ارزیابی چالش‌های امنیت سایبری در محیط‌های واقعیت مجازی VR

علی ملک لی

کارشناس ارشد مدیریت فناوری اطلاعات – دانشگاه تهران، مدرس دانشگاه

چکیده

اگرچه واقعیت مجازی (VR) فناوری جدیدی نیست، اما به تازگی در حوزه های مختلفی به جز سرگرمی مورد استفاده قرار گرفته و این موضوع باعث شده است که جامعه پژوهشیِ امنیت اطلاعات، به تهدیدات جدید سایبری که با آن همراه است توجه کند. تنوع اجزای سیستم، سطح گستره ای از حملات سایبری را ممکن می سازد که می‌تواند مورد سوء استفاده و بهره برداری غیر مجاز توسط هکرها یا دشمنان شود. در عین حال، تأکید VR بر روی غرق شدن (immersion) ، تعامل (interaction) و حضور (presence) به معنای آن است که می‌توان به صورت مستقیم کاربر را مورد هدف حمله سایبری قرار داد، ولی استفاده از دستگاه‌های نصب شده بر روی سر ممکن است، حس و مشاهده و درک این حمله را برای کاربر سخت کند. این مقاله با طبقه‌بندی سیستماتیک تهدیدات سایبری VR موجود در مقابل روشهای دفاعی سایبری مرسوم، به پژوهشگران با زمینه‌های مختلف برای شناسایی بهتر و درک هرچه بیشتر این مخاطرات کمک خواهد کرد.

واژگان کلیدی: واقعیت مجازی، حملات سایبری، امنیت سایبری، حریم خصوصی.

مقدمه

واقعیت مجازی (VR) در حال تبدیل به یک فناوری پرطرفدار می‌شود و انتظار می‌رود تا سال ۲۰۲۵ به ارزش بازار ۲۰.۹ میلیارد دلار (Market,2020) برسد. با این حال، تحقیقات در مورد خطرات امنیتی VR محدود است. این موضوع می‌تواند یک مشکل باشد زیرا که دستگاه‌های VR دید کاربر را کاملاً پوشش می‌دهند و این باعث می‌شود که برای وی سخت باشد تا حملات امنیتی و دستکاریهای مخرب را مشاهده کند. ما در این مقاله، با طبقه‌بندی سیستماتیکِ چالش‌های امنیتی برای محیط‌های واقعیت مجازی(VREs)، به پژوهشگران کمک میکنیم تا با درک بهتر تأثیر تهدیدات سایبری در این حوزه، بتوانند روشهای دفاع سایبری جدید را توسعه دهند.

مطالعات پیشین و موضوعات این مطالعه:

واقعیت مجازی (VR) یک فناوری است که تجربه‌ای شبیه‌سازی شده را برای کاربر ایجاد می‌کند. این فناوری بیش از ۵۰ سال پیش توسط ساترلند (Sutherland, 1965) پیشنهاد شد. از آن زمان به بعد، تعاریف مختلفی توسط محققان مختلف ارائه شده است. VR یک تجربه فراگیر، چند حسی است که با عینکهای سه بعدی، حسگرهای ردیابی حرکات بدن در زمینه‌های مختلفی مانند سرگرمی، آموزش و کسب و کار استفاده می‌شود. با این حال، تحقیقات در زمینه خطرات امنیت سایبری VR و طبقه‌بندی سیستماتیک از تهدیدات مختلف یا مکانیزم‌های دفاعی این حوزه بسیار محدود است. هدف این مقاله، برطرف کردن این کمبود دانش با ارائه یک طبقه‌بندی از تهدیدات سایبری در ارتباط با ویژگی‌هایی که در محیط‌های مختلف VR به طور مشترک به اشتراک گذاشته می‌شوند، است. این طبقه‌بندی به محققان کمک می‌کند تا تأثیر تهدیدات سایبری را درک کنند و راه حل های دفاعی جدیدی را توسعه دهند. این مقاله دو موضوع اصلی دارد:

- طبقه‌بندی سیستماتیک برای سازماندهی چالش‌های امنیتی VR مختلف. این طبقه‌بندی به تصویر کلی یکپارچه از انواع مختلف تهدیدات سایبری در VR کمک می‌کند.
- بررسی کلی روشهای دفاعی سایبری موجود و قابلیت اعمال آن‌ها برای تهدیدات سایبری VR .

