



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)



انجمن رمز ایران
Iranian Society of Cryptology

موضوعات کنفرانس:

- مبانی رمزشناسی و تحلیل رمز
- پیاده‌سازی الگوریتم‌های رمزنگاری و حملات مرتبط
- هوش مصنوعی و امنیت
- چالش نیروی انسانی و آموزش در امنیت
- پروتکل‌های امنیتی - روش‌ها و مدل‌های امنیتی
- امنیت شبکه - امنیت رایانش
- موضوعات نوین در رمزنگاری و افتا (امنیت سایبری)
- پنهان‌سازی اطلاعات - جرم‌یابی دیجیتال
- مدیریت امنیت و حریم خصوصی
- مقالات کوتاه علمی و صنعتی

بیست و سومین کنفرانس بین‌المللی امنیت رمزشناسی

تاریخ فراخوان مقالات

• مهلت ارسال مقالات: ۱۶ مرداد ۱۴۰۵

• اعلام نتایج داوری فراخوان: ۱۰ مهر ۱۴۰۵

• نشانی ارسال مقالات از طریق وبسایت کنفرانس: iscisc2026.aut.ac.ir

تاریخ‌های مهم کنفرانس

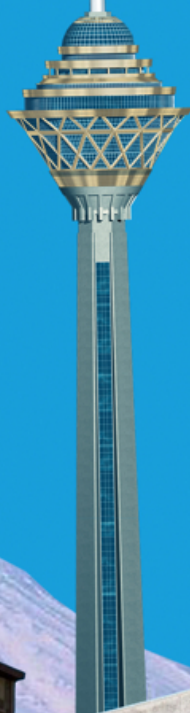
• بیست و سومین کنفرانس بین‌المللی انجمن رمز ایران
در امنیت اطلاعات و رمزشناسی

- ۲۹ و ۳۰ مهرماه ۱۴۰۵
- دانشکده ریاضی و علوم کامپیوتر
- دانشگاه صنعتی امیرکبیر - تهران



مهم: مقالات فارسی پذیرفته شده در شماره ویژه دو فصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا) با نمایه ISC و مورد تأیید وزارت عتف و مقالات انگلیسی در شماره ویژه مجله بین‌المللی ISeCure با نمایه‌های WoS-JCR و Scimago-SJR منتشر، و مقالات پذیرفته شده‌ی هر دو فراخوان در زمان برگزاری کنفرانس به صورت حضوری ارائه خواهند شد.

iscisc2026.aut.ac.ir



دانشگاه
صنعتی
امیرکبیر
(پلی تکنیک تهران)

بسم الله الرحمن الرحيم

کتابچه راهنمای

بیست و سومین کنفرانس بین‌المللی انجمن رمز ایران در امنیت اطلاعات و رمزشناسی

برگزار کننده:

انجمن رمز ایران ،
دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

محل برگزاری:

دانشگاه صنعتی امیرکبیر

مهرماه ۱۴۰۵ خورشیدی

فهرست مطالب

۱	پیشگفتار
۳	برگزارکنندگان و حامیان
۳	برگزارکنندگان
۳	حامیان معنوی
۴	حامیان مالی
۶	ساختار سازمانی کنفرانس
۹	فراخوان مقالات
۱۳	زمان‌بندی کنفرانس
۱۷	سخنرانی‌ها
۱۷	سخنرانان کلیدی
۱۹	سخنرانان مدعو
۲۸	نمایه مقالات
۵۵	کارگاه‌ها
۵۵	عناوین و ارائه‌دهندگان کارگاه‌ها
۶۷	اطلاعات کارگاه‌ها
۶۹	برترین‌ها
۶۹	رساله‌های برتر
۶۹	پایان‌نامه‌های برتر
۷۰	شاخه‌های دانشجویی برتر
۷۱	کافه امید و اشتغال

پیشگفتار

با سلام و درود بر روح عظیم الشان رهبر شهید انقلاب و تمامی شهدای سرافراز ایران در تمامی دوران؛ آنان که نامشان با عزت، ایثار و سربلندی این سرزمین گره خورده است.

بیست و سومین کنفرانس بین‌المللی انجمن رمز ایران در امنیت اطلاعات و رمزشناسی، در روزهای ۲۹ و ۳۰ مهرماه ۱۴۰۵، به میزبانی دانشکده ریاضی و علوم کامپیوتر دانشگاه صنعتی امیرکبیر برگزار می‌شود؛ رویدادی علمی که بار دیگر فرصتی فراهم آورده است تا پژوهشگران، استادان، دانشجویان و متخصصان گرد هم آیند و حاصل اندیشه، تلاش و پژوهش خود را در عرصه امنیت اطلاعات و رمزنگاری به اشتراک بگذارند.

امسال، در حالی که استقبال این گردهمایی علمی می‌رویم که مسیر برگزاری آن از فراز و نشیب‌های روزگار بی‌تأثیر نبوده است. هم‌زمان با آغاز فراخوان بهاره کنفرانس، کشورمان روزهای دشوار جنگ رمضان را تجربه کرد و در ادامه، با قطعی اینترنت و محدودیت‌های ارتباطی روبه‌رو شدیم؛ شرایطی که بی‌تردید بر روند ارتباطات علمی، تعاملات پژوهشی و فعالیت‌های اجرایی کنفرانس تأثیر گذاشت. با این همه، چراغ پژوهش و اشتیاق به دانستن خاموش نشد و همراهی جامعه علمی، تلاش اعضای کمیته‌ها و همت پژوهشگران، امکان ادامه این مسیر را فراهم آورد. برگزاری این کنفرانس در چنین شرایطی، یادآور ارزش پایداری، همدلی و امید در راه علم و دانش است.

در بیست و سومین دوره کنفرانس، در مجموع ۱۰۴ مقاله از ۴۰ دانشگاه و مرکز علمی و پژوهشی مختلف دریافت شد. در میان آثار ارسالی، علاوه بر مقالات پژوهشگران داخلی، مقالاتی از خارج از کشور نیز حضور داشتند که بر گستره علمی و بین‌المللی این رویداد افزودند. از مجموع مقالات دریافتی، ۷۰ مقاله به زبان انگلیسی و ۳۴ مقاله به زبان فارسی نگارش شده بود. برای ارزیابی علمی این آثار، در مجموع ۳۱۶ گزارش داوری دریافت شد که به‌طور متوسط معادل ۳.۰۳ داوری برای هر مقاله است. مقالات با مشارکت داوران متخصص و بر پایه بررسی علمی و تخصصی مورد ارزیابی قرار گرفتند تا آثار برگزیده با توجه به کیفیت پژوهش، نوآوری و میزان انطباق با محورهای کنفرانس انتخاب شوند. بی‌تردید، صرف وقت و دانش تخصصی داوران، از ارکان اصلی اعتبار و کیفیت علمی این رویداد بوده است.

از نظر موضوعی، حوزه هوش مصنوعی و امنیت با ۲۴ مقاله، بیشترین تعداد مقالات را به خود اختصاص داد و پس از آن، مبانی رمزنگاری با ۱۵ مقاله در جایگاه بعدی قرار گرفت. این استقبال، از یک سو بیانگر توجه فزاینده جامعه علمی به پیوند میان هوش مصنوعی و امنیت است و از سوی دیگر، اهمیت پایدار مباحث بنیادی رمزنگاری را در مواجهه با نیازها و چالش‌های نوین فناوری یادآور می‌شود.

پس از طی فرایند داوری و بررسی‌های کمیته علمی، ۲۵ مقاله در محورهای مختلف کنفرانس پذیرفته شد که شامل ۲۲ مقاله به زبان انگلیسی و ۳ مقاله به زبان فارسی است. این آثار، بخشی از تلاش‌های علمی پژوهشگران برای پاسخ‌گویی به مسائل روز و گسترش مرزهای دانش در حوزه امنیت اطلاعات، رمزشناسی و هوش مصنوعی و امنیت را بازتاب می‌دهند.

برنامه علمی این دوره، افزون بر ارائه مقالات پذیرفته‌شده، میزبان دو سخنرانی کلیدی خارجی و داخلی و ۹ سخنرانی مدعو از سوی پژوهشگران و دانش‌آموختگان جوان دکتری است. این سخنرانی‌ها فرصتی فراهم می‌آورند تا آخرین دستاوردهای علمی و پژوهشی ارائه شود و زمینه آشنایی بیشتر شرکت‌کنندگان با ایده‌ها، رویکردها و مسیرهای نوظهور پژوهش در حوزه امنیت اطلاعات و رمزشناسی فراهم آید. توجه ویژه به پژوهشگران جوان، به‌ویژه دانش‌آموختگان تازه دکتری، گامی در جهت دیده‌شدن توان علمی نسل جدید، ایجاد فرصت برای عرضه دستاوردهای آنان و تقویت پیوند میان پژوهشگران باتجربه و استعدادهای نوظهور

است.

از دیگر برنامه‌های ارزشمند این دوره، برگزاری برنامه‌ای ویژه برای دانش‌آموزان در حاشیه کنفرانس است؛ برنامه‌ای با هدف آشنا کردن نسل نوجوان با مفاهیم و اهمیت امنیت سایبری و ایجاد علاقه به دنیای رمزنگاری، حفاظت از اطلاعات و فناوری‌های امن. باور داریم که آینده علمی کشور از پرسش‌های امروز شکل می‌گیرد و آشنایی زودهنگام دانش‌آموزان با این حوزه، می‌تواند جرقه‌ای برای پرورش استعدادها و علاقه‌مندی‌هایی باشد که در سال‌های آینده به پژوهشگران و متخصصان توانمند تبدیل شوند. همچنین، در این دوره تلاش شده است ارتباط میان دانشگاه و صنعت، از سطح گفت‌وگوهای معمول فراتر رود و به فرصتی برای شناخت مسائل واقعی و شکل‌گیری ایده‌های کاربردی تبدیل شود. در همین راستا، برنامه‌ای برای حضور شرکت‌های فعال در حوزه امنیت و ارائه دیدگاه‌ها، تجربه‌ها و راهکارهای امیدبخش آنان (ارائه‌های امیدآفرین) در نظر گرفته شده است تا این شرکت‌ها ضمن معرفی فعالیت‌ها و دستاوردهای خود، نیازها، چالش‌ها و مسائل حل‌نشده حوزه کاری‌شان (رویداد Reverse Pitch) را نیز مطرح کنند. امید آن است که طرح این نیازها، جرقه‌ای در ذهن پژوهشگران بزند و زمینه‌ساز شکل‌گیری ایده‌ها و طراحی راهکارهای نوآورانه برای پاسخ‌گویی به مسائل واقعی باشد؛ چراکه گاه ارزشمندترین ایده‌های پژوهشی نه از دل پرسش‌های انتزاعی، بلکه از شناخت دقیق یک نیاز و تلاش برای برطرف کردن آن متولد می‌شوند. چنین تعاملی می‌تواند به تقویت همکاری‌های دانشگاه و صنعت، جهت‌دهی به پژوهش‌های مسئله‌محور و تبدیل دانش به راهکارهایی مؤثر و قابل استفاده کمک کند.

امیدواریم این گردهمایی، فراتر از ارائه مقاله‌ها و نتایج پژوهشی، فرصتی برای شکل‌گیری دوستی‌های علمی، آغاز همکاری‌های تازه، تبادل تجربه میان نسل‌های مختلف پژوهشگران و پرورش ایده‌هایی باشد که بتوانند در آینده، راهگشای مسائل واقعی جامعه و صنعت باشند. باور داریم که پیشرفت علمی، بیش از هر چیز، به گفت‌وگو، همفکری، اعتماد و تلاش جمعی نیاز دارد؛ ارزش‌هایی که می‌توانند حتی در دشوارترین شرایط، راه را به سوی آینده‌ای روشن‌تر هموار کنند.

در پایان، از تمامی نویسندگان و پژوهشگرانی که با ارسال آثار خود به غنای علمی این دوره افزودند، از سخنرانان گرامی، داوران ارجمند و اعضای محترم کمیته علمی بیست‌وسومین کنفرانس بین‌المللی انجمن رمز ایران که با دانش، تجربه و مسئولیت‌پذیری در برگزاری این رویداد مشارکت کردند، و از همه همکاران، برگزارکنندگان، حامیان و همراهانی که با تلاش و دلسوزی در شکل‌گیری این کنفرانس سهیم بوده‌اند، صمیمانه سپاسگزاری می‌کنیم. همچنین، قدردان میزبانی دانشگاه صنعتی امیرکبیر و همراهی تمامی عزیزانی هستیم که در تحقق این برنامه علمی یاری‌رسان ما بوده‌اند.

به امید روزهایی سرشار از آرامش، همدلی و پیشرفت برای ایران عزیزمان؛ روزهایی که در آن، دانش چراغ راه باشد، نیازها به فرصت تبدیل شوند و اندیشه‌های جوان، افق‌های تازه‌ای برای امنیت و آبادانی کشور بگشایند.

دبیران علمی بیست‌وسومین کنفرانس انجمن رمز ایران در امنیت اطلاعات و رمزشناسی
معصومه صفخانی، فرخ‌لقا معظمی

برگزارکنندگان و حامیان

برگزارکنندگان



حامیان معنوی



حامیان مالی

حامی برجسته



ریاست جمهوری
معاونت علمی، فناوری و اقتصاد دانش بنیان
دبیرخانه ستاد توسعه علوم و فناوری افق



ریاست جمهوری
مرکز همکاری های تحول و پیشرفت

حامی طلایی ویژه



پژوهشگاه توسعه فناوری های پیشرفته

حامی طلایی



شرکت خدمات انفورماتیک

حامی نقره‌ای



حامی برنزی



ساختار سازمانی کنفرانس

رئیس کنفرانس: دکتر مسعود صباغی، دانشیار دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر
دبیر کمیته علمی کنفرانس:

- دکتر معصومه صفحانی، دانشیار دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی
- دکتر فرخ لقا معظمی گودرزی، دانشگاه شهید بهشتی

دبیر کنفرانس: دکتر فرهاد رحمتی - دانشگاه صنعتی امیرکبیر
دبیر اجرایی کنفرانس: دکتر امین حسینقلی زاده، دانشگاه صنعتی امیرکبیر
کمیته علمی (مرتب شده با نام خانوادگی به ترتیب حروف الفبا)

- دکتر مهدی آبادی - دانشگاه تربیت مدرس
- دکتر رضا ابراهیمی آتانی - دانشگاه گیلان
- دکتر زهرا احمدیان - دانشگاه شهید بهشتی
- دکتر محمود احمدیان عطاری - دانشگاه صنعتی خواجه نصیرالدین طوسی
- دکتر ترانه اقلیدس - دانشگاه صنعتی شریف
- دکتر مرتضی امینی - دانشگاه صنعتی شریف
- دکتر منصور باقری - دانشگاه تربیت دبیر شهید رجایی
- دکتر مجید بیات - دانشگاه شاهد
- دکتر حسین پیل آرام - دانشگاه صنعتی شریف
- دکتر محمدحسام تدین - پژوهشگاه ارتباطات و فناوری اطلاعات
- دکتر بهروز ترک لادانی - دانشگاه اصفهان
- دکتر طلا تفضلی - پژوهشگاه ارتباطات و فناوری اطلاعات
- دکتر علی جهانیان - دانشگاه شهید بهشتی
- دکتر امین حسینقلی زاده - دانشگاه صنعتی امیرکبیر
- دکتر محمد دخیل علیان - دانشگاه صنعتی اصفهان
- دکتر صادق دری نوگورانی - دانشگاه تربیت مدرس
- دکتر مطهره دهقان - دانشگاه تربیت مدرس
- دکتر فرهاد رحمتی - دانشگاه صنعتی امیرکبیر
- دکتر پروین رستگاری - دانشگاه صنعتی اصفهان

- مهندس حبیب رستمی - سازمان جهاد دانشگاهی صنعتی شریف
- دکتر محسن رمضان یارنندی - پژوهشگاه توسعه فناوری‌های پیشرفته
- دکتر مهدی سجادیه - دانشگاه آزاد اسلامی واحد اصفهان
- دکتر محمود سلماسی زاده - دانشگاه صنعتی شریف
- دکتر هادی سلیمانی - دانشگاه شهید بهشتی
- دکتر هادی شهریار شاه‌حسینی - دانشگاه علم و صنعت ایران
- دکتر حمیدرضا شهریار - دانشگاه صنعتی امیرکبیر
- دکتر معصومه صفحانی - دانشگاه تربیت دبیر شهید رجایی
- دکتر محمدرضا عارف - دانشگاه صنعتی شریف
- دکتر محمد عبداللہی‌ازگمی - دانشگاه علم و صنعت ایران
- دکتر محمد علی - دانشگاه صنعتی امیرکبیر
- دکتر بیژن علیزاده - دانشگاه تهران
- دکتر جواد علیزاده - دانشگاه جامع امام حسین (ع)
- دکتر بهار فراهانی - دانشگاه شهید بهشتی
- دکتر فرخ‌لقا معظمی‌گودرزی - دانشگاه شهید بهشتی
- دکتر حمید ملا - دانشگاه اصفهان
- مهندس جواد مهاجری - دانشگاه صنعتی شریف
- دکتر عبدالرسول میرقدری - دانشگاه جامع امام حسین (ع)
- دکتر محمدرضا هوشمنداصل - دانشگاه محقق اردبیلی
- Dr. Karim Baghery - KU Leuven
- Dr. Joachim Posegga - Passau Institute of Digital Security
- Dr. Hamed Nemati - KTH Royal Institute of Technology
- Dr. Narges Yousefnezhad - Binare.io
- Dr. Hosein Hadipour - Ruhr University Bochum
- Dr. Hamid Bostani - University of Luxembourg
- Dr. Mohammad Eslami - Estonian Chip Competence Center

دبیر کارگاه‌ها: دکتر محمد علی، دانشگاه صنعتی امیرکبیر
دبیرخانه کنفرانس:

- مهندس نفیسه آغویی خواه، دانشگاه صنعتی امیرکبیر
- مهندس ریحانه سراج زاده، دانشگاه صنعتی امیرکبیر

دبیر تعامل دانشگاه و صنعت: دکتر بهار فراهانی، دانشگاه صنعتی امیرکبیر
مسئول تعامل دانشگاه و صنعت: جلال سبزه، دانشگاه صنعتی امیرکبیر
مسئول وبسایت: مریم اسدی نیا، دانشگاه صنعتی امیرکبیر
مسئول مالی: مهرداد حسنی، دانشگاه صنعتی امیرکبیر

فراخوان مقالات

به اطلاع می‌رساند که به حول و قوه الهی بیست و سومین کنفرانس بین‌المللی انجمن رمز ایران در زمینه امنیت اطلاعات و رمزشناسی (ISCISC 2026) در روزهای ۲۹ و ۳۰ مهرماه ۱۴۰۵ در دانشکده ریاضی و علوم کامپیوتر دانشگاه صنعتی امیرکبیر برگزار خواهد شد.

شایان ذکر است که همانند سال گذشته، مقالات فارسی پذیرفته‌شده در شماره ویژه دوفصلنامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا) با نمایه ISC و رتبه «ب» رده‌بندی وزارت عتف و مقالات انگلیسی در شماره ویژه مجله بین‌المللی ISeCure با نمایه‌های WoS-JCR و SJR-SCImago با رتبه بین‌المللی Q4 منتشر، و مقالات پذیرفته‌شده هر دو فراخوان در زمان برگزاری کنفرانس به‌صورت حضوری ارائه خواهند شد.

از همه اعضای محترم انجمن رمز ایران، اساتید گرانقدر و پژوهشگران عزیز تقاضا می‌شود هرکدام به سهم خود یاری‌گر انجمن برای اطلاع‌رسانی فراخوان این رویداد مهم باشند و با انعکاس فراخوان به همکاران، پژوهشگران آشنا و دانشجویان خود، از ایشان بخواهند تا در فرصت این فراخوان نسبت به ارسال مقالات ارزشمند خود به این کنفرانس اهتمام لازم را داشته باشند.

تاریخ‌های مهم

مهلت ارسال مقالات:

- ۱۶ مردادماه ۱۴۰۵ (تمدید شد)، ۱۶ مرداد ماه ۱۴۰۵

مهلت ارسال اصلاحات مقالات:

- ۸ مهرماه ۱۴۰۵ (تمدید شد)، ۱۲ مهر ماه ۱۴۰۵

اعلام نتایج داوری:

- ۳۱ شهریورماه ۱۴۰۵ (تمدید شد)، ۱۰ مهرماه ۱۴۰۵ (تمدید شد)، ۱۵ مهر ماه ۱۴۰۵

نشانی ارسال مقالات از طریق وبسایت کنفرانس: <https://iscisc2026.aut.ac.ir>

نشانی ارسال مقالات نویسندگان خارج از کشور: <https://easychair.org/conferences/?conf=iscisc2026>

محورهای تخصصی

کنفرانس از همه پژوهشگران و صنعتگران حوزه امنیت اطلاعات و رمزشناسی برای انتشار یافته‌های نو و بدیع در محورهای تخصصی زیر دعوت می‌کند:

مبانی رمزشناسی و تحلیل رمز

- الگوریتم‌های رمزنگاری متقارن
- الگوریتم‌های رمزنگاری نامتقارن و امضاهای رقمی
- توابع چکیده‌ساز
- امنیت نظریه اطلاعاتی
- موضوعات پیشرفته در رمزنگاری (رمزنگاری تابعی، رمزنگاری هم‌ریخت، ...)

