انجمن رمز ایران
Iranian Society of Cryptology

دانشگاه شهید بهشتی
Cyberspace Research Institute

موضوعات کنفرانس:

- مبانی رمزشناسی، طراحی و تحلیل رمز، نهان‌سازی اطلاعات
- امنیت شبکه، پروتکل‌های امنیتی، امنیت کلان داده و ابر
- امنیت سخت‌افزار و نرم‌افزار، تحلیل بدافزار
- امنیت سامانه‌های سیار، سایبرفیزیکی و اینترنت اشیاء
- کنترل دسترسی، فناوری‌های ارتقای حریم خصوصی
- مهندسی امنیت و امنیت خدمات الکترونیکی
- امنیت نرم، امنیت هوش مصنوعی
- زنجیره قالب‌ها و رمزارزها
- جرم‌یابی دیجیتال
- مقاله‌های کوتاه علمی-صنعتی

بیست و دومین کنفرانس بین‌المللی انجمن رمز ایران

در امنیت اطلاعات و رمزشناسی

کتابچه راهنمای کنفرانس

تاریخ‌های مهم کنفرانس

فراخوان اول (پائیز ۱۴۰۳)
- مهلت ارسال مقالات: ۱ بهمن ۱۴۰۳
- اعلام نتایج داوری فراخوان پائیز: ۱۵ اسفند ۱۴۰۳

فراخوان دوم (بهار ۱۴۰۳)
- مهلت ارسال مقالات: ۱۰ تیرماه ۱۴۰۴
- اعلام نتایج داوری فراخوان بهار: اول شهریورماه ۱۴۰۴

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

- ۱۶ و ۱۷ مهرماه ۱۴۰۴
- پژوهشکده فضای مجازی
- دانشگاه شهید بهشتی - تهران

ISeCure

امضای دیجیتال مبتنی بر هویت

بسم الله الرحمن الرحیم

کتابچه راهنمای
بیست و دومین کنفرانس بین‌المللی
انجمن رمز ایران در امنیت اطلاعات و رمزشناسی

برگزار کننده:

گروه امنیت شبکه و رمزنگاری،

پژوهشکده فضای مجازی، دانشگاه شهید بهشتی

محل برگزاری:

دانشگاه شهید بهشتی

مهرماه ۱۴۰۴ خورشیدی

فهرست مطالب

دبیرخانه دائمی کنفرانس‌های انجمن رمز ایران:

تهران، خیابان آزادی، غرب دانشگاه صنعتی شریف، خیابان شهید صادقی، پلاک ۲۶، طبقه ۴، واحد ۱۶

تلفن: ۶۶۰۸۸۱۳۵ - ۰۲۱

رایانامه: info@isc.org.ir, iscisc2024@isc.org.ir

وبگاه: https://www.isc.org.ir

دبیرخانه کنفرانس در دانشگاه شهید بهشتی:

تهران، ولنجک، دانشگاه شهید بهشتی، ساختمان شهدا، طبقه دوم، پژوهشکده فضای مجازی

تلفن: ۲۹۹۰۵۴۷۰– ۰۲۱

رایانامه: **iscisc2025@sbu.ac.ir**

وبگاه: **https://iscisc2025.sbu.ac.ir**

محل برگزاری:

تهران، ولنجک، دانشگاه شهید بهشتی، مرکز همایش‌های بین‌المللی دانشگاه شهید بهشتی

پیشگفتار

بیست و دومین کنفرانس بین‌المللی انجمن رمز ایران در امنیت اطلاعات و رمزشناسی امسال در دانشگاه شهید بهشتی برگزار می‌شود، که یادآور شهدای دانشمند و نخبه کشور به‌خصوص در جنگ تحمیلی ۱۲ روزه است.

سلام خدا بر ایشان روزی که متولد شدند و سلام خدا بر ایشان روزی که به شهادت رسیدند و سلام بر ایشان روزی که مبعوث خواهند شد. اَللّهُمّ ارْزُقْنا توفیق الشّهادَه فِی سَبِیلِکَ.

این کنفرانس فرصتی بی‌نظیر برای تبادل‌نظر و ارائهٔ دستاوردهای علمی در زمینه‌های مختلف امنیت اطلاعات و رمزشناسی محسوب می‌شود. در این دوره از کنفرانس، در دو فراخوان پاییز و بهار موفق به دریافت ۱۳۱ مقاله از پژوهشگران عزیز شدیم که از این تعداد، ۴۵ مقاله با کیفیت پس از داوری‌های متعدد برای ارائهٔ در کنفرانس انتخاب شدند. مقالات پذیرفته‌شده در محورهای متنوعی از جمله هوش مصنوعی و امنیت، جرم‌یابی دیجیتال، مبانی رمزشناسی، پیاده‌سازی الگوریتم‌های رمزنگاری، نهان‌سازی اطلاعات، امنیت شبکه، مدیریت امنیت و حریم خصوصی، امنیت محاسبات، پروتکل‌های امنیتی و همچنین مقالات کوتاه علمی-صنعتی پذیرفته‌شده‌اند.

از نکات درخور توجه این دوره، مشارکت بین‌المللی پژوهشگران است. امسال، از نویسندگانی از کشورهای هند، بلژیک، سنگال، دانمارک، هلند، انگلستان، کانادا، مکزیک، آلمان، فرانسه و قبرس مقالاتی به کنفرانس ارسال شد. مقالات پذیرفته‌شده در ۱۰ نشست تخصصی به بحث و بررسی گذاشته خواهند شد و همچنین شاهد سخنرانی‌های کلیدی از محققان برجستهٔ ایرانی و خارجی خواهیم بود. به‌علاوه، پنل تخصصی و نشست هم‌اندیشی با مدیران مرکز مدیریت راهبردی افتا فرصتی برای تبادل‌نظر و هم‌فکری خواهد بود.

در بیست‌ودومین کنفرانس بین‌المللی انجمن رمز، در جهت پیوند جدی‌تر صنعت و جامعهٔ علمی کشور، دو برنامهٔ ویژه با عناوین کافه اشتغال، و نشست ارائه‌های برق‌آسا در نظر گرفته شده است. رویداد کافهٔ اشتغال، بهترین فرصت برای دیدار مستقیم با بیش از ۲۵ شرکت و مرکز تحقیقاتی پیشرو در حوزهٔ امنیت و فناوری اطلاعات را با جامعهٔ علمی و دانشگاهی کشور فراهم می‌آورد. در این رویداد شرکت‌ها در فضایی صمیمی و حرفه‌ای با علاقه‌مندان گفت‌وگو می‌کنند، مصاحبه‌های اولیه و شناسایی استعدادهای جدید صورت می‌گیرد و فرصت‌های شغلی و همکاری‌های پژوهشی معرفی می‌شوند. کافهٔ اشتغال، فرصتی ارزشمند برای آغاز همکاری‌های حرفه‌ای و پیوند میان دانشگاه، صنعت و نخبگان جوان است. در نشست ارائه‌های برق‌آسا شرکت‌های منتخب در قالب ارائه‌هایی کوتاه و پویا، توانمندی‌ها، مسیرهای شغلی و نیازهای فناورانهٔ خود را معرفی خواهند کرد.

ما بر این باوریم که کنفرانس بین‌المللی انجمن رمز ایران در امنیت اطلاعات و رمزشناسی می‌تواند بستری مناسب برای ارتقای دانش و تبادل تجربیات میان پژوهشگران باشد که در نهایت به رشد و پیشرفت صنعت افتای کشور عزیزمان منجر خواهد شد. ان‌شاءالله سال آینده با کمک و همت پژوهشگران و صنعتگران عزیز، شاهد ارسال مقالات بیشتر و باکیفیت‌تر و مشارکت بیشتر و سازنده‌تر بخش‌های مختلف صنعت‌افتا خواهیم بود.

با آرزوی موفقیت برای همه علاقمندان،

دبیران علمی بیست و دومین کنفرانس انجمن رمز
ایران در امنیت اطلاعات و رمزشناسی
حمید ملا، معصومه صفخانی

برگزارکنندگان و حامیان

برگزارکنندگان

انجمن رمز ایران
Iranian Society of Cryptology

دانشگاه شهید بهشتی
Shahid Beheshti University

حامیان معنوی

ISC
Islamic World Science Citation Center

IEEE
IRAN SECTION

ECOSF

ISeCure

انجمن رمز ایران
Iranian Society of Cryptology

دانشگاه شهید بهشتی
Shahid Beheshti University

انجمن کامپیوتر ایران
Computer Society of Iran

پژوهشکده
فضای مجازی

Union of Iranian Societies of Mathematical Sciences

حامیان مالی

حامیان طلایی ویژه

حامی طلایی

حامیان نقره‌ای

حامیان برنزی

ساختار سازمانی کنفرانس

رئیس کنفرانس: دکتر سید محمودرضا آقامیری، استاد تمام دانشکده مهندسی هسته‌ای، دانشگاه شهید بهشتی

دبیر کمیته علمی کنفرانس:

- دکتر حمید ملا، دانشیار دانشکده مهندسی برق و کامپیوتر، دانشگاه اصفهان
- دکتر معصومه صفخانی، دانشیار دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی

دبیر کمیته اجرایی کنفرانس:

- دکتر هادی سلیمانی، دانشیار پژوهشکده فضای مجازی، دانشگاه شهید بهشتی
- دکتر فرخ‌لقا معظمی، استادیار پژوهشکده فضای مجازی، دانشگاه شهید بهشتی

کمیته علمی (مرتب شده با نام خانوادگی به ترتیب حروف الفبا):

- **دکتر رضا ابراهیمی آتانی- دانشگاه گیلان (مسئول محور و نشست)**
- **دکتر محمود احمدیان عطاری- دانشگاه صنعتی خواجه نصیرالدین طوسی(مسئول نشست)**
- **دکتر زهرا احمدیان- دانشگاه شهید بهشتی(مسئول نشست)**
- **دکتر محمد علی اخایی- دانشگاه تهران (مسئول نشست)**
- **دکتر ترانه اقلیدس- دانشگاه صنعتی شریف (مسئول محور و نشست)**
- دکتر بهزاد اکبری نودوزقی- دانشگاه تربیت مدرس
- دکتر هاله امین طوسی- دانشگاه فردوسی مشهد
- **دکتر مرتضی امینی- دانشگاه صنعتی شریف (مسئول محور و نشست)**
- **دکتر مهدی آبادی- دانشگاه تربیت مدرس(مسئول نشست)**
- **دکتر نصور باقری- دانشگاه تربیت دبیر شهید رجایی (مسئول محور)**
- دکتر مجید بیات- دانشگاه شاهد
- **دکتر محمد حسام تدین- پژوهشگاه ارتباطات و فناوری اطلاعات (مسئول محور و نشست)**
- **دکتر بهروز ترک لادانی- دانشگاه اصفهان (مسئول محور و نشست)**
- **دکتر علی جهانیان- دانشگاه شهید بهشتی (مسئول محور)**
- دکتر محمد دخیل علیان- دانشگاه صنعتی اصفهان
- دکتر شهرام خزائی- دانشگاه صنعتی شریف
- **دکتر صادق دری نوگورانی- دانشگاه تربیت مدرس (مسئول نشست)**
- دکتر مطهره دهقان- دانشگاه تربیت مدرس
- دکتر پروین رستگاری- دانشگاه صنعتی اصفهان
- **مهندس حبیب رستمی- سازمان جهاد دانشگاهی صنعتی شریف (مسئول نشست)**
- **دکتر راضیه سالاری فرد- دانشگاه شهید بهشتی (مسئول نشست)**
- دکتر مهدی سجادیه- دانشگاه آزاد اسلامی واحد اصفهان

- **دکتر محمود سلماسی زاده- دانشگاه صنعتی شریف (مسئول محور)**
- دکتر مهران سلیمان فلاح- دانشگاه صنعتی امیرکبیر
- **دکتر هادی سلیمانی- دانشگاه شهید بهشتی (مسئول محور)**
- **دکتر هادی شهریار شاه حسینی- دانشگاه علم و صنعت ایران (مسئول نشست)**
- دکتر سعید شکرالهی-دانشگاه شهید بهشتی
- دکتر حمیدرضا شهریاری- دانشگاه صنعتی امیرکبیر
- دکتر معصومه صفخانی- دانشگاه تربیت دبیر شهید رجایی
- دکتر محمدرضا عارف- دانشگاه صنعتی شریف
- دکتر محمد عبدالهی ازگمی- دانشگاه علم و صنعت ایران
- **دکتر بیژن علیزاده- دانشگاه تهران (مسئول نشست)**
- دکتر جواد علیزاده- دانشگاه جامع امام حسین (ع)
- دکتر عباس قائمی بافقی- دانشگاه فردوسی مشهد
- دکتر فرخ لقا معظمی-دانشگاه شهید بهشتی
- دکتر وحیده مقتدایی-دانشگاه شهید بهشتی
- **دکتر حمید ملا- دانشگاه اصفهان (مسئول محور)**
- **مهندس جواد مهاجری- دانشگاه صنعتی شریف (مسئول نشست)**
- دکتر عبدالرسول میرقدری- دانشگاه امام حسین (ع)
- دکتر محمودرضا هاشمی- دانشگاه تهران
- **دکتر محمدرضا هوشمند اصل- دانشگاه محقق اردبیلی**
- **دکتر محسن رمضای یارندی-پژوهشگاه توسعه فناوری های پیشرفته (مسئول نشست)**

- Dr. Mahtab Mirmohseni- University of Surrey, UK
- Dr. Jose L. Muñoz Tapia- Universidad Politécnica de Catalunya, Spain
- Dr. Joachim Posegga- University of Passau, Germany
- Dr. Vincent Rijmen- KU Leuven, Belgium

مسئول کارگاه‌های آموزشی و ثبت نام: دکتر وحیده مقتدایی، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی
مسئول کمیته ارتباط با صنعت و کافه اشتغال: دکتر بهار فراهانی، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی
مسئول تدوین و آماده‌سازی کتابچه راهنما: خانم سحر حبیبی، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی
ویراستار علمی و ادبی کتابچه راهنمای کنفرانس: خانم دکتر معصومه صفخانی، دانشگاه تربیت دبیر شهید رجایی
مسئول کمیته ضبط و انتشار ویدئوها: محمد مهدی نیک‌بین
کارشناس معاونت پژوهشی دانشگاه: خانم سحر حبیبی، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی
روابط عمومی: آقای هادی ساداتی، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی
مسئول کمیته اطلاع‌رسانی و وب‌سایت: دکتر سعید شکرالهی، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی
دبیرخانه کنفرانس در دانشگاه شهید بهشتی: سمیه ملک شیخی، سید هادی ساداتی

دبیرخانه دائمی انجمن کنفرانس رمز: مهندس سارا زواریان، مهندس ابوالفضل خداداد

مسئول مالی: دکتر شیما طبیبیان، پژوهشکده فضای مجازی

سمعی و بصری: محمد مهدی فرزانگان

مجری مراسم: آقای هادی خضاب

کمیته اجرایی (مرتب شده با نام خانوادگی به ترتیب حروف الفبا):

- مهندس ابوالفضل خداداد
- دکتر بهار فراهانی
- دکتر وحیده مقتدایی
- دکتر احمد محمودی
- دکتر فرخ لقا معظمی
- دکتر هادی سلیمانی
- سید هادی ساداتی
- دکتر سعید شکرالهی
- دکتر شیما طبیبیان
- سمیه ملک شیخی
- مهندس سارا زواریان

دبیرخانه دائمی کنفرانس‌های انجمن رمز ایران

- دکتر محمود سلماسی زاده، دبیر و قائم مقام انجمن رمز ایران
- دکتر نصور باقری، مسئول دبیرخانه دائمی
- دکتر رضا ابراهیمی آتانی
- مهندس حبیب رستمی
- مهندس محمد احسان حمیدیا
- دکتر هادی سلیمانی
- مهندس علیرضا کریمی
- مهندس هاشم حبیبی
- دکتر حمید ملا
- دکتر محمد حسام تدین
- دکتر محسن رمضان یارندی
- دکتر بهروز ترک لادانی
- دکتر صادق دری نوگورانی
- مهندس سارا زواریان
- ابوالفضل خداداد
- خانم فائزه نوری

فراخوان مقالات

بیست‌ودومین کنفرانس بین‌المللی انجمن رمز ایران در امنیت اطلاعات و رمزشناسی در روزهای ۱۶ و ۱۷ مهرماه ۱۴۰۴،
با هدف هم‌افزایی دانش و انتشار یافته‌های نو و بدیع در حوزهٔ امنیت اطلاعات و رمزشناسی در دانشگاه شهید بهشتی برگزار خواهد شد. آشنایی و ارتباط استادان، پژوهشگران، صنعتگران، مدیران و کلیه علاقه‌مندان این حوزهٔ، و بررسی چالش‌های علمی و اجرایی در فرایند امن‌سازی فضای تبادل اطلاعات کشور از دیگر اهداف برگزارکنندگان است. از میان رویدادهای جنبی کنفرانس می‌توان به نمایشگاه صنعت امنیت فضای تبادل اطلاعات (افتا)، سخنرانی‌های مدعو و کلیدی بین‌المللی، کارگاه‌های آموزشی و نشست‌های هم‌اندیشی اشاره کرد.

بدین وسیله از تمامی استادان، دانشجویان و صنعتگران دعوت می‌نماید با ارسال مقاله و حضور خود در این رویداد علمی شرکت کنند.

لازم به ذکر است که مقالات فارسی پذیرفته‌شده در شماره ویژه دوفصلنامه علمی منادی افتا با نمایه ISC و مورد تایید وزارت علوم و مقالات انگلیسی در شماره ویژه مجله ISeCure با نمایه‌های WoS-JCR و SCImago-SJR منتشر خواهند شد.

تاریخ‌های مهم:

- تاریخ کنفرانس: ۱۶و۱۷ مهرماه
- مهلت ارسال مقالات: ~~۱۰ تیرماه ۱۴۰۴~~-۶ مردادماه **۱۴۰۴** (تمدید)
- اعلام نتایج داوری: ~~۱ شهریور ۱۴۰۴~~ - ۱۱ **شهریورماه ۱۴۰۴** (تمدید)
- مهلت ثبت نام در کنفرانس‌ها و کارگاه‌ها: ~~۱۲ مهرماه ۱۴۰۴~~-۱۳ مهرماه۱۴۰۴کارگاه ها و ۱۴ مهرماه کنفرانس ها(تمدید)

محورهای تخصصی

کنفرانس از همه پژوهشگران و صنعتگران حوزهٔ 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

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 سیستم عامل
- امنیت پایگاه داده
- امنیت وب
- امنیت برنامهٔ‌های 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

پنهان‌سازی اطلاعات

- نهان‌نگاری و نشان‌گذاری
- نهان‌کاوی اطلاعات
- کاربردهای پنهان‌سازی اطلاعات

جرم‌یابی دیجیتال

- روش‌ها و ابزارهای جرم‌یابی دیجیتال
- جرم‌یابی پایگاه داده و شبکه
- جرم‌یابی دستگاه همراه
- جرم‌یابی جرایم سایبری

موضوعات نوین در رمزنگاری و امنیت سایبری

- رمزنگاری کوانتومی و پساکوانتومی
- فناوری زنجیره قالب و رمزارزها
- امنیت اینترنت اشیا، کلان‌داده‌ها و رایانش ابری
- امنیت سامانه‌های سایبر- فیزیکی
- امنیت و حریم خصوصی هوش مصنوعی
- یادگیری ماشین خصمانه
- امنیت شبکه‌های اجتماعی، متاورس و سامانه‌های مبتنی بر واقعیت افزوده

ارسال مقالات

- تمام مقالات باید از طریق سامانه EDAS به نشانی ذیل ارسال شوند:

https://edas.info/N۳۱۸۹۶

- مقالات انگلیسی در قالب مجله ISeCure تنظیم شوند. برای مشاهده راهنمای آماده‌سازی مقالات انگلیسی به نشانی https://www.isecure-journal.com/journal/authors.note مراجعه شود.
- مقالات فارسی در قالب مجله منادی افتا تنظیم شوند. برای مشاهده راهنمای آماده‌سازی مقالات فارسی به نشانی https://monadi.isc.org.ir مراجعه شود. (صفحه راهنمای نگارش)
- مقالات کوتاه علمی-صنعتی در قالب مجله منادی افتا با رعایت موارد ذکرشده در فراخوان ویژه این مقالات ارسال شود.
- هر مقاله ارسالی به کنفرانس توسط حداقل دو داور ارزیابی می‌شود.
- تعداد صفحات مقالات حداکثر ۸ صفحه است (صفحات بیشتر تا حداکثر ۱۱ صفحه با پرداخت هزینه اضافی قابل قبول است).
- مقالات فارسی پذیرفته‌شده در شماره ویژه دوفصلنامه علمی منادی افتا با نمایه ISC و مقالات انگلیسی در شماره ویژه مجله بین‌المللی ISeCure با نمایه‌های WoS-JCR و SCImago-SJR منتشر خواهند شد.
- برای هر مقاله پذیرفته‌شده لازم است حداقل یک نویسنده در کنفرانس ثبت‌نام کرده و مقاله را به‌صورت حضوری ارائه کند.
- مقالات ارسالی نباید به‌طور جدّی با مقالاتی که منتشر شده یا برای انتشار پذیرفته‌شده‌اند، همپوشانی داشته باشند.

