انجمن رمز ایران
Iranian Society of Cryptology

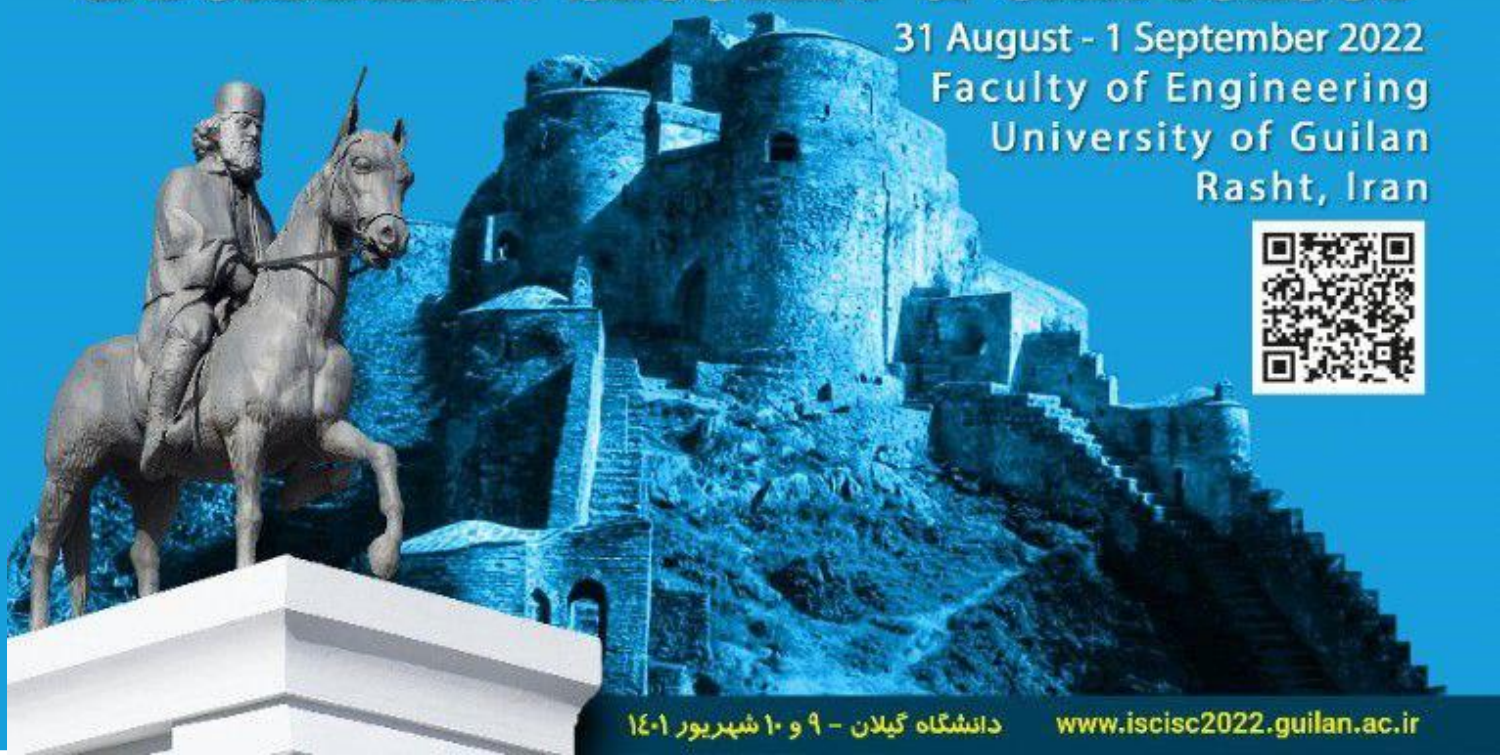
دانشگاه گیلان

نوزدهمین کنفرانس بین‌المللی انجمن رمز ایران

کتابچه راهنما و چکیده

19th International ISC Conference on INFORMATION SECURITY & CRYPTOLOGY

31 August - 1 September 2022
Faculty of Engineering
University of Guilan
Rasht, Iran



دانشگاه گیلان - ۹ و ۱۰ شهریور ۱۴۰۱ www.iscisc2022.guilan.ac.ir


بسم الله الرحمن الرحیم

بسم الله الرحمن الرحیم

کتابچه راهنمای نوزدهمین کنفرانس بین المللی انجمن رمز ایران

دانشگاه گیلان، دانشکده فنی

۹ و ۱۰ شهریور ۱۴۰۱

فهرست

دبیرخانه نوزدهمین کنفرانس بین المللی انجمن رمز ایران

دانشگاه گیلان، دانشکده فنی

تلفن ۰۱۳-۳۳۶۹۰۲۷۰

رایانامه cert@guilan.ac.ir

وبگاه https://iscisc2022.guilan.ac.ir

پیشگفتار

دانشگاه گیلان بعنوان بزرگترین دانشگاه شمال کشور برای دومین بار مفتخر است تا میزبانی از محققان، متخصصان، دانشمندان و دانشجویان علاقمند به حوزه های تحقیقاتی امنیت فضای تولید و تبادل اطلاعات را در بزرگترین کنفرانس علمی مرتبط با امنیت عهده دار باشد. در این فرصت طلایی محققین در نوزدهمین کنفرانس بین المللی انجمن رمز این گرد هم می آیند تا عالی‌ترین و نوین‌ترین عرصه‌های حوزه‌ی پراهمیت رمز و رمزنگاری را به بحث نشینند و نتایج آخرین تحقیق‌ها و دستاوردهای خود را به مشارکت گذارند. پیش از این در شهریور ماه سال ۱۳۹۴ در دوازدهمین کنفرانس انجمن رمز نیز دانشکده فنی و مهندسی دانشگاه گیلان در محیطی صمیمی و پربار افتخار بزرگ میزبانی از محققین علوم امنیتی را بر عهده داشته است. بر خلاف دوره‌ی دوازدهم این بار شهر زیبای رشت میزبان قدوم خوش شرکت‌کنندگان نیست. وقایع دردناک ناشی از همه‌گیری COVID19 متاسفانه باعث شده تا کنفرانس نوزدهم نیز به صورت مجازی برگزار شود. سخنرانی‌های درنظرگرفته‌شده از جمعی از برترین محققین حوزه‌ی رمز در ایران و جهان که ما را مفتخر به مشارکت در این کنفرانس کرده‌اند، تحقیقات ارشمند پژوهشگران ارجمند و البته حضور شرکت‌کنندگان گران‌قدر کنفرانس یقیناً این گردهمایی را پرشور و پرآورد خواهد ساخت.

بیست مقاله برای ارائه در کنفرانس نوزدهم انجمن رمز پذیرفته شده و در هفت محور امنیت رایانش، امنیت شبکه، مبانی رمز، نهان‌سازی اطلاعات، پروتکل‌های امنیتی، پیاده‌سازی الگوریتم‌های رمزنگاری و بالاخره حملات مرتبط و مهندسی امنیت و امنیت خدمات الکترونیک دسته‌بندی شده‌اند. مقالات این محورهای هفت‌گانه در مجموع در قالب شش نشست به سمع و نظر متخصصین می‌رسند. شش سخنرانی از سخنرانان مدعو در ابتدای شش نشست کنفرانس بر غنای فنی این نشست‌ها می‌افزایند. در نوزدهمین کنفرانس انجمن رمز ایران پنج سخنرانی کلیدی از محققین و متخصصین برجسته‌ی حوزه‌ی رمز در ایران و جهان ارایه خواهد شد و میزگردی در حوزه‌ی چالش‌ها و راه‌کارهای امنیتی اپراتورهای تلفن همراه از دیگر نشست‌های این گردهمایی تخصصی خواهد بود. هم‌چنین جهت افزایش بار آموزشی و عملی محتوای کنفرانس کارگاه‌هایی توسط نخبگان صنایع برگزار می‌شوند که

حوزه‌هایی پراهمیتی را شامل می‌شوند: چالش‌ها و تهدیدهای امنیتی در نسل‌های مختلف تلفن همراه و شبکه‌ی 5G، پروتکل‌های اجماع بلاک‌چین، مراحل رسیدگی به رخدادهای سایبری و DevSecOps.

با توجه به اهمیت روزافزون پاسداری از مرزهای سایبری کشور، امید است تلاش‌های برگزارکنندگان بزرگترین رویداد امنیتی کشور در ارائه‌ی تحقیقات و تعلیمات نوین علوم افتایی به عمل نشیند و با افزایش علاقه مندی فضاهای دانشجویی و صنعت با انگیزه دوچندان مسیر ارزشمندی که توسط انجمن رمز ایران در اعتلای آموزش و پژوهش علوم امنیتی ایجاد نموده را ادامه دهند. از تمامی کسانی که با مشارکت گرانقدر خویش، شکل‌گیری این همایش را ممکن ساختند تقدیر می‌کنم، سپاس خود را به کلیه‌ی استادان، محققان، متخصصان و دانشجویان اعلام می‌دارم، زحمات رییس محترم و مدیران ارجمند دانشگاه گیلان و خصوصا انجمن معظم رمز ایران را ارج می‌نهم و از حامیان برگزاری کنفرانس که سهم عمده‌ای در به بار نشستن این رخداد دارند، به ویژه شرکت خدمات انفورماتیک و همراه اول کمال امتنان را دارم.

برای همه‌ی این رهروان مسیر اعتلای دانش و فناوری آرزوی توفیق روزافزون دارم.

دکتر رضا ابراهیمی آتانی

دبیر نوزدهمین کنفرانس بین المللی انجمن رمز ایران

برگزارکنندگان

دانشگاه گیلان

انجمن رمزایران
iranian Society of Cryptology

حمایت کنندگان

مرکز منطقه‌ای اطلاع‌رسانی علوم و فناوری

امن افزار گستر شریف

هاد اول

شرکت خدمات انفورماتیک
Informatics Services Corporation

پژوهشگاه توسعه فناوری های پیشرفته

شرکت مهندسی ارتباطی پیام پرداز

پایگاه استنادی علوم جهان اسلام
ISC
Islamic World Science Citation Center

The ISC Int'l Journal of Information Security
ISeCure

صنایع الکترونیک زعیم

مرکز تولید اسناد هویتی ایران

خلیج همیشه فارس

کانون هماهنگی افتا

سازمان کنفرانس

رئیس کنفرانس: دکتر فرید نجفی

دبیر کنفرانس: دکتر رضا ابراهیمی آتانی

دبیر علمی کنفرانس: دکتر رضا ابراهیمی آتانی

دبیر اجرایی کنفرانس: دکتر سید محمدحسن شکریان

اعضای کمیته علمی

- دکتر رضا ابراهیمی آتانی- دانشگاه گیلان
- دکتر زهرا احمدیان- دانشگاه شهید بهشتی
- دکتر محمود احمدیان عطاری- دانشگاه صنعتی خواجه نصیرالدین طوسی
- دکتر محمد علی اخایی- دانشگاه تهران
- دکتر ترانه اقلیدس- دانشگاه صنعتی شریف
- دکتر هاله امین طوسی- دانشگاه فردوسی مشهد
- دکتر مرتضی امینی- دانشگاه صنعتی شریف
- دکتر نصور باقری- دانشگاه تربیت دبیر شهید رجایی
- دکتر غلامرضا باقرسلیمی- دانشگاه گیلان
- دکتر مهران سلیمان فلاح- دانشگاه صنعتی امیرکبیر
- دکتر سیاوش بیات سرمدی- دانشگاه صنعتی شریف
- دکتر علی پاینده- دانشگاه صنعتی مالک اشتر
- دکتر محمد حسام تدین- پژوهشگاه ارتباطات و فناوری اطلاعات
- دکتر بهروز ترک لادانی- دانشگاه اصفهان
- دکتر علی جهانیان- دانشگاه شهید بهشتی
- دکتر محمد دخیل علیان- دانشگاه صنعتی اصفهان
- دکتر صادق دری نوگورانی- دانشگاه تربیت مدرس