طبقه بندی مخاطرات و چالش های امنیتی VR

یک سیستم VR می‌تواند به عنوان یک مجموعه سخت‌افزار و نرم‌افزار دیده شود که با حرکت فیزیکی کاربر انسانی تعامل دارد و در عوض تحت تأثیر دریافت حسی انسانی از کاربر قرار می‌گیرد. هر یک از این مؤلفه‌های فنی و انسانی ممکن است به عنوان نقاط نفوذ و جذاب برای حملات سایبری مورد استفاده قرار گیرند. در این راستا ما به چهار سوال بزرگ پاسخ میدهیم:

- چه جنبه‌ای از سیستم ممکن است مورد نفوذ و بهره برداری غیرمجاز قرار گیرد؟ این مورد سطح حمله را نشان می‌دهد.

- چه ویژگی امنیتی ممکن است نقض شود؟ این مورد به سه‌گانه محرمانگی-صحت-دسترسی (CIA) از ویژگی‌های امنیتی ارجاع دارد.
- تأثیر چه برداشتی از تجربه VR ممکن است ناشی از نقض امنیتی باشد؟ در اینجا، ما تجربه VR را با تعامل (interaction)، غرق شدن (immersion) و حضور (presence) نشان می‌دهیم.
- حمله، به چه آسیبی ممکن است منجر شود؟ قصد حمله می‌تواند برای آسیب فیزیکی یا غیرفیزیکی باشد.

بر اساس سوالات فوق، ما چهار دسته بندی بزرگ را ارائه می دهیم: **بهره‌برداری** (exploit)، **نقض** (breach)، **تأثیر** (impact) و **قصد و نیت** (intent).

- بهره‌برداری (exploit)

بهره‌برداری یعنی فرایند نفوذ به آسیب‌پذیری‌های یک سیستم کامپیوتری از طریق یک برنامه نرم‌افزاری یا کد مخرب که باعث رفتار ناخواسته و احتمالاً صدمات سایبری، فیزیکی می‌شود. در ارتباط با یک سیستم واقعیت مجازی (VRS) ، ما یک نفوذ را به دو موضوع مختلف **سیستمی** و **انسانی**، گروه بندی میکنیم.

سیستمی

شبکه: در یک نشست و تعامل واقعیت مجازی، انواع مختلفی از داده‌ها بین منبع و مقصد تبادل می‌شوند که می‌توانند توسط حملات سایبری مانند انکار سرویس (DoS) مختل شود. حملات به شبکه می‌تواند منجر به کاهش سرعت، قطع شدن ارتباط و ... شود.

تاخیر: به تاخیر به انتقال داده‌ها اشاره دارد که کیفیت سرویس (QoS) را در یک محیط شبکه‌ای کاهش می‌دهد و می‌تواند کیفیت بصری و صوتی در جلسه واقعیت مجازی را تحت تأثیر قرار دهد.

پهنای باند: پهنای باند خوب و بالا برای عملکرد بی‌دردسر شبکه و کیفیت تجربه توسط کاربر حیاتی است. حملاتی که شبکه را مختل می‌کنند می‌توانند به عدم راحتی بصری و عدم دسترسی به محیط واقعیت مجازی منجر شوند.

نمایش: به تصاویری که عینکهای VR به چشمان کاربر ارائه میدهند، اشاره دارد. معماری نمایشگر واقعیت مجازی می‌تواند روش‌های مختلفی را برای حمله ارائه دهد که می‌تواند صدمات سایبری- فیزیکی ایجاد کند. به عنوان مثال، یک حمله‌کننده می‌تواند با پوشاندن یا ارائه محتوای ناخوشایند یا مخرب خود، جلسه واقعیت مجازی را به دست بگیرد.

