روز صفر

ماهنامه علمی

سال سوم / شماره بیستم /آبان‌ماه ۰۰

انجمن رمزایران
iranian Society of Cryptology

این ماهنامه با حمایت مادی و معنوی اداره کل امور فرهنگی دانشگاه اصفهان چاپ و منتشر شده است.

نشریه علمی روز صفرم
شماره ۲۰ - آبان ۱۴۰۰

صاحب امتیاز:
شاخه دانشجویی انجمن رمز ایران در دانشگاه اصفهان

سردبیر:
محمد آقائی

مدیر مسئول:
الهه رهبران

طراح جلد و صفحه‌آرا:
نوریه سادات مدنیان
محمد آقائی

هیئت تحریریه:
سروش ذوالفقاری
فاطمه وهابی
علی دادخواه
بهار خلیلیان

اخبار:
سروش ذوالفقاری

ویراستار:
الهه رهبران

t.me/SBISC
SBISC.ui.ac.ir
t.me/CTFprep
twitter.com/SBISC1
instagram.com/SBISC_UI

درباره انجمن:

شاخه دانشجویی انجمن رمز ایران در دانشگاه اصفهان از سال ۱۳۸۶ فعالیت خود را پیرامون مباحث مرتبط با امنیت اطلاعات آغاز کرد. این انجمن که هم‌اکنون یازده دوره از آغاز فعالیت آن می‌گذرد، تصمیم به انتشار نشریه‌ای با عنوان "**روز صفرم**" گرفته است تا از این طریق بتواند دانش امنیتی در فضای سایبر را به مخاطبان خود منتقل کند.این نشریه به صورت ماهانه و از اردیبهشت ۹۸ منتشر شده است.

روز دانشجو مبارک

رمزنگاری - قسمت اول - تاریخچه

History-Cryptography-part1

سروش ذوالفقاری

Zolfaghari.soroush@gmail.com

بشر از اولین ساعات تمدن به دنبال پیدا کردن راهکارهایی جهت انتقال مفاهیم و پیام‌ها به شکل مخفی و خصوصی بوده است. بنابراین رمزنگاری برخلاف دیدگاه عام، یک مسئله بسیار قدیمی و کهنه تاریخی است که هم‌زمان با مدنیت انسان، رشد کرده و پا به عرصه زمان حال و مدرنیته عصر جدید گذاشته است.

شاید بتوان گفت که پیدایش مقوله رمزنگاری هم‌زمان با پیدایش خط شکل گرفته است؛ به‌طوری که افرادی که قادر به خواندن و نوشتن بوده‌اند پیام‌ها و مفاهیم مهم را با استفاده از نمادها و اشکال، مخفی نگاه می‌داشتند و به این شکل راهی برای انتقال مفاهیم و پیام‌ها بدون درک عام خلق شد. برای مثال خط هروگلیف (خط هیروگلیف را مصریان باستان اولین بار جهت نوشتن مطالب خود ابداع کردند. هیروگلیف مصری‌ها یکی از قدیمی‌ترین روش‌های نوشتن است. برخی از این نوشته‌ها به ۵ هزار سال بر می‌گردد) یا همان خط مقدس جزو خطوط رمزیست که حتی در زمان خود نیز همگان قادر به خواندن و درک آن نبوده‌اند.

پس از ارتقای نوشتن از نمادها و اشکال و پیدایش خطوط حرفی مدرن (منظور نوشتار حرفی و حجایی به شکل مدرن می‌باشد) و در کنار آن پیدایش اعداد و ریاضیات راه را برای انسان جهت خلق روش‌های جدید رمزنگاری باز کرد. در این راستا معروف‌ترین ساختار رمزی حروف جُمل یا همان حروف ابجد می‌باشد. حروف ابجد درواقع تناظر حروف صامت الفبای عبری-آرامی با اعداد می‌باشد که همان‌طور از که نام آن بر می‌آید خالق این تناظر اقوام عبری و آرامی هستند که آن‌ها خود این روش را از نبطیان و فنیقی‌ها به ارث برده‌اند. این روش درواقع تبدیل کلمات به اعداد است که بر اساس ترتیبی که از قبل در حروف ابجد مشخص شده انجام می‌شود. اقوام ابری از این روش برای ارسال مفاهیم و پیام‌های زیادی در کتب مقدس و داستان‌های خود استفاده کرده‌اند و پس از آن این روش را به اعراب نیز ارائه دادند و در زمان حال حروف ابجد حتی در زبان فارسی نیز استفاده می‌شود.

نوشته دیوید کان در کتاب the codebreakers می‌گوید رمزشناسی مدرن از اعراب برای مستندسازی روش‌های رمزنگاری نشات گرفته. آل‌خلیل در قرن هشتم کتاب پیام‌های گرافیکی رمزنگاری که شامل تمام حالات حروف ترکیب و جایگشت‌های حروف صدادار و بدون صدای عربی برای اولین بار می‌باشد را نوشت. اختراع تکنیک تحلیل‌های فرکانسی برای شکاندن رمزهای تک حرفی توسط ریاضی‌دان عرب، ال کیندی، حوالی سال ۸۰۰ بزرگترین پیشرفت آنالیز رمزها تا جنگ جهانی دوم است.

در خارج از منطقه خاورمیانه روش‌های متفاوت بسیاری در تاریخ یافت

شده است که برای رمزنگاری استفاده شده‌اند. برای مثال در هند در حدود ۴۰۰ سال قبل از میلاد تا ۲۰۰ سال پس از میلاد، Mlecchita vikalpa یا "هنر درک نوشتن به زبان رمزی، و نوشتن کلمات به روشی خاص" در کاما سوترا به منظور ارتباط بین عاشقان رایج بوده است. که درواقع یک روش از رمز جایگزینی بوده است. به طور دقیق هندیان حروف زبان را در یک جدول لیست کرده و بر طبق پیمانه مشخصی تمام حروف را انتقال می‌دهند و از لیست جدید به دست آمده به جای لیست قبلی جهت نوشتن استفاده می‌کنند.(رمز جایگزینی درواقع همان رمز سزار است).

نمونه قابل توجه دیگر، روشی است که یونانیان به ویژه اسپارت‌ها برای رمز کردن نامه‌های خود استفاده می‌کرده‌اند. آن‌ها متن مورد نظر خود را بر روی چرم یا کاغذ پاپیروسی می‌نوشتند و آن را به دور یک چوب یا سفال استوانه‌ای با قطر مشخصی می‌پیچیدند. سپس به صورت مورب نامه را برش می‌دادند تا حروف کلمات از هم جدا شوند و یک نوار بلند مشتمل از حروف ناخوانا را شکل دهد. تنها فردی قادر به خواندن نامه بود که استوانه‌ای به همان قطر در اختیار داشته باشد. درواقع استوانه در این روش همان کلید رمز برای رمزگشایی متن می‌باشد.