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

زمان‌بندی کنفرانس

روز چهارشنبه ۱۶ مهرماه ۱۴۰۴(۸ اکتبر ۲۰۲۵)						
ردیف	عنوان نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل نشست
۱	مراسم افتتاحیه	سرود ملی و تلاوت قرآن کریم خوش‌آمدگویی رئیس کنفرانس (دکترمحمودرضا آقامیری) گزارش دبیر علمی و اعلام برنامهٔ کنفرانس (دکتر حمید ملا، دکتر معصومه صفخانی)		۰۸:۳۰	۰۹:۱۵	سالن اصلی (تالار ابوریحان)
۲	سخنرانی کلیدی ۱	سخنران کلیدی: مهندس عباس حسینی، مدیرعامل امن پرداز احداث مرزهای سایبری؛ گذر از دفاع پراکنده به دفاع متمرکز تهدیدات	مهندس حبیب رستمی	۰۹:۱۵	۱۰:۰۰	
پذیرایی و بازدید از کافهٔ اشتغال،				۱۰:۰۰	۱۰:۳۰	

روز چهارشنبه ۱۶ مهرماه ۱۴۰۴(۸ اکتبر ۲۰۲۵)					
۳	نشست ارائهٔ های برق آسا	ارائهٔ های کوتاه شرکت‌های حاضر در رویداد کافهٔ اشتغال	دکتر بهار فراهانی	۱۰:۳۰	۱۲:۰۰	سالن اصلی (تالار ابوریحان)
	نماز و ناهار و بازدید از کافهٔ اشتغال			۱۲:۰۰	۱۳:۳۰	
٤	نشست ۱ – مقالات کوتاه علمی-صنعتی	زهرا سهرابی بناب، محمد صادق علیزاده بازنگری در نظام تربیت نیروی انسانی سایبری: از آموزش مقطعی تا پرورش ساختار یافته استعدادها	دکتر محمد حسام تدین	۱۳:۳۰	۱۵:۳۰	سالن H1
		مهدی فرجی تکامل فایروال نسل جدید: اعمال سیاست توزیع شده در نقاط بازیابی (یک رویکرد عملی برای ایجاد پیرامون های نرم افزار-محور(SDP))				
		احسان مهدوی مقاوم‌سازی سرویس دهنده‌های لینوکس در برابر حملات منع سرویس توزیع شده بزرگ مقیاس				
		امیر فتحعلی زاده، علی پورسهی طراحی و پیاده سازی ابزار شناساگر فناوری های تحت وب				
		مرتضی ضیابخش، سید امیرحسین طباطبایی، صادق اسکندری نمونه اولیه ابزار تشخیص جعل عمیق براساس ارتقا و تلفیق شبکه‌های از پیش‌آموزش‌یافته				
		امیرحسین پورشمس، علی بنی احمدی سامانه یکپارچه مدیریت کلیدهای امنیتی اپراتور تلفن همراه اول (سیم‌کات)				

روز چهارشنبه ۱۶ مهرماه ۱۴۰۴(۸ اکتبر ۲۰۲۵)					
۵	نشست ۲ – هوش مصنوعی و امنیت (۱)	**سخنران مدعو:** دکتر امیر مهدی صادق زاده، استادیار دانشگاه صنعتی شریف **چالش‌های اعتمادپذیری در مدل‌های هوش مصنوعی مولد**	دکتر رضا ابراهیمی آتانی، دکتر مهدی آبادی	۱۳:۳۰	۱۵:۳۰	سالن H2
		پیمان حاجی زاده، حامد نادری، حسین عنایتی هتکه لویی **مروری نظام‌مند از شفافیت تا تاب‌آوری هوش مصنوعی و حاکمیت سایبری**				
		Mohammad Mohammadi, Moein Bannaye Zahmati, and Morteza Noferesti **An LSTM-DBSCAN Approach for Interpretable Insider Threat Detection via Behavioral Anomaly Analysis**				
		رضا حاجی محمدی تبریز، سجاد امینی، رضا کاظمی **روشی نوین در آموزش مدل‌های مبتنی بر انرژی به منظور تصفیه کارآمدتر تصاویر خصمانه**				
		Mohammadreza Safi and Mohammad Ali Hadavi **Genetic Algorithms in Action: Adversarial Attacks on Machine Learning-Based XSS Detection Systems**				

روز چهارشنبه ۱۶ مهرماه ۱۴۰۴(۸ اکتبر ۲۰۲۵)					
٦	نشست ۳ ـ مبانی رمز شناسی(۱)	سخنران مدعو: **Dr. Hosein Hadipour, Ruhr University Bochum** **Automating Cryptanalysis: Automated Reasoning and Structural Links Between Attacks**	دکتر ترانه اقلیدس، دکتر زهرا احمدیان	۱۳:۳۰	۱۵:۳۰	سالن H3
		Akram Khalesi and Zahra Ahmadian **Integral Attack on CHILOW**				
		Marzieh Vahid Dastjerdi, Majid Rahimi, Iman Mirzaali Mazandarani, and Sadegh Sadeghi **Evaluating CNF/SMT Encodings for SAT-Based Differential Cryptanalysis of Lightweight Ciphers**				
		Javad Alizadeh and Bahman Madadi **Differential and Linear Cryptanalysis of Reduced-Round GFRX-64 Using Neural Distinguishers and SAT/SMT-Based Technique**				
		Arka Debnath and Mohammad Mahzoun **Fast Exhaustive Search on AIM2**				
۷	نشست هم اندیشی	نشست هم اندیشی صاحب‌نظران افتا با مدیران مرکز مدیریت راهبردی افتا	دکتر محسن رمضان بارندی	۱۳:۳۰	۱۵:۳۰	**سالن** پروین اعتصامی واقع در طبقه دوم
		پذیرایی و بازدید از کافهٔ اشتغال		۱۵:۳۰	۱۶:۰۰	
۸	نشست تخصصی	**ارتقای امنیت سامانه‌های اطلاعاتی کاوشی در سیستم عامل‌های زیست بوم افتا** **با حضور اساتید دانشگاه، محققین و فعالان صنعت افتا**	دکتر رسول جلیلی	۱۶:۰۰	۱۷:۳۰	**سالن اصلی (تالار ابوریحان)**

روز پنجشنبه ۱۷ مهرماه ۱۴۰۴ (۹اکتبر ۲۰۲۴)						
ردیف	عنوان نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل نشست
۱	نشست ۴ – پیاده‌سازی الگوریتم‌های رمزنگاری و حملات مرتبط	Zahra Mohammadi, Mona Hashemi, and Siamak Mohammadi **Securing Deep Learning Hardware: A Survey of Side-Channel Vulnerabilities and Countermeasures** Marzieh Morshedzadeh, Rayhaneh Hajimohammadali, and Ali Jahanian **Defending CNNs Against Power Side-channel Attacks: A Residue Number System Solution** Farid Rajabzadeh and Ali Jahanian **Information Leakage Mitigation to Protect the Convolutional Neural Networks Against the Remote Side-Channel Analysis** Sepehr Jafari and Raziyeh Salarifard **Enhancing Kleptographic Backdoors in Hash-Based Deterministic Random Bit Generators** Vahid Soleimani Hesari, Hadi Soleimany, Ali Asghar Beigizad, and Hamed Ramzanipour Linked **Ineffective Fault Analysis on DES Cipher**	دکتر بیژن علیزاده، دکتر راضیه سالاری فرد	۸:۰۰	۱۰:۰۰	سالن H1

روز پنجشنبه ۱۷ مهرماه ۱۴۰۴ (۹ اکتبر ۲۰۲۴)					
۲	نشست ۵ – نهانگاری اطلاعات	محمد علی طائی زاده، مسعود عمومی، جلال ذهبی **روشی نوین و بهینه شده در پنهان‌نگاری دی ان ای با استفاده از تولید جدول تصادفی و قطعه بندی**	دکتر محمدعلی اخایی، دکتر زهرا سعیدی	۸:۰۰	۱۰:۰۰	سالن H2
		Donya Sadat Rezaeishad and Hossein Bahramgiri **Dual-Layered Quantum-Secure Concealing: Steganography over Quantum Key Distribution**				
		Majid Farhadi, Zohre Karimi, and Mohammad Amin Khorzani **A Secure and Verifiable Secret Sharing Scheme Using Neural Steganography and Hash Based Authentication**				
		Khashayar Jafarizade, Mohammad-Hassan Majidi, and Hossein Gholamalinejad **Architected Graph-Enhanced Neural Network Framework for Image Integrity and Tamper Precision**				
		Zahra Ghoraeian, Mohammad-Reza Sadeghi, and Samaneh Mashhadi **Time-Based Steganography in Text**				

روز پنجشنبه ۱۷ مهرماه ۱۴۰۴ (۹ اکتبر ۲۰۲۴)					
۳	نشست ۶ ـ امنیت شبکه	سخنران مدعو: دکتر سولماز سلیمی، EURECOM **تحلیل آلودگی فراتر از آسیب پذیری های کلاسیک: چالش ره‌گیری داده در مرزهای ناهمگون نرم افزار، سخت افزار و شبکه**	دکتر مرتضی امینی-دکتر صادق دری نوگورانی	۸:۰۰	۱۰:۰۰	سالن H3
		Hamid Reza Dashtabadi and Siavash Ahmadi **Network Intrusion Detection using Federated Learning in Cyber-Physical Systems**				
		Zahra Bastani, Peyman Pahlevani, Rouhollah Sadr Mohammadi, and Abolfazl Mortezapour **Evaluating DDoS Attacks Using IoT Communication Protocols Internet of Things Distributed Denial of Service attacks Cybersecurity**				
		Mahdi Jeyhoon and Maryam Rajabzadeh Asaar **5G Attacks: Realistic Scenarios and Simulations Using Open5GS**				
		Togu Novriansyah Turnip, Birger Andersen, and Cesar Vargas-Rosales **Recent Trends in Post-Quantum Cryptography Integration and Performance in the Internet Security Stack**				
		پذیرایی و بازدید از کافهٔ اشتغال		۱۰:۰۰	۱۰:۳۰	
٤	سخنرانی کلیدی ۲ و ۳	Keynote Speaker: Professor Peter Schwabe **The migration to post-quantum cryptography**	دکتر رضا ابراهیمی آتانی	۱۰:۳۰	۱۱:۱۵	سالن اصلی (تالار ابوریحان)
۵		Keynote Speaker: Professor Bart Preneel **Cybersecurity and AI: A Symbiotic Relationship?**		۱۱:۱۵	۱۲:۰۰	
		نماز و ناهار و بازدید از کافهٔ اشتغال		۱۲:۰۰	۱۳:۳۰	

روز پنجشنبه ۱۷ مهرماه ۱۴۰۴ (۹اکتبر ۲۰۲۴)					
٦	نشست ۷ – پروتکل های امنیتی	سخنران مدعو: دکتر مانده مشرف، استادیار دانشگاه شهید بهشتی **امنیت در متاورس: تحلیل تهدیدات و راهکارهای مقابله**	مهندس جواد مهاجری، دکتر هادی شهریار شاه حسینی	۱۳:۳۰	۱۵:۳۰	سالن H2
		Sina Fattahi Ardakani and Maedeh Mosharraf **Decentralized Plagiarism Detection System for Open Textual Educational Resources based on Blockchain Technology**				
		Seyede Marzieh Sadat Madani, Hamid Mala, and Mehrad Jaberi **An Efficient ECC-Based Multi-Server Authentication Scheme for 5G Environment without Online Registration Server**				
		S. Mohammad Dibaji, Taraneh Eghlidos, and Hossein Pilaram **QuMixnet: A Quantum-Safe Mixnet Protocol**				
		Keykhosro Khosravani, Taraneh Eghlidos, and Mohammad Reza Aref **Efficient Pairing-Free Adaptable k-out-of-N Oblivious Transfer Protocols**				
		Ahmad Khoureich Ka **Secure Pairing-Free IBE and CP-ABE from Inner-Product Functional Encryption**				

روز پنجشنبه ۱۷ مهرماه ۱۴۰۴ (۹اکتبر ۲۰۲۴)						
۷	نشست ۸ ـ هوش مصنوعی و امنیت محاسبات	Nima Atashin, Behrouz Tork Ladani, and Mohammadreza Sharbaf **Learning to Locate: GNN-Powered Vulnerability Path Discovery in Open Source Code**	دکتر بهروز ترک لادنی، دکتر مجتبی خلیلی	۱۳:۳۰	۱۵:۳۰	سالن H3
		Arman Moradi, Mehran Alidoost Nia, and Reza Ebrahimi Atani **A Multi-Objective Reinforcement Learning Framework for Security Enhancement in Autonomous Vehicles**				
		Mohammad Reza Mirbagheri, Seyed Mohammad Mahdi Mirkamali, Zahra Motoshaker Arani, Ali Javeri, Amir Mahdi Sadeghzadeh Mesgar, and Rasool Jalili **EPT Benchmark: Evaluation of Persian Trustworthiness in Large Language Models**				
		Amirhossein Heydari, Azadeh Mansouri, and Ahmad Mahmoudi-Aznaveh **Backdoor Defense via Aggregation of Outsourced Models using Multi-Stage Knowledge Distillation**				
		Keyhan Mohammadi, Ehsan Kozegar, and Reza Ebrahimi Atani **HashLearner: A Secure Decentralized Learning Framework Based on HashGraph**				

روز پنجشنبه ۱۷ مهرماه ۱۴۰۴ (۹اکتبر ۲۰۲۴)						
۸	نشست ۹-مدیریت امنیت و حریم خصوصی و جرم یابی دیجیتال	Sajed Yousefi Mashhour, Motahareh Dehghan, Babak Sadeghian, and Alireza Hashemi **Mission-Centric Countermeasure Selection in Cybersecurity Situation Awareness**	دکتر طلا نفضلی، دکتر صادق دری نوگورانی	۱۳:۳۰	۱۵:۳۰	سالن H3
		Sajjad Rezaei and Ali Fanian **Static Malware Detection in Windows Executables Using Deep Neural Networks**				
		Sepehr Mehregan, Mahdi Tamjidi, Amir Hossein Rahimi, Ava Razavi, Sadegh Eskandari, and Seyed Amir Hossein Tabatabaei **GP-FACL: A Dataset of FAlse Claim Descriptions and Functionalities of Google Play Apps**				
		Mostafa Shabani and Tala Tafazzoli **Lateral Movement Attack Detection using Variational Autoencoders**				
		Seyede Fateme Mazhar and Azadeh Mansouri **Feature Map Correlations in Video Face Forgery Detection**				

روز پنجشنبه ۱۷ مهرماه ۱۴۰۴ (۹اکتبر ۲۰۲۴)					
۹	نشست۱۰ اسمبانی رمزشناسی(۲)	سخنران مدعو: دکتر اکرم خالصی، پژوهشگاه توسعه فناوری‌های پیشرفته **The Division Property and Its Automation: Development and Open Research Challenges**	دکتر ترانه اقلیدس-دکتر محمود احمدیان عطاری	۱۳:۳۰	۱۵:۳۰	سالن H4
		محمد بلوکیان، علی اصغر اروجی، منیره هوشمند **آماده‌سازی حالت از راه دور سه طرفه بهینه یک حالت تک کیوبیتی شناخته شده**				
		محمد بلوکیان و منیره هوشمند **طرح نوین تسهیم راز نیمه کوانتومی مقاوم بدون تبادل مستقیم کیوبیت حاوی پیام**				
		پذیرایی و بازدید از کافهٔ اشتغال،		۱۵:۳۰	۱۶:۰۰	
۱۰	مراسم اختتامیه	**سرود ملی و تلاوت قرآن کریم** **گزارش برگزاری کنفرانس توسط دبیر اجرایی (دکترهادی سلیمانی-دکتر فرخ لقا معظمی)** **بیانیه پایانی و معرفی میزبان کنفرانس بیست و سوم** **سخنرانی ریاست محترم انجمن رمز ایران (دکترمحمود سلماسی زاده)** **اعلام برگزیدگان و تقدیر از تیم اجرایی توسط مسئول محترم دبیرخانه دائمی کنفرانس (دکتر نصور باقری)**		۱۶:۰۰	۱۷:۰۰	سالن اصلی (شهید ابوریحان)

سخنرانی‌ها

سخنرانان کلیدی

احداث مرزهای سایبری؛ گذر از دفاع پراکنده به دفاع متمرکز تهدیدات

عباس حسینی، مدیرعامل و رئیس هیات مدیره شرکت نرم‌افزاری امن‌پرداز

چکیده

برای قرن‌ها، امنیت یک ملت با مرزهای فیزیکی آن تعریف می‌شد: کوه‌ها، دریاها، دیوارها و میدان‌های نبرد. اما امروز، میدان نبرد جدیدی شکل گرفته است؛ میدانی بدون مرز، نامرئی و در حال گسترش: فضای سایبری. در این فضا، دشمنان می‌توانند در آن سوی کره زمین نشسته باشند و زیرساخت‌های حیاتی کشور را هدف بگیرند. سؤال اینجاست: آیا ما در این فضای بی‌مرز، نیاز به تعریف مرزهای جدید داریم؟ در این سخنرانی، در مورد این ایده صحبت خواهیم کرد: احداث مرز سایبری ملی، ضرورت، چگونگی و اقداماتی عملی برای دفاع در برابر تهدیدات نوین.

بیوگرافی

عباس حسینی، مدیرعامل و رئیس هیات مدیره شرکت نرم‌افزاری امن‌پرداز از سال ۱۳۸۳

فعال در حوزهٔ امنیت سایبری و سازنده محصول آنتی‌ویروس پادویش

Cybersecurity and AI: A Symbiotic Relationship?

Bart Preneel, University of Leuven, Belgium

Abstract

In today's digital economy, where data breaches plague industry and government alike, the fusion of Cybersecurity and Artificial Intelligence (AI) has emerged as a potent defense strategy. This talk explores the relationship between AI and cybersecurity, covering both its promises and perils. AI has revolutionized cybersecurity, enabling advanced capabilities such as the detection of malware, vulnerabilities and fraud. Yet, as AI empowers defenders, it also strengthens attackers. The dark side of AI reveals a landscape where malicious actors harness AI for spear phishing, automated cyberattacks, misinformation, and deepfakes. Moreover, AI itself becomes a target, as shown by adversarial machine learning and model poisoning attacks. Finally, there are concerns about AI creating a dystopia. The talk further explores technologies such as attribution (watermarking) and computing on encrypted data that can play a role in mitigating some of these risks. Overall, there is a need for a multidisciplinary approach encompassing technology, regulation, and ethics to effectively address the challenges presented by the intricate relationship between AI, cybersecurity and privacy.

Biography:

Prof. Bart Preneel, a full professor at KU Leuven, leads the renowned COSIC research group. His expertise lies in applied cryptography, cybersecurity, and privacy. Prof. Preneel has delivered over 150 invited talks across 50 countries and received prestigious awards such as the RSA Award for Excellence in Mathematics (2014), the ESORICS Outstanding Research Award (2017) and Belgian ICT Personality of the Year (2025). He served as president of IACR (International Association for Cryptologic Research) and is also a fellow of the IACR. In 2024 he was elected member of the Royal Academy of Art and Sciences Belgium and he received the title of honorary professor at Shandong University. He frequently consults for industry and government about cybersecurity and privacy technologies and he has testified multiple times for the Belgian and European Parliaments. Prof. Preneel founded the mobile authentication startup nextAuth and holds roles in Approach Belgium, Tioga Capital Partners, and Nym Technologies. Actively engaged in cybersecurity policy, he has contributed to ENISA as an Advisory Group member from 2012 to 2025.

The migration to post-quantum cryptography

Peter Schwabe, Radboud University

Abstract

With the first batch of NIST PQC standards published in 2024, the migration of our cryptographic infrastructure to post-quantum schemes has received a massive boost. We all already use post-quantum cryptography every day, typically without even noticing that we do. In my talk I will look back at how we got where we are now in terms of PQC deployment, what to expect in the near future, and what challenges are still to be tackled to migrate all systems in time before a large-scale quantum computer breaks factoring-based and discrete-log-based asymmetric cryptography.

Biography

Peter Schwabe is scientific director at MPI-SP and professor at Radboud University. He graduated from RWTH Aachen University in computer science in 2006 and received a Ph.D. from the Faculty of Mathematics and Computer Science of Eindhoven University of Technology in 2011. He then worked as a postdoctoral researcher at the Institute for Information Science and the Research Center for Information Technology Innovation of Academia Sinica, Taiwan and at National Taiwan University. His research area is cryptographic engineering; in particular, the security and performance of cryptographic software. He published more than 80 articles in journals and at international conferences presenting, for example, fast software for a variety of cryptographic primitives including AES, hash functions, elliptic-curve cryptography, and cryptographic pairings. He has also published articles on fast cryptanalysis, in particular attacks on the discrete-logarithm problem. In recent years he has focused in particular on post-quantum cryptography. He co-authored the "NewHope" and "NTRU-HRSS" lattice-based key-encapsulation schemes which were used in post-quantum TLS experiments by Google and he is co-submitter of seven proposals to the NIST post-quantum crypto project, all of which made it to the second round, five of which made it to the third round, and 3 of which were selected after round 3 for standardization. In 2021, he co-founded the Formosa-Crypto project, an effort by multiple research groups to build (post-quantum) cryptographic software with formal proofs of functional correctness and security.

سخنرانان مدعو

چالش‌های اعتمادپذیری در مدل‌های هوش مصنوعی مولد

دکتر امیرمهدی صادق‌زاده، استادیار دانشگاه صنعتی شریف، ایران

بیوگرافی

امیرمهدی صادق‌زاده استادیار دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف و مدیر آزمایشگاه "هوش مصنوعی قابل امن و اعتمادپذیر (TSAIL)" هستند. ایشان مدرک دکتری خود را در رشته مهندسی کامپیوتر از دانشگاه صنعتی شریف در سال ۱۴۰۱ دریافت کرده‌اند. حوزه‌های پژوهشی اصلی دکتر صادق‌زاده شامل امنیت یادگیری ماشین، حفظ حریم خصوصی در یادگیری ماشین، کاربردهای یادگیری ماشین در امنیت سایبری، امنیت شبکه و بلاکچین است. فعالیت‌های علمی و پژوهشی ایشان بر توسعه سامانه‌های هوش مصنوعی اعتمادپذیر و امن متمرکز است و هدف ایشان ارتقای اعتمادپذیری، امنیت و مسئولیت‌پذیری فناوری‌های نوین هوش مصنوعی در محیط‌های واقعی است.

Automating Cryptanalysis: Automated Reasoning and Structural Links Between Attacks

Hosein Hadipour, Peter Schwabe, University Bochum, Germany

Biography

Hosein Hadipour is a postdoctoral researcher at Ruhr University Bochum, specializing in the cryptanalysis of symmetric-key primitives. He received his Ph.D. in computer science with distinction from Graz University of Technology in 2024. Prior to that, he studied mathematics and electronic engineering at K. N. Toosi University (earning two bachelor's degrees) and completed a master’s degree in pure mathematics at the University of Tehran. His work has appeared in leading venues such as CRYPTO, EUROCRYPT, FSE/ToSC, and CHES.

تحلیل آلودگی فراتر از آسیب‌پذیری‌های کلاسیک: چالش ره‌گیری داده در مرزهای ناهمگونِ نرم‌افزار، سخت‌افزار و شبکه

دکتر سولماز سلیمی، EURECOM

Biography

Solmaz Salimi recently completed a postdoctoral fellowship with the Software and System Security (S3) group at EURECOM, collaborating with Aurélien Francillon on system-level security for advanced embedded devices. Her work centers on static and dynamic program analysis to harden complex software, with a focus on inter-layer communication and the interfaces between firmware, hardware, and operating systems. She earned her Ph.D. at Sharif University of Technology under Mehdi Kharrazi and was a visiting researcher with EPFL's HexHive group led by Mathias Payer, contributing to regression bug detection for the Linux kernel and software fuzzing. Beyond research, she co-founded and has organized ASIS CTF (since 2012), co-organizes CryptoCTF (since 2019), and co-organized Parcham CTF (2020) with S4Lab at Sharif.

امنیت در متاورس: تحلیل تهدیدات و راهکارهای مقابله

دکتر مائده مشرف، استادیار دانشگاه شهید بهشتی

بیوگرافی

مائده مشرف مدرک کارشناسی، کارشناسی ارشد و دکتری خود را در رشته مهندسی کامپیوتر از دانشگاه تهران اخذ نموده است. حوزه‌های تخصصی و پژوهشی ایشان شامل متاورس، فناوری بلاک چین و خدمات الکترونیکی است. تحقیقات ایشان بر روی چالش‌ها و راهکارهای نوین در تقاطع این فناوری‌های پیشرو متمرکز شده است..

ویژگی تقسیم و خودکارسازی آن: مسیر توسعه و چالش‌های باز پژوهشی

دکتر اکرم خالصی، پژوهشگاه توسعه فناوری‌های پیشرفته

بیوگرافی

اکرم خالصی در سال ۱۴۰۳ مدرک دکتری خود را در رشته مهندسی برق-مخابرات سیستم با عنوان رساله دکتری " توسعه خودکاری سازی حملات روی الگوریتم های رمز قالبی" از دانشگاه شهید بهشتی دریافت کرده است. وی از سال ۱۳۹۲ به‌عنوان پژوهشگر در حوزۀ رمز و امنیت در پژوهشگاه توسعه فناوری‌های پیشرفته فعالیت دارد. زمینه‌های پژوهشی او شامل رمزنگاری متقارن، روش‌ها و ابزارهای تحلیل و خودکارسازی آن‌ها و همچنین رمزنگاری کاربردی است.

