خبرنامه الکترونیکی ۵۳

مرکز تخصصی آپا دانشگاه سمنان

شماره پنجاه و سوم، سال پنجم، مهر ۱۴۰۱ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

تجارت یا ترفند؟

تشخیص و شناسایی توکن‌های کلاهبرداری در صرافی غیرمتمرکز Uniswap

https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert

برای مردم

پدافند دانش بنیان، حفاظت از زیرساخت‌ها، تداوم کارکردها

نکوداشت پدافند غیرعامل ٤ تا ١١ آبان ١٤٠١

مسئله‌ی پدافند غیرعامل مسئله‌ی بسیار مهمی است و هر روز که می‌گذرد بر اهمیت پدافند غیرعامل افزوده می‌شود.

حضرت امام خامنه‌ای (مدظله العالی)

فهرست

خبر

گزیده مطالب نشریات حوزه امنیت سایبری

مرکز آپا دانشگاه سمنان

خبر

گوگل از کتابخانه رمزگذاری هم‌ریخت OpenHFE استفاده می‌کند

دوالیتی تکنولوژی پیشرو در راهکارهای یکپارچه ارتباطی با حفظ حریم خصوصی داده‌های ایمن، اعلام کرد که شرکت گوگل، کتابخانه Transpiler خود را که با استفاده از XLS SDK ساخته شده است و در گیت هاب قرار دارد و همچنین منبع باز و رمزگذاری آن کاملاً هممورفیک[1] است را یکپارچه کرده تا تخصص رمزنگاری را در دسترس‌تر و ساده‌تر کند، درنتیجه پذیرش FHE توسط توسعه‌دهندگان تسریع می‌شود.

یوری پلیاکوف، مدیر ارشد تحقیقات رمزنگاری و دانشمند اصلی Duality اظهار داشت: تیم ما با کتابخانه OpenFHE به نقاط عطف مهمی دست یافته است و به سرعت تبدیل به انتخاب بسیاری از رهبران فناوری امروزی مانند گوگل شده است. Google Transpiler برای تمامی توسعه‌دهندگانی که متخصص FHE نیستند، دسترسی به آخرین ویژگی‌های OpenFHE را فراهم می‌کند.

رمزنگاری FHE به گروهی از روش‌های رمزگذاری اشاره دارد که با روش‌های معمولی تفاوت دارند زیرا امکان انجام محاسبات را مستقیماً روی داده‌های رمزگذاری‌شده بدون نیاز به کلید مخفی فراهم می‌کنند. OpenFHE که ریشه در رمزنگاری داربستی[2] منبع باز پسا کوانتومی دارد، توسط جامعه رمزنگاران مشهور جهان تأسیس شد که این کتابخانه را برای استفاده حداکثری، بهبود APIها، پیمانه‌ای بودن و قابلیت حمل بین پلتفرم‌ها طراحی کردند. این کتابخانه در صورت ادغام با سخت‌افزار، یک شتاب‌دهنده پروژه خواهد بود. OpenFHE همراه

1-FHE
2-lattice

بـا Transpiler گـوگل بـه توسـعه‌دهندگان ایـن امـکان را می‌دهـد تـا کدهـای سـطح بـالا، ماننـد C++ کـه بـه طـور معمـول روی داده‌هـای رمزگـذاری نشـده اسـتفاده می‌شـود را بـه کـد سـطح بالایـی تبدیـل کننـد کـه داده‌هـای رمزگـذاری شـده را بـدون نیـاز بـه یادگیـری رمزنـگاری بـه کارمی‌گیرنـد. میگوئـل گـوارا، مدیـر دفتـر حفاظـت از حریـم خصوصـی و داده، از شـرکت گـوگل می‌گویـد: «مـا در گـوگل قصـد داریـم دسترسـی بـه فنـاوری پیشـرفته‌ای را دموکراتیـک کنیـم کـه بـه امنیـت اینترنـت کمـک می‌کنـد و امنیـت افـراد را بـه صـورت آنلایـن حفـظ می‌کنـد. Transpiler بـا رمزنـگاری FHE یـک گام در ایـن مسـیر اسـت و مـا از همـکاری بـا شـرکت Duality خوشـحال هسـتیم. توسـعه‌دهندگان چـه روی برنامه‌هـای ابـری کار کننـد و چـه روی لبـه، مـا مشـتاقیم مـوارد اسـتفاده جدیـد و هیجان‌انگیـز Transpiler کـه بـه ارائـه خدمـات امنیـت و تضمین‌هـای امنیتـی پیشـرفته و حفـظ حریـم خصوصـی کمـک می‌کنـد را ببینیـم.»