- دکتر مجید بیات- دانشگاه شاهد
- دکتر محمود سلماسی‌زاده- دانشگاه صنعتی شریف
- دکتر هادی سلیمانی- دانشگاه شهید بهشتی
- دکتر شهریار شاه حسینی- دانشگاه علم و صنعت ایران
- دکتر امیر سیددانش- دانشگاه گیلان
- دکتر حمیدرضا شهریاری- دانشگاه صنعتی امیرکبیر
- دکتر معصومه صفخانی- دانشگاه تربیت دبیر شهید رجایی
- دکتر محمدرضا عارف- دانشگاه صنعتی شریف
- دکتر جلیل سیفعلی هرسینی – دانشگاه گیلان
- دکتر محمد عبدالهی ازگمی- دانشگاه علم و صنعت ایران
- دکتر بیژن علیزاده- دانشگاه تهران
- دکتر محمد صیاد حقیقی- دانشگاه تهران
- دکتر عباس قائمی بافقی- دانشگاه فردوسی مشهد
- دکتر علیرضا کشاورز حداد- دانشگاه شیراز
- دکتر علی شکیبا- دانشگاه ولیعصر رفسنجان
- دکتر حمید ملا- دانشگاه اصفهان
- مهندس جواد مهاجری- دانشگاه صنعتی شریف
- دکتر احمد عباسی- دانشگاه گیلان
- دکتر عبدالرسول میرقدری- دانشگاه امام حسین (ع)
- دکتر سیدامیر مرتضوی- دانشگاه تبریز
- دکتر مهتاب میرمحسنی- دانشگاه صنعتی شریف
- دکتر فرید فیضی- دانشگاه گیلان
- دکتر شاهرخ قائم مقامی- دانشگاه صنعتی شریف
- دکتر سیدمحمدحسین شکریان- دانشگاه گیلان
- دکتر اسدالله شاه‌بهرامی- دانشگاه گیلان
- دکتر محمودرضا هاشمی- دانشگاه تهران
- دکتر محمدرضا هوشمند اصل- دانشگاه محقق اردبیلی

- Dr. Amir Moradi-Ruhr- Universitaet Bochum, Germany
- Prof. Josef Pieprzyk- Mcquarie University, Australia
- Prof. Joachim Posegga- University of Passau, Germany
- Prof. Vincent Rijmen- KU Leuven, Belgium

اعضای کمیته اجرائی

- دکتر سیدمحمدحسین شکریان (دبیر کمیته اجرایی کنفرانس)
- دکتر رضا ابراهیمی آتانی (دبیر کمیته علمی کنفرانس)
- دکتر علی مرتضی پور
- دکتر سیدسیامک اشرف تالش
- دکتر غلامرضا باقرسلیمی
- دکتر اسدالله شاه بهرامی
- دکتر فرید فیضی (مسئول کمیته انتشارات)
- دکتر احمد عباسی
- دکتر جلیل سیفعلی هرسینی
- دکتر امیر سید دانش
- مهندس طه یاسین رضاپور (مسئول دبیرخانه)
- زهرا فره وشی
- فاطمه حیدری
- سعید رهسپار (مسئول کمیته اطلاع رسانی و وب سایت)
- حسین اعلایی
- هادی محمدزاده

اعضای تیم دانشجویی دانشگاه گیلان

- امیرمحسن اختیاری
- مهسا غلامی
- بهرنگ آذرباد
- مهشید علیزاده
- مریم میرصالحی
- افشین حسنی
- یزدان حقی

برنامه برگزاری کارگاه های نوزدهمین کنفرانس رمز انجمن رمز ایران

۷ و ۸ شهریور ۱۴۰۱

ردیف	جزئیات نشست کارگاه ها	شروع	پایان	محل برگزاری
۱	کارگاه شماره ۱: **مراحل رسیدگی به رخدادهای سایبری به همراه سناریوی تحلیل بدافزار** ارائه دهنده **:آقای مهندس میلاد افشار نادری** **(دو شنبه ۷ شهریور ساعت ۹ الی ۱۳)**	۹:۰۰	۱۳:۰۰	اتاق شماره ۱: https://skyroom.online/ch/uog/iscisc_room1
۲	کارگاه شماره ۲: **نسل دوم تا نسل پنجم تلفن همراه، چالش‌ها و تهدیدات امنیتی** ارائه دهنده: **آقای مهندس امیرحسین پورشمس** **(دوشنبه ۷ شهریور ساعت ۱۵ الی ۱۹)**	۱۵	۱۹	اتاق شماره ۱: https://skyroom.online/ch/uog/iscisc_room1

ردیف	جزئیات نشست کارگاه ها	شروع	پایان	محل برگزاری
۳	کارگاه شماره ۳: **پروتکل های اجماع بلاکچین** **ارائه دهنده: آقای دکتر رسول رمضانیان** **(سه شنبه ۸ شهریور ساعت ۹ الی ۱۳)**	۹	۱۳	اتاق شماره ۱: https://skyroom.online/ch/uog/iscisc_room1
۴	کارگاه شماره ۴: **مخاطرات و ریسک های امنیتی در شبکه 5G** **ارائه دهنده: آقای مهندس حسین احمدی** **(سه شنبه ۸ شهریور ساعت ۹ الی ۱۳)**	۹	۱۳	اتاق شماره ۲: https://skyroom.online/ch/uog/iscisc_room2
۵	کارگاه شماره ۵: **آشنایی عملی با DevSecOps و راه اندازی یک نمونه pipeline آن در AWS** **ارائه دهندگان: آقای دکتر علیرضا نوروزی و خانم مهندس مهسا لمیعیان** **(سه شنبه ۸ شهریور ساعت ۱۵ الی ۱۹)**	۱۵	۱۹	اتاق شماره ۱: https://skyroom.online/ch/uog/iscisc_room1

برنامه کلی کنفرانس (روز اول)، چهارشنبه ۹ شهریور ماه ۱۴۰۱

ردیف	عنوان نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل برگزاری
۱	مراسم افتتاحیه	تلاوت قرآن، سرود ملی و کلیپ معرفی کنفرانس سخنرانی رئیس دانشگاه گیلان (دکتر فرید نجفی) سخنرانی دبیر کنفرانس (دکتر رضا ابراهیمی آتانی) اعلام برنامه کنفرانس		۰۸:۳۰	۰۹:۰۰	سالن کنفرانس: https://www.skyroom.online/ch/uog/iscisc_room1
۲	سخنرانی کلیدی ۱	مهندس محمود خالقی معاونت امنیت فضای تولید و تبادل اطلاعات سازمان فناوری اطلاعات ایران **تاثیر خط‌مشی‌ها و راهبردهای امنیت و دفاع سایبری بر آسیب‌پذیری‌های فناوری اطلاعات کشور**	دکتر رضا ابراهیمی آتانی	۹:۰۰	۱۰:۰۰	اتاق شماره ۱: https://www.skyroom.online/ch/uog/iscisc_room1
		استراحت		۱۰:۰۰	۱۰:۱۵	

ردیف	عنوان نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل برگزاری
۳	سخنرانی کلیدی ۲	دکتر بهروز ترک لادانی، استاد گروه مهندسی کامپیوتر دانشگاه اصفهان **امنیت نرم: مروری بر مفاهیم، کاربرد و پژوهش‌ها**	دکتر هاله امین طوسی	۱۰:۱۵	۱۱:۱۵	اتاق شماره ۱: https://www.skyroom.online/ch/uog/iscisc_room1
	استراحت			۱۱:۱۵	۱۱:۲۰	
	نشست ارائه مقالات ۱	امنیت رایانش	دکتر محمد عبدالهی ازگمی و دکتر فرید فیضی	۱۱:۲۰	۱۱:۵۰	اتاق شماره ۱: https://www.skyroom.online/ch/uog/iscisc_room1
۴		**دکتر مریم زارع زاده، دانش‌آموخته دانشگاه اصفهان** (سخنران مدعو ۱) **محاسبه امن ضرب اسکالر برای حفظ حریم خصوصی در داده کاوی**		۱۱:۲۰	۱۱:۵۰	
۵		هاله امین‌طوسی، سید سالار قاضی و سحر پیله‌ور مؤخر ***On the Suitability of Improved TrustChain for Smartphones***		۱۱:۵۰	۱۲:۱۰	
۶		سارا مقیمی و محمدعلی هادوی **مدل‌سازی سطح توانایی مهاجم با تمرکز بر حملات تزریق روی برنامه‌های کاربردی وب**		۱۲:۱۰	۱۲:۳۰	

ردیف	عنوان نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل برگزاری
۷		امیرحسین صیاد عبدی، بهروز ترک لادانی و بهمن زمانی ***Towards a Formal Approach for Detection of Vulnerabilities in the Android Permissions System***		۱۲:۳۰	۱۲:۵۰	
		استراحت		۱۲:۵۰	۱۴:۰۰	
	نشست ارائه مقالات ۲	**امنیت شبکه، مبانی رمز و نهان‌نگاری**	دکتر مرتضی امینی و دکتر علی اخایی	۱۴:۰۰	۱۵:۵۰	اتاق شماره ۱: https://www.skyroom.online/ch/uog/iscisc_room1
۸		دکتر جواد قره‌چمنی، Hong Kong University of Science and Technology (سخنران مدعو ۲) ***Secure and Practical Search over Dynamic Encrypted Datasets***		۱۴:۰۰	۱۴:۳۰	
۹		فاطمه دلدار، مهدی آبادی و محمد ابراهیمی فرد ***Android Malware Detection using One-Class Graph Neural Networks***		۱۴:۳۰	۱۴:۵۰	
۱۰		امیر جلالی بیگدلی و سمیه مظفری ***Lightweight Identification of Android Malware with Knowledge Distillation and Deep Learning Approach***		۱۴:۵۰	۱۵:۱۰	
۱۱		وجیهه ثابتی و معصومه سبحانی سوادرودباری		۱۵:۱۰	۱۵:۳۰	

ردیف	عنوان نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل برگزاری
		نهان نگاری تصویر مبتنی بر حوزه موجک با ایده جاسازی در نواحی با تغییرات زیاد زیرباندهای فرکانس بالا				
۱۲		هادی آقایی و بهاره اخباری ***One-Shot Achievable Secrecy Rate Regions for Quantum Interference Wiretap Channel***		۱۵:۳۰	۱۵:۵۰	
	نشست ارائه مقالات ۳	**پروتکل‌های امنیتی**	دکتر حمید ملا و مهندس جواد مهاجری	۱۴:۰۰	۱۵:۳۰	اتاق شماره ۲: https://www.skyroom.online/ch/uog/iscisc_room2
۱۳		دکتر محمد علی، استادیار دانشگاه صنعتی امیرکبیر (سخنران مدعو۳) ***Attribute-based Remote Data Auditing and User Authentication for Cloud Storage Systems***		۱۴:۰۰	۱۴:۳۰	
۱۴		محمدعلی هادوی، مریم سعیدی صدر و سید غلامحسن طباطبایی ***SecureKV: Secure Searchable Outsourcing of Key-Value Databases to the Public Cloud***		۱۴:۳۰	۱۴:۵۰	
۱۵		صبا مرندی و فرخ لقا معظمی گودرزی **تحلیل امنیتی یک پروتکل تبادل کلید و احراز اصالت گمنام در شبکه حسگرهای پوششی**		۱۴:۵۰	۱۵:۱۰	

ردیف	عنوان نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل برگزاری
۱۶		علی خزائی، حسین همائی و منیره هوشمند **پروتکل چندکاربره گفت‌وگوی کوانتومی با قابلیت گسترش تعداد کاربران در زمان اجرا**		۱۵:۱۰	۱۵:۳۰	
		استراحت		۱۵:۵۰	۱۶:۱۵	
۱۷		**میز گرد: چالش‌ها و راهکارهای امنیتی اپراتورهای تلفن همراه** **مهندس حاج مبینی، کارشناس امنیت اپراتور** **مهندس اسماعیل‌نژاد، کارشناس امنیت بخش خصوصی** **مهندس احمدی، کارشناس امنیت زیرساخت اپراتور** **مهندس توکلی، کارشناس امنیت شبکه** **دکتر هاشم حبیبی، امن افزار گستر شریف**	دکتر هاشم حبیبی	۱۶:۱۵	۱۸:۱۵	اتاق شماره ۱: https://www.skyroom.online/ch/uog/iscisc_room1
پایان روز اول						

برنامه کلی کنفرانس (روز دوم)، پنج‌شنبه ۱۰ شهریور ماه ۱۴۰۱

ردیف	عنوان نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل برگزاری
۱۸	سخنرانی کلیدی ۳	**Dr. Sushmita Ruj, UNSW**, Sydney ***Proofs of Storage and Applications***	دکتر هاله امین طوسی	۸:۳۰	۹:۳۰	اتاق شماره ۱: https://www.skyroom.online/ch/uog/iscisc_room1
		استراحت		۹:۳۰	۹:۴۵	
	نشست ارائه مقالات ۴	پیاده سازی الگوریتم های رمز نگاری و حملات مرتبط	دکتر علی جهانیان و دکتر محمدحسین شکریان	۹:۴۵	۱۱:۳۵	اتاق شماره ۱: https://www.skyroom.online/ch/uog/iscisc_room1
۱۹		دکتر مهدی اصفهانی، دانش‌آموخته‌ی پسادکتری از دانشگاه صنعتی شریف (سخنران مدعو ۴) **مروری بر امنیت ریزمعماری پردازنده‌ها**		۹:۴۵	۱۰:۱۵	
۲۰		حامد رمضانی‌پور، نوید وفایی و نصور باقری ***Practical Differential Fault Attack on CRAFT, a Lightweight Block Cipher***		۱۰:۱۵	۱۰:۳۵	
۲۱		محمدعلی حاجی سلطانی، راضیه سالاری فرد و هادی سلیمانی		۱۰:۳۵	۱۰:۵۵	