نشست تخصصی

ارتقای امنیت سامانه‌های اطلاعاتی: کاوشی در سیستم عامل‌های زیست بوم افتا

با حضور اساتید دانشگاه، محققین و فعالان صنعت افتا

نمایه مقالات

تاریخ: ۱۶ مهرماه ۱۴۰۴	سالن: H1	چهارشنبه
زمان: ۱۳:۳۰ الی ۱۵:۳۰		نشست ۱
مقالات کوتاه علمی-صنعتی		
رئیس نشست: دکتر محمد حسام تدین		
نویسندگان	عنوان مقاله	
زهرا سهرابی بناب محمد صادق علیزاده	بازنگری در نظام تربیت نیروی انسانی سایبری: از آموزش مقطعی تا پرورش ساختار یافته استعدادها	
مهدی فرجی	تکامل فایروال نسل جدید: اعمال سیاست توزیع شده در نقاط بازیابی (یک رویکرد عملی برای ایجاد پیرامون های نرم افزار-محور(SDP))	
احسان مهدوی	مقاوم‌سازی سرویس‌دهنده های لینوکس در برابر حملات منع سرویس توزیع شده بزرگ مقیاس	
امیر فتحعلی زاده، علی پورسهی	طراحی و پیاده سازی ابزار شناساگر فناوری‌های تحت وب	
مرتضی ضیابخش، سید امیرحسین طباطبایی، صادق اسکندری	نمونه اولیه ابزار تشخیص جعل عمیق بر اساس ارتقا و تلفیق شبکه‌های از پیش آموزش یافته	
امیرحسین پورشمس، علی بنی احمدی	سامانه یکپارچه مدیریت کلیدهای امنیتی اپراتور تلفن همراه اول (سیم کات)	

بازنگری در نظام تربیت نیروی انسانی سایبری: از آموزش مقطعی تا پرورش ساختار یافته استعدادها

زهرا سهرابی بناب[۱]، محمدصادق علیزاده [۲]
[۱]آکادمی فن افزا، ایران- [۲]آکادمی اندیشه، منهاج علم ورزان، ایران

چکیده: یکی از چالش‌های پیشروی صنعت امنیت سایبری کشور، فقدان آموزش نظاممند در تربیت و توسعهٔ مهارت‌های انسانی متناسب با تهدیدات نوظهور سایبری است. برخلاف رشد سریع فناوری‌های دیجیتال، آموزش منابع انسانی در کشور اغلب مبتنی بر مدل‌های سنتی، بدون تمرکز بر مهارت‌محوری، همکاری بین‌بخشی و آموزش مستمر است. این شکاف موجب شده نیروی انسانی شاغل در حوزهٔ امنیت سایبری، در پاسخ به تهدیدات پیچیدهٔ امروزی دچار ضعف عملکرد، تأخیر در واکنش یا اتکا بیش از حد به ابزارهای خارجی شود.

در این مقالهٔ کوتاه، تجربه‌های موفق کشورهایی چون ایالات متحدهٔ آمریکا و بریتانیا در طراحی نظام‌های آموزشی و توسعهٔ مهارت‌های سایبری بررسی می‌شود و با بررسی تفاوت‌ها با وضعیت موجود در ایران، مجموعه‌ای از پیشنهادهای عملیاتی برای بازنگری سیاست‌های آموزشی در صنعت امنیت کشور ارائه می‌شود.

تکامل فایروال نسل جدید: اعمال سیاست توزیع شده در نقاط بازیابی (یک رویکرد عملی برای ایجاد پیرامون های نرم افزار-محور(SDP))

مهدی فرجی[۱]
[۱]تاکیان (توسعه امن کیان)، ایران

چکیده: حرکت جانبی هستهٔ اصلی حملات باج‌افزاری مدرن است که پس از نفوذ اولیه، به مهاجم اجازه می‌دهد در شبکه گسترش یافته و به دارایی‌های حیاتی دسترسی پیدا کند. راهکارهای سنتی بخش‌بندی شبکهٔ مبتنی بر VLAN یا فایروال‌های داخلی، به‌دلیل پیچیدگی در پیاده‌سازی و مدیریت، اغلب در مهار این تهدید ناکارآمد هستند. این مقاله تجربهٔ صنعتی در پیاده‌سازی رویکردی نوین برای ریزبخش‌بندی مبتنی بر میزبان را ارائه می‌دهد. در این معماری، با استفاده از عاملی نرم‌افزاری روی هر دارایی، «حباب‌های امنیتی» مستقلی پیرامون سرورها و کلاینت‌ها ایجاد می‌شود که ارتباطات مجاز را به‌صورت دقیق و براساس سیاست‌های مرکزی تعریف می‌کنند. این روش، وابستگی به تغییرات پیچیدهٔ در زیرساخت شبکه را از بین برده و ابزارهای واکنش سریع، مانند قابلیت انسداد اضطراری، را برای مهار فوری تهدید فراهم می‌آورد. نتایج عملیاتی نشانگر کاهش چشمگیر سطح حمله و توانایی بی‌نظیر در متوقف‌کردن آنی حملات باج‌افزاری در مراحل اولیه است.

مقاوم‌سازی سرویس دهنده‌های لینوکس در برابر حملات منع سرویس توزیع شده بزرگ مقیاس

احسان مهدوی[1]
[1]دانشگاه اصفهان، ایران

چکیده: این مقاله راه‌حلی برای مقابله با حملات DDoS در لایهٔ شبکه ارائه شده است که بر پایهٔ بهینه‌سازی سخت‌افزاری و نرم‌افزاری در محیط لینوکس عمل می‌کند. این روش ترکیبی از تنظیمات پیشرفتهٔ کارت شبکهٔ ۱۰گیگابیتی، بهینه‌سازی‌های هستهٔ لینوکس (مانند RPS و XPS) و همچنین استفاده از فناوری eBPF برای فیلترکردن هوشمند ترافیک است. در این رویکرد، از طریق ماژول xdp_rate_limit، داده‌های ورودی در سطح پایین هسته و قبل از رسیدن به لایه‌های بالاتر شبکه، پردازش شده و منابع مخرب حذف می شوند. آزمایش‌ها نشان دادند که این راه‌حل قادر است به‌ازای هر زوج پورت ۱۰گیگابیتی و CPU متناظر، به‌طور مؤثر ترافیکی معادل ۱۲میلیون پکت در ثانیه از بیش از ۲میلیون آدرس IP مختلف را در زمان واقعی شناسایی و ترافیک مجاز را از آن جدا کند. این دستاورد باعث کاهش قابل‌توجه بار سیستم و افزایش تحمل‌پذیری شبکه در برابر حملات DDoS می‌شود.

طراحی و پیاده‌سازی ابزار شناساگر فناوری های تحت وب

امیر فتحعلی‌زاده[1]، علی پورسهی[2]
[1]پژوهشکده فضای مجازی، دانشگاه شهید بهشتی، ایران- [2] موسسه آموزش عالی ایرانیان، دانشگاه ایرانیان، ایران

چکیده: با رشد چشمگیر فناوری‌های تحت وب، شناخت دقیق فناوری‌های به‌کاررفته در وب‌سایت‌ها به یکی از محورهای کلیدی در تحلیل‌های امنیتی، توسعه و ارزیابی دارایی‌های دیجیتال تبدیل شده است. این مقاله با تمرکز بر تحلیل از منظر کاربر، معماری چندلایه‌ای برای شناسایی فناوری‌های وب ارائه می‌دهد که مبتنی بر اطلاعات قابل مشاهده در سمت مرورگر است. ساختار پیشنهادی در سه مرحلهٔ اصلی شامل آماده‌سازی و ارسال درخواست HTTP، تحلیل ساختاریافته‌ی پاسخ‌دریافتی از سرور و تطبیق اطلاعات با پایگاه دانش طراحی شده است. در بخش تحلیل، داده‌ها از لایه‌هایی همچون سرآیندها، کوکی‌ها، کد HTML، منابع بارگذاری‌شده و متغیرهای JavaScript در زمان اجرا استخراج می‌شوند. سپس با بهره‌گیری از پایگاه دانشی قابل گسترش، فرآیند استنتاج فناوری‌ها انجام می‌شود. رویکرد پیشنهادی با قابلیت یکپارچه‌سازی با ابزارهای تحلیلی دیگر طراحی شده و می‌تواند در کاربردهایی نظیر تست نفوذ، تحلیل سطح حمله و پایش امنیتی مؤثر واقع شود.

نمونه اولیه ابزار تشخیص جعل عمیق براساس ارتقا و تلفیق شبکه های از پیش آموزش یافته

مرتضی ضیابخش[1]، سید امیرحسین طباطبایی[1،2]، صادق اسکندری[1]
[1]دانشگاه گیلان، ایران-[2]دانشگاه علمی کاربردی (THM)، آلمان

چکیده: دیپ فیک‌ها به عنوان داده‌های مصنوعی تولیدشده با فناوری‌های یادگیری عمیق، قادر به دست‌کاری یا جایگزینی هویت، اقدامات و ویژگی‌های افراد در محتوای تصویری و ویدئویی موجود هستند. این فناوری با ایجاد محتوای تقلیدی بسیار متقن و نزدیک به واقعیت، چالش‌های فنی را به همراه دارد. اگرچه کاربردهای مثبتی در حوزه‌هایی مانند هنر، صنعت فیلم و تبلیغات دارد، اما سوءاستفاده از آن جهت انتشار اطلاعات نادرست، بدنام‌سازی افراد یا احزاب، ایجاد بی‌ثباتی سیاسی و ارتکاب جرایم سایبری، تهدیدات عمیقی در ابعاد سیاسی، اجتماعی و اقتصادی ایجاد کرده است. تشدید این تهدیدات توسط گستره و قدرت تحویل اطلاعات در

شبکه‌های اجتماعی، لزوم توسعهٔ ابزارهای دقیق و کارآمد برای تشخیص و طبقه‌بندی محتوای دیپ فیک رابه امری حیاتی تبدیل نموده است. در پاسخ به این ضرورت، دستاورد ارائه‌شده به طراحی، پیاده‌سازی و توسعهٔ اپلیکیشنی تحت وب تخصصی برای تشخیص و طبقه‌بندی دیپ فیک در ویدئوها و تصاویر پرداخته است. رویکرد اصلی این ابزار دستاورد، بهبود و تلفیق چندین مدل پیش‌آموزش‌دیده مهم است که امکان شناسایی تغییرات ناشی از دیپ فیک، به‌ویژه جایگزینی چهره، را با دقتی فراتر از روش‌های فعلی فراهم می‌کند. سیستم توسعه‌یافته موفق به دستیابی به دقتی در حدود ۰,۹۹ در فرایند تشخیص و طبقه‌بندی دیپ فیک‌ها شده است.

سامانه یکپارچه مدیریت کلیدهای امنیتی اپراتور تلفن همراه اول (سیم کات)

امیرحسین پورشمس[۱]، علی بنی احمدی[۱]
[۱] شرکت ارتباطات سیار ایران (MCI)، ایران

چکیده: مدیریت امن کلیدهای رمزنگاری سیم‌کارت در اپراتورهای تلفن‌همراه، به‌ویژه در چرخهٔ عمر کلیدها، شامل تولید، ذخیره‌سازی، توزیع و بهره‌برداری، از چالش‌های اصلی امنیت سایبری به‌شمار می‌رود. این مقاله به بررسی موانع موجود در مدیریت کلیدهای سیم‌کارت در اپراتورهای تلفن‌همراه می‌پردازد و مسائلی نظیر تولید و انتقال غیرامن کلیدها، ذخیره‌سازی ناامن، نبود زیرساخت یکپارچه برای ارتباط با سامانه‌های مرتبط، فقدان سوابق جامع و متمرکز و ریسک تبانی یا سوءاستفاده را مورد توجه قرار می‌دهد. برای رفع این مشکلات، سامانه یکپارچه مدیریت کلیدهای امنیتی اپراتور تلفن همراه(سیم‌کات)طراحی و پیاده‌سازی شده است. این سامانه با بهره‌گیری از افزاره‌های امنیتی سخت افزاری بومی، الگوریتم‌های رمزنگاری پیشرفته و روش های تسهیم راز، امکان تولید، نگهداری و انتقال امن کلیدهای سیم‌کارت را فراهم می‌کند. همچنین با ارائه قابلیت‌هایی مانند احراز هویت دو عاملی، مدیریت متمرکز سوابق و پشتیبانی از مهاجرت به پیمانکاران جدید بدون ایجاد محدودیت، امنیت و کارایی فرایندهای مرتبط با کلیدهای سیم‌کارت را به طور چشم‌گیری ارتقا داده است. این راه‌کار به عنوان یک نوآوری جامع، نیازهای امنیتی اپراتورهای تلفن همراه را به‌صورت مؤثر برآورده می‌سازد.

تاریخ: ۱۶ مهرماه ۱۴۰۴	سالن: H2	چهارشنبه
زمان: ۱۳:۳۰ الی ۱۵:۳۰		نشست: ۲
هوش مصنوعی و امنیت		
روسای نشست: دکتر رضا ابراهیمی آتانی-دکتر مهدی آبادی		
سخنران مدعو: دکتر امیر مهدی صادق‌زاده، استادیار دانشگاه صنعتی شریف چالش‌های اعتمادپذیری در مدل های هوش مصنوعی مولد		
نویسندگان	عنوان مقاله	
پیمان حاجی زاده، حامد نادری، حسین عنایتی هتکه لویی	مروری نظام‌مند از شفافیت تا تاب آوری هوش مصنوعی و حاکمیت سایبری	
Mohammad Mohammadi, Moein Bannaye Zahmati, and Morteza Noferesti	An LSTM-DBSCAN Approach for Interpretable Insider Threat Detection via Behavioral Anomaly Analysis	
رضا حاجی محمدی تبریز، سجاد امینی، رضا کاظمی	روشی نوین در آموزش مدل‌های مبتنی بر انرژی به منظور تصفیه کارآمدتر تصاویرخصمانه	
Mohammadreza Safi and Mohammad Ali Hadavi	Genetic Algorithms in Action: Adversarial Attacks on Machine Learning-Based XSS Detection Systems	

مروری نظام‌مند از شفافیت تا تاب آوری هوش مصنوعی و حاکمیت سایبری

پیمان حاجی‌زاده[۱]، حامد نادری[۱]، حسین عنایتی هتکه لویی[۱]
[۱]دانشگاه آزاد اسلامی واحد تهران جنوب، ایران

چکیده: با وجود پتانسیل بالای هوش مصنوعی در امنیت سایبری، پیاده‌سازی آن با چالش‌های مدیریتی مهمی هم‌چون عدم شفافیت مدل‌ها و ظهور ریسک‌های نوین همراه است. هدف این پژوهش، تدوین یک چارچوب مفهومی یکپارچه برای همسوسازی قابلیت‌های فنی هوش مصنوعی با الزامات مدیریتی، به منظور بهینه‌سازی چارچوب امنیت سایبری مؤسسه NIST است. در این مطالعه، از روش مرور نظام‌مند ادبیات برای تحلیل ۲۴ مقاله‌ی کلیدی منتشرشده استفاده شد. یافته‌ها نشان داد پژوهش‌های پیشین عموماً پراکنده بوده و به‌صورت نامتوازنی بر عملکردهای حکمرانی و شناسایی متمرکزند، در حالی که به عملکرد بازگشت به وضعیت پایدار توجه کافی نشده است. همچنین، فقدان هوش مصنوعی قابل توضیح و ریسک حملات خصمانه، موانع اصلی پذیرش هوش مصنوعی توسط مدیران سازمان‌ها شناسایی شدند. براساس این یافته‌ها، پژوهش حاضر چارچوب مفهومی «دوگانه‌ی شفافیت-تاب آوری» را ارائه می‌دهد که استقرار موفق هوش مصنوعی را منوط به ایجاد پیوند میان شفافیت در حاکمیت از طریق هوش مصنوعی قابل توضیح و تاب‌آوری در عملیات از طریق هوش مصنوعی مولد و یادگیری تقویتی می‌داند. چارچوب پیشنهادی با ارائهٔ شاخص‌های کلیدی عملکرد مانند بازگشت سرمایه، امتیاز اعتماد و میانگین زمان پاسخ، ابزاری برای تصمیم‌گیری آگاهانه در اختیار مدیران امنیت سایبری قرار می‌دهد.

An LSTM-DBSCAN Approach for Interpretable Insider Threat Detection via Behavioral Anomaly Analysis

Mohammad Mohammadi[1], Moein Bannaye Zahmati[1], and Morteza Noferesti[1]
[1]Bozorgmehr University of Qaenat, Qaen, South Khorasan, Iran

Abstract: Insider threats pose a significant cybersecurity risk, as authorized users can exploit legitimate access to compromise sensitive systems and data. This paper proposes an integrated behavioral anomaly detection approach to address three critical challenges in AI-driven insider threat detection: lack of interpretability, misleading evaluation metrics, and misalignment with operational taxonomies. Our approach employs a three-stage pipeline: (1) an LSTM autoencoder to detect temporal anomalies in login patterns, (2) DBSCAN clustering to identify suspicious file access and device usage during anomalous sessions, and (3) DBSCAN-based URL analysis to uncover exfiltration patterns. By correlating temporal, spatial, and web-based behavioral indicators, the framework generates actionable MITRE-mapped threat chains including T1078, T1005, T1204.002, T1567.002 that bridge the gap between academic models and Security Operations Center (SOC) workflows. Evaluated on the CERT r6.2 dataset, our approach detects the data exfiltration scenario, offering interpretable alerts and operational efficiency.

روشی نوین در آموزش مدل‌های مبتنی بر انرژی به منظور تصفیه کارآمدتر تصاویر خصمانه

رضا حاجی محمدی تبریز[۱]، سجاد امینی[۱]، رضا کاظمی[۱]
[۱]دانشگاه صنعتی شریف، ایران

چکیده: کاربردهای یادگیری عمیق به سرعت در حال گسترش هستند. با این حال، در حوزه‌های حساسی مانند امنیت و سلامت، حملات خصمانه - اغتشاشات جزئی ورودی منجر به افت شدید عملکرد مدل - همچنان مانعی جدی برای پذیرش این کاربردها هستند. مدل‌های مولد با توانایی یادگیری توزیع داده‌ها، گزینه‌هایی امیدوارکننده برای بازیابی تصویر اصلی از روی نمونه‌های خصمانه در طی فرایندی به نام تصفیه هستند. در این مقاله، برای نخستین بار، روندی جدید برای تصفیه پیشنهاد می‌دهیم که در آن مدل مبتنی بر انرژی Mp، پیش از طبقه‌بند M به کار می‌رود. Mp به گونه‌ای آموزش می‌بیند که به نمونه‌های خصمانه M (نمونه های منفی در آموزش Mp)، انرژی بالا (احتمال پایین) اختصاص دهد. براساس نتایج، روش ما در برابر نمونه‌های خصمانه، دقت مقاوم بالاتری نسبت به مدل تصفیه استاندارد Mp داشته و بهبودهایی به میزان ٪۱۲,۳۱، ٪۲۲,۸۷ و ٪۱۲,۳۰ روی پایگاه‌های داده MNIST، FashionMNIST و CIFAR10 تحت \ (L_{\infty}) AutoAttack نشان داده است. همچنین با وجود سادگی فرایند آموزش، روش ما روی پایگاه داده CIFAR10 نسبت به یک مدل پیشرفته مبتنی بر انرژی، بهبودی معادل ٪۳ در دقت مقاوم نشان می‌دهد. افزون بر این، یک حمله‌ی وفقی نیز طراحی کرده‌ایم که دفاع ما را هدف قرار می‌دهد و نشان می‌دهیم Mp همچنان قادر به خنثی‌سازی آن است.

Genetic Algorithms in Action: Adversarial Attacks on Machine Learning-Based XSS Detection Systems

Mohammadreza Safi[1] and Mohammad Ali Hadavi[1]
[1]Malek Ashtar University of Technology, Iran

Abstract: Cross-Site Scripting (XSS) remains a critical web application vulnerability, consistently ranking among the OWASP Top 10 security risks. Although machine learning and deep learning techniques have improved XSS detection, these models are susceptible to adversarial attacks-carefully crafted inputs designed to evade detection. This paper proposes a novel adversarial attack framework that leverages Genetic Algorithms (GAs) to automatically generate adversarial XSS payloads targeting machine learning-based detection systems. The framework is designed for high transferability, enabling adversarial samples to bypass a variety of detection models, even those with differing architectures. By employing genetic operators such as selection, crossover, and mutation, the method systematically optimizes payloads to maximize evasion rates while maintaining syntactic validity. Experimental results demonstrate that the generated adversarial samples consistently evade multiple state-of-the-art detection models, revealing significant vulnerabilities in current XSS defenses. This work underscores the urgent need for more robust machine learning-based security solutions and provides a foundation for developing improved defenses against adaptive adversarial threats.

تاریخ: ۱۶مهرماه ۱۴۰۴	سالن: H3	چهارشنبه
زمان: ۱۳:۳۰ الی ۱۵:۳۰		نشست ۳
مبانی رمز شناسی (۱)		
روسای نشست: دکتر ترانه اقلیدس-دکتر زهرا احمدیان		
سخنران مدعو: Dr. Hosein Hadipour, Ruhr University Bochum **Automating Cryptanalysis: Automated Reasoning and Structural Links Between Attacks**		

نویسندگان	عنوان مقاله
Akram Khalesi and Zahra Ahmadian	**Integral Attack on CHILOW**
Marzieh Vahid Dastjerdi, Majid Rahimi, Iman Mirzaali Mazandarani, and Sadegh Sadeghi	**Evaluating CNF/SMT Encodings for SAT-Based Differential Cryptanalysis of Lightweight Ciphers**
Javad Alizadeh and Bahman Madadi	**Differential and Linear Cryptanalysis of Reduced-Round GFRX-64 Using Neural Distinguishers and SAT/SMT-Based Technique**
Arka Debnath and Mohammad Mahzoun	**Fast Exhaustive Search on AIM2**

Integral Attack on CHILOW

Akram Khalesi[1], Zahra Ahmadian[2]
[1]Reasearch Center for Development of Advanced Technologies, Iran-[2]Shahid Beheshti University, Iran

Abstract: CHILOW is a family of tweakable block ciphers introduced at Eurocrypt 2025, designed to prioritize decryption speed over encryption speed. This is achieved through a low-latency nonlinear layer of degree two within the round function and a minimal number of rounds. As a result, CHILOW presents an appealing target for attacks that exploit its algebraic properties. These characteristics, along with the strict query limitations imposed by the designers, motivate our investigation into CHILOW's security against integral attacks leveraging the division property. We have identified several integral distinguishers, which vary in data complexity and the number of balanced output bits. Specifically, for CHILOW-(32+t), we derived a 4-round distinguisher with 15 constant bits in the input, in which all the 32 output bits are balanced. However, the longest integral distinguisher that complies with query limitations extends up to 3 rounds. For CHILOW-40, integral distinguishers up to 5 rounds are detected; however, only those spanning 3 rounds meet the query constraints.

Evaluating CNF/SMT Encodings for SAT-Based Differential Cryptanalysis of Lightweight Ciphers

Marzieh Vahid Dastjerdi[1,2], Majid Rahimi[2], Iman Mirzaali Mazandarani[3], and Sadegh Sadeghi[1]
[1]Institute for Advanced Studies in Basic Sciences (IASBS), Iran-[2]Research Center for Development of Advanced Technologies, Tehran, Iran-[3]Shahid Rajaee Teacher Training University, Iran

Abstract: This study evaluates three encoding methods for automated differential cryptanalysis: (1) SMT formulations (using CVC), (2) standard CNF, and (3) size-optimized CNF (via Logic Friday). We assess these using four SAT/SMT solver types: single-core (CryptoMiniSat-v5, CaDiCaL), multi-core (Treengeling), and massively parallel Mallob-novel to cryptanalysis. Encoding-solver combinations are tested on seven lightweight block ciphers representing distinct design philosophies: SPECK-32 and CHAM-64 (ARX structure), SIMON-32 (AND-RX structure), PRESENT, GIFT-128, and MIDORI-64 (4-bit S-box in SPN structure), and LBLOCK (Feistel structure). For each cipher, SAT/SMT instances targeting specific rounds/differential weights were generated, with wall-clock solving time, parallel efficiency, and modeling effort measured. Our results establish criteria for optimal encoding-solver pairings that strike a balance between modeling simplicity and computational performance. Crucially, Mallob emerges as the state-of-the-art framework for large-scale automated differential cryptanalysis.