سنسورها: سنسورها به سیستم‌های IMU و دوربین که در پیگیری داده‌های موقعیتی و جهت‌گیری کاربر استفاده می‌شوند، اشاره دارند. اگر این داده‌ها به نحوی به دست مهاجم بیافتد، می‌تواند به حریم شخصی کاربر آسیب بزند. مهاجم ممکن است سعی کند داده‌های موقعیتی و جهت‌گیری کاربر را جمع‌آوری کند تا به شکلی از آن استفاده کند که می‌تواند منجر به تخریب سایبری یا جاسوسی در محیط فیزیکی کاربر شود.

انسانی

این موضوع به خروجی موارد حسی اشاره دارد که فناوری VR برای ایجاد حس غرق شدن در جهان مجازی استفاده می کند. دستگاه های VR از حس بصری و شنیداری استفاده می کنند، اما برخی از آنها نیز از لمس با استفاده از کنترلرها استفاده می کنند. هدف فناوری VR این است که مغز انسان را به گمان اینکه با اشیاء در جهان مجازی در حال تعامل است، بازسازی شود. هر چه بیشتر از این حس ها در فضاهای VR وجود داشته باشد، کاربر ممکن است به حملات سایبری آسیب پذیرتر باشد.

حس بصری: دستگاه های VR جهان مصنوعی پیش تعریف شده ای را به منظور تحریک حس بصری کاربران ایجاد میکنند. حس بینایی، حس برجسته ای در انسانهاست و کاربران به شیوه های مختلف که از طریق نمایشگر VR به آنها ارائه میشود، پاسخ می دهند. با این حال، حس بینایی کاربران به حملاتی مانند آزار و اذیت کردن و مهندسی اجتماعی آسیب پذیر است.

حس شنیداری: دستگاه های VR از بلندگوها برای تقلید از حس شنوایی کاربران از طریق صدای فضایی استفاده می کنند. یک نفوذگر یا هکر می تواند بر روی حملاتی که از طریق نشانه های صوتی مانند آزار و اذیت کردن استفاده می کند، تمرکز کند.

حس لمسی: سیستم های VR از کنترلرهایی استفاده می کنند که بازخورد لمسی را فراهم می کنند. یک حمله احتمالی که می تواند از کنترلرهای لمسی بهره برد، این است که یک کنترلر مجازی که نامرئی است، به یک حمله کننده اجازه دهد که کنترل کامپیوتر کاربر را به دست بگیرد.

حس بویایی: فناوری VR هنوز حس بو را به مقیاس گسترده ای به کار نبرده است. با این حال، تولید بویی که مخرب باشد، مانند فراخواندن یک خاطره منفی در یک فرد با اختلال استرس یا نگرانی از تهدید فیزیکی مانند دود در خانه، می تواند تأثیرات آسیب زا داشته باشد.

- نقض و نفوذ

نقض و نفوذ امنیتی به معنای دسترسی غیرمجاز به سیستم کامپیوتری، دستگاه، شبکه یا برنامه با هدف ایجاد آسیب فیزیکی یا غیرفیزیکی با عبور از مکانیزم های امنیتی است. طبقه بندی ما بر اساس سه خصوصیت مهم **محرمانگی**، **صحت** و **دسترسی** (CIA) است.

محرمانگی

محرمانگی در VR به محافظت از داده های حساس در برابر دسترسی غیرمجاز اشاره دارد. هدست های VR داده های رفتاری بیومتریک و حرکت کاربر را جمع آوری می کنند و کاربران می توانند اطلاعات شخصی مانند رمز عبور و اطلاعات ورود به سیستم را وارد کنند. Casey و همکاران (۲۰۱۹) نشان دادند که با پیاده سازی مجموعه ای از حملات سایبری بر روی OpenVR که به عنوان یک رابط مدیریت برنامه جهانی بین سخت افزار VR و برنامه ها در SteamVRعمل می کند، نفوذی در محرمانگی رخ میدهد. برای نمونه حمله دسترسی به دوربین با دسترسی به فایل های پیکربندی JSON رمزگذاری نشده SteamVR میتواند به حمله کننده اجازه دهد که دوربین را بدون هشدار کاربر فعال کند.

