ماتریس

۷

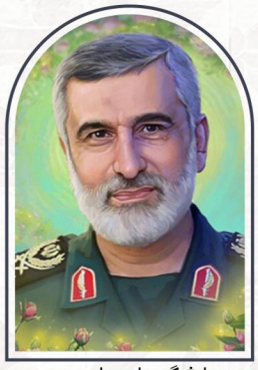
دانشگاه شاهد | انجمن علمی مهندسی کامپیوتر
مهر ۱۴۰۴

در این شماره می‌خوانیم:

سرلشگر پاسدار
شهید محمد باقری

سرلشگر پاسدار
شهید حسین سلامی

سرلشگر پاسدار
شهید غلامعلی رشید



سرلشگر پاسدار
شهید امیرعلی حاجی‌زاده

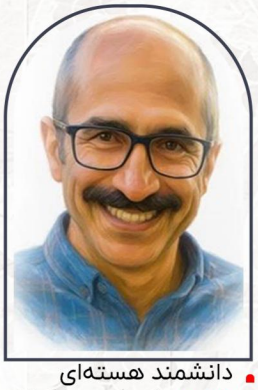
سردار پاسدار
شهید محمدسعید ایزدی

دانشمند هسته‌ای
شهید فریدون عباسی دوانی

دانشمند فیزیک هسته‌ای
شهید عبدالحمید مینوچهر

دانشمند و رئیس دانشگاه آزاد
شهید محمدمهدی طهرانچی

دانشمند فیزیک هسته‌ای
شهید مصطفی ساداتی ارمکی



دانشمند هسته‌ای
شهید علی (منصور) باکویی

دانشجوی دانشگاه شاهد
شهید علی عبدالله پور

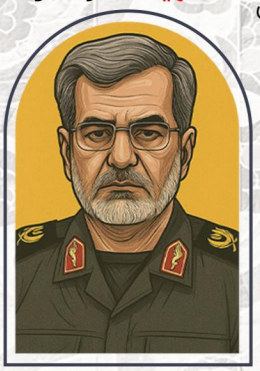
دانشمند فیزیک هسته‌ای
شهید احمدرضا ذوالفقاری

معاون سازمان انرژی اتمی
شهید سید امیرحسین فقهی

دانشمند هسته‌ای
شهید سید ایثار طباطبایی

متخصص و نخبه
شهید محمدرضا ذاکریان

مخترع و نخبه برجسته AI
شهید مجید تجن‌جاری



سرتیپ پاسدار
شهید مهدی ربانی

سرتیپ پاسدار
شهید محمد کاظمی

سرتیپ پاسدار
شهید حسن محقق

سرتیپ پاسدار
شهید غلامرضا محرابی

سرلشگر پاسدار
شهید علی شادمانی

به یاد دانشمندان، مجاهدان و غیور مردم دفاع مقدس ۱۲ روزه

دانشگاه شاهد
دانشگاه تراز انقلاب اسلامی

شناسنامه

نشریه‌ی ماتریس

صاحب امتیاز: انجمن علمی مهندسی کامپیوتر دانشگاه شاهد

مدیر مسئول: محمدمهدی عیوضی

سردبیر: علی کاظم‌پور دیزجی

نویسنده: سید علی عترتی، سید محمد عترتی، مهدی کارزاری وایقان، امیرعباس ادیب انصاری، امیر حسین فهیمی راد، سپهر نوروزی چاکلی و محمد هراتی

ویراستار: سید محمد عترتی، سید علی عترتی و مهدی کارزاری وایقان

طراح: سید علی عترتی، سید محمد عترتی و محمدمهدی قاسمی ابیانه

شماره هفتم - مهر ۱۴۰۴

ماتریس با هدف توسعه‌ی فرهنگ، آگاهی و پژوهش در فناوری‌های نوین و دنیای رایانه، از دی ۱۴۰۳ در انجمن علمی مهندسی کامپیوتر دانشگاه شاهد آغاز به کار کرده است

@MatrisMagazine

فهرست

سخن سردبیر

مرجعیت علمی، ماموریت ملی

از مرجعیت علمی ایران می‌ترسند! ملتی که روزی علم را وارد می‌کرد، امروز صادرکننده است و این مسیر، از دل دانشگاه‌ها می‌گذرد. ما باور داریم که استقلال واقعی، در مرزهای دانش و فناوری تعریف می‌شود.

وظیفه‌ی ما، سرعت بخشیدن به همین مسیر است. ما در هر شماره، به دنبال بهینه‌سازی ساختارها هستیم. ایرانِ علمی، نیاز به به‌روزرسانی مداوم دارد؛ و این، مأموریت ماست.

در این شماره، به مرور تحولات و جنگ دوازده روزه پرداختیم و با نگاهی به رویدادهای فناوری، آینده را از نوآوری‌های امروز ترسیم کرده‌ایم.

از همراهی و حمایت همه دوستان، به‌ویژه آقایان سید علی و سید محمد عترتی، و دانشجویان دغدغه‌مند، صمیمانه سپاسگزارم. به یاری خدا و همت شما، ماتریس در هر نسخه، الگوریتمی تازه از تفکر و نوآوری ایرانی خواهد بود.

علی کاظم‌پور

مختصات جدید ماتریس

همراهان ماتریس سلام.
شکر خدا با حمایت شما برای ارتقای گروه کامپیوتر انتخاب شدیم. در اولین گام قصد داریم بیشتر با هم آشنا شویم و با اعلام وظایف‌مان طبق توانایی‌ها و مهارت‌ها به سوی آینده گام برداریم.

محمد مهدی عیوضی

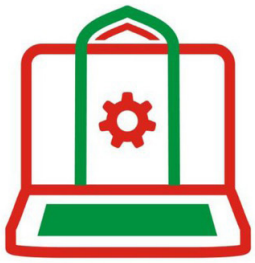
دبیر و راهبر انجمن
رهبری، مدیریت و هماهنگی اعضا، تعیین اهداف، نظارت بر فعالیت‌ها و نماینده انجمن در برابر دانشگاه.

فرید فیضی

نائب دبیر و مسئول مالی
کمک به دبیر در انجام وظایف، نظارت بر امور، مدیریت امور مالی از جمله بودجه‌بندی، ثبت درآمدها و هزینه‌ها و ارائه گزارش آن.

محمد کمال طایفه

مسئول علمی و اجرایی
طراحی، برنامه‌ریزی و انجام امور اجرایی و رویدادهای علمی مانند دوره، کارگاه آموزشی، نشست، مسابقه و بازدید.



انجمن علمی مهندسی کامپیوتر
دانشگاه شاهد

علی کاظم‌پور

دبیر و مسئول نشریه
مدیریت، تولید و انتشار نشریه‌ی انجمن، دریافت، داوری، ویرایش و صفحه‌آرایی مطالب. تشکیل و هدایت تیم نویسندگان و هیئت تحریریه.

سید علی چاوشی

مسئول پژوهشی، صنفی و تحصیلی
طراحی، اجرا و همراهی با فعالیت‌های پژوهشی، رسیدگی به مسائل و مشکلات صنفی و تحصیلی دانشجویان رشته.

محمد فاتح

مسئول رسانه و ارتباطات
مدیریت و تولید محتوای تارنماهای انجمن، برقراری ارتباط موثر با دانشگاه‌ها، شرکت‌ها و صنایع مرتبط جهت ایجاد فرصت‌های همکاری.

وقفه‌ای که ما را تعریف کرد...

سید محمد عترتی
سید علی عترتی

در بهار ۱۴۰۴، هیچ‌کس نمی‌دانست تقویم دانشگاه، در آستانه‌ی یک گسست ایستاده است. نیمسال دوم، طبق روال آغاز شد؛ فصلی که قرار بود با همهمه‌ی راهروهای دانشکده فنی، به تابستان بپیوندد. اما زمان، این خط ممتد، ناگهان از هم گسیخت و ما را در برزخی از انتظار رها کرد. این روایتی است از آن ترم ناهمسان؛ ترمی که در حافظه‌ی جمعی ما، بیش از آنکه با تاریخ‌ها شناخته شود، با احساسات به یاد آورده می‌شود.

بهار با تمام پویایی‌اش آغاز شد. تعطیلات کوتاه نوروز، کمی بیش از وقفه‌ای کوتاه، نویدبخش ادامه‌ای قدرتمند بود. اما در پس این آرامش، سایه‌ی رویدادهایی بزرگ‌تر در حرکت بود؛ سایه‌ای که در سحرگاه ۲۳ خرداد، با صدایی مهیب بر سر شهر فرود آمد و سکوت را بر دانشگاه تحمیل کرد.

آن رویداد غافلگیرکننده، نه تنها کلاس‌ها و آزمون‌ها را به تعلیق درآورد، بلکه درک ما از «زمان» را دگرگون ساخت. دانشگاه، که همواره نماد حیات و پایداری بود، برای لحظه‌ای در تاریخ متوقف شد و ما، دانشجویانی که خود را برای فتح قله‌های علم آماده می‌کردیم، در فضایی معلق به نظاره نشستیم.