پس از آن یکی از بهترین روش‌های معروف تاریخ برای رمزنگاری توسط روم باستان خلق شد که به آن رمز سزار گفته می‌شود. در این روش امپراطوری روم برای مخفی کردن نامه‌های خود حروف رومی را به اندازه مشخصی انتقال می‌دادند و عدد مورد نظر را به عنوان کلید در نظر می‌گرفتند. برای مثال اگر کلید رمز ۲ باشه عدد a به c نظیر می‌شود و الی آخر. این روش امروزه به سادگی قابل شکستن است اما در زمان خود یکی از بهترین راه‌ها برای رمز کردن نامه‌های مهم به شمار می‌آمده است.

این سبک از روش‌های جابه‌جایی و در هم ریختگی حروف تا قرون وسطی ادامه داشت تا این که همان‌طور که در ابتدا اشاره شد به دلیل خلق یک روش کارآمد توسط الکیندی به نام تحلیل آماری یا تحلیل فراکانسی، امکان شکستن این گونه رمزها بسیار ساده‌تر شد. در روش الکندی درواقع میانگین نرخ تکرار حروف در یک زبان را مشخص می‌کنند و از آنجایی که در رمزگزاری‌های این قبیل تنها هر حرف به یک حرف متناظر می‌شود می‌تواند بر اساس نرخ تکرار حروف کلمه اصلی را حدس زد و رمز را به این شکل شکست.

برای حل این مشکل در سال ۱۴۶۵، لئون آلبرتی، رمزنگاری چندالفبایی (polyalphabetic cipher) را توسعه داد که به عنوان راه‌حلی در برابر روش تحلیل فراوانی آل‌کندی به حساب می‌آمد.

در یک رمزنگاری چندالفبایی، یک پیام با استفاده از دو الفبای مجزا رمزگذاری می‌شود. یکی الفبایی‌ست که در آن پیام اصلی نوشته می‌شود و دومی الفبای کاملا متفاوتی است که در آن پیام پس از رمزگذاری، ظاهر می‌شود. با ترکیب روش سنتی رمزگذاری با روش جابه‌جایی حروف و روش رمزگذاری چند الفبایی، امنیت اطلاعات کدگذاری شده به طرز قابل توجهی افزایش می‌یابد. به استثنای حالتی که خواننده حروف الفبایی که پیام اصلی با استفاده از آن نوشته شده است را می‌دانست، روش تجزیه و تحلیل فراوانی استفاده‌ای نداشت.

علم رمزنگاری در طول قرن‌های متمادی به طور مداوم پیشرفت کرده است. یک پیشرفت عمده که در حوزه رمزنگاری توصیف شده، توسط توماس جفرسون در سال ۱۷۹۰ ارائه شده بود، هر چند شاید هیچ‌گاه ساخته نشد. ابداع او که به عنوان رمزنگاری چرخشی (cipher wheel) شناخته می‌شود، شامل ۳۶ حلقه از حروفی می‌شود که بر روی یک چرخ در حال حرکت قرار دارند، که این ایده می‌تواند برای دستیابی به یک رمزگذاری پیچیده مورد استفاده قرار گیرد. این ایده و طرح آنقدر پیشرفته بود که به عنوان پایه رمزنگاری ارتش آمریکا تا پایان جنگ جهانی دوم مورد استفاده قرار گرفت.

رمزنگاری استفاده شده در جنگ جهانی دوم نیز نمونه‌ای کامل از رمزنگاری آنالوگ است که با نام ماشین انیگما (Enigma) شناخته می‌شود. همانند رمزنگاری چرخشی، این دستگاه نیز با به‌کارگیری نیروهای محور چرخ، از چرخ‌های در حال چرخیدن برای کدگذاری یک پیام استفاده می‌کند، که این نوع رمزنگاری تقریبا خواندن آن پیام توسط هر ماشین دیگری را غیرممکن می‌سازد.

منابع:

- Wikipedia, History of cryptography
- Wikipedia, Classical cipher
- Arzdigital.com, مروری بر تاریخچه رمزنگاری و انواع روش‌های آن

امنیت دیجیتال

Digital security

فاطمه وهابی
f.vahabi78@gmail.com

ما در زمانی زندگی می‌کنیم که بیشتر زندگی شخصی و حرفه‌ای ما به صورت آنلاین است. ما امور بانکی، خرید موسیقی، پرداخت قبوض، برنامه‌ریزی اجتماعی و حتی بخش‌هایی از کارمان را در دنیای دیجیتال انجام می‌دهیم. این افزایش اتکا به اینترنت و شبکه‌های دیجیتال خطراتی را به وجود می‌آورد.

مجرمان آنلاین، هکرها، حتی شیطنت‌کنندگان که صرفا حوصله‌شان سر رفته است، در سایه‌ها کمین کرده‌اند، منتظرند تا از شما سرقت کنند، مرتکب کلاهبرداری شوند و یا هویت شما را بدزدند. بنابراین، امنیت اطلاعات دیجیتال یکی از نگرانی‌های اصلی است.

امروزه با گسترش فناوری اطلاعات و افزایش تمایل مردم به دیجیتالی شدن سیستم‌ها، دیگر کسی معاملات خود را به صورت کاغذی انجام نمی‌دهد. ترجیح اکثر مردم بر این است که به سبب انتقال آهسته و پرهزینه اسناد و نیز دشواری در بایگانی آن، از قراردادهای الکترونیکی استفاده کنند. اما از آنجایی که همواره افرادی هستند که دست به سرقت اسناد دیگران می‌زنند، مسئله‌ای که در این قراردادها به عنوان معظل شناخته می‌شود، امنیت این اسناد می‌باشد. بنابراین لازم است این اسناد به رمز در آورده شوند. در همین راستا می‌توانیم اسنادمان را به صورت دیجیتالی امضا کنیم. امضای دیجیتالی یکی از روش‌های ایمن‌سازی اطلاعات است که کاربردی مشابه با امضای معمولی در معاملات دارد و یکی از روش‌های معتبر حفظ امنیت در شبکه می‌باشد.

لازم است پیش از شناخت امضای دیجتال با امنیت دیجتال آشنا شویم و ببینیم چه مسائلی امنیت ما را در فضای دیجیتال حفظ می‌کند. در ادامه به بررسی امنیت دیجیتال خواهیم پرداخت.

امنیت دیجیتال

امنیت دیجیتال منابعی را توصیف می‌کند که برای محافظت از هویت آنلاین، داده‌ها و سایر دارایی‌های شما استفاده می‌شود. این ابزارها شامل خدمات وب، نرم‌افزار آنتی ویروس، سیم کارت گوشی‌های هوشمند، بیومتریک و دستگاه‌های شخصی ایمن می‌باشد.

به عبارت دیگر، امنیت دیجیتال فرآیندی است که برای محافظت از هویت آنلاین شما استفاده می‌شود.