پیاده‌سازی الگوریتم‌های رمزنگاری و حملات مرتبط

- پیاده‌سازی نرم‌افزاری و سخت‌افزاری الگوریتم‌های رمزنگاری
- حملات کانال جانبی و روش‌های مقابله با آن‌ها
- سامانه‌های رمزنگاری نهفته
- دست‌کاری سخت‌افزار و روش‌های مقابله با آن
- شتاب‌دهنده‌های سخت‌افزاری رمزنگاری
- تحلیل پیاده‌سازی الگوریتم‌های رمزنگاری

هوش مصنوعی و امنیت

- امنیت و حریم خصوصی هوش مصنوعی
- یادگیری ماشین خصمانه
- امنیت شبکه‌های اجتماعی، متاورس و سامانه‌های مبتنی بر واقعیت افزوده

پروتکل‌های امنیتی

- پروتکل‌های احراز اصالت و احراز هویت
- پروتکل‌ها و اثبات‌های دانش صفر
- محاسبات چندطرفه امن
- طراحی پروتکل‌های امنیتی جدید
- تحلیل پروتکل‌های امنیتی
- حملات به پروتکل‌های امنیتی
- درستی‌سنجی صوری پروتکل‌های امنیتی

روش‌ها و مدل‌های امنیتی

- کنترل دسترسی
- گمنامی، حریم خصوصی و مدیریت اعتماد
- تحلیل و مدل‌سازی تهدید
- روش‌ها و مدل‌های صوری

امنیت شبکه

- امنیت شبکه‌های بی‌سیم و موبایل
- امنیت زیرساخت شبکه
- تشخیص و جلوگیری از نفوذ به شبکه
- تحلیل امنیتی پروتکل‌های شبکه

امنیت رایانش

- امنیت سخت‌افزار
- امنیت سیستم‌عامل
- امنیت پایگاه داده
- امنیت وب
- امنیت برنامه‌های کاربردی همراه
- کشف آسیب‌پذیری و آزمون فاز
- تحلیل بدافزار

مدیریت امنیت و حریم خصوصی

- سامانه مدیریت امنیت اطلاعات
- معماری‌های امنیت
- مدیریت مخاطره
- امنیت کسب‌وکار و بانکداری الکترونیکی
- امنیت سلامت الکترونیکی
- امنیت آموزش الکترونیکی
- فناوری‌های ارتقای حریم خصوصی

پنهان سازی اطلاعات

- نهان نگاری و نشان گذاری
- نهان کاوی اطلاعات
- کاربردهای پنهان سازی اطلاعات

جرم یابی دیجیتال

- روش ها و ابزارهای جرم یابی دیجیتال
- جرم یابی پایگاه داده و شبکه
- جرم یابی دستگاه همراه
- جرم یابی جرایم سایبری

موضوعات نوین در رمزنگاری و امنیت سایبری

- رمزنگاری کوانتومی و پسا کوانتومی
- فناوری زنجیره قالب و رمزارزها
- امنیت اینترنت اشیا، کلان داده ها و رایانش ابری
- امنیت سامانه های سایبر-فیزیکی
- امنیت و حریم خصوصی هوش مصنوعی
- یادگیری ماشین خصمانه
- امنیت شبکه های اجتماعی، متاورس و سامانه های مبتنی بر واقعیت افزوده

چالش نیروی انسانی و آموزش در امنیت

- مقالات کوتاه علمی و صنعتی

ارسال مقالات

- تمام مقالات باید از طریق وبسایت کنفرانس ارسال شوند.
- مقالات انگلیسی در قالب مجله ISeCure تنظیم شوند. برای مشاهده راهنمای آماده سازی مقالات انگلیسی به نشانی «راهنمای آماده سازی مقالات انگلیسی» مراجعه شود. برای مقالات انگلیسی فرم Author Declaration on the Use of Artificial Intelligence تکمیل و امضا و ارسال شود.
- مقالات فارسی در قالب مجله منادی افتا تنظیم شوند. برای مشاهده راهنمای آماده سازی مقالات فارسی به نشانی «راهنمای آماده سازی مقالات فارسی» (صفحه راهنمای نگارش) مراجعه شود. برای مقالات فارسی فرم خوداظهاری استفاده از هوش مصنوعی تکمیل و امضا و ارسال شود.
- هر مقاله ارسالی به کنفرانس توسط حداقل دو داور ارزیابی می شود.
- تعداد صفحات مقالات حداقل ۴ صفحه و حداکثر ۸ صفحه است (ارسال مقاله تا ۱۲ صفحه با پرداخت هزینه صفحات اضافی امکان پذیر است).
- مقالات فارسی پذیرفته شده در شماره ویژه دوفصلنامه علمی منادی افتا با نمایه ISC و مورد تأیید وزارت علوم و مقالات انگلیسی در شماره ویژه مجله بین المللی ISeCure با نمایه های WoS-JCR و SCImago-SJR منتشر خواهند شد.
- برای هر مقاله پذیرفته شده لازم است حداقل یک نویسنده در کنفرانس ثبت نام کرده و مقاله را به صورت حضوری ارائه کند.
- مقالات ارسالی نباید به طور جدی با مقالاتی که منتشر شده یا برای انتشار پذیرفته شده اند، همپوشانی داشته باشند.

مشتاقانه منتظر دریافت مقالات با کیفیت، پیشنهاد کارگاه و شرکت شما در کنفرانس هستیم!



انجمن رمز ایران
Iranian Society of Cryptology



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

زمان بندی کنفرانس

چهارشنبه ۲۹ مهرماه ۱۴۰۵ (۲۱ اکتبر ۲۰۲۶)						
ردیف	نوع نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل نشست
۱	مراسم افتتاحیه	سرود ملی و تلاوت قرآن کریم خوش آمدگویی رئیس دانشگاه (دکتر عباس سروش) سخنرانی دبیر کنفرانس، گزارش مقالات و اعلام برنامه کنفرانس (دکتر فرهاد رحمتی)		۸:۳۰	۹:۰۰	سالن اصلی (مولانا)
۲	سخنرانی کلیدی بین‌المللی	International Keynote Speaker: Dr. Reza Sohizadeh Data Governance and Data Sovereignty in a Fragmenting World Cybersecurity Director @PwC Norway	دکتر منصور باقری	۹:۰۰	۱۰:۰۰	سالن اصلی (مولانا)
۱۰:۳۰ - ۱۰:۰۰ پذیرایی و بازدید از کافه امید و اشتغال						
۳	نشست ارائه‌های امیدآفرین	ارائه‌های امید آفرین (هر کدام ۱۳ دقیقه) شرکت امن پرداز. مدیر عامل آقای مهندس عباس حسینی و سال تاسیس ۱۳۸۳ شرکت امن پردازان کویر یزد. مدیر عامل مهندس نوید نصیرزاده و سال تاسیس ۱۳۸۶ شرکت سبا پردازش. بنیان‌گذار دکتر کامبیز قادری و سال تاسیس ۱۳۷۸ شرکت تاکیان. مدیر عامل مهندس مهدی فرجی و سال تاسیس ۱۳۹۶ شرکت نآد. مدیر عامل دکتر محمود اقوامی پناه. سال تاسیس ۱۳۹۳ پارک علم و فناوری امیرکبیر	دکتر بهار فرهانی	۱۰:۳۰	۱۲:۰۰	سالن اصلی (مولانا)
۱۳:۴۰ - ۱۲:۰۰ نماز و ناهار						
۴	نشست ۱: مقالات علمی - صنعتی، امنیت سامانه‌ها و مدل‌های امنیت	سخنران مدعو: دکتر محمد مهدی احمدیان استاد پژوهشگر دانشگاه صنعتی امیرکبیر، مدیرعامل شرکت دانش‌بنیان امان و رئیس کمیسیون اتوماسیون و کنترل صنعتی سازمان نظام صنفی چالش‌ها و تهدیدات سایبری در صنایع کشور از پژوهش تا صنعت و مدیریت مهندسی سخنران مدعو: مهندس محمدرضا سپیچور (شرکت ارتباطات سیار همراه اول) اعتماد صفر در امنیت سایبری Ali Rahimi, Siavash Ahmadi, and Babak Hossein Khalaj Verifiable Vector Aggregation in Federated Learning via Rational Audit Scoring فرهاد اصفهانی‌زاده، مینا زلفی و لیلی فرزین‌نژاد ارزیابی تطبیقی وضعیت استقرار سرآیندهای امنیتی HTTP در وبسایت‌های ایرانی و آلمانی در ۱۰ حوزه کاربردی جواد مظاهری، سجاد رضایی، محسن رمضان یارندی طراحی ابزار ممیزی انطباق CIS و امتیازدهی شاخص استعداد نفوذ برای بررسی برون خط پیکربندی امنیتی ویندوز در سناریوهای پاسخ به رخداد گسترده	دکتر بهروز ترک لادانی	۱۳:۴۰	۱۵:۳۰	سالن H1 (دانشکده ریاضی و علوم کامپیوتر دانشگاه صنعتی امیرکبیر اتاق ۳۱۱)
۵	نشست ۲: هوش مصنوعی و امنیت (۱)	سخنران مدعو: دکتر مهرداد جابری (دانش‌آموخته دکتری مهندسی کامپیوتر دانشگاه اصفهان) داده‌کاوی توزیع‌شده با حفظ حریم خصوصی: مطالعه‌ی موردی تحلیل اجزای اصلی Mohsen Seddighi, Mahdi Mollazadeh, and Hamidreza Lashkarian GHOST: Gradient-guided Hierarchical Optimization for Semantic-preserving Attacks on Feature-Based ML Systems Amir Bajalan, and Masoumeh Saffkhani An Uncertainty-Aware Deep Reinforcement Learning Framework for Adaptive Malware Detection Under Concept Drift Yasamin Rahimi Sadegh, and Sajad Shirali-Shahreza Collaboration-based Privacy-Preserving Firewall for Home Networks Shakiba Nazem, Mojtaba Khalili, and Ali Fanian MARS: A Multi-Agent Framework for Cyber Range Scenario Generation, Evaluation, and Deployment	دکتر رضا ابراهیمی آتانی دکتر مجید بیات	۱۳:۴۰	۱۵:۳۰	سالن H2 (دانشکده ریاضی و علوم کامپیوتر دانشگاه صنعتی امیرکبیر اتاق ۳۱۳)

چهارشنبه ۲۹ مهرماه ۱۴۰۵ (۲۱ اکتبر ۲۰۲۶)						
ردیف	نوع نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل نشست
۶	نشست ۳: مبانی رمزنگاری (۱)	سخنران مدعو: دکتر صبا کریمانی (دانش آموخته دکتری مهندسی برق دانشگاه صنعتی شریف) رمزنگذاری جست و جویذیر شبکه بنیاد Elnaz Danayan, Atiyeh Mirzaie, Siavash Ahmadi, Shahram Khazaie, and Mohammad Reza Aref Boomerang Attack on Reduced-Round LTLBC Zahra Keshavarz Rezaei, and Mohammad Ali Verifiable Homomorphic Server-Aided Computation Outsourcing with Remote Data Integrity Checking: A Quantum-Resistant Approach پژوهشگاه توسعه فناوری‌های پیشرفته معرفی برنامه‌های هسته تخصصی رمزنگاری و پروتکل‌های امن – سناد توسعه علوم و فناوری افتا برای حمایت از دانشجویان، پژوهشگران، اساتید و صنعت	دکتر ترانه اقلیدس دکتر حسین پیل آرام	۱۳:۳۰	۱۵:۳۰	سالن H3 (دانشکده ریاضی و علوم کامپیوتر دانشگاه صنعتی امیرکبیر اتاق ۲۰۶)
۷	نشست ۴: ویژه دبیران	سخنران: محمد حسام تدین (پژوهشگاه ارتباطات و فناوری اطلاعات ایران) الزامات و رویکردهای جهانی در آموزش امنیت سایبری از ابتدایی تا پایان متوسطه		۱۳:۳۰	۱۵:۳۰	سالن H4 (سالن بهمن)
۸		نشست مرکز مدیریت راهبردی افتا با حضور رئیس و مدیران مرکز مدیریت راهبردی افتا و صاحب نظران دانشگاه و صنعت از دستگاه‌های اجرایی، سازمان‌ها و بخش خصوصی		۱۳:۳۰	۱۵:۳۰	سالن H5 (سالن فجر)
۱۶:۰۰ – ۱۵:۳۰ پذیرایی و بازدید از کافه امید و اشتغال						
۹	نشست تخصصی	نشست تخصصی امنیت اینترنت اشیا با حضور ذی‌نفعان کلیدی از دستگاه‌های اجرایی، سازمان‌ها و شرکت‌های مرتبط		۱۶:۰۰	۱۷:۳۰	سالن H4 (سالن بهمن)
۱۰	نشست تخصصی	نشست تخصصی حکمرانی امنیت در زیست‌بوم بانکی کشور با حضور ذی‌نفعان کلیدی از دستگاه‌های اجرایی، سازمان‌ها و شرکت‌های مرتبط	-	۱۶:۰۰	۱۷:۳۰	سالن اصلی (مولانا)

پنجشنبه ۳۰ مهرماه ۱۴۰۵ (۱۲ اکتبر ۲۰۲۶)						
ردیف	نوع نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل نشست
۱	نشست ۴: پیاده‌سازی الگوریتم‌های رمزنگاری و حملات مرتبط و امنیت شبکه	Ahmad Karimi, and Bijan Alizadeh GRACIA: Graph-Centrality-Guided ATPG Framework for Hardware Trojan Trigger Activation Vahid Soleimani Hesari, Iman Mirzaali Mazandarani, Sadegh Sadeghi, and Nasour Bagheri Statistical Ineffective Persistent Faults on Lilliput-TBC-II-128 and SCENERY-64/80 Sepide Sadeghi Mehr, Raziye Salarifard, and Fartash Abdul Qadir Designing Stealthy Kleptographic Backdoors in AES-256 CTR DRBG: Statistical and Machine Learning-Based Evaluation Mahdi Faraji PHALANX: A Reproducible Multi-Vendor Framework for Structural Firewall Policy Analysis and Finding Prioritization Ehsan Nokandi, Mohammad Hossein Khosravi, and Maryam Azadmanesh DualShield: Confidence-Aware Selective Escalation for Lightweight IoT Intrusion Detection and Post-Gate Novelty Analysis Behnam Amiri, and Yousef Darmani Golden Path Discovery: A Transparent, Weighted Algorithm for Prioritizing Attack Paths in Enterprise Active Directory Networks	دکتر بیژن علیزاده دکتر مرتضی امینی	۸:۳۰	۱۰:۰۰	سالن H1 (دانشکده ریاضی و علوم کامپیوتر دانشگاه صنعتی امیرکبیر اتاق ۳۱۱)
۲	نشست ۵: هوش مصنوعی و امنیت (۲)	سخنران مدعو: دکتر هانی ربیعی (دانش‌آموخته دکتری کامپیوتر - گرایش رایانش امن از دانشگاه اصفهان) مدل‌سازی و تحلیل تأثیر بات‌های شبکه‌های اجتماعی بر شکل‌دهی افکار عمومی Mohammad Heydari, Ebrahim Zarei Zefreh, and Mohsen Kiani A Latent Feature-Based Medical Image Encryption Framework Using a Convolutional Autoencoder, Latin Square, and AES Nafise Aghouee, Farhad Rahmati, and Amin Hosseingholizadeh A Review of Security and Privacy in Federated Learning: Attacks, Defenses, and Open Challenges Mohammad Zare Ahangarkolaei, Masoumeh Koochak Shoostari, and Mohammad Reza Aref CredentialBound-FL: Verifiable Account-Level Sampling Across Multiple Devices Imanimehr Fatemeh, and Hamed Ebrahimi Reconstructing Multi-Stage Attack Chains Using a Context-Enriched Cyber Security Knowledge Graph	دکتر مهدی آبادی دکتر صادق دری نوگورانی	۸:۳۰	۱۰:۰۰	سالن H2 (دانشکده ریاضی و علوم کامپیوتر دانشگاه صنعتی امیرکبیر سالن ۳۱۳)
۳		بازدید از کافه امید و اشتغال برای دانش‌آموزان		۹:۰۰	۱۰:۰۰	
۱۰:۳۰ - ۱۰:۰۰ پذیرایی و بازدید از کافه امید و اشتغال						
۴	نشست ۶: برای دانش‌آموزان دبیرستان	سخنران: دکتر محمد حسام تدین (پژوهشگاه ارتباطات و فناوری اطلاعات ایران) امنیت سایبری چیست؟ چرا باید امنیت سایبری بدانیم		۱۰:۳۰	۱۲:۰۰	سالن H5 (سالن فجر)
۵	سخنرانی کلیدی داخلی	سخنران کلیدی: دکتر علی فانیان (عضو هیئت علمی دانشگاه صنعتی اصفهان، مدیر مرکز تخصصی آپا و مسئول هسته آموزش و توانمندسازی نیروی انسانی ستاد توسعه علوم و فناوری افتا) بازطراحی آموزش امنیت سایبری: از دانش تا آمادگی عملیاتی	مهندس حبیب رستمی	۱۱:۰۰	۱۲:۰۰	سالن اصلی (مولانا)
۱۲:۰۰ - ۱۲:۳۰ نماز و ناهار و بازدید از کافه امید و اشتغال						

پنجشنبه ۳۰ مهرماه ۱۴۰۵ (۱۲ اکتبر ۲۰۲۶)						
ردیف	نوع نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل نشست
۶	نشست ۷: پروتکل‌های امنیتی	سخنران مدعو: دکتر محمد مهدی مدبری (دانش‌آموخته دکتری مهندسی برق دانشگاه صنعتی شریف) ارائه یک رویه بهبودیافته جهت حفاظت از حریم خصوصی برای نسل‌های پنجم و فراتر Sajjad Rezaei Adaryani, Hamid Mala, and Mohammad Reza Saeidi PQ-PACKA: Post-Quantum Password-based Authenticated Continuous Key Agreement سخنران مدعو: دکتر پرچهر دادخواه (دانش‌آموخته دکتری مهندسی برق دانشگاه صنعتی اصفهان) تکامل رمزنگاری بدون گواهی برای اینترنت اشیا: از طراحی‌های کارآمد تا مقاومت در برابر ابر مهاجمان سخنران مدعو: دکتر گلاره عودی قدیم (دانش‌آموخته دکتری مهندسی برق دانشگاه صنعتی اصفهان) پروتکل‌های امنیتی برای اینترنت وسایل نقلیه: چالش‌ها، راهکارها و دستاوردهای نوین	دکتر هادی شهریار شاه حسینی دکتر حمید ملا	۱۳:۳۰	۱۵:۳۰	سالن H4 (سالن بهمن)
۷	نشست ۸: هوش مصنوعی و امنیت	Armin Tavakoli, and Arash Abdi Hejrandoost VishConv: A Lightweight Hybrid Deep Learning Framework for Raw-Byte Malware Detection Maryam Azadmanesh EPF-Bench: An Extended Persian Benchmark for Fairness Evaluation in Large Language Models Morteza Taheri, Sajad Haghzad Kldibary, and Mohammad Hesam Tadayon Benchmarking Data-Level Imbalance-Handling Techniques for IoT Intrusion Detection: A Cross-Dataset Evaluation on IoT-23 and CICIDS2017 سعید محمدی چارچوبی مبتنی بر هوش تهدید سایبری برای مدل‌سازی عامل‌محور گروه‌های تهدید پیشرفته و پایدار سایبری نوظهور Seyede Marzieh Sadat Madani, Ehsan Mahdavi, and Hamid Mala The Agile Forensic Collector: Automated Forensic Evidence Recovery from Ephemeral Container Layers in Living-off-the-Land Attacks	دکتر مجید بیات - دکتر طلا تفضلی	۱۳:۳۰	۱۵:۳۰	سالن HS (سالن فجر)
۱۶:۰۰ - ۱۵:۳۰ پذیرایی و بازدید از کافه امید و اشتغال						
۸	مراسم اختتامیه	سرود ملی و تلاوت قرآن کریم گزارش برگزاری کنفرانس توسط دبیر اجرایی: دکتر امین حسینی‌زاده بیانیه پایانی و معرفی میزبان کنفرانس بیست و چهارم: مهندس رستمی سخنرانی ریاست محترم انجمن رمز ایران: دکتر محمود سلماسی زاده اعلام برگزیدگان و تقدیر از تیم اجرایی: توسط مسئول محترم دبیرخانه دائمی کنفرانس (دکتر منصور باقری)	-	۱۶:۰۰	۱۷:۳۰	سالن اصلی (مولانا)

سخنرانی‌ها

سخنرانان کلیدی



Dr. Reza Sohizadeh
Cybersecurity Director
@PwC, Norway

Title

Data Governance and Data Sovereignty in a Fragmenting World

Abstract

As AI accelerates data use, cloud dependency deepens, and geopolitical uncertainty grows, organizations face a pressing question: when sensitive data is shared across institutions, clouds and jurisdictions, who actually retains the authority and capability to govern its use?

This keynote distinguishes data governance from data sovereignty) and shows why neither is sufficient without the other. Along the way, the presentation examines: •How governance rules translate into real controls and evidence, using data classification, access policy and data loss prevention as working examples.

- Why data sovereignty has at least six distinct dimensions — legal authority, location, administrative control, cryptographic control, portability and continuity — and why most sovereignty debates focus on only one.

- How the current geopolitical landscape, including shifting transatlantic technology policy, has intensified a sovereignty debate with deeper roots.



دکتر علی فانیان

عضو هیات علمی دانشگاه صنعتی
اصفهان، مدیر مرکز تخصصی آپا و
مسئول هسته آموزش و توانمند
سازی نیروی انسانی ستاد توسعه
علوم و فناوری افتا

عنوان سخنرانی

بازطراحی آموزش امنیت سایبری، از دانش تا آمادگی عملیاتی

چکیده

یک متخصص امنیت سایبری چه زمانی برای مواجهه با رخداد‌های واقعی آماده است؟ پاسخ به این پرسش، فراتر از شناخت مفاهیم و تسلط بر ابزارها، به توانایی تصمیم‌گیری و اقدام مؤثر در شرایط ابهام، اطلاعات ناقص و فشار زمانی وابسته است. مشارکت هوش مصنوعی در تحلیل و تصمیم‌سازی امنیتی نیز ضرورت بازتعریف، پرورش و ارزیابی شایستگی نیروی انسانی را برجسته می‌کند. این سخنرانی با تکیه بر آموزش مبتنی بر شایستگی (CBT)، گذار از پوشش سرفصل‌ها و اتمام دوره‌ها به کسب و احراز شایستگی عملیاتی را بررسی می‌کند. در این رویکرد، اهداف یادگیری بر اساس وظایف مشخص در نقش‌های کاری تعریف می‌شوند و پیشرفت فراگیر، نه صرفاً با ساعت‌های حضور در کلاس، بلکه با شواهد عملکرد و تسلط اثبات‌شده در انجام این وظایف سنجیده می‌شود. برای تبیین مسیر تحقق این رویکرد، فرایند آموزش و توانمندسازی نیروی انسانی در ستاد توسعه علوم و فناوری افتای کشور و تجربه راه‌اندازی میدان سایبری شیلداپ معرفی می‌شود. در معماری آموزشی این برنامه، چارچوب NICE مبنای تعریف نقش‌های کاری، وظایف و شایستگی‌های مورد نیاز است و سرفصل‌های SANS به‌عنوان مرجع تدوین محتوای دوره‌ها به کار گرفته می‌شوند. شیلداپ با فراهم کردن بستر برگزاری دوره‌های مهارت‌محور، چالش‌های امنیتی و رزمایش‌های سایبری در محیطی شبیه‌سازی‌شده و کنترل‌شده، آموزش را به تمرین و ارزیابی عملی پیوند می‌دهد. جایگاه این بستر در تمرین تصمیم‌گیری، کار تیمی و مواجهه با سناریوهای برگرفته از مسائل واقعی نیز بررسی خواهد شد.