ردیف	عنوان نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل برگزاری
		Secure and Low-area Implementation of the AES Using FPGA				
۲۲		نوید وفایی، مریم پرکار و نصور باقری ***Enhanced Differential Fault attack on SKINNY: From Theory to Practical Attack***		۱۰:۵۵	۱۱:۱۵	
۲۳		امیر اشتری، احمد شعبانی و بیژن علیزاده ***Mutual Lightweight PUF-Based Authentication Scheme Using Random Key Management Mechanism for Resource-Constrained IoT Devices***		۱۱:۱۵	۱۱:۳۵	
	نشست ارائه مقالات ۵	**پروتکل‌های امنیتی ۲**	دکتر بهروز ترک لادانی و دکتر نصور باقری	۹:۴۵	۱۱:۳۵	اتاق شماره ۲: https://www.skyroom.online/ch/uog/iscisc_room2
۲۴		دکتر سمیه دولت نژاد، دانش‌آموخته‌ی دانشگاه صنعتی شریف (سخنران مدعو۵) **راستی آزمایی صحت اجرای توابع تجمعی برون‌سپاری‌شده با منابع داده‌ی توزیع‌شده**		۹:۴۵	۱۰:۱۵	
۲۵		علیرضا شفیعی‌نژاد و سجاد پلنکی ***Attribute-Based Encryption with Efficient Attribute Revocation, Decryption Outsourcing and Multi-Keyword Searching in Cloud Storage***		۱۰:۱۵	۱۰:۳۵	

ردیف	عنوان نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل برگزاری
۲۶		علیرضا هدیه‌لو، جواد مهاجری و محمدرضا عارف **روش اجماع با امنیت بالا و بار مخابراتی کم**		۱۰:۳۵	۱۰:۵۵	
۲۷		افشین کرم‌پور، مائده عاشوری تلوکی و بهروز ترک لادانی ***Light-Weight Privacy-Preserving Data Aggregation Protocols in Smart Grid Metering Networks***		۱۰:۵۵	۱۱:۱۵	
۲۸		سپهر دماوندی کوزه‌کنان و صادق دری نوگورانی ***An Electronic Voting Scheme Based on Blockchain Technology and Zero-Knowledge Proofs***		۱۱:۱۵	۱۱:۳۵	
		استراحت		۱۱:۳۵	۱۱:۴۵	
۲۹	سخنرانی کلیدی ۴	Dr. Pedro Peris-Lopez, Carlos III University of Madrid ***Biosignals: a Powerful Tool in the World of Cybersecurity***	دکتر نصور باقری	۱۱:۴۵	۱۲:۴۵	اتاق شماره ۱: https://www.skyroom.online/ch/uog/iscisc_room1
		استراحت		۱۲:۴۵	۱۴	

ردیف	عنوان نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل برگزاری
۳۰	سخنرانی کلیدی ۵	Prof. Lejla Batina, Radboud University, The Netherlands ***Side-Channel Analysis of Cryptographic Implementations: Lessons Learned and Future Directions***	دکتر سیدمحمدحسین شکریان	۱۴:۰۰	۱۵:۰۰	اتاق شماره ۱: https://www.skyroom.online/ch/uog/iscisc_room1
		استراحت		۱۵:۰۰	۱۵:۱۵	
	نشست ارائه مقالات ۶	مهندسی امنیت و امنیت خدمات الکترونیکی	دکتر محمد حسام تدین و دکتر علیرضا کشاورز حداد	۱۵:۱۵	۱۶:۲۵	اتاق شماره ۱: https://www.skyroom.online/ch/uog/iscisc_room1
۳۱		Dr. Hayyan Salman Hasan, Albaath university Syrian Arab Republic (سخنران مدعو ۵) ***Model Driven Engineering (MDE) for Android Security***		۱۵:۱۵	۱۵:۴۵	
۳۲		علی نظری و بابک صادقیان **تشخیص پولشویی الکترونیکی در تراکنش های تامین کنندگان خدمات پرداخت**		۱۵:۴۵	۱۶:۰۵	
۳۳		محمود سعیدی، نسرین تاج و آزاده بامداد مقدم **طراحی و پیاده سازی دو نمونه آزمایشگاهی سامانه هوشمند شناساگر ترافیک رمز شده VoIP اسکایپ و ابزار گریز lantern به روش یادگیری عمیق**		۱۶:۰۵	۱۶:۲۵	

ردیف	عنوان نشست	جزئیات نشست	مسئول نشست	شروع	پایان	محل برگزاری
		استراحت		۱۶:۲۵	۱۶:۴۵	
		اختتامیه		۱۶:۴۵	۱۷:۲۵	اتاق شماره ۱: https://www.skyroom.online/ch/uog/iscisc_room1
۳۴		گزارشی از کنفرانس		۱۶:۴۵	۱۶:۵۵	
۳۵		سخنرانی رییس انجمن		۱۶:۵۵	۱۷:۰۵	
۳۶		تقدیر و تشکر از حامیان، برگزیدگان کنفرانس، همکاران و شرکت‌کنندگان		۱۷:۰۵	۱۷:۱۵	
۳۷		معرفی میزبان کنفرانس بیستم		۱۷:۱۵	۱۷:۲۰	
۳۸		قرائت بیانیه پایانی کنفرانس		۱۷:۲۰	۱۷:۲۵	
پایان روز دوم						
پایان کنفرانس نوزدهم						
به امید دیدار شما در کنفرانس بیستم						

سخنرانان کلیدی

Biosignals: a powerful tool in the world of cybersecurity

Dr. Pedro Peris-Lopez
Associate Professor (accredited as a full professor) with the Department of Computer Science, Carlos III University of Madrid

In recent years, we can observe a proliferation of the use of vital signals for the design of novel cryptographic solutions. Likewise, incorporating telemetry in implanted or semi-implanted medical devices requires solutions that guarantee the patient's safety and the device's security. We will review state of the art in the use of biosignals in the world of cybersecurity, starting from identification/authentication solutions, through key generation algorithms or random number generators, to distance verification algorithms, among others.

Biography: Pedro Peris-Lopez received an M.Sc. degree in telecommunications engineering and a PhD in computer science from the Carlos III University of Madrid, Spain, in 2004 and 2008, respectively. He is currently an Associate Professor (accredited as a full professor) with the Department of Computer Science, Carlos III University of Madrid. His research interests are in the field of cybersecurity and e-health, digital forensics and hardware security. He has published many articles in specialized journals (62) and conference proceedings (45). His works have more than 4800 citations, and his h-index is 31. For additional information, see https://www.lightweightcryptography.com/.

Proofs of Storage and Applications

Dr. Sushmita Ruj, Senior Lecturer in the School of Computer Science and Engineering, UNSW, Sydney

Cloud service providers can be malicious and tamper with the data. Proofs of storage enable clients to verify data integrity. We will discuss the concept of proofs of storage and present some of our constructions. We will then discuss limitations of existing proofs of storage and show how blockchains can address these limitations. We will discuss applications of proofs of storage for secure, privacy preserving and accountable data sharing and trading.

Biography Sushmita Ruj is Senior Lecturer at UNSW, Sydney. Before joining UNSW, she was a Senior Research Scientist at CSIRO's Data61, an Associate Professor at Indian Statistical Institute and an Assistant Professor at Indian Institute of Technology, IIT, Indore. She was a researcher/visiting faculty at University of Ottawa, Canada, Lund University, Sweden, NTU, Singapore, KDDI R&D Labs, Japan, INRIA, France, Kyushu University, Japan and intern at Microsoft Research Labs, India. She received her B.E. degree from Indian Institute of Engineering, Science and Technology (IIEST), Shibpur, India and Masters and Ph.D. from Indian Statistical Institute, India, all in Computer Science. Her research interests are in applied cryptography, blockchains, cybersecurity and data privacy. Sushmita serves on the Editorial board of Elsevier Journal of Information Security and Applications (JISA) and Pervasive and Mobile Computing (PMC). She served as a Program Co-Chair for ACISP 2021 and Indocrypt 2019. She won best paper awards at ISPA 2007, IEEE PIMRC 2011 and IEEE ANTS WIE'17. She received Samsung GRO award, NetApp Faculty Fellowship, Cisco University Research Grant, OCSP grant from IBM Research. Sushmita is a Senior member of ACM and IEEE.

Side-channel analysis of cryptographic implementations: Lessons learned and future directions

Prof. Lejla Batina, Professor, applied cryptography and embedded systems security, Radboud University, The Netherlands.

In this talk we give an overview of side-channel attacks on implementations of cryptography and countermeasures. We survey the approaches to analysis and attacks, from mutual information to deep learning and recent efforts on leakage simulators for attack prevention. In the end, we identify some avenues for future research.

Biography: Lejla Batina received her Ph.D. from KU Leuven, Belgium (2005) and prior to that studied at the Eindhoven University of Technology, (Professional Doctorate in Engineering in 2001) and worked as a cryptographer for SafeNet B.V. (2001–2003). Currently, she is a professor in embedded systems security at the Radboud University in Nijmegen, the Netherlands. She has coauthored more than 150 refereed articles. Her current research interests include implementations of cryptography and physical security. Her research group at Radboud consists of 10+ researchers and 10 Ph.D. students have graduated under her supervision. She is a senior member of IEEE and an Editorial board member of top journals in security, such as IEEE Transactions on Information Forensics and Security and ACM Transactions on Embedded Computing Systems. She was program co-chair of CHES 2014, ACM WiSec 2021 and Africacrypt 2022. Currently, she serves as a program co-chair for SPACE 2022.

تاثیر خط‌مشی‌ها و راهبردهای امنیت و دفاع سایبری بر آسیب‌پذیری‌های فناوری اطلاعات کشور

مهندس محمود خالقی
معاونت امنیت فضای تولید و تبادل اطلاعات سازمان فناوری اطلاعات ایران

چکیده: جمهوری اسلامی ایران، یکی از اولین کشورهایی بود که نسبت به تشکیل نهاد سیاست‌گذار و اتخاذ خط‌مشی‌ها و راهبردهای ملی در حوزه امنیت فضای تبادل اطلاعات خود اقدام نمود. در پی پیشنهاد انجمن رمز ایران در اسفند ۱۳۸۱ و با دستور رئیس‌جمهور وقت، شورای عالی امنیت فضای تبادل اطلاعات (افتا)، تشکیل و تدوین سند راهبردی امنیت فضای تبادل اطلاعات کشور را در اولویت اقدام قرار داد. در نهایت، سند راهبردی افتا در تاریخ ۱۳ تیرماه ۱۳۸۴ به تصویب هیأت محترم دولت ج.ا.ایران رسید. در رتبه‌بندی سال ۲۰۲۰ اتحادیه بین المللی مخابرات (ITU) بر اساس شاخص جهانی امنیت سایبری (GCI)، وضعیت انطباق امنیت فضای تبادل اطلاعات ج.ا.ایران با کسب امتیاز ۸۱,۰۷ از مجموع ۱۰۰، در جایگاه ۵۴ قرار گرفته است و مجموعاً ۶۱ کشور در رتبه‌های بالاتر قرار گرفته‌اند. از منظر اثربخشی اقدام‌های انجام‌شده در حوزه امنیت نیز وقوع حملات و حوادث متعدد در فضای تبادل اطلاعات دستگاه‌های مختلف زیرساختی و غیرزیرساختی کشور طی یک‌سال اخیر، نمایان‌گر وضعیت بحرانی امنیت در این حوزه است. چرا با وجود پیش‌تازی کشور در حوزه نهادسازی و اتّخاذ خط‌مشی‌ها و راهبردهای ملی، با گذشت نزدیک به دو دهه، نه‌تنها وضعیت اثربخشی امنیت، بلکه وضعیت انطباق امنیت با بسیاری از به‌گزینه‌های حوزه امنیت نیز قابل پذیرش نمی‌باشد؟ بر اساس بررسی‌های انجام شده، عدم توجه کارشناسان و مدیران حوزه فناوری اطلاعات و امنیت دستگاه‌ها به فرامین و هشدارهای صادر شده توسط مراجع رسمی کشور و کمبود شدید سرمایه‌های انسانی متخصص، جزء اصلی‌ترین دلایل این امر محسوب می‌شوند. این در حالی است که از یک‌سو بالغ بر ۹ مرجع رسمی، اقدام‌های دستگاه‌های دولتی در این حوزه را رصد نموده و در تمامی اسناد راهبردی منتشر شده در حوزه امنیت و دفاع سایبری کشور نیز اقدام‌هایی از قبیل آگاهی‌رسانی، آموزش، همکاری‌های داخلی و بین‌المللی، هماهنگی، امن‌سازی و ... پیش‌بینی شده‌اند. شرایط موجود، حاصل اتّخاذ خط‌مشی‌ها و راهبردهای نامتوازن، بدیل‌سازی‌ها و فقدان توجه به برخی اصول اولیه امنیت در نهادها و اسناد بالادستی حوزه امنیت و دفاع

سایبری محسوب می‌شود. از جمله این موارد، می‌توان به بومی‌سازی و امنیتی‌سازی اشاره نمود. بومی‌سازی در موارد متعدد، به‌عنوان بدیل امن‌سازی مورد تأکید قرار گرفته است و الزام به به‌روزرسانی نرم‌افزارها و نصب وصله‌های امنیتی، در سایه بی‌اعتمادی به محصولات غیربومی، در اغلب اسناد، مورد غفلت قرار گرفته‌اند. کسب‌وکارهای افتا، در فرآیندهای امنیتی پیچیده، مجوز دریافت می‌نمایند، در حالی که برای عرضه خدمت یا فروش محصول به هر دستگاه دولتی، باید مراحل امنیتی متعدد و زمان‌بر را طی کنند.