امنیت دیجیتال، محافظت از شخصیت دیجیتالی فرد است، مانند هویت فیزیکی در شبکه‌ای است که در آن کار می‌کنید یا سرویس اینترنتی که در حال استفاده از آن هستید. امنیت دیجیتال شامل ابزارهایی است که فرد برای ایمن کردن هویت، دارایی و فناوری خود در دنیای آنلاین و موبایل استفاده می‌کند. به زبان ساده، بیایید شخصیت دیجیتال را بدن انسان در نظر بگیریم. ما وظیفه داریم از بدن خود در برابر آسیب‌هایی که می‌توانیم بگوییم امنیت دیجیتال است، محافظت کنیم.

تعدادی روش (ابزار) وجود دارد که ما از آن‌ها برای محافظت از بدن خود استفاده می‌کنیم. ما غذا می‌خوریم و سالم زندگی می‌کنیم و خود را از خطر دور می‌کنیم. همین امر در مورد شخصیت دیجیتالی ما نیز صدق می‌کند.

چرا به امنیت دیجیتال نیاز داریم؟

هر روز تعداد زیادی حملات سایبری رخ می‌دهد و هر کسی ممکن است قربانی یک سرقت سایبری، هک یا جنایت شود. برندهای پیشرو جهانی با اطلاعات غلطی که در وب‌سایت‌هایشان قرار داده شده هک شده‌اند و کسب‌وکارهای کوچک و استارت‌آپ‌های نوآورانه در همه صنایع اغلب مورد هدف قرار می‌گیرند. زیرا اکثر آن‌ها سیستم‌های امنیتی دیجیتال مناسبی ندارند. هیچ کس حاضر نیست از چیزهایی که برای به دست آوردن آن‌ها سخت تلاش کرده است جدا شود.

مجرمان سایبری فرصت‌طلبانی هستند که به داده‌های ارزشمند و متنوع برای بهره‌برداری جذب می‌شوند. چیزی که آن‌ها نیاز دارند تنها یک فرصت مناسب است تا اسناد و اطلاعات شما را برباینند. اگر آن‌ها بتوانند یک کاربر را فریب دهند -برای مثال، از طریق یک حمله فیشینگ- هکرها می‌توانند هویت شما را بدزدند، اطلاعات کارت اعتباری شما را بردارند و حساب بانکی شما را مورد سرقت قرار دهند.

همانطور که در ابتدا گفتیم، افزایش اتکای ما به اینترنت به این معنی است که اگر چیزی به سمت و سوی دیجیتالی شدن پیش رفت، اسناد بیشتری برای از دست دادن داریم و خطرات افزایش می‌یابد. ما به داده‌های دیجیتالی بی‌عیب و نقص و قابل اعتماد نیاز داریم.

چه نوع اطلاعاتی ممکن است در خطر امنیت دیجیتال قرار گرفته شوند؟

لزوما هر اطلاعاتی که از شما به دست کلاهبرداران اینترنتی برسد، برای آن‌ها مفید نیست. در ادامه به برخی از اطلاعاتی که پس از ربوده شدن به کلاهبرداران امکان سرقت می‌دهد، اشاره می‌کنیم:

• داده‌های شناسایی شخصی

این داده‌ها شامل نام، شماره تلفن، آدرس، نام حساب ایمیل، آدرس IP، و از همه مهم‌تر، شماره شناسنامه شما است. همچنین شامل اطلاعاتی است که مکان شما را مشخص می‌کند. داده‌های شخصی اغلب برای سرقت هویت و مهندسی اجتماعی استفاده می‌شود. همچنین، هکری که شماره شناسنامه شما را دارد، می‌تواند حساب‌های کارت اعتباری را به نام شما باز کند و در نتیجه امتیاز اعتباری شما را از بین ببرد.

• داده‌های پرداخت شخصی

اگر مربوط به تراکنش‌های مالی باشد، داده‌های پرداخت، شخصی محسوب می‌شود. این اطلاعات شامل شماره کارت‌های اعتباری و نقدی (شامل تاریخ انقضا)، شماره‌های بانکی آنلاین (حساب و مسیریابی) و پین‌کدها است. مجرمانی که به اطلاعات بانکی آنلاین شما دسترسی پیدا می‌کنند، حتی می‌توانند وجوه خود را به خارج از حساب‌ها انتقال دهند یا خرید کنند.

• داده‌های سلامت شخصی

این نوع داده که به عنوان اطلاعات سلامت شخصی (PHI) نیز شناخته می‌شود، شامل اطلاعات مربوط به سلامتی شما، از جمله تاریخچه پزشکی، داروهای تجویزی، اشتراک بیمه سلامت، و بازدید از پزشک و بیمارستان است. این اطلاعات برای مجرمان سایبری پرمخاطب ارزشمند است. زیرا آن‌ها می‌توانند از اطلاعات سلامتی شما برای ثبت ادعاهای بیمه دروغین یا سفارش و فروش مجدد داروهای تجویزی استفاده کنند.

همانطور که گفتیم رمزنگاری اسناد و اطلاعات با استفاده از امضای دیجیتال یکی از روش‌هایی است که به ما در تأمین امنیت دیجتال یاری می‌رساند.

روش‌های مختلف امنیت دیجیتال

همانطور که می‌بینید، اگر داده‌های دیجیتالی شما به خطر بیفتد، مشکلات زیادی را به همراه خواهد داشت. خوشبختانه، امنیت در دنیای دیجیتال به اشکال مختلف وجود دارد و دامنه انتخاب گسترده‌ای از روش‌های دفاعی را در اختیار کاربران قرار می‌دهد. در ادامه با برخی از این روش‌ها اشنا خواهید شد:

• نرم‌افزار آنتی ویروس

ویروس‌هایی که از طریق بدافزار و سایر سیستم‌های مخرب منتقل می‌شوند، داده‌های شما را آلوده می‌کنند و سیستم شما را متوقف می‌کنند. یک برنامه آنتی ویروس خوب نه تنها این ویروس‌ها را شناسایی و پاک می‌کند، بلکه از نصب برنامه های مشکوک نیز جلوگیری می‌کند و تهدیدات احتمالی را نیز تشخیص می‌دهد.

• فایروال‌های به روزرسانی شده

این ابزار ترافیک وب را کنترل می‌کند، کاربران مجاز را شناسایی می‌کند، دسترسی غیرمجاز را مسدود می‌کند و در برابر ویروس‌های نسل بعدی محافظت می‌کند. فایروال‌ها سال‌هاست که وجود دارند و بسیاری از کارشناسان امنیت سایبری آن‌ها را منسوخ نمی‌دانند. با این حال، یک نسخه پیشرفته این ابزار برای دور نگه داشتن کاربران غیرمجاز ابزار مفیدی است.

