

چکیده: رمزنگاری مبتنی بر خم بیضوی به دلیل سطح امنیت یکسان ولی طول کلید کوچکتر در مقایسه با سایر روش‌های کلاسیک رمزنگاری نامتقارن، بسیار مورد توجه قرار گرفته است. ضرب نقطه‌ای اساسی‌ترین عمل در محاسبات رمزنگاری خم بیضوی است. بدین ترتیب معماری‌های با سرعت بالا و پیچیدگی کم آن موجب طراحی سامانه‌های رمزنگاری کارا می‌شود. یکی از خم‌های امن که محاسبات سبکی نیز دارد، خم۲۵۵۱۹ است. این خم امروزه بسیار مورد توجه قرار گرفته است و از جمله کاربردهای آن می‌توان به پیام‌رسان WhatsApp و آخرین نسخه استاندارد TSL اشاره کرد. در این ارائه، یک ضرب‌کننده میدانی مبتنی بر روش کاراتسوبا و یک ضرب نقطه‌ای روی خم۲۵۵۱۹ با تأخیر کم ارائه می‌شود که بهبود این ضرب نقطه‌ای به دلیل استفاده از ضرب‌کننده میدانی خط‌لوله‌ای با تأخیر کم و زمان‌بندی کارای عملگرهای میدانی می‌باشد. به منظور ارزیابی این معماری با کارهای پیشین از پیاده‌سازی با استفاده از FPGA استفاده شده است. نتایج پیاده‌سازی گویای کاهش ۳۳ درصدی پیچیدگی و افزایش ۸۹ درصدی سرعت می‌باشد.

روند پژوهش‌های دانش رمزنگاری در سطح بین‌الملل

دکتر محمدعلی ارومیه‌چی‌ها

چکیده: شناخت موضوعات و چالش‌های کلیدی رمزنگاری در حال و آینده و فهم عمیق از جهت‌گیری پژوهش‌های جامعه رمزنگاری در سطح بین‌الملل نقش به‌سزایی در آینده‌نگری و اتخاذ تصمیمات راهبردی در این حوزه دارد. همچنین برآورد نیازهای پژوهشی-کاربردی آتی صنعت و استفاده از راه‌حل‌های بدیع و مبتنی بر دانش رمزنگاری راهکاری قابل تکیه برای بازیگران اصلی این حوزه ایجاد می‌کند. در این ارائه ضمن تأکید بر نقش روندشناسی در دانش رمزنگاری، به بررسی موضوعات و زمینه‌های علمی پژوهشی که در دنیای امروز مورد توجه قرار گرفته است می‌پردازیم.

نمایی از نشست‌های ارائه مقالات کنفرانس

۱۰- نشست‌های ارائه مقاله

شماره نشست	عنوان نشست	مقاله‌های ارائه شده
۱	امنیت اینترنت اشیاء و سامانه‌های صنعتی و جرم‌یابی	۳ مقاله
۲	پروتکل‌های امنیتی ۱	۴ مقاله
۳	امنیت شبکه	۳ مقاله
۴	پروتکل‌های امنیتی ۲	۴ مقاله
۵	مبانی رمزنگاری، پیاده‌سازی الگوریتم‌ها و پروتکل‌های رمزنگاری و حملات مرتبط	۳ مقاله
۶	نهان‌سازی	۳ مقاله
۷	مبانی رمزنگاری	۲ مقاله
۸	امنیت رایانش	۳ مقاله

۱۱- مقاله‌های ارائه شده شفاهی

مقاله‌های شفاهی ارائه شده در شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران			
ردیف	عنوان نشست	عنوان مقاله	نویسندگان
۱	امنیت اینترنت اشیاء و سامانه‌های صنعتی و جرم‌یابی	طرح زنجیره قالب با قابلیت تغییرپذیری تراکنش‌ها	آرین عرب نوری رضا ابراهیمی آتانی سپیده رهنما حمید شعبانی پور
۲		ارزیابی مجموعه حملات نشأت گرفته شده از حمله مردمیانی در شبکه‌های کنترل صنعتی با نگاه ویژه به پروتکل DNP3	محمد نوروززادگان فاطمه بابایی سعدان زکایی
۳		Blind Multipurpose Image Watermarking Based on Secret Sharing	زیبا اسلامی سرور شیدانی
۴	پروتکل‌های امنیتی ۱	Improvement of Digest Based Authentication Scheme for Biometric Verification	فائزه سادات بابامیر Murvet Kirci
۵		GSLHA: Group-based Secure Lightweight Handover Authentication Protocol for M2M Communication	محمدمهدی مدیری جواد مهاجری محمود سلماسی زاده
۶		A New RF-PUF Based Authentication of Internet of Things Using Random Forest Classification	امیر اشتری احمد شبانی بیژن علیزاده

مقاله‌های شفاهی ارائه شده در شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران			
ردیف	عنوان نشست	عنوان مقاله	نویسندگان
۷	پروتکل‌های امنیتی ۱	An Ultra-Lightweight RFID Mutual Authentication Protocol	عباس رهنما محمد بهشتی ترانه اقلیدس محمدرضا عارف
۸	امنیت شبکه	Investigating the Streaming Algorithms Usage in Website Fingerprinting Attack Against Tor Privacy Enhancing Technology	ریحانه عطاریان ستار هاشمی
۹	امنیت شبکه	فانوس: راهکار مقابله با حملات انگشت‌نگاری وب‌سایت	سعید شیروی امیرمهدی صادق‌زاده رسول جلیلی
۱۰	امنیت شبکه	شناسایی ربات‌های وب با استفاده از ترکیب رویکردهای مبتنی بر ماشین‌های بردار پشتیبان فازی	مجتبی سبزه‌کار مصطفی سبزه‌کار ابوالفضل اسلامی علی مهری خانیکی
۱۱	پروتکل‌های امنیتی ۲	A Lightweight Anonymous Authentication Protocol for IoT Wireless Sensor Networks	عباس رهنما محمد بهشتی ترانه اقلیدس محمدرضا عارف
۱۲	پروتکل‌های امنیتی ۲	ارزیابی عملکرد روش‌های تشخیص شبکه‌های بات در مقابل حملات تقلیدی	عطیه محمدخانی فاطمه فرجی مقصود عباس‌پور

مقاله‌های شفاهی ارائه شده در شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران

ردیف	عنوان نشست	عنوان مقاله	نویسندگان
۱۳	پروتکل‌های امنیتی ۲	یک تمایزگر تفاضلی برای دو دور الگوریتم رمزگذاری احرازاصالت شده π-Cipher	بهزاد سعیدی زهرا احمدیان
۱۴	پروتکل‌های امنیتی ۲	ارائه مدل عملی حفظ حریم خصوصی در قراردادهای هوشمند مبتنی بر زنجیره بلوکی با کاهش سربار	امیر میرزایی محمدحسین فرزام سیاوش بیات‌سرمدی
۱۵	مبانی رمزنگاری، پیاده‌سازی الگوریتم‌ها و پروتکل‌های رمزنگاری و حملات مرتبط	یک طرح تسهیم راز مقاوم در برابر تقلب مبتنی بر گراف	میثم نوروزی ترانه اقلیدس محمدرضا عارف
۱۶		Cryptanalysis of SP2DAS and 3PDA, Two Data Aggregation Schemes for Smart Grid	حمید امیریوسف زهرا احمدیان
۱۷		ارائه و پیاده‌سازی حمله‌ی زمانی برنشتاین بهبود یافته بدون داشتن دسترسی ریشه	وحید معراجی هادی سلیمانی
۱۸	نهان‌سازی	A Novel Steganography Algorithm Using Edge Detection and MPC Algorithm	عارف رضایی لیلی فرزین‌وش علی فرزام‌نیا
۱۹	نهان‌سازی	Blind Image Watermarking Based on Area Quantization	رامین طوسی محمدرضا صادقی محمدعلی اخایی
۲۰	نهان‌سازی	کاربرد یادگیری عمیق و شبکه عصبی پیچشی در نهان‌کاوی	مهدیه سمیعی وجیحه ثابتی

مقاله‌های شفاهی ارائه شده در شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران

ردیف	عنوان نشست	عنوان مقاله	نویسندگان
۲۱	مبانی رمزنگاری	Lightweight Involutive Components for Symmetric Cryptography	مجتبی دهنوی محمدرضا میرزایی اکبر محمودی
۲۲	مبانی رمزنگاری	Cryptanalysis of a Certificateless Signcryption Scheme	پروین رستگاری محمد دخیل علیان
۲۳	امنیت رایانش	Ransomware Detection Using Process Mining and Classification Algorithms	آلا بحرانی امیر جلالی بیدگلی
۲۴	امنیت رایانش	Inferring API Correct Usage Rules: A Tree-based Approach	مجید ذوالفقاری سولماز سلیمی مهدی خرازی
۲۵	امنیت رایانش	An Anonymous Attribute-based Access Control System Supporting Access Structure Update	مصطفی چگینی‌زاده محمد علی جواد مهاجری محمدرضا عارف

به یاد شادروان
دکتر مهدی برنجکوب

از مؤسسین
و همراهان همیشگی
انجمن رمز ایران

۱۲- چکیده مقاله‌های ارائه شده شفاهی

طرح زنجیره قالب با قابلیت تغییرپذیری تراکنش‌ها

آرین عرب نوری، رضا ابراهیمی آتانی، سپیده رهنمای لشکامی، حمید شعبانی پور

دانشگاه گیلان

چکیده: طی دهه اخیر مبحث زنجیره قالب، به یکی از جذاب‌ترین موضوعات روز تبدیل شده است. ویژگی‌های آن مانند غیر متمرکز بودن و عدم نیاز به طرف سوم قابل اعتماد، قابلیت انجام تراکنش‌های نظیر به نظیر، توافق جمعی و توزیع‌شده و قابلیت گم‌نامی با استقبال گسترده روبه‌رو شده است. زنجیره قالب که در ابتدا برای مقاصد مالی و رمزارزها استفاده می‌شد، با عنایت به مزایای مذکور، کاربردهای فراوانی در زمینه‌های مختلف یافته است. از جمله این زمینه‌ها می‌توان به اقتصاد و بانکداری، بازی و سرگرمی، سلامت الکترونیک و پزشکی، اینترنت اشیاء و زنجیره تأمین اشاره نمود. با وجود نیاز این زمینه‌ها به ویژگی‌های زنجیره قالب به‌نظر می‌رسد، زنجیره قالب در هر زمینه نیاز به شخص‌سازی دارد. زیرا در هر کاربرد، برخی از ویژگی‌ها مناسب بوده و برخی دیگر با توجه به کاربرد نیاز به تغییر دارند. یکی از این ویژگی‌ها، خصوصیت تغییر ناپذیری تراکنش‌های ثبت شده است که در بسیاری از کاربردها، به‌دلیل امنیت بالا ضروری است. با این وجود به‌نظر می‌رسد در بسیاری از موارد اعطای قابلیت تغییر تراکنش‌ها به شخص یا گروهی معتبر (در صورت وجود) می‌تواند مفید باشد. در همین راستا طرحی برای این منظور ارائه گردیده که این قابلیت را دارد که به افراد واجد شرایط امکان این تغییر را بدهد. طرح مذکور کاملاً منطبق بر ساختار و معماری زنجیره قالب بوده و با اندک تغییراتی قابل پیاده‌سازی است.

ارزیابی مجموعه حملات نشأت گرفته شده از حمله مردمیانی در شبکه‌های کنترل‌صنعتی با نگاه ویژه به پروتکل DNP3

محمد نوروززادگان، فاطمه بابایی، سعدان زکایی

دانشگاه صنعتی خواجه نصیرالدین طوسی - دانشگاه صنعتی امیرکبیر

چکیده: شبکه‌های کنترل‌صنعتی همواره بخش اصلی زیرساخت یک کشور محسوب می‌شوند و هرگونه آسیب رساندن به آنها می‌تواند آثار فاجعه‌باری را به همراه داشته باشد. تأمین امنیت این نوع از شبکه‌ها که امروزه به چالشی برای کشورها تبدیل شده است، از زمانی اهمیت پیدا کرد که نیروگاه اتمی نطنز قربانی این نوع از حملات شد. پس از آن شاهد افزایش این نوع از حملات بودیم چنانکه در سال ۲۰۱۵ حمله‌ای دیگر به زیرساخت برق کشور ترکیه صورت گرفت. بنابراین ما در این مقاله سعی کرده‌ایم مجموعه حملاتی که در یک شبکه‌ی کنترل‌صنعتی بعد از حمله‌ی مردمیانی قابلیت اجرا دارند را، پیاده‌سازی کرده و سپس براساس عامل زمان، حداقل تأخیری که این حملات می‌توانند براساس پروتکل DNP3 در یک شبکه‌ی کنترل‌صنعتی ایجاد کنند را به صورت تئوری بررسی کرده و نشان خواهیم داد که حملاتی که در شبکه‌های کامپیوتری مهم تلقی نمی‌شوند، در شبکه‌های کنترل‌صنعتی نقشی اساسی را ایفا می‌کنند.

Blind Multipurpose Image Watermarking Based on Secret Sharing

Sorour Sheidani, Ziba Eslami

Shahid Beheshti University

Abstract - In this paper, in order to accomplish two goals of multimedia authentication and copyright protection, we present a multipurpose watermarking method based on a commonly used cryptographic primitive called verifiable secret sharing scheme. Utilizing this primitive, our scheme achieves blindness meaning that it needs neither the original host image nor the embedded watermark. Our scheme also does not need two distinct watermarks to authenticate the images and at the same time protect their copyright. Experimental results show that the features of the shares, obtained by the used primitive from watermark, enables our method to reconstruct extracted tampered watermarks after various attacks such as JPEG compression, cropping, salt and pepper noise, median filtering, some combined attacks, etc. Comparisons are provided with other multipurpose watermarking methods which primarily aim at protecting copyright of media and authenticating it simultaneously. We also show the superiority of our proposed method to three watermarking methods attaining the goals of copyright protection and authentication.

Improvement of Digest Based Authentication Scheme for Biometric verification

Faezeh Sadat Babamir, Murvet Kirci

Istanbul Technical University

Abstract - Normally, authenticating a system in an untrusted environment is performed through mechanisms such as identification card, password checking and etc. However, by the development of technology, cracking such systems through forging password or stealing identification card may be done leading to the lack of security and hence privacy. This is why biometric based authentication systems are appropriate offer to provide security of clients. Through such systems, clients are verified and permitted to login to the system according to their physical or behavioral traits. Biometric systems offer several advantages over traditional authentication methods. Moreover,

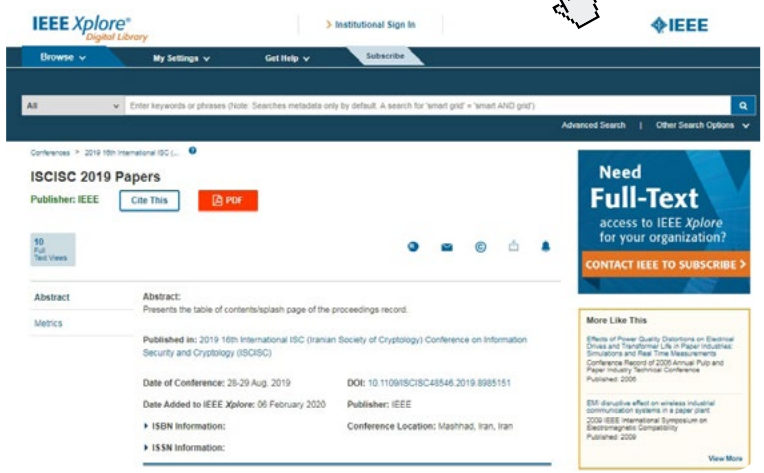
A New RF-PUF Based Authentication of Internet of Things Using Random Forest Classification

Amir Ashtari, Ahmad Shabani, Bijan Alizadeh

University of Tehran – School of Computer Science, IPM

Abstract - This paper presents a novel RF-PUF based authentication framework which exploits the intrinsic non-idealities in physical characteristic of a device/medium to generate a unique identity for wireless nodes. It also takes the advantage of Random Forest classification to securely identify the sender nodes based on their unique features extracting from already-existing modules in the receiver side. In contrast to the neural network-based schemes, our proposed approach incurs lower design complexity and overheads, while it no longer needs a large amount of preparatory and preprocessing works related to the learning process and adjusting the network parameters. Thus, the overall runtime required to preparing and testing of network is drastically lessened. The experimental results show that the proposed scheme can reach to 100% accuracy in the identification of 225 nodes when a forest network with 100 trees and depth of 20 is developed, posing a negligible overhead on the receiver side. This high accuracy can be nearly achieved even in the presence of channel variations as our approach has less sensitivity to environmental conditions.

مقالات انگلیسی کنفرانس در IEEE Xplore نمایه شده‌اند.



these systems, protects the privacy of clients, confidentiality and integrity of critical information for emerging technology such as smartphones and other appliances. In this paper, we improved our previous biometric authentication system and through some practical scenarios, we considered different attacks from client, server, and network sides to intrude into the privacy. We mathematically proved that our scheme is indistinguishable and prevents the attacker to threat legitimate individuals› information and privacy. Finally, we showed our computation and memory efficiency compared with related studies.

GSLHA: Group-based Secure Lightweight Handover Authentication Protocol for M2M Communication

Mohammad Mahdi Modiri, Javad Mohajeri, Mahmoud Salmasizadeh

Sharif University of Technology

Abstract - Machine to machine (M2M) communication, which is also known as machine type communication (MTC), is one of the most fascinating parts of mobile communication technology and also an important practical application of the Internet of Things. The main objective of this type of communication, is handling massive heterogeneous devices with low network overheads and high security guarantees. Hence, various protocols and schemes were proposed to achieve security requirements in M2M communication and reduce computational and communication costs. In this paper, we propose the group-based secure lightweight handover authentication (GSLHA) protocol for M2M communication in LTE and future 5G networks. The proposed protocol mutually authenticates a group of MTC devices (MTCDs) and a new eNodeB (eNB) when these simultaneously enter the coverage of the eNB with considering all the cellular network requirements. The security analysis and formal verification by using the AVISPA tool show that the protocol has been able to achieve all the security goals and overcome various attacks. In addition, the comparative performance analysis of the handover authentication protocols shows that the proposed protocol has the best computational and communication overheads.