در ادامه، ظرفیت استفاده از هوش مصنوعی به‌عنوان دستیار تحلیل‌گر، ابزار کمک به طراحی سناریو و پشتیبان آموزشی، مورد بررسی قرار می‌گیرد. در این بخش، توانایی راستی‌آزمایی خروجی‌های هوش مصنوعی، تشخیص خطاها و محدودیت‌های آن و ارائه استدلال برای پذیرش یا رد پیشنهاد‌های ماشین، به‌عنوان بخشی از شایستگی حرفه‌ای مطرح خواهد شد؛ شایستگی‌ای که بهره‌گیری آگاهانه از ابزار را با مسئولیت‌پذیری در تصمیم‌گیری همراه می‌سازد.

در پایان، با تکیه بر این تجربه، راهکارهایی برای پیوند مؤثرتر دانشگاه، صنعت و نیازهای عملیاتی سازمان‌ها ارائه می‌شود. پیام محوری سخنرانی آن است که بازطراحی آموزش امنیت سایبری، صرفاً افزودن آزمایشگاه به دوره‌های موجود نیست؛ بلکه بازتعریف رابطه میان نیاز شغلی، محتوای آموزشی، تمرین، شواهد عملکرد و احراز شایستگی است. هدف نهایی، تربیت متخصصانی است که بتوانند در موقعیت‌های پیچیده و مبهم، مسئولانه، هوشمندانه و اثربخش عمل کنند.

کلیدواژه‌ها: آموزش امنیت سایبری، آموزش مبتنی بر شایستگی (CBT)، شایستگی عملیاتی، میدان سایبری شیلداپ، رزمایش سایبری، ارزیابی مبتنی بر عملکرد، هوش مصنوعی.

سخنرانان مدعو



دکتر مهرداد جابری

عنوان سخنرانی

داده‌کاوی توزیع‌شده با حفظ حریم خصوصی: مطالعه‌ی موردی تحلیل اجزای اصلی

چکیده

داده‌کاوی کاربردهای زیادی در زمینه‌های مختلف مانند بانکداری، بازاریابی، مراقبت‌های سلامت و کشف تقلب دارد. یکی از ابزارهای ارزشمند در داده‌کاوی، تحلیل اجزای اصلی (PCA) است. تحلیل اجزای اصلی یک روش ریاضیاتی برای تغییر فضای نمایش داده‌ها و به نوعی کاهش ابعاد داده‌ها است. محاسبه PCA بر روی داده‌های متعلق به چندین صاحب داده با توجه به حریم خصوصی آن‌ها در بسیاری از موارد مانند مراکز درمانی یک نیاز است. در نشست حاضر، با استفاده از تجزیه‌ی QR، روش جاکوبی، رمزنگاری هم‌ریخت و مبهم‌سازی پروتکل‌هایی برای محاسبه‌ی PCA با حفظ حریم خصوصی ارائه می‌شود. این پروتکل‌ها اولین طرح‌های موجود برای محاسبه‌ی امن PCA می‌باشند که هم در افراز افقی و هم در افراز عمودی قابل استفاده بوده و همچنین تمامی اجزای اصلی را محاسبه می‌کنند. لازم به ذکر است که در مقایسه با طرح‌های معرفی‌شده‌ی پیشین، طرح‌های پیشنهادی اولین طرح‌های محاسبه‌ی امن PCA در افراز عمودی هستند. در ادامه، نحوه‌ی اثبات امنیت این پروتکل‌ها با استفاده از روش دنیای ایده‌آل-دنیای واقعی و همچنین پیاده‌سازی آن‌ها در چارچوب Microsoft SEAL و بر روی داده‌های نجومی صحبت خواهد شد. در انتهای بحث، مسیرهای پیش رو و کارهای آینده در راستای این پژوهش معرفی خواهند شد.

بیوگرافی

مهرداد جابری مدرک دکتری خود را از دانشگاه اصفهان در رشته‌ی مهندسی کامپیوتر و گرایش رایانش امن در سال ۱۴۰۳ اخذ کرد و از آن پس پژوهش‌های خود را در زمینه‌های پروتکل‌های امنیتی، محاسبات امن چندسویه، بلاکچین و امنیت پساکوانتومی ادامه داده است. در کنار فعالیت‌های پژوهشی، وی در حوزه‌ی پیاده‌سازی استانداردهای بین‌المللی امنیتی در سازمان‌ها و کارخانجات صنعتی فعال بوده و همچنین به تدریس دروس امنیت اطلاعات در دانشگاه‌ها و مراکز آموزش عالی پرداخته است.

عنوان سخنرانی

پروتکل‌های امنیتی برای اینترنت وسایل نقلیه: چالش‌ها، راهکارها، و دستاوردهای نوین

دکتر گلاره عودی قدیم

چکیده

گسترش ارتباطات بی‌سیم، محاسبات سیار و اینترنت اشیاء، زمینه‌ساز شکل‌گیری اینترنت وسایل نقلیه به‌عنوان یکی از ارکان اصلی سامانه‌های حمل‌ونقل هوشمند شده است. در این محیط، تبادل گسترده و بلادرنگ اطلاعات میان وسایل نقلیه، زیرساخت‌های ارتباطی و مراکز مورد اعتماد، در کنار مزایایی همچون افزایش ایمنی و بهبود مدیریت ترافیک، چالش‌های جدی در زمینه امنیت ایجاد می‌کند. افزون بر این، محدودیت منابع محاسباتی و ارتباطی، پویایی شبکه، الزامات حریم خصوصی و حضور مهاجمان قدرتمند، چالش‌های جدی دیگری در این حوزه ایجاد می‌کنند. از این رو، طراحی پروتکل‌های احراز اصالت و توافق کلید که به‌طور هم‌زمان امنیت، حریم خصوصی، کارایی و مقیاس‌پذیری را تأمین کنند، از چالش‌های اساسی در این حوزه به شمار می‌رود. در این سخنرانی، ابتدا مهم‌ترین الزامات و چالش‌های امنیتی و حریم خصوصی در پروتکل‌های ارتباطی اینترنت وسایل نقلیه بررسی شده و آسیب‌پذیری‌های متداول در طرح‌های موجود، از جمله حملات جعل، افشای کلید نشست، افشای اسرار موقت، فرد در میان، افشای کلید بلندمدت، مورد بحث قرار می‌گیرند. سپس، رویکردهای مختلف برای طراحی پروتکل‌های بهینه و مقاوم در برابر این تهدیدها، با تمرکز بر احراز اصالت چندعاملی، حفظ گمنامی و حریم خصوصی، توافق امن کلید نشست و استفاده از فناوری‌هایی نظیر توابع فیزیکی تکثیرناپذیر، زنجیره قالب، توابع چکیده‌ساز، استخراج فازی، و رمزنگاری مبتنی بر خم بیضوی ارائه می‌شوند.

بخش دیگری از سخنرانی به دستاوردهای پژوهشی حاصل از رساله دکتری و مطالعات اخیر اختصاص خواهد داشت. در این بخش، نمونه‌هایی از تحلیل امنیتی پروتکل‌های موجود، شناسایی نقاط ضعف آن‌ها و ارائه راهکارهای بهبودیافته برای دستیابی به امنیت و کارایی بیشتر در محیط اینترنت وسایل نقلیه معرفی می‌شوند. همچنین، نقش روش‌های صوری و ابزارهایی نظیر تامارین، پرووریف، سایتر، منطق بن، و مدل پیشگوی تصادفی در ارزیابی دقیق ویژگی‌های امنیتی پروتکل‌ها بررسی خواهد شد. در نهایت، نتایج ارزیابی‌های محاسباتی و شبیه‌سازی شبکه با استفاده از شبیه‌ساز NS-3 نشان می‌دهد که می‌توان با طراحی مناسب، میان الزامات امنیتی، حفظ حریم خصوصی، سربر محاسباتی و مخابراتی، و مقیاس‌پذیری در سامانه‌های اینترنت وسایل نقلیه توازن مطلوبی برقرار کرد.

بیوگرافی

گلاره عودی قدیم دانش‌آموخته دکتری مهندسی برق- مخابرات- سیستم از دانشگاه صنعتی اصفهان است. ایشان در سال ۲۰۱۵ مدرک کارشناسی مهندسی برق- مخابرات را از دانشگاه سیستان و بلوچستان و در سال ۲۰۱۸ مدرک کارشناسی ارشد مهندسی برق- مخابرات امن و رمزنگاری را از دانشگاه شهید بهشتی دریافت کردند و در سال ۲۰۲۵ موفق به اخذ مدرک دکتری مهندسی برق- مخابرات- سیستم از دانشگاه صنعتی اصفهان شدند. زمینه‌های پژوهشی ایشان شامل رمزنگاری، زنجیره قالب، اینترنت اشیاء، امنیت شبکه، تحلیل و طراحی پروتکل‌های احراز اصالت و توافق کلید، و امنیت سامانه‌های ارتباطی است. ایشان در پژوهش‌های خود از مدل‌ها و ابزارهای تحلیل صوری و همچنین شبیه‌سازها، از جمله تامارین، پرووریف، سایتر، منطق بن، مدل پیشگوی تصادفی، و شبیه‌ساز NS-3، استفاده کرده‌اند.



دکتر هانی ربیعی

عنوان سخنرانی

مدل سازی و تحلیل تأثیر بات های شبکه های اجتماعی بر شکل دهی افکار عمومی

چکیده

در این پژوهش، یک مدل پیوست ترجیحی همسان گرای جهت دار (DHPA) به عنوان زیرساخت مدل سازی اجزای شبکه اجتماعی، از جمله موجودیت های مصنوعی، ارائه شده است. این مدل قابلیت ایجاد و بازتنظیم اتصالات در شبکه اجتماعی را داشته و همزمان پویایی نگرش ها را با در نظر گرفتن ویژگی های کاربران، مانند تمایل به بیان نظر و گرایش به ایجاد رابطه با دیگران، مد نظر قرار می دهد. در مدل پیشنهادی، کاربران مصنوعی به عنوان نوع خاصی از کاربران با ویژگی های قابل تنظیم در کنار کاربران انسانی در نظر گرفته می شوند. علاوه بر این، تمایل به همسان گرایی در کاربران و اثر آن در شکل گیری پدیده های اجتماعی مانند اجماع یا قطبیت در افکار عمومی نیز در مدل دیده شده است. ترکیب این ویژگی ها منجر به نتایج واقعی تری در مقایسه با مدل های مشابه می شود.

در ارزیابی ها نشان داده شده است که ویژگی های شبکه اجتماعی تولید شده توسط مدل (DHPA)، مانند توزیع درجه قانون توانی و خاصیت کوچک جهان، به خوبی با شبکه های اجتماعی واقعی مطابقت دارد. این مدل می تواند به تحلیل شرایط مختلف برای رسیدن به انواع حالت های نهایی افکار عمومی مانند اجماع، قطبیت یا واگرایی کمک کند. به طور خاص، با استفاده از این مدل، نحوه و میزان تأثیر گذاری کاربران مصنوعی بررسی و عوامل مؤثر در شکل دهی افکار عمومی توسط آن ها تحلیل شده است. نتایج نشان می دهد که ویژگی های مختلف کاربران مصنوعی، از جمله نحوه اتصال آن ها به کاربران انسانی، سطح هوش و طول عمر آن ها، چگونه بر شکل دهی افکار عمومی تأثیر می گذارند. همچنین با تحلیل سناریوهای مختلف مشخص شد که ویژگی ها، میزان و نحوه حضور کاربران مصنوعی تا چه اندازه در ایجاد پدیده های اجتماعی مانند اجماع یا قطبیت مؤثر هستند. با درک عوامل مؤثر بر موفقیت کاربران مصنوعی، سیاست گذاران، بسترهای شبکه های اجتماعی، سازمان های حاکمیتی و شرکت ها می توانند آن ها را مؤثرتر مدیریت کنند.

بیوگرافی

هانی ربیعی کارشناسی ارشد خود را در رشته مهندسی فناوری اطلاعات - امنیت اطلاعات از دانشگاه صنعتی مالک اشتر تهران و کارشناسی را در مهندسی کامپیوتر - نرم افزار از دانشگاه مازندران دریافت کرده است. پایان نامه دکتری او با عنوان «مدل سازی و تحلیل تأثیر بات های شبکه اجتماعی بر شکل دهی افکار عمومی» بر پویایی شبکه های اجتماعی، مدل سازی افکار عمومی، موجودیت های مصنوعی و مدل سازی عامل بنا متمرکز است. زمینه های پژوهشی او شامل تحلیل شبکه های اجتماعی، بات های اجتماعی، امنیت نرم، پویایی نظرات و شبکه اجتماعی است. از سوابق علمی او می توان به انتشار مقالاتی در نشریه های معتبر بین المللی اشاره کرد. همچنین سابقه همکاری در حوزه های مختلف امنیت اطلاعات در زیرساخت های کشور دارد.



**Dr. Kasa
Abbaszadeh**

University of Maryland,
College Park

Title

Single-Server Private Outsourcing of zk-SNARKs

Abstract

Succinct zero-knowledge arguments (zk-SNARKs) enable a prover to convince a verifier of the truth of a statement via a succinct, efficiently verifiable proof without revealing any additional information about the witness. A barrier to the practical deployment of zk-SNARKs is their high proving cost. With this motivation, we study server-aided zk-SNARKs, where a client/prover outsources most of its work to a single, untrusted server, while the server learns nothing about the witness, the statement, or even the proof. We formalize this notion and show how to efficiently realize server-aided proving for widely deployed zk-SNARKs such as Nova, Groth16, and Plonk.

The key building block underlying our designs is a new primitive, encrypted multi-scalar multiplication (EMSM), which enables private delegation of multi-scalar multiplications (MSMs).

We construct an EMSM from variants of the LPN assumption in which the client does $O(1)$ group operations, while the server's work matches that of the native plaintext MSM.

We implement and evaluate our constructions. Compared to local proving, our techniques lower the client's computation by up to $18\times$ and reduce the proving latency by up to $8\times$.

Biography

Kasa Abbaszadeh earned his Ph.D. in Computer Science from the University of Maryland, College Park, where he was advised by Prof. Jonathan Katz. His research spans applied cryptography and computer security, with a recent focus on cryptographic proof systems and their applications to privacy and verifiability in information systems. During his doctoral studies, he was a Student Researcher in the Private Computing group at Google. He holds a B.Sc. in Electrical Engineering from Sharif University of Technology.



دکتر پریچهر دادخواه

عنوان سخنرانی

تکامل رمزنگاری بدون گواهی برای اینترنت اشیا: از طراحی‌های کارآمد تا مقاومت در برابر ابرمهاجمان

چکیده

با گسترش اینترنت اشیا (IoT) و افزایش استفاده از تجهیزات هوشمند در حوزه‌هایی نظیر سلامت دیجیتال، خانه هوشمند، حمل‌ونقل و شهر هوشمند، تأمین امنیت و محرمانگی تبادل اطلاعات در این شبکه‌ها به یکی از چالش‌های اساسی تبدیل شده است. محدودیت منابع محاسباتی، حافظه و انرژی در بسیاری از تجهیزات IoT، استفاده از روش‌های رمزنگاری با سربار محاسباتی بالا را با محدودیت مواجه می‌سازد. در این میان، رمزنگاری کلید عمومی مبتنی بر منحنی‌های بیضوی (ECC) به دلیل فراهم‌سازی سطح امنیتی مناسب با کلیدهای کوتاه‌تر، گزینه‌ای مناسب برای محیط‌های محدود از نظر منابع محسوب می‌شود. همچنین، رمزنگاری بدون گواهی (Certificateless Cryptography) با حذف نیاز به مدیریت گواهی‌های دیجیتال و در عین حال جلوگیری از مشکل کلیدگذاری امانی، می‌تواند راهکاری مناسب برای تأمین امنیت ارتباطات در شبکه‌های IoT باشد. زمینه اصلی فعالیت‌های پژوهشی اینجانب در حوزه رمزنگاری کلید عمومی و به‌ویژه رمزنگاری بدون گواهی قرار دارد و بخشی از این فعالیت‌ها به طراحی، تحلیل امنیتی و بهبود طرح‌های رمزنگاری و رمزآمضا، با تمرکز بر کاربرد آن‌ها در اینترنت اشیا و شبکه‌های بی‌سیم با منابع محدود اختصاص یافته است. در این مطالعات، ویژگی‌های امنیتی و کارایی طرح‌های مختلف، از جمله مقاومت در برابر حملات شناخته‌شده، پیچیدگی محاسباتی و ارتباطی و میزان مصرف منابع مورد بررسی قرار گرفته و تلاش شده است با بهره‌گیری از روش‌های مبتنی بر منحنی‌های بیضوی و مدل‌های امنیتی متداول، راهکارهایی امن‌تر و کارآمدتر برای محیط‌های محدود ارائه شود. این حوزه پژوهشی همچنین شامل بررسی و تحلیل آسیب‌پذیری‌های طرح‌های موجود و ارائه بهبودهایی با هدف افزایش سطح امنیت و کارایی آن‌ها است.

بیوگرافی

پریچهر دادخواه در سال‌های ۲۰۱۳ و ۲۰۱۷ به ترتیب موفق به دریافت مدارک کارشناسی و کارشناسی ارشد مهندسی برق با گرایش سیستم‌های مخابراتی از دانشگاه صنعتی اصفهان شد. وی در سال ۲۰۲۵ مدرک دکتری مهندسی برق خود را از دانشگاه صنعتی اصفهان دریافت کرد. ایشان در حال حاضر در زمینه تدریس و فعالیت‌های پژوهشی دانشگاهی در حوزه مخابرات و امنیت اطلاعات فعالیت دارد. زمینه‌های پژوهشی وی شامل رمزنگاری کلید عمومی، رمزنگاری بدون گواهی، امضای دیجیتال، رمزآمضا و امنیت رمزنگاری در شبکه‌های اینترنت اشیا و شبکه‌های بی‌سیم با منابع محدود است و تمرکز اصلی پژوهش‌های وی بر طراحی، تحلیل امنیتی و بهبود کارایی طرح‌های رمزنگاری بدون گواهی قرار دارد.



دکتر محمد مهدی مدیری

عنوان سخنرانی

ارائه یک رویه بهبودیافته جهت حفاظت از حریم خصوصی برای نسل های پنجم و فراتر

چکیده

امروزه با گسترش شبکه‌های نسل پنجم و فراتر (5G/6G) و افزایش چشمگیر افزاره‌های ناهمگن، تأمین امنیت و حفظ حریم خصوصی در سه حوزه «داده»، «شناسه» و «موقعیت» به یکی از چالش‌های مهم معماری‌های 3GPP تبدیل شده است. در این ارائه، رویه‌ای جامع با هدف ارتقای حریم خصوصی ارائه شده که در آن برای حفاظت از داده‌ها، ساختاری نوین برای احراز اصالت و توافق کلید بر پایه پروتکل‌های 5G AKA و EAP-AKA معرفی می‌شود و برای دستیابی به حریم شناسه-موقعیت، از نسخه‌ی بهبودیافته‌ی شناسه مخفی (SUCI) استفاده می‌گردد. امنیت این ساختار با روش‌های اثبات‌پذیر تحلیل شده و نشان داده شده است که رویه پیشنهادی در برابر انواع حملات نظیر فرد-در-میان، جعل هویت و سرقت شناسه مقاوم بوده و با تأمین الزامات مهمی همچون احراز اصالت دوسویه، رازمانی پیش‌سو و پس‌سو و پیوندناپذیری، الزامات امنیتی مطرح را برآورده می‌کند. در نهایت، ارزیابی‌ها مؤید آن است که این رویه ضمن ارتقای امنیت، نسبت به پروتکل‌های موجود در استاندارد 3GPP، از سربارهای محاسباتی، ارتباطی و ذخیره‌سازی بهینه‌تری برخوردار است.

بیوگرافی

محمد مهدی مدیری دارای مدرک دکتری و کارشناسی ارشد مهندسی برق (گرایش سیستم) از دانشگاه صنعتی شریف و کارشناسی از دانشگاه تهران، با تمرکز ویژه بر معماری امنیتی شبکه‌های نسل پنجم و فراتر (5G/6G) هستند. همچنین، در تحلیل پروتکل‌های استاندارد 3GPP، رمزنگاری و امنیت اثبات‌پذیر، با ترکیب سوابق پژوهشی آکادمیک و تجربه عملیاتی در محیط‌های زیرساختی مانند Rightel CT، در زمینه‌های تحلیل امنیت سیگنالینگ، ارزیابی ریسک و طراحی پروتکل‌های محافظت از حریم خصوصی (داده، شناسه و موقعیت) صاحب‌نظر بوده و توانمندی بالایی در حل مسائل پیچیده مخابراتی با رویکردی نوآورانه و کاربردی دارند.