• پروکسی‌ها

پروکسی‌ها ابزارهای امنیت دیجیتالی هستند که با استفاده از قوانین فیلتر مطابق با خط مشی‌های IT سازمان، باگ و عیوب بین کاربران و اینترنت را پر می‌کنند. پروکسی‌ها وب‌سایت‌های خطرناک را مسدود می‌کنند و از یک سیستم احراز هویت استفاده می‌کنند که می‌تواند دسترسی را کنترل کرده و چگونگی استفاده را نظارت کند.

• نرم‌افزار مانیتورینگ از راه دور

نظارت از راه دور به تیم امنیت داده اجازه می‌دهد تا اطلاعات را جمع‌آوری کند، مشکلات را تشخیص دهد و بر همه برنامه‌ها و سخت‌افزارها از راه دور نظارت کند. نظارت از راه دور انعطاف‌پذیری و راحتی را فراهم می‌کند و مدیران را قادر می‌سازد تا هر مشکلی را در هر زمان و هر مکان حل کنند.

• اسکنر آسیب‌پذیری

این ابزار نقاط ضعف سیستم سازمان شما را شناسایی، ارزیابی و مدیریت می‌کند. اسکنرهای آسیب‌پذیری نه تنها نقص‌ها را شناسایی می‌کنند، بلکه آن‌ها را اولویت‌بندی می‌کنند تا به شما در سازماندهی اقدامات متقابل کمک کنند. تیم‌های امنیتی فناوری اطلاعات می‌توانند از اسکنرها هم برای برنامه‌های کاربردی وب و هم برای سیستم‌های داخلی استفاده کنند.

امروزه یکی از روش‌هایی که در حفظ امنیت اسناد و مدارک در ارتباطات دیجیتالی تاثیر به سزایی گذاشته است، استفاده از امضای دیجیتال است. در نسخه بعدی مجله با امضای دیجیتال آشنا خواهیم شد.

منابع:

• An Overview of Digital Security, safeonline.ng

• What is Digital Security: Overview, Types, and Applications Explained, Simpli-

کاردینگ و نحوه مقابله با آن

Card Security

علی دادخواه
ali.d_lt@yahoo.com

امنیت در خرید و فروش‌های آنلاین یک مقوله مهم به شمار می‌آید. معمولا شما تا قبل از مواجهه با درگاه پرداخت جوانب امنیتی را رعایت نمی‌کنید و یا اصلا اهمیتی نمی‌دهید و تمرکز خود را بر روی قیمت‌های بهتر و کیفیت و تنوع محصولات می‌گذارید. اما به محض ورود به درگاه پرداخت احساس می‌کنید که اینجا دیگر باید احتیاط کرد تا اطلاعات مالی من توسط دیگران دزدیده نشود.
اطلاعات مالی شما در درگاه‌های پرداخت که شامل شماره کارت، تاریخ انقضا، CVV2 و ... می‌شود، اطلاعاتی هستند که افرادی خاص به نام کاربر سعی در به دست آوردن آن‌ها دارند تا با استفاده از آن‌ها یا حساب‌های بانکی شما را خالی کنند و یا با خرید محصولات و سپس فروش آن‌ها به دیگران سود کسب کنند.

کاردینگ چیست؟

کاردینگ به نوعی سرقت از کارت‌های اعتباری گفته می‌شود که با استفاده از تکنیک‌های مختلف و استفاده از روش‌های مهندسی اجتماعی (Social Engineering) حساب بانکی متصل به کارت اعتباری را را خالی می‌کنند. تعریف بالا از کاردینگ با توجه به تفاوت نظام بانک‌داری ایران با سایر نقاط جهان و عدم وجود کارت اعتباری در ایران ممکن است تفاوت‌های جزئی با تعریف مراجع داشته باشد اما معنا و مفهوم یکسانی را می‌رساند.
واضح است که به فردی که کاردینگ انجام می‌دهد کاردر گفته می شود. اما کاردینگ و کاردرها به دو دسته تقسیم می‌شوند:
۱ - کاردینگ فیزیکی (Real Carding)
۲-کاردینگ مجازی
بخش عمده کاردینگ فیزیکی به وسیله اسکن کردن کارت با دستگاه‌های مخصوص صورت می‌پذیرد. به این صورت که اطلاعات موجود بر نوار مغناطیسی کارت‌ها که شامل اطلاعات حساب شماست در دستگاه کپی می‌شود و بر روی کارت‌های خام دیگر نوشته می‌شود. با توجه به این که شما برای انجام تراکنش خود رمز کارت را نیز روی دستگاه وارد خواهید کرد، کار بسیار آسان می‌شود و سختی آن تنها به نحوه استفاده از تجهیزات نوشتن روی نوار مغناطیسی ختم می‌شود.
اما کاردینگ مجازی که بیشتر به آن خواهیم پرداخت به مراتب سخت‌تر است. شما هیچ وقت به کارت مشتری دسترسی کامل نخواهید داشت. اطلاعات کارت در این روش یا با حدس‌هایی که کاربر می‌زند به دست می‌آید یا با هک کردن درگاه و دیتابیس پرداخت‌ها که هک کردن دیتابیس پرداخت باز هم از حدس زدن اطلاعات سخت‌تر است.

کاردینگ در ایران و خارج از ایران و نحوه کاردینگ

در ایران بیشتر کاردینگ‌ها به حوزه فیشینگ و مهندسی اجتماعی مربوط می‌شود که افراد با سوءاستفاده از دانش پایین افراد در زمینه پرداخت آنلاین آن‌ها را به لینک‌ها و صفحات مخرب می‌کشانند و در آن جا اطلاعات کارت بانکی افراد را از آن‌ها می‌دزدند. بخش دیگر نیز با ورود 2FA به درگاه‌های پرداخت شاپرک با مشکل مواجه شده‌اند و سعی خود را بر روی دزدیدن رمزهای دوم یک بار مصرف گذاشته‌اند.

اما در خارج از کشور و در رابطه با درگاه‌های پرداخت مرسوم مثل PayPal و MasterCard با توجه به جامعه بزرگتر کاردرها، ابزارهای پیشرفته توسعه یافته و تکنیک‌های مختص به هر سایت شکل گرفته است که با وجود امنیت بالای درگاه‌ها و به روز رسانی دائم بلک لیست آن‌ها، باز هم مورد حملات کاردینگ قرار می‌گیرند.