در حـال حاضـر، پیاده‌سـازی HFE از پایـه، مسـتلزم تخصـص بالایـی اسـت. یادگیـری تخصـص HFE بـه خصـوص در ابتـدای کار بـه تـلاش زیـادی نیـاز دارد. Transpiler فرآینـد اسـتفاده از برنامه‌هـای کاربـردی مبتنـی بـر FHE را بـدون نیـاز بـه چنیـن تخصصـی فراهـم می‌کنـد.

پولیاکـوف افـزود: یکـی از اهـداف اصلـی اسـتراتژیک OpenFHE ایـن اسـت کـه FHE را بـرای بسـیاری از مسـائل مهـم عملـی بـا تمرکـز ویـژه بـر برنامه‌هـای یادگیـری ماشـین قابـل اسـتفاده کند. همـکاری ما بـا تیـم Google Transpiler نقـش مهمـی در تحقـق ایـن چشـم‌انداز دارد.

گوگل از کتابخانه رمزگذاری هم‌ریخت OpenHFE استفاده می‌کند

مرکز آپا دانشگاه سمنان

کارگاه امنیت کاربری

برای مردم

پدافند دانش‌بنیان،
حفاظت از زیرساخت‌ها،
تداوم کارکردها

مدرس:

مهندس غزاله مصطفائی علائی
کارشناس ارشد مهندسی کامپیوتر،
فعال حوزه امنیت فناوری اطلاعات

روز برگزاری: ۱۱ آبان

ساعت ۹ الی ۱۱

تمام افرادی که از اینترنت،
تلفن هوشمند، تبلت، لپ‌تاپ
و... استفاده می‌کنند

هزینه: رایگان

لینک ورود به کارگاه:

http://stm.semnan.ac.ir

اعطای گواهی معتبر از مرکز آپا دانشگاه سمنان
دارای مجوز رسمی از سازمان فناوری اطلاعات ایران

023-31535021 / 023-31535019
@semcert
info.cert@semnan.ac.ir
@semcert_admin

جهت ثبت نام به وب‌سایت https://cert.semnan.ac.ir مراجعه کنید.

مرکز آپا دانشگاه سمنان

گزیده مطالب

نشریات منتشر شده

در حوزه امنیت سایبری

تجارت یا ترفند؟
تشخیص و شناسایی توکن‌های کلاهبرداری در صرافی غیرمتمرکز Uniswap

در این مقاله که در سال ۲۰۲۱ در مجله علمی Proceedings of the ACM on Measurement and Analysis of Computing Systems چاپ شده به ارائه یک راهکار برای تشخیص توکن‌های کلاهبرداری در صرافی غیرمتمرکز Uniswap پرداخته می‌شود.

محققان در این پژوهش ابتدا به معرفی گسترش اکوسیستم ارزهای دیجیتالی پرداخته که نیاز به ایجاد برنامه‌های دادوستد را ایجاب می‌کند. مبادلات ارز دیجیتالی را می‌توان دودسته مبادلات متمرکز[1] و مبادلات غیرمتمرکز[2] تقسیم کرد. مبادلات متمرکز، به عنوان یک روش تجاری سنتی نیازمند یک نهاد مرکزی به عنوان واسطه برای تکمیل فرآیندهای دادوستد بین کاربران است. بنابراین، ازآنجاکه تمام اعمال کاربران و اموال دیجیتالی تحت نظارت اپراتورهای مرکزی هستند، اعتبار واسطه‌ها نقش حیاتی در این سیستم دادوستد ایفا می‌کند.