اما این نظاره، برای هیچ‌یک از ما نباید به معنای سکون و انفعال باشد. در همان روزهای تعلیق و عدم قطعیت، وظیفه‌ی ما به عنوان بخشی از جامعه‌ی علمی، نه تنها فراموش نشد، بلکه سنگین‌تر از همیشه احساس می‌شد. این یک انتخاب بود: می‌توانستیم منتظر بمانیم تا شرایط به حالت عادی بازگردد، یا می‌توانستیم از این وقفه‌ی تحمیلی، فرصتی برای اثرگذاری بسازیم. ما راه دوم را برگزیدیم، زیرا باور داریم که استقلال واقعی یک ملت و پایداری یک جامعه، در مرزهای دانش و فناوری آن تعریف می‌شود.

در میدان نبرد امروز، که مرزهای آن بیش از هر زمان دیگری با دانش و فناوری ترسیم می‌شود، اثرگذارترین ابزار ما، اندیشه، تحلیل و خلاقیت ماست. هر خط کدی که برای حل یک مسئله نوشته می‌شود، هر تحلیلی که برای درک بهتر یک پدیده ارائه می‌گردد و هر ایده‌ای که در مسیر پیشرفت علمی به پختگی می‌رسد، گامی در جهت تقویت بنیان‌های جامعه است. پیام ما باید این باشد: اهل علم، حتی در دل بحران، رسالتی جز جابجا کردن مرزهای دانش و تبدیل تهدیدها به فرصت ندارند. باید ثابت کنیم که سکوت فیزیکی دانشگاه و خالی بودن راهروها، هرگز به معنای توقف تفکر، پژوهش و خلق ارزش نیست، بلکه می‌تواند سرآغازی برای تمرکز عمیق‌تر و جهش‌های فکری بزرگ‌تر باشد.

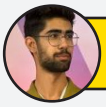
تابستان ۱۴۰۴، فصل تعطیلات نبود؛ فصل تأمل بود. با تعویق امتحانات به شهریور، ماه‌های پیش رو به دورانی برای بازاندیشی بدل شدند. هم‌زمانی این تعلیق با ایام محرم، به این درنگ عمقی دوچندان بخشید. هیئت‌های مسجد دانشگاه، دیگر نه فقط یک آیین، که تبلور پیوند روایت‌های تاریخیِ استقامت با بحرانِ حال بودند. در آن تابستان، ما درسی را آموختیم که در هیچ سرفصلی گنجانده نشده بود:

درس تاب‌آوری در برابر گسست و یافتن معنا در دلِ بی معنایی.

نقطه‌ی اوج این ترم ناهمسان، در تلاقی شهریور و مهر رقم خورد. در حالی که هنوز غبار امتحانات پایان ترم بر شانه‌هایمان سنگینی می‌کرد و نمرات در حال ثبت شدن بود، زنگ آغاز نیمسال جدید به صدا درآمد. ما نسلی هستیم که در یک لحظه‌ی منحصر به فرد تاریخی، همزمان هم درگیر تلاش برای حفظ گذشته بودیم و هم در حال برداشتن نخستین گام‌ها به‌سوی آینده. این تجربه‌ی متناقض، معنای «زمان» و «پیوستگی» را برای همیشه دگرگون ساخت.

اکنون، در پاییز ۱۴۰۴، نشریه «ماتریس» در چنین بستر پرفراز و نشیبی، حیاتی دوباره می‌یابد. این شماره، تنها یک نشریه نیست؛ بلکه نخستین خروجی انجمن علمی جدید مهندسی کامپیوتر و سرآغاز دومین سال فعالیت «ماتریس» است.

فناوری در خط مقدم



مهدی کارزاری

در دنیای امروز، میدان نبرد دیگر صرفاً به گلوله و آتش محدود نمی‌شود. ابزارهای جنگی مدرن، ابعاد جدیدی از درگیری را پیش روی دولت‌ها قرار داده‌اند. سلاح‌های سنتی جای خود را به ابزارهای نامرئی و در عین حال مخرب‌تری داده‌اند؛ سلاح‌هایی که در حوزه جنگ اطلاعاتی و سایبری به کار گرفته می‌شوند.

جنگ اطلاعاتی

جنگ اطلاعاتی نوعی از درگیری نوین است که بر نفوذ در افکار عمومی و ایجاد اختلال در باورها و تصمیم‌گیری‌های جوامع هدف تمرکز دارد. در این جنگ، رسانه‌ها، اخبار جعلی و عملیات‌های روانی جایگزین اسلحه و باروت می‌شوند. هدف، تسخیر ناخودآگاه مردم و هدایت آنها به سمت تصمیماتی از پیش برنامه‌ریزی‌شده است؛ تصمیماتی که به ظاهر با اراده‌ی خود آن‌ها گرفته می‌شوند، اما در حقیقت طراحی دشمن هستند.

میدان نبرد سایبری

با گسترش فناوری اطلاعات و وابستگی عمیق کشورها به زیرساخت‌های دیجیتال، حملات سایبری به یکی از رایج‌ترین و مؤثرترین اشکال نبرد تبدیل شده‌اند. در چنین نبردهایی، مهاجمان با نفوذ به **شبکه‌های ارتباطی، به دنبال تحقق سه هدف اصلی هستند :**

- نفوذ به سامانه‌ها
- ایجاد خرابکاری در عملکرد آن‌ها

- سرقت یا نابودی اطلاعات حیاتی

جنگ سایبری در جریان درگیری ۱۲ روزه

در جریان جنگ ۱۲ روزه میان ایران و اسرائیل، حملات سایبری گسترده‌ای به زیرساخت‌های حیاتی کشور صورت گرفت. گروه‌های مهاجم، منتسب به رژیم صهیونیستی و شناخته‌شده با نام‌های مختلف APT، اهداف مهمی از جمله دو نهاد مالی کلیدی کشور را هدف قرار دادند:

۱. بانک سپه

۲. صرافی ارز دیجیتال نوبیتکس

هک بانک سپه؛ حمله‌ای برنامه‌ریزی‌شده

بانک سپه به عنوان یکی از اصلی‌ترین بانک‌های کشور، نقش کلیدی در پرداخت حقوق نیروهای نظامی و سایر امور مالی کشور را ایفا می‌کند. از این رو، انتخاب آن به‌عنوان هدف حمله سایبری، انتخابی دور از ذهن نیست، آن هم در زمانی که کشور درگیر جنگ مستقیم است.

بر اساس گزارش‌های رسمی و تحلیل‌های فنی، گروه هکری گنجشک درنده (منتسب به رژیم صهیونیستی) که مسئولیت این حمله را بر عهده گرفت، با استفاده از آسیب‌پذیری‌های موجود در سامانه‌های بانک سپه، اقدام به نفوذ، تخریب اطلاعات و مختل‌سازی زیرساخت‌های حیاتی بانک کرد.

تحلیل‌های انجام‌شده نشان می‌دهد مهاجمان از طریق درگاه‌های مدیریتی سرورهای HP موسوم به ILO (Integrated Lights-Out) که به‌اشتباه به اینترنت متصل بودند، موفق به نفوذ شده‌اند. این پورت‌ها امکان دسترسی کامل سخت‌افزاری به سرورها را فراهم می‌کنند، و در این مورد، به‌دروازه‌ای مخرب برای نفوذ به عمق شبکه بانکی تبدیل شده‌اند.

حمله به بانک سپه، با هدف سرقت اطلاعات صورت نگرفته بود؛ بلکه ماهیت آن کاملاً تخریبی بود. مهاجمان با نفوذ به تجهیزات ذخیره‌سازی، اطلاعات حیاتی را به‌طور کامل پاک کرده و حتی نسخه‌های پشتیبان (Backup) را نیز نابود کردند. در برخی موارد، سیستم‌ها پس از بازیابی نیز مجدداً آلوده شدند، که نشان‌دهنده‌ی دسترسی عمیق و پایدار مهاجمان بوده است.

گزارش‌ها حاکی از آن است که بین ۳۰۰ تا ۴۰۰ سرور فیزیکی بانک سپه تحت تأثیر مستقیم حمله قرار گرفتند و نیاز به بازسازی کامل یا جایگزینی داشتند. شدت حمله به‌گونه‌ای بود که خدمات مختلف بانکی شامل برداشت، انتقال وجه، پرداخت حقوق و تراکنش‌های کارت‌های بانکی برای مدت‌ها متوقف یا با اختلال شدید همراه شدند.

یکی از نقاط ضعف حیاتی که در این حمله آشکار شد، عدم وجود یک سایت پشتیبان فعال مناسب بود. این ضعف موجب شد بانک سپه نتواند به‌سرعت عملیات بازیابی را آغاز کند و بازگشت به وضعیت عادی، ماه‌ها به‌طول انجامید.

پس از این حمله، شرکت داتین (ارائه‌دهنده زیرساخت نرم‌افزاری بانک سپه) در بیانیه‌ای اعلام کرد که منشأ حمله، ماهیت

سخت‌افزاری داشته و ارتباطی با افشای داده‌های پیشین در سامانه‌های نرم‌افزاری آنها نداشته است.