An Ultra-Lightweight RFID Mutual Authentication Protocol

Abbas Rahnama, Mohammad Beheshti-Atashgah, Taraneh Eghlidos, Mohammad Reza Aref

Sharif University of Technology - Malek-Ashtar University of Technology

Abstract - In some applications of the Internet of Things (IoT), for privacy preserving and authentication of entities, it is necessary to use ultra-lightweight cryptographic algorithms. In this paper, we propose a new ultra-lightweight authentication protocol between RFID components, in which only simple operations are used. In this protocol, the server has access to the data gathered by the tag in the same authentication phase through the reader interface, instead of sharing a secret key. The proposed protocol is secure against several attacks, such as replay attacks, denial of service, offline guessing attacks, modification attacks, full disclosure attacks and impersonation attacks, in addition to its practicality when compared to the previously proposed RFID authentication protocols. It also provides anonymity of tags against readers and the other tags involved in the protocol.

Investigating the Streaming Algorithms Usage in Website Fingerprinting Attack Against Tor Privacy Enhancing Technology

Reyhane Attarian, Sattar Hashemi

Shiraz University Shiraz

Abstract - Website fingerprinting attack is a kind of traffic analysis attack that aims to identify the URL of visited websites using the Tor browser. Previous website fingerprinting attacks were based on batch learning methods which assumed that the traffic traces of each website are independent and generated from the stationary probability distribution. But, in realistic scenarios, the websites› concepts can change over time (dynamic websites) that is known as concept drift. To deal with data whose distribution change over time, the classifier model must update its model permanently and be adaptive to concept drift. Streaming algorithms are dynamic models that have these features and lead us to make a comparison of various representative data stream classification algorithms for website fingerprinting. Given to our experiments and results, by considering streaming algorithms along with statistical flow-based network traffic features, the accuracy grows significantly.

فانوس: راهکار مقابله با حملات انگشت‌نگاری وب‌سایت

سعید شیروی، امیرمهدی صادق‌زاده، رسول جلیلی

دانشگاه صنعتی شریف

چکیده: حملات انگشت‌نگاری وب‌سایت از جمله حملات تحلیل ترافیک هستند که مهاجم با نظارت بر ترافیک کاربران به شناسایی فعالیت وب آنان می‌پردازد. این حملات حتی زمانی‌که کاربران از سازوکارهای ارتقای حریم خصوصی، مانند شبکه تُر بهره برده باشند نیز مؤثرند. تحقیقات اخیر نشان داده‌اند که مهاجم با استفاده از شبکه عصبی عمیق، قادر است با دقت ۹۸٪، وب‌سایت‌های بازدید شده توسط کاربر را شناسایی کند. این درحالیست که سازوکارهای ارائه شده به منظور مقابله با این حملات، یا سربار پهنای باند و زمانی بالایی به کاربران تحمیل می‌کنند یا آنکه در مقابل حملات اخیر، عملاً مؤثر نیستند. در این مقاله سازوکار دفاعی جدیدی بر اساس آزمایش انسداد معرفی خواهیم کرد. در روش پیشنهادی آنچه یک شبکه عصبی به عنوان الگو از داده‌ها برداشت می‌کند را شناسایی خواهیم کرد و بر این اساس، الگوی ترافیک شبکه را به گونه‌ای تغییر خواهیم داد که شبکه عصبی در دسته‌بندی ترافیک کاربران با خطا مواجه شود. این روش با کاهش دقت مهاجم از ۹۸٪ به ۱۹٪ تنها با سربار پهنای باند ۴۷٪ و بدون داشتن سربار زمانی، در مقابل حملاتی که از شبکه عصبی بهره برده‌اند کاملاً مؤثر است.

شناسایی ربات‌های وب با استفاده از ترکیب رویکردهای مبتنی بر ماشین‌های بردار پشتیبان فازی

مصطفی سبزه‌کار، مجتبی سبزه‌کار، سید ابوالفضل اسلامی، علی مهری خانیکی

دانشگاه صنعتی بیرجند- دانشگاه آزاد اسلامی واحد بیرجند

چکیده: ربات‌های وب، برنامه‌هایی هستند که به طور خودکار و به صورت بازگشتی اطلاعات و محتوای وب سایت‌ها را بازبینی می‌نمایند. برخی از این ربات‌ها نقش مخربی دارند. بنابراین، تشخیص ربات‌های وب از جمله مهم‌ترین چالش‌ها در زمینه امنیت وب است. در این مقاله به ارائه یک روش جدید ترکیبی بر مبنای ماشین‌های بردار پشتیبان فازی با هدف افزایش کارایی در تشخیص ربات‌های وب پرداخته شده است. به این منظور از سه روش ماشین بردار پشتیبان فازی استفاده شده و توابع تعلق آنها به منظور افزایش دقت پیش‌بینی، با یکدیگر ترکیب شده است. نتایج روش پیشنهادی با ماشین بردار پشتیبان استاندارد و همچنین هر یک از سه ماشین بردار پشتیبان فازی مورد استفاده، مقایسه شده است. معیارهای مورد مقایسه، دقت، ویژگی و حساسیت می‌باشد. نتایج حاکی از برتری روش پیشنهادی در معیارهای مورد بررسی نسبت به الگوریتم‌های مورد مقایسه در این مقاله است.

A Lightweight Anonymous Authentication Protocol For IoT Wireless Sensor Networks

Abbas Rahnama, Mohammad Beheshti-Atashgah, Taraneh Eghlidos, Mohammad Reza Aref

Sharif University of Technology - Malek-Ashtar University of Technology

Abstract - Lightweight authentication protocols are crucial for privacy preserving in Internet of Things (IoT). Authentication protocols should be implementable for devices with constrained memory and computational power in this area, in addition to resistance against cryptographic threats. On the other hand, these protocols should not impose a heavy computational load on such devices. In this paper we proposed an authentication protocol that properly meets these features. Our protocol is suitable for wireless sensor networks (WSNs). In this protocol, authentication is fulfilled with low communication and computational loads between sensors and users through the gateway interface using a hash function and XOR operations. Besides, the user has access the required data, collected by the sensor, in the same authentication phase.

ارزیابی عملکرد روش‌های تشخیص شبکه‌های بات در مقابل حملات تقلیدی

عطیه محمدخانی، فاطمه فرجی دانشگر، مقصود عباسپور

دانشگاه شهید بهشتی

چکیده: امروزه شبکه‌های بات به عنوان یکی از مهم‌ترین تهدیدات در امنیت اینترنت مطرح هستند. تاکنون تحقیقات بسیاری برای تشخیص شبکه‌های بات صورت گرفته است. دسته‌ای از روش‌های تشخیص شبکه‌های بات مبتنی بر رفتار، از ویژگی‌های آماری برای تشخیص ترافیک نرمال از بات استفاده می‌کنند. در اکثر این روش‌ها، ویژگی‌های آماری مربوط به «اندازه طول» بسته‌ها و «زمان‌بندی» جز ویژگی‌های اصلی، می‌باشد. در یک شبکه بات، یک مهاجم می‌تواند با دستکاری این ویژگی‌ها، رفتار یک شبکه نرمال را تقلید کند. در این مقاله با تغییر اندازه طول بسته‌های بات بر اساس توزیع نرمال P2P، یک شبکه بات P2P تقلیدی ارائه شده است که در آن توزیع طول بسته‌های بات و ویژگی‌های رفتاری مربوط به اندازه طول بسته‌ها، مشابه با ترافیک نرمال می‌باشد. سپس، میزان مقاومت و عملکرد روش‌های تشخیص شبکه بات P2P مبتنی بر رویکردهای آماری موجود در برابر حمله تقلیدی مورد ارزیابی قرار می‌گیرد. نتایج آزمایشات صورت گرفته، کاهش حدود ۲۸ الی ۶۳ درصدی نرخ تشخیص را نشان می‌دهد.

یک تمایزگر تفاضلی برای دو دور الگوریتم رمزگذاری احرازاصالت شده π-Cipher

بهزاد سعیدی، زهرا احمدیان

دانشگاه شهید بهشتی

چکیده: الگوریتم π-Cipher یکی از ۲۹ طرح راه یافته به دور دوم رقابت سزار می‌باشد. این الگوریتم دارای ساختاری موازی و اسفنجی است که از جایگشتی از نوع ARX بهره می‌برد و در دو نسخه و هر یک در انواع متعدد ارائه شده است. در این مقاله، الگوریتم π-Cipher با کلمات ۱۶ بیتی مورد بررسی قرار گرفته است. با تمرکز بر روی ساختار داخلی جایگشت π استفاده شده در این الگوریتم و با تحلیل تفاضلی بر روی دو دور آن، یک تمایزگر تفاضلی با احتمال 2^{-95} معرفی می‌شود. این نخستین تحلیل روی این الگوریتم با در نظر گرفتن جزئیات ساختار داخلی جایگشت آن می‌باشد.

ارائه مدل عملی حفظ حریم خصوصی در قراردادهای هوشمند مبتنی بر زنجیره بلوکی با کاهش سربار

امیر میرزایی، سیدمحمدحسین فرزام، سیاوش بیات سرمدی

دانشگاه صنعتی شریف

چکیده: در سال‌های اخیر با رشد روزافزون رمزارزها و فناوری زنجیره بلوکی، مدل‌های مختلفی از ارزهای دیجیتال ارائه شده است. هر یک از این رمزارزها دارای ویژگی‌های خاص خود می‌باشند. رمزارز اتریوم دارای قابلیت نوشتن قطعه کدهایی در داخل بلوک‌های زنجیره بلوکی می‌باشد که به صورت خودکار اجرا می‌شوند و به قراردادهای هوشمند معروف هستند. در اتریوم این قطعه کدها به صورت شفاف و بدون حفظ حریم خصوصی قابل اجرا هستند؛ این در حالی است که محرمانگی و حفظ حریم خصوصی از مهم‌ترین مؤلفه‌های امنیت در حوزه داده و شبکه می‌باشد. پیش‌تر نمونه‌هایی مانند اِنیگما، شُدوات و هاک برای رسیدن به این مهم ارائه شده است که دارای سربار قابل توجهی می‌باشند. همچنین بخشی از این نمونه‌ها خارج از زنجیره اجرا می‌شوند که دارای معایب خاص خود هستند. در این مقاله با بهبود مدل هاک سازوکاری برای حفظ حریم خصوصی در قراردادهای هوشمند ارائه شده است که سربار محاسباتی زمان اجرا را به میزان قابل توجهی کاهش می‌دهد. نتایج پیاده‌سازی مزایده دومین قیمت با استفاده از راهکار پیشنهادی نشان از بهبود نزدیک به ۵۰ درصدی در زمان اجرای قرارداد هوشمند در سمت مدیر دارد.

یک طرح تسهیم راز مقاوم در برابر تقلب مبتنی بر گراف

میثم نوروزی، ترانه اقلیدس، محمدرضا عارف

دانشگاه صنعتی شریف

چکیده: طرح تسهیم راز آستانه‌ای امکان تسهیم یک راز را در میان تعدادی از اعضا، به‌نام شرکت‌کنندگان، با ارائه سهم‌هایی به آنان فراهم می‌سازد. بازیابی راز تنها به کمک تعداد مشخص از سهم‌ها امکان‌پذیر است. بازیابی درست راز در این طرح‌ها منوط به رفتار درست شرکت‌کنندکان است. اما در دنیای واقعی ممکن است برخی از شرکت‌کنندگان تلاش کنند سهم‌های نادرستی ارائه دهند، که تقلب نام دارد. یک طرح تسهیم راز مقاوم این امکان را فراهم می‌کند که با حضور تعدادی متقلب هم‌چنان راز به‌درستی بازیابی شود. در این مقاله طرح تسهیم راز مقاومی ارائه می‌شود که با وجود تعداد بیشینه ممکن از شرکت‌کنندگان متقلب، راز به درستی بازیابی شود. در این طرح برای متقلب‌ها توانایی‌های زیادی در نظر می‌گیریم. آنان می‌توانند سهم‌های خود را متناسب با سهم‌های سایرین تغییر دهند و با یکدیگر ارتباط داشته باشند تا بهترین شیوه را برای تقلب به‌کارگیرند. این طرح امکان شناسایی و حذف متقلب‌ها را به کمک یک گراف جهت‌دار فراهم می‌سازد و نسبت به طرح‌های پیشین از پیچیدگی کمتری برای بازیابی راز برخوردار است. در عین حال دارای طول سهم کمتری نسبت به طرح‌های موجود است، که به کاهش سربار مخابراتی طرح می‌انجامد. به این ترتیب، طرح تسهیم راز پیشنهادی از دو جنبه پیچیدگی بازیابی راز و طول سهم از کارآیی بیشتری نسب به طرح‌های موجود برخوردار است.

Cryptanalysis of SP2DAS and 3PDA, Two Data Aggregation Schemes for Smart Grid

Hamid Amiryousefi, Zahra Ahmadian

Shahid Beheshti University

Abstract - This paper analyses the security of two recently proposed privacy preserving data aggregation schemes, called SP^{2}DAS and 3PDA. We show that, for both of these protocols, despite the designers› claims, there are efficient forgery attacks on the signature schemes used in. We present a selective forgery attack on the signature scheme of SP^{2}DAS in the key-only attack model and a selective forgery attack on the 3PDA›s signature scheme in the known-message attack model, requiring only two pairs of message-signature. Our results show that in both of these schemes, the attacker can inject any arbitrary faulty data into the data aggregated by the network, without being detected, which is a serious threat to the performance of the whole network.

ارائه و پیاده‌سازی حمله‌ی زمانی برنشتاین بهبود یافته بدون داشتن دسترسی ریشه

وحید معراجی، هادی سلیمانی

پژوهشکده فضای مجازی دانشگاه شهیدبهشتی

چکیده: دسته‌ی مهمی از حملات کانال‌جانبی با بهره‌بری از اختلاف زمانی موجود بین دسترسی پردازنده به اطلاعات حافظه‌ی اصلی و حافظه‌ی نهان، سعی بر استخراج مقادیر کلید سیستم رمزنگاری دارند. حمله‌ی زمانی برنشتاین یکی از حملات مهم مبتنی بر حافظه‌ی نهان محسوب می‌شود که قابل اعمال به پیاده‌سازی نرم‌افزاری AES است. حمله‌ی برنشتاین را می‌توان به دو مرحله‌ی مهم جمع‌آوری اطلاعات زمانی و استخراج مقادیر کلید از اطلاعات به دست‌آمده در مرحله‌ی اول تقسیم نمود. تاکنون روش‌های مختلفی برای بهبود حمله برنشتاین با تمرکز بر روی هر یک از مراحل این حمله جهت استخراج مقادیر بیش‌تر از کلید و یا اجرای حمله به ازای نمونه‌های اندازه‌گیری کم‌تر صورت گرفته‌است. فرض تمامی حملات ارائه شده، دسترسی مهاجم به آدرس‌های مجازی و در نتیجه داشتن دسترسی ریشه (access root) است. در این مقاله، روشی به منظور کاهش تعداد نمونه‌های اندازه‌گیری لازم برای اجرای حمله برنشتاین ارائه می‌کنیم که ویژگی مهم آن، عدم‌دسترسی به آدرس‌های مجازی بلوک‌های جداول مراجعه‌ی سیستم رمزنگاری است. به عبارت دیگر، ویژگی مهم روش ارائه شده این است که مهاجم نیازی به داشتن دسترسی ریشه در حین اجرای حمله ندارد. برهمین اساس در این مقاله نشان می‌دهیم، جلوگیری از دسترسی ریشه نمی‌تواند روش مناسبی به منظور جلوگیری از حمله برنشتاین باشد. روش ارائه شده به صورت عملی پیاده‌سازی و بر روی پردازنده‌ی intel4200 ui5 اجرا شده است. نتایج عملی نشان می‌دهد نه تنها روش ارائه شده نیاز به دسترسی ریشه ندارد، بلکه تعداد نمونه‌های اندازه‌گیری موردنیاز برای اجرای این حمله را از ۲۲۵ نمونه در مقاله اصلی به ۲۱۹ کاهش می‌یابد.

A Novel Steganography Algorithm using Edge Detection and MPC Algorithm

Aref Rezaei, Leili Farzinvash, Ali Farzamnia

University of Tabriz - University Malaysia Sabah Kota Kinabalu

Abstract - With the rapid development of the Internet, preserving the security of confidential data has become a challenging issue. An effective method to this end is to apply steganography techniques. In this paper, we propose an efficient steganography algorithm which applies edge detection and MPC algorithm for data concealment in digital images. The proposed

edge detection scheme partitions the given image, namely cover image, into blocks. Next, it identifies the edge blocks based on the variance of their corner pixels. Embedding the confidential data in sharp edges causes less distortion in comparison to the smooth areas. To diminish the imposed distortion by data embedding in edge blocks, we employ LSB and MPC algorithms. In the proposed scheme, the blocks are split into some groups firstly. Next, a full tree is constructed per group using the LSBs of its pixels. This tree is converted into another full tree in some rounds. The resultant tree is used to modify the considered LSBs. After the accomplishment of the data embedding process, the final image, which is called stego image, is derived. According to the experimental results, the proposed algorithm improves PSNR with at least 5.4 compared to the previous schemes.

Blind Image Watermarking Based on Area Quantization

Ramin Toosi, Mohammadreza Sadeghi, Mohammad Ali Akhaee

University of Tehran

Abstract - One of the ways to protect the intellectual property of a digital media is watermarking. In this paper, an image watermarking method based on quantization index modulation is proposed. The quantized parameter is the area formed by host signal samples considered as vertices of a polygon. In real images, host signal samples are the wavelet coefficient of the image block. The embedding distortion is minimized using an optimization method minimizing the mean square error value. Thus, the watermarked signal is close to the host signal as much as possible, which leads to a high imperceptible algorithm. The optimization problem is solved using the gradient descent method. The performance of the proposed method is investigated under different attacks, including: noise addition, compression, filtering and geometrical attacks using real world images. The results illustrate that the proposed method has better performance than other state-of-the-art methods in terms of robustness.

کاربرد یادگیری عمیق و شبکه عصبی پیچشی در نهان‌کاوی

مهدیه سمیعی، وجیهه ثابتی

دانشگاه الزهرا (س)

چکیده: نهان‌نگاری، ابزاری برای ارتباط محرمانه و در مقابل نهان‌کاوی علم کشف حضور اطلاعات نهان در رسانه دیجیتال می‌باشد. تاکنون نهان‌کاوی تصاویر دیجیتالی روی ویژگی‌های دست‌ساز پیچیده متمرکز بوده‌اند که از جمله آن می‌توان به مدل معروف و موفق SRM اشاره کرد، اما امروزه با استفاده از مدل‌های یادگیری عمیق می‌توان ویژگی‌هایی را به صورت خودکار استخراج کرد به عبارت دیگر مراحل استخراج ویژگی و طبقه‌بندی تحت یک معماری واحد قرار گرفتند. تکنیک‌های نهان‌کاوی مختلفی در تصاویر با استفاده از الگوریتم‌های یادگیری عمیق از جمله شبکه‌های عصبی پیچشی پیاده‌سازی شده‌اند. در این مقاله، به معرفی چهار تکنیک نهان‌کاوی GNCNN، Xu-NET، Ye-NET، YEDROUDJ-NET در این حوزه پرداخته شده است. پس از بررسی و مقایسه نتایج این چهار روش مشاهده شد که تکنیک YEDROUDJ-NET توانسته است به خطای احتمالی مشابه و در اغلب موارد کمتر از مدل SRM دست یابد. بنابراین روش‌های نهان‌کاوی مبتنی بر شبکه‌های عصبی پیچشی توانسته‌اند کارایی مشابه و حتی در مواردی بهتر از روش‌های نهان‌کاوی سنتی ارائه دهند.