صحت

صحت به تغییرات یا اصلاحات غیرمجاز داده ها اشاره دارد. داده های VR می توانند برای ایجاد آسیب سایبری یا دستکاری در سیستم تغییر یابند. یک مثال حمله ایجاد گیجی برای کاربر توسط Casey و همکاران (۲۰۱۹) است که شامل تغییر اسکریپت JSON برای فایل پیکربندی chaperone میشد که به کاربر حس گیجی و عدم تعادل را القا میکرد.

دسترسی

دسترسی به معنای دسترسی ساده و مجاز کاربران به داده ها و سیستم هایی است که نیاز دارند. یکی از ویژگی های اصلی یک سیستمVR ، توانایی فراهم کردن غرق شدن و حضور به کاربرانش است. اما برای رسیدن به این هدف، باید ارتباط بی وقفه بین اجزای مختلف سیستم VR وجود داشته باشد، به طوری که هرگونه وقفه باعث شکست غرق شدن و حضور شود. یک مثال از حمله انکار سرویس (DoS) به یک سیستمVR ، که توسط Odeleye و همکاران (۲۰۲۱) و Valluripally و همکاران (۲۰۲۰) نشان داده شده است.

- تأثیر (Impact)

این بخش نشان دهنده تأثیر نفوذ سایبری بر تعامل، غرق شدن و حضور است.

تعامل

تعامل در VR شامل تبادل داده های حسگرها برای انطباق حرکت فیزیکی به یک محیط مجازی است. برای دستیابی به این هدف از کنترلرهای لمسی و دوربین های عمق استفاده می شود. تعامل را می توان به ناوبری، انتخاب و مدیریت تقسیم کرد. ناوبری به حرکت در فضای VR اشاره دارد که به روش های مختلفی انجام می شود. انتخاب شامل تعامل با اشیاء مجازی مانند برداشتن آنها یا کلیک کردن روی آنها است. مدیریت به کاربران اجازه می دهد تا شکل، موقعیت یا جهت

اشیاء مجازی را تغییر دهند. حملات سایبری می توانند به آسیب پذیری های این تعاملات، مانند تغییر اشیاء یا پیگیری حرکت فیزیکی، بهره ببرند.

غرق شدن

غرق شدن در VR شامل تبادل داده های حسگری با ردیابی موقعیت و جهت بدن کاربر با دقت بالا است. معمولاً با استفاده از کنترلرهای لمسی یا دوربین های عمق، حرکات دست واقعی را در محیط VR بازتاب می دهد. این تعامل باعث می شود که VR به یک هدف جذاب برای حملات سایبری تبدیل شود. یک مثال از یک حمله که می تواند از حرکت فیزیکی کاربر در فضای VR بهره ببرد، توسط Casey و همکاران (۲۰۱۹) توصیف شده است.

انتخاب کردن اشیاء مجازی، مانند برداشتن اشیاء یا کلیک کردن روی آنها است. یک حمله کننده می تواند الگوهای حرکات دست کاربران را از طریق اطلاعات وضعیت کانالی که توسط سیگنال های WiFi تولید شده است، استخراج کند و از الگوریتم های یادگیری ماشین برای تشخیص کلیک های کاربران استفاده کند، همانطور که توسط Al Arafat و همکاران (۲۰۲۰) نشان داده شده است.