هک و سوزانده شدن بیش از ۵۰ میلیون دلار

در میانه‌ی روزهای پرتنش جنگ ۱۲ روزه میان ایران و اسرائیل، خبر یک حمله سایبری تازه در فضای دیجیتال کشور پیچید؛ حمله‌ای که نه پالایشگاه بود، نه بانک، بلکه صرافی رمزارز نوبیتکس (بزرگترین بستر مبادله رمزارز در ایران) را هدف گرفته بودند. حمله‌ای که ظرف چند ساعت، میلیون‌ها دلار دارایی دیجیتال کاربران را از بین برد و ردی عمیق از خود در تاریخ امنیت سایبری ایران بر جای گذاشت.

بر اساس گزارش‌های رسمی و تأیید منابع فنی، عملیات توسط گروه هکری گنجشک درنده انجام شد؛ همان گروهی که پیشتر مسئولیت حمله به بانک سپه را برعهده گرفته بود. الگوی رفتاری این گروه همیشه مشخص است: حمله‌ای سریع، دقیق و پر از پیام‌های روانی. در این مورد هم، برخلاف حملات معمول سایبری که با هدف سرقت و فروش دارایی انجام می‌شوند، هدف اصلی ظاهراً تخریب و ایجاد بی‌ثباتی بود.
نوبیتکس در روز ۲۸ خرداد ۱۴۰۴ هدف قرار گرفت. بر اساس تحلیل‌های فنی، مهاجمان نه از بیرون دیوارهای امنیتی، بلکه از داخل شبکه سازمانی نفوذ کرده بودند. بررسی‌ها نشان می‌دهد که منشأ حمله نه صرفاً یک آلوده‌سازی عمومی، بلکه نشت اطلاعات احراز هویت از طریق بدافزارهای استیلر (Stealer Malware) بوده است. بر روی تعدادی از سیستم‌های شخصی مرتبط با تیم داخلی، بدافزارهایی شناسایی شده که پیش‌تر اقدام به جمع‌آوری و ارسال داده‌های حساس از جمله نام کاربری و گذرواژه‌ها کرده بودند. یکی از این مجموعه داده‌ها شامل نام کاربری و رمز عبور یکی از ادمین‌های اصلی نوبیتکس بود. همین افشای ساده اما حیاتی، نقطه‌ی ورود مهاجمان به زیرساخت داخلی صرافی را فراهم کرد و در نهایت مسیر اجرای کامل حمله را هموار ساخت.

پس از نفوذ، مهاجمان بلافاصله به سراغ زیرساخت مدیریت تراکنش و امضای دیجیتال صرافی رفتند؛ جایی که کلیدهای خصوصی کیف‌پول‌های گرم (Hot Wallets) نگهداری می‌شد. این کیف‌پول‌ها، به دلیل اتصال مستقیم به اینترنت برای انجام تراکنش‌های روزمره کاربران، همواره آسیب‌پذیرترین بخش هر صرافی رمزارز هستند.

اما ویژگی خاص این حمله در همینجا بود: بخش قابل توجهی از رمزارزهای منتقل‌شده. بیش از پنجاه میلیون دلار. به آدرس‌هایی فرستاده شد که هیچ کلید خصوصی برای آنها وجود ندارد. به بیان ساده‌تر، این دارایی‌ها عملاً «سوزانده» شدند؛ برای همیشه از بین رفتند و امکان بازیابی شان وجود ندارد. این اقدام آشکارا نشان می‌دهد که هدف مهاجمان، نه سرقت مالی، بلکه تخریب اقتصادی و روانی بوده است.

گزارش‌ها نشان می‌دهد که نخستین تراکنش‌های مشکوک در ساعت ۰۷:۵۸ صبح آغاز شده‌اند و عملیات ظرف کمتر از نیم ساعت به پایان رسیده است. همزمان، اختلال شدید اینترنت در کشور، روند واکنش اضطراری تیم امنیتی نوبیتکس را کند کرد. ارتباط با دیتاسنترها قطع شده بود و تیم فنی نمی‌توانست در لحظه واکنش نشان دهد یا کیف‌پول‌های باقی مانده را تخلیه کند. همین تأخیر چند دقیقه‌ای، حجم خسارت را چند برابر کرد.

پس از آنکه تیم مانیتورینگ حمله را شناسایی کرد، بلافاصله اقدامات اضطراری از جمله قطع دسترسی‌های مشکوک، ایزوله‌سازی سرورها، تخلیه باقیمانده موجودی کیف‌پول‌های گرم و انتقال فوری آنها به کیف‌پول‌های سرد (Cold Wallets) که به اینترنت متصل نبودند آغاز شد.

چند ساعت بعد، نوبیتکس با انتشار اطلاعیه‌ای، وقوع حمله را تأیید و اعلام کرد که «دارایی کاربران از بین نخواهد رفت». مدیرعامل صرافی نیز در بیانیه‌ای رسمی مسئولیت کامل حادثه را پذیرفت و وعده داد که خسارات وارده از محل منابع داخلی جبران خواهد شد.

به گفته منابع نزدیک به شرکت، این فرآیند طی ماه‌های بعد انجام شد و بخش عمده دارایی کاربران بازپرداخت گردید.

اما از منظر فنی، این حادثه یک زنگ خطر جدی بود. بررسی‌ها نشان داد که کلیدهای خصوصی برخی کیف‌پول‌ها روی سیستم‌های داخلی ذخیره شده و از ماژول‌های سخت‌افزاری مدیریت کلید (HSM) یا سامانه‌های ایزوله استفاده نشده بود. همچنین، ساختار شبکه نوبیتکس فاقد معماری «Zero Trust» بوده و محیط توسعه و عملیات به‌صورت کامل از یکدیگر جدا نشده بودند. نبود سامانه واکنش سریع (Incident Response System) و وابستگی بیش از حد به اقدامات انسانی نیز باعث شد زمان طلایی مقابله با حمله از دست برود.

در سطحی گسترده‌تر، این حمله تنها به نوبیتکس آسیب نزد؛ بلکه لرزه‌ای به کل اکوسیستم رمزارز ایران وارد کرد. بسیاری از کاربران دارایی‌های خود را از صرافی‌های داخلی خارج کردند و اعتماد عمومی به امنیت پلتفرم‌های ایرانی برای مدت‌ها کاهش یافت.

کارشناسان امنیت سایبری این رویداد را نخستین نمونه‌ی واقعی از جنگ مالی سایبری در خاورمیانه می‌دانند: حمله‌ای نه به‌دنبال پول، بلکه به‌دنبال فروپاشی اعتماد و ضربه به ثبات اقتصادی...

نابرده رنج، هک میسر نمی‌شود:)

امیرعباس ادیب انصاری

در جهانی که هر روز خبر از حملات سایبری تازه‌ای می‌رسد، امنیت دیجیتال دیگر یک مهارت تخصصیِ محدود به کارشناسان نیست، بلکه به ضرورتی همگانی بدل شده است. همه در برابر تهدیدهای اینترنتی آسیب‌پذیرند. حال پرسش این است: چگونه می‌توان هکر شد، بدون آنکه به کسی آسیبی رساند؟ پاسخ در فضایی نهفته است که مرز میان بازی و آموزش را از میان برداشته است؛ یعنی TryHackMe. این وب‌سایت انقلابی در یادگیری امنیت سایبری به‌پا کرده است. برخلاف کلاس‌های نظری، در TryHackMe، یادگیری با تجربه واقعی گره خورده؛ جایی که به دنیایی مجازی از شبکه‌ها، سامانه‌ها و تهدیدات وارد می‌شوی و در نقش هکر، تحلیل‌گر یا مدافع امنیتی ظاهر می‌گردی.

این وب‌سایت در سال ۲۰۱۸ توسط اشو ساوانی (Ashu Savani) و بن اسپرینگ (Ben Spring) ساخته شد. آن‌ها با انگیزه ساختن چیزی ساده، ارزان و عملی کار را شروع کردند و به‌سرعت علاقه جامعه امنیت باعث رشدشان شد. این آغازِ حرکتی بود که حالا میلیون‌ها کاربر دارد و دانشگاه‌ها و شرکت‌ها از آن استفاده می‌کنند.

در گزارش رسمی سال ۲۰۲۴ اعلام شده که بیش از چهار میلیون نفر از این وب‌سایت استفاده کرده‌اند و صدها سازمان بزرگ از آن برای آموزش نیروهای خود بهره می‌برند. در واقع، این وب‌سایت فقط برای یادگیری فردی نیست؛ شرکت‌ها نیز با استفاده از آن می‌توانند توانمندی کارکنانشان را بسنجند یا ارتقا دهند.

در ظاهر، TryHackMe فقط یک وب‌سایت آموزشی است، اما در باطن، دنیایی است که قواعد خودش را دارد. هر درس، یک «اتاق» است و هر اتاق، سناریویی واقعی از دنیای هک و امنیت سایبری. گاهی مأموریت داری تا به یک سرور نفوذ کنی و با یافتن نقاط ضعف، پرچم دیجیتالی‌اش را به‌دست آوری. گاهی هم در نقش تحلیل‌گر امنیت، باید ردپای یک مهاجم را دنبال کنی و بفهمی چه چیزی باعث نفوذ شده است.