امنیت نرم: مروری بر مفاهیم، کاربرد و پژوهش‌ها

دکتر بهروز ترک لادانی
استاد تمام دانشکده مهندسی کامپیوتر دانشگاه اصفهان

امروزه پیشرفت در حوزه های مختلف محاسباتی و ارتباطی منجر به تحول و گذار به عصر نوینی شده است که در آن اغلب به جای سامانه‌های سنتی بسته، کوچک و با مدیریت متمرکز، با سامانه‌های باز، وسیع، قابل گسترش و با مدیریت توزیع شده سروکار داریم. شبکه‌های اجتماعی و سامانه‌های مبتنی بر اینترنت اشیاء نمونه‌هایی از این تحول به شمار می‌آیند. این تحول را می‌توان حرکت از رویکرد سنتی «سازمان محور» به رویکرد جدید «اجتماع محور» تفسیر نمود. با این تلقی ویژه، مفهوم امنیت در سامانه‌ها نیز دستخوش تغییر و توسعه شده است:

- در حالی که امنیت در رویکرد سازمان محور مبتنی بر وضع و اعمال خط مشی‌های امنیتی از طریق بکارگیری سازوکارهای سخت (صفر و یک) نظیر رمزنگاری و کنترل دسترسی است، از آنجا که سامانه‌های جدید محاسباتی به ویژه از جنبه‌ی تعاملات، بسیار به جامعه بشری شبیه شده‌اند، دیگر صرف استفاده از روش‌های متمرکز و سازمان‌محور پاسخگوی نیازها نیست، و لذا به جای تکیه بر رویکردهای امنیتی سازمان محور، یک رویکرد امنیتی اجتماع محور که مبتنی بر تعریف و تبعیت از هنجارها، ارزش‌ها و کنترل‌های اجتماعی از طریق بکارگیری سازوکارهای نرم (فازی) است مورد استفاده قرار می گیرد.
- در حالی که در رویکرد سازمان محور، امنیت مفهومی وضعی و مبتنی بر یقین (اثبات) محاسباتی است، در رویکرد اجتماع‌محور امنیت مفهومی اکتشافی و مبتنی بر تجربه (اطمینان) دارد.

رویکرد تامین امنیت اجتماع محور که برگرفته از هوش تجمعی انسانی در برخورد با مسئله امنیت است، «امنیت نرم» نامیده می‌شود. امنیت نرم ریشه در تجربه‌ی هزاران ساله‌ی زندگی اجتماعی بشر و دستاوردهای معنوی وی دارد و امنیتی است که نه صرفاً بر مبنای قدرت بازدارندگی (کنترل سلبی)، بلکه بر اساس «اعتماد» افراد به یکدیگر شکل گرفته و مبتنی بر کنترل ایجابی است. در واقع انسان‌ها در جامعه غالباً به خوبی یاد می‌گیرند که چگونه موجودیت‌های قابل اعتماد را از موجودیت‌های غیر قابل اعتماد تمیز داده

و راهبردهای مناسب را در مواجهه با آنان در پیش گیرند. دقت کنید که امنیت نرم جایگزین امنیت سخت نیست، بلکه امنیت نرم یک مکمل اجتناب‌ناپذیر امنیت سخت در برخی سامانه‌های جدید محاسباتی است.

به عنوان نمونه‌ای از سازوکارهای امنیت نرم، سامانه‌های محاسبه و مدیریت «اعتماد» راه کارهای شناخته شده ای برای ایجاد «اصالت نرم» در محیط‌های محاسباتی جدید به شمار می‌روند. در حالی که اصالت در امنیت سنتی یک مفهوم صفر و یکی است، دوگان آن در امنیت نرم یعنی اعتماد، یک مفهوم فازی است. سامانه‌های اعتماد به موجودیت‌های محیط اجازه می‌دهند که بر اساس تجارب خود و دیگران، میزان درستکاری سایر اعضاء را پیش‌بینی و بر اساس آن «معتمدترین اعضاء» را جهت همکاری یا درخواست ارائه خدمت شناسایی نمایند. به عنوان نمونه در شبکه‌های نظیر به نظیر برای اشتراک منابع و یا در محیط‌های محاسباتی مشبک برای انتخاب گره همکار، هر گره از سیستم در نتیجه تراکنش‌هایی که با دیگر گره‌ها انجام می‌دهد، تجربه‌ای به دست می‌آورد که می‌تواند راهنمای وی در انتخاب گره‌های دیگر جهت انجام تراکنش‌های پیش رو باشد. در صورتی که تجربه قبلی نشان‌دهنده رفتار خصمانه یک گره (مانند ارسال فایل‌های آلوده به ویروس در شبکه‌های نظیر به نظیر، یا عدم پایبندی یک گره به تعهدات زمانی در محیطهای محاسباتی مشبک) باشد، برای جلوگیری از آسیب‌های بیشتر می‌توان از انجام تراکنش‌های جدید با وی خودداری نمود. سامانه‌های اعتماد چکیده تجارب گذشته را در قالب کمیتی مقایسه‌پذیر (تحت عنوان میزان اعتماد) در اختیار موجودیت‌های سامانه قرار می‌دهند. این قابلیت موجب می شود که سامانه‌های اعتماد در هر محیطی که نیاز به همکاری و تعامل دو به دو بین موجودیت‌هاست، کاربرد داشته باشند. امروزه از محاسبه و مدیریت اعتماد به صورت وسیعی در اغلب سامانه‌ها از قبیل تجارت الکترونیکی، شبکه‌های اجتماعی، ارتباطات بی‌سیم، سامانه‌های چندعامله، شبکه‌های اقتضایی و نظیر به نظیر، محاسبات مشبک و اینترنت اشیاء استفاده می شود.

به عنوان کاربردی از مفهوم امنیت نرم نیز می‌توان به موضوع کنترل انتشار شایعه در شبکه های اجتماعی به عنوان یک سازوکار تأمین «صحت نرم» اشاره نمود. اگر چه رشد روز افزون فضای مجازی و به ویژه شبکه‌های اجتماعی در بسیاری از کاربردها ارزشمند و ارزش آفرین است، با این حال، سادگی و فراگیری استفاده از امکانات این فضا و نقصان در فرهنگ بکارگیری آن و کمبود امکانات کافی مدیریت این فضا موجب شده که حجم شایعات موجود در آن نیز روز به روز افزایش یابد. این شایعات می توانند در اندک زمانی به دست میلیون‌ها کاربر رسیده و موجب خسارات فراوان شوند. در سال‌های اخیر، رواج شایعات در شبکه های اجتماعی که به ویژه با هدف فریب افکار عمومی ساخته می‌شوند، به یکی از نگرانی‌های جدی در جوامع مختلف تبدیل شده است. شایعات می‌تواند با قصد آسیب‌رسانی در حوزه های مختلف مدیریتی و یا حاکمیتی در اجتماع تهیه و هدایت شود. بنابر

این، با توجه به حجم بالای شایعات و لزوم تشخیص سریع آن‌ها، توسعه مدل‌هایی برای تحلیل نحوه انتشار و ردیابی شایعات و همچنین ارزیابی کارایی و اثربخشی سازوکارهای مختلف مقابله با شایعه به عنوان بخشی از سازوکارهای امنیت نرم از اهمیت و جایگاه ویژه‌ای برخوردار است. علاوه بر این، توسعه سامانه‌هایی که بتواند در مراحل اولیه انتشار، شایعه را به صورت خودکار تشخیص داده و اقدام به جلوگیری از انتشار بیشتر آن کند، از اولویت‌های سرمایه گذاری برای هر جامعه به شمار می‌رود.

با دیدگاه امنیت نرم مفاهیم نوظهوری همچون جنگ نرم و تهدید نرم نیز قابل تقسیر خواهد بود. از آنجا که فضای سایبر در سالهای اخیر امکانات رسانه‌ای بسیار قوی‌تر و اثرگذارتری را نسبت به رسانه های سنتی مثل روزنامه، رادیو و تلویزیون فراهم کرده است، تلاش می‌شود که از این امکانات در جهت اثرگذاری بر مخاطبین در راستای راه اندازی عملیات روانی، کاهش سرمایه اجتماعی، اعمال فشار برای ایجاد تغییر در اصول و رفتار یک نظام و یا به طور خاص تغییر خود نظام استفاده شود. به این مفهوم جنگ نرم سایبری گفته می شود. اگر از دیدگاه دو نوع کنترل سخت و نرم به موضوع نگاه کنیم، در مقابله با جنگ نرم سایبری هم هر دو نوع ساز و کار دفاعی سخت و نرم قابل تصور است. از آنجا که رویکرد اصلی در جنگ نرم فریبکارانه و مبتنی بر اغوای مخاطبین است، هر چند بکارگیری رویکرد کنترل سخت یا سلبی (روش هایی مثل ایجاد محدودیت در دسترسی مردم به اطلاعات نامناسب) برای مقابله در مواقع و مراحلی اجتناب ناپذیر است، ولی قطعاً رویکرد اصلی مقابله با جنگ نرم رویکردی ایجابی و مبتنی بر کنترل نرم است. محققین علوم کامپیوتری برای مدل سازی انتشار شایعه در شبکه‌های اجتماعی، از مدل انتشار ویروسی استفاده می کنند. ما می دانیم که در مدل انتشار ویروس، رویکرد واقعی و نجات دهنده واکسیناسیون عمومی یعنی مصونیت بخشی به مردم است. هر چند می دانیم در مواقعی که شدت انتشار و اثرگذاری ویروس رو به وخامت می گذارد، استفاده از روش‌هایی مثل قرنطینه، جدا کردن، فاصله گذاری و ... هم اجتناب ناپذیر است. مصونیت بخشی از طریق تزریق واکسن در مدل انتشار ویروس معادل کنترل نرم یا ایجابی برای جلوگیری از انتشار شایعه در شبکه های اجتماعی است و قرنطینه و فاصله گذاری معادل روشهای کنترل سخت یا سلبی است. همانطور که در مقابله با ویروس کرونا این نهایتاً واکسیناسیون بود که مسئله را فیصله داد نه فاصله گذاری و قرنطینه و ...، در مقابله با ناامنی های ناشی از جنگ نرم سایبری هم دفاع ایجابی یعنی بصیرت افزائی، روشنگری، تلاش برای بالا بردن سطح بلوغ فکری و سواد رسانه ای مخاطبین روش اصلی است و باید روی آن تمرکز شود. همانگونه که برای مقابله با جنگ سخت سایبری (نفوذگری، حملات سایبری و ...) در امنیت سنتی به سیاست‌گذاری، برنامه‌ریزی، نهادسازی، ابزارسازی و ارائه آموزش‌های تخصصی نیاز است، برای مقابله با تأثیرات جنگ نرم سایبری نیز، به صورت مشابه ایجاد تمهیداتی به اقتضاء موضوع برای مقابله و دفاع مؤثر اجتناب ناپذیر است. متاسفانه تا به حال تا حد زیادی از این موضوع در کشور غفلت شده است.