به طور معمول هرچند وقت یکبار مشکلات امنیتی و حریم شخصی از مبادلات متمرکز[3] گزارش می‌شوند. برای تسهیل تجارت آزاد و حذف مشکلات امنیتی و حریم شخصی احتمالی مبادلات غیرمتمرکز[4] معرفی شده‌اند تا به کاربران اجازه دهند بدون انتقال ارزهای دیجیتال خود به واسطه آنها مبادله کنند.

Uniswap یکی از برجسته‌ترین پلتفرم مبادلات غیرمتمرکز (DEXS) بوده که بر روی بلاک چین اتریوم ساخته شده است. برخلاف اکثر دادوستدها که خریداران و فروشندگان را برای تعیین قیمت و انجام معاملات باهم مطابقت می‌دهند، Uniswap از مدل بازار ساز خودکار[5] استفاده می‌کند. در این مدل

1-CEX
2-DEX
3-CEXS
4-DEXS
5-AMM

با استفاده از قراردادهای هوشمند استخرهای نقدینگی ایجادشده که به طور خودکار بر اساس الگوریتم‌های از پیش تعیین شده خریدوفروش انجام می‌شود. در مبادلات غیرمتمرکز (DEX) هر کس می‌تواند با پرداخت هزینه‌ای ناچیز برای جابجایی بین ارزهای دیجیتال از استخرها استفاده کند. Uniswap یک DEX (صرافی غیرمتمرکز) پیشرو بوده که بر روی اتریوم و برای تسهیل مبادله تراکنش‌های خودکار بین توکن‌های اتریوم (ERC-20) و عرضه خودکار نقدینگی ساخته شده است. Uniswap بزرگترین صرافی غیرمتمرکز ارز دیجیتال بر اساس حجم مبادله روزانه تا زمان این مطالعه است. Uniswap V1، اولین نسخه از پروتکل، در نوامبر ۲۰۱۸ توسط Adams Hayden ایجاد شد و از تمام استخرهای نقدینگی ETH به ERC-20 پشتیبانی می‌کند. در ماه می ۲۰۲۰، Uniswap نیز نسخه V2 خود را با بسیاری از ویژگی‌ها و بهینه‌سازی‌های جدید راه‌اندازی کرد.

محبوبیت روزافزون Uniswap به مرور باعث جذب کلاهبرداران شده است. Uniswap هیچ قانون یا معیاری را برای لیست ارزهای دیجیتال در نظر نمی‌گیرد، به این معنی که هرکسی می‌تواند یک توکن را برای تبادل ثبت کند. کلاهبرداران بسیاری تا کنون از این فرصت برای ثبت توکن‌های جعلی و فریب دادن کاربران ناآگاه استفاده کرده‌اند.

در این مقاله، پژوهشگران سعی بر ارائه روشی جهت تشخیص و شناسایی نشانه‌های کلاهبرداری در Uniswap ارائه می‌کنند. ابتدا تمامی تراکنش‌های مربوط به مبادله Uniswap جمع‌آوری و از زوایای مختلف بررسی می‌شود، سپس یک رویکرد چندکاره برای پرچم‌گذاری توکن‌های جعلی استخرهای نقدینگی کلاهبرداری در Uniswap ارائه خواهد شد.

در مرحله بعد به طور دستی یک مجموعه داده از معیارهای توکن جعلی برچسب‌گذاری شده تا ویژگی‌های انواع رمز ارزها شناخته و متمایز شوند. رویکرد تشخیص در این پژوهش با روش بسط مبتنی بر جرم به وسیله ارتباط، تکنیک تشخیص و راستی آزمایی مبتنی بر یادگیری ماشین است.