این سایت از بخش‌های متعددی تشکیل شده است: Dashboard برای مشاهده‌ی پیشرفت، Rooms به‌عنوان اتاق‌های تمرین شامل توضیحات، مراحل و محیط عملی، و Learning Paths که مجموعه‌ای از اتاق‌ها را به‌صورت مسیر آموزشی منظم در اختیار کاربر قرار می‌دهد. بخش AttackBox یا آزمایشگاه، محیطی ایمن برای اجرای دستورات و حملات شبیه‌سازی‌شده فراهم می‌کند، در حالی که بخش Practice برای سنجش مهارت‌ها و تجربه‌ی واقعی در سناریوهای مختلف طراحی شده است.

آنچه TryHackMe را متمایز می‌کند، حس زنده‌بودن تجربه است. هیچ آموزش ویدئویی یا کتابی نمی‌تواند جای لحظه‌ای را بگیرد که خودت دستورها را می‌نویسی، خطا می‌کنی، به بن‌بست می‌رسی و دوباره راه‌حل تازه‌ای پیدا می‌کنی. این بستر طوری طراحی شده که یادگیری در آن، با کشف و هیجان همراه است نه حفظ کردن فرمول‌ها.

جذابیت دیگر TryHackMe سادگی ورود به آن است. نیازی به نصب ماشین مجازی یا پیکربندی سیستم نداری؛ همه‌چیز از درون مرورگر انجام می‌شود. با چند کلیک، یک محیط مجازی اختصاصی در اختیارت قرار می‌گیرد که می‌توانی در آن تمرین کنی، بدون ترس از خراب کردن سیستم اصلی‌ات. همین سادگی هزاران علاقه‌مند تازه‌کار را وارد این دنیای جذاب کرده است.

اما شاید بخش خلاقانه‌تر ماجرا، نحوه‌ی روایت آموزش باشد. TryHackMe مانند یک بازی داستان‌محور عمل می‌کند. هر مرحله روایتی دارد: گاهی در یک شرکت فرضی نفوذی رخ داده و باید عامل آن را شناسایی کنی؛ گاهی مأمور بررسی یک بدافزار می‌شوی. این قالب داستانی، فرآیند یادگیری را از حالت نظری به یک تجربه جذاب و ماجراجویانه تبدیل می‌کند. به‌تدریج، مسیرهای تخصصی‌تر در دسترس قرار می‌گیرد؛ از تست نفوذ تا تحلیل بدافزار و مهندسی معکوس. هر مسیر با تمرین‌های گام‌به‌گام و آزمون‌های کوچک تغذیه می‌شود. در پایان، احساس می‌کنی واقعاً کاری را یاد گرفته‌ای، نه اینکه صرفاً متنی را خوانده باشی.

یکی از داستان‌های موفقیت، داستان Angus است که با استفاده از مسیرهای TryHackMe در زمان فراغت، در نهایت به‌عنوان تحلیل‌گر امنیت مشغول به کار شد. او می‌گوید که مسیرهای آموزشی و ساختار واضح آن به او کمک کرده تا مرحله‌به‌مرحله رشد کند. داستان‌های متعدد دیگری نیز از افرادی وجود دارد که بدون زمینه تخصصی وارد حوزه امنیت شده‌اند و مسیر شغلی خود را تغییر داده‌اند. در میان دانشجویان، بسیاری این سایت را نخستین پله‌ی ورود به دنیای واقعی هک اخلاقی می‌دانند.

البته این وب‌سایت فقط برای تازه‌کارها نیست. برای کاربران حرفه‌ای چالش‌های پیچیده‌تری طراحی شده که شبیه به شرایط واقعی حملات سازمانی است. در چنین اتاق‌هایی، هیچ راهنمای دقیقی نیست و باید با تکیه بر تجربه و خلاقیت، نفوذ را تحلیل و راه دفاع را پیدا کرد. این رویکرد باعث می‌شود متخصصان باتجربه هم مهارت‌هایشان را بهتر کنند و روش‌های جدید را امتحان کنند.

یکی دیگر از ابعاد جذاب TryHackMe، جنبه‌ی اجتماعی و تعاملی آن است. کاربران در انجمن‌ها گفت‌وگو می‌کنند، تجربه‌ها را به اشتراک می‌گذارند و تیم تشکیل می‌دهند. این حس تعلق به جامعه‌ای جهانی از هکرهای اخلاقی، در بقیه کلاس‌ها به‌ندرت یافت می‌شود.

با این حال، TryHackMe بی‌نقص نیست. برخی منتقدان معتقدند چون بسیاری از تمرین‌ها با راهنمای مرحله‌به‌مرحله ارائه می‌شود، کاربران ممکن است صرفاً دستورها را کپی کنند بدون آنکه بفهمند چرا این روش کار می‌کند. همین مسئله سبب می‌شود یادگیری سطحی بماند.

از سوی دیگر، بخشی از محتوای پیشرفته در حالت اشتراک پولی قرار دارد و کاربران رایگان به بخشی از مسیرها دسترسی دارند. این سیاست مالی قابل‌درک است، زیرا نگهداری و توسعه چنین زیرساختی هزینه‌بر است. با این حال، بسیاری از دانشگاه‌ها با خرید اشتراک گروهی، این امکان را برای دانشجویان خود فراهم کرده‌اند تا بدون پرداخت شخصی، از امکانات کامل بهره‌مند شوند، که جا دارد در کشور خودمان نیز دانشگاه‌ها به این موضوع توجه داشته باشند.

این ابزار صرفاً وب‌سایتی برای یادگیری هک نیست، بلکه پلی است میان دانش، تجربه و تخیل؛ جایی که امنیت نه به‌عنوان دیواری برای محدود کردن، بلکه به‌عنوان هنری برای حفاظت و خلاقیت شناخته می‌شود.

داستان کانتینرها؛
اینجا کار میکنه ولی اونجا نه!!!

امیر حسین فهیمی

روزی روزگاری در گوشه‌ای از این کره خاکی، عده‌ای برنامه‌نویس بودن که انصافاً برنامه‌های خوب و تمیزی می‌نوشتن. اما یک مشکل بزرگ داشتن: برنامه‌هاشون روی سیستم‌های همدیگه اجرا نمی‌شد!
موقع برنامه‌نویسی، انتخاب زبان، کتابخانه‌ها و پکیج‌ها هم متفاوت می‌شد. همین تفاوت‌ها باعث می‌شد که توسعه تیمی کند و دشوار بشه.
و اینجاست که ایدهٔ کانتینر متولد شد: یک راه حل ساده برای یک مشکل بزرگ.

ساده‌ترین تشبیه برای کانتینر، کانتینرهای حمل بار در دنیای واقعی است. فرقی نمی‌کند داخل کانتینر موز باشد یا قطعات ماشین؛ خود کانتینر یک استاندارد مشخص دارد و هر کشتی یا جرثقیلی می‌تواند آن را جابجا کند.
در دنیای نرم‌افزار هم کانتینر دقیقاً همین کار را می‌کند: یک بسته استاندارد که برنامه و تمام وابستگی‌هایش (کتابخانه‌ها، تنظیمات و...) را در خودش جا می‌دهد. این بسته در هر محیطی (لپ‌تاپ توسعه‌دهنده، سرور تست، یا فضای ابری) به یک شکل اجرا می‌شود و مشکل «فقط روی سیستم من کار می‌کنه!» را برای همیشه حل می‌کند.

۱۹۷۹: اولین جرقه – chroot در UNIX

در سال ۱۹۷۹، قابلیتی به نام chroot در UNIX عرضه شد.
chroot یک «ریشهٔ ساختگی» برای فایل‌سیستم ایجاد می‌کرد؛ به‌طوری‌که برنامه فکر می‌کرد کل سیستم فقط همون پوشه‌ایه که براش تعیین شده.
- این اولین قدم در مسیر ایزوله‌سازی بود.
ولی محدودیت داشت: فقط فایل‌سیستم رو جدا می‌کرد، نه منابع دیگه مثل شبکه، پردازه‌ها یا حافظه.

۲۰۰۰: FreeBSD Jails

در حوالی سال ۲۰۰۰، پروژه‌ی FreeBSD Jails توسعه یافت. این قابلیت طراحی شد تا روی یک سرور واحد، بتوان چند محیط ایزوله و امن برای سرویس‌های مختلف (وب‌سرور، ایمیل، FTP و ...) اجرا کرد.
- این نقطه‌ی عطفی در تکامل ایزوله‌سازی سیستم‌ها بود.

شاخهٔ موازی: Virtual Machines و Hypervisors (دهه ۱۹۹۰–۲۰۰۰)

یک مسیر جداگانه در دنیای فناوری هم شکل گرفت: مجازی‌سازی (Virtualization).
اینجا مکانیزم ایزوله‌سازی به‌وسیله‌ی Hypervisor انجام می‌شد: هر ماشین مجازی یک سیستم‌عامل کامل (Guest OS) داشت و منابع سخت‌افزار به‌طور کامل شبیه‌سازی و جدا می‌شد.
VMها پایه‌گذار دیتاسنترهای مدرن شدند، اما بعدها کانتینرها با هزینه کمتر و سرعت بالاتر به‌عنوان رویکردی متفاوت برای ایزوله‌سازی در سطح سیستم‌عامل معرفی شدند.