Differential and Linear Cryptanalysis of Reduced-Round GFRX-64 Using Neural Distinguishers and SAT/SMT-Based Technique

Javad Alizadeh[1] and Bahman Madadi[1]
[1]Imam Hossein University, Iran

Abstract: In 2023, Zhang et al. introduced the lightweight block cipher family GFRX-b/k, based on SIMON. The designers referenced the cryptanalysis conducted on the SIMON-32 and claimed that the GFRX-64/128, with higher than 19 and 13 rounds, is resistant to differential and linear cryptanalysis, respectively. In this paper, we examine the differential and linear cryptanalysis of GFRX-64/96 and GFRX-64/128.We first introduce baseline neural distinguishers for up to 7 rounds of the GFRX-64/96. Subsequently, we extend a 6-round neural distinguisher by adding 2 rounds to perform a key recovery attack, achieving an 8-round key rank analysis through a deep learning-based approach. Furthermore, we conduct an automated cryptanalysis of GFRX-64 using a SAT/SMT-based framework, identifying an 11-round differential distinguisher with a probability of \math (2^{-62}), a 14-round linear distinguisher with a correlation of \math(2^{-31}), and a 17-round linear hull with a correlation of \math(2^{-31.61}). These results indicate that reducing the differential and linear cryptanalysis of the GFRX block cipher to the differential and linear cryptanalysis of the SIMON block cipher cannot yield accurate results or bounds. To the best of our knowledge, this work represents the first third-party cryptanalysis of the GFRX block cipher, offering new insights into its security.

Fast Exhaustive Search on AIM2

Arka Debnath[1] and Mohammad Mahzoun[2]
[1]KU Leuven, Belgium- [2]Eindhoven University of Technology, Netherlands

Abstract: This paper describes a fast exhaustive search preimage attack on AIM2, an improved version of the one-way function AIM, proposed to address algebraic vulnerabilities found in its predecessor. Our attack transforms the polynomial system describing AIM2 over \(\mathbb{F}_{2^{\lambda}}\) to a boolean polynomial system over \(\mathbb{F}_{2}\), allowing for an exhaustive search by guessing input bits and solving a resulting linear system. Solving the whole system is not necessary for most incorrect guesses, and use of gray code helps optimizing the iteration over all the possible guesses. Our results show that the complexity of exhaustive search on AIM2, especially AIM2-I and AIM2-III is lower than previously estimated, though still higher than that of AES.

تاریخ: ۱۶مهرماه ۱۴۰۴	سالن: H1	پنجشنبه
زمان: ۸:۰۰ الی ۱۰:۰۰		نشست ۴
پیاده‌سازی الگوریتم‌های رمزنگاری و حملات مرتبط		
روسای نشست: دکتر بیژن علیزاده-دکتر راضیه سالاری فرد		

نویسندگان	عنوان مقاله
Zahra Mohammadi, Mona Hashemi, and Siamak Mohammadi	**Securing Deep Learning Hardware: A Survey of Side-Channel Vulnerabilities and Countermeasures**
Marzieh Morshedzadeh, Rayhaneh Hajimohammadali, and Ali Jahanian	**Defending CNNs Against Power Side-channel Attacks: A Residue Number System Solution**
Farid Rajabzadeh and Ali Jahanian	**Information Leakage Mitigation to Protect the Convolutional Neural Networks Against the Remote Side-Channel Analysis**
Sepehr Jafari and Raziyeh Salarifard	**Enhancing Kleptographic Backdoors in Hash-Based Deterministic Random Bit Generators**
Vahid Soleimani Hesari, Hadi Soleimany, Ali Asghar Beigizad, and Hamed Ramzanipour	**Linked Ineffective Fault Analysis on DES Cipher**

Securing Deep Learning Hardware: A Survey of Side-Channel Vulnerabilities and Countermeasures

Zahra Mohammadi[1], Mona Hashemi[1], and Siamak Mohammadi[1]
[1] University of Tehran, Iran

Abstract: As deep learning models are increasingly deployed in critical sectors such as healthcare, finance, and security, ensuring their protection against emerging threats has become crucial. Among these threats, side-channel attacks(SCAs) represent a particular challenge since they can extract sensitive information such as model architectures, parameters, and even user inputs without requiring direct access to the model. By leveraging the physical and micro-architectural properties of the hardware, attackers can compromise systems. This survey begins by classifying leakage sources and attacker objectives, then analyzes representative studies that demonstrate practical side-channel exploits against deep-learning hardware. It also reviews existing defenses aimed at mitigating these vulnerabilities and concludes by outlining key open research challenges and potential future directions.

Defending CNNs Against Power Side-channel Attacks: A Residue Number System Solution

Marzieh Morshedzadeh[1], Rayhaneh Hajimohammadali[1], and Ali Jahanian[1]
[1]Shahid Beheshti University, Iran

Abstract: The capabilities of neural networks are advancing rapidly, enabling solutions to a wide range of problems, such as autonomous vehicles and medical applications. Despite their advancements, these models embed sensitive information, making them attractive targets for attackers. As a result, attacks on neural networks, particularly side-channel attacks that aim to expose key parameters, have become increasingly prevalent. Researchers are actively exploring various methods to defend against these adversarial attacks. Thispaper examines how modular arithmetic enhances the security of neural networks against side-channel attacks. Our approach involves demonstrating how modular arithmetic can improve neural network security. We conduct a thorough analysis to understand the impact and parameters that influence this improvement. By carefully selecting factors within the computational system and the target network, neural network security can be significantly enhanced through appropriate modular arithmetic systems. Experimental results on FPGA hardware validate our approach, showing a 2 to 3 times increase in resilience against side-channel attacks, while preserving classification accuracy.

Information Leakage Mitigation to Protect the Convolutional Neural Networks Against the Remote Side-Channel Analysis

Farid Rajabzadeh[1] and Ali Jahanian[1]
[1]Shahid Beheshti University, Iran

Abstract: Machine learning systems, despite exhibiting high inference accuracy in practical applications, are susceptible to security and reliability concerns both during the training phase and the inference phase. In this paper, we have demonstrated that it is possible to extract internal information from a neural network without physical access. This attack was executed through the utilization of a power sensor. This paper reveals that between 20,000 and 50,000 power samples of a 16-bit neural network weight can be retrieved. The final step involved hardening the neural

network against side-channel attacks. Test results in this section demonstrate that it is possible to make the neural network resistant to first-order side-channel attacks with an area overhead of about 6%. The degree of reinforcement was measured using the assumption test method, revealing that the attack has become eight times more challenging.

Enhancing Kleptographic Backdoors in Hash-Based Deterministic Random Bit Generators

Sepehr Jafari[1] and Raziyeh Salarifard[1]
[1]Shahid Beheshti University, Iran

Abstract: Deterministic Random Bit Generators (DRBGs) are essential for cryptographic security but remain vulnerable to covert kleptographic attacks that implant backdoors to leak sensitive information. Despite being known for two decades - as demonstrated by incidents like Snowden revelations and Dual-EC - these attacks persist in modern protocols, including TLS and post-quantum systems. This paper introduces a novel kleptographic backdoor for hash-based DRBGs using a dual-phase design: secret information is split across two complementary infected output phases, requiring both for recovery. This significantly increases complexity compared to conventional approaches. To enhance indistinguishability, we integrate randomness derived from the discrete logarithm problem, ensuring statistical conformity. Leveraging El-Gamal encryption for compatibility with this approach, we create a highly covert backdoor. Rigorous validation via the NIST Statistical Test Suite (STS) and neural network-based anomaly detection confirms the backdoor passes all NIST tests while evading machine learning detection, maintaining statistical integrity and structural consistency.

Linked Ineffective Fault Analysis on DES Cipher

Vahid Soleimani Hesari[1], Hadi Soleimany[1], Ali Asghar Beigizad[1], and Hamed Ramzanipour[2]
[1] Shahid Beheshti University, Iran, Iran-[2]Shahid Rajaee Teacher Training University, Iran

Abstract: Linked Ineffective Fault Analysis (LIFA) is a novel fault analysis technique that operates withoutrequiring input control and demonstrates resilience against noise compared to Statistical Ineffective Fault Analysis (SIFA), while maintaining similar attack assumptions. However, prior studies on LIFA have focused primarily on SPN block ciphers, leaving the security of the DES cipher one of the Feistel ciphers unexplored. Furthermore, the application of LIFA in the presence of multiple faults remains unaddressed. This paper bridges these gaps by applying LIFA to the widely utilized DES cipher, aiming to evaluate the effectiveness of this attack on Feistel-based structures. We effectively apply LIFA across various scenarios and demonstrate the feasibility of inducing multiple linked faults. Our results reveal that the nibble-based structure of DES allows for the establishment of two simultaneous links instead of one, significantly enhancing the efficacy of fault attacks on DES. To validate our approach, we conducted both simulations and real-world experiments using frequency glitch fault injection on an ATMEGA328p microcontroller. The results show that the proposed LIFA framework for the DES cipher achieves superior performance compared to existing methods such as SIFA, further advancing the state of cryptographic fault analysis.

تاریخ: ۱۶ مهرماه ۱۴۰۴	سالن: H2	پنجشنبه
زمان: ۸:۰۰ الی ۱۰:۰۰		نشست ۵
نهان‌نگاری اطلاعات		
روسای نشست: دکتر محمدعلی اخایی-دکتر زهرا سعیدی		
نویسندگان	**عنوان مقاله**	
محمد علی طائی زاده، مسعود عمومی، جلال ذهبی	**روشی نوین و بهینه شده در پنهان‌نگاری دی ان ای با استفاده از تولید جدول تصادفی و قطعه‌بندی**	
Donya Sadat Rezaeishad and Hossein Bahramgiri	**Dual-Layered Quantum-Secure Concealing: Steganography over Quantum Key Distribution**	
Majid Farhadi, Zohre Karimi, and Mohammad Amin Khorzani	**A Secure and Verifiable Secret Sharing Scheme Using Neural Steganography and Hash Based Authentication**	
Khashayar Jafarizade, Mohammad-Hassan Majidi, and Hossein Gholamalinejad	**Architected Graph-Enhanced Neural Network Framework for Image Integrity and Tamper Precision**	
Zahra Ghoraeian, Mohammad-Reza Sadeghi, and Samaneh Mashhadi	**Time-Based Steganography in Text**	

روشی نوین و بهینه شده در پنهان‌نگاری دی ان ای با استفاده از تولید جدول تصادفی و قطعه‌بندی

محمد علی طائی‌زاده[۱]، مسعود عمومی[۱]، جلال ذهبی[۱]
[۱]دانشگاه صنعتی اصفهان، ایران

چکیده: به‌دلیل محدودیت‌های رسانه‌هایی مانند تصویر، ویدئو و صوت در پنهان‌سازی اطلاعات، پژوهشگران به استفاده از رسانه‌های جایگزین روی آورده‌اند. امروزه دی ان ای به عنوان یکی از رسانه‌های پوششی جهت پنهان‌سازی اطلاعات پیشنهاد شده است. ویژگی هایی همچون ظرفیت بالای پنهان‌سازی، ساختارهای غیرقابل پیش بینی و نیاز کمتر به توان محاسباتی، آن را از سایر رسانه‌ها متمایز می‌کند. پژوهش‌های متعددی در زمینه استفاده از دی ان ای جهت پنهان‌سازی اطلاعات انجام شده است؛ برخی از این روش‌ها از خواص بیولوژیکی دی ان ای جهت پنهان سازی استفاده می‌کنند. با این حال، چالش‌هایی همچون ظرفیت پایین، بی‌توجهی به ساختار ژنتیکی و استفاده از الگوهای پنهان‌سازی منظم، در بسیاری از روش‌های موجود مشاهده می‌شود که می‌تواند احتمال شناسایی پیام پنهان را افزایش دهد. در این پژوهش، روشی ارائه شده که با استفاده از جدول‌های رمزگذاری تصادفی و الگوهای پنهان‌سازی غیرقابل پیش‌بینی، عملکرد بهتری نسبت به روش‌های قبلی فراهم می‌کند. این روش ویژگی‌هایی نظیر پیلود صفر، کوری، حفظ عملکرد بیولوژیکی، ظرفیت پنهان‌سازی بالا، نرخ تغییر پایین و احتمال پایین شناسایی را فراهم می‌کند.

Dual-Layered Quantum-Secure Concealing: Steganography over Quantum Key Distribution

Donya Sadat Rezaeishad[1] and Hossein Bahramgiri[2]
[1]Isfahan University of Technology, Iran- [2]Malek-Ashtar University of Technology, Iran

Abstract: In the quantum computing era, classical encryption faces unprecedented vulnerabilities, while Quantum Key Distribution (QKD) alone remains insufficient for top-secret data transmission due to practical hardware flaws. This paper proposes a novel dual-layered framework integrating steganography with QKD to enhance security and concealment. Our protocol embeds encrypted messages within QKD keys during post-processing, leveraging existing infrastructure without hardware modifications. The message is first compressed, encodes, and encrypted using a pre-shared QKD key via one-time-pad encryption. A block-based search mechanism then hides message bits within the sifted key while preserving statistical randomness. Crucially, this approach provides two-layer security: information-theoretic encryption via QKD and undetectable message existence. Evaluations confirm ultra-low failure probabilities of embedding (below \(10^{-12}\) for 1,000-bit messages) and minimal deviations in sifted key length (under \(1\%\) for typical blocks). The solution enables eavesdropper detection, maintaining full compatibility with standard QKD post-processing. By unifying steganographic stealth with QKD's theoretical security, this work establishes a practical solution for transmitting top-secret data against evolving quantum threats.

A Secure and Verifiable Secret Sharing Scheme Using Neural Steganography and Hash Based Authentication

Majid Farhadi[1], Zohre Karimi[1], and Mohammad Amin Khorzani[1]

[1] Damghan University, Iran

Abstract: This study presents a resilient and efficient architecture for secure secret distribution over public and untrusted networks. The proposed method combines Shamir's Verifiable Secret Sharing with AES-GCM encryption to ensure confidentiality and authentication. Each share is validated through cryptographic hash-based signatures and seamlessly concealed within cover images using a neural steganographic framework built upon an Attention U-Net augmented with transformer mechanisms. The training process is guided by a joint perceptual and structural loss function, improving both visual fidelity and feature retention. Experimental evaluations indicate superior performance in terms of PSNR and SSIM, along with minimal Bit Error Rate under various distortions such as noise addition, image blurring, and JPEG compression. Compared to existing approaches, the framework exhibits stronger resistance to fraudulent behavior by participants or the dealer, removes the dependency on secure private communication channels, enables reusability of system components, and maintains robust compression tolerance. Its lightweight computational demands make it especially suited for environments with limited processing power, ensuring its practicality for scalable, media-based secure secret sharing applications.

Architected Graph-Enhanced Neural Network Framework for Image Integrity and Tamper Precision

Khashayar Jafarizade[1], Mohammad-Hassan Majidi[1], and Hossein Gholamalinejad[2]

[1]University of Birjand, Iran- [2]Bozorgmehr University of Qaenat, Iran

Abstract: Image authenticity is a perennial issue with the evolution of advanced tampering techniques, particularly grid-aligned manipulations and spatial vulnerability-exploiting post-processing attacks. The paper presents a novel architecture for a neural network fusing Graph Neural Networks (GNNs), Convolutional Neural Networks (CNNs), and digital watermarking to detect tampering successfully and localize it. CNNs are trained on learning local spatial features, and an invisible low-dropout convolutional encoder places watermarks to ensure authenticity. GNNs address the inherent problem of modeling long-range structural relations for blind tampering pattern detection that is accurate. With a graph-based representation of image blocks, the framework learns complex spatial relations, which alleviates the rigid receptive field limitation. Extensive experiments on benchmark datasets confirm the framework's superiority, achieving an F1-Score of 0.94 in tampering localization, which significantly outperforms the 0.88 F1-Score of leading state-of-the-art methods. This approach creates a new standard for image authentication, offering an interpretable and scalable solution with far-reaching applications in digital content protection**.**

Time-Based Steganography in Tex

Zahra Ghoraeian[1], Mohammad-Reza Sadeghi[1], and Samaneh Mashhadi[2]
[1]Amirkabir University of Technology, Iran-[2] Iran University of Science & Technology, Iran

Abstract: Preserving data confidentiality is crucial in today's digital world where data exchange is increasingly becoming digital. This paper presents a novel text steganography algorithm. Initially, the text is converted into a bit stream, then the bit stream is shuffled using a random sequence, and finally, the data is converted into "time" (including date and hour), and an image suitable for embedding is generated, and the date is embedded within it. The results demonstrate that the proposed algorithm is robust against a variety of attacks, including retyping, OCR, printing and photocopying, compression, document feature modification, non-Unicode environment conversion, and semantic

paraphrasing. The algorithm is language-independent and applicable to all languages. The scheme exhibits high transparency against visual and machine attacks and has a capacity of 18 bits per "time". Embedding information bits using a random sequence enhances the scheme's resistance against detection attacks**.**

تاریخ: ۱۷مهرماه ۱۴۰۴	سالن: H3	پنجشنبه
زمان:۰۰:۸ الی ۰۰:۱۰		نشست ۶
علم و صنعت افتا		
سخنران مدعو: دکتر سولماز سلیمی، EURECOM تحلیل آلودگی فراتر از آسیب‌پذیری‌های کلاسیک: چالش ره‌گیری داده در مرزهای ناهمگون نرم افزار، سخت افزار و شبکه		
روسای نشست: دکتر مرتضی امینی-دکتر صادق دری نوگورانی		

نویسندگان	عنوان مقاله
Hamid Reza Dashtabadi and Siavash Ahmad	**Network Intrusion Detection using Federated Learning in Cyber-Physical Systems**
Zahra Bastani, Peyman Pahlevani, Rouhollah Sadr Mohammadi, and Abolfazl Mortezapour	**Evaluating DDoS Attacks Using IoT Communication Protocols Internet of Things Distributed Denial of Service attacks Cybersecurity**
Mahdi Jeyhoon and Maryam Rajabzadeh Asaar	**5G Attacks: Realistic Scenarios and Simulations Using Open5GS**
Togu Novriansyah Turnip, Birger Andersen, and Cesar Vargas-Rosales	**Recent Trends in Post-Quantum Cryptography Integration and Performance in the Internet Security Stack**

Network Intrusion Detection using Federated Learning in Cyber-Physical Systems

Hamid Reza Dashtabadi[1] and Siavash Ahmadi[1]
[1]Sharif University of Technology, Iran

Abstract: The increasing integration of modern network infrastructure into industrial control systems elevates the need for robust cyber intrusion detection for industrial protocols. Unsupervised, anomaly-based machine learning methods are particularly well-suited for this task, as they can identify novel attacks by learning a model of normal network behavior without requiring access to scarce attack samples. While techniques like autoencoders, which use reconstruction error to flag deviations, can be effective, their application is often hindered by practical challenges, such as regulatory constraints and the large volumes of data that prohibit the centralized collection required for training. Federated learning offers a solution by distributing the training process to local clients and aggregating only the resulting model parameters, thus preserving data privacy and locality. This paper proposes an anomaly-based intrusion detection framework built on federated learning. Using the CIC-Modbus2023 dataset, which comprises raw Modbus traffic from a smart grid, we systematically extract and label network flows based on attack logs. We then train and evaluate several autoencoder variants-including standard, variational, and adversarial autoencoders-within this federated setting. Our results demonstrate strong performance in detecting malicious activities, highlighting the framework's potential as a promising approach for mitigating threats against the Modbus protocol without centralized data access.

Evaluating DDoS Attacks Using IoT Communication Protocols Internet of Things Distributed Denial of Service Attacks Cybersecurity

Zahra Bastani[1], Peyman Pahlevani[1], Rouhollah Sadr Mohammadi[1], and Abolfazl Mortezapour[1]
[1]Institute for Advanced Studies in Basic Sciences (IASBS), Iran

Abstract: With the rapid expansion of the Internet of Things (IoT) and the growing dependence on connected devices, cybersecurity has become one of the major challenges in this domain. Distributed Denial of Service (DDoS) attacks, by exploiting vulnerabilities in communication protocols, can disrupt legitimate user access and degrade system performance. This study evaluates and compares the performance of three common IoT communication protocols-HTTP, MQTT, and CoAP-under various DDoS attack scenarios. The evaluation metrics include system saturation time, CPU utilization, and memory consumption. The results indicate that MQTT at QoS level 1 exhibits the highest CPU usage and the lowest resistance to saturation. Although HTTP shows relatively stable resource consumption in some scenarios, due to its high memory and processing overhead, it is considered more vulnerable compared to lightweight protocols such as CoAP and MQTT (QoS 0).

5G Attacks: Realistic Scenarios and Simulations Using Open5GS

Mahdi Jeyhoon[1] and Maryam Rajabzadeh Asaar[1]
[1]Islamic Azad University, Science and Research Branch, Iran

Abstract: The evolution of fifth-generation cellular networks (5G) brings unprecedented improvements in speed, latency, and scalability. However, it also introduces significant new security challenges. This paper presents a scenario-based simulation study of three distinct denial-of-service (DoS) attacks targeting critical components of the 5G architecture. Using open-source tools such as Open5GS, the study simulates and analyzes vulnerabilities affecting the next-generation NodeB (gNB), the Access and Mobility Management Function (AMF), and the User Equipment (UE). In the first scenario, a large volume of registration requests is used to overload both the gNB and the AMF. The second scenario specifically targets the AMF, where a flood of fraudulent gNB registration attempts consumes its

resources and prevents it from handling legitimate connections. The third scenario involves the misuse of a security-related field in the UE registration process and disrupting the authentication procedures. For the evaluation, the consumption of processing resources is used as the main criterion. In each scenario, a specific attack idea is used. In addition, the scenario-based simulation approach adopted in this study allows exploring and implementing different types of attacks at different layers of the 5G network**.**

Recent Trends in Post-Quantum Cryptography Integration and Performance in the Internet Security Stack

Togu Novriansyah Turnip[1], Birger Andersen[1], and Cesar Vargas-Rosales[2]
[1]Technical University of Denmark, Denmark- [2]Tecnologico de Monterrey, Mexico

Abstract: The rapid advancement of quantum computing poses a direct threat to classical public-key cryptographic systems at the core of Internet security protocols. Post-quantum cryptography (PQC) has therefore become central to ongoing standardization and early deployment efforts. This paper presents a comparative analysis of PQC integration into TLS, SSH, and IPsec, examining cross-cutting challenges, protocol-specific trade-offs, and deployment considerations. Our findings show that PQC adoption introduces markedly uneven overheads across protocols: handshake latency may increase by up to 600% in TLS, by 29% in SSH, and by up to 300% in IPsec, while memory requirements in hybrid configurations can exceed 300 KB in resource-constrained environments. We further demonstrate that message fragmentation, certificate chain expansion, and cumulative rekeying costs emerge as protocol-dependent bottlenecks, underscoring that migration strategies must be tailored to the architecture and operational context of each protocol. Beyond performance, we identify interoperability gaps, downgrade vulnerabilities, and side-channel risks as critical obstacles to secure deployment. By combining empirical performance evidence with a structured review of challenges and deployment strategies, our study provides actionable insights for practitioners, informs ongoing standards development, and highlights research priorities essential to building a resilient, quantum-resistant Internet infrastructure.