جمع‌آوری مجموعه داده: در این پژوهش برای جمع‌آوری رویدادهای تراکنش (همچون mintswap و سوزاندن) مربوط به Uniswap از یک رویکرد گراف جعبه شنی به منظور جستجوی داده و نقاط پایانی برای توسعه‌دهندگان بلاک چین استفاده شده است. این گراف یک تصویر لحظه‌ای از وضعیت فعلی Uniswap را ارائه کرده و همچنین تاریخچه داده‌ها را ردیابی می‌کند. لازم به ذکر است که برخی اطلاعات مهم نظیر لاگ‌های مربوط به مقادیر معامله در تراکنش‌ها ثبت نخواهد شد. تمام توکن‌ها و رویدادها را از پنجم می ساعت UTC 00:21 تا ششم دسامبر ساعت UTC 00:18 2020 جمع‌آوری شده است (جدول ۱ نمای کلی از مجموعه داده را نشان می‌دهد). Uniswap تعداد زیادی توکن را جذب کرده و یک محیط تجاری موفق ایجاد کرده است. با این وجود، بسیاری از استخرهای نقدینگی موجود به علت نقدینگی پایین برای مصارف بلندمدت ایجاد نشده‌اند.

تحقیقات اولیه نشان می‌دهند که کلاهبرداران معمولاً توکن‌ها و استخرها را به دلیل عدم وجود مقررات مناسب ثبت می‌کنند. پروژه‌های هدف، توکن‌های رسمی مانند USDT بوده که قبلاً در پروژه‌های Uniswap منتشرشده‌اند.

علاوه بر این، استخرهای کلاهبرداری معمولاً کوتاه مدت هستند زیرا این افراد پس از افتادن قربانیان در تله مربوطه نقدینگی را حذف می‌کنند. این نشان می‌دهد که توکن‌های جعلی و استخر نقدینگی در مقایسه با سایر توکن‌ها/پول‌های معمولی، ویژگی‌های کاملاً منحصر به فردی دارند. این ویژگی‌ها می‌توانند برای تشخیص توکن‌های کلاهبرداری از نمونه‌های معمولی استفاده شود.

گردش کار کلی چهارچوب پیشنهادی تشخیص کلاهبرداری در شکل شماره ۱ آورده شده است.

در این شکل برچسب‌زنی حقیقی پایه هر جزء (component labeling truth Ground) برای جمع‌آوری توکن‌های رسمی (عادی) و قابل اعتمادترین توکن‌های جعلی است. مؤلفه جرم به واسطه‌ی مشارکت برای توسعه مجموعه داده توکن‌های جعلی براساس دو روش اکتشافی قابل اعتماد به کار گرفته می‌شود.

نهایتاً مؤلفه تشخیص و تأیید کلاهبرداری مبتنی بر یادگیری ماشین جهت شناسایی بیشتر توکن‌های جعلی براساس ویژگی‌های آموخته شده از مجموعه داده برچسب خورده به کار گرفته می‌شود. برای از بین بردن موارد مثبت کاذب احتمالی نیز از یک استراتژی راستی آزمایی سختگیر فقط برای برچسب‌گذاری قابل اعتمادترین توکن‌های جعلی استفاده خواهد شد.

در واقع رویکرد اصلی ویژگی‌های نام‌گذاری و رفتارهای معامله توکن‌های جعلی را در نظر می‌گیرد.