در یک نگاه:
ماشین مجازی (VM): سخت‌افزار را مجازی می‌کند. هر VM یک سیستم‌عامل کامل و مجزا (Guest OS) دارد و به همین دلیل سنگین‌تر است.
کانتینر: سیستم‌عامل را مجازی می‌کند. همه کانتینرها از هسته (Kernel) سیستم‌عامل میزبان (Host OS) به صورت مشترک استفاده می‌کنند و به همین دلیل بسیار سبک و سریع هستند.

۲۰۰۶ تا ۲۰۱۳: پایه‌گذاری فناوری کانتینر در لینوکس

در این بازه‌ی زمانی، سه ستون اصلی فناوری کانتینر در لینوکس شکل گرفت:

۱. cgroups (۲۰۰۶): این قابلیت که توسط مهندسان گوگل توسعه یافت، امکان مدیریت و محدودسازی منابعی مثل CPU و حافظه را فراهم کرد.

۲. Linux Namespaces (۲۰۰۲-۲۰۱۳): این ویژگی به فرایندها یک «دید ایزوله» از سیستم می‌دهد. برای مثال، یک فرایند در یک Namespace شبکه، فقط پورت‌ها و کارت‌های شبکه خودش را می‌بیند، نه کل سیستم را.

۳. LXC (۲۰۰۸): این پروژه اولین ابزاری بود که cgroups و namespaces را با هم ترکیب کرد تا یک محیط کانتینری کامل و کاربردی ارائه دهد. LXC را می‌توان پدربزرگ داکر نامید.

۲۰۱۳: تولد Docker – انقلاب در دنیای کانتینرها

در سال ۲۰۱۳، پروژه‌ای به نام Docker معرفی شد که توانست فناوری‌های پیچیده‌ای مثل cgroups و namespaces را به شکل ساده، قابل‌فهم و کاربردی برای همه ارائه دهد. داکر در ابتدا بر پایهٔ LXC ساخته شده بود، اما کمی بعد به سوی libcontainer، یعنی runtime اختصاصی خودش، مهاجرت کرد.

هنر داکر در چند نوآوری کلیدی بود:

معرفی مفهوم ایمیج (Image): داکر یک «نقشه ساخت» یا «قالب» به نام ایمیج را معرفی کرد. ایمیج یک بسته ثابت و غیرقابل تغییر است که تمام نیازمندی‌های یک برنامه را در خود جای داده است. در واقع، کانتینر یک نمونهٔ در حال اجرا از یک ایمیج است.

استفاده از ایمیج‌های لایه‌ای (Layered Images): هوشمندی اصلی داکر، طراحی لایه‌ای ایمیج‌ها بود. هر دستورالعمل در فرآیند ساخت، یک لایه جدید ایجاد می‌کند. این ساختار باعث صرفه‌جویی فوق‌العاده در فضا و افزایش سرعت شد، زیرا لایه‌های مشترک بازاستفاده می‌شوند.

ایجاد یک ریجستری عمومی (Docker Hub): داکر فضایی شبیه به «گیت‌هاب برای ایمیج‌ها» به نام Docker Hub را فراهم کرد تا توسعه‌دهندگان ایمیج‌های خود را منتشر کرده یا از ایمیج‌های آماده استفاده کنند.

ارائه ابزارهای ساده و توسعه‌محور: داکر با دستورات ساده‌ای مثل `docker run`، `docker build` و `docker push`، فرآیند پیچیده ساخت و مدیریت کانتینرها را روان کرد.

این نوآوری‌ها باعث شدند که کانتینرها از یک فن اوری زیرساختی پیچیده، به ابزاری روزمره برای توسعه‌دهندگان تبدیل شوند و راه را برای جریان‌های مدرنی مثل DevOps و در نهایت Kubernetes هموار کردند.

۲۰۱۵-۲۰۱۶: توافق بر سر یک قانون‌نامه مشترک (OCI)

با محبوبیت داکر، ابزارهای دیگری هم ساخته شدند. این اتفاق یک خطر بزرگ ایجاد کرد: تصور کنید هر شرکت خودروسازی، بنزین مخصوص به خودش را تولید کند!

برای جلوگیری از چنین مشکلی، داکر و بنیاد لینوکس یک قانون‌نامه مشترک به نام Open Container Initiative (OCI) نوشتند.

این قانون‌نامه دو چیز اصلی را مشخص کرد:

۱. یک فرمت استاندارد برای ایمیج‌ها: همه توافق کردند که نقشه ساخت کانتینرها (ایمیج‌ها) باید یک ساختار واحد داشته باشد.

۲. یک روش استاندارد برای اجرا: همه توافق کردند که «موتور» اجراکننده کانتینرها (که به آن Runtime می‌گویند) باید از دستورات یکسانی پیروی کند.

در نتیجه، این توافق باعث سازگاری و آزادی عمل شد و از قفل شدن کاربران به یک ابزار خاص جلوگیری کرد.

۲۰۱۴ تا امروز: مدیریت کانتینرها به روش رهبر ارکستر!

داکر کار را برای اجرا و مدیریت چند کانتینر آسان کرده بود. اما وقتی تعداد کانتینرها به صدها یا هزاران عدد می‌رسید، یک چالش بزرگ به وجود می‌آمد: مدیریت، راه‌اندازی مجدد در صورت خرابی، و تقسیم بار کاری.

اینجا بود که به ابزاری برای رهبری و مدیریت خودکار کانتینرها نیاز پیدا شد. این فرآیند ارکستراسیون (Orchestration) نام گرفت.

در پاسخ به این نیاز، شرکت گوگل در سال ۲۰۱۴ پروژه‌ای متن‌باز به نام Kubernetes را معرفی کرد. Kubernetes که بر پایه تجربه سیستم داخلی خود (Borg) ساخته شده بود، به سرعت به محبوب‌ترین «رهبر ارکستر» در دنیای کانتینرها و استاندارد صنعتی برای مدیریت برنامه‌های بزرگ‌مقیاس بدل گشت.

امروز: یک اکوسیستم بالغ

امروز کانتینرها به ستون فقرات زیرساخت ابری، میکروسرویس‌ها و معماری‌های مدرن نرم‌افزار تبدیل شده‌اند. از سرویس‌های استریم ویدیو گرفته تا اپلیکیشن‌های بانکی و هوش مصنوعی، تقریباً تمام سرویس‌های دیجیتال مدرن بر پایه کانتینرها اجرا می‌شوند.

ویژگی های کلیدی کانتینر های امروزی:

قابلیت حمل (Portability): برنامه‌ای که یک‌بار داخل کانتینر بسته‌بندی بشه، بدون تغییر روی هر محیطی (از لپ‌تاپ تا دیتاسنتر یا کلاود عمومی) اجرا می‌شه.

مقیاس‌پذیری (Scalability): کانتینرها سبک و سریع هستن؛ همین باعث می‌شه هزاران سرویس در کسری از ثانیه بالا یا پایین بیان. این برای معماری‌های میکروسرویسی ضروریه.

یکپارچگی با DevOps: کانتینرها به تیم‌ها اجازه می‌دن چرخهٔ توسعه، تست و استقرار (CI/CD) رو کاملاً خودکار و تکرارپذیر کنن.

استانداردسازی محیط‌ها: از اونجا که همه‌چیز داخل کانتینر تعریف می‌شه، «ولی روی سیستم من کار می‌کنه» عملاً دیگه وجود نداره.

امنیت و جداسازی: هر سرویس در یک فضای جدا اجرا می‌شه؛ بنابراین خرابی یا حمله به یک سرویس، لزوماً روی بقیه اثر نمی‌ذاره.

آینه‌ی هوشمند:
اینترنت اشیاء و رابط‌های کاربری تعاملی

سپهر نوروزی

در دنیای مهندسی کامپیوتر، جایی که فناوری‌های نوین مانند اینترنت اشیاء، هوش مصنوعی و رابط‌های انسان-رایانه زندگی روزمره را دگرگون می‌کنند، آینه هوشمند به عنوان یک مفهوم جذاب و کاربردی ظاهر شده است. مفهوم آینه هوشمند، اساساً یک آینه معمولی است که با افزودن لایه‌های دیجیتال هوشمند، به ابزاری تعاملی تبدیل می‌شود. تصور کنید آینه‌ای که نه تنها بازتاب چهره شما را نشان می‌دهد، بلکه اخبار، آب و هوا، تقویم شخصی و حتی راهنمایی‌های سلامتی را بر روی سطح خود نمایش می‌دهد، بدون اینکه نیاز به لمس یا دستگاه اضافی باشد. این مفهوم از ایده‌های اولیه دهه ۲۰۱۰، مانند پروژه‌های متن‌باز Magic Mirror، ریشه می‌گیرد و امروزه در محصولات تجاری شرکت‌هایی مثل سامسونگ و گوگل به کار رفته است. آینه هوشمند یک سیستم جاسازی‌شده است که سخت‌افزار و نرم‌افزار را ترکیب می‌کند تا داده‌های لحظه‌ای را پردازش و نمایش دهد. این دستگاه با سنسورها و اتصال به شبکه، کاربر را شناسایی کرده و محتوای شخصی‌سازی‌شده ارائه می‌کند، مانند پیشنهاد لباس بر اساس آب و هوا یا نظارت بر وضعیت سلامتی. در مهندسی کامپیوتر، این مفهوم بر پایه اصول برنامه‌نویسی، پردازش سیگنال و شبکه‌های توزیع‌شده بنا شده. بر اساس گزارش‌های جهانی، بازار آینه‌های هوشمند با رشد سالانه ۲۵ درصدی، تا سال ۲۰۳۵ به ارزش بالایی می‌رسد، که نشان‌دهنده پتانسیل آن در خانه‌های هوشمند و کاربردهای آموزشی است.