Lightweight Involutive Components for Symmetric Cryptography

S. M. Dehnavi, M. R. Mirzaee Shamsabad, and A. Mahmoodi Rishakani

Kharazmi University – Shahid Beheshti University – Shahid Rajaee Teacher Training University

Abstract - Lightweight components are used in the design of modern lightweight ciphers. In the current paper, firstly we investigate a new family of lightweight 4 _ 4 almost MDS diffusion layers, mathematically, and determine when they are involutive. The proposed diffusion layers are suitable for software applications and have less fixed points, compared with the existent ones. Then, we examine the cryptographic properties of nonlinear components constructed by a 2-round Feistel scheme, theoretically, and propose some concrete examples of them, including lightweight hardware-oriented 8_8 S-boxes. We compare the presented S-boxes with the ones in Midori-128.

Cryptanalysis of a Certificateless Signcryption Scheme

Parvin Rastegari, Mohammad Dakhilalian

Isfahan University of Technology

Abstract - Certificateless public key cryptography (CL-PKC) is a useful method to solve the problems of traditional public key infrastructure (PKI) (i.e. necessity of requiring certificate managements) and identity-based (ID-based) setting (i.e. the key escrow problem) concurrently. Signcryption is an important cryptographic primitive which provides the goals of both signature and encryption schemes much more efficient than the sign-then-encrypt way. Proposing efficient certificateless signcryption (CL-SC) schemes in the standard model (without random oracles) has been a focus of many recent researches. In 2016, Zheng and Li proposed a CL-SC scheme and claimed that their scheme is confidential (IND-CCA) and unforgeable (EUF-CMA) against both key replacement and malicious KGC attacks, in the standard model. In this paper, we propose both key replacement and malicious KGC attacks against confidentiality and unforgeability of Zheng and Li›s scheme. Our proposed attacks show that in contrast to Zheng and Li›s claim, their scheme is neither confidential (IND-CCA) nor unforgeable (EUF-CMA) against key replacement and malicious KGC attacks.

Ransomware detection using process mining and classification algorithms

Ala Bahrani, Amir Jalaly Bidgoly

University of Qom

Abstrac - The fast growing of ransomware attacks has become a serious threat for companies, governments and internet users, in recent years. The increasing of computing power, memory and etc. and the advance in cryptography has caused the complicating the ransomware attacks. Therefore, effective methods are required to deal with ransomwares. Although, there are many methods proposed for ransomware detection, but these methods are inefficient in detection ransomwares, and more researches are still required in this field. In this paper, we have proposed a novel method for identify ransomware from benign software using process mining methods. The

proposed method uses process mining to discover the process model from the events logs, and then extracts features from this process model and using these features and classification algorithms to classify ransomwares. This paper shows that the use of classification algorithms along with the process mining can be suitable to identify ransomware. The accuracy and performance of our proposed method is evaluated using a study of 21 ransomware families and some benign samples. The results show j48 and random forest algorithms have the best ccuracy in our method and can achieve to 95% accuracy in detecting ransomwares.

Inferring API Correct Usage Rules: A Tree-based Approach

Majid Zolfaghari, Solmaz Salimi, Mehdi Kharrazi

Sharif University of Technology

Abstract - The lack of knowledge about API correct usage rules is one of the main reasons that APIs are employed incorrectly by programmers, which in some cases lead to serious security vulnerabilities. However, finding a correct usage rule for an API is a time-consuming and error-prone task, particularly in the absence of an API documentation. Existing approaches to extract correct usage rules are mostly based on majority API usages, assuming the correct usage is prevalent. Although statistically extracting API correct usage rules achieves reasonable accuracy, it cannot work correctly in the absence of a fair amount of sample usages. We propose inferring API correct usage rules independent of the number of sample usages by leveraging an API tree structure. In an API tree, each node is an API, and each node›s children are APIs called by the parent API. Starting from lower-level APIs, it is possible to infer the correct usage rules for them by utilizing the available correct usage rules of their children. We developed a tool based on our idea for inferring API correct usages rules hierarchically, and have applied it to the source code of Linux kernel v4.3 drivers and found 24 previously reported bugs.

An Anonymous Attribute-based Access Control System Supporting Access Structure Update

Mostafa Chegenizadeh, Mohammad Ali, Javad Mohajeri, Mohammad Reza Aref

Sharif University of Technology- Amirkabir University of Technology

Abstract - It is quite common nowadays for clients to outsource their personal data to a cloud service provider. However, it causes some new challenges in the area of data confidentiality and access control. Attribute-based encryption is a promising solution for providing confidentiality and fine-grained access control in a cloud-based cryptographic system. Moreover, in some cases, to preserve the privacy of clients and data, applying hidden access structures is required. Also, a data owner should be able to update his defined access structure at any time when he is online or not. As in several real-world application scenarios like e-health systems, the anonymity of recipients, and the possibility of updating access structures are two necessary requirements. In this paper, for the first time, we propose an attribute-based access control scheme with hidden access structures enabling the cloud to update access structures on expiry dates defined by a data owner.

مسئولین برخی از نشست‌های ارائه مقالات کنفرانس

دکتر محمود احمدیان - دکتر هادی سلیمانی

مسئولین برخی از نشست‌های ارائه مقالات کنفرانس

دکتر رسول جلیلی

دکتر زهرا احمدیان

دکتر حمید ملا

دکتر نصور باقری - مهندس جواد مهاجری

۱۳- مقاله‌های ارائه شده به صورت پوستر

مقاله‌های پوستری ارائه شده در شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران

ردیف	عنوان مقاله	نویسندگان
۱	Threat Extraction in IoT-Based Systems Focusing on Smart Cities	عباس نجاتی‌فر محمدعلی هادوی
۲	Classical-Quantum Multiple Access Wiretap Channel	هادی آقایی بهاره اخباری
۳	Fault tolerant non-linear techniques for scalar multiplication in ECC	زهرا صفار سیامک محمدی
۴	IoT-Based Anonymous Authentication Protocol Using Biometrics in Smart Homes	شایان مهران‌پور ناصر محمدزاده حسین قرایی
۵	An Efficient Secret Sharing-Based Storage System for Cloud-Based IoTs	مجید فرهادی حمیده بابپور رضا مرتضوی
۶	Analysis of Machine Learning Techniques for Ransomware Detection	فرخ‌الدین نوربهبهانی فرزانه رسولی محمد صابری
۷	CRT-Based Robust Data Hiding Method by Extracting Features in DCT Domain	علیرضا قائمی حبیب‌الله دانیالی
۸	SANUB: A new method for Sharing and Analyzing News Using Blockchain	آرین بلوچستانی مجتبی مهدوی یگانه حلاج دلارام جاودانی
۹	ارزیابی امنیت و کارایی طرح‌های توأم رمزنگاری و فشرده‌سازی تصویر به منظور ارائه رویکردهای جدید در ارتباطات بی‌سیم	رضا احمدیان بهروز خادم

مقاله‌های پوستری ارائه شده در شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران

ردیف	عنوان مقاله	نویسندگان
۱۰	طراحی شبکه امن با یکسوسازی و کنترل جریان داده‌ها	احسان واثقی محمود نادران طحان
۱۱	محدودسازی حمله سیاهچاله در شبکه‌های متحرک اقتضایی با استفاده از روش یادگیری Q	علی ناظمی حسین بهرامگیری
۱۲	تحلیل و بهبود «طرح احرازاصالت با حفظ مشروط حریم خصوصی CPPA» در شبکه‌های خودرویی	علیرضا آقاباقرلو جواد مهاجری محمود سلماسی‌زاده مهشید دلاور
۱۳	ارزیابی امنیتی بستر ابری اوپن استک در مقابل حملات از کاراندازی سرویس	نیما جوادی علیرضا شفیعی‌نژاد
۱۴	دسته‌بندی مشتریان شرکت‌های ارائه‌دهنده سرویس‌های پرداخت با استفاده از تارنمای فروشگاهی آنان به کمک روش‌های داده‌کاوی	محمدحسین حجتی بابک صادقیان
۱۵	پیاده‌سازی حمله لغت‌نامه‌ای به گذرواژه‌ها بر روی GPU	ابوالفضل سالمی بهبد کشاورزی محسن منصوری
۱۶	تشخیص تروجان سخت‌افزاری بر مبنای تحلیل توان مصرفی، با استفاده از الگوریتم PCA و شبکه عصبی مصنوعی MLP	علی فریدونی محمدعلی دوستاری حامد یوسفی
۱۷	آزمایش و مقایسه سامانه تشخیص نفوذ suricata در تعامل با بهترین سامانه‌های انتقال سریع بسته	رضا غلامعلی تبار مسعود رفیقی محسن عسکری
۱۸	سیستم‌های رأی‌گیری الکترونیکی مبتنی بر بلاکچین	زهرا سالار حمیدرضا محروقی سبحان علی‌آبادی

۱۴- چکیده مقاله‌های ارائه شده به صورت پوستر

Threat Extraction in IoT-Based Systems Focusing on Smart Cities

Abbas Nejatifar, Mohammad Ali Hadavi

Malek Ashtar University of Technology

Abstract - IoT-based services are widely increasing due to their advantages such as economy, automation, and comfort. Smart cities are among major applications of IoT-based systems. However, security and privacy threats are vital issues challenging the utilization of such services. Connectivity nature, variety of data technology, and volume of data maintained through these systems make their security analysis a difficult process. Threat modeling is one the best practices for security analysis, especially for complex systems. This paper proposes a threat extraction method for IoT-based systems. We elaborate on a smart city scenario with three services including lighting, car parking, and waste management. Investigating on these services, firstly, we identify thirty-two distinct threat types. Secondly, we distinguish threat root causes by associating a threat to constituent parts of the IoT-based system. In this way, threat instances can be extracted using the proposed derivation rules. Finally, we evaluate our method on a smart car parking scenario as well as on an E-Health system and identify more than 50 threat instances in each cases to show that the method can be easily generalized for other IoT-based systems whose constituent parts are known.

Classical-Quantum Multiple Access Wiretap Channel

Hadi Aghaee, Bahareh Akhbari

K. N. Toosi University of Technology

Abstract - In this paper, the quantum wiretap channel (QWTC) and quantum multiple access channel (QMAC) are used so as to introduce the classical-quantum multiple access wiretap channel (C-QMA-WTC). In this regard, the classical concepts about the multiple access wiretap channel (MA-WTC) are defined. Moreover, the multiple access wiretap channel with

classical inputs and quantum output is considered. An achievable secrecy rate region of C-QMA-WTC is derived. After presenting the results of quantum wiretap channel, we illustrate how mutual information can be used instead of the Holevo information in the expression of the secrecy capacity region.

Fault tolerant non-linear techniques for scalar multiplication in ECC

Zahra Saffar, Siamak Mohammadi

School of Electrical and Computer Engineering Tehran

Abstract - Elliptic curve cryptography (ECC) has shorter key length than other asymmetric cryptography algorithms such as RSA with the same security level. Existing faults in cryptographic computations can cause faulty results. If a fault occurs during encryption, false information will be sent to the destination, in which case channel error detection codes are unable to detect the fault. In this paper, we consider the error detection in elliptic curve scalar multiplication point, which is the most important operation in ECC. Our technique is based on non-linear error detection codes. We consider an algorithm for scalar multiplication point proposed by Microsoft research group. The proposed technique in our methods has less overhead for additions (36.36%) and multiplications (34.84%) in total, compared to previous works. Also, the proposed method can detect almost 100% of injected faults.

IoT-Based Anonymous Authentication Protocol Using Biometrics in Smart Homes

Shayan Mehranpoor, Naser Mohammadzadeh, Hossein Gharaee

Shahed University – ICT Research Institute (ITRC)

Abstract - The smart home is increasingly being considered as one of the Internet of Things applications. With the development of mobile networks and the speed of data transfer, the expansion of smartphones and increasing of interest in raising the safety factor in personal life, many companies have entered the smartphone market. With the help of the Internet of things portal, it is possible to monitor wireless sensors and use non-computerized alert systems. Therefore, it is essential to secure such a system to create a sense

of relaxation in the lives of users and homeowners to deal with possible occurrences. The integration of technologies for the automation of home affairs with the Internet of things means that all physical objects can be accessed on cyberspace; therefore, the concerns raised by users about the lack of privacy and security are a serious argument that science and technology should answer. This paper proposes an anonymous secure framework in connected smart home environments, using solely lightweight operations. The proposed framework in this paper provides efficient authentication and key agreement, and enables devices (identity and data) anonymity and unlinkability. It is demonstrated that computation complexity of the proposed framework is low as compared to the existing schemes, while security has been significantly improved. The proposed scheme ensures that even if the stakeholder's device or the Internet of Things device is attacked, the system remains secure.

An efficient secret sharing-based storage system for cloud-based IoTs

Majid Farhadi, Hamideh Bypour, Reza Mortazavi

Damghan University

Abstract -Internet of Things is the newfound information architecture based on the Internet that develops interactions between objects and services in a secure and reliable environment. As the availability of many smart devices rises, secure and scalable mass storage systems for aggregate data is required in IoTs applications. In this paper, we propose a new method for storing aggregate data in IoTs by use of (t; n)-threshold secret sharing scheme in the cloud storage. In this method, original data is divided into t blocks that each block is considered as a share. This method is scalable and traceable, i.e., new data can be inserted or part of original data can be deleted, without changing shares, also cloud service providers' fault in sending invalid shares are detectable.

Analysis of Machine Learning Techniques for Ransomware Detection

Fakhroddin Noorbehbahani, Farzaneh Rasouli, Mohammad Saberi

Isfahan University - Isfahan Aghigh Institute of Higher Education

Abstract - In parallel with the increasing growth of the Internet and computer networks, the number of malwares has been increasing every day. Today, one of the newest attacks and the biggest threats in cybersecurity is ransomware. The effectiveness of applying machine learning techniques for malware detection has been explored in much scientific research, however, there is few studies focused on machine learning-based ransomware detection. In this paper, the effectiveness of ransomware detection using machine learning methods applied to CICAndMal2017 dataset is examined in two experiments. First, the classifiers are trained on a single dataset containing different types of ransomware. Second, different classifiers are trained on datasets of 10 ransomware families distinctly. Our findings imply that in both experiments random forest outperforms other tested classifiers and the performance of the classifiers are not changed significantly when they are trained on each family distinctly. Therefore, the random forest classification method is very effective in ransomware detection.

CRT-Based Robust Data Hiding Method by Extracting Features in DCT Domain

Alireza Ghaemi, Habibollah Danyali

Shiraz University of Technology

Abstract - In this paper a robust data hiding method is presented by applying Discrete Cosine Transform (DCT) to the host signal and performing feature extraction, based on Chinese Remainder Theorem (CRT). Improving the robustness reduces the imperceptibility in watermarking systems due to the tradeoff between imperceptibility, robustness and capacity in data hiding schemes. The proposed method offers high imperceptibility alongside robustness. To embed the hidden information CRT based feature extraction process is carried out in DCT domain. Extracted features are distances of CRT remainders. These distances are not varied much in noisy situations thus it is possible to extract the hidden bits with high accuracy. To analyze the robustness of the proposed method common signal processing manipulations are applied to the watermarked images. Bit Correct Rate (BCR) values are calculated for extracted watermarks to evaluate the robustness. Results are compared to other state of the art methods and confirm the superiority of the proposed method.

SANUB: A new method for Sharing and Analyzing News Using Blockchain

Arian Balouchestani, Mojtaba Mahdavi, Yeganeh Hallaj, Delaram Javdani

University of Isfahan – Iran University of Science and Technology

Abstract - Millions of news are being exchanged daily among people. With the appearance of the Internet, the way of broadcasting news has changed and become faster, however it caused many problems. For instance, the increase in the speed of broadcasting news leads to an increase in the speed of fake news creation. Fake news can have a huge impression on societies. Additionally, the existence of a central entity, such as news agencies, could lead to fraud in the news broadcasting process, e.g. generating fake news and publishing them for their benefits. Since Blockchain technology provides a reliable decentralized network, it can be used to publish news. In addition, Blockchain with the help of decentralized applications and smart contracts can provide a platform in which fake news can be detected through public participation. In this paper, we proposed a new method for sharing and analyzing news to detect fake news using Blockchain, called SANUB. SANUB provides features such as publishing news anonymously, news evaluation, reporter validation, fake news detection and proof of news ownership. The results of our analysis show that SANUB significantly outperformed the existing methods.

به‌منظور ارائه رویکردهای جدید در ارتباطات بی‌سیم

رضا احمدیان، بهروز خادم

دانشگاه جامع امام حسین (ع)

چکیده: امروزه با توسعه روش‌های تصویربرداری در ارتباطات بی‌سیم، افزایش امنیت و کارایی در ارسال تصاویر نیازمند طرح‌های توأم رمزگذاری و فشرده‌سازی است. در روش‌های غیرتوأم، رمزگذاری و فشرده‌سازی دو فرآیند جدا از هم هستند و مهاجم می‌تواند حمله خود را به‌طور ساده‌تر ساماندهی کند. با وابسته کردن این دو عملیات به یکدیگر، خروجی دارای عدم قطعیت بیشتری می‌شود و سختی کار مهاجم و در نتیجه امنیت طرح افزایش می‌یابد. به همین دلیل اخیراً طرح‌های توأم رمزنگاری و فشرده‌سازی تصویر اهمیت و جایگاه خاصی یافته است. در این مقاله تعدادی از مهم‌ترین معیارهای کارایی و امنیتی در این طرح‌ها معرفی و بر اساس این معیارها این طرح‌ها با یکدیگر مقایسه شده‌اند. به‌علاوه در این مقاله بر اساس نتایج حاصل از مقایسه

این طرح‌ها، راهکارها و پیشنهادهایی برای طراحی یک طرح توأم امن و کارآمد ارائه شده است تا همزمان با توسعه دانش و فناوری ارتباطات بی‌سیم، کاربران بتوانند بر اساس نیازمندی‌های امنیتی و کارایی موردنظر خود یک طرح مناسب را انتخاب کنند.