تاریخ: ۱۷ مهرماه۱۴۰۴	سالن: H1	پنجشنبه
زمان: ۱۳:۳۰ الی ۱۵:۳۰		نشست ۷
پروتکل‌های امنیتی		
روسای نشست: مهندس جواد مهاجری، دکتر هادی شهریار شاه حسینی		
سخنران مدعو: دکتر مانده مشرف، استادیار دانشگاه شهید بهشتی امنیت در متاورس: تحلیل تهدیدات و راهکارهای مقابله		

نویسندگان	عنوان مقاله
Sina Fattahi Ardakani and Maedeh Mosharraf	**Decentralized Plagiarism Detection System for Open Textual Educational Resources based on Blockchain Technology**
Seyede Marzieh Sadat Madani, Hamid Mala, and Mehrad Jaberi	**An Efficient ECC-Based Multi-Server Authentication Scheme for 5G Environment without Online Registration Server**
S. Mohammad Dibaji, Taraneh Eghlidos, and Hossein Pilaram	**QuMixnet: A Quantum-Safe Mixnet Protocol**
Keykhosro Khosravani, Taraneh Eghlidos, and Mohammad Reza Aref	**Efficient Pairing-Free Adaptable k-out-of-N Oblivious Transfer Protocols**
Ahmad Khoureich Ka	**Secure Pairing-Free IBE and CP-ABE from Inner-Product Functional Encryption**

Decentralized Plagiarism Detection System for Open Textual Educational Resources based on Blockchain Technology

Sina Fattahi Ardakani[1] and Maedeh Mosharraf[1]
[1]Shahid Beheshti University, Iran

Abstract: Open Educational Resources (OER) have become a valuable tool for expanding access to quality education. However, managing intellectual property rights in OER environments remains a challenge, particularly in verifying content authenticity and protecting creators' rights. To address this, the study proposes a decentralized approach to copyright management for OER. Our solution processes OER textual content using defined windows and the Locality Sensitive Hashing (LSH) algorithm to efficiently detect exact and partial similarities. By integrating blockchain technology and the InterPlanetary File System (IPFS), we establish a transparent, decentralized platform for storing and managing resources. The proposed system was implemented and tested on 2600 OER articles achieving 100 percent precision and recall, on direct and paraphrased plagiarism test sets. The results indicate that this technological integration can serve as a robust foundation for enhancing transparency and protecting authors' rights within the OER ecosystem.

An Efficient ECC-Based Multi-Server Authentication Scheme for 5G Environment without Online Registration Server

Seyede Marzieh Sadat Madani[1], Hamid Mala[1], and Mehrad Jaberi[1]
[1]University of Isfahan, Iran

Abstract: Multi-Server Authentication and Key Agreement (MAKA) protocols in 5G networks play a pivotal role in securing communications due to their widespread applications in domains such as drones, cellular networks, and secure communications. We propose a novel and efficient protocol for multi-server authentication and key agreement in 5G networks, based on Elliptic Curve Cryptography (ECC). The proposed protocol is secure against attacks such as user and server impersonation, password guessing, insider attacks, tracking, session key disclosure, replay, denial-of-service, and man-in-the-middle attacks. Additionally, distinctive features such as user anonymity, avoidance of bilinear pairing, key confirmation, perfect forward secrecy, and the ability to perform authentication without an online registration server make the proposed scheme more efficient and secure, compared to previous schemes. Formal analysis using Proverif cryptographic protocol verifier, confirms the protocol's confidentiality and authentication properties, while its computational and communication efficiency demonstrates relative superiority over comparable schemes.

QuMixnet: A Quantum-Safe Mixnet Protocol

S. Mohammad Dibaji[1], Taraneh Eghlidos[1], and Hossein Pilaram[1]
[1]Sharif University of Technology, Iran

Abstract: The emergence of quantum computing threatens the security of traditional cryptographic primitives underpinning anonymous communication protocols like mix networks (mixnets), necessitating quantum-resistant alternatives. This paper introduces QuMixnet, a mixnet protocol designed to withstand quantum attacks while ensuring robust anonymity and privacy. QuMixnet employs post-quantum cryptographic primitives, utilizing CRYSTALS-Dilithium for digital signatures to guarantee authenticity and CRYSTALS-Kyber for key encapsulation to secure message encryption with symmetric ciphers (e.g., AES-GCM). Operating on a peer-to-peer (P2P) architecture, every node can serve as a sender, receiver, or mix node, enhancing anonymity by obscuring participant roles. Sender-determined routing ensures that only the sender knows the full message path, with onion routing layered encryption across nodes. To counter traffic analysis, QuMixnet implements message padding to a fixed size, dummy messages

for traffic covering, and batch processing with shuffling. A security model, evaluated through formal security games, confirms resilience of QuMixnet against adversaries with quantum capabilities, achieving strong sender and receiver anonymity, communication anonymity, confidentiality, and integrity. QuMixnet advances anonymous communication by offering a scalable, quantum-safe solution that fortifies privacy against evolving threats.

Efficient Pairing-Free Adaptable k-out-of-N Oblivious Transfer Protocols

Keykhosro Khosravani[1], Taraneh Eghlidos[1], and Mohammad Reza Aref[1]
[1] Sharif University of Technology

Abstract: Oblivious Transfer (OT) is one of the fundamental building blocks in cryptography that enables various privacy-preserving applications. Constructing efficient OT schemes has been an active research area. This paper presents three efficient two-round pairing-free k-out-of-n oblivious transfer protocols with standard security. Our constructions follow the minimal communication pattern: the receiver sends k messages to the sender, who responds with n+k messages, achieving the lowest data transmission among pairing-free k-out-of-n OT schemes. Furthermore, our protocols support adaptivity and also, enable the sender to encrypt the n messages offline, independent of the receiver's variables, offering significant performance advantages in one-sender-multiple-receiver scenarios. We provide security proofs under the Computational Diffie-Hellman (CDH) and RSA assumptions, without relying on the Random Oracle Model. Our protocols combine minimal communication rounds, adaptivity, offline encryption capability, and provable security, making them well-suited for privacy-preserving applications requiring efficient oblivious transfer.

Secure Pairing-Free IBE and CP-ABE from Inner-Product Functional Encryption

[1]Ahmad Khoureich Ka

[1]Alioune Diop University of Bambey, Senegal

Abstract: The potential of Attribute-Based Encryption (ABE) in the context of IoT has driven researchers to propose pairing-free ABE schemes that are suitable for resource-constrained devices. Unfortunately, many of these schemes turned out to be insecure. This fact seems to reinforce the point of view of some researchers according to which instantiating an Identity-Based Encryption (IBE) in plain Decisional Diffie-Hellman (DDH) groups is impossible. In this paper, we provide a generic Ciphertext-Policy ABE (CP-ABE) scheme with secret AND gate policy from Inner-Product Functional Encryption (IPFE). We also propose an instantiation of that generic CP-ABE scheme from the DDH assumption. From our generic CP-ABE scheme we derive an IBE scheme by introducing the concept of Clustered Identity-Based Encryption (CIBE). Our schemes show that it is possible to construct secure IBE and ABE schemes based on the classical DDH assumption. An implementation of our CIBE in Python using the Charm framework is available on GitHub.

تاریخ: ۱۷ مهرماه ۱۴۰۴	سالن: H2	پنجشنبه
زمان: ۱۳:۳۰ الی ۱۵:۳۰		نشست ۸

هوش مصنوعی و امنیت محاسبات

روسای نشست: دکتر بهروز ترک لادنی-دکتر مجتبی خلیلی

نویسندگان	عنوان مقاله
Nima Atashin, Behrouz Tork Ladani, and Mohammadreza Sharbaf	**Learning to Locate: GNN-Powered Vulnerability Path Discovery in Open Source Code**
Arman Moradi, Mehran Alidoost Nia, and Reza Ebrahimi Atani	**A Multi-Objective Reinforcement Learning Framework for Security Enhancement in Autonomous Vehicles**
Mohammad Reza Mirbagheri, Seyed Mohammad Mahdi Mirkamali, Zahra Motoshaker Arani, Ali Javeri, Amir Mahdi Sadeghzadeh Mesgar, and Rasool Jalili	**EPT Benchmark: Evaluation of Persian Trustworthiness in Large Language Models**
Amirhossein Heydari, Azadeh Mansouri, and Ahmad Mahmoudi-Aznaveh	**Backdoor Defense via Aggregation of Outsourced Models using Multi-Stage Knowledge Distillation**
Keyhan Mohammadi, Ehsan Kozegar, and Reza Ebrahimi Atani	**HashLearner: A Secure Decentralized Learning Framework Based on HashGraph**

Learning to Locate: GNN-Powered Vulnerability Path Discovery in Open Source Code

Nima Atashin[1], Behrouz Tork Ladani[1], and Mohammadreza Sharbaf[1]
[1]University of Isfahan, Iran

Abstract: Detecting security vulnerabilities in open-source software is a critical task in research communities. Several approaches have been proposed for detecting vulnerable code and identifying classes of vulnerabilities. However, there is room to improve the explanation of root causes of detected vulnerabilities by locating vulnerable statements and discovering paths that lead to activation of the vulnerability. While frameworks like SliceLocator offer explanations by identifying vulnerable paths, they rely on rule-based sink identification that limits generalization. In this paper, we introduce VulPathFinder, an explainable vulnerability path discovery framework that enhances SliceLocator's methodology by utilizing a Graph Neural Network (GNN) for detecting sink statements, rather than predefined rules. The GNN captures semantic and syntactic dependencies to find potential sink points (PSPs), candidate statements where vulnerable paths end. After detecting PSPs, program slicing extracts vulnerable paths, which are ranked by feeding them into the graph-based detector. The most probable path is returned, explaining the root cause of the detected vulnerability. We demonstrate effectiveness by evaluations on a benchmark of buffer overflow CWEs from the SARD dataset, providing explanations for detected vulnerabilities. Results show VulPathFinder outperforms SliceLocator and GNNExplainer in discovery of vulnerability paths to identified PSPs.

A Multi-Objective Reinforcement Learning Framework for Security Enhancement in Autonomous Vehicles

Arman Moradi[1], Mehran Alidoost Nia[2], and Reza Ebrahimi Atani[1]
[1] University of Guilan, Iran-[2]Shahid Beheshti University, Iran

Abstract: Autonomous vehicles must balance road-safety objectives with growing cyber-security threats. In this paper, we present a reinforcement-learning framework that jointly optimizes driving performance and resilience to Denial-of-Service (DoS) attacks. The problem is formalized as a multi-objective Markov Decision Process that fuses a safety reward with a security reward, while partial observability of attacks is captured through a Bayesian belief. A Proximal Policy Optimization (PPO) agent controls steering, throttle, and dedicated mitigation actions. The system is implemented in the CARLA simulator with camera and LiDAR inputs and evaluated on urban driving scenarios. Experiments show that the agent maintains stable lane-keeping and target-speed behavior, while reduces collision-prone episodes and preserves over 90 % of nominal travel distance under attack conditions. The framework outperforms safety-only PPO baseline and a rule-based security countermeasure.

EPT Benchmark: Evaluation of Persian Trustworthiness in Large Language Models

Mohammad Reza Mirbagheri[1], Seyed Mohammad Mahdi Mirkamali[1], Zahra Motoshaker Arani[1], Ali Javeri1[1], Amir Mahdi Sadeghzadeh Mesgar[1], and Rasool Jalili[1]
[1]Sharif University of Technology, Iran

Abstract: Large Language Models (LLMs), trained on extensive datasets using advanced deep learning architectures, have demonstrated remarkable performance across a wide range of language tasks, becoming a cornerstone of modern AI technologies. However, ensuring their trustworthiness remains a critical challenge, as reliability is essential not only for accurate performance but also for upholding ethical, cultural, and social values. Careful alignment of training data and culturally grounded evaluation criteria are vital for developing responsible AI systems. In this study, we

introduce the EPT (Evaluation of Persian Trustworthiness) metric, a culturally informed benchmark specifically designed to assess the trustworthiness of LLMs across six key aspects: truthfulness, safety, fairness, robustness, privacy, and ethical alignment. We curated a labeled dataset and evaluated the performance of several leading models-including ChatGPT, Claude, DeepSeek, Gemini, Grok, LLaMA, Mistral, and Qwen-using both automated LLM-based and human assessments. Our results reveal significant deficiencies in the safety dimension, underscoring the urgent need for focused attention on this critical aspect of model behavior. Furthermore, our findings offer valuable insights into the alignment of these models with Persian ethical-cultural values and highlight critical gaps and opportunities for advancing trustworthy and culturally responsible AI. The dataset is publicly available at: \url{https://github.com/Rezamirbagheri110/EPT-Benchmark**}.**

Backdoor Defense via Aggregation of Outsourced Models using Multi-Stage Knowledge Distillation

Amirhossein Heydari[1], Azadeh Mansouri[1], and Ahmad Mahmoudi-Aznaveh[2]
[1]Kharazmi University, Iran-[2] Shahid Beheshti University, Iran

Abstract: Backdoor attacks pose a significant threat to deep learning systems by injecting hidden malicious behavior to the model while preserving high accuracy on clean data. Such attacks are particularly dangerous in scenarios where users rely on pre-trained models or outsource training to untrusted parties. In this work, we propose a practical defense strategy that assumes no knowledge of the backdoor trigger or the training process, relying on a small trusted clean dataset. Our method introduces a two-stage pipeline: First, we aggregate predictions from multiple potentially compromised models to train an intermediate Teacher-Aggregation (TA) model; then, we distill this knowledge into a compact light-weight student model. This multi-stage approach effectively alleviates backdoor effects while preserving clean accuracy. Experimental results on MNIST and CIFAR-10 demonstrate that our method significantly reduces the Attack Success Rate (ASR)-to approximately 0.1\% on MNIST and 2.6\% on CIFAR-10-outperforming baseline ensemble defenses. Furthermore, our lightweight student model is suitable for edge deployment, providing a generic and scalable defense that remains robust under minimal assumptions, making it well-suited for real-world applications in adversarial environments. Our code is available at: https://github.com/mr-pylin/backdoor-toolbox

HashLearner: A Secure Decentralized Learning Framework Based on HashGraph

Keyhan Mohammadi[1], Ehsan Kozegar[1], and Reza Ebrahimi Atani[1]

[1]University of Guilan, Rasht, Iran

Abstract: Federated learning enables collaborative model training without centralized data collection, but existing frameworks rely on a central server, introducing risks of single points of failure, adversarial manipulation, and privacy leakage. To address these challenges, we propose HashLearner, a secure decentralized learning framework that utilizes the HashGraph consensus protocol for model aggregation without trusted authorities. HashLearner introduces two key innovations: (i) a consensus-driven decentralized aggregation mechanism resilient to Byzantine adversaries, and (ii) a privacy-preserving shuffling strategy that mitigates gradient reconstruction and poisoning attacks. To handle heterogeneous data distributions, the framework further employs transfer learning–based personalization. The simulation results of HashLearner, tested on benchmark Kaggle datasets, demonstrate that the platform maintains high accuracy while significantly enhancing scalability, security and privacy. These findings demonstrate that HashLearner provides a practical path toward scalable, privacy-preserving, and trustworthy decentralized federated learning.

تاریخ: ۱۷ مهرماه ۱۴۰۴	سالن:H3	پنجشنبه
زمان: ۱۳:۳۰ الی ۱۵:۳۰		نشست ۹
مدیریت امنیت و حریم خصوصی و جرم‌یابی دیجیتال		
روسای نشست: دکترطلا تفضلی-دکتر صادق دری نوگورانی		
نویسندگان	عنوان مقاله	
Sajed Yousefi Mashhour, Motahareh Dehghan, Babak Sadeghian, and Alireza Hashemi	**Mission-Centric Countermeasure Selection in Cybersecurity Situation Awareness**	
Sajjad Rezaei and Ali Fanian	**Static Malware Detection in Windows Executables Using Deep Neural Networks**	
Sepehr Mehregan, Mahdi Tamjidi, Amir Hossein Rahimi, Ava Razavi, Sadegh Eskandari, and Seyed Amir Hossein Tabatabaei	**GP-FACL: A Dataset of FAlse Claim Descriptions and Functionalities of Google Play Apps**	
Mostafa Shabani and Tala Tafazzoli	**Lateral Movement Attack Detection using Variational Autoencoders**	
Seyede Fateme Mazhar and Azadeh Mansouri	**Feature Map Correlations in Video Face Forgery Detection**	

Mission-Centric Countermeasure Selection in Cybersecurity Situation Awareness

Sajed Yousefi Mashhour[1], Motahareh Dehghan[2], Babak Sadeghian[1], and Alireza Hashemi[1]

[1]Amirkabir University of Tehran, Iran- [2]Tarbiat Modares University, Iran

Abstract: Selecting optimal cybersecurity countermeasures requires integration with mission-critical objectives beyond technical risk minimization. This paper presents a mission-centric framework for countermeasure selection in cybersecurity situation awareness systems by extending the RiskMAP methodology with agent-based and discrete-event simulation. The framework employs a multi-criteria decision-making approach based on the Confidentiality, Integrity, and Availability (CIA) triad, weighing mission objectives and mapping vulnerabilities and threats using MITRE ATT&CK and D3FEND taxonomies. Candidate countermeasures are evaluated considering risk reduction, implementation cost, operational impact, and mission alignment. We demonstrate the approach through a case study on a critical infrastructure organization's network modeled in AnyLogic. Results show improved alignment between security posture and organizational priorities while maintaining effective risk reduction, outperforming traditional methods. This framework enables quantitative visualization and optimization of security investments relative to mission continuity. All simulation models, data, and scripts are openly available to support reproducibility.

Static Malware Detection in Windows Executables Using Deep Neural Networks

Sajjad Rezaei[1] and Ali Fanian[1]

[1]Isfahan University of Technology, Iran

Abstract: The widespread use of malware targeting Windows systems, especially through Portable Executable (PE) files, has led to considerable research in the field of malware detection. Although many approaches have been proposed, the increasing complexity and evasiveness of modern malware continue to present significant challenges, underscoring the need for further advancements indetection strategies [1]. This paper introduces a static malware detection framework based on deep learning and a set of carefully engineered binary features extracted directly from raw PE files. In contrast to conventional methods that rely on metadata or dynamic analysis, our approach performs detailed parsing of file headers, section layouts, entropy levels, import/export tables, and embedded resources to form a comprehensive feature set. A deep neural network is trained on these features, with its architecture and hyperparameters fine-tuned using Bayesian optimization. The model is evaluated on a balanced dataset of benign and malicious PE files, achieving high accuracy (98.81%) and an F1-score of 98.95%. Fully automated and independent of dynamic execution or commercial tools, the proposed solution is well-suited for deployment in real-world applications such as antivirus systems and intrusion detection platforms.

GP-FACL: A Dataset of FAlse Claim Descriptions and Functionalities of Google Play Apps

Sepehr Mehregan[1], Mahdi Tamjidi[1], Amir Hossein Rahimi[2], Ava Razavi[3], Sadegh Eskandari[1], and Seyed Amir Hossein Tabatabaei[1]

[1]University of Guilan, Iran- [2]Aston University, United Kingdom- [3] Brock University St. Catharines, Canada

Abstract: Mobile phones are among the most significant technological advancements, offering unmatched convenience and seamlessly integrating into modern lifestyles. However, their widespread use also facilitates both beneficial and harmful practices. The absence of comprehensive datasets with reliable app descriptions undermines user confidence in Google Play as a trustworthy software marketplace. In order to fill this gap, we present a brand new dataset in this study called GP-FACL. This dataset contains ``fake app" that make FAlse CLaims in their descriptions and pretend to offer features that do not actually exist. Applications were first manually collected, after which keywords were extracted to generate 2-gram key phrases. Then these key phrases were used to automate the collection of more applications. The final dataset provides a systematic approach for identifying false-claim applications across a variety of app categories. Our approach resulted in 117 applications verified to contain erroneous or misleading claims. This dataset offers researchers and practitioners a valuable resource for advancing fraud detection and mitigating deceptive applications on mobile platforms.
https://github.com/Sepehr-Mehregan/GP-FACL-A-Dataset-of-FAlse-CLaim-Descriptions-and-Functionalities-of-Google-Play-Apps.

Lateral Movement Attack Detection using Variational Autoencoders

Mostafa Shabani [1]and Tala Tafazzoli[1]

[1]ITRC, Iran

Abstract: Lateral movement, a sophisticated cyberattack strategy, enables adversaries to stealthily infiltrate networks following an initial breach. Detecting such maneuvers is exceptionally challenging, as they are designed to seamlessly

blend with legitimate system operations and network traffic, rendering traditional signature-based defenses ineffective. Supervised machine learning approaches, while promising, are constrained by their dependence on pre-labeled datasets of known attack patterns. To overcome these limitations, this study introduces a novel hybrid deep learning framework that integrates a Variational Autoencoder (VAE) for robust feature extraction, coupled with a supervised classifier to identify lateral movement. Through meticulous feature engineering on the LMD dataset, the VAE is trained exclusively on normative system and network behavior, constructing a probabilistic representation of legitimate activity. Anomalies, detected via reconstruction error, signal potential malicious intrusions. Empirical evaluation demonstrates the framework's superior performance, achieving a detection time of 00:00:02:54 and an AUC of 99.6983%, reflecting exceptional class separation and computational efficiency. This hybrid architecture delivers a scalable, high-accuracy solution, establishing the VAE as a pivotal tool for combating advanced persistent threats with unparalleled precision and operational viability.

Feature Map Correlations in Video Face Forgery Detection

Seyede Fateme Mazhar[1] and Azadeh Mansouri[1]

[1]Kharazmi University, Iran

Abstract: Face manipulation techniques have raised widespread public concern. Although conventional convolutional neural networks (CNNs) demonstrate satisfactory performance, they exhibit limitations in capturing the critical features that are directly affected by manipulation artifacts. Fake faces often exhibit unnatural correlations between feature maps, particularly in local patterns. The Gram matrix can illustrate these irregularities in feature map relationships and support the discrimination between real images from fake ones. In this paper, we show that the relationships among convolutional neural network feature maps typically display natural and coherent patterns, whereas manipulated faces tend to disrupt this consistency which can be effectively captured through analysis of the Gram matrix of the feature maps. Experimental results demonstrate that the proposed correlation-based features achieve satisfactory performance in both single-dataset and cross-dataset validation.

تاریخ: ۱۷ مهرماه ۱۴۰۴	سالن:H4	پنجشنبه
زمان: ۱۳:۳۰ الی ۱۵:۳۰		نشست ۱۰
مبانی رمزشناسی		
روسای نشست: دکتر ترانه اقلیدس-دکتر محمود احمدیان عطاری		
سخنران مدعو: دکتر اکرم خالصی، پژوهشگاه توسعهٔ فناوری‌های پیشرفته The Division Property and Its Automation: Development and Open Research Challenges		
نویسندگان	عنوان مقاله	
محمد بلوکیان، علی اصغر اروجی، منیره هوشمند	آماده‌سازی حالت از راه دور سه طرفه بهینه یک حالت تک کیوبیتی شناخته‌شده	
محمد بلوکیان و منیره هوشمند	طرح نوین تسهیم راز نیمه کوانتومی مقاوم بدون تبادل مستقیم کیوبیت حاوی پیام	

آماده‌سازی حالت از راه دور سه طرفه بهینه یک حالت تک کیوبیتی شناخته‌شده

محمد بلوکیان[۱]، علی اصغر اروجی[۱]، منیره هوشمند[۲]

[۱]دانشگاه سمنان، ایران- [۲]دانشگاه بین‌المللی امام رضا، ایران

چکیده: انتقال از راه دور کوانتومی، یکی از مهم‌ترین کاربردهای درهم‌تنیدگی کوانتومی است که با بهره‌گیری از زوج‌های درهم‌تنیده از پیش به اشتراک گذاشته‌شده، اعمال عملیات یکانی محلی و تبادل اطلاعات کلاسیکی، امکان ارسال حالت‌های کوانتومی ناشناخته را بدون انتقال فیزیکی ذره فراهم می‌سازد. در مقابل، در فرایند آماده‌سازی از راه دور حال، فرستنده از ابتدا نسبت به حالت کوانتومی هدف آگاهی دارد و تلاش می‌کند تا این حالت با کمترین میزان منابع کلاسیکی و کوانتومی در سمت گیرنده بازسازی شود. در این پژوهش، یک پروتکل نوین آماده‌سازی از راه دور سه‌طرفه ارائهٔ می‌شود که در آن سه کاربر قادرند هم‌زمان حالت‌های تک‌کیوبیتی دلخواه خود را ارسال و دریافت نمایند. کارایی این پروتکل نسبت به طرح‌های اخیر بررسی و مقایسه شده که نشان‌دهنده پیشرفت آن در ارتباطات کوانتومی است. پروتکل ارائه شده نه‌تنها بهره‌وری ارتباطی را افزایش می‌دهد، بلکه چنین ساختاری، با کاهش پیچیدگی محاسباتی و استفاده بهینه از منابع درهم‌تنیده، می‌تواند در کاربردهایی مانند کنترل و هماهنگی چندجانبه، رمزنگاری کوانتومی چندطرفه، و توزیع منابع کوانتومی بین چند کاربر مورد استفاده قرار گیرد. این ویژگی امکان می‌دهد یک حالت کوانتومی مشخص هم‌زمان بین چند گیرنده مشترک باشد، که در سناریوهای عملی شبکه‌های کوانتومی با چند کاربر اهمیت بالایی دارد.