حضور

حضور تجربه ذهنیِ بودن در یک جهان VR است که به غرق شدن و مشارکت وابسته است. این به کاربر اجازه میدهد تا به صورت ذهنی به جهان مجازی واکنش نشان دهد، همانند آنچه در جهان فیزیکی انجام می دهد. حضور حس قابل اعتمادی را ایجاد می کند. تکنولوژی VR بر روی بینایی و صدا در محیط های سه بعدی مصنوعی تمرکز می کند . VR می تواند ترس از ارتفاعات را در کاربر ایجاد کند یا کاربر را در یک جعبه پر از مارهای مختلف در جهان VR غرق کند و حس واقعی از تجربه ترس را به کاربر انتقال دهد. یک حمله کننده ممکن است محیط مجازی را به زور به یک کاربر از ترس هایش القا کند. برای پرداختن به تأثیرات چالش های امنیت سایبری در محیط VR ، حضور را به حضور فیزیکی و حضور اجتماعی تقسیم بندی کردیم.

حضور فیزیکی: حضور فیزیکی درجه ای است که یک محیط مجازی به یک فرد در جهان VR واکنش نشان می دهد یا به آن پاسخ می دهد. یک مثال از یک حمله هدفمند به حضور فیزیکی، حمله "جوی استیک انسان" است که در آن کاربر به حرکت به مکان فیزیکی هدف بدون دانستن خود فریب می خورد. یک حمله کننده ممکن است محیط مجازی را به زور به یک کاربر از ترس هایش افشا کند.

جابجایی فیزیکی VR :به کاربر اجازه می دهد تا به صورت فضایی در یک فضای هندسی حرکت کند. راه هایی مانند راهنمایی هدایت شده، حسگرها و دیگر "تلاش های دریافتی مجازی-فیزیکی" که ظرفیت کاربر را برای تعامل با VR فراتر از آنچه که به طور معمول فیزیکی ممکن است، گسترش می دهد ممکن است خطرناک باشد. اینگونه مدیریت ها از دانش مرزهای ادراک انسان برای ایجاد تغییرات در حرکات فیزیکی کاربر استفاده می کنند. یک حمله کننده ممکن است محیط مجازی را به زور به یک کاربر از ترس هایش افشا کند.

تعامل فیزیکی: تعامل فیزیکی قابلیت تعامل با اشیاء در فضای VR را فراهم می کند. یک کاربر که در مراحل دوم یا سوم غرق شدن است، می تواند به راحتی با اشیاء مخرب در فضای VR تعامل کند که می تواند محرمانگی، صحت و دسترسی را نقض کند. یک حمله کننده ممکن است یک پنجره بازی که نیاز به تعاملی از کاربر دارد، به کاربر ارائه دهد.

حضور اجتماعی: حضور اجتماعی توانایی درک دیگران و پاسخ مناسب با آنها را شامل میشود که باعث رفتارهای اجتماعی و اخلاقی مشابه با رفتارهای جهان واقعی می شود. کاربران به حملات سایبری مانند آنچه در جهان واقعی اتفاق می افتد، واکنش نشان می دهند. یک حمله کننده ممکن است با استفاده از آواتار یک کاربر معتبر، به هدف گرفتن اطلاعات از شخصی که توسط آن شناخته شده است یا هک کردن یک رویداد یا فضای مجازی، به محیط مجازی وارد شود تا محتوای نامناسبی را نمایش دهد.

ارتباط: ارتباط در فضای VR می تواند به صورت مستقیم مانند در جهان واقعی باشد که دو فرد به صورت مستقیم با یکدیگر ارتباط برقرار می کنند و این فرصت را برای حملات مهندسی اجتماعی فراهم می کند. حملات شبکه می توانند کیفیت صدا در طول ارتباط را تحت تأثیر قرار دهند.

عوامل مجازی: عوامل مجازی شخصیت های کامپیوتری مبتنی بر هوش مصنوعی هستند که با کاربر در یک محیط مجازی تعامل می کنند. عوامل مجازی در چندین برنامه برای تقویت تعامل انسانی در فضاهای VR استفاده شده اند. یک حمله کننده ممکن است از یک عامل مجازی تقلید شده برای مهندسی اجتماعی کاربر استفاده کند.