دکتر صبا کریمانی

عنوان سخنرانی

رمزگذاری جستجوپذیر شبکه‌بنیاد

چکیده

با گسترش استفاده از فضای ابری برای ذخیره‌سازی داده‌ها، ایجاد توازن میان حفظ محرمانگی اطلاعات و امکان جستجو بر روی داده‌های برون سپاری شده به یکی از چالش‌های اساسی امنیت تبدیل شده است. در این راستا، طرح‌های رمزگذاری جستجوپذیر مطرح شده‌اند که به دو دسته متقارن و نامتقارن تقسیم می‌شوند. در طرح‌های رمزگذاری جستجوپذیر متقارن، اشتراک کلید میان مالک داده و کاربر مستلزم برقراری تعامل برخط میان طرفین است. به منظور رفع این محدودیت، طرح‌های رمزگذاری جستجوپذیر کلید عمومی معرفی شده‌اند. در این طرح‌ها، مالک داده کلمات کلیدی مورد نظر را با استفاده از کلید عمومی کاربر به صورت جستجوپذیر رمزگذاری می‌کند؛ به گونه‌ای که تنها کاربر دارنده کلید خصوصی متناظر قادر به انجام فرایند جستجو باشد. با این حال، در صورت واگذاری عملیات جستجو به یک کارساز ابری غیرقابل اعتماد، اطمینان از صحت نتایج بازگردانده شده نیز اهمیت می‌یابد. از این رو، برای تأیید صحت نتایج جستجو، لازم است ویژگی واریسی‌پذیری در چنین سامانه‌هایی فراهم شود. همچنین، با ظهور رایانش کوانتومی و تهدید آن برای رمزنگاری کلاسیک، رمزنگاری شبکه‌بنیاد مبتنی بر مسائل سختی نظیر یادگیری با خطا و گونه‌های ساختاریافته آن، به عنوان رویکردی مناسب در رمزنگاری پساکوانتومی مورد توجه قرار گرفته است. در این ارائه، دو طرح رمزگذاری جستجوپذیر نامتقارن مبتنی بر مسائل سخت شبکه معرفی می‌شوند که با هدف تأمین امنیت پساکوانتومی و فراهم کردن مجموعه‌ای از ویژگی‌های امنیتی و کارکردی طراحی شده‌اند. این طرح‌ها از قابلیت‌هایی نظیر واریسی‌پذیری، کامل بودن نتایج جستجو، مقاومت در برابر حملات کلمه کلیدی منتخب و حدس کلمه کلیدی توسط مهاجم داخلی برخوردارند.

بیوگرافی

صبا کریمانی دانش‌آموخته مقاطع کارشناسی، کارشناسی ارشد و دکتری مهندسی برق از دانشگاه صنعتی شریف است. زمینه‌های پژوهشی وی شامل رمزنگاری پساکوانتومی، به ویژه رمزنگاری شبکه‌بنیاد، رمزگذاری جستجوپذیر، تسهیم راز و تحلیل حملات کوانتومی علیه سامانه‌های رمزنگاری است.



دکتر محمد مهدی احمدیان

عنوان سخنرانی

چالش‌ها و تهدیدات سایبری در صنایع کشور (از پژوهش تا صنعت، از مدیریت تا مهندسی)

چکیده

در یک دهه اخیر، امنیت سایبری سیستم‌های کنترل و اتوماسیون صنعتی به دلیل به کارگیری وسیع در زیرساخت‌های حساس، حیاتی و مهم دنیا، حرکت صنایع به سمت تحول دیجیتال و سوءاستفاده مهاجمین و پیاده‌سازی حملات مبتنی بر APT، به حدی پراهمیت شده که به عنوان یک دغدغه مهم بین‌المللی عنوان گردیده است. سامانه‌های دوقلوی دیجیتال (Digital Twin)، سیستم‌های اجرایی تولید (MES)، اینترنت اشیا صنعتی (IIoT)، پایش وضعیت (CM)، تحلیل پیشرفته و هوش مصنوعی از نمونه‌های مصادیق تحول دیجیتال در صنایع هستند که در صورت طراحی و پیاده‌سازی امن، بهره‌وری، قابلیت اطمینان، ایمنی، مصرف انرژی و پایداری را می‌توانند بهبود دهند. در یک دهه اخیر، این موضوع به یکی از حوزه‌های قابل توجه و جذاب پژوهشگران امنیت و مهاجمین سایبری تبدیل شده است. به دلایل متعدد از جمله طولانی بودن چرخه عمر محصولات، مسائل مدیریتی و فنی در صنایعی نظیر برق، فولاد، نفت، آب، گاز، پالایش، پتروشیمی، سنگ آهن، مس و ... روند انتقال دستاوردهای پژوهشی، از مرحله تحقیق و پژوهش، به مراحل مهندسی و طراحی، ساخت نمونه‌های اولیه، تولید انبوه و بهره‌برداری در زیرساخت‌ها، با چالش‌هایی روبه‌رو بوده است. متأسفانه صنایع و زیرساخت‌های صنعتی مختلف در کشور به دلیل اهمیت بسیار بالای خود از منظر امنیت ملی یا شاخص‌های اقتصادی، از حملات و رخدادهای سایبری بی‌بهره نبوده‌اند. در این سخنرانی تلاش خواهد شد به نمونه‌ای از چالش‌ها و تهدیدات سایبری پرداخته شود. اهم این موارد به اجمال در دو حوزه چالش‌های مدیریتی و فنی-مهندسی تشریح خواهند شد.

بیوگرافی

دکتر محمد مهدی احمدیان مشاور، سخنران، مدرس و مجری حوزه امنیت سیستم‌های کنترل صنعتی (ICS) و زیرساخت‌های حیاتی است که تحصیلات کارشناسی خود را در رشته مهندسی کامپیوتر (گرایش نرم‌افزار) و سپس کارشناسی ارشد خود را در رشته فناوری اطلاعات (گرایش امنیت اطلاعات) پشت سر گذاشت و مدرک دکتری تخصصی رشته فناوری اطلاعات (گرایش امنیت اطلاعات) را از دانشگاه صنعتی امیرکبیر و با رساله‌ای در حوزه امنیت صنعتی که به عنوان رساله برتر کشور از سوی وزارت علوم برگزیده شد، دریافت کرده است. وی در حال حاضر استاد پژوهشگر همکار دانشگاه صنعتی امیرکبیر (مرکز آپا)، مدیرعامل شرکت دانش‌بنیان امان (پیشگامان امن آرمان) و رئیس کمیسیون اتوماسیون و کنترل صنعتی سازمان نظام صنفی رایانه‌ای کشور (استان تهران) است که تجربه تدریس و مشاوره در بسیاری از صنایع کشور از جمله وزارت نیرو و شرکت‌های مربوطه، شرکت ملی نفت، مجتمع‌های مس کشور، شرکت‌های فولادی کشور، نیروگاه‌های حرارتی کشور و غیره را داراست. وی بالغ بر ۱۲ سال است که در پروژه‌های متعدد امنیت سایبری در حوزه‌های کنترل صنعتی و زیرساخت‌های حیاتی در سطوح مختلف کشوری و در رده‌های گوناگون (مشاوره، نظارت، آموزش، مدیریت، طراحی، اجرا و غیره) فعالیت داشته است.

دکتر احمدیان سابقه طولانی در حوزه آموزش تخصصی امنیت سایبری OT، با بالغ بر ۴۵۰۰۰ نفر/ساعت تدریس، را در کارنامه خود دارد و بنیان‌گذار درس امنیت سایبری صنعتی در دانشگاه صنعتی امیرکبیر است.



عنوان سخنرانی

اعتماد صفر در امنیت سایبری

مهندس محمدرضا سمیع‌پور
شرکت ارتباطات سیار همراه اول

چکیده

در یک شبکه اپراتوری، چه زمانی می‌توان به یک تجهیز، سرویس، کاربر یا ارتباط اعتماد کرد؟ و مهم‌تر از آن، چه چیزی مشخص می‌کند که این اعتماد باید ادامه پیدا کند یا مورد بازنگری قرار گیرد؟ با گسترش سرویس‌ها، تجهیزات، کاربران، دسترسی‌ها و ارتباطات میان اجزای شبکه، دیگر نمی‌توان اعتماد را صرفاً بر اساس محل قرارگیری یک موجودیت در شبکه یا عبور موفق آن از یک نقطه کنترل در نظر گرفت. یک موجودیت ممکن است امروز در شرایط قابل قبول قرار داشته باشد، اما با تغییر وضعیت، سطح دسترسی، شرایط عملیاتی یا سطح ریسک، فردا به کنترل و نظارت متفاوتی نیاز داشته باشد. از این منظر، اعتماد صفر در امنیت دیجیتال را می‌توان نه صرفاً به‌عنوان حذف اعتماد، بلکه به‌عنوان تغییری در نحوه مدیریت، ارزیابی و بازنگری اعتماد در نظر گرفت.

این ارائه با تکیه بر تجربه عملیاتی در حوزه امنیت شبکه‌های اپراتوری، به این سؤال می‌پردازد که چگونه می‌توان اعتماد را از یک فرض ثابت به یک تصمیم امنیتی قابل ارزیابی و قابل مدیریت تبدیل کرد. در این رویکرد، زنجیره‌ای عملیاتی میان نقطه اعتماد، سطح اعتماد، ریسک، نیازمندی امنیتی، قابلیت امنیتی، کنترل و پایش شکل می‌گیرد. هدف، اجرای یکباره مجموعه‌ای از کنترل‌های اعتماد صفر نیست؛ بلکه شناخت نقاطی است که نیازمند بازنگری اعتماد هستند، شناسایی شکاف‌های امنیتی، تعیین قابلیت‌های موردنیاز و اولویت‌بندی اقدامات بر اساس شرایط واقعی شبکه.

خروجی ارائه، چارچوبی عملی برای وارد کردن اصول اعتماد صفر به چرخه مدیریت امنیت شبکه‌های اپراتوری است؛ رویکردی که در آن اعتماد یک وضعیت ثابت نیست، بلکه تصمیمی است که باید متناسب با ریسک و وضعیت امنیتی، به‌صورت مستمر ارزیابی و در صورت نیاز بازنگری شود.

نمایه مقالات

شناسه مقاله	عنوان مقاله	نویسندگان	مؤسسه/دانشگاه (نویسندگان)	محور مقاله	زبان مقاله
۱۰۲۴	An Uncertainty-Aware Deep Reinforcement Learning Framework for Adaptive Malware Detection Under Concept Drift	Amir Bajalan – Masoumeh Safkhani	دانشگاه تربیت دبیر شهید رجایی – دانشکده تربیت دبیر شهید رجایی	امنیت و حریم خصوصی هوش مصنوعی	انگلیسی
۱۰۹۱	Statistical Ineffective Persistent Faults on Lilliput-TBC-II-128 and SCENERY-64/80	Vahid Soleimani Hesari – Iman Mirzaali Mazandarani – Sadegh Sadeghi – Nasour Bagheri	Shahid Beheshti University – Tarbiat Modares University – Institute for Advanced Studies in Basic Sciences (IASBS) – Shahid Rajaei Teacher Training University	دستکاری سختافزار و روش‌های مقابله با آن	انگلیسی
۱۰۳۷	Boomerang Attack on Reduced-Round LTLBC	Elnaz Danayan – Atiyeh Mirzaie – Siavash Ahmadi – Shahram Khazaie – Mohammad Reza Aref	Department of Mathematical Sciences, Sharif University of Technology, Tehran, Iran – Information Systems and Security Lab (ISSL), Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran – Electronics Research Institute, Sharif University of Technology, Tehran, Iran	الگوریتم‌های رمزنگاری متقارن	انگلیسی
۱۰۸۸	Designing Stealthy Kleptographic Backdoors in AES-256 CTR DRBG: Statistical and Machine Learning-Based Evaluation	Sepide Sadeghi Mehr – Raziye Salarifard – Fartash Abdul Qadir	دانشگاه شهید بهشتی – دانشگاه شهید بهشتی	پایاده‌سازی نرم‌افزاری و سخت‌افزاری الگوریتم‌های رمزنگاری	انگلیسی
۱۰۶۲	GRACIA: Graph-Centrality-Guided ATPG Framework for Hardware Trojan Trigger Activation	Ahmad Karimi – Bijan Alizadeh	دانشگاه تهران – دانشگاه تهران	دستکاری سختافزار و روش‌های مقابله با آن	انگلیسی
۱۰۶۷	PQ-PACKA: Post-Quantum Password-based Authenticated Continuous Key Agreement	Sajjad Rezaei Adaryani – Hamid Mala – Mohammad Reza Saeidi	دانشگاه اصفهان – دانشگاه اصفهان	طراحی پروتکل‌های امنیتی جدید	انگلیسی
۱۰۶۴	طراحی ابزار ممیزی انطباق CIS و امتیازدهی شاخص استعداد نفوذ برای بررسی برون‌خط پیکربندی امنیتی ویندوز در سناریوهای پاسخ به رخداد گسترده	جواد مظاهری – سجاد رضایی – محسن رمضان یارندی	دانشگاه صنعتی اصفهان – انجمن رمز ایران	مقالات کوتاه علمی و صنعتی	فارسی
۱۰۹۶	GHOST: Gradient-guided Hierarchical Optimization for Semantic-preserving Attacks on Feature-Based ML Systems	Mohsen Seddighi – Mahdi Mollazadeh – Hamidreza Lashkarian	دانشگاه جامع امام حسین (ع) – دانشگاه جامع امام حسین (ع) – دانشگاه جامع امام حسین (ع)	یادگیری ماشین خصمانه	انگلیسی
۱۰۳۱	PHALANX: A Reproducible Multi-Vendor Framework for Structural Firewall Policy Analysis and Finding Prioritization	Mahdi Faraji	Takian Co.	امنیت زیرساخت شبکه	انگلیسی
۱۰۴۷	The Agile Forensic Collector: Automated Forensic Evidence Recovery from Ephemeral Container Layers in Living-off-the-Land Attacks	Seyede Marzieh Sadat Madani – Ehsan Mahdavi – Hamid Mala	University of Isfahan – University of Isfahan – University of Isfahan	روش‌ها و ابزارهای جرم‌یابی دیجیتال	انگلیسی
۱۰۶۵	EPF-Bench: An Extended Persian Benchmark for Fairness Evaluation in Large Language Models	Maryam Azadmanesh	دانشگاه بیرجند	امنیت و حریم خصوصی هوش مصنوعی	انگلیسی

شناسه مقاله	عنوان مقاله	نویسندگان	مؤسسه/دانشگاه (نویسندگان)	محرور مقاله	زبان مقاله
۱۱۰۱	Verifiable Vector Aggregation in Federated Learning via Rational Audit Scoring	Ali Rahimi – Siavash Ahmadi – Babak Hossein Khalaj	دانشگاه صنعتی شریف – دانشگاه صنعتی شریف – دانشگاه صنعتی شریف	روش‌ها و مدل‌های صوری	انگلیسی
۱۰۵۵	MARS: A Multi-Agent Framework for Cyber Range Scenario Generation, Evaluation, and Deployment	Shakiba Nazem – Mojtaba Khalili – Ali Fanian	دانشگاه صنعتی اصفهان – دانشگاه صنعتی اصفهان – دانشگاه صنعتی اصفهان	امنیت و حریم خصوصی هوش مصنوعی	انگلیسی
۱۰۰۸	Collaboration-based Privacy-Preserving Firewall for Home Networks	Yasamin Rahimi Sadegh – Sajad Shiralil-Shahreza	دانشگاه صنعتی امیرکبیر – دانشگاه صنعتی امیرکبیر	امنیت و حریم خصوصی هوش مصنوعی	انگلیسی
۱۰۳۳	چارچوبی مبتنی بر هوش تهدید سایبری برای مدلسازی عامل‌محور گروه‌های تهدید پیشرفته و پایدار سایبری نوظهور	سعید محمدی	دانشگاه جامع امام حسین (ع)	تحلیل و مدلسازی تهدید	فارسی
۱۰۸۰	ارزیابی تطبیقی وضعیت استقرار سرآیندهای امنیتی HTTP در وب‌سایت‌های ایرانی و آلمانی در ۱۰ حوزه‌ی کاربردی	فرهاد اصفهانی‌زاده – مینا زلفی – لیلی فرزین‌نوش	دانشگاه تبریز – دانشگاه تبریز – دانشگاه تبریز	امنیت وب	فارسی
۱۰۴۳	Verifiable Homomorphic Server-Aided Computation Outsourcing with Remote Data Integrity Checking: A Quantum-Resistant Approach	Zahra Keshavarz Rezaei – Mohammad Ali	دانشگاه صنعتی امیرکبیر – دانشگاه صنعتی امیرکبیر	الگوریتم‌های رمزنگاری نامتقارن و امضاهای رقمی	انگلیسی
۱۰۲۲	A Latent Feature-Based Medical Image Encryption Framework Using a Convolutional Autoencoder, Latin Square, and AES	Mohammad Heydari – Ebrahim Zarei Zefreh – Mohsen Kiani	University of Isfahan – University of Isfahan – University of Isfahan	امنیت و حریم خصوصی هوش مصنوعی	انگلیسی
۱۰۴۰	A Review of Security and Privacy in Federated Learning Attacks, Defenses, and Open Challenges	Nafise Aghouee – Farhad Rahmati – Amin Hosseingholizadeh	دانشگاه صنعتی امیرکبیر – دانشگاه صنعتی امیرکبیر	امنیت و حریم خصوصی هوش مصنوعی	انگلیسی
۱۰۷۳	CredentialBound-FL: Verifiable Account-Level Sampling Across Multiple Devices	Mohammad Zare Ahangarkolaei – Masoumeh Koochak Shoostari – Mohammad Reza Aref	دانشگاه صنعتی شریف – دانشگاه صنعتی شریف – دانشگاه صنعتی شریف	امنیت و حریم خصوصی هوش مصنوعی	انگلیسی
۱۰۷۵	DualShield: Confidence-Aware Selective Escalation for Lightweight IoT Intrusion Detection and Post-Gate Novelty Analysis	Ehsan Nokandi – Mohammad Hossein Khosravi – Maryam Azadmanesh	دانشگاه بیرجند – دانشگاه بیرجند – دانشگاه بیرجند	تشخیص و جلوگیری از نفوذ به شبکه	انگلیسی
۱۰۶۶	Golden Path Discovery: A Transparent, Weighted Algorithm for Prioritizing Attack Paths in Enterprise Active Directory Networks	Behnam Amiri – Yousef Darmani	دانشگاه صنعتی خواجه نصیرالدین طوسی – دانشگاه صنعتی خواجه نصیرالدین طوسی	امنیت زیرساخت شبکه	انگلیسی
۱۰۱۷	Reconstructing Multi-Stage Attack Chains Using a Context-Enriched Cyber Security Knowledge Graph	Imanimehr Fatemeh – Hamed Ebrahimi	ICT Research Institute (ITRC) – ICT Research Institute (ITRC)	تحلیل و مدلسازی تهدید	انگلیسی
۱۰۰۷	VishConv: A Lightweight Hybrid Deep Learning Framework for Raw-Byte Malware Detection	Armin Tavakoli – Arash Abdi Hejrandoust	Amnnpardaz Software Corporation – Iran University of Science and Technology	امنیت و حریم خصوصی هوش مصنوعی	انگلیسی
۱۰۳۹	Benchmarking Data-Level Imbalance-Handling Techniques for IoT Intrusion Detection: A Cross-Dataset Evaluation on IoT-23 and CICIDS2017	Morteza Taheri – Sajad Haghzad Klidbary – Mohammad Hesam Tadayon	دانشگاه زنجان – دانشگاه زنجان – پژوهشگاه ارتباطات و فناوری اطلاعات	امنیت و حریم خصوصی هوش مصنوعی	انگلیسی

An Uncertainty-Aware Deep Reinforcement Learning Framework for Adaptive Malware Detection Under Concept Drift

Amir Bajalan, Masoumeh Safkhani

Shahid Rajaee Teacher Training University

Abstract: Evasive, rapidly drifting malware challenges classifiers that must output a definitive label regardless of confidence, causing severe performance loss and escalating decision costs in non-stationary environments. We propose an adaptive deep reinforcement learning framework that couples dynamic multi-objective reward weighting with an uncertainty-aware reject option, replacing the static reward topologies of prior Reinforcement Learning (RL) detectors. An Adaptive Meta-Controller continuously recalibrates the trade-off among detection accuracy, reject quality, and decision cost, while an adaptive confidence threshold and dynamically scaled temperature govern exploration-exploitation and let the agent abstain from classifying highly ambiguous samples. Robustness is evaluated under a strict chronological train-test protocol on EMBER, BODMAS, and KronoDroid. The proposed method consistently outperforms static-reward RL policies and a supervised deep learning baseline in Accuracy, F1-score, and Matthews Correlation Coefficient (MCC), reaching 99.50% Accuracy, 99.52% F1-score, and 99.00% MCC on BODMAS, and 97.20% F1-score with 93.68% MCC under the severe temporal drift of EMBER 2018—a 5.30-point F1 gain over the strongest RL baseline in that regime. By jointly optimizing sample-adaptive abstention and classification under realistic drift, the framework attains its best performance on BODMAS while sustaining resilience across all three benchmarks, establishing a practical paradigm for automated, uncertainty-aware malware triage.

Keywords: Cybersecurity, Malware Detection, Deep Reinforcement Learning, Selective Classification, Multi-Objective Optimization, Adaptive Learning

Statistical Ineffective Persistent Faults on Lilliput-TBC-II-128 and SCENERY-64/80

Vahid Soleimani Hesari¹, Iman Mirzaali Mazandarani², Sadegh Sadeghi³, Nasour Bagheri⁴
¹Shahid Beheshti University - ²Tarbiat Modares University - ³Institute for Advanced Studies in Basic Sciences (IASBS) - ⁴Shahid Rajaei Teacher Training University

Abstract: This paper applies Statistical Ineffective Persistent Faults Analysis (SIPFA) to the 32-round Lilliput-TBC-II-128 v1.1 and the 28-round SCENERY-64/80 under four settings combining known or unknown persistent faults with detection- or infection-based countermeasure models. In the fixed software experiments on Lilliput-TBC-II-128, one corrupted entry of the shared 8-bit S-box biases all eight lanes. The complete final-round tweakey is recovered in all four settings, while the known-fault detection and unknown-fault infection settings also recover the penultimate-round tweakey. These two tweakeys define a rank-128 linear system whose unique solution is the 128-bit master key. In SCENERY-64/80, eight lane-specific runs recover the complete 32-bit final-round subkey in each known-fault setting. In the unknown-fault settings, evaluating 2^{20} active-subkey hypotheses identifies the fault location and input and recovers 18 of the 20 active subkey bits. The remaining four hypotheses form a structural equivalence class under the reconstructed variable and the statistical observations considered. The SCENERY results are further evaluated over 100 independent trials. All experiments use a software-based single-entry persistent S-box fault model without missed injections, multiple faults, or observation noise.