به طور کلی کاردرها اطلاعات کارت‌های اعتباری افراد را از روش‌هایی مثل ایمیل‌های فیشینگ، جاسوس افزارها، نفوذ از طریق شبکه‌های وای‌فای عمومی و چیزهایی قدیمی‌تر مانند یادداشت‌ها و کاغذهایی که اطلاعات شخصی و بانکی شما روی آن‌ها درج شده است، به دست می‌آورند. سپس با چندین ابزار متنوع مثل چک‌کننده اتوماتیک موجودی کارت (که معمولا توسط خودشان برنامه‌نویسی شده‌اند) و نرم‌افزارهای تغییر مک آدرس، VPNها و پروکسی‌ها خودشان را در چندین لایه محافظتی دیجیتال می‌پوشانند و به سراغ فروشگاه‌های اینترنتی می‌روند.آن‌ها با ترفندهایی سیستم‌های Verification سایت‌ها مثل AVS (Address Verification System) و ... را دور می‌زنند و به هر نحو شده سفارش خود را ثبت می‌کنند. تا اینجا کاردرها می‌توانستند به خوبی فعالیت خود را مخفی نگه دارند و حتی کاردرهای مبتدی نیز می‌توانند خیلی سریع به این مرحله برسند. اما بخش مهم از اینجا به بعد شکل می‌گیرد که چگونه سبد خرید خود را دریافت کنم؟

خرید اشیاء فیزیکی و دریافت آن‌ها کار دشواری است چرا که احتمال لو رفتن عملیات کاردینگ زیاد است و کاردر را به خطر می‌اندازد. خوب است بدانید که انجام کاردینگ در آمریکا برای بار اول از یک تا سه سال حبس و از ۱۰۰۰ تا ۱۰۰۰۰ دلار جریمه نقدی به همراه دارد. برای همین کاردرهای مبتدی بیشتر سراغ خدمات و محصولات دیجیتالی می‌روند تا در دنیای واقعی به خطر نیفتند. کاردرهای بزرگ اما ریسک این کار را پذیرفته‌اند و محصولات فیزیکی گران‌قیمتی مانند تلفن‌های همراه، تلویزیون و ... نیز به سبد کاردینگ خود اضافه می‌کنند. لازم به ذکر است اکثر روند های کاردینگ در دارک وب انجام می‌گیرد و صرفا خرده فروشی محصولات در سطح وب عادی انجام می‌شود.

جلوگیری از کاردینگ در فروشگاه

اگر صاحب یک فروشگاه آنلاین هستید و می‌خواهید از حملات کاردینگ و عواقب آن در امان باشید چند راه حل زیر به شما کمک خواهند کرد:

- استفاده از کپچا (Captcha): قرار دادن یک کپچا در مراحل انتهایی پرداخت می تواند بسیاری از ربات‌هایی که کاردینگ را اتوماتیک می‌کنند را دچار مشکل کند. البته استفاده از کپچا در فروشگاه‌های خارجی چندان مرسوم نیست و می‌تواند بر Interaction سایت شما تاثیرگذار باشد.
- استفاده از AVS: سیستم تایید آدرس که بالاتر به آن اشاره شد از جمله روش‌هایی است که می‌تواند جمعیت زیادی از کاردرها را از کارشان منصرف کند. این سیستم در هنگام خرید از خریدار آدرسی درخواست می‌کند و آن را با آدرس مرتبط با کارت مطابقت می‌دهد و بر اساس میزان تطابق درجه‌بندی می‌کند. حال شما با توجه به میزان تطابق می‌توانید اجازه تکمیل تراکنش را بدهید یا ندهید.
- **چک کردن IP و پروکسی:** برخی IPهای مرتبط با VPNها در بلک لیست سایت‌های تشخیص IP قرار گرفته‌اند و در هنگام مشاهده سایت‌ها مرتبا از این کلاینت‌ها در خواست حل کپچا می‌شود. لیستی از این نوع IPها تهیه کنید و از خرید آن‌ها جلوگیری کنید. همچنین با استفاده از تکنیک‌های مختلف مثل اسکن کردن پورت‌های پروکسی کلاینت (باز یا بسته بودن) و یا بررسی هدرهای HTTP می‌توانید به فعال بودن پروکسی پی ببرید و از خریدار بخواهید تا VPN یا پروکسی خود را غیرفعال کند.
- **چک کردن BINهای مشابه:** BIN (Bank Identification Number) چند شماره اول کارت‌های بانکی است که بیانگر بانک صادر کننده و نوع کارت اعتباری است. (یک متد کاردینگ ساده به همین نام BIN وجود دارد) اگر به حملات کاردینگ مشکوک هستید با چک کردن BINهای مشابه می‌توانید به وقوع این حملات پی ببرید. برای مثال اگر طی یک روز چندین خرید مشکوک با BINهای مشابه داشته باشید احتمالا سایت شما با حملات BIN مواجه است.

درباره صاحبان کارت نیز حفاظت از اطلاعات مالی و شخصی، اهمیت دادن به حریم به خصوصی چه در دنیای واقعی و چه مجازی، با سایت‌ها و افراد به بهانه‌هایی مثل قرعه کشی و ... می‌تواند کارساز باشد. همچنین افزایش دانش در رابطه با نحوه اجرای این حملات و نقاط ضعف آن‌ها می‌تواند به مبارزاتی که پلیس‌های سایبری علیه کاردرها و دیگر افرادِ خارج از دایره قانون کمک و از سوءاستفاده‌های مالی گسترده‌تر جلوگیری کند.

منابع:

- blog.shift4shop.com, What is Carding and How to Prevent it in Your Online Store
- www.ipqualityscore.com, How to Detect Proxies with PHP

رمزنگاری اطلاعات

Data Encryption

بهار خلیلیان
bahaar.khalilian@gmail.com

رمزنگاری اطلاعات چیست؟

رمزنگاری در حیطه امنیت سایبری به معنای تبدیل اطلاعات از فرمی قابل خواندن به فرمی کدگذاری شده است. اطلاعات رمزنگاری شده، که به صورت متنی در هم ریخته دیده می‌شوند، تنها در صورتی قابل خوانده شدن و پردازش هستند که با استفاده از کلید مخصوص به کد رمزگشایی شوند.

رمزنگاری اطلاعات، پایه‌ترین، ساده‌ترین و مهم‌ترین اقدام در راستای امنیت اطلاعات است که توسط نرم‌افزارها یا همان الگوریتم‌های رمزنگاری انجام می‌شود و تنها با استفاده از قدرت محاسباتی بالا قابل شکسته شدن است. اشخاص و کمپانی‌ها از این روش در راستای محافظت از اطلاعات شخصی افراد استفاده می‌کنند. بنابراین این اطلاعات می‌توانند دارای گونه‌های متفاوتی باشند. جزئیات حساب بانکی کاربران در یک کمپانی و اطلاعات دولتی از نمونه‌هایی است که باید مورد حفاظت قرار بگیرند.

برای مثال در یک پیام رسان، رمزنگاری اطلاعات موجب امنیت در زمینه‌های احراز هویت، تمامیت و عدم انکار می‌شوند.

به اطلاعات در فرم ساده و رمزنگاری نشده plaintext و به فرم رمزنگاری شده آن ciphertext گفته می‌شود.

رمزنگاری اطلاعات به چه صورتی انجام می‌شود؟

هنگامی که اطلاعات در اینترنت و شبکه‌ها به جریان می‌افتند، در معرض حملات سایبری و خطرات هکرها قرار می‌گیرند. به منظور جلوگیری از این خطرات، از رمزنگاری در امنیت شبکه استفاده می‌شود. به این صورت که فرستنده و گیرنده بر روی یک کلید رمزنگاری توافق می‌کنند. هر چقدر این کلید دشوارتر باشد امنیت شبکه نیز بالاتر می‌رود و احتمال این‌که هکرها بتوانند با الگوریتم‌های تلاش تصادفی آن را بشکنند پایین‌تر می‌آید.