طراحی شبکه امن با یکسوسازی و کنترل جریان داده‌ها

احسان واثقی، محمود نادران طحان

دانشگاه شهید چمران اهواز

چکیده: حفظ اطلاعات برای سازمان‌های دولتی، نظامی، شرکت‌های خصوصی و کاربران رایانه‌های شخصی از دیرباز موضوع مهمی بوده است و با فراگیر شدن اینترنت، این موضوع مهمتر از قبل شده است. یکی از راهکارهایی که برای استفاده در محیط‌های نظامی و صنعتی در سال‌های اخیر مورد توجه قرار گرفته، استفاده از یکسوسازهای جریان داده است. یکسوساز یک سکو برای حفظ داده‌های سازمانی و جلوگیری از نشت اطلاعات است که تبادل داده‌های بین دو کامپیوتر یا دو شبکه کامپیوتری را یک طرفه می‌کند. بر مبنای این سکو، قابلیت دریافت اطلاعات توسط یک شبکه حساس و امنیتی از یک شبکه غیرحساس و ناامن فراهم است در حالی که شبکه ناامن امکان دریافت اطلاعات از شبکه حساس و امن را نخواهد داشت. در این مقاله برای طراحی یک شبکه امن، یک راهکار برای طراحی سخت‌افزار یکسوساز جریان داده و یک سیستم نرم‌افزاری کنترل امنیت اطلاعات برای جلوگیری از ورود بدافزار به شبکه‌های امن ارائه خواهد شد. پیاده‌سازی اولیه سخت‌افزار و نرم‌افزار نشان می‌دهد که طراحی چنین سکویی با استفاده از سخت‌افزارهای ارزان قیمت و موجود در بازار قابل انجام است ضمن آن که هزینه ساخت و طراحی آن نیز نسبت به نمونه‌های مشابه کمتر است.

محدودسازی حمله سیاه‌چاله در شبکه‌های متحرک اقتضایی با استفاده از روش یادگیری Q

علی ناظمی، حسین بهرامگیری

دانشگاه صنعتی مالک اشتر

چکیده: شبکه‌های متحرک اقتضایی از جمله سیستم‌های خودکاری هستند که بدون ساختار مرکزی فرآیندهای جاری شبکه مانند مسیریابی، ارسال بسته‌ها و امن‌سازی ارتباط را انجام می‌دهند. محدودیت منابع، ساختار پویا، عدم وجود ساختار مرکزی از جمله چالش‌های موجود در این شبکه‌ها هستند. الگوریتم‌های مسیریابی بسیاری در این شبکه‌ها وجود دارند که مبنای تمامی آن‌ها لینک‌های قابل اعتماد و عدم وجود عامل مخرب می‌باشد. لذا الگوریتم‌های

مسیریابی به صورت اولیه مکانیزم امنیتی خاصی برای جلوگیری و تشخیص حملات شبکه را ندارند و بر این اساس روش‌های مختلفی در جهت افزایش امنیت این پروتکل‌ها ارائه شده است. ایجاد سامانه‌های شناسایی هوشمند و بهینه‌سازی مصرف انرژی در فرآیند تشخیص نفوذ از جمله چالش‌های سامانه‌های ارائه شده می‌باشد. هدف ما نیز در این مقاله ارائه روشی برای امنیت پروتکل مسیریابی AODV در مقابله با حمله سیاه‌چاله می‌باشد که قابلیت هوشمندسازی فرآیند تشخیص نفوذ را داشته باشد و همچنین سربار کمی بر روی توان مصرفی بگذارد. در این جا با استفاده از الگوریتم Q-Learning که یکی از روش‌های یادگیری تکاملی می‌باشد، پروتکل مسیریابی AODV را به گونه‌ای تغییر می‌دهیم که هر گره به عنوان یک عامل مؤثر در فرآیند مسیریابی با توجه به شرایط محیطی و بازخوردی که از تعامل با گره‌های همسایه خود دارد بتواند اثر حمله سیاه‌چاله را کاهش دهد و در نتیجه باعث افزایش گذردهی شبکه شود. ما با استفاده از شبیه‌ساز NS3 محیط آزمایشی را برای مقایسه روش ارائه شده ایجاد کرده‌ایم و عملکرد پروتکل AODV و روش ارائه شده، زمانی که شبکه تحت حمله سیاه‌چاله می‌باشد را مقایسه کرده و بهبود عملکرد شبکه را نشان می‌دهیم. همچنین پارامترهای الگوریتم Q-Learning و نقش آنها در عملکرد شبکه بررسی کرده و تأثیر هر کدام را نشان می‌دهیم.

تحلیل و بهبود «طرح احراز اصالت با حفظ مشروط حریم خصوصی CPPA» در شبکه‌های خودرویی

علیرضا آقاباقرلو، جواد مهاجری، محمود سلماسی زاده ، مهشید دلاور

دانشگاه صنعتی شریف

چکیده: استفاده از شبکه‌های اقتضایی خودرویی، می‌تواند نقشی مهم در کاهش سوانح جاده‌ای و کنترل ترافیک ایفا کند. احراز اصالت داده و حفظ حریم خصوصی مالک آن از مهم‌ترین الزامات امنیتی به شمار می‌آیند که برای تأمین همزمان این دو ویژگی طرح‌های مختلفی ارائه شده‌اند. یکی از طرح‌های شناخته شده مبتنی بر افزاره‌های غیر قابل نفوذ، طرح احراز اصالت با حفظ مشروط حریم خصوصی (CPPA(Conditional Privacy-Preserving Authentication)) است که الهام بخش بسیاری از طرح‌های دیگر نیز شده است. نشان داده شده است که این طرح ضمن برخورداری از کارایی قابل قبول، درصورت برقرار بودن فرض دسترس ناپذیری مهاجمین به مقدار مخفی مشترک ذخیره شده در افزاره‌های غیر قابل نفوذ تعبیه شده در تمامی خودروهای موجود در شبکه، قادر به برآورده ساختن بسیاری از ویژگی‌های امنیتی در نظر گرفته شده برای این گونه شبکه‌هاست. با توجه به امکان نقض فرض نفوذناپذیری افزاره‌ها به صورت عملی، در این مقاله نشان داده می‌شود که نقض این فرض و نفوذ به حتی یکی از افزاره‌ها و افشای مقدار مخفی، منجر به نقض گمنامی، حریم خصوصی و آسیب‌پذیری کامل طرح در برابر حملات جعل هویت و پیام می‌شود. سپس با ایجاد تغییرات و اصلاحاتی در این طرح و ارائه یک طرح بهبود

یافته، نشان خواهیم داد که طرح ارائه شده، حتی در صورت نفوذ به هریک از افزاره‌ها، ضمن حفظ ویژگی‌های امنیتی مدنظر در شبکه‌های خودرویی از جمله گمنامی و حفظ مشروط حریم خصوصی و مقاومت در برابر حمله جعل هویت، از راهکاری برای تشخیص نفوذ، برخوردار است.

ارزیابی امنیتی بستر ابری اوپن استک در مقابل حملات از کاراندازی سرویس

نیما جوادی، علیرضا شفیعی‌نژاد

دانشگاه تربیت مدرس

چکیده: امروزه امنیت رایانش ابری در حوزه‌های اجرا پذیری و حریم خصوصی به یکی از چالش‌های مهم روز بدل شده است. این پژوهش با ارائه چندین آزمون امنیتی به بررسی سطح کیفیت خدمات در صورت بروز اخلال عمدی در شبکه داخلی و مدیریتی (متغیرهای پهنای باند و تأخیر) می‌پردازد. این آزمون‌ها در دو حالت وجود ایمیج سیستم‌عامل بر روی ماشین کنترلر یا ماشین ذخیره‌سازی اجرا خواهد شد. این چارچوب ارزیابی به صورت یک نرم‌افزار برای اندازه‌گیری مباحث مذکور بر بستر رایانش ابری اوپن استک پیاده‌سازی شده است. نتایج نشان می‌دهد، در صورتی که ایمیج بر روی ماشین کنترلر باشد، در صورت بروز اخلال در پهنای باند، کیفیت خدمات به صورت چشم‌گیری کاهش خواهد یافت. همچنین تغییر در تمامی این متغیرها بر روی هر دو حالت اجرا، تأثیر مستقیم بر کیفیت خدمات داشته به گونه‌ای که در صورت افزایش اخلال بیشتر از آستانه مرزی، که ما به دست آورده‌ایم، انجام بعضی از عملیات با خطا روبه‌رو خواهد شد.

دسته‌بندی مشتریان شرکت‌های ارائه‌دهنده سرویس‌های پرداخت با استفاده از تارنمای فروشگاهی آنان به کمک روش‌های داده‌کاوی

محمدحسین حجتی، بابک صادقیان

دانشگاه صنعتی امیرکبیر

چکیده: شرکت‌های ارائه‌دهنده سرویس‌های پرداخت بنگاه‌هایی هستند که امر تجارت و نقل و انتقالات مالی بین‌بانکی را تسهیل نموده‌اند. در این بین افراد سودجو به‌راحتی می‌توانند با استفاده از سرویس‌های ارائه شده در این بنگاه‌ها، درآمدهای نامتعارف خود را به سیستم و نظام بانکی کشور وارد کنند. لذا لزوم یک نظارت دقیق بر عملکرد مشتریان این سامانه‌ها احساس می‌شود. یکی از روش‌های رایج برای شناسایی موارد مشکوک، مقایسه عملکرد این

مشتریان درون گروه‌هایی است که بیشترین شباهت را با یکدیگر دارا هستند. اما گروه‌بندی مشتریان مشکلاتی نیز به همراه دارد، ازجمله می‌توان به مشکل شروع سرد، عدم دقت در تعیین صنف کاری در زمان ثبت‌نام و راه‌اندازی چندین کسب‌وکار با در اختیار داشتن یک درگاه اینترنتی اشاره نمود. در این مقاله سعی شده است به کمک روش‌های داده‌کاوی به این موضوع پرداخته و به‌صورت نیمه‌خودکار گروه‌بندی مشتریان انجام پذیرد. مجموعه دادگان واقعی یک شرکت PSP و کلمات کلیدی مناسب برای هر صنف در اختیار است. با استفاده از یک خزشگر و تکنیک‌های وب کاوی دایره کلمات کلیدی را وسیع‌تر کرده، درنهایت به کمک روش TF-IDF و KNN گروه‌بندی هر یک از وب‌سایت‌های مرتبط با مشتری انجام می‌شود. تعداد ۱۰ صنف به صورت دقیق مورد ارزیابی قرار گرفته و نتایج به دست آمده در مجموع دقت مناسب روش پیشنهادی در دسته‌بندی را نشان می‌دهد.

پیاده‌سازی حمله لغت‌نامه‌ای به گذرواژه‌ها بر روی GPU

ابوالفضل سالمی، بهبد کشاورزی، محسن منصوری

دانشگاه علم و صنعت ایران - دانشگاه شاهد - دانشگاه صنعتی مالک اشتر

چکیده: در این مقاله حمله لغت‌نامه با استفاده از مدل مارکوف طراحی شده است. ابتدا با استفاده از یک پایگاه داده از گذرواژه‌های لو رفته احتمالات مارکوف مرتبه اول و دوم به‌دست آمده است. نتایج نشان می‌دهد که این احتمالات با آنچه در مورد متون معمولی محاسبه شده تفاوت دارد. در حالی که در بسیاری از کارها به احتمالات مارکوف حروف در متون معمولی اشاره می‌شود. سپس نحوه پیاده‌سازی حمله لغت‌نامه‌ای به گذرواژه‌ها بر روی gpu تشریح می‌شود. به علت وجود هسته‌های زیاد gpu امکان موازی‌سازی بسیاری در این پردازنده فراهم آمده‌است. در نتیجه سرعت عملکرد در مقایسه با cpu بسیار بیشتر است.

تشخیص تروجان سخت‌افزاری برمبنای تحلیل توان مصرفی، با استفاده از الگوریتم PCA و شبکه عصبی مصنوعی MLP

علی فریدونی، محمدعلی دوستاری، حامد یوسفی

دانشگاه شاهد - پژوهشگاه توسعه فناوری‌های پیشرفته خواجه نصیرالدین طوسی

چکیده: به علت جهانی‌شدن صنعت نیمه‌هادی و طراحی مراحل مختلف تراشه در نقاط مختلف جهان، تولید تراشه به‌طور فزاینده‌ای از طریق برون‌سپاری انجام می‌شود. این امر یک خطر مهم برای مدارهای مجتمع‌هایی است که در کاربردهای مهم امنیتی استفاده می‌شود. مهاجمان می‌توانند تراشه‌ها را در هنگام ساخت در کارخانه‌های غیرقابل‌اعتماد تغییر دهند و یا ممکن

است در فازهای مختلف طراحی به‌نوعی به طراحی دست برده شود و تغییراتی در آن اعمال شود. این تغییرات مخرب و توابع پنهان به‌عنوان «تروجان سخت‌افزاری» نامیده می‌شود. کشف چنین مدارهای تروجان دار با استفاده از راهبردهای آزمون معمولی، تقریبا غیرممکن است. در پژوهش‌های انجام‌شده روش‌های مختلفی برای کشف تروجان ارائه شده است که روش کشف با استفاده از پارامترهای کانال جانبی از مهم‌ترین و مؤثرترین آن‌هاست. در این روش‌ها با تحلیل‌های آماری و اعمال الگوریتم‌های مختلف بر روی پارامترهای کانال جانبی می‌توان به وجود تروجان در مدار پی برد. در پژوهش‌های انجام‌شده هر الگوریتم و تحلیل به‌تنهایی قادر به کشف ۱۰۰ درصد تروجان‌های کوچک نیست لذا در روش جدید ارائه شده در این مقاله به کمک ترکیب الگوریتم PCA و شبکه‌های عصبی مصنوعی MLP نشان داده می‌شود که توان مصرفی مدار AES128 آلوده به تروجان نشت کلید از نمونه طلایی آن به‌راحتی قابل‌تفکیک بوده و با این روش می‌توان تراشه آلوده به تروجان‌های نشت کلیدی که ردپای بسیار کوچکی بر روی مساحت و توان مصرفی دارند را با دقت بسیار بالایی تشخیص داد.

آزمایش و مقایسه سامانه تشخیص نفوذ suricata در تعامل با سامانه‌های انتقال سریع بسته

رضا غلامعلی‌تبار فیروزجایی، مسعود رفیقی، محسن عسکری

دانشگاه صنعتی مالک اشتر

چکیده: سامانه‌های تشخیص نفوذی که بر روی سیستم‌عامل همه‌منظوره نصب می‌شوند، با تکیه‌بر مجموعه‌ای از زیربرنامه‌های کتابخانه‌ای (که به آن سامانه انتقال بسته میان برنامه کاربردی و سخت‌افزار شبکه می‌گویند) عملیات دریافت بسته را انجام می‌دهند. هر یک از این سامانه‌ها، با توجه به سرویس‌های مختلف سیستم‌عامل سرعت و کارایی متفاوتی دارند. تبادل بسته‌های دریافتی در بعضی سامانه‌های انتقال بسته، نیاز به حافظه بسیار زیاد، به‌کارگیری بخش عمده‌ای از توان پردازنده و اشغال زیاد گذرگاه‌های رایانه دارد. درنتیجه، سامانه تشخیص نفوذ در پهنای باند بالا با کمبود منابع و اتلاف بسته‌های دریافتی مواجه می‌شود. تغییر الگوریتم‌های محاسباتی و بهبود سامانه تشخیص نفوذ منجر به کاهش مصرف حافظه و توان پردازشی (منابع) موردنیاز می‌شود، ولی با افزایش پهنای باند، افزایش پیچیدگی روزافزون حملات شبکه و پردازش‌های پیچیده و سنگین در سامانه تشخیص نفوذ، میزان نیاز سامانه تشخیص نفوذ به منابع مختلف افزایش خواهد یافت. لذا در آزمایش‌های انجام شده، با استفاده حداکثر از منابع پردازنده، مقدار حافظه و عدم مطابقت هر بسته با تمامی قوانین، سامانه تشخیص نفوذ در بدترین شرایط آزمایش شده است تا به شبکه واقعی با پهنای باند بالا شبیه باشد. انواع سامانه‌های انتقال سریع بسته در مقالات علمی مختلف مقایسه و آزمایش شده‌اند، ولی سامانه انتقال بسته در هم‌جواری با یک سامانه سنگین پردازش بسته (مانند سامانه‌های تشخیص نفوذ) آزمایش نشده است.

در این مقاله، یک سامانه تشخیص نفوذ انتخاب شده است که در تعامل با تعدادی از سامانه‌های انتقال سریع بسته (که به ادعای پژوهشگران در نوع خود سریع‌ترین بوده‌اند) برای تعیین بالاترین کارایی، آزمایش شده‌اند. سامانه تشخیص نفوذ برای کار با هر یک از (سه نمونه) سامانه‌های انتقال بسته، به‌صورت مجزا تغییر داده شده است. نتایج آزمایش‌ها، افزایش میانگین سرعت پردازش و کاهش تعداد بسته‌های پردازش‌نشده (در سامانه انتقال سریع بسته و سامانه تشخیص نفوذ) را نشان می‌دهد و در یکی از نمونه‌های سامانه تشخیص نفوذ پیاده‌سازی شده علاوه بر بهبود سرعت انتقال بسته، منابع کمتری صرف انتقال بسته‌ها شده که این امر منابع پردازشی بیشتری، برای سامانه تشخیص نفوذ فراهم می‌آورد.

سیستم‌های رأی‌گیری الکترونیکی مبتنی بر بلاکچین

زهرا سالار، حمیدرضا محروقی، سبحان علی‌آبادی

دانشگاه بین‌المللی امام رضا (ع)

چکیده: رأی‌گیری یکی از مهم‌ترین ارکان دموکراسی به شمار می‌آید که مردم می‌توانند دیدگاه‌های خود را به‌طور رسمی به دولت اعلام نمایند. در انتخابات عمومی هنوز از یک سیستم متمرکز استفاده می‌شود و یک نهاد وجود دارد که فرایند آن را مدیریت می‌کند. برخی از مشکلات موجود در بسیاری از سیستم‌های انتخاباتی الکترونیکی متمرکز با سازمان‌هایی است که دارای کنترل کامل بر پایگاه داده و سیستم رأی‌گیری می‌باشند. امکان دسترسی به پایگاه داده فرصت‌های قابل ملاحظه‌ای را برای دستکاری داده‌ها به وجود می‌آورد و باعث سلب اعتماد عمومی می‌گردد. فناوری بلاکچین به عنوان یک راه‌حل برای این مشکل معرفی می‌شود، که مبتنی بر یک بستر غیرمتمرکز بوده و کل پایگاه داده متعلق به بسیاری از کاربران است. استفاده از فناوری بلاکچین در سیستم‌های رأی‌گیری الکترونیکی می‌تواند برخی از چالش‌های موجود در سیستم‌های سنتی را حل کند. این مقاله ضمن مرور و بررسی سیستم‌های رأی‌گیری مبتنی بر فناوری بلاکچین، یک سیستم نمونه را بر اساس نیازمندی‌های یک سیستم رأی‌گیری مورد تحلیل و ارزیابی امنیتی قرار می‌دهد.