Keywords: Statistical Ineffective Persistent Fault Analysis, Persistent Fault Analysis, Feistel Ciphers, Lightweight Cryptography, Key Recovery

Boomerang Attack on Reduced-Round LTLBC

Elnaz Danayan¹, Atiyeh Mirzaie², Siavash Ahmadi³, Shahram Khazaie¹, Mohammad Reza Aref²

¹Department of Mathematical Sciences Sharif University of Technology, ²Information Systems and Security Lab (ISSSL) Department of Electrical Engineering Sharif University of Technology, ³Electronics Research Institute Sharif University of Technology

Abstract: With the growing demand for security in the Internet of Things (IoT), lightweight block ciphers have become increasingly important due to their ability to provide security under strict resource constraints. This paper analyzes the security of a newly proposed SPN-based lightweight block cipher, LTLBC, recognized for its low-latency property. We evaluate the resistance of LTLBC against boomerang cryptanalysis. Our approach combines a systematic search for differential trails using SMT solvers with experimental verification of boomerang probabilities via experimental sampling. Following a step-by-step methodology, we construct a 6-round boomerang distinguisher, which is further extended to an 8-round key-recovery attack. The resulting attack has a time complexity of $2^{103.44}$, a memory complexity of 2^{44} bytes, and a data complexity of 2^{51} . In addition, we present a 7-round distinguisher with a probability of $2^{-62.44}$. To the best of our knowledge, this work presents the best cryptanalytic results on LTLBC to date, providing new insights into its security margin against advanced differential attacks.

Keywords: Boomerang Cryptanalysis, LTLBC, Block cipher, IoT

Designing Stealthy Kleptographic Backdoors in AES-256 CTR_DRBG: Statistical and Machine Learning-Based Evaluation

Sepide Sadeghi Mehr, Raziye Salarifard, Fartash Abdul Qadir
Shahid Beheshti University

Abstract: Deterministic random bit generators (DRBG) serve as trust anchors for cryptographic keys, nonces, and ephemeral secrets. In black-box deployments, however, a malicious implementer can covertly leak internal state information through the output stream while maintaining statistical properties comparable to the original output. This paper presents an empirical study of an AES-256-based CTR_DRBG prototype augmented with a kleptographic channel that enables recovery of the embedded 48-byte seed via a 108-byte hybrid-encryption payload. The payload integrates X25519 key agreement, HKDF-SHA256 key derivation, and AES-GCM authenticated encryption. A 32-byte ephemeral public key serves as a synchronization header, while the remaining 76 bytes are scattered at SHA-256-derived positions. Baseline and modified streams are evaluated using NIST SP 22-800 and a 2-20-30-6 multilayer perceptron predicting the next bit from a six-bit context. Both the modified and baseline streams satisfied the NIST SP 22-800 acceptance criteria. Mean ANN prediction accuracy is 500248.0 for the baseline stream and 500150.0 for the modified stream, whereas a weak LCG baseline reaches .591714.0. The implemented recovery procedure successfully reconstructed the embedded seed in the evaluated experiment. These findings indicate that, under the evaluated statistical and learning-based detectors, the modified implementation was not distinguished from the baseline implementation.

Keywords: CTR_DRBG, Kleptography, Backdoor, NIST STS, Artificial Neural Networks

GRACTA: Graph-Centrality-Guided ATPG Framework for Hardware Trojan Trigger Activation

Ahmad Karimi, Bijan Alizadeh
University of Tehran

Abstract: Hardware Trojans that activate under rare internal conditions are difficult to detect after fabrication, especially when their triggers depend on multiple inputs. Existing test-generation methods can improve trigger activation, but many are not scalable and provide limited coverage of multi-input triggers. This paper presents GRACTA, a graph-centrality-guided automatic test pattern generation (ATPG) framework for hardware Trojan trigger activation. GRACTA represents a gate-level netlist as a directed graph and uses betweenness, degree, and eigenvector centrality to identify structurally important ATPG targets. Test vectors are generated for the less probable logic value of each node, or for both logic values when their probabilities are equal. Probability-based controllability is used to identify rare nodes, SAT-based analysis removes infeasible two- to eight-input trigger combinations, and circuit simulation evaluates the coverage of the remaining feasible combinations. Experiments on the ISCAS-85 benchmark circuits show that GRACTA reduces the test-set size by an average factor of 167 while improving the mean trigger coverage by approximately 27.2 percentage points compared with a related method.

Keywords: Automatic Test Pattern Generation, Graph Centrality, Hardware Trojan, Rare Nodes, Testability Analysis

PQ-PACKA: Post-Quantum Password-based Authenticated Continuous Key Agreement

Sajjad Rezaei Adaryani, Hamid Mala, Mohammad Reza Saeidi
University of Isfahan

Abstract: Continuous Key Agreement (CKA) schemes facilitate the continuous generation of fresh keys in secure messaging applications using ratchet mechanisms. Most existing CKA schemes have only been analyzed against passive adversaries and lack built-in authentication. Other continuous key agreement schemes that do provide authentication properties rely on hard problems that are vulnerable to quantum attacks, creating a need for secure post-quantum designs. This paper presents a new post-quantum password-based ACKA scheme that, in addition to achieving sender authentication, offers very low bandwidth overhead compared to other quantum-resistant CKA schemes. The proposed scheme combines Ding's key exchange scheme and Lamport's authentication scheme within the continuous key agreement setting, providing a post-quantum continuous key agreement scheme with competitive computational complexity and low communication overhead.

Keywords: Authentication, Continuous Key Agreement, Password, Post-Quantum Cryptography

طراحی ابزار ممیزی انطباق CIS و امتیازدهی شاخص استعداد نفوذ برای بررسی برون خط پیکربندی امنیتی ویندوز در سناریوهای پاسخ به رخداد گسترده

جواد مظاهری^۱، سجاد رضایی^۱، محسن رمضان یارندی^۲

^۱دانشگاه صنعتی اصفهان، ^۲انجمن رمز ایران

چکیده: سنجش انطباق پیکربندی امنیتی ویندوز با CIS Benchmark در پزشکی قانونی دیجیتال معمولاً دستی و پراکنده و بدون تفکیک روشن میان مقدار پیکربندی شده و مدرک واقعی رویدادی است. در رخدادهای گسترده با ده‌ها ایمج دیسک، این مشکل جدی‌تر می‌شود، چون سازوکاری برای پاسخ سریع به این سؤال وجود ندارد: کدام ایمج باید ابتدا بررسی شود؟ این مقاله ابزاری خودکار و آفلاین معرفی می‌کند که با بازگذاری موقت رجیستری SYSTEM و SOFTWARE از روی ایمج دیسک، بدون تغییر سیستم اصلی، نزدیک به صد بررسی در دوازده رده کنترل هم‌راستا با CIS انجام می‌دهد. نوآوری اصلی سه بخش دارد: نخست، موتوری که برای هر تنظیم، مقدار واقعاً اعمال شده را از میان سه منبع (پیکربندی GPO، رجیستری محلی، پیش‌فرض ویندوز) تعیین می‌کند و آن را از مدرک رویدادی مربوطه جدا نگه می‌دارد. دوم، لایه‌ای که وقتی روش استاندارد روی فایل رویداد آسیب‌دیده شکست می‌خورد، به‌طور خودکار به ابزار EvtxECmd روی می‌آورد. سوم، موتور امتیازدهی که نتیجه دوازده رده کنترل را در شاخص استعداد نفوذ (Breach Susceptibility Index) ترکیب می‌کند؛ این شاخص در حوادث گسترده مشخص می‌کند کدام ایمج باید زودتر بررسی شود. ماژول مکملی جدول زمانی نشست‌های دسترسی از راه دور را نیز بازسازی می‌کند.

کلیدواژه‌ها: پزشکی قانونی دیجیتال، انطباق پیکربندی امنیتی، تحلیل رویدادهای ویندوز، پاسخ به رخداد

GHOST: Gradient-guided Hierarchical Optimization for Semantic-preserving Attacks on Feature-Based ML Systems

Mohsen Seddighi, Mahdi Mollazadeh, Hamidreza Lashkarian

Imam Hossein Comprehensive University

Abstract: Deep learning classifiers deployed in high-stakes domains such as network intrusion detection, financial fraud detection, and medical diagnosis increasingly rely on hand-crafted feature vectors rather than raw inputs. Despite growing interest in adversarial robustness, existing attack frameworks predominantly target raw pixel spaces using uniform perturbation budgets (L_p norms), ignoring the heterogeneous nature of feature-vector domains where each feature carries distinct semantic importance and domain-specific constraints. This paper introduces GHOST, a general-purpose framework for generating semantic-preserving adversarial examples in feature space. GHOST contributes four key innovations: (1) a 5-tier Feature Constraint System (IMMUTABLE, BOUNDED, FUNC, STEALTH, FREE) that encodes domain-specific feature criticality; (2) SHAP-weighted Gradient Masking with a tunable β parameter controlling the Pareto trade-off between attack success rate (ASR) and anomaly-detector evasion (IF-Pass); (3) a unified optimizer, the Consistency Engine, that combines Multi-Start Initialization (MSI), cosine-decay momentum, gradient consensus, and the `ghost_clip` projection as a single executable core; and (4) two novel metrics, Utility and Integrity, for quantifying semantic preservation. We evaluate GHOST on the CIC IoT 2023 dataset with 24 multiclass neural classifiers across 4 architectural families and 6 attack classes. GHOST achieves 93.4% ASR and 43.0% IF-Pass under its ASR-optimized setting, 61.4% ASR and 64.7% IF-Pass under its stealth-optimized setting, and 96.4% ASR with 64.9% IF-Pass under a class-specific adaptive policy, while maintaining approximately 75.5% Utility and at least 98.5% Integrity. The framework also adapts conceptually to financial fraud, ECG diagnosis, and image classification.

Keywords: Adversarial machine learning, Feature-space attacks, Anomaly detection, Semantic preservation, IoT security, Constraint-aware

PHALANX: A Reproducible Multi-Vendor Framework for Structural Firewall Policy Analysis and Finding Prioritization

Mahdi Faraji

Takian co.

Abstract: Firewall rulesets continuously change as networks evolve. Rules introduced under operational pressure may later become redundant, conflict with existing rules, or unintentionally expand access beyond their original purpose. These issues are policy-management defects rather than software vulnerabilities, and periodic manual audits are often insufficient for tracking gradual policy drift. This paper presents PHALANX, a reproducible framework for structural firewall policy analysis across multiple platforms. PHALANX uses separate native parsers to map platform-specific configurations into a unified policy model that preserves the distinction between an unsupported concept (N/A) and an explicitly unrestricted value (any). A shared deterministic analysis engine identifies five classes of structural findings and assigns configurable prioritization scores while maintaining traceable evidence for each detected relation. The controlled benchmark comprises 2,503 rules across five platform-specific renditions of a shared policy intent: FortiGate, Palo Alto, pfSense, OPNsense, and IPImen. Following multidimensional predicate validation and anchor-level aggregation, PHALANX reported 970 structural findings across the five configurations; this count represents reported outputs, not independent incidents. In a stratified expert review of operational relevance, 74 of 100 findings received the genuine label. The raters showed 94% raw agreement (Cohen's $\kappa = 0.84$; 95% bootstrap CI: [0.70, 0.95]). This proportion describes the reviewed sample and is not an estimate of precision across all reported findings. In the synthetic scalability experiment, detector execution on the 3,383 enabled rules in a 4,000-rule policy took 54.62 seconds on the reported hardware. This measurement covers detection only; peak memory and end-to-end configuration processing were not measured.

Keywords: Network security, Configuration drift, Firewall policy analysis, Misconfiguration, Deterministic anomaly detection, Multi-vendor normalization

The Agile Forensic Collector: Automated Forensic Evidence Recovery from Ephemeral Container Layers in Living-off-the-Land Attacks

Seyede Marzieh Sadat Madani, Ehsan Mahdavi, Hamid Mala
University of Isfahan

Abstract: Containers are ephemeral by design. When a container is removed, its writable filesystem layer (UpperDir) is deleted with it. This layer may be the only record of an attacker's activity. Living-off-the-Land (LotL) attackers can exploit this by removing the container as soon as they achieve their objective. On our testbed, the layer disappeared a median of 514 ms after `docker rm -f`. We present the Agile Forensic Collector (AFC), a host-side agent with three layers. The Observation Layer arms containers started with dangerous configurations and triggers collection when an armed container is deleted. The Agile Discovery Layer resolves UpperDir from the kernel mount table without querying the container runtime. The Preservation Layer retains the whole layer with hard links and then packages it with SHA-256 digests. In four LotL scenarios, AFC made evidence safe with median latencies of 7.2-1.2 ms and recovered the artifact in every trial. Methods that must first find the artifact needed 9.5-23.0 s. When removal was already under way, AFC recovered 20 of 20 artifacts up to 300ms after the command and 14 of 20 at 500 ms. A direct runtime API copy with the artifact path supplied in advance matched AFC up to 300 ms. In 80 end-to-end trials without manual triggers, AFC preserved the evidence every time, with a median latency of 8.3 ms from the container event. Retention takes about 68 ms per 1000 files, so layers with thousands of files can exceed the window.

Keywords: Cloud-Native Security, Container Forensics, Incident Response, Threat Hunting, Union Filesystem

EPF-Bench: An Extended Persian Benchmark for Fairness Evaluation in Large Language Models

Maryam Azadmanesh
University of Birjand

Abstract: As Large Language Models (LLMs) are increasingly integrated into Persian-speaking societal and industrial domains, ensuring their ethical alignment and fairness is critical. However, evaluating fairness in Persian remains a significant challenge due to the lack of culturally nuanced benchmarks and the sensitivity of models to prompt formulation. This study introduces EPF-Bench, an extended Persian benchmark designed for the multi-dimensional evaluation of fairness in LLMs. By systematically expanding 200 source stereotypes into 1,400 rigorously controlled instances across seven distinct templates, our framework evaluates model behavior under ambiguous contexts, explicit evidence, counterfactual substitutions, and source framing. We evaluated five state-of-the-art LLMs (GPT-6.5 Sol, Claude 5 Sonnet, Gemini 1.3 Pro, DeepSeek V4 Flash, and Qwen 3) using metrics such as Accuracy, Recall, Epistemic Avoidance Rate (EAR), and Framing Sensitivity Rate (FSR). Our findings reveal that while most models perform well in evidence-rich scenarios, they exhibit significant systematic bias and epistemic failures in ambiguous contexts. Specifically, models like Qwen 3 show high propensity for stereotypical guessing (low EAR) and extreme sensitivity to superficial framing (high FSR), demonstrating that fairness in Persian LLMs is deeply tied to internal priors and decision stability rather than mere linguistic proficiency. The complete benchmark dataset is publicly available at <https://github.com/maryamazadmanesh/EPF-Bench>.

Keywords: Bias Evaluation, Fairness Metrics, Large Language Models, Persian Benchmark, Prompt Framing, Social Stereotypes

Verifiable Vector Aggregation in Federated Learning via Rational Audit Scoring

Ali Rahimi, Siavash Ahmadi, Babak Hossein Khalaj
Sharif University of Technology

Abstract: Aggregation is the cornerstone of federated learning, yet clients have no practical way to verify that the server has correctly computed the global model update. Existing solutions based on cryptographic verifiable computation provide strong integrity guarantees but incur substantial computational overhead, limiting their practicality in large-scale federated systems. We propose a lightweight alternative based on rational audit scoring, in which each client evaluates a Brier reward function against the server’s claimed aggregate, making truthful reporting the unique reward-maximizing strategy for a rational aggregator. We introduce two audit protocols, a single-coordinate protocol and a multi-coordinate protocol, that offer different computation–reliability trade-offs. We prove that both protocols provide the same expected audit gap, proportional to the squared deviation between the claimed and true aggregate, while the multi-coordinate protocol substantially reduces the variance of the audit score, producing a more stable audit signal. We clarify the cryptographic assumptions, formalize an adversary model covering equivocation, client honesty, and Byzantine behavior, discuss privacy implications, and compare with cryptographic and incentive-based alternatives. We further implement both protocols in a simulated federated prototype learning environment, and experimental results closely match the theoretical analysis, confirming the predicted audit gap and the improved detection reliability of the multi-coordinate design.

Keywords: Federated learning, Rational Proofs, Brier Score, Verifiable Aggregation, Federated Prototype Learning

MARS: A Multi-Agent Framework for Cyber Range Scenario Generation, Evaluation, and Deployment

Shakiba Nazem, Mojtaba Khalili, Ali Fanian
Isfahan University of Technology

Abstract: Realistic cyber range scenario generation remains a challenging and time-consuming task due to its strong reliance on expert knowledge and manual design. Although large language models have recently been employed to assist scenario generation, existing approaches typically utilize them in isolated stages rather than within an integrated framework. This paper presents MARS, a multi-agent framework for automated cyber range scenario generation and deployment. The proposed framework employs specialized agents to acquire user requirements, select vulnerable machines, construct attack scenarios, generate Docker Compose configurations, and automatically evaluate the quality of the generated scenarios. An Evaluation Agent assesses each generated scenario against predefined quality criteria and, when necessary, requests regeneration to improve the generated output. The proposed framework was evaluated using 100 cyber range scenarios, which were independently assessed by cybersecurity experts based on user requirement satisfaction, realism, service and machine diversity, technology freshness, and attack scenario consistency. Experimental results demonstrate that MARS automates the cyber range scenario generation workflow, including deployment configuration generation, while producing realistic and consistent scenarios. Furthermore, the Evaluation Agent showed strong agreement with expert assessments, indicating its potential for automated scenario quality assessment.

Keywords: Cyber Range, Large Language Models, Multi-Agent Systems, Automated Scenario Generation, Docker Compose

Collaboration-based Privacy-Preserving Firewall for Home Networks

Yasamin Rahimi Sadegh, Sajad Shirali-Shahreza

Amirkabir University of Technology

Abstract: The rise of IoT devices has increased security risks, requiring faster and more effective defenses. Although home gateways are the first line of defense, they struggle against advanced threats. Current learning-based detection methods offer speed, but face scalability and privacy issues in distributed IoT environments. To address this, our research proposes a collaborative firewall using federated learning. It enables attack detection at the gateway while maintaining raw training records on participating clients. The firewall employs federated tree models that exchange training summaries with an aggregator rather than centrally collecting raw gateway traffic. On Edge-IIoTSet dataset, our feature selection reduces the number of input features from 61 to 22, cutting training time by 75% and per-packet inference time by more than 65%, while the accuracy slightly reduced from 93.6% to 92.53%. When the federated training was used, the accuracy slightly increased to 93.8%. This shows that collaborative training did not reduce detection accuracy in our setting. Our framework combines local attack detection, collaborative training, and reduced feature and execution costs for smart-home security.

Keywords: Federated Learning, Firewall, Smart Home, IoT Security

چارچوبی مبتنی بر هوش تهدید سایبری برای مدلسازی عامل محور گروه‌های تهدید پیشرفته و پایدار سایبری نوظهور

سعید محمدی

دانشگاه جامع امام حسین (ع)

چکیده: کمپین‌های تهدید پیشرفته مداوم (APT) با رفتارهای تطبیقی و هماهنگ مشخص می‌شوند که مکانیسم‌های دفاع سایبری سنتی را به چالش می‌کشند. این مقاله یک روش تکرارپذیر برای تبدیل هوش تهدید سایبری (CTI) به رفتارهای مبتنی بر عامل قابل اجرا ارائه می‌دهد که در ۱۳ توالی کمپین مرتبط با APT29 و APT41 نشان داده شده است. یک ماتریس انتقال تجربی از طریق تخمین حداکثر احتمال از توالی‌های TTP بازسازی شده ATT&CK استخراج می‌شود. پارامترهای TTP با استفاده از اطلاعات دید و فرضیات رفتاری منبع آگاه مشخص می‌شوند. CVSS نسخه 3.1 به عنوان اطلاعات قابلیت بهره‌برداری زمینه‌ای، به جای یک معیار مستقیم تشخیص ریسک، در نظر گرفته می‌شود. دو خط پایه مارکوف از یک ماتریس انتقال یکسان استفاده می‌کنند: یک خط پایه بدون محدودیت و یک خط پایه منطبق با مدافع، بدون حافظه یا پشتیبان تطبیقی. موفقیت کمپین از نظر آماری بین ABM تطبیقی و خط پایه منطبق با مدافع قابل تشخیص نیست ($p = 0.859$), در حالی که تشخیص، توالی‌های TTP جدید و تنوع رفتاری متفاوت هستند. از آنجا که حافظه و پشتیبان تطبیقی به طور همزمان در خط پایه منطبق با مدافع حذف می‌شوند، اثرات مستقل آن‌ها را نمی‌توان با طراحی فعلی جدا کرد. مقایسه‌های خارجی نشان‌دهنده همسویی رفتاری با فعالیت مستند شده APT41/APT29 هستند. سهم روش شناختی اصلی، ادغام انتقال‌های TTP مشتق شده از CTI با تصمیم‌گیری مبتنی بر عامل تطبیقی در یک خط لوله شبیه‌سازی واحد است.