این کلید رمزنگاری با استفاده از مقادیر عددی و ریاضی تولید می‌شود. مثالی بسیار ساده از این فرایند، جایگزینی حروف با مقادیر عددی‌شان است که سپس در عدد X ضرب می‌شوند. عدد X نمایانگرکننده کلید خواهد بود. هنگامی که گیرنده پیام رمزنگاری شده را دریافت می‌کند، آن را با استفاده از کلید به متن اولیه تبدیل می‌کند.

رمزنگاری متقارن و نامتقارن

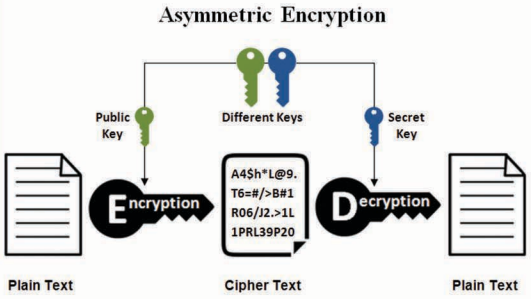
در رمزنگاری متقارن، هنگام رمزنگاری و رمزگشایی از یک کلید یکسان استفاده می‌شود. این روش به آسانی قابل اجرا است و زمان کمتری نیز صرف آن می‌شود. اما این روش مشکلاتی به وجود می‌آورد. برای مثال اگر در نامه‌نگاری الکترونیکی از رمزنگاری متقارن استفاده شود، فرد فرستنده کلید شخصی خود را در اختیار تمامی گیرندگان قرار می‌دهد و باعث پایین آمدن سطح امنیت می‌شود.

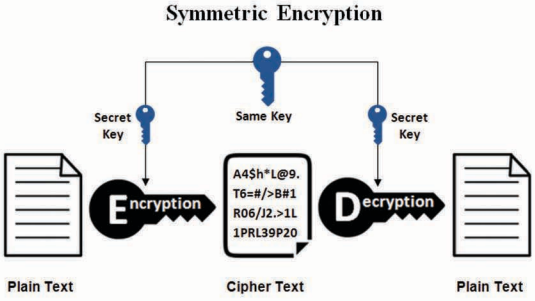
در رمزنگاری نامتقارن به جای استفاده از یک کلید یکسان برای رمزنگاری و

رمزگشایی، از دو کلید عمومی و شخصی استفاده می‌شود. کلید عمومی در اختیار کسانی قرار می گیرد که برای گیرنده پیام می فرستند. اما کلید شخصی فقط در اختیار صاحب حساب کاربری قرار می‌گیرد. پس فرستندگان باید پیام خود را با کلید عمومی گیرنده رمزنگاری کنند. در مرحله بعد اگر کلید عمومی با کلید شخصی مطابقت داشت، متن رمزنگاری شده تنها با کلید شخصی گیرنده قابل رمزگشایی شدن است.

رمزنگاری نامتقارن نسبت به روش متقارن زمان بیشتری می‌گیرد ولی نیازی به اشتراک‌گذاری کلید ندارد. اما از مشکلات این روش این است که در صورتی که فردی کلید شخصی خود را فراموش کند، غیر قابل بازیابی خواهد بود و همچنین فرستندگان تنها در صورتی می‌توانند پیامی را بفرستند که فرد گیرنده کلیدهای جفت شده درست کرده باشد.

در نتیجه می‌توان گفت استفاده از یکی از این دو روش در صورتی که متناسب با موقعیت باشد، به صرفه است. رمزنگاری متقارن در پیام‌های سریع و یا پیام‌هایی که نیازی به امنیت بالا ندارند مناسب‌تر است و رمزنگاری متقارن در مواقعی که اطلاعات به اشتراک‌گذاری شده نیاز به محافظت بیشتری دارند بهتر است.





الگوریتم‌های متفاوت رمزنگاری

الگوریتم‌های مختلف با توجه به اهداف رمزنگاری‌های مختلف ابداع می‌شوند. هنگامی که الگوریتم‌های قدیمی‌تر شکسته می‌شوند و کارآمدی خود را از دست می‌دهند، الگوریتم‌های جدیدتری توسعه داده می‌شوند. در ادامه به معرفی تعدادی از بهترین الگوریتم‌های رمزنگاری می‌پردازیم.

• الگوریتم DES:

استاندارد رمزنگاری اطلاعات (Data Encryption Standard) یا به اختصار DES، شیوه رمزنگاری متقارنی است که توسط IBM توسعه داده شد و سپس به عنوان استاندارد ملی در آمریکا معرفی شد. DES به دلیل محدودیت پنجاه و شش بیتی که بر روی کلید دارد، امنیت نسبتا پایینی دارد. با شکسته شدن کلید DES در سال ۱۹۹۹ این الگوریتم به طور کامل کنار گذاشته شد و با AES جایگزین شد.

• الگوریتم AES:

استاندارد پیشرفته رمزنگاری (Advanced Encryption Standard) یا به اختصار AES، بعد از شکسته شدن کلید DES ابداع شد. این الگوریتم نیز متقارن است و اولین شیوه رمزنگاری‌ای است که به صورت رایگان در دسترس عموم قرار گرفت و به عنوان استاندارد صنعتی استفاده می‌شود. AES دارای طول کلید متغیر است و پایداری آن به عنوان استاندارد به این دلیل است که چندین دور از رمزنگار عبور می‌کند و تا کنون شکسته نشده است.

• الگوریتم 3DES:

الگوریتم 3DES (Triple Data Encryption Standard) همان الگوریتم DES است با این تفاوت که اطلاعات سه دفعه از الگوریتم عبور داده می‌شوند. این روش به تدریج در حال حذف شدن است. با این حال، هنوز در رمزنگاری سخت‌افزار در زمینه‌های خدمات اقتصادی و دیگر صنایع در حال استفاده است.

• الگوریتم RSA:

نام این الگوریتم مخفف شده اسامی ریاضیدان‌هایی است که آن را ابداع کردند. Rivest، Shamir و Adleman. این الگوریتم از دو کلید برای رمزنگاری استفاده می‌کند و به همین دلیل اولین الگوریتم رمزنگاری نامتقارن است. RSA به دلیل طول کلیدش در انتقال امن داده‌ها قابل استفاده است.

• الگوریتم Twofish:

این الگوریتم هم در نرم‌افزار و هم در سخت‌افزار قابل استفاده است و در نوع خود از سریع‌ترین‌ها شناخته می‌شود. الگوریتم Twofish ثبت اختراع نشده است و به همین دلیل در بسیاری از برنامه‌های رمزگذاری مانند PhotoEncrypt و GPG و TrueCrypt استفاده می‌شود و به صورت رایگان در دسترس عموم قرار گرفته است.