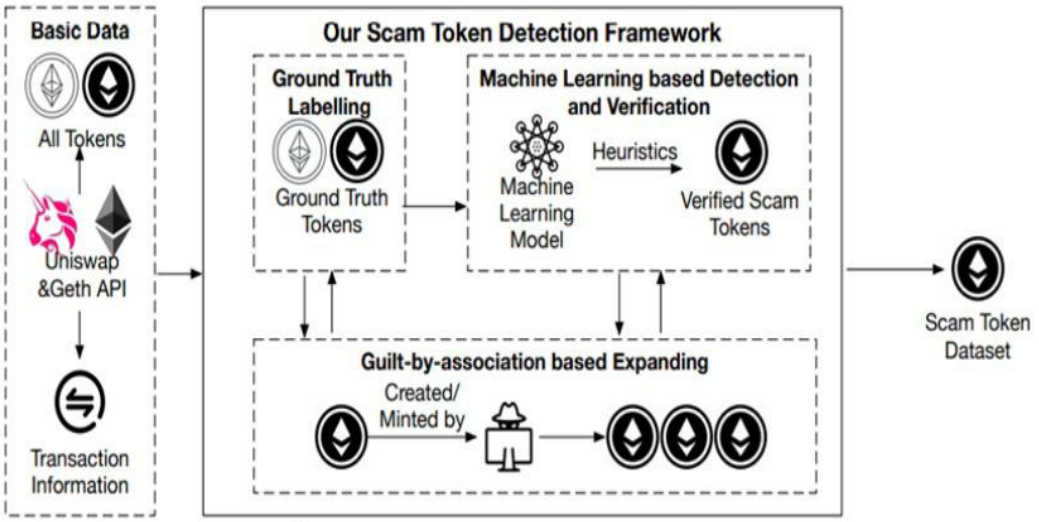
برچسب‌زدن حقیقت پایه

توکن‌های رسمی: برای شناسایی توکن‌های رسمی ابتدا لیستی از توکن‌های محبوب از رتبه‌بندی CoinMarketCap، برای شبکه Etherscan جمع‌آوری می‌شود. سپس با بررسی برخی معیارها نظیر چک کردن صرافی‌های معتبر تأیید دستی آنها انجام خواهد شد. توکن‌های رسمی محبوب معمولاً در CEXهای بزرگ فهرست شده و توسط اپراتورها تائید می‌شوند.

توکن‌های جعلی: اتریوم هیچگونه محدودیتی در نام و نماد توکن‌های جدید اعمال نمی‌کند برخی از توکن‌های جعلی از نام‌های شناسایی مشابه با توکن‌های رسمی قدیمی استفاده می‌کنند.

Data Type	# of Entities	Event Type	# of Events
Token	21,778	Mint	804,077
Pair (pool)	25,131	Burn	415,919
Events	20,306,762	Swap	19,086,766

جدول ۱ : نمای کلی از مجموعه داده جمع‌آوری‌شده



شکل ۱ : نمای کلی از مجموعه داده جمع‌آوری‌شده

همانطور که Etherscan معمولاً توکن‌های فیشینگ یا کلاهبرداری را علامت‌گذاری می‌کند، در این پژوهش نیز یک کاوشگر برای جمع‌آوری برچسب‌ها برای این نوع موارد پیاده‌سازی شده است.

بسط مبتنی بر جرم به واسطه مشارکت:

از نظر تجربی، کلاهبرداران معمولاً بیش از یک توکن جعلی ایجاد می‌کنند تا مقیاس کمپین‌های کلاهبرداری خود را بزرگتر کنند. بنابراین، در این روش تمام حساب‌های اتریوم مربوط به یک توکن جعلی یا استخر نقدینگی (یعنی استخری که توکن‌های کلاهبرداری را معامله می‌کند) برچسب‌گذاری خواهد شد. در واقع سایر توکن‌ها/استخرهای ایجاد شده توسط این سازندگان، به شدت مشکوک به کلاهبرداری هستند. این استراتژی «جرم به واسطه مشارکت» نامگذاری شده است.