کلیدواژه‌ها: تهدید پیشرفته پایدار، MITRE ATT&CK، مدل‌سازی عامل محور، هوش تهدید سایبری

ارزیابی تطبیقی وضعیت استقرار سرایندهای امنیتی HTTP در وبسایتهای ایرانی و آلمانی در ۱۰ حوزه ی کاربردی

فرهاد اصفهانی زاده، مینا زلفی، لیلی فرزین وش
دانشگاه تبریز

چکیده: این پژوهش وضعیت استقرار 18 هدر امنیتی پروتکل انتقال ابرمتن (HTTP)، که در برابر حملاتی مانند اسکریپت نویسی بین سایتی (XSS) و افشای اطلاعات فنی سرور محافظت ایجاد می کنند، را در 1000 وبسایت (500 ایرانی و 500 آلمانی) در 10 حوزه کاربردی به صورت تطبیقی بررسی می کند. هدرها در چهار گروه وزن دار امتیازدهی و به شاخصی صفر تا صد تبدیل شدند. آزمون Mann-Whitney U نشان داد میانگین امتیاز وبسایت های آلمانی (38.3) به طور معناداری بالاتر از ایران (28.0) است. این برتری در سه مدل وزن دهی متفاوت پایدار ماند. شکاف پس از تعدیل برای مقایسه های چندگانه در پنج حوزه (آموزش، سلامت، فناوری اطلاعات، اخبار و فروشگاه های آنلاین) معنادار باقی ماند، درحالی که در بانک ها، نهادهای انتظامی، خدمات دولتی، سرگرمی و دانشگاه ها معنادار نبود. آزمون Kruskal-Wallis نشان داد حوزه کاربردی در هر دو کشور اثر معناداری بر امتیاز دارد، با اندازه اثر تقریباً دوبرابری در ایران نسبت به آلمان. پس از بررسی، الگوی معکوسی در هدرهای افشاکننده مشاهده شد؛ به طوری که X-Powered-By در ایران (26.2% در برابر 8.6% و Via در آلمان (15.4% در برابر 2.2%) بیشتر افشا می شدند. یافته ها نشان می دهند شکاف امنیتی میان دو کشور یکنواخت نیست و به شدت به حوزه کاربردی وابسته است.

کلیدواژه ها: هدرهای امنیتی HTTP، امنیت وب، تحلیل تطبیقی

Verifiable Homomorphic Server-Aided Computation Outsourcing with Remote Data Integrity Checking: A Quantum-Resistant Approach

Zahra Keshavarz Rezaei, Mohammad Ali
Amirkabir University of Technology

Abstract: Cloud computing allows users store large amounts of data and run computations on remote servers instead of locally. Because the server is run by an untrusted third party, users need a way to check that their data is unchanged and that computations performed on their behalf are correct. Remote Data Integrity Checking (RDIC) addresses the first need: it lets a client publicly audit outsourced data without downloading it. However, existing RDIC schemes focus on the integrity of stored data and do not verify computations performed on it. As a result, users who need both storage auditing and delegated computation have to rely on separate mechanisms. We propose a scheme that enables public RDIC for both outsourced data and computation results while supporting the homomorphic evaluation of leveled arithmetic circuits over authenticated blocks. Computed results are periodically re-authenticated through a short interactive refresh, keeping the evaluated values within the supported bound and preventing the server from adding forged data. This refresh requires a fixed, small amount of client work, independent of the computation size. We prove the correctness of our construction and demonstrate its security in the random oracle model under the R-SIS assumption, providing post-quantum security for both outsourced storage and delegated computation.

Keywords: Remote Data Integrity Checking, Homomorphic Signatures, Lattice-Based Cryptography, Post-Quantum Security

A Latent Feature-Based Medical Image Encryption Framework Using a Convolutional Autoencoder, Latin Square, and AES

Mohammad Heydari, Ebrahim Zarei Zefreh, Mohsen Kiani

University of Isfahan

Abstract: Medical image encryption has become increasingly important with the rapid deployment of the Internet of Medical Things (IoMT), where resource-constrained devices require efficient processing and secure data transmission. This paper proposes a latent feature-based medical image encryption framework centered on a lightweight convolutional autoencoder (CAE). The CAE generates a compact $64 \times 32 \times 32$ latent representation from 512×512 grayscale medical images while preserving spatial information through a constrained bottleneck without encoder-decoder skip connections. The latent features are quantized to 8-bit values and rearranged using a key-dependent Latin square whose permutation vectors are generated from domain-separated HKDF-SHA-256 key material. The resulting byte stream is protected using AES-256-GCM, providing authenticated encryption and ciphertext integrity. Experiments on the NYU fastMRI knee dataset show a validation SSIM of 0.91 and PSNR of 35.26 dB for the selected Ultra-light CAE. The quantized latent representation contains 65,536 bytes compared with 262,144 bytes for an 8-bit 512×512 image, corresponding to a nominal 4 : 1 reduction in raw payload size before encryption metadata. The encrypted representations exhibit near-maximal entropy of approximately 7.997 bits and negligible linear correlation, while one-bit key variations produce BCR values close to 50%. The Ultra-light model uses 350,623 trainable parameters and achieves 95.9% of the Heavy model's validation SSIM while requiring 25.2% of its parameters. These results demonstrate a practical trade-off among latent representation compactness, reconstruction fidelity, computational complexity, and authenticated protection for secure medical-image transmission in IoMT environments.

Keywords: Medical image, Latent feature encryption, Convolutional autoencoder, Latin square, AES

A Review of Security and Privacy in Federated Learning Attacks, Defenses, and Open Challenges

Nafise Aghouee, Farhad Rahmati, Amin Hosseingholizadeh
Amirkabir University of Technology

Abstract: Federated learning (FL) is a distributed machine learning paradigm that enables collaborative model training across decentralized devices while preserving data privacy by keeping raw data locally. Although this framework significantly preserves user privacy and prevents attackers from accessing raw data, the system remains exposed to various security threats, including data and model poisoning attacks, user collusion, inference attacks, client dropouts, and many others. In response to these challenges, various privacy preserving methods have been proposed to secure FL systems. Despite these efforts, no single approach is without limitations, and many fundamental challenges remain open. This paper presents a selective review of FL, including a taxonomy of system architectures, an analysis of privacy-compromising and security attacks, and a comparative evaluation of existing defense mechanisms with their respective advantages and limitations. We also highlight the open research questions and persistent challenges that continue to hinder the widespread adoption of FL in privacy-sensitive applications.

Keywords: Federated Learning, Machine Learning, Privacy Preserving, Security Attacks

CredentialBound-FL: Verifiable Account-Level Sampling Across Multiple Devices

Mohammad Zare Ahangarkolaei, Masoumeh Koochak Shooshtari, Mohammad Reza Aref
Sharif University of Technology

Abstract: Cross-device federated learning (FL) typically samples and clips devices even when the intended privacy unit is an account that may own several devices. If an account owns m devices sampled independently with probability q , device-level participation increases its worst-case sensitivity from C to mC , its inclusion probability from q to $1 - (1 - q)^m$, and its expected learning weight from q to mq . We propose CredentialBound-FL, a credential-based anonymous admission layer that establishes coherent account eligibility and limits each admitted account to one representative-device contribution per round. We define, analyze, and implement an admission relation that verifies membership in a fixed epoch credential set, correct account sampling, possession of the selected device key, a one-use nullifier, and binding to a public update handle. The epoch credential root is committed before an unpredictable public round beacon is revealed. A holder-generated account secret then determines eligibility, representative-device selection, and the nullifier without revealing the account identity. We prove the sampling and multiplicity properties of the admission layer. Our account-level computational-DP result is a theoretical blueprint conditional on an external binding vector commitment, norm validation, secure aggregation, and calibrated noise. Our Circom/Groth16 admission relation has 9,893 constraints, with median proving and verification times of 506.15 ms and 17.00 ms, respectively, over 464 proofs. A common UCI HAR/WISDM evaluation uses subject-disjoint splits, linear and non-linear models, and matched learning controls at the ideal per-run $(\epsilon, \delta) = (4.4747, 10^{-5})$. It measures accuracy, Macro-F1, local training time, data use, and availability on both datasets. WISDM retains paired phone/watch streams in the primary evaluation.

Keywords: Federated Learning, Differential Privacy, Anonymous Admission, Contribution Bounding, Zero-Knowledge Proofs

DualShield: Confidence-Aware Selective Escalation for Lightweight IoT Intrusion Detection and Post-Gate Novelty Analysis

Ehsan Nokandi, Mohammad Hossein Khosravi, Maryam Azadmanesh
University of Birjand

Abstract: The proliferation of Internet of Things (IoT) networks has broadened the cyber-attack landscape while exposing a fundamental weakness in conventional intrusion detection systems: closed-set classifiers must map every flow to a known class, even when the resulting decision is ambiguous or uncertain. Yet running computationally demanding open-set recognition (OSR) on all incoming traffic is often impractical in resource-constrained IoT environments. This paper introduces DualShield, a lightweight multi-stage framework that couples closed-set intrusion classification with confidence-aware selective escalation. A Decision Tree performs the initial multiclass prediction. A confidence-aware gate then routes only the least confident 5% of samples to two complementary recognition experts, whose scores are normalized against known-only reference distributions and fused through a parameter-free Simple-Max rule. The secondary stage is evaluated through nested pseudo-unknown leave-one-class-out validation without access to the outer held-out attack family. On CICIOT2023, the Decision Tree attained 0.9957 accuracy, 0.8655 macro-F1, and 0.9956 weighted-F1 while retaining a compact model footprint. Under the stricter all-known-negative post-gate protocol, DualShield achieved a macro routed detection rate of 22.71% at an all-known false-alarm rate of 5.02%. These findings indicate that selective escalation can provide controlled post-gate novelty recognition for routed samples while preserving an efficient primary detection path for IoT intrusion detection.

Keywords: Anomaly Scoring, Cyberattack Classification, Decision Trees, Leave-One-Class-Out Evaluation, Out-of-Distribution Analysis, Uncertainty Estimation

Golden Path Discovery: A Transparent, Weighted Algorithm for Prioritizing Attack Paths in Enterprise Active Directory Networks

Behnam Amiri, Yousef Darmani

K. N. Toosi University of Technology

Abstract: Active Directory serves as the backbone of identity management in most enterprises, making it a prime target for Advanced Persistent Threats. Attackers exploit chains of misconfigurations, excessive permissions, or vulnerabilities to reach critical assets like Domain Controllers. While BloodHound can graph these paths, the enormous volume of possible routes in real networks overwhelms manual analysis and obscures the truly dangerous ones.

In this paper, we present Golden Path Discovery (GPD), a transparent algorithm that prioritizes attack paths by focusing on “golden assets” and computing the weighted shortest distance from every node to those assets.

Using a reverse weighted graph traversal, the method assigns a risk score to each node and extracts only the most direct, high-impact paths. Unlike black-box industrial tools such as Forest Druid, our algorithm is fully documented, auditable, and extensible, supporting configurable edge weights based on organizational threat models. We evaluate GPD on the GOAD simulation environment and show that it reduces the number of paths requiring analyst attention by over 99.9%, while placing all true critical attack paths from documented scenarios within the top 5 risk-ranked results ($\text{Recall@5} = 100\%$), computed over non-golden nodes to avoid overestimation. Comparisons with standard graph-based baselines, including unweighted BFS, PageRank, and Betweenness Centrality, confirm the effectiveness of the approach.

Keywords: Active Directory Security, Attack Path Prioritization, APT Detection, Golden Assets, Enterprise Networks

Reconstructing Multi-Stage Attack Chains Using a Context-Enriched Cyber Security Knowledge Graph

Imanimehr Fatemeh, Hamed Ebrahimi
ICT Research Institute (ITRC)

Abstract: Advanced Persistent Threats (APTs) execute stealthy and multi-stage campaigns in which adversaries gradually compromise systems and move across the network. Understanding how individual security events relate to each other and reconstructing the underlying attack chain are critical for effective incident investigation and threat analysis. However, enterprise security event logs collected by Security Information and Event Management (SIEM) systems are typically analyzed as isolated records, making it difficult to identify the sequence of attacker activities and the progression of an attack. This paper presents a context-enriched Cyber Security Knowledge Graph (CSKG) framework for reconstructing multi-stage attack chains from heterogeneous event logs. The proposed approach enriches raw event logs with contextual attributes and threat intelligence and models security entities, events, and their relationships within a unified knowledge graph. By capturing temporal dependencies between events, the framework enables the identification of event sequences and their abstraction into higher-level behavioral patterns that describe the progression of adversarial activities. The reconstructed behaviors are further aligned with the MITRE ATT&CK framework to provide semantic interpretation of attacker tactics and techniques. Evaluation on a realistic APT emulation dataset demonstrates that the proposed CSKG framework enables systematic reconstruction of attack chains from event logs and supports more effective investigation of complex multi-stage attacks.

Keywords: Threat Intelligence, Attack Chain Graph, Cyber Security Knowledge Graph, Multi-Stage Attack Analysis

VishConv: A Lightweight Hybrid Deep Learning Framework for Raw-Byte Malware Detection

Armin Tavakoli¹, Arash Abdi Hejrandoost²

¹Amnpardaz Software Corporation, ²Iran University of Science and Technology

Abstract: The increasing volume and sophistication of malware have reduced the effectiveness of traditional signature-based detection methods, particularly against previously unseen, packed, and obfuscated threats. Deep learning models such as MalConv address this challenge by learning directly from raw executable bytes; however, their feature extraction capability can be further improved. Moreover, malware datasets are often highly imbalanced, and packed or obfuscated samples tend to produce overlapping feature representations, making accurate classification more difficult. This paper presents VishConv, an enhanced MalConv architecture with refined network layers for improved hierarchical feature learning while preserving end-to-end raw-byte processing. To address class imbalance, a weighted combination loss incorporating Focal Loss is employed to emphasize difficult samples. Furthermore, Contrastive Loss is integrated to improve feature discrimination by reducing intra-class variation and increasing inter-class separation. Experimental results demonstrate that VishConv consistently outperforms the original MalConv, achieving more robust malware detection while maintaining computational efficiency suitable for real-time CPU-based deployment.

Keywords: Cybersecurity, Deep Learning, Executable Files, Raw Byte Analysis, Representation Learning, Windows Portable Executable Files

Benchmarking Data-Level Imbalance-Handling Techniques for IoT Intrusion Detection: A Cross-Dataset Evaluation on IoT-23 and CICIDS2017

Morteza Taheri¹, Sajad Haghzad klidbary¹, Mohammad Hesam Tadayon²

¹University of Zanjan, ²ICT Research Institute

Abstract: The rapid expansion of IoT environments has intensified the demand for robust anomaly-based intrusion detection systems. However, severe class imbalance-where malicious activity is a small minority-often biases classifiers and hampers anomaly detection. This paper presents a reproducible cross-dataset benchmark comparing data-level imbalance-handling strategies for IoT intrusion detection using the IoT-23 and CICIDS2017 datasets. We evaluate eight machine learning classifiers across ten data-level balancing configurations (including an unmitigated baseline), ranging from random and heuristic resampling (SMOTE, ADASYN, Borderline-SMOTE, NearMiss) and hybrid cleaning (TomekLinks, SMOTETomek) to deep generative augmentation (WGAN-GP). Using a strict, leak-free 5-fold stratified cross-validation pipeline, we assess performance on untouched test sets using PR-AUC, Recall, Precision, False Positive Rate (FPR), and execution time. Results show that balancing effectiveness is highly dataset-dependent. On the complex IoT-23 dataset, heuristic oversampling boosts Recall but compromises Precision, whereas WGAN-GP maintains high Precision with limited Recall gains. Conversely, CICIDS2017 exhibits such high class separability that robust tree-based ensembles achieve near-perfect performance on raw data, rendering explicit balancing statistically redundant. Ultimately, evaluated through a multi-objective Pareto efficiency lens, lightweight configurations-such as LightGBM paired with minimal or targeted resampling-outperform computationally heavy synthetic augmentation pipelines, providing an optimal trade-off for resource-constrained, real-time IoT deployments.

Keywords: Anomaly Detection, IoT Intrusion Detection, Class Imbalance, Data-Level Balancing, SMOTE, LightGBM, IoT-23

کارگاه‌ها

عناوین و ارائه‌دهندگان کارگاه‌ها

حمله عامل محور در برابر دفاع عامل محور: فراتر از KYC در بانکداری دیجیتال

حسین معاصر

شرکت توسعه فناوری رفاه پردیس (وابسته به بانک رفاه کارگران)

توضیحات: اگر مهاجم بتواند با کمک هوش مصنوعی هویت را جعل کند، کنترل یک نشست معتبر (Session) را به دست بگیرد و رفتار خود را براساس واکنش سیستم تغییر دهد، آیا کنترل‌های امنیتی فعلی هنوز کافی‌اند؟ در این کارگاه، تقابل واقعی حمله عامل محور (Agentic Attack) و دفاع عامل محور (Agentic Defence) از نزدیک بررسی می‌شود؛ از سامانه مصنوعی رسانه (Synthetic Media) و تلاش برای دور زدن زنده‌سنجی و تشخیص حملات PAD Bypass تا تزریق جریان تصویر (Stream Injection)، رایش نشست (Session Hijacking) و تصاحب حساب (Account Takeover). سپس می‌بینیم دفاع عامل محور چگونه می‌تواند شواهد را جمع‌آوری کند، فرضیه بسازد، تصمیم بگیرد و در برابر رفتار مهاجم خود را تطبیق دهد. این کارگاه فقط مجموعه‌ای از اسلایدها نیست؛ شرکت‌کنندگان با آزمایش‌های عملی، حلقه‌های تصمیم‌گیری و یک آزمایشگاه کوچک (Micro-Lab) سناریوهای حمله را تحلیل می‌کنند، حمله را تشخیص می‌دهند و درباره اقدامات دفاعی تصمیم می‌گیرند.

تحول خدمات مالی با هوش مصنوعی و امنیت سایبری در اکوسیستم فین‌تک

محمدحسین میرزاشاه جعفری

ایرانیکارت

توضیحات: رشد شتابان خدمات مالی دیجیتال (از پرداخت‌های بین‌المللی و رمزارز تا خرید آنلاین از پلتفرم‌های خارجی) سطح جدیدی از تهدیدات امنیتی نظیر سرقت حساب کاربری، فیشینگ، سوءاستفاده از API و پول‌شویی را به همراه آورده است. در چنین فضایی، هوش مصنوعی هم‌زمان به ابزاری کلیدی برای کشف و پیشگیری از تقلب و هم به میدان جدیدی از ریسک، مانند حملات Deepfake و حملات خودکار مبتنی بر AI، تبدیل شده است. این کارگاه با هدف تبیین هم‌گرایی هوش مصنوعی و امنیت سایبری در فین‌تک طراحی شده و شرکت‌کنندگان را از مفاهیم پایه خدمات مالی دیجیتال، عبور از تهدیدات رایج امنیتی، تا نقش یادگیری ماشین در Fraud Detection، تحلیل رفتار کاربر و معماری‌های نوین امنیتی (از جمله API Security و Zero Trust IAM) همراهی می‌کند. محتوای کارگاه با مطالعه موردی حملات واقعی در صنعت فین‌تک و مروری بر چشم‌انداز آینده در AI و امنیت مالی تکمیل می‌شود و بر مبنای منابع معتبر بین‌المللی OWASP، NIST CSF، ISO/IEC 27001 و گزارش‌های تهدید شناخته‌شده، از جمله McKinsey و Gartner، ارائه خواهد شد. هدف، توانمندسازی شرکت‌کنندگان برای طراحی و پیاده‌سازی راهکارهای امنیتی متناسب با نیازهای سازمانی و تقویت فرهنگ امنیت در سازمان‌های فین‌تک خواهد بود.

از مدل‌های زبانی تا عامل‌های هوشمند در جرم‌یابی دیجیتال

رویا نوری، امیرمحمد محمودخانی
پژوهشگاه توسعه فناوری‌های پیشرفته

توضیحات: افزایش حجم و پیچیدگی شواهد دیجیتال، استفاده از روش‌های هوشمند برای تحلیل و بررسی پرونده‌های جرم‌یابی دیجیتال را به یک ضرورت تبدیل کرده است. این کارگاه به بررسی نقش مدل‌های زبانی بزرگ و عامل‌ها در فرایند تحقیقات دیجیتال می‌پردازد. در بخش نخست، نمونه‌هایی از کاربرد AI و LLM در عامل‌ها در آخرین نسخه‌های ابزارهای مطرح جرم‌یابی دیجیتال مورد بررسی قرار می‌گیرد. در بخش دوم، یک دستیار تحقیقاتی مبتنی بر Model Context Protocol و Autopsy معرفی می‌شود که قادر است از طریق ابزارهای MCP به صورت ساختاریافته به فایل‌ها، آرتیفکت‌ها، تایم‌لاین و حساب‌های کاربری دسترسی پیدا کند. شرکت‌کنندگان مشاهده خواهند کرد که چگونه یک سؤال طبیعی می‌تواند به مجموعه‌ای از عملیات چندمرحله‌ای برای بازیابی و تحلیل شواهد تبدیل شود.

امنیت اینترنت اشیا: چالش‌ها، تهدیدها و راهکارهای حفاظت از سامانه‌های متصل

حامد رمضانی‌پور، سمیرا نظری
پژوهشگاه توسعه فناوری‌های پیشرفته

توضیحات: گسترش سریع سامانه‌های اینترنت اشیا و افزایش استفاده از تجهیزات متصل در حوزه‌های مختلف، موضوع امنیت این سامانه‌ها را به یکی از چالش‌های مهم حوزه فناوری اطلاعات تبدیل کرده است. برخلاف سامانه‌های رایانه‌ای متداول، تجهیزات اینترنت اشیا معمولاً با محدودیت‌هایی در منابع پردازشی، حافظه، انرژی و قابلیت‌های ارتباطی مواجه هستند که طراحی و پیاده‌سازی راهکارهای امنیتی مناسب را با چالش‌های ویژه‌ای همراه می‌کند. این کارگاه به بررسی مفاهیم بنیادین امنیت اینترنت اشیا، تهدیدهای رایج، الزامات امنیتی تجهیزات محدودمنابع، نقش الگوریتم‌های رمزنگاری سبک‌وزن، مدیریت کلید، احراز هویت، ارتباطات امن و روش‌های ارزیابی امنیت سامانه‌های اینترنت اشیا می‌پردازد. هدف از این کارگاه، ایجاد دیدگاهی جامع نسبت به چالش‌های امنیتی تجهیزات متصل و معرفی رویکردهای مناسب برای طراحی، پیاده‌سازی و ارزیابی سامانه‌های امن اینترنت اشیا است.