طرح نوین تسهیم راز نیمه کوانتومی مقاوم بدون تبادل مستقیم کیوبیت حاوی پیام

[۱] محمد بلوکیان و[۲] منیره هوشمند

[۱]دانشگاه سمنان، ایران- [۲]دانشگاه بین‌المللی امام رضا، ایران

چکیده: در این مقاله یک طرح تسهیم راز نیمه کوانتومی ارائه شده که کاربر کوانتومی می‌خواهد یک پیام معین را با دو کاربر کلاسیکی به اشتراک بگذارد. کاربران به تنهایی نمی‌توانند به پیام معین دسترسی پیدا کنند و باید برای دسترسی به پیام معین با همدیگر همکاری کنند. در این مقاله یک پروتکل تسهیم راز نیمه کوانتومی با استفاده از مخابره از راه دور کوانتومی پیشنهاد شده و امنیت آن در برابر انواع حمله‌های دشمن بررسی می‌گردد. برخلاف پروتکل‌های قبلی تسهیم راز نیمه کوانتومی، در پروتکل پیشنهادی، فرستنده نیاز به حافظه کوانتومی و گیرنده‌ها نیاز به تولید کیوبیت جدید ندارند. هم‌چنین از آنجا که پروتکل پیشنهادی مبتنی بر مخابره از راه دور کوانتومی است، کیوبیت حامل اطلاعات بر روی کانال ارسال نمی‌گردد.

کارگاه‌ها

روز دوشنبه ۱۴ مهر ۱۴۰۴

زمان / مکان	۸:۳۰–۱۰:۰۰	۱۰:۳۰–۱۰:۴۵	۱۰:۳۰–۱۲:۰۰	۱۲–۱۳	۱۳–۱۴:۳۰	۱۴:۳۰–۱۵	۱۵–۱۶:۳۰
سالن همایش ها	آناتومی حملات سایبری کشور: بازیگران تهدید، تاکنیک‌ها و پیامدها (جلسه اول)	پذیرایی	آناتومی حملات سایبری کشور: بازیگران تهدید، تاکنیک ها و پیامدها (جلسه دوم)	استراحت	آموخته‌های حمایت سایبری: از تهدیدشناسی تا دفاع پیشگیرانه (جلسه اول)	استراحت	آموخته‌های حمایت سایبری: از تهدیدشناسی تا دفاع پیشگیرانه (جلسه دوم)
سالن همایش ها	هوش مصنوعی عاملی برای امنیت سایبری، خودکارسازی مدیریت ریسک با عامل‌های هوشمند (جلسه اول)	پذیرایی	هوش مصنوعی عاملی برای امنیت سایبری، خودکارسازی مدیریت ریسک با عامل‌های هوشمند (جلسه دوم)	استراحت	تحلیل عمیق، تصمیم دقیق، واکنش سریع؛ مرزهای تازه امنیت سایبری با هوش مصنوعی (جلسه اول)	استراحت	تحلیل عمیق، تصمیم دقیق، سریع؛ مرزهای تازه امنیت سایبری با هوش مصنوعی (جلسه دوم)
سالن همایش ها	سیستم‌های ارتباطات امن کوانتومی: مبانی، کاربردها و مسیرهای پیش‌رو (جلسه اول)	پذیرایی	سیستم‌های ارتباطات امن کوانتومی: مبانی، کاربردها و مسیرهای پیش‌رو (جلسه دوم)	استراحت	مقدمه‌ای کاربردی بر واترمارکینگ دیجیتال و استگانوگرافی با استفاده از MATLAB	استراحت	استنادپذیری ادله دیجیتالی موجود در تصاویر

روز سه شنبه ۱۵ مهر ۱۴۰۴

زمان / مکان	۸:۳۰-۱۰:۰۰	۱۰:۳۰-۱۰:۴۵	۱۰:۳۰-۱۲:۰۰	۱۲-۱۳	۱۳-۱۴:۳۰	۱۴:۳۰-۱۵	۱۵-۱۶:۳۰
سالن همایش‌ها	رفتار شناسی گروه‌های APT فعال در زیرساخت های حیاتی کشور	پذیرایی	امنیت برنامک‌های موبایل: تهدیدات نوین و ابزارهای تحلیل و تست نفوذ	استراحت	امنیت زنجیره تامین نرم افزار	استراحت	افزایش صحت و امنیت کد با استفاده از مدل های زبانی بزرگ: یک کارگاه عملی
سالن همایش‌ها	مرور بر حملات القای خطا	پذیرایی	مرور حملات بازخوانی کد در میکروکنترلرها ارائهٔ دو مورد عملی	استراحت	بایوس، امنیت و شخصی‌سازی آن	استراحت	احراز هویت با کارت هوشمند در سامانه‌های کنترل دسترسی: تحلیل آسیب‌ها و راهکارهای امن مبتنی بر استانداردهای جهانی
سالن همایش‌ها	فریب سایبری	پذیرایی	فارنزیک فناوری عملیاتی(OT)	استراحت	شناسایی و شکار مهاجمان سایبری در سیستم‌های کنترل صنعتی (جلسه اول)	استراحت	شناسایی و شکار مهاجمان سایبری در سیستم‌های کنترل صنعتی (جلسه دوم)

عناوین و ارائه‌دهندگان کارگاه‌ها

ردیف	نام کارگاه	ارائهٔ دهنده / دهندگان	سازمان	مدت
روز دوشنبه ۱۴ مهر ۱۴۰۴				
۱	آناتومی حملات سایبری کشور: بازیگران تهدید، تاکنیک‌ها و پیامدها (جلسه اول)	وحید خدابخشی-سجاد زیادپور اصل	شرکت شاپرک	۱:۳۰ ساعت
۲	هوش مصنوعی عاملی برای امنیت سایبری، خودکارسازی مدیریت ریسک با عامل‌های هوشمند (جلسه اول)	الناز عبادی	شرکت تپسی	۱:۳۰ ساعت
۳	سیستم‌های ارتباطات امن کوانتومی: مبانی، کاربردها و مسیرهای پیش-رو(جلسه اول)	دنیا سادات رضائی شاد-حسین بهرامگیری-مهدی خواجه	دانشگاه صنعتی اصفهان و دانشگاه صنعتی مالک اشتر	۱:۳۰ ساعت

۴	آناتومی حملات سایبری کشور: بازیگران تهدید، تاکنیک‌ها و پیامدها (جلسه دوم)	وحید خدابخشی-سجاد زیادپور اصل	شرکت شاپرک	۱:۳۰ ساعت
۵	هوش مصنوعی عاملی برای امنیت سایبری، خودکارسازی مدیریت ریسک با عامل‌های هوشمند (جلسه دوم)	الناز عبادی	شرکت تپسی	۱:۳۰ ساعت
۶	سیستم‌های ارتباطات امن کوانتومی: مبانی، کاربردها و مسیرهای پیش‌رو (جلسه دوم)	دنیا سادات رضائی شاد-حسین بهرامگیری-مهدی خواجه	دانشگاه صنعتی اصفهان و دانشگاه صنعتی مالک اشتر	۱:۳۰ ساعت
۷	آموخته‌های حمایت سایبری: از تهدیدشناسی تا دفاع پیشگیرانه (جلسه اول)	سجاد نفیسی	شرکت امن پرداز	۱:۳۰ ساعت
۸	تحلیل عمیق، تصمیم دقیق، واکنش سریع؛ مرزهای تازه امنیت سایبری با هوش مصنوعی (جلسه اول)	سولماز سلیمی	موسسه یورکام فرانسه	۱:۳۰ ساعت
۹	مقدمه‌ای کاربردی بر واترمارکینگ دیجیتال و استگانوگرافی با استفاده از MATLAB	زهرا قرائیان	دانشگاه صنعتی امیرکبیر	۱:۳۰ ساعت
۱۰	آموخته‌های حملات سایبری: از تهدیدشناسی تا دفاع پیشگیرانه (جلسه دوم)	سجاد نفیسی	شرکت امن پرداز	۱:۳۰ ساعت
۱۱	تحلیل عمیق، تصمیم دقیق، واکنش سریع؛ مرزهای تازه امنیت سایبری با هوش مصنوعی (جلسه دوم)	سولماز سلیمی	موسسه یورکام فرانسه	۱:۳۰ ساعت
۱۲	استنادپذیری ادله دیجیتالی موجود در تصاویر	حسین سهلانی	پلیس فتا	۱:۳۰ ساعت
روز سه شنبه ۱۵ مهر۱۴۰۴				

۱	رفتار شناسی گروه های APT فعال در زیرساخت‌های حیاتی کشور	علی امینی-امین قربانی	شرکت گراف	۱:۳۰ ساعت
۲	مرور بر حملات القای خطا	حامد رمضانی‌پور-علی نوری	پژوهشگاه توسعهٔ فناوری‌های پیشرفته	۱:۳۰ ساعت
۳	فریب سایبری	سیدعلی صموتی	شرکت مدیریت امن الکترونیکی کاشف	۱:۳۰ ساعت
۴	امنیت برنامک‌های موبایل: تهدیدات نوین و ابزارهای تحلیل و تست نفوذ	محمدعلی زمانی-محمد حسین هاتفی-محمدحسام تدین	پژوهشگاه فناوری اطلاعات و ارتباطات	۱:۳۰ ساعت
۵	مرور حملات بازخوانی کد در میکروکنترلرها ارائهٔ دو مورد عملی	فاطمه رحیمی	پژوهشگاه توسعهٔ فناوری‌های پیشرفته	۱:۳۰ ساعت
۶	فارنزیک فناوری عملیاتی(OT)			۱:۳۰ ساعت
۷	امنیت زنجیره تامین نرم افزار	سید حسین نیکونیا	شرکت مهسان	۱:۳۰ ساعت
۸	بایوس، امنیت و شخصی سازی آن	فاطمه باجلان، رضا آدینه‌پور	پژوهشگاه توسعهٔ فناوری‌های پیشرفته	۱:۳۰ ساعت
۹	شناسایی و شکار مهاجمان سایبری در سیستم‌های کنترل صنعتی (جلسه اول)	علی میرزایی، مهدی صیاد	شرکت رایان پرداز کاوش	۱:۳۰ ساعت

۱۰	افزایش صحت و امنیت کد با استفاده از مدل‌های زبانی بزرگ: یک کارگاه عملی	رضا ابراهیمی آتانی، سید امیرحسین طباطبایی، کیاوش دادپور، عسل محمودی نژاد	مرکز آپا دانشگاه گیلان	۱:۳۰ ساعت
۱۱	احراز هویت با کارت هوشمند در سامانه‌های کنترل دسترسی: تحلیل آسیب‌ها و راهکارهای امن مبتنی بر استانداردهای جهانی	اکرم خالصی، زینب سعیدی	پژوهشگاه توسعهٔ فناوری‌های پیشرفته	۱:۳۰ ساعت
۱۲	شناسایی و شکار مهاجمان سایبری در سیستم‌های کنترل صنعتی (جلسه دوم)	علی میرزایی، مهدی صیاد	شرکت رایان پرداز کاوش	۱:۳۰ ساعت

اطلاعات کارگاه‌ها

آناتومی حملات سایبری کشور: بازیگران تهدید، تاکنیک‌ها و پیامدها(جلسه اول و دوم)

وحید خدابخشی-سجاد زیادپور اصل

شرکت شاپرک

چکیده

در عصر دیجیتال، حملات سایبری به یکی از مهم‌ترین تهدیدات علیه امنیت ملی کشورها تبدیل شده‌اند. این ارائه به بررسی ساختار، ماهیت و ابعاد حملات سایبری صورت‌گرفته علیه کشور می‌پردازد و تلاش می‌کند با شناسایی بازیگران تهدید (اعم از دولتی، غیردولتی و هکتیویستی)، روش‌های عملیاتی آن‌ها و پیامدهای ناشی از این اقدامات، درکی جامع از چشم‌انداز تهدیدات سایبری ارائه دهد.تحلیل انجام‌شده، تاکتیک‌هایی نظیر نفوذ به زیرساخت‌های حیاتی، عملیات فیشینگ پیشرفته، حملات زنجیره تأمین، جاسوسی سایبری، و مهندسی اجتماعی را به‌عنوان ابزارهای کلیدی این حملات معرفی می‌کند. همچنین پیامدهایی چون نشت اطلاعات طبقه‌بندی‌شده، اختلال در خدمات حیاتی، تخریب اعتماد عمومی، و تهدید حاکمیت سایبری بررسی شده‌اند. این بررسی در نهایت بر ضرورت ارتقاء توان دفاع سایبری، به‌کارگیری رویکردهای پیش‌دستانه، و هماهنگی میان‌بخشی برای مقابله مؤثر با این نوع تهدیدات تأکید دارد.

دستاوردهای علمی و عملی شرکت کنندگان

شرکت‌کنندگان با مفاهیم کلیدی جنگ سایبری، تهدیدات پیشرفته و تاکتیک‌های نفوذ آشنا شده و توانستند از طریق تحلیل موارد واقعی، دانش نظری خود را به مهارت‌های عملی در شناسایی و مقابله با حملات سایبری تبدیل کنند.

پیش نیازها و ملزومات شرکت کنندگان

شرکت‌کنندگان در این کارگاه آموزشی، با مفاهیم علمی و تکنیک‌های عملی مرتبط با موضوع آشنا شده و توانسته‌اند دانش نظری خود را با تمرین‌ها و سناریوهای واقعی تلفیق نمایند. این تجربه آموزشی موجب ارتقاء مهارت‌های فنی، تحلیلی و تصمیم‌گیری ایشان در حوزهٔ مورد نظر گردیده است.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مقدمه و تعریف مفاهیم (جنگ سایبری، تفاوت با جنگ اطلاعاتی، اهمیت تهدیدات)	۱۵ دقیقه
۲	بازیگران تهدید (Threat Actors) (معرفی دولت‌ها، گروه‌های سایبری، تهدیدات داخلی و زنجیره تأمین)	۲۵ دقیقه
۳	تاکتیک‌ها و تکنیک‌ها (TTPs) (تکنیک‌های حمله: phishing، zero-click، مهندسی اجتماعی)	۳۰ دقیقه
۴	اهداف حملات سایبری (زیرساخت‌های حیاتی، بانک‌ها، پلتفرم‌های دیجیتال، نهادهای حاکمیتی)	۴۰ دقیقه
۵	مطالعه موردی (Case Studies) (تحلیل عملیات‌های مهم (Stuxnet، Pegasus، افشای اطلاعات)	۳۰ دقیقه
۶	پیامدها و آسیب‌ها (نشت اطلاعات، تخریب اعتماد عمومی، تأثیر اقتصادی-اجتماعی)	۱۵ دقیقه
۷	راهبردها و راهکارهای دفاعی (SIEM، Threat Intelligence، Zero Trust، آموزش منابع انسانی)	۲۵ دقیقه
۸	جمع‌بندی، پرسش و پاسخ (مرور مطالب، جمع‌بندی کلیدی، تعامل با شرکت‌کنندگان)	۲۵ دقیقه

هوش مصنوعی عاملی برای امنیت سایبری،خودکارسازی مدیریت ریسک با عامل‌های هوشمند(جلسه اول و دوم)

الناز عبادی
شرکت تپسی

Abstract: This workshop, "Agentic Al for Cybersecurity: Automating Risk Management with Intelligent Agents," explores how autonomous Al agents can transform cybersecurity by addressing the growing complexity of threats and limitations of traditional risk management. The first part focuses on theory-examining current challenges, global adoption trends, and the risks and ethical considerations of using Al agents in security operations. The second part provides a practical, step-by-step experience in implementing Al agents for tasks such as risk assessment, vulnerability prioritization, and incident response. Participants will leave with both strategic insights and hands-on skills to begin applying agentic Al in their own cybersecurity environments.

دستاوردهای علمی و عملی شرکت کنندگان

شرکت‌کنندگان در این کارگاه با مفهوم و کاربردهای هوش مصنوعی عاملی در امنیت سایبری آشنا می‌شوند و چالش‌ها و روندهای جهانی آن را بررسی می‌کنند. آنها چارچوب‌های علمی مانند MAESTRO و TRISM را برای مدل‌سازی تهدید و مدیریت ریسک می‌آموزند. به‌صورت عملی تجربه‌ی طراحی و پیاده‌سازی یک عامل هوشمند برای وظایف امنیتی مثل پایش لاگ و مدیریت آسیب-پذیری را کسب می‌کنند. هم‌چنین با بهترین شیوه‌های امنیتی و اعتمادسازی در استفاده از عامل‌های هوشمند آشنا می‌شوند. در پایان توانایی شروع پروژه‌های آزمایشی و کاربردی در محیط‌های سازمانی را خواهند داشت.

پیش نیازها و ملزومات شرکت کنندگان

شرکت در این کارگاه نیاز به پیش نیاز پیچیده‌ای ندارد و برای عموم علاقه مندان آزاد است. با این حال داشتن آشنایی اولیه با مفاهیم اولیه سایبری (مانند مدیریت ریسک، آسیب‌پذیری‌ها و واکنش به رخدادها) و آشنایی مقدماتی با هوش مصنوعی یا یادگیری ماشین می‌تواند به درک بهتر این مباحث کمک کند. تجربه عملی در استفاده از ابزارهای امنیتی یا برنامه‌نویسی ضروری نیست. اما برای بخش عملی کارگاه یک امتیاز محسوب می‌شود.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	Introduction & Motivation - Why cybersecurity needs agentic	۱۵دقیقه
	Foundations of Agentic Al - Concepts, definitions, and differences	۱۵دقیقه
۲	Applications & Use Cases - Risk assessment, SOC automation, incident responses lo	۱۰ دقیقه
۳	Global Trends - Industry adoption & case studies	۱۵دقیقه
	Challenges & Risks - Adversarial use, authentication, governance	۲۰ دقیقه
	Frameworks - MAESTRO, TRISM, NIST AI RMF	۱۰ دقیقه
	Hands-On Practice - Designing and implementing a simple Al agent	۳۰ دقیقه

۳۰ دقیقه	Threat Modeling Exercise - Applying MAESTRO	
۱۵دقیقه	Building Trustworthy Agents - Guardrails, monitoring, human-in-the-loop	۴
۱۰ دقیقه	Wrap-Up & Discussion- Key takeaways & Q&A	

سیستم‌های ارتباطات امن کوانتومی: مبانی، کاربردها و مسیرهای پیش‌رو(جلسه اول و دوم)

دنیا سادات رضائی شاد[۱]-حسین بهرامگیری[۲]-مهدی خواجه[۲]

[۱]دانشگاه صنعتی اصفهان، [۲]دانشگاه صنعتی مالک اشتر

چکیده:

با رشد سریع فناوری‌های کوانتومی، طراحی و پیاده‌سازی سیستم‌های مخابراتی امن بر پایه اصول مکانیک کوانتومی به یکی از حوزه‌های راهبردی در علم و صنعت تبدیل شده است. این کارگاه با هدف ارائهٔ مروری جامع بر مبانی علمی و کاربردی ارتباطات کوانتومی، تلاش دارد مخاطبان را با مفاهیم پایه، ابزارهای نظری و فناوری‌های روز در این حوزه آشنا سازد. در بخش اول کارگاه، مفاهیم کلیدی مکانیک کوانتومی نظیر برهم‌نهی، درهم‌تنیدگی و نمایش برداری حالت‌ها مرور می‌شود. سپس ساختار سیستم‌های مخابرات کوانتومی، اجزای اصلی آن‌ها، مفاهیم اندازه‌گیری و تئوری اطلاعات کوانتومی معرفی می‌گردند. در ادامه، کاربردهای درهم‌تنیدگی در ارتباطات نظیر فرابرد کوانتومی و توزیع کلید کوانتومی مطرح می‌شوند. بخش دوم کارگاه بر رمزنگاری بر استفاده از توزیع کلید کوانتومی تمرکز دارد. سپس ساختار و چالش‌های طراحی شبکه‌های کوانتومی در مقیاس‌های مختلف بررسی می‌شود. در پایان نیز مفاهیم نوظهوری چون اینترنت کوانتومی، اینترنت اشیای کوانتومی و حسگری کوانتومی بیان خواهد شد. این کارگاه علاوه بر جنبه‌های علمی، مسیرهای پژوهشی و مراکز فعال در این حوزه در کشور را نیز معرفی می‌کند و فرصتی برای علاقه‌مندان جهت ورود و فعالیت در مرزهای دانش فناوری‌های کوانتومی فراهم می‌آورد.

دستاوردهای علمی و عملی شرکت کنندگان

علمی:

- مرور مفاهیم مکانیک کوانتومی
- آشنایی با مخابرات کوانتومی و کاربرد آن در حوزه‌های مختلف
- آشنایی با سیستم‌های ارتباطات امن کوانتومی، شبکه‌سازی آن‌ها، نیازمندی‌ها

کاربردی:

- بیان حوزه‌های پژوهشی در زمینه‌ی مخابرات کوانتومی، ارتباطات امن کوانتومی
- آشنایی با مفاهیم اصلی در این زمینه برای شروع مطالعه و پژوهش

- معرفی مراکز کوانتومی کشور و ایجاد ارتباط جهت فعالیت‌های بیشتر

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی با مفاهیم پایه مکانیک کوانتومی ضروری نیست، اما مفید است.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مقدمه	۱۵دقیقه
۲	مفاهیم مکانیک کوانتومی	۳۰ دقیقه
۳	کاربردهای درهم تنیدگی در ارتباطات	۲۰ دقیقه
۴	توزیع کلید کوانتومی	۶۰ دقیقه
۵	شبکه و اینترنت کوانتومی	۳۰ دقیقه
۶	سیستم‌های مخابرات کوانتومی	۱۵ دقیقه
۷	پرسش و پاسخ	۱۰ دقیقه

آموخته‌های حمایت سایبری: از تهدیدشناسی تا دفاع پیشگیرانه(جلسه اول و دوم)

سجاد نفیسی

شرکت امن پرداز

چکیده

در دنیای امروز که تهدیدات سایبری به سرعت در حال تحول هستند، درک «تاکتیک، تکنیک و روال‌های (TTPs)» مهاجمان و مرور «آموخته‌های دفاعی» از حملات گذشته برای ساخت سیستم‌های مقاوم، حیاتی است. این کارگاه نظری – عملی، به بررسی حوادث واقعی سایبری شاخص در سالیان گذشته (با حفظ محرمانگی) پرداخته و بینش‌های کاربردی را برای افزایش توانایی تشخیص تهدیدات، کاهش خطرات و استراتژی‌های امنیتی پیشگیرانه ارائه می‌دهد.