مقالات انگلیسی برتر

مقالات انگلیسی برتر کنفرانس با داوری مجدد در اولویت چاپ در مجله ISeCure قرار می‌گیرند.

www.isecure-journal.org

ISeCure، مجله علمی ـ پژوهشی انجمن رمز ایران

۱۵- کارگاه‌های آموزشی

عنوان	برگزارکننده	ارائه‌دهنده
طراحی و استقرار مراکز عملیات امنیت	آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد مرکز ماهر سازمان فناوری اطلاعات ایران	مهندس سبحان علی‌آبادی
امنیت اینترنت اشیاء صنعتی	قرارگاه پدافند سایبری سازمان پدافند غیرعامل	مهندس هادی کریمی
حفاظت از زیرساخت‌های حیاتی سایبری	قرارگاه پدافند سایبری سازمان پدافند غیرعامل	مهندس هادی کریمی
امنیت نرم، از نظریه تا عمل: مدل‌سازی و تحلیل انتشار، کنترل و شناسایی خودکار شایعه در شبکه‌های اجتماعی	دانشگاه اصفهان	دکتر بهروز ترک لادانی مهندس ابراهیم صحافی‌زاده مهندس مژگان عسگری‌زاده مهندس میلاد رادنژاد
تجزیه و تحلیل حملات سایبری و سناریوهای نفوذ به صنعت برق: نکته‌ها و آموزه‌ها	پژوهشگاه نیرو	مهندس محمدمهدی احمدیان
عمومی‌سازی امنیت رمز در مدارس (ویژه معلمان و دبیران)	دهکده امنیت و رمز دانشگاه فردوسی مشهد	دکتر عباس قائمی بافقی مهندس علی احمدیان رمکی مهندس مسعود خسروی فارمد
ماراتن عمومی‌سازی امنیت و رمز (ویژه شاخه‌های دانشجویی)	شاخه دانشجویی انجمن رمز ایران در دانشگاه فردوسی مشهد	دکتر عباس قائمی بافقی مهندس مسعود خسروی فارمد مهندس علی احمدیان رمکی

۱۶- نمایشگاه تخصصی افتا

در کنفرانس شانزدهم با هدف هم‌افزایی بیشتر صنعت و دانشگاه و با همکاری کمیته ارتباط با صنعت انجمن رمز ایران و مرکز منطقه‌ای شهید فهمیده در شمال‌شرق، نمایشگاه و سمینارهای تخصصی حوزه افتا نیز برگزار شد. نمایشگاه در فضای ۱۰۰۰ متر مربعی با حضور ۱۰ شرکت و مرکز فعال این حوزه برگزار شد. اسامی مشارکت‌کنندگان در نمایشگاه در جدول زیر آمده است.

ردیف	عنوان شرکت / مرکز
۱	شرکت امن پردازان کویر
۲	مرکز مدیریت راهبردی افتا
۳	شرکت امن‌افزارگستر شریف
۴	شرکت داده‌پردازان دوران
۵	شرکت صاافتا
۶	شرکت ژرف پویان توس
۷	شرکت سویاب گستر
۸	شرکت پالایش داده پایا
۹	شرکت لینکپ فناپ
۱۰	دفتر همکاری‌های علمی شهید فهمیده

۱۷- ارائه‌های علمی- کاربردی افتا

ردیف	عنوان	برگزارکننده	ارائه‌دهنده
۱	SCADA Network Security Monitoring	شرکت امن پردازان کویر	دکتر مهدی سلطانی
۲	تکنیک‌های کسب اطلاعات توسط سازمان‌های جاسوسی	دانشگاه راهبرد روابط بین‌الملل	مهندس روح‌اله لطفی
۳	معرفی راهبردها در حوزه توسعه محصولات و خدمات امنیتی	شرکت امن‌افزار گستر شریف	مهندس وحید خدابخشی
۴	موبایل‌های هوشمند درون سازمان‌ها، مخاطرات و فرصت‌ها	شرکت سویاب گستر خراسان	مهندس عباسعلی چزگی
۵	امنیت سخت‌افزار	شرکت ژرف پویان طوس	مهندس تبسم محنتی
۶	راهبرد ملی متدولوژی و شاخص ۲۰۱۸ و تحلیل وضعیت ایران (رویکرد ITU)	مؤسسه تحقیقات دفاعی	دکتر محمدرضا کریمی قهرودی
۷	طرح امن‌سازی راهبردی برای تعیین و ارتقا سطوح بلوغ امنیتی زیرساخت‌های حیاتی و رونق صنعت افتا	مرکز مدیریت راهبردی افتا	مهندس کیانی
۸	امنیت زیرساخت‌های کنترل صنعتی	مرکز مدیریت راهبردی افتا	مهندس جباری

۱۸- میزگرد هم‌اندیشی

میزگرد هم‌اندیشی «مسائل سیاست‌گذاری، قانون‌گذاری و مدیریتی در امنیت زیرساخت‌های حیاتی و حساس کشور» با هدف بررسی مسائل و چالش‌های حوزه امن‌سازی زیرساخت‌های حیاتی و حساس کشور و جمع‌بندی بایسته آنها با دعوت از نمایندگان مراکز و سازمان‌های مرتبط با این حوزه در نخستین روز شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران و به عنوان یکی از نشست‌های ویژه این کنفرانس با حضور جمع کثیری از اهالی صنعت افتا و صنایع منطقه برگزار شد. در این میزگرد مدعوین زیر نظرات خود را در خصوص سؤالات میزگرد بیان نمودند و در انتها به سؤالات حاضرین در نشست نیز پاسخ داده شد.

- مرکز ملی فضای مجازی - مهندس مجتبی جعفری
- سازمان فناوری اطلاعات ایران - دکتر ابراهیم صادقی
- مرکز مدیریت راهبردی افتای ریاست جمهوری - مهندس محمود روزبهانی
- سازمان پدافند غیرعامل - دکتر رضا جلایی
- انجمن رمز ایران - مهندس هاشم حبیبی
- دانشگاه فردوسی مشهد - دکتر عباس قائمی بافقی (مدیر نشست)

سؤالات میز گرد تخصصی:

مسائل مدیریتی، سیاست‌گذاری و قانون‌گذاری در امنیت زیرساخت‌های حیاتی و حساس کشور

۱. قوانین و سیاست‌های ابلاغی درباره امنیت زیرساخت‌های حیاتی کشور چه میزان در جهت رفع مشکلات مؤثر بوده است؟ چرا؟ چگونه؟

۲. نقش ساختارهای حاکمیتی برای افزایش توان مدیریت و ارتقا امنیت زیرساخت‌های حیاتی و حساس کشور چگونه بوده است؟

۳. چه چالش‌های پیشِ روی زیرساخت‌های حیاتی کشور وجود دارد؟ چه راه‌حل‌هایی را برای آن پیشنهاد می‌کنید؟

۴. سیاست شما در ارتقا محصولات بومی امن به‌ویژه در بکارگیری زیرساخت‌های حیاتی کشور چیست؟

۱۹- نشست طرح مسأله

نشست طرح مسأله «امنیت سامانه‌های کنترل صنعتی و اینترنت اشیاء» نیز در کنفرانس شانزدهم با هدف شناسایی چالش‌های پیش رو و تعریف مسائل فنی و علمی مرتبط و یافتن راهکارهای حل موانع این حوزه با مشارکت اساتید و پژوهش‌گران دانشگاهی و مدیران و کارشناسان صنایع برگزار شد. مدعوین این نشست نیز به شرح زیر می‌باشد.

- سازمان نظام صنفی رایانه‌ای خراسان رضوی - دکتر ایرج لایق
- آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد - مهندس سبحان علی‌آبادی
- فن‌بازار منطقه‌ای خراسان رضوی - مهندس ظریفیان
- سندیکای افتا - مهندس روحانی
- پژوهشگاه نیرو - مهندس محمدمهدی احمدیان
- شرکت پیام‌پرداز - مهندس مسعود رجایی
- شرکت فناپ - دکتر محمدحسین نورانیان
- انجمن رمز ایران - دکتر محمود سلماسی‌زاده (مدیر نشست)

سؤالات نشست طرح مسأله:

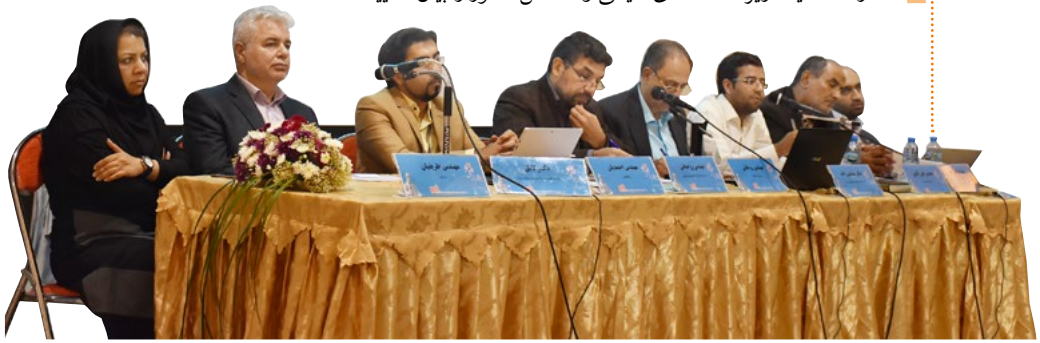
امنیت سامانه‌های کنترل صنعتی و اینترنت اشیاء

۱. در سازمان شما چقدر به امنیت و بطور خاص بکارگیری به محصولات بومی امن تأکید می‌شود؟ چرا؟

۲. آیا محصولات امنیتی بومی توانسته نیازهای ملی را در زیر ساخت‌های حیاتی و حساس و اینترنت اشیاء برآورده سازد؟ چرا؟ چگونه؟

۳. چالش‌های توسعه امنیت در زیرساخت‌های حیاتی و حساس و اینترنت اشیاء چیست؟ چه راهکارهایی برای غلبه بر آنها پیشنهاد می‌کنید؟

۴. در قالب یک سؤال درخواست خود از شورایعالی فضای مجازی برای افزایش توان مدیریت و ارتقاء امنیت زیرساخت‌های حیاتی و حساس کشور را بیان نمایید؟



۲۰- پیش رویداد کنفرانس

با هدف تأثیرگذاری اجتماعی، هم‌اندیشی و هم‌افزایی صنعت و دانشگاه در جهت توسعه و ارتقای امنیت صنایع مرتبط با فناوری‌های نوین اطلاعاتی و ارتباطی و ترویج مفاهیم و اصول امنیت و رمز در راستای برنامه‌های اصلی و جانبی کنفرانس شانزدهم انجمن رمز ایران، نشست پیش رویداد شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران با حضور مدیران و کارشناسان سازمان‌ها، صنایع و شرکت‌های بخش خصوصی در روز سه‌شنبه ۱ مرداد ۱۳۹۸ در دانشگاه فردوسی مشهد برگزار شد.

در این نشست آقایان دکتر قائمی بافقی، مدیر گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد و دبیر شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران، مهندس حبیبی، عضو شورای اجرایی و دبیر کمیته ارتباط با صنعت انجمن رمز ایران، دکتر حسینی سنو، رئیس مرکز فناوری اطلاعات و ارتباطات و دبیر کمیته اجرایی کنفرانس، مهندس زارع، مدیر منطقه شمال شرق مرکز شهید فهمیده و خانم دکتر امین‌طوسی، دبیر کمیته علمی کنفرانس و بیش از ۵۰ نفر از مدیران و کارشناسان از ۳۰ سازمان و شرکت مرتبط حضور داشتند.

براساس این هم‌اندیشی مقرر شد دو میزگرد هم‌اندیشی و نشست طرح مسأله در برنامه کنفرانس درنظرگرفته شده و کارگاه‌ها و نمایشگاه تخصصی حاشیه کنفرانس به سه شکل زیر برگزار شود:

- غرفه ارائه توانمندی‌ها: ایجاد فضای نمایشگاهی و امکان ارائه و انتقال تجربه‌ها و محصولات صنایع، مراکز پژوهشی و پژوهش‌گران با تأکید به دو جنبه انتقال دانش فنی و ارائه آخرین محصولات و دستاوردهای ملی
- میز بیان نیازمندی‌ها: بیان مشکلات و چالش‌های امنیتی در سازمان یا صنعتی که حداقل ۵ مسأله تعریف شده در قالب پیشنهاده انجام پروژه کارشناسی و پایان‌نامه‌های تحصیلات تکمیلی و یا قرارداد کاری دارد، به منظور استعدادیابی و جلب مشارکت و همکاری در طرح‌های پیشنهادی
- پوسترهای کاربردی: فرصت بیان مشکلات و چالش‌های امنیتی در سازمان یا صنایع کوچک برای دریافت راهنمایی و مشاوره علمی و فنی

۲۱- رویداد دهکده امنیت و رمز

رویداد دهکده امنیت و رمز با هدف آموزش و ترویج مفاهیم و اصول امنیت و رمز و نیز کشف و پرورش استعدادهای جوان در آموزش و پرورش، برای دانش‌آموزان دبیرستانی پایه نهم، دهم و یازدهم به عنوان یکی از برنامه‌های شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران طراحی شد. این مجموعه شامل سه رویداد نیم روزه فصلی زمستانه، بهاره و تابستانه بود. رویداد اول همزمان با جشن چهلمین سالگرد پیروزی انقلاب اسلامی در دهه فجر ۱۳۹۷، رویداد دوم هم‌زمان با هفته آموزش در اواخر بهار ۱۳۹۸ و رویداد آخر و رقابت شرکت‌کنندگان برتر همزمان با برگزاری کنفرانس در شهریور ۱۳۹۸ انجام شد.

در هریک از این رویدادهای نیم روزه، دو کارگاه آموزشی و ترویجی و یک مسابقه برگزار شد. کارگاه‌ها شامل تور آشنایی با مفاهیم کلی امنیت رمز و نشست‌های آموزشی الگوریتم‌های رمزنگاری، پنهان‌نگاری و پروتکل‌های امنیتی بود. در این کارگاه‌ها سعی شد با عمومی‌سازی و تصویرسازی مفاهیم علمی- فنی و بیان آن در قالب مثال‌های ساده، مهیج و کاربردی، مطالب به‌صورت قابل فهم برای دانش‌آموزان ارائه شود، در هر کارگاه، ارزیابی‌های کوتاه و در پایان، یک مسابقه گروهی بین شرکت‌کنندگان انجام شد. جزئیات کارگاه‌ها و نشست‌های آموزشی برگزارشده عبارتند از:

- معرفی اجمالی امنیت سایبری و بررسی ابعاد آن
- معرفی و بررسی حملات جذاب امنیتی
- مکانیزم‌های مقابله و پیشگیری از حملات امنیتی
- الگوریتم‌های رمزنگاری و نهان‌نگاری و پروتکل‌های امنیتی
- امنیت در کاربردهای مختلف و تجهیزات امنیتی مربوطه
- امنیت کامپیوترهای شخصی و شبکه‌های کامپیوتری
- مسائل امنیتی شبکه‌های اجتماعی و جرم‌یابی

۲۲- ماراتن عمومی‌سازی امنیت و رمز

شاخه دانشجویی انجمن رمز ایران در دانشگاه فردوسی مشهد با کمک دهکده امنیت و رمز در شانزدهمین کنفرانس انجمن رمز ایران، رویدادی را با عنوان ماراتن عمومی‌سازی امنیت و رمز برگزار نمود. هدف از برگزاری این ماراتن آموزش چگونگی بیان مطالب تخصصی امنیتی به شکل ساده و قابل فهم برای مخاطب‌هایی در سنین مختلف و با سطوح مختلف دانش امنیتی بود. این رویداد از دو بخش کارگاه و مسابقه تشکیل شده بود که بخش کارگاه با سرفصل‌های زیر برگزار شد:

- چگونگی بیان مطالب تخصصی امنیتی به شکل ساده و قابل فهم برای دانش‌آموزان
- عمومی‌سازی و تصویرسازی روش‌های رمزنگاری کلاسیک و مدرن
- عمومی‌سازی و تصویرسازی پروتکل‌های امنیتی و حملات علیه آن‌ها
- عمومی‌سازی و تصویرسازی روش‌های پنهان‌نگاری داده‌ها در متن و تصویر
- عمومی‌سازی و تصویرسازی مباحث امنیت شبکه و تجهیزات امنیتی
- عمومی‌سازی هک و نفوذ در قالب مثال‌های ساده و مهیج عملی
- انتخاب یکی از عناوین محورهای کنفرانس توسط هر یک از تیم‌ها

۲۳- بیانیه پایانی کنفرانس

در راستای دستیابی به اهداف مذکور در سند چشم‌انداز جمهوری اسلامی ایران و اسناد بالادستی کشور، بویژه بیانیه گام دوم انقلاب، برای رسیدن به جایگاه برتر و تأثیرگذار منطقه‌ای در علم رمزشناسی و فناوری امنیت فضای تولید و تبادل اطلاعات (افتا) و افزایش توانمندی‌های دفاع از زیرساخت‌های حیاتی، حساس و مهم کشور در برابر حملات سایبری بیگانگان و توسعه فناوری‌های نوین برای نیل به خوداتکایی و سرآمدی صنعت بومی افتا، و همچنین ایجاد فضای مناسب برای کارآفرینی، دانش‌افزایی و اشتغال فارغ‌التحصیلان مقاطع مختلف دانشگاهی حوزه رمز و افتا در صنایع داخلی و تشکل‌های دانش‌بنیان، بسیار ضروری است که نهادهای مسئول، بیش از گذشته به افزایش توان علمی و تخصصی کشور در این حوزه توجه کنند. بر این مبنا و در پایان برگزاری شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران، بر انجام موارد زیر از سوی نهادهای سیاست‌گذار، قانون‌گذار و دستگاه‌های اجرایی مسئول، با هدف هم‌افزایی توانمندی‌های موجود، تقویت بنیان‌های علمی، توسعه نیروی انسانی و رشد صنعت داخلی در حوزه افتا تأکید می‌کنیم:

۱. همزمان با تقویت منابع لازم برای ارتقاء کیفی تحصیلات تکمیلی و پژوهش‌های بنیادین حوزه افتا به عنوان یک حوزه راهبردی در کشور، ضروری است به طراحی و اجرای روش‌های اصولی به منظور مهارت‌آموزی، تربیت، جذب و نگهداشت نیروی انسانی مورد نیاز برای افزایش توانمندی در بخش دفاع سایبری، امنیت شبکه‌ها، امن‌سازی سامانه‌های اطلاعاتی و رشد صنعت افتا توجه جدی صورت گیرد که بدون آن، دستیابی به توسعه امن و کارآمد فناوری‌ها در بخش‌های وسیعی از صنایع و خدمات مورد نیاز کشور تقریباً غیرممکن خواهد بود.