بررسی چالش‌های امنیتی کنترل دسترسی ارتباطات بلادرنگ در شبکه‌های اینترنت اشیا

محمدحسام تدین، پیمان ویسی، پریان نخعی، کیمیا ملک‌نژاد
پژوهشگاه ارتباطات و فناوری اطلاعات

توضیحات: تحول دیجیتال و گسترش سامانه‌های هوشمند، صنایع را بیش از گذشته به ارتباطات بلادرنگ و تصمیم‌گیری خودکار وابسته کرده است. این کارگاه با هدف بررسی چالش‌های امنیتی کنترل دسترسی در ارتباطات بلادرنگ شبکه‌های اینترنت اشیا (IIoT)، مبانی و معماری این سامانه‌ها را بررسی می‌کند. ابتدا ساختار سامانه‌های کنترل صنعتی و SCADA و چالش‌های امنیتی آن‌ها تبیین شده و ارتباط آن‌ها با IoT تشریح می‌شود. سپس ضرورت به‌کارگیری IIoT در صنایع و محیط‌های آن

در سه مقیاس خرد، متوسط و کلان، براساس پیچیدگی، گستره جغرافیایی و میزان اهمیت، بررسی می‌گردد. در ادامه، معماری ارتباطات بلادرنگ و نقش پروتکل MQTT در تبادل داده‌های صنعتی بررسی شده و الزامات کنترل دسترسی، از جمله احراز هویت، مجوزدهی و حفاظت از تبادل داده، تحلیل می‌شوند. همچنین چالش‌های امنیتی کنترل دسترسی در محیط‌های پویا و ناهمگون IIoT بررسی شده و نقش مدل‌های Trust و چارچوب‌های نوین کنترل دسترسی در ایجاد سازوکارهای امن، پویا و متناسب با شرایط عملیات تبیین می‌گردد. در پایان، با ارائه یک مطالعه موردی، ارتباط میان معماری سامانه، الزامات کنترل دسترسی و مدیریت اعتماد تحلیل شده و ضمن جمع‌بندی چالش‌های اصلی، مسیرهای آینده برای توسعه راهکارهای امن و کارآمد در ارتباطات بلادرنگ IIoT مطرح می‌شوند.

هوش مصنوعی و امنیت سایبری

محمدحسن صالح

روبال پرداز تیام

توضیحات: جایگاه هوش مصنوعی در امنیت سایبری؛ در این بخش به کاربردهایی از هوش مصنوعی در انجام فعالیت‌های متداول امنیت سایبری با دو رویکرد تهاجمی و تدافعی پرداخته می‌شود. دو مثال عملی از کاربرد هوش مصنوعی در فرایند ارزیابی امنیت و استفاده از هوش مصنوعی در فرایند مرکز عملیات امنیت بیان می‌شود.

امنیت هوش مصنوعی؛ در این بخش به تهدیدات امنیتی هوش مصنوعی و راهکارهای امن‌سازی پرداخته می‌شود. مواردی همچون انواع Prompt Injection تشریح خواهد شد و به‌صورت عملی نمایش داده خواهد شد. در ادامه مقایسه‌ای بین متدولوژی‌های مختلف انجام خواهد شد.

Federated RAG: استفاده از دانش چندمنبع بدون تجمیع اطلاعات

رویا نوری، زینب عربشاهی

پژوهشگاه توسعه فناوری‌های پیشرفته

توضیحات: با گسترش روزافزون استفاده از مدل‌های هوش مصنوعی در سامانه‌های مختلف، نیاز به استفاده از داده‌های بخش‌های مختلف مراکز داده در پاسخگویی به سؤالات و ایجاد دانش متمرکز و قابل تجمیع به‌طور فزاینده‌ای اهمیت پیدا کرده است. بااین‌حال، در بسیاری از کاربردها، داده‌های سازمان شامل اطلاعات خصوصی و حساس هستند که انتقال آن‌ها به یک سرور مرکزی می‌تواند خطراتی مانند افشای اطلاعات، دسترسی غیرمجاز و نقض حریم خصوصی را به همراه داشته باشد. بنابراین، یکی از چالش‌های مهم در توسعه سامانه‌های هوشمند، ایجاد امکان پرسش جامع و استخراج اطلاعات مفهومی از داده‌های حساس بدون انتقال داده‌های خام به یک مرکز متمرکز است. در بخش نخست، مفاهیم Federated RAG و Federated Learning و بررسی می‌شود. سپس نحوه طراحی و پیاده‌سازی Federated RAG نشان داده می‌شود. هدف، ارائه معماری هوش مصنوعی خصوصی و غیرمتمرکزی است که از داده‌ها و دانش چندمنبع به‌صورت هم‌زمان استفاده کند، بدون اینکه نیازی به انتقال داده‌های خصوصی به یک مرکز متمرکز باشد.

آشنایی با پروتکل‌های تبادل کلید احراز هویت‌شده مبتنی بر گذرواژه (PAKE)

احمد رحمتی

دانشگاه صنعتی امیرکبیر

توضیحات: هدف از این کارگاه، آشنایی با پروتکل‌های تبادل کلید احراز هویت‌شده مبتنی بر گذرواژه (PAKE) و ارائه چند مثال از آن‌هاست. همچنین حملات مختلفی که این نوع پروتکل‌ها را تهدید می‌کنند و آسیب‌پذیری‌های ذاتی آن‌ها را بررسی می‌کنیم.

پروتکل‌های PAKE گونه‌ای از پروتکل‌های کلاینت-سروری هستند که در آن‌ها هر کاربر در مرحله ثبت‌نام، نام کاربری (شناسه کاربری) و گذرواژه (پسورد) خود را با سرور به اشتراک می‌گذارد و بعداً به کمک همین شناسه و گذرواژه می‌تواند در هر زمان کلید نشست با سرور را به اشتراک بگذارد. در این پروتکل‌ها خبری از کلید خصوصی بلندمدت برای کاربران نیست و به‌جای آن از گذرواژه استفاده می‌شود که نسبت به کلید خصوصی متداول، آنتروپی کمتری دارد ولی در عوض نیاز به ذخیره‌سازی امن ندارد؛ چراکه به خاطر سپرده می‌شود. از آنجا که گذرواژه مستعد اعمال حمله دیکشنری (جستجوی جامع) است، این امر در ظاهر برقراری امنیت این پروتکل‌ها را با چالش مواجه می‌کند، ولی درواقع طراحی هوشمندانه پروتکل‌های PAKE مانع از حمله دیکشنری آفلاین (برای مهاجم غیرفعال) و حمله دیکشنری آنلاین (برای مهاجم فعال) می‌شود.

مهندسی امنیتی زیرساخت‌های مبتنی بر Kubernetes

مهدی زمانی

شرکت خدمات انفورماتیک

توضیحات: این کارگاه به بررسی اصول، الزامات و چالش‌های امنیتی زیرساخت‌های مبتنی بر Kubernetes با تمرکز بر طراحی، استقرار و بهره‌برداری امن می‌پردازد. مباحث اصلی شامل مدیریت دسترسی و مجوزها، تفکیک منابع و Workloadها، امنیت شبکه و ارتباطات، سخت‌سازی و اعمال سیاست‌های امنیتی است. همچنین، امنیت Imageها و زنجیره تأمین نرم‌افزار، ثبت و تحلیل رویدادهای امنیتی و پایش تهدیدات در زمان اجرا مرور می‌شود. ملاحظات هم‌زیستی سرویس‌های مختلف در یک کلاستر و چالش‌های ناشی از ماهیت پویا و توزیع‌شده Kubernetes نیز مورد بحث قرار می‌گیرد. هدف کارگاه، ارائه درکی منسجم از مخاطرات و کنترل‌های امنیتی و کمک به اولویت‌بندی اقدامات امن‌سازی در محیط‌های عملیاتی است. مطالب به‌صورت نظری و تحلیلی ارائه می‌شوند.

تحلیل رمز خودکار رمزهای متقارن: مدل سازی قیودی و پیاده سازی عملی

ایمان میرزاعلی، مجید رحیمی، وحید سلیمانی
پژوهشگاه توسعه فناوری های پیشرفته

توضیحات: تحلیل رمز خودکار یکی از رویکردهای نوین و مؤثر در ارزیابی امنیت الگوریتم های رمزنگاری متقارن است که با تبدیل ویژگی ها و روابط به مسائل صوری، امکان استفاده از روش هایی مانند SAT، SMT، CP و MILP را فراهم می کند. در این کارگاه ابتدا مبانی و ضرورت تحلیل رمز خودکار و تفاوت آن با روش های دستی معرفی می شود. سپس نحوه مدل سازی رفتار تفاضلی و خطی الگوریتم های متداول رمزنگاری و روش های کدگذاری قیود در قالب های SMT، CNF و DIMACS بررسی خواهد شد. در بخش عملی، ساختار و نحوه استفاده از چارچوب CryptoSMT و همچنین تولید و حل مدل های CNF برای تحلیل رمزهای سبک وزن آموزش داده می شود. تمرکز کارگاه بر تحلیل تفاضلی رمزهای قالبی سبک وزن و تفسیر خروجی حل کننده ها خواهد بود.

شکاف اعتماد: در آمدی بر معماری امنیت در دنیای بدون رمز

شهریار بیژنی
دانشگاه شاهد

توضیحات: نفوذهای مکرر سایبری به سازمان ها، به خصوص سازمان های متولی زیرساخت های حیاتی در کشورها، نیاز به روش های پیشرفته امنیت فضای سایبری را نشان می دهد. تجربیات نه چندان موفق در معماری امنیتی لایه زیرساخت شبکه و لایه خدمات، بیانگر نیاز به رویکرد متفاوتی در روش های طراحی و پیاده سازی معماری امنیتی رایج است. مخاطبین در این کارگاه با رویکردی بنام معماری مبتنی بر عدم اعتماد (Zero Trust Architecture) در مدیریت امنیت آشنا می شوند که پیاده ساز آن می تواند در ارتقای امنیت سازمان ها و زیرساخت های حیاتی کشور نقش مؤثری داشته باشد.

سیستم ها و شبکه های توزیع کلید کوانتومی

فاطمه رضازاده، حمید عسگری، امیرحسین دده خانی، مجید خداینده
تکفن

توضیحات: در این کارگاه ابتدا مباحث پایه ای کوانتوم تأثیرگذار در ساختار توزیع کلید کوانتومی و اولین پروتکل توزیع کلید کوانتومی، خصوصیات آن و نحوه شناسایی شنودگر بیان می شود. سپس چالش های عملیاتی پروتکل های اولیه معرفی و یکی از پروتکل های امروزی منطبق با ساختارهای آزمایشگاهی موجود تبیین و نتایج آزمایشگاهی اجرای این پروتکل ارائه خواهد شد. در گام آخر به اهمیت و کاربرد شبکه توزیع کلید کوانتومی و توپولوژی این شبکه در بستر فیبر نوری که توسط شرکت توسعه و کاربرد فناوری های نو و پژوهشگاه ارتباطات و فناوری اطلاعات کشور در حال اجراست، خواهیم پرداخت و نحوه کارکرد لایه های مختلف این شبکه ارائه خواهد شد. این کارگاه برای دانشجویان و پژوهشگران حوزه های فناوری های کوانتومی، امنیت سایبری و اپتیک طراحی شده است و شرکت کنندگان در پایان کارگاه، درباره مفاهیم اولیه توزیع کلید کوانتومی و نحوه کارکرد لایه های مختلف شبکه توزیع کلید کوانتومی در حال اجرا در کشور، درک جامعی خواهند داشت.

امنیت شبکه‌های مخابراتی سیار 6G با رویکرد معماری Zero Trust

محمدحسین محمدیان سرچشمه، زهرا آخوداد

مرکز مدیریت راهبردی افتای ریاست جمهوری

توضیحات: با گذار به نسل ششم مخابرات سیار (6G) و معماری دسترسی رادیویی باز (O-RAN)، راهکارهای سنتی امنیت پیرامونی (Perimeter Security) در محیط‌های چندتأمین‌کننده‌ای (Multi-vendor) ناکارآمد هستند. این کارگاه به پیاده‌سازی معماری «عدم اعتماد صفر» (Zero Trust Architecture - ZTA) در شبکه‌های 6G O-RAN می‌پردازد. محورهای اصلی شامل تحلیل سطح حمله در رابط‌های AI، EY و OI، ریزبخش‌بندی پویا (Micro-segmentation) با بهره‌گیری از ایزوله‌سازی امن (Secure Isolation)، و مدل‌سازی نقطه تصمیم‌گیری (Policy Decision Point - PDP) با نقاط اعمال سیاست (Policy Enforcement Point - PEP) توزیع‌شده است. همچنین، کاربرد هوش مصنوعی سبک‌وزن (Lightweight AI) و یادگیری فدرال (Federated Learning) برای ارزیابی پیوسته اعتماد (Continuous Trust) و مهار حملات بلادرنج، نظیر مسموم‌سازی (Poisoning) و نفوذ، بررسی می‌شود. در نهایت، شاخص‌های کلیدی عملکرد (KPI) از جمله تأخیر استنتاج (زیر ۱۰ میلی‌ثانیه) و سربار محاسباتی در کنار چالش‌های پژوهشی تبیین خواهند شد.

امنیت سایبری نتیجه‌محور: از پیامدهای کسب‌وکار تا اعتبارسنجی اثربخشی امنیت

معین فاتحی

مدیریت امن الکترونیکی کاشف

توضیحات: استقرار تجهیزات امنیتی، اجرای ارزیابی‌های فنی و افزایش سطح بلوغ، به‌تنهایی نشان نمی‌دهد که پیامدهای بحرانی حملات سایبری برای سازمان کنترل شده‌اند. این کارگاه با معرفی رویکرد امنیت سایبری نتیجه‌محور، ارتباط میان اهداف کسب‌وکار، رویدادهای غیرقابل تحمل، وابستگی‌های فناوری و شواهد اثربخشی کنترل‌ها را بررسی می‌کند. تمرکز بر تبدیل دغدغه‌های مدیریتی به سناریوهای مشخص و قابل ارزیابی است. مطالب با یک مطالعه موردی ساختگی در خدمات بانکی دنبال می‌شود. شرکت‌کنندگان با راهنمایی مدرس، یک پیامد نامطلوب را تعریف می‌کنند و آستانه اثر، وابستگی‌های کلیدی و معیار اولیه اعتبارسنجی آن را مشخص می‌سازند. تمرکز نسخه فشرده بر درک روش و تکمیل یک کاربرگ کوتاه است. رویکرد ارائه‌شده مکمل مدیریت ریسک و ارزیابی بلوغ است و به محصول یا فروشنده خاصی وابسته نیست.

امن سازی عملی سامانه های سایبر-فیزیکی صنعتی: از شناسایی دارایی تا پیاده سازی کنترل های امنیتی

مهدی صیاد

گروه امنیت سامانه های صنعتی

توضیحات: محیط های صنعتی و سایبر-فیزیکی (CPS/OT) به دلیل ماهیت عملیاتی خود، وابستگی شدیدی به در دسترس بودن (Availability) و ایمنی فیزیکی (Safety) دارند. همگرایی روزافزون شبکه های فناوری اطلاعات (IT) و فناوری عملیاتی (OT) در نسل چهارم صنعت (Industry 4.0)، این زیرساخت ها را در معرض تهدیدات سایبری پیچیده ای قرار داده است که می توانند به خسارات فیزیکی و جانی منجر شوند. این کارگاه تخصصی با تمرکز بر چالش های عملیاتی در محیط های صنعتی واقعی، تلاش می کند فاصله میان تئوری های امنیتی و واقعیت های کف کارخانه را پوشش دهد. با مبنا قرار دادن استانداردهای بین المللی مرجع نظیر سری IEC 62443 و راهنمای NIST SP 800-82، شرکت کنندگان فرایند شناسایی دارایی ها، تحلیل ریسک های سایبر-فیزیکی با متدولوژی های پیامد محور و در نهایت کنترل های دفاعی عمیق در قالب یک نقشه راه امنیت در سازمان خود را فرا می گیرند.

چارچوب مدیریت مخاطرات هوش مصنوعی با متدولوژی AI RMF 1.0

مهرداد جابری

دانشگاه اصفهان

توضیحات: این کارگاه با هدف معرفی مفاهیم اصلی مدیریت ریسک هوش مصنوعی، با تمرکز بر مخاطرات امنیتی در سازمان های IT و با استفاده از چارچوب AI RMF 1.0 برنامه ریزی شده و تجربیات ارائه دهنده در این حوزه مطرح می شود. به این منظور ابتدا مفاهیم کلیدی مدیریت ریسک معرفی شده و سپس به توضیح چارچوب AI RMF 1.0 پرداخته می شود. این کارگاه همچنین قصد دارد مهم ترین مخاطرات موجود در توسعه، چرخه عمر و استفاده از هوش مصنوعی را بررسی نموده و با معرفی مهم ترین ذی نفعان در چرخه عمر هوش مصنوعی، نقش هر یک را در مدیریت مخاطرات آن مطرح نماید. از سوی دیگر، این کارگاه به معرفی چارچوب NIST AI 600 می پردازد که مختص استفاده از هوش مصنوعی مولد (Generative AI) تهیه شده است و مهم ترین مخاطرات امنیتی را در این حوزه معرفی می کند. در انتهای این کارگاه مثال های عملی از ارتباط امن با GAI ارائه می شود.

تهدیدات بدافزاری در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی کشور و راهکارهای مقابله با آنها

دکتر محمدمهدی احمدیان، بهاره ملکی‌راد
شرکت امنان (پیشگامان امن‌پرداز)، گروه شرکت‌های امن‌پرداز

توضیحات: امروزه صنایع کشور، از سیستم‌های کنترلی قابل برنامه‌ریزی نظیر کنترل‌گرهای منطقی برنامه‌پذیر PLC، RTU، DCS و سیستم‌های اسکادا استفاده می‌نمایند. علیرغم پیشرفت‌هایی که در این سیستم‌ها وجود داشته، متأسفانه در عمده صنایع کشور از دیدگاه تهدیدات بدافزاری دارای ضعف‌های بسیاری بوده و همین امر باعث شده که مورد حملات سایبری قرار بگیرند. از آنجا که بروز هرگونه نارسایی در بخش‌های مذکور نه تنها می‌تواند باعث توقف تولید شود، بلکه ممکن است اثرات مخربی نیز بر جای گذارد، از این رو اهمیت شناخت تهدیدات بدافزاری و APT و پیاده‌سازی راهکارهای تدافعی و تهاجمی و بهبود امنیت این سیستم‌ها بیش از پیش احساس می‌شود. در این ارائه به شکل فشرده به اهم موضوعات مرتبط پرداخته خواهد شد و ضمن بررسی نمونه سناریوهای واقعی حملات در کشور، راهکارها و دموهای عملی مرتبط نیز ارائه خواهد شد. این ارائه برای صنایع مختلف کشور نظیر نفت، گاز، پالایش، پتروشیمی، برق، آب، فولاد، مس، سنگ‌آهن، خودروسازی و ... و وزارتخانه‌های مرتبط کاربرد اجرایی خواهد داشت.

مهندسی ایمنی مدل‌های زبانی بزرگ

فاطمه کسانی، صادق دری‌نوگورانی
دانشکده مهندسی برق و کامپیوتر دانشگاه تربیت مدرس

توضیحات: امروزه مدل‌های زبانی بزرگ به مؤلفه فعال در دستیارها و سامانه‌های هوشمند، ابزارهای برنامه‌نویسی و عامل‌های مصنوعی تبدیل شده‌اند و در بسیاری از موارد با پایگاه‌های داده، APIها، حافظه‌های بلندمدت و ابزارهای اجرایی تعامل مستقیم دارند. همین امر سبب شده که مسئله ایمنی (خطرناک نبودن) و امنیت مدل‌های زبانی بزرگ به مسئله‌ای در سطح معماری و مهندسی تبدیل شود. در چنین معماری‌هایی، ورودی کاربر تنها یکی از اجزای اثرگذار بر رفتار سیستم است. دستور، اطلاعات زمینه‌ای، داده‌های بازبازی شده از منابع خارجی، حافظه، ابزارها، APIها و ... همگی می‌توانند بر رفتار سیستم تأثیر بگذارند. مهندسی ایمنی مدل‌های زبانی بزرگ به دنبال طراحی سامانه‌هایی مبتنی بر مدل‌های زبانی است که علاوه بر توانمندی، ایمن، امن، قابل اعتماد و کنترل‌پذیر باشند. در این کارگاه، با مهم‌ترین مفاهیم این حوزه با رویکردی عمل‌گرا و ترکیبی از توضیح نظری و نمونه‌های عملی آشنا می‌شویم و نهایتاً راهکارهای موجود را معرفی می‌کنیم.

مروری بر امنیت موبایل

امیرمحمد کشانی

مدیریت راهبردی افتای ریاست جمهوری

توضیحات: در عصر حاضر، با گسترش روزافزون استفاده از دستگاه‌های هوشمند در زندگی فردی و سازمانی، امنیت برنامه‌ها و زیرساخت‌های موبایل به یکی از حیاتی‌ترین چالش‌های حوزه امنیت سایبری تبدیل شده است. این ارائه به بررسی جامع پلتفرم‌های اصلی موبایل (اندروید و iOS)، معماری امنیتی آن‌ها و محبوب‌ترین بردارها و تکنیک‌های حمله می‌پردازد. در ادامه، روش‌های اصلی ارزیابی امنیتی اعم از تحلیل ایستا و دینامیک، تحلیل رفتار برنامه‌ها در زمان اجرا (Runtime Hooking)، ابزارهای کاربردی حوزه مهندسی معکوس و نیز تهدیدات نوظهور مورد بحث قرار می‌گیرند. هدف این ارائه، ایجاد یک دیدگاه ساختاریافته و کاربردی از امنیت موبایل برای متخصصان و علاقه‌مندان جهت شناسایی، تحلیل و مقابله با آسیب‌پذیری‌های رایج است.