از نظر مفهومی، آینه هوشمند بر پایه یک طراحی دوگانه عمل می‌کند: لایه نوری و لایه دیجیتال. لایه نوری شامل شیشه نیمه‌نقره‌ای است که ۹۰ درصد نور را بازتاب می‌دهد، در حالی که لایه پشتی با نمایشگر LED یا OLED محتوای دیجیتال را نشان می‌دهد. این ترکیب، بر اساس اصول فیزیک نور مانند قانون فرنل، اجازه می‌دهد آینه در حالت عادی مانند آینه معمولی کار کند، اما با فعال‌سازی نور پس‌زمینه، اطلاعات را بدون اختلال نمایش دهد. در قلب سیستم، یک برد محاسباتی جاسازی‌شده مانند Raspberry Pi ٤ قرار دارد، که پردازش‌های همزمان را مدیریت می‌کند. این برد با مصرف انرژی پایین (۷-۱۰ وات) و اتصال Wi-Fi، به عنوان دروازه اینترنت اشیاء عمل می‌کند. سنسورهای جانبی، مانند میکروفون‌ها، دوربین و سنسورهای حرکتی، داده‌ها را جمع‌آوری می‌کنند. این اجزا از طریق باس‌های ارتباطی مانند I2C و GPIO متصل شده و داده‌ها را با نرخ مناسب ارسال می‌کنند. هزینه ساخت یک نمونه اولیه حدود ۱۰۰-۲۰۰ دلار است، که می‌توان با ابزارهای ساده مانند Breadboard و نرم‌افزار KiCad آن را پیاده‌سازی کرد. این ساختار ساده، آینه را به یک دستگاه هوشمند خانگی تبدیل می‌کند که با سیستم‌های دیگر مانند لامپ‌های هوشمند ارتباط برقرار می‌سازد.

عملکرد آینه هوشمند بر پایه یک معماری نرم‌افزاری ماژولار و رویدادمحور استوار است، که پردازش ورودی‌ها را با خروجی‌های تعاملی ترکیب می‌کند. فرآیند با تشخیص حضور کاربر شروع می‌شود: سنسورهای حرکتی با الگوریتم‌های ساده آستانه‌ای (مانند مقایسه سیگنال مادون قرمز با سطح نویز) سیستم را فعال می‌کنند و سرعت پردازنده را از حالت خواب به فعال می‌برند. برای تعامل صوتی، میکروفون داده‌ها را دریافت کرده و الگوریتم‌های تشخیص کلمه بیدارکننده مانند مدل‌های Picovoice، دستوراتی مثل "آب و هوا را نشان بده" را با دقت بالا (۹۵

درصد در محیط‌های معمولی) شناسایی می‌کنند. این پردازش با تبدیل فوریه سریع برای استخراج ویژگی‌های فرکانسی و مدل‌های پنهان مارکوف برای تشخیص گفتار انجام می‌شود. دوربین نیز با کتابخانه OpenCV، تشخیص چهره را بر پایه شبکه‌های عصبی کانولوشنی مانند MTCNN برای شناسایی و FaceNet برای تطبیق (با شباهت کسینوسی ۰.۶) اجرا می‌کند، که حریم خصوصی را با ذخیره داده‌های محلی حفظ می‌نماید.

از منظر نرم‌افزاری، سیستم بر پایه لینوکس جاسازی‌شده اجرا می‌شود، با کرنل بهینه‌شده برای تأخیر کم (کمتر از ۱۰۰ میلی‌ثانیه). پلتفرم MagicMirror در محیط Node.js ماژول‌ها را با فایل‌های پیکربندی JSON مدیریت می‌کند؛ برای مثال، ماژول آب و هوا داده‌ها را از APIای عمومی با درخواست‌های HTTP دریافت و تجزیه می‌کند. هوش مصنوعی با نسخه سبک TensorFlow Lite ادغام می‌شود، مانند مدل MobileNet برای تخمین وضعیت بدن در برنامه‌های ورزشی، با زمان پردازش ۵۰ میلی‌ثانیه. اتصال به اینترنت اشیاء از طریق پروتکل MOTT با کارگزار Mosquitto برقرار می‌شود، که آینه را به یک ناشر/مشترک در شبکه تبدیل می‌کند. مثلاً ارسال دستور کنترل لامپ‌ها از طریق موضوعات MOTT. این روش، تأخیر را کاهش داده و قابلیت گسترش را افزایش می‌دهد. کل فرآیند در یک حلقه رویدادمحور جریان دارد: جمع‌آوری ورودی‌ها، پردازش الگوریتم‌ها، رندر با HTML۵ و CSS۳ برای انیمیشن‌های ساده، و همگام‌سازی با ابر اگر لازم باشد. این معماری، با ابزارهایی مانند Watchdog Timers، از خرابی سیستم جلوگیری می‌کند و برای پروژه‌های دانشجویی ایده‌آل است.

کاربردهای آینه هوشمند در مهندسی کامپیوتر، از رابط‌های تعاملی تا سیستم‌های هوشمند، گسترده است. به عنوان یک رابط چندوجهی که صدا، ژست و لمس را ترکیب می‌کند. در آموزش، آینه برنامه‌های درسی را نمایش داده، آزمون‌های تعاملی اجرا می‌کند یا بازخورد لحظه‌ای با WebSockets ارائه می‌دهد. در اینترنت اشیاء، به عنوان دستگاه لبه ، داده‌های سنسور را محلی پردازش کرده و حجم انتقال به ابر را ۸۰ درصد کاهش می‌دهد. کاربردهای دیگر شامل نظارت سلامتی با بینایی کامپیوتری مانند مدل YOLO برای تشخیص اشیاء در ورزش، با دقت ۹۲ درصد یا ادغام با بلاکچین برای امنیت داده‌هاست. چالش‌های اصلی، بهینه‌سازی مصرف انرژی، DVFS هستند. تحقیقات نشان می‌دهد این دستگاه‌ها تعامل کاربر را ۴۰ درصد افزایش می‌دهند، که برای پایان‌نامه‌های دانشگاهی مفید است.

آینده آینه هوشمند با پیشرفت‌هایی مانند هوش مصنوعی generative و شبکه‌های ۵G، روشن است. ادغام واقعیت افزوده برای نمایش‌های مجازی مانند امتحان لباس ممکن می‌شود، و الگوریتم‌های الهام‌گرفته از

کوانتوم برای بهینه‌سازی شبکه‌ها بررسی خواهد شد. در ایران، با تمرکز دانشگاه‌ها بر مدل‌های بومی مانند تشخیص گفتار فارسی برای مثال PersianBERT یا ParsBert، می‌توان وابستگی به فناوری خارجی را کاهش داد. چالش‌هایی مانند آسیب‌پذیری‌های پروتکل اینترنت اشیاء و مسائل اخلاقی هوش مصنوعی زمینه‌های پژوهشی جالبی هستند که امروزه بسیار مورد توجه پژوهشگران و صنعتگران قرار گرفته‌اند. پیش‌بینی‌ها حاکی از رشد چشمگیر این فناوری در شهرهای هوشمند است.

در نهایت باید گفت، آینه هوشمند مفهومی است که مهندسی کامپیوتر را به زندگی واقعی متصل می‌کند و نوآوری در تعاملات دیجیتال را پیش می‌برد.

آینده رونمایی شد!
نگاهی به نمایشگاه جیتکس و الکامپ

سید محمد عترتی

سید علی عترتی

برای دانشجویان مهندسی کامپیوتر، دنبال کردن آخرین روندهای فناوری فقط یک علاقه نیست، یک ضرورت است.اکنون که این مطلب را می‌خوانید یکی از بزرگترین رویدادهای علمی فناوری و تجاری جهان را از دست دادید! البته جای نگرانی نیست:) ما در این گزارش، چکیده تمام آن چیزی را که باید از نمایشگاه شگفت‌انگیز جیتکس گلوبال ۲۰۲۵ بدانید، گردآوری کرده‌ایم. خودتان را برای سفری به پنج سال آینده آماده کنید؛ سفری که در آن، هوش مصنوعی دیگر یک ابزار نیست، بلکه یک همکار، پزشک و حتی کارمند دولت است.