• الگوریتم RC4:

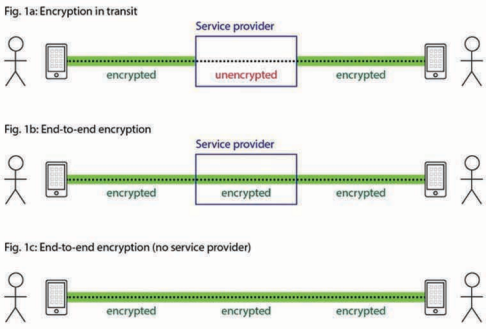
این الگوریتم در رمزنگاری روترهای بی‌سیم (Wireless Routers) مانند WEP و WPA استفاده می‌شود و از داده‌ها را یک بایت یک بایت رمزنگاری می‌کند. با اینکه RC4 به دلیل سادگی و سرعتش در نرم‌افزارها شناخته شده است، دارای آسیب‌پذیری‌هایی است که استفاده از آن را ناامن کرده است.

شش الگوریتم معرفی شده از قوی‌ترین و بهترین الگوریتم‌ها هستند که هم اکنون در حال استفاده می‌باشند.

رمزگذاری سرتاسر:

رمزگذاری سرتاسر (End to End Encrypted) یا به اختصار E2EE، سیستم ارتباطی‌ای است که اجازه دسترسی به اطلاعات و پیام‌ها را تنها به گیرنده و فرستنده اطلاعات می‌دهد. در بسیاری از پیام‌رسان‌ها علاوه بر فرستنده و گیرنده، شخص ثالثی نیز اجازه دسترسی به اطلاعات را دارد. به این معنی که پیام در مسیر رسیدن به گیرنده توسط واسطه‌ای ذخیره می‌شود و این واسطه می‌تواند اطلاعات را رمزگشایی کند. برای مثال پیام‌رسان‌های تحت پوشش گوگل اجازه دسترسی به اطلاعات فرستاده شده را دارند و از آن‌ها در تبلیغات شخصی سازی شده برای افراد استفاده می‌کنند.

رمزگذاری سرتاسر از هک شدن اطلاعات در طول مسیر جلوگیری می‌کند و حتی واسطه ارتباطی نیز قادر به رمزگشایی آن‌ها نخواهد بود. قابل توجه است که در E2EE طرفین باید کلید عمومی یکدیگر را داشته باشند و در صورتی که دستگاه هر یک از طرفین هک شود، این اطلاعات قابل دسترسی خواهند بود. البته این مشکل بیشتر به امنیت دستگاه‌ها بستگی دارد تا به شیوه رمزگذاری سرتاسر. علاوه بر آن رمزگذاری سرتاسر با اینکه از خود اطلاعات محافظت می‌کند، توانایی مخفی کردن هویت گیرنده و یا زمان فرستاده شدن پیام را ندارد. این موضوع ممکن است منجر به توجهات ناخواسته دیگری بشود.

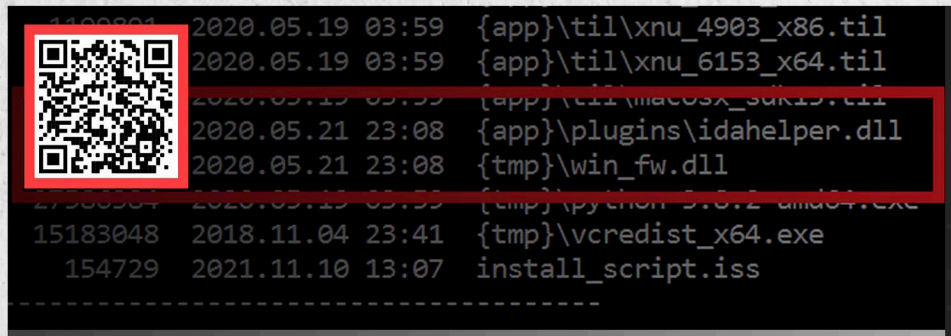


منابع:

• blog.mailfence.com, Symmetric vs Asymmetric Encryption
• www.kaspersky.com, What is data encryption?
• digitalguardian.com, What is data encryption?
• www.thalesgroup.com, Brief History of Encryption
• searchsecurity.techtarget.com, End to End Encryption

گزیده اخبار آبان‌ماه

گردآورنده: سروش ذوالفقاری
zolfaghari.soroush@gmail.com



کشف تروجان در نصب کننده IDA Pro

محققان امنیتی شرکت ESET اخیرا از کشف یک نمونه نصب‌کننده IDA pro خبر دادند که به تروجان‌های ویندوزی آلوده شده است. به گفته منابع خبری هکرهایی که عامل آلودگی این نصب‌کننده بوده‌اند تحت حمایت کره‌ی شمالی فعالیت می‌کنند.

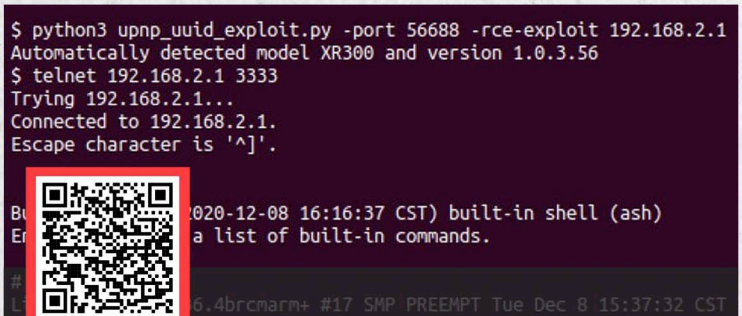
نرم‌افزار IDA یا همان Interactive Disassembler یک نرم‌افزار تحلیل فایل‌های باینری و مهندسی معکوس می‌باشد که برای تحلیل و کرک فایل‌ها مورد استفاده قرار می‌گیرد.

همچنین قابل ذکر است که تروجان یک نوع بدافزار است که در بین فایل‌های باینری عادی قابل اجرا جاسازی می‌شود و بیشتر به هدف ایجاد دستری پشتی (Back door) در سیستم‌عامل‌ها استفاده می‌شود. (نام تروجان برگرفته از داستان معروف یونان باستان است که به اسب چوبی جنگ تروجان اشاره دارد)

هشدار مایکروسافت در مورد روی آوردن 6 گروه هکری ایرانی به باج افزار

محققان مرکز اطلاعات تهدیدات سایبری مایکروسافت (MSTIC) فاش کردند که کمتر از شش عامل تهدید وابسته به کشورهای غرب آسیایی کشف شده‌اند که باج‌افزار را برای دستیابی به اهداف استراتژیک خود به کار می‌گیرند و افزودند: «این باج‌افزارها به طور متوسط هر شش تا هشت هفته یک‌بار به صورت موجی راه‌اندازی می‌شوند.