- هدف، قصد و نیت (Intent)

یک هکر ممکن است به سیستم VR حمله کرده و باعث آسیب رساندن به کاربر یا خود سیستم VR شود. حملات فیزیکی می توانند در طول تجربهVR ، آسیب جسمی یا ناراحتی فیزیکی ایجاد کنند. سیستم های VR شامل اجزای سخت افزاری و نرم افزاری هستند که در برابر حمله قرار دارند. حملات غیر فیزیکی می توانند آسیب روانی ایجاد کنند، مانند مهندسی اجتماعی یا اختلال در تجربه سیستم .VR دستگاه های VR انواع مختلفی از داده ها را جمع آوری می کنند که ممکن است بدون رضایت کاربر به صورت بدبینانه دسترسی پیدا کنند و باعث نقض حریم خصوصی و تأثیر روانی شوند. حملات می توانند کیفیت غوطه وری تجربه شده توسط کاربر را کاهش دهند. بسیار مهم است که از خطرات سلامتی مرتبط با فناوریVR ، مانند سقوط یا ضربه به سر یا شکست عضو، آگاه باشید.

بررسی راه های دفاع امنیت سایبری در واقعیت مجازی

همان‌طور که برای محیط‌های دیجیتال نسبتاً جدید معمول است، بیشتر تحقیقات در زمینه محافظت در برابر تهدیدات امنیتی سایبری در واقعیت مجازی بر روی پیشگیری و از طریق احراز هویت تمرکز داشته است، اما در اواخر دیده می‌شود که فعالیت‌هایی در زمینه حفظ حریم خصوصی، ارزیابی ریسک سایبری و تشخیص نفوذ برای واقعیت مجازی نیز وجود دارد.

احراز هویت

تحقیقات در زمینه ریسک‌های امنیتی VR محدود است که می‌تواند یک مشکل باشد زیرا حملات سایبری می‌توانند تحریک حسی را تغییر دهند و آگاهی و رفتار هدفمند را تغییر دهند. روش‌های مختلفی برای احراز هویت کاربران در VRوجود دارد، مانند استفاده از احراز هویت بیومتریک یا سیستم‌های احراز هویت موجود در دنیای واقعی. به عنوان مثال، RubikBiomو RubikAuth از احراز هویت بیومتریک مبتنی بر دانش استفاده می‌کنند، در حالی که RepliCueAuth قابلیت اجرای روش احراز هویت مبتنی بر نشانه‌های صفحه نمایشی را بررسی می‌کند. تحقیقات دیگر از تکنیک‌هایی استفاده می‌کنند که در بیشتر محیط‌های دیجیتال معمولی غیرقابل اجرا هستند، اما در VR معنی دارند. به عنوان مثال، Iskander و همکارانش (۲۰۱۹) استفاده از هر دو چشم و فعالیت‌های عضلانی چشم برای تأیید هویت کاربر در حین استفاده از VR را نشان دادند. یکی دیگر از خصوصیات مطلوب احراز هویت، قابلیت اجرا در دستگاه‌های مختلف VR است. مثالی که در Miller و همکارانش (۲۰۲۰) ارائه شده است، احراز هویت مبتنی بر رفتار در دستگاه‌های مختلف VR مانندOculus Quest ، HTC Vive و HTC Vive Cosmos را نشان می‌دهد. در زمینه احراز هویت، یکی دیگر از مسائل مورد علاقه، شناسایی کاربران در بین گروه‌های کوچک کاربران مانند خانواده یا دفتر است. به عنوان مثال، Pfeuffer و همکارانش (۲۰۱۹) رابطه بین بخش‌های انتخاب شده بدن را برای افزایش شناسایی و احراز هویت کاربران بررسی کردند.