در این سمینار ضمن تبیین نظری مفاهیم پایه امنیت نرم، به تشریح دیدگاه، رئوس فعالیت‌ها و برخی دستاوردهای علمی حاصل شده در «گروه پژوهشی مدل‌سازی و تحلیل امنیت دانشگاه اصفهان» در طی حدود یک دهه گذشته در حوزه پژوهشی امنیت نرم مشتمل بر موارد زیر خواهیم پرداخت:

- طراحی مدل‌ها و سامانه‌های محاسبه اعتماد
- وارسی و اعتبارسنجی مدل‌های اعتماد
- مدل‌سازی و تحلیل نحوه انتشار و کنترل شایعه در شبکه های اجتماعی
- مدل‌سازی و تحلیل تأثیر بات‌های شبکه اجتماعی بر شکل‌دهی افکار عمومی در جنگ نرم سایبری

سخنرانان مدعو

محاسبه امن ضرب اسکالر برای حفظ حریم خصوصی در داده کاوی

دکتر مریم زارع زاده، فارغ التحصیل مقطع دکتری رشته فناوری اطلاعات، گرایش امنیت اطلاعات، دانشگاه اصفهان

محاسبات امن زیرشاخه‌ای از رمزنگاری نوین است که برای دو یا بیش از دو موجودیت این امکان را فراهم می‌آورد که به طور امن تابع دلخواهی از ورودی‌های محرمانه خود را محاسبه کنند. این تابع می‌تواند هر عمل محاسباتی توزیع شده از محاسبات ساده همچون پرتاب سکه تا محاسبات پیچیده همانند رأی‌گیری الکترونیکی و حراج الکترونیکی باشد. ضرب امن اسکالر یک نمونه کاربردی از محاسبات امن در بسیاری از زمینه‌های حفظ کننده‌ی حریم خصوصی می‌باشد. به عنوان مثال در داده‌کاوی و ادغام داده‌ها از منابع مختلف، چالش‌های امنیتی و حریم خصوصی زیادی وجود دارد. امنیت راهکار حفظ کننده‌ی حریم خصوصی در عملیات داده‌کاوی به امنیت پروتکل ضرب اسکالر بستگی دارد. تاکنون روش‌هایی برای ضرب امن اسکالر ارائه شده است اما با تهدید کامپیوترهای کوانتومی، موضوع ارائه راهکارهایی امن در مقابل حمله‌کنندگان کوانتومی مطرح می‌باشد. به عبارت دیگر حمله کننده، پروتکل ضرب داخلی را اجرا کرده و با کمک کامپیوترهای کوانتومی تلاش میکند ورودی دو بردار در عملیات داده‌کاوی را بدست آورد. در این سخنرانی راهکاری برای محاسبه امن ضرب اسکالر به روشی مقیاس‌پذیر و غیرتعاملی ارائه می‌گردد.

راستی آزمایی صحت اجرای توابع تجمعی برون‌سپاری‌شده با منابع داده‌ی توزیع‌شده

دکتر سمیه دولت نژاد، فارغ التحصیل مقطع دکتری رشته مهندسی کامپیوتر
دانشگاه صنعتی شریف

در سال‌های اخیر، یکی از موضوعات مورد پژوهش در حوزه‌ی امنیت محاسبات برون‌سپاری شده، راستی‌آزمایی صحت احرای محاسبات برون‌سپاری شده بر روی داده‌های دریافتی از چندین منبع‌داده است. در این ارایه، مسئله‌ی راستی‌آزمایی صحت اجرای پرسمان‌های درخواستی کاربر در کارساز غیرقابل اعتماد، برای توابع تجمعی بررسی شده است. در خصوص بررسی درستی نتایج اجرای توابع تجمعی، تا کنون راه‌حلی جامع که انواع توابع آماری همچون بیشینه، کمینه، چند-بالاترین/چند-پایین‌ترین، میانه و پرسمان‌های بازه‌ای را پوشش دهد، ارایه نشده است. در این رساله، ابتدا با استفاده از امضای همریخت RSA، ساختی برای بررسی درستی نتایج اجرای توابع خطی ارایه شده است. به دلیل اینکه هزینه بررسی درستی خروجی توابع خطی در این ساخت ثابت است و با افزایش تعداد منابع‌داده افزایش نمی‌یابد، در ادامه با استفاده از این ساختار، ساختاری برای بررسی درستی نتایج اجرای توابع تجمعی آماری و پرسمان بازه‌ای ارایه شده است. در انتها، راه‌حل‌های ارایه شده برای پرسمان‌های دارای پنجره نیز توسعه داده شده‌اند. راه‌حل‌های ارایه شده بر اساس مساله RSAدر مدل اوراکل تصادفی، امن و دارای ویژگی‌های درستی و اختصار هستند. در راه‌حل‌های ارایه شده، سربار ارتباطی به صورت لگاریتمی به اندازه وروی وابسته است و سربار محاسباتی به پارامترهای ثابت موجود در ساختارها که در زمان راه‌اندازی تنظیم‌شده‌اند وابسته است.

مروری بر امنیت ریزمعماری پردازنده ها

دکتر مهدی اصفهانی، فارغ التحصیل مقطع دکتری رشته ریاضی کاربردی از دانشگاه آزاد اسلامی واحد کرج و دوره پسادکتری دانشگاه صنعتی شریف

اخیراً نشت اطلاعات محرمانه از برخی اجزای ریزمعماری پردازنده‌ها با استفاده از روش‌های نرم‌افزاری، دغدغه‌ای جدی بین طراحان و سازندگان پردازنده-های اینتل و ARM ایجاد کرده و حتی تبدیل به یک چالش جدی بین تولیدکنندگان نرم‌افزارهای امنیتی و سیستم‌عامل‌ها شده است. به وسیله‌ی آسیب‌پذیری‌های سخت‌افزاری مبتنی بر ریزمعماری، حملاتی مانند Spectre و Meltdown در پردازنده‌های مدرن شناسایی شدند که مهاجم می‌تواند با استفاده از این آسیب‌پذیری‌ها، گذرواژه‌ها و داده‌های مخفی در حال پردازش را استخراج کند. در حالت عادی، برنامه‌ها مجوز خواندن داده‌ی برنامه‌های دیگر یا سیستم‌عامل را ندارند اما یک برنامه‌ی مخرب که از آسیب‌پذیری‌های Spectre و Meltdown استفاده می‌کند، می‌تواند داده‌های مخفی خود سیستم‌عامل یا برنامه‌های دیگر را مانند: گذرواژه‌های ذخیره‌شده در مدیریت رمز عبور یا در مرورگرها، عکس‌های شخصی، ایمیل‌ها و غیره را استخراج نماید. حملات مبتنی بر Spectre و Meltdown در کامپیوترها، موبایل‌ها و فضای ابر قابل کاربرد است. در سال ۲۰۱۸ اینتل طی گزارشی اعلام کرد که برای مقابله با حملات مبتنی بر Spectre و Meltdown، روی پردازنده‌ها طراحی مجدد انجام داده است. در سال ۲۰۱۹ لیپ و همکارانش حمله‌ای را تحت عنوان Fallout معرفی کردند و نشان دادند پردازنده‌هایی که در برابر Meltdown مقاوم‌اند، هنوز در برابر این نوع حملات آسیب‌پذیر هستند. در این ارائه ابتدا اهمیت و هدف حملات ریزمعماری پردازنده‌ها مورد بررسی قرار گرفته و سپس مبانی اولیه و تشریح کامل حملات Spectre و Meltdown بیان خواهد شد. اشاره‌ای به واریانت‌های مختلف حملات Spectre و Meltdown خواهد شد و امنیت انواع مختلف پردازنده‌های اینتل و ARM در برابر این حملات مورد بررسی قرار خواهند گرفت.

Model Driven Engineering (MDE) for Android Security

Dr. Hayyan Slman Hasan
Dept. Computer and automatic control engineering
Faculty of Mechanical and Electrical Engineering
Albaath university Syrian Arab Republic

Android OS is the most used operation system in the mobile marketplace, and the number of Android users is growing tremendously. As a result, the number of risks that threatens Android users is increasing and cannot be ignored. These risks are coming from the vulnerable applications that have been uploaded every day into google play or into any other online store. Another source of risks is Android malware which have become real and growing risks to Android users. Traditional approaches tried to handle the various Android risks. These approaches used static or dynamic analyses to detect the vulnerable points or malicious payloads in the Android application code. However, these approaches have many shortcomes in the case of scalability, reusability or integration. Another shortcome is the need to provide suitable and easy way to involve the analyzer in the analysis process. In this speech we highlight the impact of using Model Driven Engineering (MDE) approach on various Android security aspects. Using MDE provides the ability to extract the required information from the Android applications and integrate them into one model. Using models provides high level representations of the extracted information from Android applications and provides the ability to involve the analyzer in the analysis processes to achieve better results with less time and efforts.

Attribute-based remote data auditing and user authentication for cloud storage systems

Dr. Mohammad Ali

Assistant Professor of the Department of Mathematics and computer science, Amirkabir University of Technology

Remote data auditing (RDA) protocol enables a cloud server to persuade an auditor that it is storing a data file honestly. Unlike digital signature (DS) schemes, in RDA protocols, the auditor can carry out the auditing procedure without having the entire data file. Therefore, RDA protocols seem to be attractive alternatives to DSs as they can effectively reduce bandwidth consumption. However, existing RDA protocols do not provide adequately powerful tools for user authentication. In this paper, we put forward a novel attribute-based remote data auditing and user authentication scheme. In our proposed scheme, without having a data file outsourced to a cloud server, an auditor can check its integrity and authenticity of its issuer. Indeed, through a challenge-response protocol, the auditor can check whether 1) the cloud server has changed the content of the data file or not; 2) the data owner possesses a specific attribute set or not. We present the formal security definition and prove the security of our scheme under the hardness assumption of the bilinear Diffie-Hellman (BDH) problem. Our experimental results indicate that our scheme is efficient and applicable.

Secure and Practical Search over Dynamic Encrypted Datasets

Dr. Javad Gharreh Chamani

Hong Kong University of Science and Technology

We study the problem of dynamic symmetric searchable encryption (DSE) where one or more data owners store their encrypted data on an untrusted remote server, and wishes to efficiently search on it. We specifically focus on dynamic schemes with efficient support for data insertion, deletion, and modification. In particular, it is crucial to minimize the information revealed to the server as a result of not only search queries, but also updates. We present schemes that achieve the two strongest privacy notions for DSE: forward and backward privacy. The first makes it hard for the server to link an update operation with previous queries, while the second limits what the server can learn about entries that were deleted from the database, from queries that happen after the deletion. Our results improve the state-of-the-art in this area across multiple aspects, as we describe next.

First, we introduce novel constructions that are extremely lightweight while also achieving stronger backward privacy notions than existing ones. Our first scheme Mitra achieves Type-II backward privacy and is, to the best of our knowledge, the fastest and easiest to implement DSE scheme to date. Our second scheme Orion achieves even stronger Type-I backward privacy and is the only implemented scheme in the literature of its kind. Finally, our third scheme Horus improves the second one by reducing the number of communication roundtrips during queries but reveals slightly more information to the server (Type-III backward privacy). Second, we explicitly focus on DSE with efficient (optimal/quasi-optimal) search in the presence of deletions, i.e., constructions where the search overhead is within a polylogarithmic multiplicative factor of the theoretical optimal (i.e., the result size of a search). This property is achieved by our schemes Orion and Horus but we next aim at much more practically efficient schemes. Towards that end, we first propose OSSE, the first DSE scheme that can achieve asymptotically optimal search time, improving the previous state-of-the-art by a multiplicative logarithmic factor. We also propose an alternative scheme LLSE, that achieves a sublogarithmic search overhead compared to the optimal. While this is slightly worse than the previous scheme, it still outperforms all prior works, while also achieving faster deletions and smaller server storage. Finally, we prototype all our schemes and open-source their code. We evaluate their performance for different datasets and queryloads, experimentally compare them with prior state-of-the-art DSE schemes, and report the results.

چکیده مقالات ارائه شده در کنفرانس

تحلیل امنیتی یک پروتکل تبادل کلید و احراز اصالت گمنام در شبکه حسگرهای پوششی

صبا مرندی، فرخ لقا معظمی‌گودرزی (پژوهشکده فضای مجازی دانشگاه شهید بهشتی)

در زمینه‌ی پزشکی شبکه حسگرهای پوششی شبکه‌ی حسگرهایی است که روی بدن یا داخل بدن انسان‌ها قرار می‌گیرند و سرویس‌های آسان و بهینه ای را برای بیماران و پرسنل پزشکی فراهم می‌کنند. اطلاعات فیزیولوژیکی بیماران بسیار حساس و شخصی می‌باشد، بنابراین تبادل آنها از طریق کانال ناامن نیازمند گمنامی، عدم وابستگی و حفظ حریم خصوصی می‌باشد. علاوه بر این، شبکه حسگرهای پوششی زیر مجموعه‌ای از شبکه اینترنت اشیا است که به دلیل داشتن منابع محدود نیازمند پروتکل‌های سبکی هستند که اصالت، تمامیت و صحت اطلاعات آنها را تضمین کنند، بنابراین پروتکل‌های زیادی برای تامین امنیت این بستر توسط محققان ارائه شده‌است که برخی از آنها دارای مشکلات امنیتی هستند. این موضوع باعث به وجود آمدن زمینه تحقیقاتی گسترده‌ای روی این مساله‌ها شده‌است. اخیرا آنکور گوپتا و همکارانش پروتکل احراز هویت متقابل و تبادل کلید سبکی را ارائه داده‌اند و امن بودن آن را در برابر حملات شناخته شده اثبات کرده‌اند. ما در این مقاله نشان می‌دهیم که پروتکل پیشنهادی آنها در برابر حمله جعل هویت گره حسگر دارای ضعف می‌باشد و لذا امنیت مورد نیاز این بستر را فراهم نمی‌کند و به ارائه طرحی برای جلوگیری از این امر می‌پردازیم.