نقص سرریز بافر پیش از احراز هویت در روترهای اداری کوچک و اداری خانگی (SOHO) می تواند منجر به اجرای کد با بالاترین امتیازات شود. شرکت تجهیزات شبکه Netgear دور دیگری از وصله‌های امنیتی را (security patches) برای اصلاح آسیب‌پذیری (اجرای کد از راه دور با اولویت بالا) منتشر کرده است.

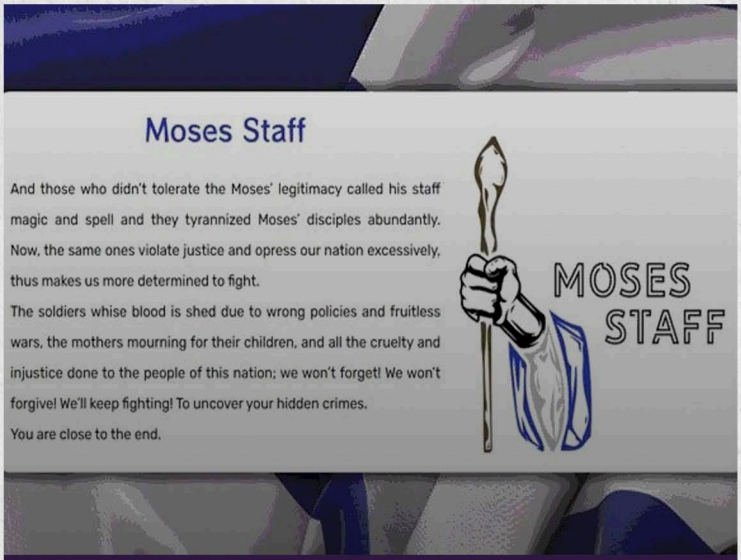


اشکال RCE بحرانی بر چندین مدل روتر Netgear SOHO تأثیر گذاشت

اکسپلویت جدید آهنگر(Blacksmith)، راه های دفاعی حمله کنونی Rowhammer را دور می‌زند

محققان امنیت سایبری یک نوع دیگر از حمله Rowhammer را نشان داده‌اند که بر تمام تراشه‌های DRAM (حافظه دسترسی تصادفی پویا) تأثیر می‌گذارد که اقدامات کاهش‌دهنده فعلی را دور می‌زند و در نتیجه به طور مؤثر امنیت دستگاه‌ها را به خطر می‌اندازد.

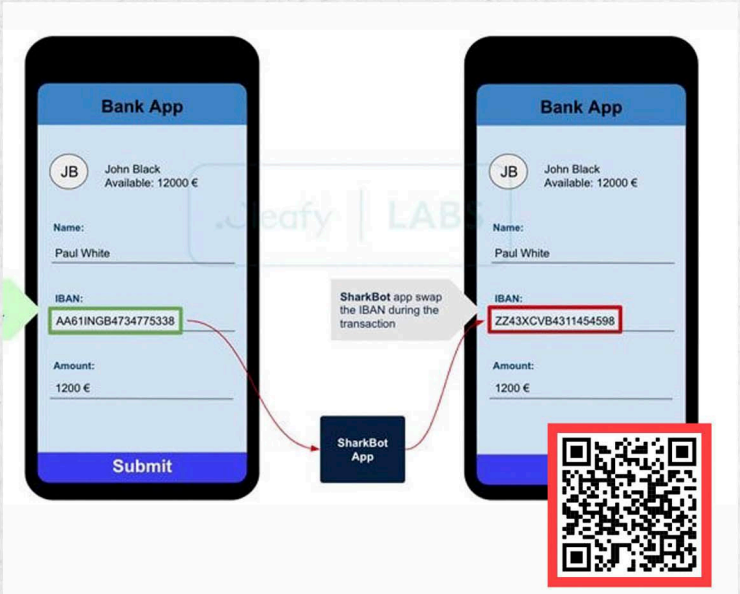
چکش ردیفی یا Row hammer یک سوء استفاده امنیتی است که از یک اثر جانبی ناخواسته و نامطلوب در حافظه تصادفی پویا (DRAM) استفاده می‌کند که در آن سلول‌های حافظه شارژ بین خود را با تعامل با یکدیگر نشت می‌دهند. در این حالت احتمال نشت یا تغییر اطلاعات در ردیف‌های مجاور ردیفی که به طور مستقیم به آن دسترسی داریم وجود دارد. عدم ایزوله بودن سلول‌های حافظه DRAM نسبت به یکدیگر بخاطر تراکم بالای سلول در DRAMهای مدرن می‌باشد.



گروه جدید هکری به نام «کارمندان موسی» شرکت‌های اسرائیلی را با حملات مخرب هدف قرار می دهند

یک گروه جدید هکری با انگیزه سیاسی به نام "کارکنان موسی" از سپتامبر ۲۰۲۱ با موجی از حملات هدفمند که سازمان‌های اسرائیلی را هدف قرار می‌دهند. این گروه با هدف غارت و افشای اطلاعات حساس قبل از رمزگذاری شبکه‌هایشان، دست به حمله میزنند؛ و تا به حال به دنبال هیچ مذاکره‌ای مبنی بر دریافت باج و ... نبوده است.

محققان امنیت سایبری یک تروجان اندروید جدید را معرفی کردند که از ویژگی‌های دسترسی در دستگاه‌های تلفن همراه برای جذب اعتبار از خدمات بانکی و ارزهای دیجیتال در ایتالیا، بریتانیا و ایالات متحده استفاده می‌کند.



SharkBot - یک تروجان اندرویدی جدید که حساب‌های بانکی و ارزهای دیجیتال را می‌دزدد

تاریخچه رمزنگاری

امنیت دیجیتال

کاردینگ و نحوه مقابله با آن

رمزنگاری اطلاعات

Cyber news

روز صفرم ترجمه ی عبارت Zero Day می‌باشد که در تعبیر لغوی یعنی روزی که هنوز به آن نرسیده‌ایم و از وجود چنین چیزی هم خبر نداریم، وقتی صحبت از حمله Zero Day می‌شود یعنی در خصوص حمله ای صحبت می کنیم که هیچکس تا کنون آن را شناسایی نکرده است و هیچ دانشی هم در خصوص آن وجود ندارد که چگونه آن را تشخیص و بعضا از بروز آن جلوگیری کنیم.

در این نشریه سعی بر آن است تا زوایای پنهان و ناشناخته در دنیای امنیت اطلاعات مورد بررسی قرار گرفته و به جدیدترین اخبار و تکنولوژی‌های این حوزه پرداخته شود. مخاطبین این نشریه تمامی دانشجویان و افرادی خواهند بود که به حوزه امنیت اطلاعات علاقمند هستند.

برای ارسال مقالات جهت چاپ در نشریه به @elahe_rahbaran در تلگرام پیام دهید.