دستاوردهای علمی و عملی شرکت کنندگان

- کسب «بینش‌های مبتنی بر داده» از حملات سایبری گذشته
- توسعهٔ مهارت در «تشخیص الگوهای حمله» و «دفاع پیشگیرانه»
- تمرین «تحلیل تهدیدات در زمان واقعی» در یک محیط آزمایشگاهی کنترل‌شده

پیش نیازها و ملزومات شرکت کنندگان

- دانش اولیه شبکه‌های کامپیوتری
- آشنایی با مفاهیم پایه امنیت سایبری

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	تحلیل تهدیدات	۳۰ دقیقه
۲	نمونه مطالعه موردی	۶۰ دقیقه
۳	شبیه‌سازی زنده حمله	۹۰ دقیقه

تحلیل عمیق، تصمیم دقیق، واکنش سریع؛ مرزهای تازه امنیت سایبری با هوش مصنوعی (جلسه اول و دوم)

سولماز سلیمی

موسسه یورکام فرانسه

چکیده

این کارگاه به بررسی تغییرات بنیادینی می‌پردازد که پژوهش‌های مبتنی بر هوش مصنوعی در حوزه‌های مختلف امنیت سایبری ایجاد کرده‌اند. به جای تمرکز بر هیاهوی رسانه‌ای، حوزه‌هایی مرور می‌شوند که در آن‌ها هوش مصنوعی پیشرفت‌های واقعی به همراه داشته، محدودیت‌ها مشخص می‌شوند و فرصت‌های تازه پژوهشی بررسی خواهند شد. هوش مصنوعی امنیت سایبری را از قواعد سنتی به سمت روش‌های معنایی، سازگار و مولد برده است. این کارگاه هم دستاوردها و هم چالش‌های باقی‌مانده برای به‌کارگیری مسئولانه آن را مرور می‌کند.

از طریق جلسات تعاملی و تمرین‌های عملی، شرکت کنندگان یاد می‌گیرند که:

- تهدیدات انتزاعی سایبری را به معیارهای مالی ملموس ترجمه کنند.
- از مدل‌های احتمالی برای ارزیابی و اولویت‌بندی ریسک‌ها استفاده کنند.
- از تکنیک‌های اندازه‌گیری پیشرفته برای عوامل امنیتی به ظاهر غیرقابل اندازه‌گیری استفاده کنند.
- استراتژی‌های داده محور برای تخصیص منابع و کاهش ریسک را توسعه دهند.

این کارگاه شکاف بین امنیت سایبری و تصمیم‌گیری برای مدیران ارشد و میانی امنیت را پر می‌کند و شرکت‌کنندگان را با ابزارهایی برای برقراری ارتباط موثر ریسک با ذینفعان و هدایت سرمایه‌گذاری‌های امنیتی آگاهانه مجهز می‌کند. شرکت‌کنندگان چه یک CISO، مدیر ریسک، یا متخصص امنیت باشند، بینش‌های ارزشمندی برای ارتقای شیوه‌های ارزیابی ریسک سازمان خود و همسو کردن تلاش‌های امنیتی با اهداف کسب و کار به دست خواهند آورد.

دستاوردهای علمی و عملی شرکت کنندگان

- مرور حوزه‌هایی که هوش مصنوعی در آن‌ها پیشرفت داشته است.
- مشخص کردن محدودیت‌های این حوزه
- بررسی فرصت‌های تازه پژوهشی

پیش نیازها و ملزومات شرکت کنندگان

این کارگاه برای پژوهشگران، دانشجویان تحصیلات تکمیلی و کارشناسان خبره‌ی صنعت در حوزهٔ امنیت سایبری طراحی شده است. انتظار می‌رود شرکت‌کنندگان با مفاهیم پایه‌ای امنیت نرم افزار، تحلیل بدافزار و شبکه آشنا باشند. آشنایی مقدماتی با یادگیری ماشین و مدل‌های زبانی بزرگ توصیه می‌شود، اما این پیش نیاز الزامی نیست.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	انگیزه و چشم‌انداز	۴۵ دقیقه
۲	مرور عمیق موضوعات	۹۰ دقیقه
۳	تجربه‌های عملی و جمع‌بندی	۴۵دقیقه

مقدمه‌ای کاربردی بر واترمارکینگ دیجیتال و استگانوگرافی با استفاده از MATLAB

زهرا قرائیان

دانشگاه صنعتی امیرکبیر

چکیده:

این کارگاه آموزشی با هدف ارائهٔ تجربهٔ کاربردی، به مبانی نظری و پیاده‌سازی الگوریتم‌های نهان‌نگاری و واترمارکینگ در تصاویر دیجیتال می‌پردازد. شرکت‌کنندگان با مشاهده نمایش زنده پیاده‌سازی گام به گام این الگوریتم ها در محیط نرم افزار MATLAB با مفاهیم و تکنیک‌های کلیدی این حوزه آشنا خواهند شد.

دستاوردهای علمی و عملی شرکت کنندگان

در این کارگاه، شرکت‌کنندگان با مفاهیم اصلی نهان‌نگاری و واتر مارکینگ، معیارهای ارزیابی (PSNR، SSIM)، انواع واترمارکینگ و تفاوت‌ها آشنا خواهند شد. هم‌چنین اجرای عملی در MATLAB شامل خواندن تصاویر، پیاده‌سازی دو روش، مقایسه ظرفیت و مقاومت، و ارزیابی در برابر حملات انجام خواهد شد. فایل کد و اسلایدها برای تمرین فردی ارائه می‌شود.

پیش نیازها و ملزومات شرکت کنندگان

پیش نیاز علمی:

این کارگاه با رویکردی کاملاً مقدماتی طراحی شده و شرکت‌کنندگان برای بهره‌مندی از آن به هیچ‌گونه دانش قبلی در زمینه نهان‌نگاری، واتر مارکینگ یا پردازش تصویر نیاز ندارند.

ملزومات عملی:

به‌دلیل محدودیت زمانی، انجام فعالیت‌های عملی توسط شرکت‌کنندگان امکان پذیر نخواهد بود. لذا داشتن لپ تاپ الزامی نیست.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مقدمه	۱۵دقیقه
۲	تعاریف و اصطلاحات کلیدی	۲۰ دقیقه
۳	حوزه‌های درج واترمارک	۱۵ دقیقه
۴	معیارهای ارزیابی	۲۰ دقیقه
۵	تفاوت در حملات	۱۰ دقیقه
۶	جمع بندی و بحث سوالات	۱۰دقیقه

استنادپذیری ادله دیجیتالی موجود در تصاویر

حسین سهلانی

پلیس فتا

چکیده:

در این کارگاه تخصصی به بررسی جامع استنادپذیری ادله دیجیتالی استخراج شده از تصاویر پرداخته می‌شود. به طور خاص، تلاش خواهیم کرد تا با مرور روش‌های علمی، استخراج تحلیل و اعتبارسنجی، ادله شرکت‌کنندگان را با چالش‌ها و راهکارهای پیشرو آشنا کنیم. طی،کارگاه مباحثی نظیر شناسایی تغییرات دست‌کاری شده درتصاویر، فرمت‌ها و متادیتای مرتبط با استانداردهای حقوقی و فنی برای پذیرش این ادله در دادگاه‌ها مطرح خواهد شد. تمرکز اصلی روی کاربردی بودن کارگاه و پژوهش مربوطه بوده و شامل روش‌های الگوریتمی ابزارهای نرم افزاری مانند تکنیک‌های تشخیص تقلب در تصویر، تحلیل لایه‌های مختلف تصویر و اعتبارسنجی زنجیره تأمین داده‌های تصویری است. کارگاه نمونه‌هایی عملی و مطالعات موردی واقعی ارائه می‌دهد که می‌تواند در پژوهش‌های علمی و فعالیت‌های قضایی مورد استفاده قرار گیرد.

دستاوردهای علمی و عملی شرکت کنندگان

- درک عمیق از مفاهیم و چالش‌های استنادپذیری ادله تصویری
- توانایی کاربرد الگوریتم‌ها و ابزارهای معتبر برای تحلیل تصاویر از نظر اصالت و دست‌کاری
- قابلیت تفسیر نتایج تحلیل در بین رشته‌های علمی و حقوقی
- مهارت طراحی فرایند زنجیره تأمین امن برای مدارک تصویری در پروژه‌های پژوهشی یا قضایی
- آشنایی با گزارش‌دهی علمی و حقوقی ادله دیجیتال برای کاربرد در کنفرانس‌ها و دادگاه‌ها

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی پایه با مباحث علوم کامپیوتر به ویژه پردازش تصویر
- آشنایی مقدماتی با مفاهیم حقوقی یا قضایی مربوط به مدارک دیجیتال
- دانشی پایه‌ای از فرمت‌ها و ساختارهای تصاویر دیجیتال
- درک مقدماتی از مفاهیم امنیت اطلاعات و رمزنگاری
- آشنایی پایه با مباحث حوزهٔ فارنزیک

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مقدمه اهمیت و چالش‌های استنادپذیری ادله دیجیتال تصویری	-دقیقه
۲	مبانی علمی استخراج و تحلیل داده‌های تصویری	-دقیقه
۳	روش‌ها و ابزارهای تشخیص دست‌کاری و جعل تصویر	-دقیقه
۴	بررسی استانداردها و مراجع حقوقی پذیرش ادله تصویری	-دقیقه
۵	تحلیل متادیتا و زنجیره تأمین داده‌ها	- دقیقه
۶	مطالعات موردی علمی و قضایی، نمونه‌های کاربردی	- دقیقه
۷	کارگاه عملی؛ تحلیل نمونه تصاویر و گزارش‌نویسی ادله	- ساعت
۸	جمع‌بندی و بحث سوالات	-دقیقه

رفتار شناسی گروه‌های APT فعال در زیرساخت‌های حیاتی کشور

علی امینی-امین قربانی

شرکت گراف

چکیده

با توجه به افزایش حجم حملات سایبری در سال‌های اخیر و آسیب دیدن زیرساخت‌های حیاتی کشور و به سرقت رفتن اطلاعات مهم و حساس کشور لازم است که متخصصین و مدیران سازمان‌ها و شرکت‌ها آگاهی‌های لازم در خصوص گروه‌های APT فعال علیه زیرساخت‌های کشور را کسب کنند. از این رو بر آن شدیم تا کارگاهی برگزار کنیم که در این کارگاه تلاش بر این است که متخصصین هوش تهدید شرکت گراف با به‌کارگیری تجربیات خود که بر پایه عملیات‌های متعدد شکار تهدید که در سال‌های اخیر در زیرساخت ها و سازمان‌های کشور بوده است به بررسی رفتار و اهداف گروه‌های APT فعال علیه زیر ساخت‌های کشور بپردازند و این تجربیات را در اختیار شرکت‌کنندگان قرار دهند. متخصصین شرکت گراف با انجام تحلیل‌های دقیق و عمیق بر روی نمونه‌های بدافزارهای استفاده شده در حملات توسط گروه های APT و تقویت پایگاه هوش تهدید خود بر پایه اطلاعات به‌دست آمده و همچنین استفاده از OSINT و رهگیری گروه‌های APT و تجمیع آنها اقدام به ایجاد ساز و کاری در محصولات خود کرده است که بتوان با مشاهده سرنخ‌های مرتبط با گروه های APT، به راحتی نسبت به شناسایی و جلوگیری از حمله اقدام کنند. در این کارگاه، نتایج و دستاوردهای حاصل از مجموعه تحلیل‌های تخصصی در حوزهٔ تهدیدات سایبری ارائه خواهد شد. این تحلیل‌ها با تمرکز بر فعالیت‌ها و تکنیک‌های مورد استفاده توسط گروه‌های APT انجام شده و منجر به شناسایی الگوهای رفتاری اهداف راهبردی و روش‌های عملیاتی این گروه‌های فعال علیه کشور گردیده است. ارائهٔ این یافته‌ها به شرکت‌کنندگان امکان آشنایی عمیق‌تر با ماهیت تهدیدات پیشرفته و درک بهتر از شیوه‌های مقابله و دفاع در برابر آنها را فراهم خواهد کرد. در پایان انتظار می‌رود شرکت‌کنندگان با درک روشن‌تری از رفتار و اهداف گروه های APT بتوانند این دانش را در مسیر تقویت سامانه‌ها و راهبردهای دفاعی کشور به کار گیرند.

دستاوردهای علمی و عملی شرکت کنندگان

- شرکت‌کنندگان پس از گذراندن این کارگاه، نسبت به گروه‌های هکری فعال و نحوه فعالیت آن‌ها در زیرساخت‌های کشور آگاه شده و می‌توانند دانش و راهکارهای جلوگیری از آنها را کسب کنند.

پیش نیازها و ملزومات شرکت کنندگان

- شرکت برای عموم آزاد است و نیاز به پیش نیاز خاصی ندارد.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مروری بر جرایم سایبری و حملات هدفمند در سال‌های اخیر	
۲	معرفی سه مورد از فعال‌ترین بازیگران تهدید پیشرفته (APT) در ایران	

۳	بررسی اهداف و انگیزه بازیگران تهدید از حملات	
۴	بررسی روشهای اخذ دسترسی اولیه (initial access)	
۵	نقش فراهم آورندگان دسترسی اولیه (IAB) در حملات اخیر	
۶	رفتارشناسی بازیگران تهدید	
۷	روش شکار و کشف شاخص‌های حمله	
۸	اهمیت شاخص‌های حمله در هوش تهدید (CTI)	
۹	ارائه پیشنهاد و معرفی روش‌های پیشگیرانه برای مقابله با تهدیدات	

مرور بر حملات القای خطا

حامد رمضانی پور-علی نوری
پژوهشگاه توسعهٔ فناوری‌های پیشرفته

چکیده

در حملات القای خطا در دو دهه اخیر توجه بسیاری را در زمینه ارزیابی امنیتی پیاده¬سازی سخت¬افزاری الگوریتم-های رمزنگاری به خود جلب کرده است. این رویکرد با القای مقادیر تصادفی یا از پیش تعیین شده براساس دسترسی مهاجم، باعث ایجاد خطا و انحراف کمّی در مقادیر میانی الگوریتم¬های رمزنگاری تعبیه شده در تکنولوژی¬های ارتباطی می¬شوند. در نتیجه این خطا¬های موثر یا انحرافات قابل بهره¬برداری توسط تحلیل¬گران ارزیابی شده و با تکیه بر محاسبات آماری موجب کاهش پیچیدگی محاسباتی کلید اصلی رمزنگاری یا در برخی موارد بازیابی کامل آن در فاز تحلیل خواهند شد. از پرکاربرد¬ترین ابزارها در زمینه القای خطا می¬توان به اشعه لیزر، پالس الکترومغناطیس، گلیچ ولتاژ و فرکانس اشاره کرد. در این کارگاه سعی داریم با توصیف اولیه نحوه بهره-برداری از این ادوات همچنین تاثیر آن¬ها در بازیابی مقادیر مخفی الگوریتم¬های آسیب¬پذیر در سریع‌ترین زمان ممکن، با ذکر چند مثال عملی، آشنایی کلی با موضوع مربوطه ایجاد کنیم.

دستاوردهای علمی و عملی شرکت کنندگان

- دانش پیاده‌سازی حملات القای خطا در بستر نرم افزار و سخت افزار

پیش نیازها و ملزومات شرکت کنندگان

- دانش اولیه رمزنگاری

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مقدمات دانش القا خطا	۳۰ دقیقه
۲	تاثیر القای خطا در بازیابی مقادیر حساس الگوریتم¬های رمزنگاری و کاهش پیچیدگی محاسباتی	۱۵ دقیقه
۳	انواع روش‌های پرکاربرد در القای خطا	۱۵ دقیقه
۴	ترکیب القای خطا با دیگر حملات کانال جانبی	۱۵ دقیقه
۵	میزان موفقیت به‌کارگیری روش¬های القای خطا در بازیابی مقادیر حساس	۱۵ دقیقه
۶	کاربرد القای خطا در مقابل سطوح امنیتی سخت افزاری تجهیزات صنعتی و آزمایشگاهی	۱۵ دقیقه

فریب سایبری

سیدعلی صموتی
شرکت مدیریت امن الکترونیکی کاشف

چکیده

این کارگاه به بررسی جامع مفاهیم فریب سایبری به عنوان یک استراتژی پیشرفته در دفاع از زیرساخت‌های دیجیتال اختصاص دارد. در این رویداد، شرکت‌کنندگان با تکنیک‌های طراحی و پیاده‌سازی محیط‌های فریبنده آشنا خواهند شد که می‌تواند به طور مؤثری مهاجمان را از دستیابی به اهداف خود بازدارد. همچنین، ساختارهای مختلف فریب و تأثیر آن‌ها بر هزینه‌های عملیاتی مهاجمان و قابلیت‌های شناسایی و خنثی‌سازی حملات تحلیل خواهد شد. به علاوه، پلتفرم‌های پیشرو در شبیه‌سازی خدمات آسیب‌پذیر و ثبت فعالیت‌های مخرب مورد بررسی قرار می‌گیرند. هدف این کارگاه، ارتقاء توانمندی‌های شرکت‌کنندگان در استفاده از فریب سایبری به عنوان ابزاری کلیدی در امنیت سایبری است. این رویداد فرصتی را برای تبادل‌نظر و همکاری میان متخصصان و پژوهشگران در این حوزه فراهم می‌آورد.

دستاوردهای علمی و عملی شرکت کنندگان

- آشنایی با فریب سایبری

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی با مفاهیم اولیه دفاع سایبری و امنیت سایبری

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مفاهیم فریب سایبری	
۲	تکسونامی فریب سایبری	
۳	طبقه‌بندی	
۴	ابزارها و روش‌ها	
۵	معرفی پلتفرم‌ها	
۶	ارائهٔ سه روش	

امنیت برنامک‌های موبایل: تهدیدات نوین و ابزارهای تحلیل و تست نفوذ

محمدعلی زمانی-محمد حسین هاتفی-محمدحسام تدین

پژوهشگاه فناوری اطلاعات و ارتباطات

چکیده

در دهه‌ی اخیر، با گسترش فراگیر تلفن‌های هوشمند و افزایش وابستگی کاربران به برنامک‌های موبایل در حوزه‌های حساس مانند بانکداری دیجیتال، خدمات درمانی، آموزش آنلاین، و دولت الکترونیک، سطح حملات سایبری نیز به‌صورت کمّی و کیفی دچار تحول شده است. برنامک‌های موبایل به‌دلیل ویژگی‌های خاص خود از جمله تعامل مستقیم با کاربر، دسترسی به منابع حساس دستگاه، و ارتباطات دائمی با سرورهای خارجی، به یکی از اصلی‌ترین اهداف مهاجمان در فضای سایبری تبدیل شده‌اند. در این میان، ضعف در طراحی امنیتی، استفاده ناصحیح از کتابخانه‌های رمزنگاری، آسیب‌پذیری‌های لایه‌ی ذخیره‌سازی و شبکه، و نبود تست امنیتی پیش از انتشار، باعث ایجاد خطرات جدی برای کاربران و سازمان‌ها می‌شود.

کارگاه تخصصی حاضر با عنوان «امنیت برنامک‌های موبایل: تهدیدات نوین و ابزارهای تحلیل و تست نفوذ»، با هدف ارتقاء دانش و مهارت شرکت‌کنندگان در زمینه‌ی تحلیل امنیتی و تست برنامه‌های موبایل برگزار می‌گردد. این کارگاه به‌صورت یک جلسه به مدت یک ساعت و نیم، طراحی شده که در قالب دو زیرکارگاه تخصصی برگزار خواهد شد.

مخاطبان این کارگاه شامل پژوهشگران حوزهٔ امنیت، کارشناسان تست نفوذ، توسعهٔدهندگان برنامک‌های موبایل، و دانشجویان علاقه‌مند به امنیت موبایل هستند. شرکت در این کارگاه می‌تواند درک عمیقی از ساختار و آسیب‌پذیری‌های برنامک‌ها و نیز توانایی اجرای تست‌های امنیتی هدفمند در محیط واقعی به شرکت‌کنندگان ارائه دهد. استفاده‌ی ترکیبی از تئوری، دموهای عملی، و سناریوهای واقعی باعث خواهد شد که شرکت‌کنندگان تجربه‌ای کامل و کاربردی در حوزهٔ امنیت برنامک‌های موبایل کسب نمایند.

دستاوردهای علمی و عملی شرکت کنندگان

- درک عمیق از آسیب پذیری های اپلیکیشن‌های موبایلی
- آشنایی با مهم‌ترین و نوین‌ترین حملات اپلیکیشن‌های موبایلی
- درک عمیق از OWASP MASTG و OWASP MASVS
- توانایی تحلیل آسیب‌پذیری‌های اپلیکیشن‌های موبایلی
- درک عمیق از فرایند مهندسی معکوس اندروید و نقش فایل‌های Smali
- آشنایی با تکنیک‌های پیشرفته تزریق کد از طریق دست‌کاری Smali
- درک اصول Code Obfuscation و Integrity Checking به عنوان ابزارهای دفاعی
- توانایی تحلیل اولیه فایل‌های Smali و درک منطق آن‌ها
- توانایی پیاده‌سازی کدهای دفاعی برای تشخیص دست‌کاری و جلوگیری از اجرای برنامه در محیط‌های ناامن

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی با زبان‌های برنامۀنویسی Java
- دانش پایه از توسعۀ اپلیکیشن اندروید
- آشنایی مقدماتی با مفاهیم امنیت سایبری (توصیه می‌شود اما اجباری نیست.)
- این کارگاه برای توسعه‌دهندگان، مهندسان امنیت و علاقه‌مندان به مهندسی معکوس بسیار مفید خواهد بود.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مقدمه	۵ دقیقه
۲	آسیب‌پذیری‌ها و حملات اپلیکشین‌های موبایلی	۱۵ دقیقه
۳	راهکارهای دفاعی و چارچوب OWASP	۲۰ دقیقه
۴	جمع‌بندی و پرسش و پاسخ	۵ دقیقه
بخش دوم		
۱	مقدمه	۵ دقیقه
۲	فرایند حمله	۱۵ دقیقه
۳	راهکارهای دفاعی و پیشگیری	۲۰ دقیقه
۴	جمع‌بندی و پرسش و پاسخ	۵ دقیقه

مرور حملات بازخوانی کد در میکروکنترلرها ارائۀ دو مورد عملی

فاطمه رحیمی
پژوهشگاه توسعۀ فناوری های پیشرفته

چکیده

در این کارگاه تخصصی، حملات فیزیکی از نوع تزریق خطا (Fault Injection) با تمرکز بر گلیچ ولتاژ بررسی می‌شوند. پس از معرفی معماری امنیتی میکروکنترلرها و ابزارهای موجود در حوزۀ گلیچ مانند ChipWhisperer و PicoGlitcher، شرکت‌کنندگان با یک ابزار اختصاصی طراحی‌شده توسط تیم برگزارکننده آشنا می‌شوند که به‌صورت سخت‌افزاری و نرم‌افزاری بازطراحی شده است. این ابزار با قیمت پایین، انعطاف بالا و عملکرد دقیق می‌تواند گلیچ ولتاژ قابل تنظیم تولید کند. در ادامه، با استفاده از این ابزار، حمله عملی روی STM32 انجام شده و دسترسی به حافظه محافظت‌شده flash memory بررسی می‌شود. همچنین این کارگاه در انتها به یکی از حملات نرم افزاری به میکروکنترلرها جهت دستیابی به حافظه محافظت شده آن‌ها پرداخته و روش حمله مبتنی بر وقفه را به طور کامل توضیح می‌دهد.