روش تشخیص: نتایج حاصل از مرحله برچسب‌زدن حقیقت پایه در مجموعه داده برای آموزش یادگیری ماشین طبقه‌بندی شده و جهت شناسایی سایر توکن‌های کلاهبرداری استفاده خواهند شد. این مرحله فقط می‌تواند آشکارترین توکن‌های کلاهبرداری را علامت‌گذاری کنند. با این حال، بسیاری از توکن‌های دیگر وجود داشته که فروش را برای پروژه‌های محبوب DeFi جعل می‌کنند. محققان برای این منظور به ارائه پردازش دیگری جهت شناسایی توکن‌های جعلی با توجه به رفتار تراکنش‌ها در Uniswap پرداخته‌اند. در این راهکار ابتدا یک طبقه‌بندی کننده یادگیری ماشین آموزش داده شده و بر تمام توکن‌های بدون برچسب اعمال می‌شود. سپس توکن‌های مشکوک و پرچم‌گذاری شده بررسی و روش‌های اکتشافی قابل اعتماد برای تأیید آنها انجام خواهد شد (شامل بررسی‌های دستی نشانه‌ها). لازم به ذکر است که برای توکن‌های کلاهبرداری جدید نیز روش گسترش بررسی می‌شود (بسط مبتنی بر جرم به واسطه مشارکت).

بر اساس تجزیه وتحلیل‌های انجام شده در این پژوهش ۱۰، ۹۲۰ توکن کلاهبرداری با اطمینان بسیار بالا علامت‌گذاری شده‌اند. ۴۰۴۸ کلاهبرداری در مرحله برچسب‌زدن حقیقت پایه، ۳,۱۲۲ =(۲, ۴۴۸ + ۶۷۴) مورد براساس بسط مبتنی بر جرم شناسایی شده‌اند. ۳۷۵۰ توکن نیز با استفاده از تکنیک تشخیص و راستی آزمایی مبتنی بر یادگیری ماشین کشف شده است. لازم به ذکر است که این توکن‌های کلاهبرداری با ۱۱۲۱۵ استخر نقدینگی نیز مرتبط هستند.

نتایج آزمایش نشان می‌دهد که معیارهای، Recall Precision و F1 برای مدل مورد استفاده در این پژوهش به ترتیب ۹۶/۴۵٪ ، ۹۶/۷۹ ٪ و ۹۶/۶۲ ٪ است. این نشان دهنده دقت بالای رویکرد مورد استفاده هست. اگرچه طبقه‌بندی کننده مورد استفاده در این پژوهش می‌تواند به نتایج عالی دست یابد، اما نمی‌تواند به دقت ۱۰۰٪ برسد. امری که با توجه به هدف این پژوهش یعنی شناسایی توکن‌های کلاهبرداری در Uniswap مناسب است.

منبع: ماهنامه مرکز تخصصی آپا دانشگاه بین المللی امام خمینی(ره) - شماره ۳۲ - بهار ۱۴۰۱

مرکز آپا دانشگاه سمنان

کارگاه وایرشارک

از معرفی تا تجزیه و تحلیل داده‌ها

برای مردم
پدافند دانش‌بنیان،
حفاظت از زیرساخت‌ها،
تداوم کارکردها

مدرس:
مهندس غزاله مصطفائی علائی
کارشناس ارشد مهندسی کامپیوتر،
فعال حوزه امنیت فناوری اطلاعات

لینک ورود به کارگاه:
http://stm.semnan.ac.ir

روز برگزاری:
۸ آبان ساعت ۹ الی ۱۱

مخاطب: مدیران، کارشناسان و دانشجویان IT

هزینه: رایگان

نصب نرم‌افزار و انجام تمرین در حین کارگاه

اعطای گواهی معتبر از مرکز آپا دانشگاه سمنان
دارای مجوز رسمی از سازمان فناوری اطلاعات ایران

023-31535021 / 023-31535019
@semcert
info.cert@semnan.ac.ir
@semcert_admin

جهت ثبت نام به وب‌سایت https://cert.semnan.ac.ir مراجعه کنید.

تلاش ما
حفظ امنیت
شماست...