شبکه حسگرهای پوششی، احراز هویت متقابل، تبادل کلید، حمله‌ی جعل هویت گره حسگر

روش اجماع با امنیت بالا و بار مخابراتی کم

علیرضا هدیه‌لو، جواد مهاجری، محمدرضا عارف (دانشگاه صنعتی شریف)

برای ایجاد هماهنگی بین گره‌های شبکه و افزایش مقاومت سامانه‌های توزیع شده در برابر خطا از پروتکل‌های اجماع استفاده می‌شود. در این مقاله، یک روش اجماع همگام جدید معرفی می‌شود. روش پیشنهادی، نسخه‌ای بهبود یافته از پروتکل Abraham است که در آن از امضای تجمیعی برای کاهش بار مخابراتی استفاده کرده‌ایم. در پروتکل Abraham بار مخابراتی و بار محاسباتی پروتکل، به ترتیب از مرتبه‌ی $\boldsymbol{O(n^3 s_s)}$ و $\boldsymbol{O(n^3)}$ است در حالی که در پروتکل پیشنهادی بار مخابراتی و بار محاسباتی به ترتیب از مرتبه‌ی $\boldsymbol{O(m_a n^2[\log k_t] + m_a n s_s)}$ و $\boldsymbol{O(m_a n^2)}$ است، که در آن $\boldsymbol{n}$ تعداد گره‌های شبکه، $\boldsymbol{s_s}$ اندازه‌ی یک امضای دیجیتال، $\boldsymbol{k_t}$ حداکثر تعداد تکرارهای پروتکل و $\boldsymbol{m_a}$ یک پارامتر امنیتی است که می‌تواند بسیار کوچکتر از $\boldsymbol{n}$ باشد. بنابراین در شبکه‌هایی با تعداد گره زیاد، کاهش بار مخابراتی و بار محاسباتی محسوس خواهد بود. همچنین در این پروتکل برای مقاومت در برابر $\boldsymbol{f}$ گره‌ی بیزانسی به حداقل $\boldsymbol{n = 2f + 1}$ گره نیاز داریم و با احتمال حداقل $\boldsymbol{1 - \frac{1}{2^{m_a}}}$ روند اجماع به درستی انجام می‌شود.

اجماع، شبکه‌ی همگام، گره بیزانسی، امضای تجمیعی

پروتکل چندکاربره گفت‌وگوی کوانتومی با قابلیت گسترش تعداد کاربران در زمان اجرا

علی خزائی، حسین همائی، منیره هوشمند(دانشگاه تربیت مدرس، دانشگاه تربیت مدرس، دانشگاه بین‌المللی امام رضا)

گفت‌وگوی کوانتومی به نوعی از ارتباطات کوانتومی گفته می‌شود که در آن کاربران می‌توانند به صورت همزمان برای یکدگیر پیام ارسال کنند. اولین نمونه‌های پروتکل‌های گفت‌وگوی کوانتومی با مشکلات امنیتی نظیر نشت اطلاعات و آسیب‌پذیری‌هایی همچون دریافت و ارسال مجدد روبرو بودند. از این رو، پروتکل‌های متعددی ارائه شده که سعی در برطرف نمودن این نواقص دارند. با وجود این پیشرفت‌ها، گفت‌وگوهای کوانتومی همچنان با چالش‌هایی روبرو هستند. در حال حاضر، محدود بودن تعداد شرکت‌کنندگان و عدم امکان گسترش کاربران در زمان گفت‌وگو از جمله مهم‌ترین چالش‌های این نوع پروتکل‌ها محسوب می‌شود. در این پژوهش یک پروتکل گفت‌وگوی کوانتومی چندکاربره طراحی کرده‌ایم که چالش‌های فوق را برطرف نماید. پروتکل پیشنهادی حالت تعمیم یافته گفت‌وگوی کوانتومی است که در آن هر کاربر می‌تواند به صورت همزمان با کاربران دیگر ارتباط برقرار کند. تعداد کاربران شرکت‌کننده محدود نیست و به صورت پویا (یعنی بدون نیاز به راه‌اندازی مجدد پروتکل) نیز قابل تغییر است. بنابراین، در زمان اجرای پروتکل، یک کاربر می‌تواند گفت‌وگو را ترک کند و یا کاربری جدید می‌تواند به آن ملحق شود. ارتباط میان کاربران از طریق یک سرور نیمه‌صادق مرکزی برقرار می‌شود. بررسی‌های انجام شده نشان می‌دهد که پروتکل پیشنهادی نسبت به نشت اطلاعات مقاوم است. یعنی، هیچ کاربر غیرمجازی (حتی سرور مرکزی) نمی‌تواند به داده‌های خام مبادله شده میان افراد دسترسی پیدا کند.

پروتکل‌های امنیتی، امنیت کوانتوم، گفت‌وگوی کوانتومی چند کاربره

طراحی و پیاده سازی دو نمونه آزمایشگاهی سامانه هوشمند شناساگر ترافیک رمز شده VoIP اسکایپ و ابزار گریز lantern به روش یادگیری عمیق

محمود سعیدی، نسرین تاج، آزاده بامداد مقدم (پژوهشگاه ارتباطات و فناوری اطلاعات)

روش پیشنهادی جهت پیاده‌سازی سامانه های شناساگر ترافیک رمزی و ابزار گریز دراین مقاله، روش مبتنی بر یادگیری عمیق بوده که با توجه به اهمیت استخراج بهینه و خودکار ویژگی‌ها از مجموعه دادگان ورودی، از شبکه‌ی کدگذار خودکار در فاز استخراج ویژگی استفاده شده است. سپس، خروجی لایه‌ی پنهان میانی این شبکه به یک شبکه عصبی پیچشی عمیق اعمال می‌گردد. شبکه‌های عصبی پیچشی عمیق با توجه به در نظر گرفتن ارتباطات مکانی میان ویژگی‌ها، می‌توانند در ارتقاء عملکرد سامانه نقش موثری ایفا نمایند. در نهایت، خروجی شبکه عصبی پیچشی عمیق نیز به منظور انجام فرایند طبقه‌بندی، به دو لایه تمام متصل اعمال می‌گردد. به گونه‌ای که تعداد نورون‌ها در لایه تمام متصل دوم، برابر با تعداد طبقه‌های مورد انتظار از سامانه خواهد بود. در قسمت اول این مقاله ابتدا به مشخصات سامانه‌های پیشنهادی پیاده‌سازی شناساگر ترافیک رمزی و ابزار گریز از نظرمعماری عملیاتی و ویژگی ها اشاره خواهد شد. سپس به اختصار مشخصات شبکه‌های به کار رفته در پیاده‌سازی سامانه، و شیوه‌ی یکپارچه‌سازی آن‌ها جهت تشکیل سامانه‌ی شناساگر نهایی بیان می‌گردد. پس از آن، مرحله آموزشی سامانه و شیوه‌ی اجرای آن معرفی شده و در انتها، چگونگی تنظیم پارامترهای مدل و ساز وکارهای به کار رفته جهت بهبود عملکرد کلی سامانه و نتایج ارزیابی عملکرد آن ارائه خواهد شد.

معماری پیشنهادی سامانه هوشمند شناساگر ترافیک رمزی و ابزار گریز، یادگیری عمیق، شبکه‌ی کدگذار خودکار پیشنهادی، شبکه‌های عصبی پیچشی عمیق، ارزیابی تست‌های عملکرد سامانه

مدل‌سازی سطح توانایی مهاجم با تمرکز بر حملات تزریق روی برنامه‌های کاربردی وب

سارا مقیمی، محمدعلی هادوی (دانشگاه صنعتی مالک اشتر)

چگونگی سوءاستفاده از آسیب‌پذیری‌ها و اثرات آن در کنار الگوهای شناخته شده، متأثر از توانمندی مهاجم‌ها می‌باشد. هرچه مهاجم توانمندتر باشد، مخاطره تهدیدها و آسیب‌پذیری‌ها افزایش پیدا می‌کند. بنابراین، تحلیل و ارزیابی امنیتی سامانه‌ها وابسته به توانمندی مهاجم است. علاوه بر این، اطلاع از سطح توانمندی مهاجم ارتباط مستقیمی با هزینه مورد نیاز برای امنیت و بکارگیری کنترل‌ها و اقدامات امنیتی متناسب با توان مهاجم دارد. بر این اساس، این مقاله مدل‌سازی توانمندی مهاجم را هدف‌گذاری کرده است. ما در این مقاله با تکیه بر تزریق پیلودهایی که مهاجم برای سوءاستفاده از آسیب‌پذیری‌های تزریق استفاده می‌کند، توانمندی مهاجم را با سه‌گانه‌ی ⟨Type, Technique, Entry_Point⟩ مدل می‌کنیم. مؤلفه‌ی Type بیانگر نوع تزریق می‌باشد که شامل مجموعه‌ای شناخته‌شده از انواع حمله تزریق است که مهاجم در طول حمله به کار برده است. مؤلفه‌ی Technique بیانگر تکنیک‌هایی است که مهاجم در طول حمله به کار برده است، و مؤلفه‌ی Entry_Point نشان‌دهنده‌ی مجموعه‌ای از نقاط شناخته‌شده تزریق پیلود است. از این مدل هم برای سطح‌بندی و مقایسه توانمندی مهاجم و هم برای سطح‌بندی امنیت یک سامانه با توجه به سطح توان مهاجمی که می‌تواند امنیت آن‌را به خطر بیاندازد استفاده می‌شود. نتایج ارزیابیِ تجربیِ انجام شده نشان می‌دهد که مدل ارائه شده برای تعیینِ سطحِ توانمندیِ مهاجم قابل استفاده است. با این‌که مدل ارائه شده با تمرکز بر حملات تزریق SQL است، اما قابل توسعه به بسیاری از حملات دیگر می‌باشد.

سطح توان مهاجم، تزریق SQL، نوع تزریق، تکنیک تزریق، نقطه‌ی ورود تزریق، امنیت سامانه.

تشخیص پولشویی الکترونیکی در تراکنش‌های تامین‌کنندگان خدمات پرداخت

علی نظری، بابک صادقیان (دانشگاه صنعتی امیر کبیر)

مجرمان پولشویی در پوشش کسب و کارهای قانونی با سوء استفاده از خدمات شرکت‌های ارائه کننده خدمات پرداخت (PSP) اقدام به پولشویی الکترونیکی می‌نمایند. به منظور فورنسیک پولشویی در تراکنش‌های مالی شرکت‌های PSP، روشی توسط حجتی و همکاران ارائه شده است که از طریق تشخیص تراکنش‌های خارج از الگوی صنف فروشندگان و با روش تحلیل درون گروهی انجام می‌گردد. بررسی‌های ما نشان می‌دهد که استفاده از روش مطرح شده در تشخیص تراکنش‌های خارج از الگوی صنف، نرخ اعلام‌های مثبت نادرست حدودا ٪۱۳ را در تشخیص پولشویی نتیجه می‌دهد. ما در این مقاله با اصلاح راه‌حل مطرح شده، نرخ اعلام‌های مثبت نادرست را ٪۱۲ درصد کاهش داده و به کمتر از ٪۱ رساندیم. برای این منظور در تحلیل درون گروهی، حجم تراکنش‌های مالی فروشندگان را در کنار حجم بازدیدکنندگان وب‌سایت‌های آنها مورد تحلیل قرار دادیم و بر اساس تعداد بازدیدکنندگان وب‌سایت‌های صنف مربوطه، حجم تراکنش‌های هر فروشنده را تخمین زدیم و حجم فروش بیش از تخمین را نامتعارف در نظر گرفتیم. با استفاده از ماشین بولتزمن محدود دقت تشخیص تراکنش‌های خارج از الگوی صنف را ارتقاء دادیم و با کمک استدلال مبتنی بر مورد، نرخ اعلام‌های منفی نادرست را کاهش دادیم. سیستم پیشنهادی ما، از یک پنجره لغزان چهارهفته‌ای برای تشخیص برخط پولشویی استفاده می‌نماید. نتایج ارزیابی‌ها نشان داد که راه‌حل پیشنهادی ما دارای دقت تشخیص ٪۹۹ می‌باشد.

پولشویی الکترونیکی، پول غیر قانونی، تراکنش نامتعارف، ماشین بولتزمن محدود، استدلال مبتنی بر مورد، پی‌جویی جرم.