دستاوردهای علمی و عملی شرکت کنندگان

- یادگیری مفاهیم پایه ی حفاظت از محتوای حافظه میکروکنترلرها و همچنین برخی روش‌های تهدید حفاظت
- یادگیری تئوری کامل گلیچ ولتاژ و Fault Injection
- شناخت ابزارهای گلیچینگ رایج و مشکلات آن‌ها
- آشنایی با طراحی یک ابزار اختصاصی برای تزریق گلیچ
- اجرای موفق حمله روی STM32
- قابلیت بازطراحی ابزار و پیاده‌سازی شخصی

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی با معماری ARM و مفاهیم حافظه.
- نکته: علاقه‌مندان عمومی نیز می‌توانند از کارگاه استفاده کنند اما شرکت‌کنندگان فنی بهره بیشتری خواهند برد.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مقدمه: امنیت در معماری حافظه میکروکنترلرها	۱۰ دقیقه
۲	آشنایی با حملات فیزیکی و نرم‌افزاری	۱۰ دقیقه
۳	معرفی ابزارهای گلیچینگ و چالش‌های آن‌ها	۱۰ دقیقه
۴	طراحی سخت‌افزار ابزار جدید و تحلیل مدارات	۱۰ دقیقه
۵	پیاده‌سازی نرم‌افزار تولید پالس گلیچ	۱۰ دقیقه
۶	اجرای عملی حمله با ابزار اختصاصی روی STM32	۱۵ دقیقه
۷	آشنایی با حمله نرم افزاری اینتراپت	۱۰ دقیقه
۸	تحلیل نتایج، بحث امنیتی و اقدامات مقابله‌ای	۱۵ دقیقه

فارنزیک فناوری عملیاتی OT

چکیده

سامانه‌های کنترل صنعتی (OT) به منظور کنترل و اتوماسیون فرایند در صنایع بزرگ نفت، گاز، پتروشیمی، نیروگاهی و صنایع تولیدی مورد استفاده قرار می‌گیرند. هرگونه مخاطره برروی این سیستم‌ها دارای تبعات انسانی، اقتصادی، اجتماعی و محیط زیستی بسیار گسترده می‌باشد. از طرف دیگر با توجه به افزایش روز افزون حملات سایبری برروی سامانه‌های کنترل صنعتی و در معرض خطر قرار گرفتن این سیستم‌ها، اهمیت حفاظت از این سیستم‌ها دو چندان شده است. با توجه به اینکه به طور معمول سیستم‌های OT ایزوله طراحی شده‌اند، بنابراین حملات بر روی سیستم‌های صنعتی به‌صورت ترکیبی و دارای پیچیدگی‌های زیادی می‌باشند. فارنزیک OT، روشی برای شناسایی نقاط نفوذ و آسیب‌پذیری‌ها می‌باشد و درک عمیقی از رفتارهای سیستم‌های OT را ایجاد می‌کند. هدف از این کارگاه آموزش مفاهیم پایه فارنزیک سیستم‌های کنترل صنعتی در سطح سخت‌افزار، شبکه و نرم افزار می‌باشد.

دستاوردهای علمی و عملی شرکت کنندگان

- مناسب عموم

پیش نیازها و ملزومات شرکت کنندگان

- این کارگاه به شرکت‌کنندگان محترم، مفاهیم پایه فارنزیک سخت افزار و پروتکل‌های صنعتی را آموزش خواهد داد.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	معرفی فارنزیک OT	
۲	آشنایی با ذخیره‌سازهای داده در تجهیزات صنعتی	
۳	نحوه ی ارتباط با سخت افزار	
۴	مقدمه‌ای بر ابزارها و روش تحلیل firmware	
۵	آشنایی با مفاهیم شبکه و انواع پروتکل‌های صنعتی تحلیل یک پروتکل صنعتی نمونه	
۶	انجام یک پروژه عملی	

امنیت زنجیره تامین نرم افزار

سید حسین نیکونیا
شرکت مهستان

چکیده

در دنیای امروز که نرم‌افزارها به ستون فقرات کسب‌وکارها و زیرساخت‌های حیاتی تبدیل شده‌اند، امنیت زنجیره تأمین نرم‌افزار از اهمیت ویژه‌ای برخوردار است. با افزایش وابستگی به اجزای متن باز، کتابخانه‌های شخص ثالث و فرایندهای پیچیدهٔ توسعه و استقرار، نقاط آسیب‌پذیری جدیدی در این زنجیره ایجاد شده است. یک نقص امنیتی در هر مرحله از این زنجیره، از کدنویسی اولیه تا استقرار نهایی، می‌تواند منجر به حملات سایبری، نشت اطلاعات، و خسارات مالی و اعتباری جبران‌ناپذیری شود.
این کارگاه ۱,۵ ساعته با هدف افزایش آگاهی و توانمندسازی شرکت‌کنندگان در زمینه شناسایی، پیشگیری و مقابله با تهدیدات امنیتی در زنجیره تأمین نرم‌افزار طراحی شده است. ما به بررسی مفاهیم کلیدی، انواع حملات رایج، و ارائهٔ راه‌کارهای عملی و ابزارهای مؤثر برای ایجاد یک زنجیره تأمین نرم‌افزاری امن خواهیم پرداخت. این کارگاه برای توسعه‌دهندگان، مدیران امنیت، معماران نرم‌افزار، و هر کسی که در چرخه عمر توسعهٔ نرم‌افزار نقش دارد، مفید خواهد بود.

دستاوردهای علمی و عملی شرکت کنندگان

این کارگاه یک و نیم ساعته با هدف افزایش آگاهی و توانمندسازی شرکت‌کنندگان در زمینه شناسایی، پیشگیری و مقابله با تهدیدات امنیتی در زنجیره تأمین نرم‌افزار طراحی شده است. ما به بررسی مفاهیم کلیدی، انواع حملات رایج، و ارائهٔ راه‌کارهای عملی و

ابزارهای مؤثر برای ایجاد یک زنجیره تأمین نرم‌افزاری امن خواهیم پرداخت. این کارگاه برای توسعۀدهندگان، مدیران امنیت، معماران نرم‌افزار، و هر کسی که در چرخه عمر توسعۀ نرم‌افزار نقش دارد، مفید خواهد بود.

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی با فرایند توسعۀ نرم افزار

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مقدمه ای بر امنیت زنجیره تامین نرم افزار	
۲	تهدیدات و بردارهای حمله رایج	
۳	راهکارهای عملی و ابزارهای دفاعی	

بایوس، امنیت و شخصی سازی آن

فاطمه باجلان، رضا آدینه‌پور

پژوهشگاه توسعۀ فناوری‌های پیشرفته

چکیده

بایوس (BIOS) به عنوان نخستین نرم افزاری که پس از روشن شدن رایانه اجرا می‌شود، نقش حیاتی در شناسایی و پیکربندی سخت افزار و آغاز فرایند راه اندازی (Boot) ایفا می‌کند. این مؤلفه، نقطه شروع زنجیره اعتماد در معماری سیستم بوده و هرگونه ضعف امنیتی در آن می‌تواند منجر به نفوذهای ماندگار و غیرقابل تشخیص شود. در سال‌های اخیر حملات پیشرفته‌ای مانند LoJax MoonBounce و BlackLotus نشان داده‌اند که BIOS می‌تواند هدف حملاتی قرار گیرد که حتی پس از نصب مجدد سیستم عامل نیز فعال باقی بمانند. با توجه به اهمیت امنیت و کنترل کامل بر فرایند بوت، استفاده از راه‌کارهای متن باز مانند coreboot امکان شفافیت کد و شخصی‌سازی BIOS را متناسب با نیازهای سخت افزاری و سیاست‌های امنیتی فراهم می‌کند. در این راستا، کارگاه حاضر با هدف آموزش مفاهیم پایه، معرفی ابزارهای تخصصی و ارائه مراحل عملی ساخت و برنامه‌ریزی BIOS شخصی‌سازی شده طراحی شده است. انتظار می‌رود شرکت‌کنندگان پس از اتمام این کارگاه، توانایی تحلیل ساختار BIOS، شناسایی تهدیدات امنیتی و مهارت توسعۀ نسخه‌های امن و بهینه متناسب با کاربردهای خاص را کسب کنند. این مهارت‌ها علاوه بر ارتقاء توان دفاع سایبری گامی مهم در مسیر خودکفایی فناوری و کاهش وابستگی به محصولات خارجی خواهد بود.

دستاوردهای علمی و عملی شرکت کنندگان

- معرفی ساختار و کارکردهای اصلی BIOS از اولین نسخه تا زمان حاضر
- شناخت و درک تهدیدات امنیتی در سطح BIOS و اهمیت آن در زنجیره اعتماد

- آشنایی با مفهوم SecureBoot و روش‌های مقابله با حملات در سطح میان افزار
- شناخت روش‌های‌امن سازیBIOS و راه‌کارهای مناسب برای کاهش خطرات امنیتی در سیستم‌های‌مبتنی برBIOS
- توانایی پیکربندی و تا حدودی شخصی‌سازیBIOS با استفاده از ابزار متن بازCoreboot
- توانایی استفاده از ابزارهای برنامه‌ریزیو تحلیل ساختار BIOS مانند flashrom و cbfstool

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی با مفاهیم پایه‌ای سیستم‌های کامپیوتری و ساختار سخت افزار رایانه‌ای
- درک اولیه از سیستم عامل و فرایندهای راه اندازی سیستم
- آشنایی با مفاهیم امنیت سایبری و تهدیدات رایج بدافزارها

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مفاهیم پایه و اهمیت بایوس	۴۰ دقیقه
۲	ابزارها و محیط توسعه	۱۵ دقیقه
۳	شخصی‌سازی	۳۵ دقیقه

شناسایی و شکار مهاجمان سایبری در سیستم‌های کنترل صنعتی (جلسه اول و دوم)

علی میرزایی، مهدی صیاد
شرکت رایان پرداز کاوش

چکیده

Detection and Hunting of Cyber Intruders in Industrial Control Systems.

دستاوردهای علمی و عملی شرکت کنندگان

- توانایی تحلیل نفوذ مهاجمان و مانیتورینگ شبکه‌های صنعتی
- مهارت در اجرای حملات کنترل‌شده و بازسازی مسیر مهاجم
- طراحی داشبوردهای امنیتی و Ruleهای تشخیص حمله
- تسلط بر مستندسازی فنی و طراحی پاسخ به حادثه
- آمادگی برای مشارکت در تیم‌های SOC ،OT و پروژه‌های امنیت زیرساخت

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی مقدماتی با مفاهیم شبکه و امنیت سایبری(ترجیحا)
- تجربه با علاقه‌مندی به سیستم‌های کنترل صنعتی
- آشنایی با ابزارهای تحلیل شبکه امتیاز محسوب می‌شود.
- شرکت برای عموم آزاد است.
- محتوای کارگاه برای سطوح مختلف قابل فهم و اجرا است.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	جلسه اول: شناخت ساختار و روش‌های حمله مهاجمان کنترل صنعتی ICS	۹۰ دقیقه
۲	جلسه دوم: ایجاد قابلیت پایش و واکنش در برابر حملات سایبری صنعتی	۹۰ دقیقه

افزایش صحت و امنیت کد با استفاده از مدل‌های زبانی بزرگ: یک کارگاه عملی

رضا ابراهیمی آتانی، سید امیرحسین طباطبایی، کیاوش دادپور، عسل محمودی نژاد

مرکز آپا دانشگاه گیلان

چکیده

با گسترش روزافزون کاربرد نرم‌افزار در سامانه‌های حیاتی و امنیت‌محور، صحت و امنیت کد به یکی از چالش‌های اساسی در مهندسی نرم‌افزار و رمزنگاری تبدیل شده است. روش‌های سنتی تحلیل و آزمون امنیتی، اگرچه همچنان پرکاربرد هستند، اما در بسیاری از موارد زمان‌بر بوده و پوشش محدودی از آسیب‌پذیری‌ها را ارائه می‌دهند. در سال‌های اخیر، مدل‌های زبانی بزرگ به عنوان ابزاری نوین برای کمک به تولید، تحلیل و بهبود کد مورد توجه بوده‌اند. این مدل‌ها با تکیه بر قابلیت درک متن و کد، می‌توانند در شناسایی خطاهای منطقی، کشف آسیب‌پذیری‌های امنیتی و پیشنهاد اصلاحات مؤثر نقش مهمی ایفا کنند. در این کارگاه عملی، شرکت‌کنندگان ابتدا با مبانی نظری امنیت نرم افزار و تحلیل کد ایستا و همچنین مفاهیم پایه استفاده از مدل های زبانی بزرگ در حوزهٔ صحت و امنیت نرم‌افزار آشنا خواهند شد. سپس با بهره‌گیری از مثال‌های واقعی، توانایی استفاده از این مدل‌ها برای تحلیل و اصلاح کدهای آسیب‌پذیر در چند زبان برنامه‌نویسی مختلف از قبیل C++، C#، PHP، Phython و JAVA به‌صورت گام‌به‌گام تمرین می‌کنند. همچنین محدودیت‌ها، تهدیدات و چالش‌های امنیتی ناشی از استفاده از مدل‌های زبانی بزرگ در فرایند توسعهٔ نرم‌افزار خصوصا در کاربردهایی که سامانه‌های حیاتی هستند، نیز مورد بحث قرار خواهد گرفت. انتظار می‌رود در پایان کارگاه، شرکت‌کنندگان توانایی به‌کارگیری ابزارهای مبتنی بر هوش مصنوعی را در جهت افزایش صحت و امنیت کد کسب کرده و درک روشن‌تری از فرصت‌ها و تهدیدهای این فناوری در حوزه امنیت نرم‌افزار و رمزنگاری به دست آورند.

دستاوردهای علمی و عملی شرکت کنندگان

- نحوه استفاده از مدل‌های زبانی بزرگ به‌عنوان مکمل ابزارهای سنتی تحلیل ایستا

- به‌کارگیری تکنیک‌های مهندسی پرامپت برای افزایش دقت و کارایی در تحلیل کد.
- کاربردهای عملی LLMها در زمینه اسکن امنیتی، شناسایی باگ‌ها و بررسی‌های انطباق (Compliance Checks).
- شناسایی و درک محدودیت‌ها و ریسک‌های ناشی از تکیه بر مدل‌های زبانی بزرگ در تحلیل امنیتی.
- روش‌های ادغام LLMها در خطوط CI/CD و ترکیب آن‌ها با ابزارهای SAST موجود

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی اولیه با مفاهیم امنیت و مهندسی نرم افزار

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مروری بر مفاهیم امنیت نرم افزار و انواع تحلیل کد و معرفی چارچوب‌های تحلیل ایستاکد در زبان‌های برنامه‌نویسی	
۲	محدودیت‌ها و چالش‌های ابزارهای سنتی تحلیل ایستا کد	
۳	معرفی اجمالی مدل‌های زبانی بزرگ و ترازکردن این مدل‌های بزرگ ماشینی برای کاربردهای تحلیل کد	
۴	جایگاه مدل‌های زبانی بزرگ در تکمیل فرایند تحلیل ایستا کد	
۵	قابلیت‌های کلیدی مدل‌های زبانی بزرگ در شناسایی باگ‌ها و آسیب‌پذیری‌ها	
۶	تکنیک‌های مهندسی پرامپت برای بازبینی کد	
۷	شناسایی نمونه آسیب‌پذیری‌ها: SQL Injection، XSS، Buffer Overflow	
۸	مقایسه روش‌های Fine-tuning و Zero-shot/Few-shot prompting	
۹	ارزیابی و مقایسه عملکرد مدل‌های زبانی بزرگ در برابر ابزارهای SAST سنتی	
۱۰	تمرین ۱: استفاده از LLM برای شناسایی آسیب‌پذیری در قطعه‌کدهای چند زبان برنامه‌نویسی	
۱۱	تمرین ۲: طراحی یک بازبین کد خودکار ساده با پایتون و API مدل زبانی	
۱۲	تمرین ۳: تحلیل نتایج (False Positive / False Negative) و بهبود پرامپت‌ها	
۱۳	پیاده‌سازی بررسی‌های مبتنی بر LLM در چرخه‌های CI/CD	
۱۴	ترکیب مدل‌های زبانی بزرگ با ابزارهای سنتی SAST	
۱۵	ملاحظات اخلاقی، محدودیت‌ها و چالش‌های امنیتی	

احراز هویت با کارت هوشمند در سامانه‌های کنترل دسترسی: تحلیل آسیب‌ها و راهکارهای امن مبتنی بر استانداردهای جهانی

اکرم خالصی، زینب سعیدی

پژوهشگاه توسعهٔ فناوری‌های پیشرفته

چکیده

این ارائه، ساختاری ویژه را به‌عنوان یک مدل یک‌پارچه برای احراز هویت مبتنی بر کارت‌های هوشمند در یک سامانه کنترل دسترسی معرفی می‌کند و جایگاه آن در فرایند مدیریت مخاطره سازمانی را تبیین می‌نماید. اجزای فنی کلیدی شامل ساختار کارت، قالب‌های زیست‌سنجی، مکانیزم‌های رمزنگاری و مدیریت کلید و چرخه عمر کارت مورد بررسی قرار می‌گیرند. آسیب‌پذیری‌های مرتبط با کارت‌های هوشمند غیرتماسی (RFID) و روش‌های کاهش مخاطرات و تهدیدات مرتبط (در سه سطح مدیریتی، فنی، عملیاتی) مطرح می‌شود. در انتها نقش‌های مرتبط و نگاشت اسناد مرجع به مسئولیت‌ها برای استقرار پایدار و امن سامانه پیشنهاد می‌گردد. این ساختار می‌تواند به عنوان نقشه راهی برای اصلاح سامانه‌های موجود و بهبود طراحی سامانه‌های آینده به کار رود.

دستاوردهای علمی و عملی شرکت کنندگان

- آشنایی با مفهوم PIV به‌عنوان ساختاری برای احراز هویت در سامانه‌های کنترل دسترسی
- شناخت اجزای ساختار PIV به ویژه کارت هوشمند
- درک چالش‌ها و محدودیت‌های کارت‌های غیرتماسی، تهدیدات و روش‌های مقابله
- نقشه‌ی راه پیاده‌سازی PIV در سازمان: ساختاری که مراحل صدور کارت، مدیریت چرخه‌عمر، نکات فنی و سیاستی از زمان تصمیم‌گیری بر اجرا تا پیاده‌سازی و ارزیابی را توضیح می‌دهد.
- فهرست الزامات امنیتی پیاده‌سازی و ارزیابی کارت‌های غیرتماسی: فهرستی قابل اجرا برای ارزیابی آسیب‌پذیری‌های RFID، پیشنهاد کنترل‌های فنی و سیاستی برای احصا آسیب‌ها و مدیریت مخاطرات.
- نگاشت نقش‌ها و مسئولیت‌ها به مراجع و استانداردها: جدولی که نقش‌های سازمانی (مدیر امنیتی، طراح، پیاده‌ساز، ارزیاب، کاربر نهایی و ...) را به اسناد مختلف منطبق کند تا وظایف هر نقش در چرخه ی امنیت کارت مشخص شود.

این دستاوردها می‌توانند به شرکت‌کنندگان کمک کنند تا دانش و مهارت‌های خود را در زمینه طراحی سامانه‌های امن مدیریت دسترسی ارتقاء دهند و بتوانند با شناسایی بهتر الزامات و آسیب‌پذیری‌های کارت هوشمند در این سامانه‌ها در مدیریت امنیت سازمان خود و همچنین در طراحی و ساخت چنین سامانه‌هایی موفق‌تر باشند.

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی با مبانی مدیریت امنیت در سازمان
- آشنایی با مبانی کارت‌های هوشمند(درک اولیه از انواع و نحوه کارکرد کارت های هوشمند)
- کارگاه به طور عمومی برای همه علاقه‌مندان به این حوزه قابل استفاده می‌باشد.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مقدمه	۱۰ دقیقه
۲	معرفی مفهوم PIV	۳۰ دقیقه
۳	امنیت در کارت‌های هوشمند مبتنی بر RFID	۳۰ دقیقه
۴	نگاشت به نقش‌ها	۱۰ دقیقه
۵	جمع‌بندی و پرسش و پاسخ	۱۰ دقیقه

برترین‌ها

رساله‌های برتر

ردیف	عنوان رساله	نویسنده/ دانشگاه	استاد راهنما / استاد مشاور	نتیجه ارزیابی
۱	رمزگذاری داده‌ها بر روی ابر با قابلیت جستجو در بستر رمزنگاری شناسه-مبنا	دانیال شیرالی/دانشگاه شهید بهشتی	خانم دکتر زیبا اسلامی	رساله برتر
۲	شناسایی و پیشگیری از سخت افزارهای جعلی با قفل منطقی مقیاس پذیر و قابل اطمینان	خانم مونا هاشمی/دانشگاه تهران	آقای دکتر سیامک محمدی	رساله شایسته تقدیر

پایان‌نامه‌های برتر

ردیف	عنوان رساله	نویسنده/ دانشگاه	استاد راهنما / استاد مشاور	نتیجه ارزیابی
۱	تحلیل رمزهای متقارن سبک‌وزن با استفاده از یادگیری عمیق	ایمان میرزاعلی مازندرانی/دانشگاه تربیت دبیر شهید رجایی	آقای دکتر نصور باقری و آقای دکتر صادق صادقی	پایان‌نامه برتر

۲	کنترل دسترسی برای دستگاه‌های پزشکی قابل کاشت با بهره‌گیری از زیست‌سنجهECG	خانم نرگس مختاری/ دانشگاه تربیت دبیر شهید رجایی	آقای دکتر نصور باقری و آقای دکتر صادق صادقی	پایان‌نامه شایسته تقدیر
۳	تشخیص ناهنجاری در بارهای کاری رایانش ابری براساس استفاده از منابع	خانم پریا جورابچی/دانشگاه صنعتی سهند	خانم دکتر آرزو جهانی	پایان‌نامه شایسته تقدیر
۴	پرداخت‌های خرد امن در زیست‌بوم اینترنت اشیاء	آقای عرفان بهرامی/دانشگاه صنعتی شریف	آقای دکتر مرتضی امینی	پایان‌نامه شایسته تقدیر
۵	ارائۀ روشی جهت حفظ حریم خصوصی در به اشتراک‌گذاری مسیر	آقای محمد حسین فرحناکیان/دانشگاه صنعتی شیراز	آقای دکتر رسول اسماعیلی فرد	پایان‌نامه شایسته تقدیر

شاخه‌های دانشجویی برتر

ردیف	عنوان شاخه دانشجویی	نماینده شاخه دانشجویی	رئیس شاخه دانشجویی	دبیر شاخه دانشجویی
۱	دانشگاه علم و صنعت ایران	دکتر ابوالفضل دیانت	دکتر زهرا سعیدی	امیرحسین قدیمی

نمایشگاه

شرکت‌ها و سازمان‌های زیر در بخش نمایشگاه بیست‌ودومین کنفرانس بین‌المللی انجمن رمز ایران غرفه داشتند و محصولات و خدمات خود را معرفی نمودند.

- همراه اول
- هلدینگ فناوری و نوآوری صاد
- ناوک ارتباط هوشمند اوراسیا (سایبرلند)
- مرکز تحقیقات هوش مصنوعی دانشگاه صنعتی شریف
- متیران
- گروه صنعتی گلرنگ
- گروه تجارت الکترونیک دیجی‌کالا
- گروه آموزشی لیان
- گراف
- صنایع مخابرات صاایران
- صنایع الکترونیک زعیم
- شرکت نوآوران امن اندیش شریف (نآد)
- شرکت نرم‌افزاری امن پرداز
- شرکت توسعهٔ زیرساخت‌های فناوری اطلاعات سیگما
- سباپردازش
- رویال پرداز تیام
- دژافزارنت
- توسعهٔ امن کیان (تاکیان)
- تپسی
- پیام پرداز
- پژوهشگاه توسعهٔ فناوری‌های پیشرفته
- پژوهشگاه ارتباطات و فناوری اطلاعات
- پژوهشکده رایاسامانه‌های امن پارسا شریف
- بانک شهر
- ایرانسل
- امن‌پردازان کویر
- امن‌افزار گستر شریف
- آکادمی فن‌افزا
- آکادمی راوین
- آکادمی آکادینو