۲. ارزیابی، تحلیل و بازنگری اجرای سند «امنیت فضای تولید و تبادل اطلاعات کشور (افتا)» و روزآمدسازی آن بر اساس شرایط و نیازهای روز کشور از جمله امور بسیار مهمی است که لازم است مورد اهتمام نهادهای ذی‌ربط قرار گیرد.

۳. لازم است از طریق هماهنگی اقدامات دستگاه‌های مسئول، تدابیر لازم برای تدوین سیاست‌ها، قوانین و دستورالعمل‌های اجرایی مناسب، شفاف و متوازن به منظور توجه نهادینه به انتظام امور و تنظیم مقررات مرتبط با امنیت سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی، حساس و مهم کشور، با هدف تشویق و ترغیب شرکت‌های داخلی برای تولید و توسعه محصولات پیشگیری، مقابله و مهارکننده تهدیدات روزافزون این سامانه‌ها، به نحو بایسته اتخاذ شوند.

۴. تدوین برنامه راهبردی و نقشه‌راه توسعه امنیت در حوزه‌های مختلف صنعتی کشور به‌خصوص امن‌سازی سامانه‌های کنترل صنعتی با هدف جلوگیری و مقابله با تهدیدات سایبری در زیرساخت‌های ارتباطی و اطلاعاتی کشور یک ضرورت انکارناپذیر است

که باید از سوی نهادهای مسئول به آن توجه شده و برای جلوگیری از حملات قابل پیش‌بینی به سازمان‌های حیاتی، حساس و مهم کشور مورد اقدام عاجل قرار گیرد.

۵. با تأکید بر ضرورت تدوین قوانین پایه و راهگشا توسط مجلس محترم شورای اسلامی برای حمایت از توسعه صنعت دانش‌بنیان افتا در کشور و با توجه به اهمیت و ضرورت مشارکت و پیشگامی جمهوری اسلامی ایران در شکل‌دهی قواعد بین‌المللی فضای مجازی و توان‌افزایی درونی در حوزه افتا، لازم است با استفاده از ظرفیت‌های علمی موجود در کشور، اهتمام جدی از سوی نهادهای مسئول برای توسعه تعاملات با نهادهای علمی کشورهای دیگر و میزبانی برگزاری نشست‌های جهانی و منطقه‌ای حوزه افتا صورت گیرد.

۶. با توجه به اهمیت استفاده از روش‌های رمزنگاری برای به‌اشتراک‌گذاری و توزیع داده‌ها که می‌تواند به راهکارهای امن برای انواع تبادل اطلاعات در فضای مجازی بیانجامد، ضروری است در بکارگیری فناوری‌های نوین مانند «زنجیره قالب‌ها» و کاربردهای آن در بخش‌های مختلف بویژه در بخش اقتصادی و تولید رمزارزها، از تصمیمات غیرکارشناسی و نادیده گرفتن مبانی علمی این فناوری‌ها به شدت اجتناب شود و با طراحی برنامه راهبردی و نقشه‌راه مورد نیاز، در جهت مواجهه هوشمندانه با مخاطرات این نوع فناوری‌ها و استفاده مطمئن از مزایا و منافع آنها برای کشور اقدام گردد.

۷. با توجه به الزامات و اقتضائات امنیت ملی و بر مبنای اصول اقتصاد مقاومتی، علاوه بر ایجاد باور حاکمیت در مورد امنیت به عنوان یک ضرورت تداوم کسب‌وکارهای فناورانه مورد نیاز جامعه، لازم است تدوین و اجرای سیاست‌های حمایت از تولید و کاربرد محصولات داخلی در حوزه افتا و همچنین ممنوعیت واردات تجهیزات این حوزه (که امکان ساخت آنها در داخل کشور وجود دارد) بیش از پیش توسط مراجع ذی‌ربط مورد توجه واقع شود.

۸. با هدف جذب دانش‌آموزان و ترغیب خانواده‌ها برای تحصیل فرزندانشان در علوم ریاضی، لازم است به موضوع عمومی‌سازی آموزش رمزشناسی و افتا به عنوان یکی از زمینه‌های جذاب برای فارغ‌التحصیلان این علوم، از طریق گسترش رویدادهایی مانند «دهکده امنیت و رمز» که در شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران تجربه شده است، و برگزاری دوره‌های آموزش ضمن خدمت دبیران آموزش و پرورش برای توسعه و تعمیق آموزش‌های پایه رمزشناسی در مقاطع پیش از دانشگاه توجه بایسته به عمل آید.

۹. انجمن رمز ایران با ایجاد محیط علمی‌آموزشی و تعامل با بازیگران مختلف حوزه افتای کشور در کنفرانس‌های سالانه خود و برگزاری نشست‌های جانبی در این

کنفرانس‌ها مانند میزگرد «هم‌اندیشی مسائل مدیریتی، سیاست‌گذاری و قانون‌گذاری در امنیت زیرساخت‌های حیاتی کشور» و نشست «طرح مسأله امنیت سامانه‌های کنترل صنعتی و امنیت اینترنت اشیاء» در شانزدهمین دوره این کنفرانس‌ها، توانسته است با مشارکت و همراهی ارزشمند دست‌اندرکاران، نقش مؤثری در بیان مشکلات و پیشنهاد راهکارهای مورد نیاز این حوزه ایفا نماید. ضمن تأکید بر ضرورت استمرار این رویه و ادامه آن از طریق برگزاری نشست‌های تخصصی و مشورتی در طول سال با حضور نمایندگان عموم بازیگران، لازم است نسبت به پیگیری و مطالبه نتایج حاصله از مراجع ذی‌ربط اقدام گردد.

۱۰. نظر به اهمیت فعالیت‌های انجمن رمز ایران برای ایجاد فضای پویا در حوزه تحقیقات علمی و آینده‌پژوهی رمزشناسی و افتا، از طریق استمرار برگزاری کنفرانس‌های بین‌المللی، انتشار مجلات علمی‌پژوهشی و علمی‌ترویجی، جذب و تشویق دانش‌پژوهان جوان و همچنین حمایت از خلاقیت‌ها و نوآوری‌های صنعت افتا، ضروری است مساعدت و پشتیبانی نهادها و دستگاه‌های اجرایی مرتبط با امنیت ارتباطات و فناوری اطلاعات در کشور از تداوم وتوسعه این فعالیت‌ها بیش از گذشته مورد توجه و اقدام قرار گیرد.

چشم‌انداز انجمن رمز ایران در افق سال ۱۴۰۴

انجمن رمز ایران در افق ۱۴۰۴، کانونی است نظام‌مند، پیشرو، مرجعی قابل اعتماد و تعامل‌گرا در سطح کشور و منطقه که در آسیب‌شناسی، تحلیل و اولویت بندی موضوعات و مسائل اساسی حوزه امنیت فضای تولید و تبادل اطلاعات (افتا) مشارکت نموده و مشاوره و راهکارهای لازم را ارائه خواهد داد.

به زودی به صورت الکترونیکی و همراه با واژه‌های پیشنهادی گروه واژه گزینی انجمن رمز ایران که به تصویب فرهنگستان زبان و ادب فارسی رسیده‌اند، در اختیار عموم علاقه‌مندان قرار خوهد گرفت.

۲۴- گزارش تصویری

برگزاری جلسات کمیته‌های علمی واجرایی کنفرانس

برگزاری پیش‌رویداد کنفرانس

تشکیل جلسه با مدیران و کارشناسان مرتبط از سازمان‌ها، صنایع و شرکت‌های استان خراسان رضوی در تاریخ ۱ مرداد ۱۳۹۸

برگزاری کارگاه‌های آموزشی

برگزاری کارگاه‌های آموزشی

افتتاحیه کنفرانس

سخنرانی و خیر مقدم آقای دکتر محمد کافی، ریاست دانشگاه فردوسی مشهد

افتتاحیه کنفرانس

سخنرانی و خیر مقدم آقای دکتر محمد کافی، ریاست دانشگاه فردوسی مشهد

سخنرانی و ارائه گزارش آقای دکتر عباس قائمی بافقی، دبیر کنفرانس

سخنرانی کلیدی کنفرانس، آقای دکتر مهدی پاکروان

با موضوع:

درس‌ها و تجربه‌هایی از توسعه توانمندی‌های ملی در حوزه سیستم‌های مخابرات نوری

سخنرانی کلیدی کنفرانس، خانم دکتر ترانه اقلیدس

با موضوع:

رمزنگاری در عصر کوانتوم

مجمع عمومی انجمن رمز ایران

بازدید ریاست انجمن رمز ایران از نمایشگاه جانبی کنفرانس

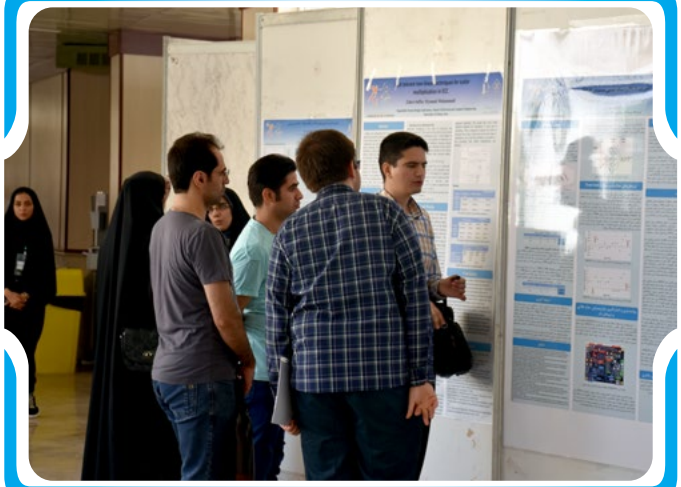
بازدید ریاست انجمن رمز ایران از نمایشگاه جانبی کنفرانس

ارائه‌های علمی-کاربردی کنفرانس

میزگرد هم‌اندیشی

«مسائل مدیریتی، قانون‌گذاری و سیاست‌گذاری در امنیت زیرساخت‌های حیاتی کشور»

ارائه مقاله‌های پوستری کنفرانس



نشست طرح مسأله

امنیت سامانه‌های کنترل صنعتی و اینترنت اشیاء

مراسم اختتامیه کنفرانس

برپایی نمایشگاه جانبی کنفرانس

سخنرانی ریاست انجمن رمز ایران در مراسم اختتامیه کنفرانس

قرائت بیانیه کنفرانس توسط دبیر انجمن رمز ایران

تقدیر از سخنرانان کلیدی کنفرانس

تقدیر از مقالات برگزیده، داور برتر، حامیان کنفرانس و همکاران دبیرخانه کنفرانس

تقدیر از مقالات برگزیده، داور برتر، حامیان کنفرانس و همکاران دبیرخانه کنفرانس

تقدیر از مقالات برگزیده، داور برتر، حامیان کنفرانس و همکاران دبیرخانه کنفرانس

تقدیر از دبیر کنفرانس

عکس یادگاری در پایان مراسم اختتامیه کنفرانس

پذیرش کنفرانس

پذیرایی بین نشست‌های کنفرانس

پذیرایی ناهار کنفرانس

پذیرایی ناهار کنفرانس

بادبودهای تصویری دیگر از شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران

هماهنگی نشست‌های کنفرانس

دانشجویان همکار در برگزاری کنفرانس

ضیافت شام کنفرانس

ضیافت شام کنفرانس

۲۵- شرح کوتاه رویداد دهکده امنیت و رمز

با توجه به استقبال دانش‌آموزان از مسابقه شهر ریاضی دانشگاه فردوسی مشهد با ۱۷ سال تجربه موفق، همزمان با شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران، «دهکده امنیت و رمز» با هدف آموزش و ترویج مفاهیم و اصول امنیت و رمز و نیز کشف و پرورش استعدادهای جوان در آموزش و پرورش، برای دانش‌آموزان دبیرستانی پایه نهم، دهم و یازدهم طراحی در قالب سه رویداد نیم روزه فصلی زمستانه، بهاره و تابستانه در دانشکده مهندسی دانشگاه فردوسی مشهد برگزار شد.

در رویداد اول همزمان با جشن چهلمین سالگرد پیروزی انقلاب اسلامی در دهه فجر ۱۳۹۷، حدود ۱۱۰ دانش‌آموز رقابت کردند.

در رویداد دوم همزمان با هفته آموزش در اردیبهشت ۱۳۹۸ و رویداد آخر، رقابت شرکت‌کنندگان برتر همزمان با برگزاری کنفرانس در شهریور ۱۳۹۸ به انجام رسید و از سه تیم برتر در مراسم اختتامیه کنفرانس تقدیر به عمل آمد. جزئیات برگزاری مراحل رویدادها، کارگاه‌ها و مسابقات از طریق وبگاه کنفرانس به آدرس http://iscisc2019.um.ac.ir اطلاع‌رسانی گردید.

در هریک از این رویدادهای نیم روزه، دو کارگاه آموزشی و ترویجی و یک مسابقه شامل تور آشنایی با مفاهیم کلی امنیت رمز و نشست‌های آموزشی الگوریتم‌های رمزنگاری، پنهان‌نگاری و پروتکل‌های امنیتی برگزار شد. در این کارگاه‌ها سعی شده است با عمومی‌سازی و تصویرسازی مفاهیم علمی- فنی و بیان آن در قالب مثال‌های ساده، مهیج و کاربردی، مطالب به‌صورت قابل فهم برای دانش‌آموزان ارائه شود، در هر کارگاه، ارزیابی‌های کوتاه و در پایان، یک مسابقه گروهی بین شرکت‌کنندگان انجام شده است که امتیازهای دریافتی در صعود به دوره‌های بعدی و نیز در ارزیابی نهایی تیم‌های منتخب مؤثر بوده است.

همچنین همزمان با کنفرانس کارگاه آموزشی برای معلمان برگزار شد که با توجه به استقبال خوب از آن امید است با مشارکت و حضور فعال معلمان و مدیران مدارس و نیز حمایت ادارات آموزش و پرورش، برنامه‌های دهکده در سال تحصیلی جدید با برگزاری رویدادهای دانش‌آموزی و نیز کارگاه‌های فصلی

توسعه یابد. بعلاوه ماراتن عمومی سازی امنیت و رمز برای شاخه‌های دانشجویی انجمن رمز ایران نیز برگزار شد که به یاری خداوند و به عنوان یک حرکت برنامه‌ریزی شده از سوی انجمن رمز ایران برای گسترش برنامه‌های دهکده در سطح ملی ادامه خواهد یافت.

برگزاری شایسته این رویدادها مانند هر کار بزرگی تنها در سایه توجه و عنایت حضرت حق میسر می‌شود و مرهون مشارکت جمعی و همگانی،

بهره‌مندی از خردجمعی و نیز حمایت مسئولین محترم است. در اینجا لازم است از تلاش‌های مستمر گروه بزرگ همکاران دهکده امنیت رمز در دانشگاه فردوسی مشهد تشکر و قدردانی شود. با سپاس فراوان از همکاری‌های ارزشمند اعضای این گروه، بویژه آقایان مهندس احمدیان و مهندس خسروی، دبیر شهر ریاضی آقای دکتر میرزاوزیری و همکار خوب ایشان خانم فراشاهی، همکاران محترم گروه مهندسی کامپیوتر مخصوصاً خانم دکتر امین طوسی، دبیر گرامی کنفرانس آقای دکتر قائمی بافقی و آقایان دکتر عربان، دکتر کدخدایان، دکتر پوررضا، و سایر عزیزان دبیرخانه کنفرانس و مسئولین محترم دانشگاه، امیدواریم رویداد دهکده امنیت و رمز در دوره‌های آتی کنفرانس‌های سالیانه انجمن رمز ایران نیز به نحو گسترده‌تری و با حمایت همه‌جانبه وزارت آموزش و پرورش برگزار شود.

۲۶- چکیدهٔ ارائه‌های علمی- کاربردی افتا

موضوع:

معرفی راهبردها در حوزه توسعه محصولات و خدمات امنیتی

ارائه دهنده:

مهندس وحید خدابخشی - شرکت امن‌افزار گستر شریف

در مسیر رشد فزاینده‌ی فناوری‌های نوین در حوزه فناوری اطلاعات و ارتباطات، اکنون در زمانی قرار داریم که بسیاری از زیرساخت‌های این حوزه دچار تغییرات بنیادی و شگرفی شده‌اند. به عنوان نمونه می‌توان به معرفی زیرساخت‌های جدید ارتباطی مانند 5G، رشد خیره‌کننده هوش مصنوعی، محیط‌های محاسباتی چندعاملی و توزیع‌شده، اینترنت اشیاء، محیط‌های ابری و بسیاری از پدیده‌های نوین دیگر در سال‌های اخیر اشاره کرد. این تغییرات به مثابه یک انقلاب همه جانبه در حوزه فناوری اطلاعات و ارتباطات، بخش‌های بسیاری از علوم دیگر و حتی زندگی جوامع بشری را دستخوش دگرگونی کرده است. از این رو در نگاهی همه جانبه، ایجاد فرصت‌های جدید در کنار چالش‌ها و تهدیدات پیش‌رو، موجب ایجاد تأثیرات شگرفی در حوزه‌های راهبردی و تاکتیکی این حوزه شده است. از دیدگاه شرکت‌های فناور در حوزه امنیت اطلاعات، این فرصت‌ها و تهدیدات باید به شکلی پیوسته، پایش، واکاوی و به دقت مورد ارزیابی قرار گرفته و محصولات و خدمات آن‌ها در مسیر پاسخ‌گویی به نیازهای جدید و همچنین رفع چالش‌ها و مدیریت تهدیدات نوین، بازتعریف و بازآرایی شوند. در این فضا آن‌چه که در کنار به‌کارگیری روش‌های معمول، برای کسب مزیت رقابتی در شرکت‌ها اهمیت پیدا می‌کند، افزایش انعطاف‌پذیری، چابکی، ایده‌پردازی و سرمایه‌گذاری بلند مدت نسبت به موارد فوق است.