جیتکس گلوبال در چهل و پنجمین دوره خود، یک نمایشگاه تجاری صرف نبود؛ بلکه به یک پلتفرم جهانی برای تعریف آینده تبدیل شده بود. با حضور بیش از ۶,۸۰۰ غرفه‌دار، ۲,۰۰۰ استارت‌آپ پیشرو و نمایندگانی از ۱۸۰ کشور، این رویداد محل تلاقی سیاست‌گذاران، غول‌های فناوری و سرمایه‌گذارانی بود که مجموعاً ۱.۱ تریلیون دلار دارایی را مدیریت می‌کنند.

اما فراتر از این اعداد خیره‌کننده، جیتکس امسال بر پنج حوزه «حیاتی برای آینده» تمرکز داشت: بیوتکنولوژی، روباتیک، محاسبات کوانتومی، نیمه‌رساناها و مراکز داده و هوش مصنوعی که بازار آن طبق برآوردها تا سال ۲۰۳۳ به ۴.۸ تریلیون دلار خواهد رسید، محور اصلی بوند.

حاکمیت هوش مصنوعی!!!

شاید جاه‌طلبانه‌ترین بخش نمایشگاه، غرفه دولت ابوظبی بود. امارات متحده عربی چشم‌انداز خود را برای تبدیل شدن به اولین دولت جهان که تا سال ۲۰۲۷ به طور کامل بر پایه هوش مصنوعی فعالیت می‌کند، به نمایش گذاشت.

هوش مصنوعی و اداره‌ی کشور: «Autogov»

ابوظبی از «تم ۴.۰» (TAM ٤٫٠)، نسل جدید پلتفرم خدمات یکپارچه خود رونمایی کرد که بیش از ۱٬۱۰۰ خدمت دولتی و خصوصی را در یکجا جمع کرده است. اما نقطه عطف آن، معرفی «Autogov» بود: اولین کارمند دولتی هوش مصنوعی در جهان!

تصور کنید دیگر نیازی به پر کردن فرم برای تمدید گواهینامه، پرداخت قبوض یا رزرو نوبت دکتر نداشته باشید. «Autogov» یک دستیار شخصی هوشمند است که با یادگیری ترجیحات شما، تمام این کارها را به صورت خودکار و پیش‌دستانه انجام می‌دهد.

خودروی «رعد» (Raad): سازمان دفاع مدنی ابوظبی از این خودروی چندمنظوره رونمایی کرد که ترکیبی از هوش مصنوعی و روباتیک برای واکنش به شرایط اضطراری است.

پلتفرم «LivAI»: یک «دوقلوی دیجیتال» پیشرفته برای مدیریت و برنامه‌ریزی توسعه شهری با استفاده از داده‌های زنده و تحلیل‌های پیش‌بینانه.

کوانتوم در انرژی: برای اولین بار در امارات، یک اپلیکیشن محاسبات کوانتومی در بخش انرژی (توسط ATRC و ADNOC) معرفی شد که هدف آن بهینه‌سازی عملیات و کاهش انتشار کربن برای رسیدن به هدف کربن خنثی تا ۲۰۴۵ است.

سلامت پیش‌بینانه: دپارتمان بهداشت ابوظبی اولین پلتفرم جهانی اطلاعات سلامت جمعیت مبتنی بر هوش مصنوعی را معرفی کرد که می‌تواند ریسک‌های سلامتی را در سطح جامعه پیش‌بینی کند.

فناوری‌هایی که مرزهای علم را جابجا کردند

اگر فکر می‌کنید نوآوری‌ها به همین‌جا ختم شد، سخت در اشتباهید. جیتکس ۲۰۲۵ ویترین فناوری‌هایی بود که مستقیماً از دل داستان‌های علمی-تخیلی بیرون آمده بودند:

۱. درمان بیماری‌های ژنتیکی

CRISPR و هوش مصنوعی: مدیرعامل شرکت Mammoth Biosciences، ترِوور مارتین، توضیح داد که چگونه فناوری برنده‌ی نوبل ویرایش ژن (CRISPR) در ترکیب با هوش مصنوعی، پتانسیل درمان قطعی بیماری‌های ژنتیکی را فراهم می‌کند.

ایمپلنت مغز-کامپیوتر: شرکت Paradromics از اولین ایمپلنت موفق مغز-کامپیوتر خود رونمایی کرد که می‌تواند افکار را با کمک هوش مصنوعی رمزگشایی کرده و به گفتار تبدیل کند.

لنزهای تماسی هوشمند: استارت‌آپ Xpanceo پنج نمونه اولیه از لنزهای تماسی هوشمند مجهز به هوش مصنوعی را به نمایش گذاشت که کاربردهای همزمان در واقعیت افزوده، نظارت بر سلامت و سخت‌افزار مصرفی دارند.

۲. هوش مصنوعی فیزیکی

روبوکار شخصی: شرکت Tensor از اولین روبوکار شخصی (Personal Robocar) جهان رونمایی کرد؛ یک خودروی خودران که به عنوان هوش مصنوعی عامل بر روی چرخ توصیف شد.

روبات‌های انسان‌نما: شرکت K2 نسل جدید روبات‌های انسان‌نما و یک خودروی مفهومی برای

گسترش روباتیک در محیط‌های صنعتی را معرفی کرد.

۳. محاسبات کوانتومی (آینده محاسبات)

IBM Quantum System Two: تیم آبی (IBM) از سیستم کوانتومی نسل دو خود رونمایی کرد که گامی بزرگ به سوی ساخت سیستم‌های مقاوم در برابر خطا و در مقیاس بزرگ است.

یونیکورن ۶ میلیارد دلاری: شرکت PsiQuantum، که ۶ میلیارد دلار ارزش‌گذاری شده، نقشه راه خود را برای رسیدن به حاکمیت کوانتومی تشریح کرد.

۴. نیمه‌رساناها و مراکز داده (موتور محرک هوش مصنوعی)

قدرت پردازش: AMD جدیدترین پردازنده‌های گرافیکی Instinct و پردازنده‌های مرکزی EPYC خود را که برای سنگین‌ترین بارهای کاری هوش مصنوعی طراحی شده‌اند، به نمایش گذاشت.

هوش مصنوعی مستقل (Sovereign AI): جیم کلر، مدیرعامل شرکت Tenstorrent، درباره اهمیت هوش مصنوعی مستقل سخنرانی کرد؛ اینکه کشورها باید با طراحی تراشه‌های اختصاصی، کنترل آینده هوش مصنوعی خود را در دست بگیرند.

بزرگترین مرکز داده جهان: شرکت O'Leary Ventures اعلام کرد که در حال ساخت بزرگترین پارک صنعتی مرکز داده هوش مصنوعی جهان در کانادا است.

امنیت سایبری در عصر هوش

با این همه قدرت، سوال اساسی نمایشگاه این بود: چگونه از جهانی که توسط هوش مصنوعی و داده‌ها قدرت گرفته، محافظت کنیم؟

این شد که رهبران امنیت سایبری جهان در جیتکس گرد هم آمدند:

سیاست‌گذاری چابک: عمر سلطان العلما، وزیر هوش مصنوعی امارات، جیتکس را گردهم‌آورنده جهان خواند و بر نیاز مبرم به سیاست‌گذاری چابک برای مدیریت ریسک‌های هوش مصنوعی تأکید کرد.

خط اول دفاع: دکتر محمد الکویتی، رئیس امنیت سایبری دولت امارات، هنگام رونمایی از چشم‌انداز امنیت سایبری ۲۰۲۵ امارات گفت: مردم ما، همیشه اولین خط دفاعی ما خواهند بود.

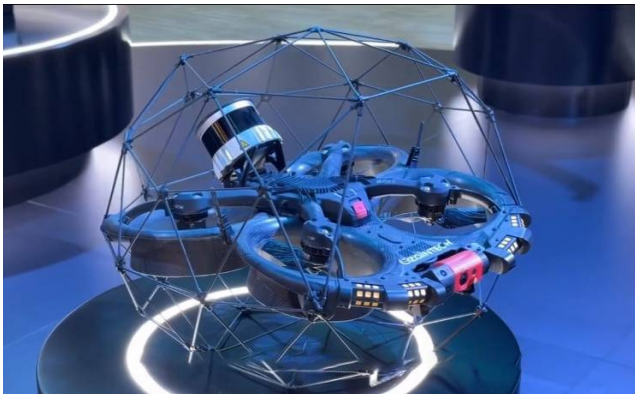
همکاری بین‌المللی: هم اینترپل و هم وزیر دادگستری و امور دیجیتال استونی هشدار دادند که مجرمان به سرعت در حال استفاده از هوش مصنوعی هستند و تنها راه مقابله، همکاری یکپارچه جهانی است.

ابزارهای دفاعی: شرکت‌هایی مانند Fortinet، Crowdstrike، و OPSWAT جدیدترین راه‌حل‌های امنیتی مبتنی بر هوش مصنوعی، از جمله دیودهای نوری برای جداسازی ایمن شبکه‌های صنعتی (OT/IT) را به نمایش گذاشتند.