نهان‌نگاری تصویر مبتنی بر حوزه موجک با ایده جاسازی در نواحی با تغییرات زیاد زیرباندهای فرکانس بالا

وجیهه ثابتی، معصومه سبحانی سوادرودباری(دانشگاه الزهرا)

نهان‌نگاری، علم و هنر پنهان‌سازی وجود ارتباط است. در نهان‌نگاری با پنهان کردن اطلاعات در یک رسانه دیجیتال، وجود ارتباط از دید فرد متخاصم مخفی می‌ماند. ایده روش‌های تطبیقی در حوزه‌ی مکان، جاسازی بیشتر در نواحی لبه تصویر است. در این روش‌ها، نواحی‌ای از تصویر که تغییرات بیشتری دارند، در اولویت جاسازی قرار دارند. از طرفِ دیگر روش‌های حوزه تبدیل موجک، برای مطابقت با سیستم بینایی انسان، جاسازی را در زیرباندهای فرکانس بالا انجام می‌دهند. ایده پیشنهادی در این مقاله، جاسازی با اولویت بیشتر در نواحی‌ای از زیرباندهای فرکانس بالای حاصل از تبدیل موجک است که تغییرات زیادی دارند. ابتدا با توجه به طول داده، یک حد آستانه تعیین می‌شود که براساس آن نواحی مناسب جاسازی در هر زیرباندِ فرکانس بالا شناسایی می‌شود و سپس فرآیند جاسازی در آن انجام می‌شود. این فرآیند به نحوی است که گیرنده نیز می‌تواند با تکرار آن، داده را به صورت کامل استخراج کند. نتایج پیاده‌سازی نشان می‌دهد در روش پیشنهادی استفاده از تبدیل موجک عدد صحیح نسبت به تبدیل موجک گسسته موفقیت بیشتری را به همراه دارد. کیفیت تصویر خروجی روش پیشنهادی، نسبت به روش‌های حوزه تبدیل مورد مقایسه، بالاتر و امنیت آن بیشتر است.

نهان‌نگاری، نهان‌کاوی، تبدیل موجک گسسته، تبدیل موجک عدد صحیح

Towards a Formal Approach for Detection of Vulnerabilities in the Android Permissions System

Amirhosein Sayyadabdi, Behrouz Tork Ladani, Bahman Zamani (University of Isfahan)

Android is a widely used operating system that employs a permission-based access control model. The Android Permissions System (APS) is responsible for mediating application resource requests. APS is a critical component of the Android security mechanism; hence, a failure in the design of APS can potentially lead to vulnerabilities that grant unauthorized access to resources by malicious applications. In this paper, we present a formal approach for modeling and verifying the security properties of APS. We demonstrate the usability of the proposed approach by showcasing the detection of a well-known vulnerability found in Android's custom permissions.

Android security, formal methods, verification

On the Suitability of Improved TrustChain for Smartphones

Seyed Salar Ghazi Haleh Amintoosi, Sahar Pilevar Moakhar (Ferdowsi University of Mashhad)

In recent years, Blockchain technology has been used in many fields, including IoT and Smartphones. Since most of these devices are battery constrained and have low processing capabilities, conventional Blockchains are not suitable for these types of systems. In this field, critical challenges that need to be addressed are providing security for transactions and power consumption. An available solution to meet the mentioned challenges is TrustChain. Unlike conventional Blockchains, TrustChain does not have a single global chain. Instead, each node is responsible for building and maintaining its own local chain. With all the benefits, TrustChain is vulnerable to the Whitewashing attack and suffers from client vulnerability issues. Moreover, once a fatal error occurs, the recovery time of each TrustChain node is considerably high. In this paper, we propose a solution to address the above-mentioned attacks by the implementation of an authentication system with MongoDB on top of TrustChain. Moreover, we connected TrustChain to the distributed cloud storage, with the aim of significantly reducing the recovery time of nodes in fatal errors (up to 80%). Finally, we evaluate improved TrustChain with the PoW-based smartphone-oriented Blockchains from two aspects of security and power consumption, and prove that improved TrustChain does not significantly affect the lifetime of the smartphone battery, its power consumption is less than mentioned Blockchains, and it is more secure than these systems against main attacks too.

Distributed Systems, Blockchain, TrustChain, Distributed Cloud, Whitewashing, Battery consumption

Android Malware Detection using One-Class Graph Neural Networks

Fatemeh Deldar, Mahdi Abadi, Mohammad Ebrahimifard (Tarbiat Modares University)

With the widespread use of Android smartphones, the Android platform has become an attractive target for cybersecurity attackers and malware authors. Meanwhile, the growing emergence of zero-day malware has long been a major concern for cybersecurity researchers. This is because malware that has not been seen before often exhibits new or unknown behaviors, and there is no documented defense against it. In recent years, deep learning has become the dominant machine learning technique for malware detection and could achieve outstanding achievements. Currently, most deep malware detection techniques are supervised in nature and require training on large datasets of benign and malicious samples. However, supervised techniques usually do not perform well against zero-day malware. Semi-supervised and unsupervised deep malware detection techniques have more potential to detect previously unseen malware. In this paper, we present MalGAE, a novel end-to-end deep malware detection technique that leverages one-class graph neural networks to detect Android malware in a semi-supervised manner. MalGAE represents each Android application with an attributed function call graph (AFCG) to benefit the ability of graphs to model complex relationships between data. It builds a deep one-class classifier by training a stacked graph autoencoder with graph convolutional layers on benign AFCGs. Experimental results show that MalGAE can achieve good detection performance in terms of different evaluation measures.

Android application, Attributed function call graph, Graph convolutional layer, Malware detection, One-class classification, Semi-supervised deep learning, Stacked graph autoencoder

Lightweight Identification of Android malware with knowledge distillation and deep learning approach

Somayeh Mozafari, Amir Jalaly Bidgoly (University of Qom)

Today, with the advancement of science and technology, the use of smartphones has become very common, and the Android operating system has been able to gain lots of popularity in the meantime. However, these devices face many security challenges, including malware. Malware may cause many problems in both the security and privacy of users. So far, the state-of-the-art method in malware detection is based on deep learning, however, this approach requires a lot of computing resources and leads to high battery usage, which is unacceptable in smartphone devices. This paper proposes the knowledge distillation approach for lightening android malware detection. To this end, first, a heavy model is taught and then with the knowledge distillation approach, its knowledge is transferred to a light model called student. To simplify the learning process, soft labels are used here. The resulting model, although slightly less accurate in identification, has a much smaller size than the heavier model. Moreover, ensemble learning was proposed to recover the dropped accuracy. We have tested the proposed approach on CISC datasets including dynamic and static features, and the results show that the proposed method is not only able to lighten the model up to 99%, but also maintain the accuracy of the lightened model to the extent of the heavy model.

Android, malware detection, deep learning, knowledge distillation, lightening, ensemble learning

Attribute-Based Encryption with efficient Attribute Revocation, Decryption Outsourcing and Multi-Keyword Searching in Cloud Storage

Sajjad palanki, Alireza Shafieinejad (Tarbiat Modares University)

Reliable access control is a major challenge of cloud storage services. This paper presents a cloud-based file sharing architecture with ciphertext-policy attribute-based encryption (CP-ABE) access control mechanism. In CP-ABE, the data owner can specify the ciphertext access structure, and if the user key satisfies this access structure, the user can decrypt the ciphertext. The trusted authority embeds the private key of each attribute in a so-called attribute access polynomial and stores its coefficients publicly on the cloud. By means of the access polynomial, each authorized user will be able to retrieve the private key of the attribute by using her/his owned pre-shard key. In contrast, the data owner encrypts the file with a random selected key, namely cipher-key. The data owner encrypts the cipher-key by CP-ABE scheme with the desired policies. Further, the data owner can create a different polynomial called query access polynomial for multi-keyword searching. Finally, the data owner places the encrypted file along the encrypted cipher-key and query access polynomial in the cloud. The proposed scheme supports fast attribute revocation by means of updating the corresponding access polynomial and re-encrypting the affected cipher-keys by the cloud server. Moreover, most of the calculations at the decryption and searching phases are outsourced to the cloud server, thereby allowing the lightweight nodes with limited resources to act as data user. Our analysis shows that the proposed scheme is both secure and efficient.

Cloud Storage, Attribute-Based Encryption, Attribute Revocation, Multi-Keyword Searching

Enhanced Differential Fault Attack on SKINNY: From Theory to Practical Attack

Navid Vafaei, Maryam Porkar, Hamed Ramzanipour, Nasour Bagheri (Shahid Rajaee Teacher Training University, Institute for Research in Fundamental Sciences)

SKINNY is a lightweight tweakable block cipher that for the first time introduced in CRYPTO 2016. SKINNY is considered in two block sizes: 64 bits and 128 bits, as well as three TWEAK versions. In the beginning, this paper reflects our findings that improve the effectiveness of DFA analysis on SKINNY, then accomplishes the hardware implementation of this attack on SKINNY. Assuming that TWEAK is fixed, we first present the Enhanced DFA on SKINNY64-64 and SKINNY128-128. In order to retrieve the master key with the minimum number of faults, this approach depends on fault propagation in intermediate rounds. In our latest evaluations we can retrieve the master key with 2 and 3 faults in SKINNY64-64 and SKINNY128-128 respectively. This result should be compared with 3 and 4 faults for 64-bit and 128-bit versions respectively, in the models presented in the former work. Using the glitch model as well as a set of affordable hardware equipment, we injected faults into various rounds of the SKINNY algorithm in the implementation phase. More accurately, we can inject a single nibble fault into a particular round by determining the precise timing of the execution sub-function.

Differential fault attack, SKINNY, Glitch frequency, Nibble fault injection

Light-Weight Privacy-Preserving Data Aggregation Protocols in Smart Grid Metering Networks

Afshin Karampour, Maede Ashouri-Talouki, Behrouz Tork Ladani (University of Isfahan)

Smart grids using information technology (IT) and communication networks controls smart home appliances to reduce the costs and increase the reliability and transparency. Preserving the privacy of the user data is one of the biggest challenges in smart grid researches; by disclosing the user-related data, an internal or external adversary can understand habits and behavior of the users. A solution to address this challenge is however, data aggregation mechanism in which the aggregated data of all of the users in a residential area. The security and efficiency of data aggregation approach are important. The drawback of the pervious works is leaking fine-grained user data, or the high computation and communication overhead. In this paper, we present an efficient privacy-preserving data-aggregation protocol, called PPDA, based on the Elliptic Curve Cryptography (ECC) and Anonymous Veto network protocol. The PPDA protocol aggregates metering data in an efficient and secure manner, so that it becomes applicable for resource-constraint metering devices. We also present an improved multi-cycle proposal of PPDA, called MC-PPDA. In the improved approach, the system initialization step runs only at the first cycle of the protocol which increases the efficiency of the protocol. Evaluation results show that the proposed approaches preserve the privacy of the fine-grained user data against an internal and external adversary; the improved multi-cycle approach is also secure against collusion. Compared to the previous approaches, the proposed approaches incur less computation and communication overhead.

Smart grid, Smart Meter, Data aggregation, privacy preserving, Elliptic curve cryptography, AV-net mask

Practical Differential Fault Analysis on CRAFT, a Lightweight Block Cipher

Hamed Ramzanipour, Navid Vafaei, Nasour Bagheri (Shahid Rajaee Teacher Training University)

Differential fault analysis, a kind of active non-invasive attacks, is an effective way of analyzing cryptographic primitives that have lately earned more attention. In this study, we apply this attack on CRAFT, a recently proposed lightweight tweakable block cipher, supported by simulation and experimental results. This cipher accepts a 64-bit Tweak, a 64-bit plaintext, and a 128-bit key to produce a 64-bit ciphertext. Although the algorithm is based on AES, its better characteristics in terms of implementing and counteracting faults have satisfied the criteria of many security protocols that require a lightweight yet secure implementation. The fault detection power of this algorithm, which resists fault injection by implementing the countermeasures section, is one of these characteristics. We assume that the target implementation of CRAFT does not use countermeasures in this paper. The considered fault model in the initial phase of this paper is a single bit but random nibble injected fault, where we first present the fault injection attack as a simulation and then report on how to retrieve the round sub-keys. Next, we use frequency glitch as a fault injection technique in the experimental phase. This part aims to produce a single fault at a nibble in a specific round of the CRAFT. Following our statistical analysis, and according to the simulation findings, we can reduce the key space to 30.28 and 24.37 bits, respectively, by using 4 and 5 faults. The location of random faults injected by the hardware mechanism is also identified in the experimental section.

Differential fault analysis - CRAFT - Implementation of fault attack - Glitch frequency

One-Shot Achievable Secrecy Rate Regions for Quantum Interference Wiretap Channel

Hadi Aghaee, Bahareh Akhbari (K. N. Toosi University of Technology)

In this paper, we want to derive achievable secrecy rate regions for quantum interference channel with classical inputs under one-shot setting. The main idea to this end is to use the combination of superposition and rate splitting for encoding scheme and constructing a decoding scheme based on simultaneous decoding.