فرار از سندباکس: رده‌بندی سیستماتیک حملات تزریق پرامپت، راهکارهای کاهش تهدیدات و چالش‌های باز در استقرار امن LLM

رضا ابراهیمی آتانی، سیدامیرحسین طباطبایی، کیارش داودی‌پور، عسل محمودی‌نژاد

گروه‌های مهندسی و علوم کامپیوتر دانشگاه گیلان

توضیحات: حملات تزریق پرامپت به‌عنوان مهم‌ترین آسیب‌پذیری سیستم‌های مبتنی بر مدل‌های زبانی بزرگ (LLM) در رتبه‌بندی OWASP در سال ۲۰۲۵ معرفی شده است. این کارگاه به بررسی جامع این تهدید نوظهور در حوزه امنیت هوش مصنوعی می‌پردازد. شرکت‌کنندگان با رده‌شناسی کامل حملات تزریق پرامپت شامل حملات مستقیم، غیرمستقیم، چندوجهی، بهره‌برداری از ابزارها و عوامل هوشمند، و تکنیک‌های زنجیره‌ای آشنا می‌شوند. در این کارگاه با پیاده‌سازی عملی برخی حملات بر روی سیستم‌های واقعی هوش مصنوعی عامل‌محور، چالش‌ها و نقاط شکست در طراحی و استقرار سیستم‌های مزبور نمایش داده می‌شوند. همچنین راهکارهای دفاعی موجود از جمله پیش‌پردازش ورودی، دفاع‌های معماری و روش‌های تشخیص مورد بررسی قرار می‌گیرد. این کارگاه با ارائه مطالعات موردی از حملات واقعی و بررسی چالش‌های پژوهشی باز، به شرکت‌کنندگان کمک می‌کند تا درک عمیقی از این تهدید و راه‌های مقابله با آن پیدا کنند. کارگاه به‌صورت نظری-عملی طراحی شده و شامل جلسات پرسش و پاسخ و بحث گروهی می‌باشد.

روش‌های تحلیل و ارزیابی امنیتی فریمور در سامانه‌های نهفته

مسعود زبوری اخلاص

پژوهشکده علوم و فناوری انرژی شریف

توضیحات: فریمور نقش مستقیمی در کنترل و راهاندازی سخت‌افزار و پیاده‌سازی قابلیت‌های امنیتی تجهیزات دارد. از این رو، تحلیل فریمور می‌تواند اطلاعات ارزشمندی درباره ساختار، رفتار و سطح امنیت یک تجهیز فراهم کند. این تحلیل علاوه بر بررسی سازوکارهایی مانند یکپارچگی، اصالت و زنجیره اعتماد، امکان شناسایی ضعف‌های امنیتی موجود در کد و پیکربندی فریمور را نیز فراهم می‌سازد. در این کارگاه، با رویکردی عملی، روش‌های مختلف تحلیل و ارزیابی امنیتی، از جمله استخراج فریمور، بررسی کد و شناسایی آسیب‌پذیری، معرفی می‌شود. شرکت‌کنندگان با ابزارهایی مانند Ghidra و مفاهیمی از جمله ارزیابی ایستا و پویای فریمور، سازوکارهای اصالت‌سنجی و شبیه‌سازی فریمور آشنا شده و نمونه‌هایی از روش‌های شناسایی و تحلیل ضعف‌های امنیتی در فریمور را بررسی خواهند کرد.

تحلیل ساختار فایل‌های اجرایی ویندوز، مهندسی معکوس و تحلیل هوشمند بدافزار

رسول کیانی، سجاد رضائی

مرکز مدیریت راهبردی افتای ریاست جمهوری

توضیحات: فایل‌های اجرایی سیستم‌عامل ویندوز، هسته اصلی اجرای نرم‌افزارها، سرویس‌ها و همچنین بدافزارها را تشکیل می‌دهند. درک عمیق ساختار درونی این فایل‌ها و نحوه تعامل آن‌ها با سیستم‌عامل، نقش کلیدی در فهم مسائل امنیت سایبری، تحلیل بدافزار، فارنزیک دیجیتال، مهندسی معکوس و کشف تهدیدات پیشرفته دارد. این کارگاه آموزشی با رویکردی کاربردی، به بررسی کامل ساختار فایل‌های اجرایی ویندوز از سطح باینری تا سطح اجرا در حافظه می‌پردازد و شرکت‌کنندگان را با فرآیندهای تحلیل استاتیک و تحلیل پویا، نحوه بارگذاری فایل‌ها در حافظه، استخراج اطلاعات ساختاری، و شناسایی رفتارهای مشکوک آشنا می‌کند.

شکار تهدید در شبکه‌های صنعتی (Threat Hunting in OT Networks)

زهره عظیمی

مرکز مدیریت راهبردی افتا ریاست جمهوری

توضیحات: با گسترش تهدیدات سایبری علیه سامانه‌های کنترل صنعتی، شناسایی و تحلیل رفتار مهاجمان پیش از ایجاد اختلال در فرایند صنعتی اهمیت ویژه‌ای دارد. در این کارگاه ابتدا مفهوم اطلاعات منبع باز (OSINT) و کاربرد آن در شناسایی تهدیدات سایبری صنعتی معرفی می‌شود. سپس چارچوب بین‌المللی MITRE ATT&CK for ICS به‌عنوان یکی از مراجع مهم برای شناخت تاکتیک‌ها و تکنیک‌های مورد استفاده مهاجمان در شبکه صنعتی بررسی خواهد شد. در ادامه، با استفاده از یک مطالعه موردی واقعی، رفتار مهاجم به این چارچوب نگاشت خواهد شد. در بخش عملی کارگاه، شرکت‌کنندگان با استفاده از شواهد ترافیک شبکه و ابزارهایی نظیر Wireshark، یک سناریوی شکار تهدید در شبکه صنعتی را در قالب حل چالش‌ها بررسی خواهند کرد. هدف این چالش‌ها، ایجاد درک عملی از فرایند شکار تهدید در شبکه‌های صنعتی است.

از تحلیل بدافزار و شکار تهدید تا کشف آسیب پذیری: هوش مصنوعی در امنیت سایبری

حسین کرمی
امن پرداز

توضیحات: در عصر حاضر، هوش مصنوعی پارادایم امنیت سایبری را به شکلی بنیادین تغییر داده و به ابزاری قدرتمند و دوگانه در دست مدافعان و مهاجمان تبدیل شده است. این کارگاه به طور اختصاصی بر نقش کلیدی و تحول آفرین هوش مصنوعی در تمام ابعاد امنیت سایبری تمرکز دارد و با کالبدشکافی دقیق رفتار بدافزارها و تحول متدولوژی های تشخیص از روش های سنتی مبتنی بر امضا به روش های مدرن مبتنی بر رفتار و ناهنجاری می پردازد. شرکت کنندگان در این دوره کاربردی یاد می گیرند که چگونه از ابزارها و مدل های هوش مصنوعی برای تحلیل سریع فایل های مشکوک، مهندسی معکوس و همچنین کشف خودکار آسیب پذیری ها در سورس کد نرم افزارها بهره ببرند. در سمت مقابل، کارگاه به جنبه های تاریک فناوری نیز پرداخته و نحوه استفاده مهاجمان از هوش مصنوعی را برای تولید بدافزارهای پیچیده و خودتطبیق پذیر، دور زدن مکانیزم های دفاعی و اجرای حملات مهندسی اجتماعی فوق العاده طبیعی (مانند فیشینگ هدفمند و جعل هویت) تحلیل می کند. در نهایت، الگوریتم ها و قابلیت های هوش مصنوعی به کاررفته در سامانه های EDR جهت الگوشناسی و شکار تهدیدات پیشرفته تبیین می شود.

فرضیه تهدید: تبدیل تهدیدات به سناریوهای قابل تشخیص و آزمون

وحید خدابخشی، سجاد زیادریور
مدیریت امن الکترونیکی کاشف، شاپرک

توضیحات: در فضای امنیت سایبری، اتکا به شاخص های پراکنده کننده مانند IP، دامنه یا هش فایل به تنهایی برای شناسایی تهدیدات پیشرفته کافی نیست. سازمان ها نیاز دارند تهدیدات را به شکل سناریوهای قابل فهم، قابل اندازه گیری و قابل آزمون تحلیل کنند. مفهوم Threat Hypothesis یا «فرضیه تهدید» دقیقاً با همین هدف مطرح می شود؛ یعنی تبدیل دانش تهدید، رفتار مهاجم و دارایی های حیاتی سازمان به فرضیه هایی که بتوان آن ها را در محیط واقعی جست و جو، اعتبارسنجی و به کنترل های دفاعی تبدیل کرد. در این ارائه، مفهوم Threat Hypothesis، اجزای اصلی آن و ارتباط آن با MITRE ATT&CK، Threat Hunting، Threat Intelligence و Threat-Informed Detection Engineering بررسی می شود. همچنین نشان داده می شود که چگونه یک فرضیه تهدید می تواند از یک نگرانی کلی امنیتی به یک سناریوی عملیاتی شامل دارایی هدف، مسیر حمله، تکنیک مهاجم، شواهد لاگ، منطق کشف و روش آزمون تبدیل شود. هدف اصلی این ارائه، تبیین نقش فرضیه تهدید در دفاع سایبری تهدیدمحور است؛ رویکردی که به تیم های امنیتی کمک می کند به جای واکنش صرف به رخدادها، به صورت پیش دستانه تهدیدات محتمل را شناسایی، کشف و اعتبارسنجی کنند و شکاف های دفاعی سازمان را بهبود دهند.

معرفی زیست‌بوم فناوری تهدیدات شناختی و امنیت نرم

بهرز ترک‌لادانی، امین محمدیان، هانی ربیعی

دانشگاه اصفهان، پژوهشگاه توسعه فناوری‌های پیشرفته و هسته تخصصی تهدیدات شناختی و امنیت نرم

توضیحات: امروزه امنیت سایبری تنها یک موضوع فنی نیست، بلکه حوزه‌ای پیچیده و چندبعدی است که ابعاد فیزیکی، اجتماعی و انسانی را دربرمی‌گیرد. رشد هوش مصنوعی و شبکه‌های اجتماعی، فرصت‌ها و تهدیدهای گسترده فرهنگی، اجتماعی، اقتصادی و سیاسی پدید آورده است. در این میان، کانون تهدیدها از آسیب‌پذیری‌های فنی به حوزه شناختی و مهندسی اجتماعی پیشرفته جابه‌جا شده و هدف حملات از ماشین‌ها و زیرساخت‌ها به ذهن و رفتار انسان تغییر یافته است. از این‌رو، ابزارهای سنتی مانند رمزنگاری، دیواره آتش و ضدویروس به‌تنهایی کافی نیستند و دفاع از ادراک، قضاوت، تصمیم‌گیری و باور انسان‌ها نیز ضروری است؛ همان چیزی که امنیت نرم نامیده می‌شود. این کارگاه به معرفی زیست‌بوم فناوری تهدیدات شناختی و امنیت نرم، مبانی و فناوری‌های کلیدی، راهکارهای مقابله و وضعیت پژوهش و بازار جهانی می‌پردازد و بر ضرورت آماده‌سازی پژوهشگران، سرمایه‌گذاری شرکت‌های فناوری و سیاست‌گذاری ملی تأکید می‌کند.

آناطومی یک حمله: تشریح یک عملیات APT هدفمند با سوءاستفاده از آسیب‌پذیری Zero-Day در تجهیزات ذخیره‌سازی

علی امینی
گراف

توضیحات: در حملات پیشرفته سایبری جدید علیه زیرساخت‌های حیاتی، مهاجمین از رمز سیستم‌عامل عبور کرده و به لایه‌های عمیق‌تر، از جمله Firmware تجهیزات ذخیره‌سازی، رسیده‌اند. فریمور به‌عنوان نقطه اتصال بین سخت‌افزار و نرم‌افزار، به یکی از اهداف اصلی گروه‌های APT تبدیل شده است؛ چراکه نفوذ در این لایه، امکان کنترل کامل سیستم و نابودی غیرقابل‌بازگشت را فراهم می‌کند. امنیت فریمور، به‌عنوان لایه‌ای زیرین و حیاتی در زیرساخت‌ها، اغلب از دیدگاه امنیت سایبری نادیده گرفته می‌شود و همین امر جذابیت این لایه را برای مهاجمان بیشتر کرده است. این کارگاه بر پایه یک مطالعه حمله واقعی از یک گروه APT طراحی شده است. حمله‌ای که در آن مهاجم با بهره‌برداری از یک آسیب‌پذیری Zero-Day و ترکیب آن با تکنیک‌هایی مانند تزریق کد، ارسال دستورات مستقیم SCSI و Exploit آسیب‌پذیری موجود در Stack، زنجیره‌ای را برای نابودی و در نهایت از مدار خارج کردن تجهیزات لایه ذخیره‌سازی اجرا می‌کند.

اطلاعات کارگاه‌ها

برنامه زمان‌بندی کارگاه‌های آموزشی در روز دوشنبه، ۲۷ مهرماه ۱۴۰۵
محل برگزاری: دانشکده ریاضی و علوم کامپیوتر دانشگاه صنعتی امیرکبیر

ساعت	۹:۳۰ - ۸:۰۰	۱۱:۳۰ - ۱۰:۰۰	۱۳:۰۰ - ۱۴:۳۰	۱۵:۰۰ - ۱۶:۳۰
مشخصات کارگاه‌ها	عنوان کارگاه	هوش مصنوعی و امنیت سایبری	از مدل‌های زبانی تا عامل‌های هوشمند در جرم‌یابی دیجیتال	Federated RAG: استفاده از دانش چند منبع بدون تجمیع اطلاعات
	ارائه‌دهنده	رویال پرداز	پژوهشگاه توسعه فناوری‌های پیشرفته	پژوهشگاه توسعه فناوری‌های پیشرفته
	عنوان کارگاه	فراتر از KYC: نبرد مهاجم عامل‌محور و عامل‌محور برای اعتبارسنجی هویت و رفتار در بانکداری دیجیتال	مهندسی امنیتی زیرساخت‌های مبتنی بر Kubernetes	تحلیل رمز خودکار رمزهای متقارن: مدل‌سازی قیودی و پیاده‌سازی عملی
	ارائه‌دهنده	شرکت توسعه فناوری رفاه پردیس (وابسته به بانک رفاه کارگران)	شرکت خدمات انفورماتیک	پژوهشگاه توسعه فناوری‌های پیشرفته
	عنوان کارگاه	امنیت اینترنت اشیا: چالش‌ها، تهدیدها و راهکارهای حفاظت از سامانه‌های متصل	بررسی چالش‌های امنیتی کنترل دسترسی ارتباطات بلادرنگ در شبکه‌های اینترنت اشیا صنعتی	آمادگی و تاب‌آوری نظام بانکی در عصر کوانتوم: از تهدیدات رمزنگاری تا نقشه راه گذار به امنیت کوانتومی
	ارائه‌دهنده	هسته تخصصی رمزنگاری و پروتکل امن، پژوهشگاه توسعه فناوری‌های پیشرفته	پژوهشگاه ارتباطات و فناوری اطلاعات	شرکت خدمات انفورماتیک
	عنوان کارگاه	سیستم‌ها و شبکه‌های توزیع کلید کوانتومی	سیستم‌ها و شبکه‌های توزیع کلید کوانتومی	شکاف اعتماد: درآمدی بر معماری امنیت در دنیای بدون رمز
	ارائه‌دهنده	شرکت تک فن	شرکت تک فن	دانشگاه شاهد

برنامه زمان‌بندی کارگاه‌های آموزشی در روز سه شنبه، ۲۸ مهرماه ۱۴۰۵
محل برگزاری: دانشکده ریاضی و علوم کامپیوتر دانشگاه صنعتی امیرکبیر

ساعت	۸:۰۰ - ۹:۳۰	۱۰:۳۰ - ۱۱:۳۰	۱۳:۰۰ - ۱۴:۳۰	۱۵:۳۰ - ۱۶:۳۰
مشخصات کارگاه‌ها	عنوان کارگاه	امنیت شبکه‌های مخابراتی سیار 5G با رویکرد معماری Zero Trust	مروری بر امنیت موبایل	تحلیل ساختار فایل‌های اجرائی ویندوز، مهندسی معکوس و تحلیل هوشمند بدافزار (نیازمند لپ‌تاپ)
	ارائه‌دهنده	مرکز مدیریت راهبردی افتای ریاست جمهوری	مدیریت راهبردی افتای ریاست جمهوری	افتا
	عنوان کارگاه	مهندسی ایمنی مدل‌های زبانی بزرگ	فرار از سندباکس: رده‌بندی سیستماتیک حملات تزریق پرامپت، راهکارهای کاهش تهدیدات و چالش‌های باز در استقرار امن LLM	چارچوب مدیریت مخاطرات هوش مصنوعی با متدولوژی AI RMF 1.0
	ارائه‌دهنده	دانشکده مهندسی برق و کامپیوتر دانشگاه تربیت مدرس	گروه‌های مهندسی و علوم کامپیوتر دانشگاه گیلان	دانشگاه اصفهان
	عنوان کارگاه	تهدیدات بدافزاری در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی کشور و راهکارهای مقابله با آن‌ها	روش‌های تحلیل و ارزیابی امنیتی فریمور در سامانه‌های هفته	امن‌سازی عملی سامانه‌های سایبرفیزیکی صنعتی: از شناسایی دارایی و تحلیل ریسک تا پیاده‌سازی کنترل‌های امنیتی
	ارائه‌دهنده	شرکت امان (پیشگامان امن آرمان)	پژوهشکده علوم و فناوری‌های انرژی شریف	گروه امنیت سامانه‌های صنعتی
	عنوان کارگاه	آناطومی یک حمله: تشریح یک عملیات APT هدفمند با سوءاستفاده از آسیب‌پذیری Zero-Day در تجهیزات ذخیره‌سازی	فرضیه تهدید: تبدیل تهدیدات به سناریوهای قابل تشخیص و آزمون	از تحلیل بدافزار و شکار تهدید تا کشف آسیب‌پذیری: هوش مصنوعی در امنیت سایبری
	ارائه‌دهنده	شرکت گراف	شرکت شاپرک	امن‌پرداز
	عنوان کارگاه	معرفی زیست‌بوم فناوری تهدیدات شناختی و امنیت نرم	معرفی زیست‌بوم فناوری تهدیدات شناختی و امنیت نرم	افتا
	ارائه‌دهنده	دانشگاه اصفهان، پژوهشگاه توسعه فناوری‌های پیشرفته - هسته تخصصی تهدیدات شناختی و امنیت نرم	دانشگاه اصفهان، پژوهشگاه توسعه فناوری‌های پیشرفته - هسته تخصصی تهدیدات شناختی و امنیت نرم	

نتایج ارزیابی رساله‌های دکتری به شرح ذیل تصمیم‌گیری گردیدند نتایج ارزیابی رساله‌های دکتری به شرح ذیل تصمیم‌گیری گردید

برترین‌ها

رساله‌های برتر

نتایج ارزیابی رساله‌های دکتری به شرح ذیل تصمیم‌گیری گردید:

ردیف	نام و نام خانوادگی	دانشگاه محل تحصیل	استاد (اساتید) راهنما	رتبه‌بندی
۱	محمد مهدی مدبری	صنعتی شریف	دکتر محمود سلماسی‌زاده ، دکتر جواد مهاجری	شایسته تقدیر
۲	پرچهر دادخواه	صنعتی اصفهان	دکتر سید محمد دخیل علیان	شایسته تقدیر
۳	زهرا عظیمی	صنعتی امیرکبیر	دکتر احمد افشار	شایسته تقدیر
۴	سعادت ایزدی	رازی	دکتر محمود احمدی	شایسته تقدیر

پایان‌نامه‌های برتر

نتایج ارزیابی پایان‌نامه کارشناسی ارشد به شرح ذیل تصمیم‌گیری گردید:

ردیف	نام و نام خانوادگی	دانشگاه محل تحصیل	استاد (اساتید) راهنما	رتبه‌بندی
۱	مهدی ابری	اصفهان	دکتر مجتبی رفیعی	برتر
۲	علیرضا جواد	علوم پایه زنجان	دکتر پیمان پهلوانی ، دکتر صادق صادقی	شایسته تقدیر
۳	امیرحسین صفری	علوم پایه زنجان	دکتر پیمان پهلوانی ، دکتر صادق صادقی	شایسته تقدیر
۴	محمود قربانی فرد	تربیت دبیر شهید رجایی	دکتر معصومه صفخانی	شایسته تقدیر
۵	فاطمه‌السادات سیدقاسمی	اصفهان	دکتر مجتبی رفیعی	شایسته تقدیر

شاخه‌های دانشجویی برتر

شاخه رتبه اول مشترک – دانشگاه گیلان

- مسئول شاخه: دکتر رضا ابراهیمی آتانی
- اعضا: آبتین حسین‌نژاد، امیرحسین باقرنیا، هیراد آذرنوش، فاطمه صحرایی، امیرسعید بلارک، عرفان مجتبی‌زاده و سینا نظمی

شاخه رتبه اول مشترک – دانشگاه اصفهان

- نماینده انجمن و مسئول شاخه: دکتر بهروز ترک‌لادانی
- اعضا: تیمام موسوی‌سجاد، محمدصادق جیحانی، محسن مشرفی، محمدمتین عباسی، سبحان واعظزاده، جواد مرادی و سپهر رجبی

شاخه رتبه دوم – دانشگاه صنعتی شریف

- نماینده انجمن و مسئول شاخه: دکتر سیاوش احمدی
- نماینده انجمن: فریدوش حامدنژاد، محمدصادق احمدی، علیرضا انصاری، حمیدرضا دست‌آبادی، ندا نجاری، الناز دانیال و محمد دیباجی

کافه امید و اشتغال

در حاشیه کنفرانس رمز و امنیت داده، «کافه امید و اشتغال» با هدف ایجاد ارتباطی مؤثر میان دانشگاه و صنعت و فراهم کردن بستری برای تعامل مستقیم میان متخصصان، دانشجویان، مدیران و کارآفرینان حوزه امنیت داده برگزار می‌شود. در ادامه، نام شرکت‌های مشارکت‌کننده در بخش کافه امید و اشتغال آمده است.

- توسعه امن کیان (تاکیان)
- فناوری راه نو (سورین)
- گراف
- ناد
- سبا پردازش
- امن پرداز
- گروه رایانه‌ای تدبیر پرداز
- توسعه و کاربرد فناوری‌های نو (تکفن)
- ابر آروان
- سیگما
- هاست ایران
- رویال پرداز تیام
- دیجی کالا
- پیام‌پرداز
- مهسان - حامی برنزی
- شاپرک - حامی طلایی
- پژوهشگاه ارتباطات و فناوری اطلاعات - حامی طلایی
- صنایع الکترونیک زعیم - حامی طلایی
- فراز ارتباط - حامی طلایی
- متیران
- پارک علم و فناوری دانشگاه امیرکبیر