مقایسه با الکامپ؛ جهانی در برابر ملی

دیدن این حجم از نوآوری، سرمایه‌گذاری (بیش از ۴۰ شرکت یونیکورن فقط در بخش استارت‌آپی اکسپند نورث استار حضور داشتند) و همکاری‌های استراتژیک (مانند مشارکت وزارت انرژی امارات با Google Cloud و MBZAI یا شهرداری دبی با Fortinet)، ما را به مقایسه با نمایشگاه الکامپ خودمان وا می‌دارد.

جیتکس گلوبال یک رویداد جهانی و آینده‌نگر است. هدف آن تعریف روندهای دهه آینده، جذب سرمایه‌های تریلیون دلاری و تبدیل شدن به بستری برای سیاست‌گذاری‌های بین‌المللی (مانند حاکمیت کوانتومی یا هوش مصنوعی مستقل) است. جیتکس محلی است که استارت‌آپ‌ها برای تبدیل شدن به یونیکورن و غول‌های فناوری برای نمایش دستاوردهای بخش R&D خود (مانند درمان ژنتیکی یا ایمپلنت



مغـزی) بـه آن می‌آینـد.

الکامـپ ایـران امـا، یک رویـداد بسـیار مهـم ملـی و منطقـه‌ای است. الکامـپ ویتریـن توانمندی‌هـای داخلی، محلـی بـرای شبکه‌سـازی اکوسیسـتم اسـتارت‌آپی ایـران و بسـتری بـرای ارائـه راه‌حل‌هـای بومی‌سازی‌شـده جهـت رفـع نیازهـای مشـخص بـازار ایـران (ماننـد فین‌تـک، دولـت الکترونـیک و امنیـت شـبکه داخلـی) اسـت.

نتیجه‌گیری

جیتکـس بـه مـا نشـان می‌دهـد کـه «سـقف» نـوآوری کجاسـت و جهـان بـه کـدام سـو حرکـت می‌کنـد. از کارمنـد هـوش مصنوعـی ابوظبـی تـا بزرگتریـن ابرکامپیوتـر هـوش مصنوعـی جهـان کـه توسـط Cerebras بـه نمایـش درآمـد، همـه نشان‌دهنده یک جهش پارادایمی هستند. الکامـپ آینـه دسـتاوردهای مـا در شـرایط موجـود اسـت و جیتکـس، قطب‌نمایـی بـرای تعییـن مقصـد بعـدی.

امیدواریـم ایـن گـزارش، توانسـته باشـد شـما را بـه قلـب جیتکـس ببـرد و دیـد روشـنی از آینـده‌ای کـه در راه اسـت ارائـه دهـد. آینـده‌ای کـه در آن، مـرزی بیـن دیجیتـال، فیـزیک و حتـی بیولـوژیک وجـود نـدارد!

پسا جنگ و آینده‌ی سایبری

پیشرفت فناوری و سایبری کشور در گرو چیست؟

محمد هراتی

در دهه‌های اخیر، نبردها به فضای دیجیتال منتقل شده‌اند و قدرت سایبری به بخش جدایی‌ناپذیری از امنیت ملی تبدیل شده است. در دوران پساجنگ، تاب‌آوری زیرساخت‌های دیجیتال اهمیت یافته و در ایران، «کد» به‌اندازه‌ی سلاح اهمیت پیدا کرده است.

جنگ سایبری در ایران؛ از حمله تا دفاع

ایران یکی از اهداف اصلی حملات سایبری در خاورمیانه بوده است؛ در زمستان ۱۴۰۳، بیش از ۱۰۱ هزار حمله مهار شد که ۸۲ درصد آن‌ها با هدف از کار انداختن خدمات عمومی بودند.

هم‌زمان با درگیری نظامی میان ایران و اسرائیل در تابستان ۱۴۰۴، موج تازه‌ای از حملات سایبری متقابل رخ داد. این حملات (شامل مهندسی اجتماعی و نفوذ به سامانه‌های مالی) نشان دادند که جنگ‌های آینده، مرز مشخصی میان فیزیکی و سایبری ندارند.

در این دوره، پلیس فتا اعلام کرد که ماهیت تهدیدها از سرقت اطلاعات به سمت «تخریب پایگاه‌های داده» و اختلال دائمی در سرویس‌ها تغییر کرده است. به عنوان نمونه، هکرهای ایرانی به شرکت دفاعی اسرائیلی «مایا» نفوذ کردند، در حالی که در داخل، سه حمله بزرگ به زیرساخت‌های حیاتی (عمدتاً مراکز داده) دفع شد. اختلال گسترده در سامانه سوخت‌رسانی در سال ۲۰۲۱، عملاً آغازگر موج جدیدی از تلاش‌ها برای تاب‌آوری سایبری بود.

زیرساخت دیجیتال و بازسازی فناوری

حملات تابستان ۱۴۰۴ (مانند حملات سنگین DDoS به وب‌سایت‌های دولتی) بار دیگر ریسک اتکای بیش از حد به فناوری‌های خارجی را نشان داد. در واکنش، ایران پروژه‌هایی را برای توسعه‌ی دیتاسنترهای بومی و گسترش شبکه ملی اطلاعات فعال کرد تا سامانه‌های حیاتی (بانکداری، انرژی و ...) مقاوم‌سازی شوند.

اما بزرگ‌ترین چالش، «کمبود نیروی متخصص» امنیت سایبری است. در حالی که حجم حملات در برخی بازه‌های بحرانی به بیش از ۲۵ تا ۳۰ هزار مورد در روز می‌رسد، تعداد مهندسان واکنش سریع کافی نیست. به همین دلیل، از نیمه‌ی دوم ۱۴۰۴، دانشگاه‌ها موظف شدند رشته‌های جدیدی در حوزه‌ی دفاع دیجیتال، رمزنگاری و امنیت ابری راه‌اندازی کنند.

تحولات در صنعت نرم‌افزار، هوش مصنوعی و اکوسیستم امنیتی

پس از بحران تابستان ۱۴۰۴، صنعت فناوری شاهد جهشی در حوزه‌ی امنیت سایبری و هوش مصنوعی بود. شرکت‌های دانش‌بنیان، ابزارهای تشخیص نفوذ خودکار با استفاده از یادگیری ماشین را توسعه دادند. چند تیم داخلی موفق شدند سامانه‌های IDS/IPS بومی را با هوش مصنوعی ترکیب کنند که اکنون در مراکز داده ملی نصب شده‌اند.

در کنار این، پژوهشگران ایرانی تحقیقاتی را در حوزه‌ی «امنیت کوانتومی» و رمزنگاری مقاوم در برابر آن آغاز کرده‌اند. مفهوم «پایداری سایبری» (Cyber Resilience) - به معنای تاب‌آوری سیستم‌ها حتی در صورت آسیب‌دیدگی - به یکی از ارکان اصلی طراحی

تبدیل شده است. این بحران همچنین به تقویت همکاری میان بخش خصوصی، دانشگاه و دولت برای آموزش سریع نیرو و توسعه‌ی آزمایشگاه‌های قرمز و آبی (red/blue team labs) برای تمرین دفاع دیجیتال انجامید.

درس‌ها و نگاه به آینده

جنگ تابستان ۱۴۰۴ نشان داد که امنیت سایبری یکی از ارکان قدرت ملی است. درس اصلی این بحران آن بود که تاب‌آوری سایبری باید در طراحی زیرساخت‌ها گنجانده شود و هماهنگی میان نهادها برای پاسخ سریع، حیاتی است.

حملات اخیر «پیچیده‌تر و چندلایه» (ترکیبی از فیشینگ و تخریب داده) شده‌اند، که نشان می‌دهد استراتژی‌های دفاعی باید به‌طور مداوم به‌روز شوند و از هوش مصنوعی برای شناسایی تهدیدات و آموزش مستمر کاربران استفاده شود.

آینده‌ی امنیت دیجیتال ایران وابسته به میزان سرمایه‌گذاری در دانش بومی، آموزش نیروهای متخصص و ارتقای فناوری‌های هوش مصنوعی خواهد بود. اگر مسیر فعلی توسعه‌ی شبکه ملی اطلاعات و مراکز داده داخلی ادامه یابد، ایران می‌تواند تا سال‌های آینده در حوزه‌ی دفاع دیجیتال به سطحی از خوداتکایی فناورانه برسد.

همکاری در نشریه‌ی ماتریس

نشریه ی ماتریس در جهت ارتقای کیفیت و مشارکت همه دانشجویان در حوزه‌های تحریریه، ویراستاری و طراحی عضویت می پذیرد.

منتظر انتقادات، پیشنهادات و دست یاری شما هستیم :)

MatrisMagazine

کودک ۱۲ ساله
شهید امیرعلی امینی

نوزاد ۷ ماهه
شهیده زهرا ذاکریان

کودک ۴ ساله
شهیده هیدا زینلی

کودک ۷ ساله
شهید طاها بهروزی

کودک ۵ ساله
شهید مهراد خیری

کودک ۴ ساله
شهیده هانیه بهمن‌آبادی

کودک ۸ ساله
شهیده زهرا بهمن‌آبادی

نوزاد ۹ ماهه
شهید محمدعلی بهمن‌آبادی

۱۰۶۴ شهیـــــد