Quantum Channel; Mutual Information; Secrecy Capacity; Multiple Access Channel

Mutual Lightweight PUF-Based Authentication Scheme Using Random Key Management Mechanism for Resource-Constrained IoT Devices

Amir Ashtari, Ahmad Shabani, Bijan Alizadeh (University of Tehran)

This paper presents a novel RF-PUF based authentication scheme, called RKM-PUF which takes advantage of a dynamic random key generation that depends upon both communication parties in the network to detect intrusion attacks. Unlike the existing authentication schemes, our proposed approach takes the physical characteristics of both involved parties into account to generate the secret key, resulting in securely mutual authentication of both nodes in a wireless network. The experimental results of the proposed authentication scheme show that the RKM-PUF can reach up to 99% in identification accuracy.

IoT, network security, radio frequency identification, physical layer security

SecureKV: Secure Searchable Outsourcing of Key-Value Databases to the Public Cloud

Maryam Saeedi Sadr, Mohammad Ali Hadavi, Sayed Gholam Hassan Tabatabaei (Malek Ashtar University of Technology)

The use of NoSQL data and its storage in the Cloud is growing rapidly. Due to the accumulation of data in the Cloud, data security against untrusted service providers as well as external attackers becomes a more serious problem. Over the past few years, there are some efforts on secure outsourcing of NoSQL data, especially column-based and document-based models. However, practical solutions for secure outsourcing of key-value databases have not been identified. This paper attempts to introduce SecureKV as a secure method for outsourcing key-value databases. This method employs a multi-Cloud storage scenario to preserve outsourced data confidentiality. Besides security issues, the proposed method supports executing major key-value queries directly on outsourced data. A prototype on the Redis database management system has been implemented to show the efficiency and effectiveness of the proposed method. The results imply that, besides security issues, it is efficient and scalable enough in executing key-value specific queries.

NoSQL; key-value database; security; confidentiality; data outsourcing; query processing; multi-Cloud

Secure and Low-area Implementation of the AES Using FPGA

MuhamadAli HajiSoltani, Raziyeh Salarifard, Hadi Soleimany (Shahid Beheshti University)

Masking techniques are used to protect hardware implementation of cryptographic algorithms against side-channel attacks. Reconfigurable hardware, such as FPGA, is an ideal target for the secure implementation of cryptographic algorithms. Due to the restricted resources available to the reconfigurable hardware, efficient secure implementation is crucial in an FPGA. In this paper, a two-share threshold technique for the implementation of AES is proposed. In continuation of the work presented by Shahmirzadi et al. at CHES 2021, we employ built-in Block RAMs (BRAMs) to store component functions. Storing several component functions in a single BRAM may jeopardize the security of the implementation. In this paper, we describe a sophisticated method for storing two separate component functions on a single BRAM in order to reduce area complexity while retaining security. Out design is well suited for FPGAs, which support both encryption and decryption. Our synthesis results demonstrate that the number of BRAMs used is reduced by 50% without affecting the time or area complexities.

Side-Channel Attacks, FPGA, Threshold Implementation, AES

An Electronic Voting Scheme Based on Blockchain Technology and Zero-Knowledge Proofs

Sepehr Damavandi, Sadegh Dorri Nogoorani (Tarbiat Modares University)

Voting is a fundamental mechanism used by many human societies, organizations and nations to make collective decisions. There has been tremendous effort on making this mechanism more fair, error-free and secure. Electronic voting aims to be a solution to some deficiencies of existing paper-based voting systems. While there have been excellent technical and practical advances in e-voting, and some of them were great in defining the needs and musts of an ideal voting system, there are also severe critics to existing solutions mostly related to end-to-end verifiability and software-independence. In this paper, we use blockchain and zero-knowledge proofs for a secure e-voting scheme that satisfies these requirements while preserving the privacy of the voters. We also evaluate our scheme from security and performance aspects.

Applied Cryptography, Blockchain Voting, Blockchain Privacy, Electronic Voting, ZK-SNARKs

برنامه کارگاه‌ها

روز	۹-۱۱	۱۱-۱۳	۱۲_۱۳	۱۳_۱۴	۱۵-۱۷	۱۷-۱۹
دوشنبه ۱۴۰۱/۶/۷	WS-A1		-	_	WS-A2	
سه شنبه ۱۴۰۱/۶/۸	WS-B1 WS-B2			_	WS-B3	

نام کارگاه	کد کارگاه
مراحل رسیدگی به رخدادهای سایبری بهمراه سناریوی تحلیل بدافزار میلاد افشار نادری	**WS-A1**
نسل دوم تا نسل پنجم تلفن همراه، چالش‌ها و تهدیدات امنیتی حمید ریاضی، مصطفی درودیان، امیرحسین پورشمس، همراه اول	**WS-A2**
پروتکل‌های اجماع بلاکچین رسول رمضانیان، هیات دانشگاه فردوسی مشهد، دانشکده علوم ریاضی، راهبر بتای بلاکچین امن افزار- امن افزار گسترشریف	**WS-B1**
مخاطرات و ریسک‌های امنیتی در شبکه 5G حسین احمدی، کارشناسی ارشد مهندسی فناوری اطلاعات – شبکه های کامپوتری- شرکت امن افزار گستر شریف	**WS-B2**
آشنایی عملی با DevSecOps و راه اندازی یک نمونه pipeline آن در AWS علیرضا نوروزی، هیات علمی دانشکده فنی دانشگاه صدا و سیما، مشاور مرکز تحقیق و توسعه همراه اول مهسا لمیعیان، واحد تحقیق و توسعه همراه اول	**WS-B3**

کارگاه مراحل رسیدگی به رخدادهای سایبری بهمراه سناریوی تحلیل بدافزار

مهندس میلاد افشار نادری

لینک کارگاه: https://www.skyroom.online/ch/uog/iscisc_room1

چکیده کارگاه

بدون توجه به اندازه سازمان یا شرکت و یا نوع فعالیت‌های سازمان، دیر یا زود رخدادی در آن اتفاق خواهد افتاد. هیچ شکی در خصوص احتمال وقوع رخداد در سازمان‌ها وجود ندارد تنها سوالی که در این خصوص مطرح می باشد این است که چه زمانی این رخداد به وقوع خواهد پیوست؟ بنابراین می‌بایست سازمان برای آن زمان آماده بوده و طرحی برای مقابله با رخداد و کاهش خسارات ناشی از آن داشته باشد. در صورت عدم وجود چنین آمادگی در سازمان، در هنگام بروز رخداد خسارات جبران‌ناپذیر به آن سازمان وارد خواهد شد .از این رو متدهایی در یک تیم Incident Response یا تیمی مثل Forensic معمولاً مبتنی بر ۷ گام یک طرح Incident Response هستند که در این کارگاه به توضیح هر یک از این گام ها خواهیم پرداخت. این گام ها خود شامل "چرخه حیات پاسخدهی به رخداد" که از روی NIST مشخص شده در ۴ مرحله "آماده سازی"، "شناسایی و تحلیل"، "محدود سازی، کنترل و بازیابی" و "فعالیت های پس از رخداد" با یکدیگر در ارتباط هستند .در انتها بعنوان یک سناریو عملیاتی، رسیدگی به یک رخداد (تحلیل بدافزار) نمایش داده خواهد شد.

کارگاه نسل دوم تا نسل پنجم تلفن همراه، چالش‌ها و تهدیدات امنیتی

مهندس امیرحسین پورشمس، همراه اول

لینک کارگاه: https://www.skyroom.online/ch/uog/iscisc_room1

چکیده کارگاه

توسعه در دنیایی که ارتباطات موبایلی و شبکه‌های دیجیتال به بخشی از زندگی روزمره ما تبدیل شده است، مسائل مربوط به حریم خصوصی، حفاظت از داده ها و امنیت سایبری ضروری است. این موضوعات بخشی از طیف گسترده ای از موضوعاتی هستند که در سال های اخیر به آنها پرداخته شده است. از طرف دیگر، برای دستیابی به اهداف تجاری، اپراتورهای تلفن همراه نیز باید امنیت سایبری را به عنوان بخش مبنایی در نظر بگیرند. برای دستیابی به این هدف، دانش کافی در مورد جزئیات معماری سرویس ها، تهدیدات و آسیب پذیری های مربوطه لازم می‌باشد. در این کارگاه ابتدا مروری بر نسل‌های مختلف شبکه های تلفن همراه ارائه و سپس به تهدیدات، آسیب پذیری ها، خطرات و همچنین راهکارهایی که می تواند بر خدمات اپراتور و کسب و کار آن تاثیر گذار باشد به بحث و گفت و گو پرداخته خواهد شد.

کارگاه پروتکل‌های اجماع بلاکچین

دکتر رسول رمضانیان، هیات دانشگاه فردوسی مشهد، دانشکده علوم ریاضی، راهبر بتای بلاکچین امن افزار- امن افزار گسترشریف

لینک کارگاه: https://www.skyroom.online/ch/uog/iscisc_room1

چکیده کارگاه:

بلاکچین یک دفترکل نامتمرکز است که برای اتصال یک بلوک جدید به دفترکل نیاز به اجماع گره‌های شبکه است. برای این منظور پروتکل های اجماع مختلفی مبتنی بر ابزارهای رمزنگاری طراحی شده است. در این کارگاه پروتکل های اجماع بلاکچین که تاکنون معرفی شده اند مورد بررسی و مقایسه قرار می‌گیرد. بلاکچین های عمومی و خصوصی کاربردهای زیادی از جمله در امورمالی نامتمرکز تا ترابری و کارخانه هوشمند دارند. پروتکل های اجماع بخش اصلی تکنولوژی بلاکچین است و طراحی یک پروتکل اجماع مناسب برای یک بلاکچین با توجه به هدفی که آن بلاکچین می خواهد به کار گرفته شود یک تخصص است. این کارگاه، با مرور پروتکل های اجماع این دانش را به متخصصین ایرانی در دانشگاه و صنعت منتقل خواهد کرد.

کارگاه مخاطرات و ریسک های امنیتی در شبکه 5G

حسین احمدی، کارشناسی ارشد مهندسی فناوری اطلاعات – شبکه های کامپوتری- شرکت امن افزار گستر شریف

لینک کارگاه: https://www.skyroom.online/ch/uog/iscisc_room2

چکیده کارگاه:

در پایان سال ۲۰۱۸، GPP۳ مشخصات کامل زیرساخت را منتشر کرد. این مشخصات به دو صورت مستقل (SA) و غیر مستقل (NSA) است. روش مستقل جایی است که 5G بدون اتکا به نسل های قبلی سلولی پیاده سازی می شود. روش غیر مستقل راهی برای پیاده سازی 5G از 4G/LTE در یک رویکرد مرحله ای است. در 5G تجهیزات کاربر می تواند هر دستگاهی باشد که از شبکه 5G استفاده می کند. به عنوان مثال می توان به تلفن های همراه، وسایل نقلیه، اینترنت اشیاء 5G و موارد دیگر اشاره کرد. لذا با فراگیرتر شدن G۵ در سراسر جهان، جامعه امنیتی از این فرصت برای بررسی و درک خطرات امنیتی بالقوه مرتبط با اجرای استاندارد استفاده می کند. مخطاطرات امنیتی شامل مخاطرات ارثی و مخاطرات خارج از محدوده است. در این کارگاه مخاطرات و روشهای امن سازی نسل پنجم مورد بررسی قرار می‌گیرند.

کارگاه آشنایی عملی با DevSecOps و راه اندازی یک نمونه pipeline آن در AWS

دکتر علیرضا نوروزی، هیات علمی دانشکده فنی دانشگاه صدا و سیما، مشاور مرکز تحقیق و توسعه همراه اول

مهندس مهسا لمیعیان، واحد تحقیق و توسعه همراه اول

لینک کارگاه: https://www.skyroom.online/ch/uog/iscisc_room1

چکیده کارگاه

توسعه عملیات (DevOps) مجموعه‌ای از روشها و فرایندها و ابزارهایی است که با تمرکز بر ارتباطات و همکاری و یکپارچگی بین تیمهای توسعه نرم‌افزار و عملیات فناوری اطلاعات، ارزش‌های تولیدشده را به طور سریع و مداوم به مشتریان نهایی می‌رساند. در کنار DevOps مفهوم توسعه، امنیت و عملیات (DevSecOps) به عنوان نسخه تقویت شده معرفی شده است تا امکان ادغام اقدامات امنیتی در رویکرد DevOps را فراهم کند. هدف این رویکرد یکپارچه سازی امنیت به عنوان یک مسئولیت مشترک در کل چرخه حیات فناوری اطلاعات (برخلاف مدل سنتی تیم امنیتی متمرکز) می‌باشد. در این کارگاه، ابتدا چرخه کامل DevSecOps بررسی شده و در ادامه ابزارهای مناسب برای هر یک از گام‌هایCI/CD در این چرخه معرفی می‌گردد. در انتهای این کارگاه نحوه ایجاد یک pipeline CI/CD با استفاده از خدمات AWS ارائه می‌گردد به طوری که تجزیه و تحلیل امنیتی را در سراسر pipeline صورت پذیرد.