مواردی نظیر تاب‌آوری امنیتی، راهبرد و طرح جامع امنیت فناوری اطلاعات و ارتباطات، طرح تداوم کسب و کار، آمادگی امنیتی در آستانه ورود به عصر رایانش کوانتومی و ... می‌توانند ترسیم‌کننده‌ی افق پیش‌روی توسعه محصولات و خدمات امنیتی باشند. در کنار این موارد که عمدتا لازمه تغییر در زاویه دید راهبران این شرکت‌ها، سیاست‌گذاران و بخش‌های نظارتی است، نگاهی رو به جلو در خصوص نوسازی و بازآرایی محصولات و خدمات این حوزه باید مد نظر قرار گیرد. این نگاه باید در کنار ایجاد ویژگی‌های نوین، ظرفیت، دقت و گستردگی لازم را در ارائه ویژگی‌های امنیتی ایجاد کند. مورد دیگری که در این فرآیند گذار، نیاز به سرمایه‌گذاری و پژوهش دارد ایجاد خدمات و محصولات ترکیبی و تسری بخشیدن محصولات و خدمات فعلی به حوزه‌های جدید فناوری است.

موضوع:

SCADA Network Security Monitoring

ارائه دهنده:

دکتر مهدی سلطانی - شرکت امن پردازان کویر

سامانه کنترل صنعتی (ICS) یک تجهیز یا مجموعه ای از تجهیزات است که رفتار سیستم یا تجهیز دیگری را مدیریت، هدایت و تنظیم می‌کند. این سامانه‌ها با توجه به ابعاد و وسعت جغرافیایی می‌توانند به سه دسته DCS ،SCADA و PLC تقسیم‌بندی می‌شوند. مهم‌ترین تفاوت سامانه‌های کنترل صنعتی با سامانه‌های حوزه فناوری اطلاعات در میزان حساسیت و خسارت بالا در صورت خرابی و اهمیت دسترس‌پذیری در مقایسه با محرمانگی است. با توجه به کاربرد سامانه‌های صنعتی در نقاط حیاتی، امنیت در این حوزه از اهمیت زیادی برخوردار است. اولین گام در بررسی امنیت در حوزه سامانه‌های صنعتی، بررسی سطوح حمله (Attack Surface) در این شبکه‌ها است. این سطوح به‌صورت کلی به ۴ دسته تقسیم می‌شوند:

۱- حملات به UI و HMI

دسترسی به پنل HMI به معنی دسترسی به تمامی پردازش‌های شبکه صنعتی است. همچنین وجود سامانه‌های عامل قدیمی و آسیب‌پذیر این نقاط رو به جذاب‌ترین نقاط حمله از دید مهاجم تبدیل می‌کند.

۲- حملات به سرورهای کنترلی

تنظیمات پیش‌فرض (پسوردها و تنظیمات امنیتی) از جمله دلایل نقص امنیتی در این سرورها است. همچنین به دلیل قدیمی بودن نسخه سامانه‌های عامل و برنامه‌های کاربردی این سرورها، حملات سرریز بافر (buffer overflow) و اجرای از راه دور کد (Remote Code Execution) از جمله مهم‌ترین حملات این حوزه هستند.

۳- حملات به ارتباطات شبکه‌ای

ارتباطات در شبکه‌های صنعتی از طریق خطوط سریال نقطه به نقطه، واسط‌های Ethernet و ارتباطات رادیویی انجام می‌شود. همچنین از پروتکل‌های ICS (مانند modbus، و غیره)، پروتکل‌های مدیریتی (مانند SSH، و غیره)، و پروتکل‌های وب (مانند HTTPS، و غیره) در شبکه‌های صنعتی استفاده می‌شود. این طیف گسترده از تجهیزات و پروتکل‌های ارتباطی زمینه‌های آسیب‌پذیری زیادی را فراهم می‌کند که در هر حوزه به صورت مستقل باید بررسی گردند.

۴- حملات به دستگاه‌های راه دور[1]

دستگاه‌های راه دور معمولات در مکان‌هایی با حفاظت فیزیکی کم قرار می‌گیرند. در این محل‌ها حفاظ‌ها به راحتی شکسته شده و دوربین‌ها معمولاً بررسی نمی‌شوند. در صورت دستیابی فیزیکی به این دستگاه‌ها، ارسال سیگنال در اختیار مهاجم قرار می‌گیرد. این حمله در نهایت حتی می‌تواند منجر به تسخیر سرور کنترلی نیز گردد.

موضوع:

امنیت سخت‌افزار

ارائه دهنده:

مهندس تبسم محتی - شرکت ژرف پویان طوس

درآمدی بر امنیت سخت‌افزاری

امروزه مسأله تأمین امنیت سخت‌افزاری تجهیزات همتراز با ملاحظات نرم‌افزاری سیستم‌ها، بسیار مورد توجه قرار می‌گیرد. در این حوزه به صورت کلی به هرآنچه که سخت‌افزار سیستم را مورد تهاجم قرار داده و با ایجاد تغییر در سخت‌افزار، بخشی از عملکرد سیستم را دستخوش تغییرات ناخواسته سازد، هک سخت‌افزاری گفته می‌شود. درگذشته در زمینه حملات تروجانی به ICها مطالعات بسیاری شده است، اما امروزه موضوع جدیدی که در حوزه امنیت سخت‌افزار ذهن متخصصین را به خود مشغول کرده است، حملات سخت‌افزاری در بالاترین سطح با هدف ایجاد تغییر در عملکرد سیستم، تغییر ماهیت سیستم، نشت اطلاعات و یا تخریب تجهیزات است. این حملات به طور خاص برد الکترونیکی محصول یا همان برد مدار چاپی (PCB) را هدف می‌گیرند. با توجه به گسترده بودن این حوزه و جزئیات بیشمار آن، در ادامه با هدف ایجاد حساسیت در طراحان سخت‌افزار، سعی بر آن است به طور مختصر گزارشی از برخی از این نوع حملات و امنیت در این سطح ارائه گردد. ما به طور کلی دو نوع از این حملات را بررسی می‌کنیم.

الف) طراحی مدار و PCB به صورت نا امن:

در این فرآیند، برد الکترونیکی محصول می‌تواند در هر یک از مراحل طراحی مدار یا طراحی PCB مورد حمله هکر سخت‌افزاری قرار گرفته باشد! افزودن تروجان سخت‌افزاری می‌تواند از طریق افزودن یک مدار جانبی به مدار اصلی یا تغییر در سایز و فاصله ترک‌های موجود در PCB اتفاق بیافتد و در نهایت منجر به ضعف عملکرد یا اختلال سیستم در سناریوهای خاص شود؛ علاوه بر این، بسیاری از کمپانی‌های مطرح جهان، محصولات حساس خود را به گونه‌ای طراحی می‌کنند که پس از فروش نیز امکان نظارت بر آن‌ها وجود داشته باشد.

1. Remote Devices

ب) قطعه‌گذاری نا امن:

قطعه‌گذاری نا امن زمانی رخ می‌دهد که طراحی مدار توسط مصرف کننده اصلی یا با نظارت او و به شیوه‌ای امن انجام شده باشد اما مونتاژ و قطعه‌گذاری برد برون سپاری شده باشد. با توجه به اینکه مونتاژ قطعات SMD بسیار ریز، نیاز به ابزار پیشرفته و مهارت کافی دارد که شرکت‌های طراح، به علت هزینه بالا تمایلی به تهیه آن ندارند، کمپانی‌هایی به طور تخصصی این پروسه را انجام می‌دهند؛ در این شرایط هکر می‌تواند المان‌های جعلی خود را روی برد مونتاژ کند تا علاوه بر فرآیند اصلی، پردازش‌های دیگری نیز انجام شود و به این ترتیب امکان اینکه محصول ما در شرایط خاصی خود را در سناریو مشخصی قرار دهد، وجود دارد، چرا که المان‌های جعلی نه تنها ناکارآمد نیستند که به مراتب پیشرفته تر از چیپ‌های اصلی بوده و علاوه بر قابلیت‌های اصلی مجموعه‌ای از قابلیت‌های جانبی مورد نظر هکر را نیز دارند.

اگرچه این حملات بسیار پیچیده و به صورت پیشرفته صورت می‌گیرد، ولی یکی از راهکارهای مقابله با آنها، نظارت بر طراحی برد الکترونیکی محصول و ایجاد ابهام در طراحیست.

موضوع:

راهبرد ملی متدولوژی و شاخص ۲۰۱۸ و تحلیل وضعیت ایران (رویکرد ITU)

ارائه دهنده:

دکتر محمدرضا کریمی قهرودی - مؤسسه تحقیقات دفاعی

بخش اول ارائه به بررسی تحولات و انقلاب‌های نوین آینده فضای سایبر و بازآفرینی جوامع در فضای سایبر و نیز بررسی تصاویر جامعه و تمدن صنعتی آینده کشورهای پیشتاز در این حوزه می‌پردازد. در این صنشست تصاویر تمدنی و چشم‌اندازهای آینده شش کشور پیشتاز جهان شامل ژاپن(جامعه پنجم[1] یا جامعه اَبَر هوشمند)، مالزی(مالزی پیشرفته ۲۰۵۰ و جوامع هوشمند[2]) و اتحادیه اروپا بویژه کشور آلمان(جامعه شبکه‌محور مشارکتی و انقلاب چهارم صنعتی[3])، چین(جامعه سایبری- فیزیکی- اجتماعی، ساخت چین ۲۰۲۵ و ابرقدرت برتر تولید در ۲۰۴۹)، آمریکا(اینترنت اشیا صنعتی، تولید پیشرفته[5] و هوشمند) و نیز سنگاپور(ملت هوشمند[6]) ارائه و معرفی می‌گردد.

1. Society5.0
2. Smart Communities
3. Made in China 2025
4. Industry 4.0
5. IIoT, Advance Manufacturing
6. Smart Nation

با توجه به تحولات و انقلاب‌های فوق، بخش دوم ارائه به لزوم بازتعریف امنیت سایبری در جامعه و عصر سایبری- فیزیکی می‌پردازد. امنیت سایبری زیست بومی است که به منظور بیشترین اثربخشی نیازمند هماهنگ بودن قوانین، سازمان‌ها، مهارت‌ها، همکاری‌ها، اقدامات فنی و ... است. در ادامه به معرفی اجمالی بسته جامع امنیت سایبری ITU شامل دستور کار امنیت سایبری، راهنمای تدوین راهبردهای امنیت سایبری ملی و نهایتاً تبیین شاخص جهانی امنیت سایبری(GCI) می‌پردازد. اهداف و شاخص جهانی امنیت سایبری دربرگیرنده پنج رکن قانونی، فنی، سازمانی، ظرفیت‌سازی و همکاری‌های مشترک است. رکن قانونی، بر اساس وجود نهادها و چارچوب‌های قانونی مرتبط با امنیت و جرایم سایبری و رکن فنی بر اساس وجود نهادها و چارچوب‌های فنی که با امنیت سایبری سر و کار دارند اندازه‌گیری می‌شود، رکن سازمانی مرتبط با نهادها و راهبردهای هماهنگ‌ساز و سیاستگذاری برای توسعه امنیت سایبری در سطح ملی و رکن ظرفیت‌سازی بر تحقیقات و توسعه، برنامه‌های تحصیلاتی و آموزشی، متخصصان مجاز و نهادهای بخش عمومی که ظرفیت‌سازی را ترویج می‌کنند، تأکید دارد و بالاخره رکن همکاری بر اساس وجود مشارکت‌ها، چارچوب‌های همکاری و سازوکارها و شبکه‌های به اشتراک‌گذاری اطلاعات تعریف می‌شود.

نهایتاً بخش پایانی ارائه به معرفی نتایج ارزیابی شاخص جهانی امنیت سایبری GCI 2017-2018 و تحلیل وضعیت کشورها و جایگاه کشورمان می‌پردازد. بر اساس ارزیابی اتحادیه بین‌المللی مخابرات، کشورهای عضو به سه دسته تقسیم و تحلیل شده‌اند، کشورهای در مرحله آغازین رشد، کشورهای در حال بلوغ و کشورهای پیشتاز، در انتها بر اساس نتایج ارزیابی GCI 2017-2018 جایگاه کشورها و نقاط قوت و ضعف کشورمان بررسی شده و مهمترین تجارب و یافته‌های کلیدی درس‌ها، آموزه‌ها، دلالت‌ها برای کشور معرفی می‌شود.

محورهای این ارائه عبارتند از:

- مقدمه‌ای بر تحولات راهبردی و تصویرسازی آینده فضای سایبر در افق ۲۰۵۰
- لزوم بازتعریف امنیت سایبری در جامعه و عصر سایبری- فیزیکی
- معرفی بسته مدیریت راهبردی امنیت سایبریITU و شاخص جهانی امنیت سایبری
- معرفی مدل مرجع و متدولوژی ارزیابی GCI 2017-2018
- بررسی وضعیت و جایگاه ایران و درس‌ها، آموزه‌ها، دلالت‌ها برای کشور

۲۷- چکیدهٔ کارگاه‌های آموزشی

کارگاه آموزشی

طراحی و استقرار مراکز عملیات امنیت

مهندس سبحان علی‌آبادی

آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد
مرکز ماهر سازمان فناوری اطلاعات ایران

چکیده:

هدف از این کارگاه آموزشی انتقال تجربه در خصوص نمونه‌های موردی طراحی و استقرار پروژه‌های مرکز عملیات امنیت در کشور می‌باشد، تا شرکت‌کنندگان به قدرت تحلیل و تصمیم‌گیری صحیح در این خصوص دست پیدا نمایند. شرکت‌کنندگان با معماری و مؤلفه‌های کلیدی مرکز عملیات امنیت (SOC) متناسب در سازمان‌ها و دستگاه‌های اجرایی آشنا خواهند شد، همچنین تشریح فرآیند فنی استخراج و تدوین مناسب نیازمندی‌ها و استقرار پروژه و چالش‌ها به همراه راهکارهای فنی موجود بیان می‌گردد.

سرفصل‌های آموزشی کارگاه:

- نیازمندی‌های فنی حال و آینده؛
- چالش‌های فنی در طراحی و استقرار؛
- استراتژی‌های فنی استقرار و پشتیبانی؛
- توانمندی‌های شرکت‌ها و محصولات داخلی.

مدت زمان کارگاه: ۸ ساعت

کارگاه آموزشی

امنیت اینترنت اشیای صنعتی (IIOT Security)

مهندس محمدرضا فرجی‌پور
مهندس هادی کریمی

قرارگاه پدافند سایبری
سازمان پدافند غیرعامل

سرفصل‌های آموزشی کارگاه:

- اکوسیستم امنیت اینترنت اشیای صنعتی؛
- پلتفرم‌های امنیت اینترنت اشیای صنعتی؛
- کاربردهای امنیت اینترنت اشیای صنعتی؛
- چالش‌های امنیت اینترنت اشیای صنعتی؛
- آسیب‌پذیری‌های اجزای مختلف فناوری امنیت اینترنت اشیای صنعتی؛
- طیف تهدیدات مترتب بر اینترنت اشیای صنعتی؛
- الزامات و ملاحظات پدافند سایبری برای فناوری اینترنت اشیای صنعتی.

مدت زمان کارگاه: ۴ ساعت

کارگاه آموزشی

حفاظت از زیرساخت‌های حیاتی سایبری (CIIP)

مهندس محمدرضا فرجی‌پور
مهندس هادی کریمی

قرارگاه پدافند سایبری
سازمان پدافند غیرعامل

سرفصل‌های آموزشی کارگاه:

- تهدیدات نوین زیرساخت‌های حیاتی با تأکید بر زیرساخت‌های صنعتی (CPS)؛
- تهدیدات، آسیب‌پذیری‌ها، مخاطرات و پیامدها در زیرساخت‌های دارای وابستگی متقابل (Infrastructure Interdependencies)؛
- Threat Intelligence در حفاظت از زیرساخت‌های حیاتی سایبری؛
- سازوکار به اشتراک‌گذاری اطلاعات تهدیدات در سطح ملی در زیرساخت‌های حیاتی(ISAC & ISAS)؛
- متدولوژی مدل‌سازی تهدیدات و ارزیابی مخاطرات در زیرساخت‌های حیاتی؛
- مدل‌های تاب‌آوری و پایداری زیرساخت‌های حیاتی؛
- مطالعه موردی: حفاظت از زیرساخت‌های سایبری صنعت برق.

مدت زمان کارگاه: ۴ ساعت

کارگاه آموزشی

امنیت نرم، از نظریه تا عمل: مدل‌سازی و تحلیل انتشار، کنترل و شناسایی خودکار شایعه در شبکه‌های اجتماعی

دکتر بهروز ترک لادانی، مهندس ابراهیم صحافی‌زاده، مهندس مژگان عسگری‌زاده، مهندس میلاد رادنژاد

دانشگاه اصفهان

چکیده:

رشد روز افزون فضای مجازی و به ویژه شبکه‌های اجتماعی در بسیاری از کاربردها ارزشمند و ارزش‌آفرین است. با این حال، سادگی و فراگیری استفاده از امکانات این فضا و نقصان در فرهنگ بکارگیری آن و کمبود امکانات کافی مدیریت این فضا موجب شده که حجم شایعات موجود در آن نیز روز به روز افزایش یابد. این شایعات می‌توانند در اندک زمانی به دست میلیون‌ها کاربر رسیده و موجب خسارات فراوان شوند. در سال‌های اخیر، رواج شایعات در شبکه‌های اجتماعی که به ویژه با هدف فریب افکار عمومی ساخته می‌شوند، به یکی از نگرانی‌های جدی در جوامع مختلف تبدیل شده است. شایعات می‌توانند با قصد آسیب‌رسانی در حوزه‌های مختلف مدیریتی و انجام عملیات جنگ نرم تهیه و هدایت شوند.

بنابراین، با توجه به حجم بالای شایعات و لزوم تشخیص سریع آنها، توسعه مدل‌هایی برای تحلیل نحوه انتشار و ردیابی شایعات و همچنین ارزیابی کارایی و اثربخشی سازوکارهای مختلف مقابله با شایعه، به عنوان بخشی از سازوکارهای «امنیت نرم» از اهمیت و جایگاه ویژه‌ای برخوردار است. علاوه بر این، توسعه سامانه‌هایی که بتواند در مراحل اولیه انتشار، شایعه را به صورت خودکار تشخیص داده و اقدام به جلوگیری از انتشار بیشتر آن کند، از اولویت‌های سرمایه‌گذاری برای هر جامعه به شمار می‌رود. هدف کلی از ارائه این کارگاه، معرفی و تبیین اهمیت موضوع «امنیت نرم» به ویژه در حوزه مدیریت شایعات در فضای مجازی از دیدگاه علمی برای مخاطبین کنفرانس انجمن رمز ایران و فعالین حوزه امنیت اطلاعات و همچنین ارائه نتایج مطالعات و دستاوردهای پژوهشی ارائه کنندگان در این زمینه در سال‌های اخیر است. برای این منظور، ضمن معرفی مفاهیم تهدید و امنیت نرم و تبیین جایگاه مقابله با شایعات در فضای مجازی به عنوان یک روش تأمین «صحت نرم»، مفاهیم، روش‌ها و آخرین فعالیت‌های علمی مرتبط در این زمینه مرور شده و سپس به تشریح رویکردهای پیشنهادی ارائه‌کنندگان در حوزه‌های مدل‌سازی و تحلیل نحوه انتشار و کنترل شایعه و همچنین تشخیص خودکار شایعه خواهیم پرداخت. مخاطبین این کارگاه ضمن آشنایی با زمینه‌های موضوعی بحث، سرخط‌های تحقیقاتی فراوانی برای انجام فعالیت‌های علمی هدفمند و مفید برای جامعه و یا توسعه سامانه‌های کاربردی مرتبط دریافت خواهند کرد.

سرفصل‌های آموزشی کارگاه:

- امنیت نرم و صحت نرم: مفاهیم، رویکردها و چالش‌های موجود؛
- مدل‌سازی انتشار و کنترل نرم شایعه در پیام‌رسان‌های موبایلی؛
- شناسایی خودکار شایعه در شبکه‌های اجتماعی با رویکرد یادگیری عمیق؛
- مدل‌سازی و تحلیل رویکردهای مقابله با شایعه در شبکه‌های اجتماعی با سازوکار کنترل نرم به کمک یک مدل بازی تکاملی.

مدت زمان کارگاه: ۸ساعت

چکیده:

کارگاه آموزشی

تجزیه و تحلیل حملات سایبری و سناریوهای نفوذ به صنعت برق: نکته‌ها و آموزه‌ها

مهندس محمدمهدی احمدیان

پژوهشگاه نیرو

امنیت سایبری سامانه‌های کنترل و اتوماسیون صنعتی و اسکادا به دلیل به‌کارگیری در زیرساخت‌های حساس، حیاتی و مهم در این دهه به حدی پراهمیت شده است که به عنوان یک دغدغه مهم بین‌المللی عنوان شده است. از آنجا که صنعت برق به عنوان مادر زیرساخت‌ها، دارای حوزه‌های مختلف تولید، انتقال، فوق توزیع، توزیع، بازار، مصرف و بهره‌برداری است، مقوله امنیت سایبری در آن اهمیت ویژه‌ای دارد. طبیعتاً سامانه‌های کنترل و اتوماسیون صنعتی حوزه برق (انرژی) به دلیل اهمیت بسیار بالای خود از حملات و رخدادهای سایبری بی‌بهره نبوده‌اند، سروصدایی که بدافزارهای BlackEnergy و Industroyer در حمله به زیرساخت‌های برق اوکراین (۲۰۱۵ تا ۲۰۱۷) به راه انداختند موجب شد توجه نفوذگران به سمت سامانه‌های کنترل صنعتی حوزه برق بیشتر جلب شود و این نکته روشن شد که این سامانه‌ها تا چه میزان حساس و آسیب‌پذیر هستند. با توجه به اهمیت و ضرورت مسأله، مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق پژوهشگاه نیرو بر خود واجب می‌داند در شانزدهمین کنفرانس بین المللی انجمن رمز ایران در دانشگاه فردوسی مشهد شرکت نماید و جهت آگاه‌سازی بیشتر مسئولین، مدیران و کارشناسان صنعت برق به‌ویژه حوزه‌های توزیع، فوق توزیع و تولید برق با برگزاری کارگاه تخصصی، گستره‌ی وسیع تهدیدات سایبری و سهولت دسترسی به سامانه‌های حیاتی این صنعت و به خطر انداختن آنها را نشان دهد.

سرفصل‌های آموزشی کارگاه:

- مقدمه‌ای از وضعیت امنیت سایبری در شبکه‌های کنترل و اتوماسیون صنعتی؛
- مقدمه‌ای از بدافزارها و تهدیدات مانای پیشرفته (APT)؛
- دسته‌بندی حملات در سامانه‌های کنترل صنعتی (با محوریت حوزه توزیع، فوق توزیع- انتقال و تولید)؛
- تجزیه و تحلیل حملات سایبری، رخدادهای امنیتی و سناریوهای نفوذ به صنعت برق؛
- نمایش اجرای عملی حملات سایبری به شبکه اتوماسیون توزیع آزمایشگاهی.

مدت زمان کارگاه: ۴ ساعت

چکیده:

کارگاه آموزشی

کارگاه عمومی‌سازی امنیت و رمز در مدارس ویژه معلمان و دبیران

دهکده امنیت و رمز

دانشگاه فردوسی مشهد

از دیدگاه برخی از صاحبنظران، شناسایی استعدادهای برتر برای پرورش افراد نخبه باید از مدارس آغاز شود. کشف و شناسایی استعدادهای برتر و ایجاد زمینه‌های لازم برای پرورش و رشد علمی این استعدادها، از مهمترین گام‌هایی است که باید برداشته شود. از آنجایی که معلم یکی از مهمترین پایه‌های رشد و تربیت افراد با استعداد می‌باشد، دهکده امنیت و رمز با هدف ترویج رمز و امنیت و استعدادیابی در آموزش و پرورش، برای دانش‌آموزان متوسطه در طی یک سال گذشته سه رویداد دانش‌آموزی برگزار کرده است. در این کارگاه قصد داریم تا با اشتراک تجربیات بدست آمده دهکده با معلمان دبیران توانمند و علاقمند و نیز استفاده از تجربیات ایشان، فراگیری این برنامه را توسعه دهیم. در نتیجه، هدف اصلی این کارگاه زمینه‌سازی گسترش آموزش و ترویج مفاهیم و اصول امنیت و رمز و نیز کشف و پرورش استعدادهای جوان در آموزش و پرورش، با کمک دانشگاه و آموزش و پرورش می‌باشد. محوریت اصلی این کارگاه نیز بر روی چگونگی عمومی‌سازی و تصویرسازی مفاهیم علمی- فنی امنیتی و بیان آنها در قالب مثال‌های ساده، مهیج و کاربردی توسط معلمان برای دانش‌آموزان می‌باشد.

سرفصل‌های آموزشی کارگاه:

- هم‌اندیشی چگونگی بیان مطالب تخصصی امنیتی به‌شکل ساده و قابل فهم برای دانش‌آموزان؛
- چگونگی عمومی‌سازی و تصویرسازی روش‌های رمزنگاری کلاسیک و مدرن؛
- چگونگی عمومی‌سازی و تصویرسازی پروتکل‌های امنیتی و حملات علیه آنها؛
- چگونگی عمومی‌سازی و تصویرسازی روش‌های پنهان‌نگاری داده‌ها در متن و تصویر؛
- چگونگی عمومی‌سازی و تصویرسازی مباحث امنیت شبکه و تجهیزات امنیتی؛
- چگونگی عمومی‌سازی هک و نفوذ در قالب مثال‌های ساده و مهیج عملی؛
- نمونه سؤالات مسابقات دهکده به سبک شهر ریاضی.

مدت زمان کارگاه: ۴ ساعت

۲۸- سابقه برگزاری کنفرانس‌های سالیانه انجمن رمز ایران

دوره برگزاری	تاریخ برگزاری	دانشگاه میزبان	دبیرکنفرانس
کنفرانس اول	آبان ۱۳۸۰	دانشگاه امام حسین (ع)	دکتر حسین ثامتی
کنفرانس دوم	مهر ۱۳۸۲	دانشگاه صنعتی شریف	دکتر محمود سلماسی‌زاده
کنفرانس سوم	اسفند ۱۳۸۴	دانشگاه صنعتی اصفهان	مرحوم دکتر مهدی برنجکوب
کنفرانس چهارم	مهر ۱۳۸۶	دانشگاه علم‌وصنعت ایران	دکتر مجید نادری
کنفرانس پنجم	مهر ۱۳۸۷	دانشگاه صنعتی مالک اشتر تهران	دکتر مرتضی براری
کنفرانس ششم	مهر ۱۳۸۸	دانشگاه اصفهان	دکتر بهروز ترک لادانی
کنفرانس هفتم	شهریور ۱۳۸۹	دانشگاه خواجه نصیرالدین طوسی	دکتر محمود احمدیان
کنفرانس هشتم	شهریور ۱۳۹۰	دانشگاه فردوسی مشهد	دکتر محسن کاهانی

دوره برگزاری	تاریخ برگزاری	دانشگاه میزبان	دبیرکنفرانس
کنفرانس نهم	شهریور ۱۳۹۱	دانشگاه تبریز	دکتر ضیاءالدین کوزه‌کنانی
کنفرانس دهم	شهریور ۱۳۹۲	دانشگاه یزد	دکتر فضل‌الله ادیب‌نیا
کنفرانس یازدهم	شهریور ۱۳۹۳	دانشگاه تهران	دکتر محمودرضا هاشمی
کنفرانس دوازدهم	شهریور ۱۳۹۴	دانشگاه گیلان	دکتر رضا ابراهیمی آتانی
کنفرانس سیزدهم	شهریور ۱۳۹۵	دانشگاه شهید بهشتی	دکتر علی جهانیان
کنفرانس چهاردهم	شهریور ۱۳۹۶	دانشگاه شیراز	دکتر محمدحسین شیخی
کنفرانس پانزدهم	شهریور ۱۳۹۷	دانشگاه تربیت دبیر شهید رجایی	دکتر نصور باقری
کنفرانس شانزدهم	شهریور ۱۳۹۸	دانشگاه فردوسی مشهد	دکتر عباس قائمی بافقی

امن افزار گستر شریف

ارائه راهکارهای یکپارچه فناوری اطلاعات و ارتباطات امن

- تجهیزات امنیت شبکه (Firewall, UTM, WAF, IPS, DFS, NAT)
- مشاوره و امن‌سازی (ISMS, PCI DSS, ...)
- تیم واکنش به رخدادهای امنیتی (CSIRT)
- مرکز عملیات امنیت (SOC)
- سامانه پیشگیری از نشت داده (DLP/DRM)
- امنیت سیستم‌های کنترل صنعتی (ICS)
- آزمون نفوذ (Penetration Test)
- زیرساخت کلید عمومی (PKI)

ارتباط با ما

۰۲۱ - ۴۳۶۵۲۰۰۰

info@amnafzar.ir

www.amnafzar.ir

شرکت مهندسی ارتباطی

پیام پرداز

پیشران اطلاعات و ارتباطات امن

شکل‌گیری از سال ۱۳۶۵
تشکیل هسته علمی در دانشگاه صنعتی اصفهان

۱۵۰ نفر پرسنل
شرکت دانش‌بنیان با زبده‌ترین کارشناسان

بیش از ۴۰ الگوریتم و پروتکل
تنها شرکت خصوصی فعال در حوزه طراحی و تحلیل الگوریتم‌ها و پروتکل‌های امنیتی

بیش از ۳۰۰ سازمان
طیف وسیعی از مشتریان

تأسیس در سال ۱۳۷۵
تبدیل هسته علمی دانشگاهی به شرکت خصوصی با هدف ارائه خدمات تخصصی در زمینه امنیت اطلاعات و ارتباطات

۳۰ محصول
طراحی و تولید محصولات حوزه افتا با بکارگیری الگوریتم‌ها و پروتکل‌های بومی

بیش از ۱۵۰ پروژه
اجرای پروژه‌های امنیتی راهبردی و غیر راهبردی

بیش از ۴۵۰ هزار کاربر
محصول کیهان با بیشترین کاربری در سطح کشور

گواهی‌نامه‌ها

- رتبه یک شورای عالی انفورماتیک در حوزه امنیت فضای تبادل اطلاعات
- دارای گواهی‌نامه فعالیت و تأیید محصول از مرکز مدیریت راهبردی افتا، سازمان پدافند غیرعامل و سازمان فناوری اطلاعات
- دارای گواهی‌نامه ثبت اختراع ماژول امنیتی کیا و سامانه امن‌ساز شبکه کیهان
- دارای گواهی‌نامه سمتا

افتخارات

- شرکت برتر در جشنواره ملی فاوای وزارت ارتباطات (۱۳۹۰ و ۱۳۹۳)
- واحد فناوری برتر پژوهشی، منتخب وزارت علوم، تحقیقات و فناوری (۱۳۹۲)
- قرار گرفتن در لیست شرکت‌های دانش‌بنیان معاونت علمی نهاد ریاست جمهوری (۱۳۹۳)
- طراحی و ساخت محصول راوین، تنها مرکز عملیات امنیت (SOC) بومی با حمایت، نظارت و تأیید مرکز تحقیقات مخابرات ایران (ITRC)

www.payampardaz.com

APK

Engineering and Technical Company

Amn Pardazan Kavir

بـزرگترین ارائه دهنده سیستم ها و خدمات
در حوزه امنیت شبکه وامنیت اطلاعـات

UTM APKGate
Unified Threat Management
سیستم مدیریت یکپارچه تهدیدات

APK SIEM
Security Information and Event Management
سامانه مدیریت وقایع و رخدادهای امنیتی

APK InfoSIS
Information Security Impelementation System
سامانه مدیریت امنیت اطلاعات

APK SWAP
Security Web Access Platform
سامانه دسترسی امن به اینترنت

SOC
Security Operation Center
مرکز عملیات امنیت

ISMS
Information Security Management System
سیستم مدیریت امنیت اطلاعات

PenTest
Penetration Test
تست نفوذپذیری

www.apk-group.net
021- 42273
Unit 505, No.2, Shahid Naderi St
Keshavarz Blvd., Tehran, Iran

روتر بومی سودار

پشتیبانی از کارتهای 10G تا 100G

VPLS | QoS/Firewall | MPLS | IPV6 | BGP
Tunnels | OSPF | VXLAN | VRF | EIGRP

محصولی دانش بنیان و جایگزینی شایسته برای روترهای سیسکو

اَمنش

همدار موبایل امن سازمانی

راه حلی برای استفاده‌ی موبایل‌های هوشمند در محیط کار

مـــهـــار | موبایل کاملا کنترل شده
احاطه ی کامل بر تمامی امکانات نرم افزاری و سخت افزاری موبایل و امکان تعیین محدودیت های لازم بر روی آن

جـــزیـــره | موبایل محیط کاری مجزا
ایجاد محیطی امن و کنترل شده در کنار محیط شخصی و حفظ حریم خصوصی

کـــیـــوسک | موبایل تک کاره
ارائـه ی خدمـات در قالـب اطـلاع رسـانی، ثبـت سفارشـات روابط عمومی و سرگرمی

اختصاصی | موبایل سفارشی
یک سیستم عامل کاملا سفارشی شده بر پایه سیستم عامل پیش فرض نصب شده بر روی گوشی

WWW.AMNESH.IR

برگزاری هفدهمین کنفرانس بین‌المللی انجمن رمز ایران

بزرگترین رویداد علمی سالیانه کشور در حوزه رمزشناسی و امنیت اطلاعات

به میزبانی دانشگاه علم‌وصنعت ایران

هفدهمین کنفرانس بین‌المللی انجمن رمز ایران روزهای ۱۹ و ۲۰ شهریور ۱۳۹۹ به میزبانی دانشگاه علم و صنعت ایران در محل این دانشگاه برگزار خواهد شد.

هفدهمین کنفرانس بین‌المللی انجمن رمز ایران با هدف دانش‌افزایی اساتید، پژوهشگران و متخصصین حوزه رمزشناسی و امنیت اطلاعات و نیز انتشار یافته‌های نو و بدیع در این زمینه، در دانشگاه علم و صنعت ایران برگزار خواهد شد. آشنایی و ارتباط استادان، محققین، دانشجویان، مدیران و تمامی علاقه‌مندان این حوزه به همراه بررسی چالش‌های علمی و اجرایی کشور در حوزه افتا (امنیت فضای تولید و تبادل اطلاعات) با تأکید بر امن‌سازی سامانه‌های اطلاعاتی و ارتباطی از دیگر اهداف این کنفرانس است.

نظر به مخاطرات و تهدیدات فزاینده سایبری، موضوع بسیار مهم «امن‌سازی زیرساخت‌های حیاتی و حساس کشور» نیز به عنوان محور علمی-ترویجی کنفرانس انتخاب شده است تا فضای تعامل بیشتری برای ارتباط دانشگاهیان و محققین حوزه افتا با مدیران و متخصصین شاغل در صنایع کشور، بویژه دست‌اندرکاران سامانه‌های کنترل صنعتی در صنایع نفت، گاز و انرژی ایجاد شود.

کمیته علمی این کنفرانس از تمامی استادان، دانشجویان و متخصصین حوزه افتا دعوت می‌نماید با ارسال مقالات و حضور ارزشمند خود در این رویداد علمی مشارکت نمایند.

عناوین محورهای کنفرانس:

- مبانی رمزشناسی
- پیاده‌سازی الگوریتم‌های رمزنگاری و حملات مرتبط
- امنیت شبکه
- پروتکل‌های امنیتی
- امنیت رایانش
- مهندسی امنیت و امنیت خدمات الکترونیکی
- نهان سازی اطلاعات
- جرم یابی در فضای مجازی
- امنیت زیرساخت‌های حیاتی و حساس کشور (محور علمی-ترویجی)

علاقه‌مندان می‌توانند برای کسب اطلاعات بیشتر از طریق رایانامه iscisc2020@iust.ac.ir و یا شماره تماس ۰۲۱۷۳۲۲۵۴۱۵ با دبیرخانه کنفرانس تماس حاصل نمایند. همچنین آخرین اطلاعات و اخبار مربوط به کنفرانس بر روی وبگاه آن به نشانی http://iscisc2020.iust.ac.ir قابل دسترس خواهد بود.

با امید به دیدار شما در ایام برگزاری

هفدهمین کنفرانس انجمن رمز ایران

دبیرخانه انجمن رمز ایران

خیابان آزادی - غرب دانشگاه صنعتی شریف - خیابان شهید صادقی - پلاک۲۶ - طبقه۴ - واحد۱۶

تلفن: ۶۶۰۲۱۱۵۰ - فکس: ۶۶۰۲۱۱۴۹ - وبگاه: www.isc.org.ir - رایانامه: info@isc.org.ir