تشخیص نفوذ

تشخیص نفوذ یک جنبه مهم از امنیت VR است. کارهای اولیه به هدف توسعه چارچوب‌هایی برای تعیین سطح حمله و پیامدهای محتمل که می‌تواند منجر به تدابیر تشخیص نفوذ در آینده شود، انجام شده است. Valluripally و همکارانش (۲۰۲۰) از یک ابزار نظارت رویداد برای محیط‌های آموزشی VR استفاده کرده‌اند که بر اساس سنسورهای ساده، هشدارها را فعال می‌کند. Odeleye و همکارانش (۲۰۲۱) اولین سیستم تشخیص نفوذ را که برای حملات سایبری مبتنی بر نرخ فریم در VR اختصاصی است، توسعه داده‌اند. آنها از یک روش یادگیری ماشین ساده بدون نظارت برای ارائه هشدار زودهنگام از چنین حملاتی استفاده کرده‌اند که احتمالاً قبل از اینکه تأثیر قابل توجهی بر سیستم VR و کاربرشان داشته باشد، شناسایی می‌شوند.

ارزیابی ریسک سایبری

Gulhane و همکارانش (۲۰۱۹)؛ Valluripally و همکارانش (۲۰۲۱) یک چارچوب شامل آسیب‌پذیری و ارزیابی جامع را ارائه کرده‌اند که برای اختلالات سایبری در محیط‌های آموزشی VR اجرا شده است، اما می‌تواند در امنیت VRبه طور گسترده‌تری نیز به کار رود. این چارچوب شامل ایجاد یک مدل درخت حمله-خطای نوین است، سپس تبدیل این درخت‌ها به الگوریتمهای زمان‌بندی تصادفی و استفاده از بررسی مدل آماری برای تعیین سناریوهای تهدید است

که می‌تواند باعث بروز بیشتر اختلالات سایبری شود. این چارچوب می‌تواند با نشان دادن جایگاه و نحوه یکپارچه‌سازی اصول طراحی تقویت، تنوع، تکرار برای حفظ ایمنی کاربر موثر باشد.

حفظ حریم خصوصی

Maloney و همکارانش (۲۰۲۰) مصاحبه‌هایی را انجام دادند و متوجه شدند که کاربران در فضاهای اجتماعی VR با افشای اطلاعات شخصی خود راحت هستند، اما نگران افشای اطلاعات به غریبه‌ها هستند. آنها چهار راهبرد برای حمایت از حریم خصوصی کاربران پیشنهاد دادند، از جمله آموزش کاربران، استفاده از مدولاتور صدا، تولید آواتارهای غیر قابل شناسایی و تطبیق تنظیمات حریم خصوصی رسانه‌های اجتماعی.

Falchuk و همکارانش (۲۰۱۸) یک ابزار حفظ حریم خصوصی را پیشنهاد دادند که به کاربران امکان کنترل گزینه‌های حفظ حریم خصوصی ارائه شده به آنها در حین استفاده از VR را می‌دهد. چندین تکنیک حفظ حریم خصوصی مورد بحث قرار گرفت، مانند ایجاد ابر از کلون‌های آواتار کاربر، اجازه به کاربران برای سکونت در یک کپی خصوصی از دنیای مجازی و اجازه به کاربر برای تبدیل شدن به نامرئی برای آواتارهای دیگر به مدت مشخصی.

John و همکارانش (۲۰۱۹) یک راه‌حل مبتنی بر فاکوس برای حفاظت از داده‌های ردیابی چشم با یک مکانیزم سخت‌افزاری که یک فیلتر ماتی را به تصاویر چشم پیش‌تصویرگری شده اعمال می‌کند، پیشنهاد دادند تا قبل از آنکه این ویژگی توسط حسگر دوربین چشم ضبط شود، آن را حذف کند.

مطالب و حوزه ها برای تحقیقات بیشتر

تحقیقات در زمینه امنیت سایبری VR هنوز در مراحل اولیه خود است و بسیاری از حوزه‌ها نیاز به بررسی بیشتر دارند. این حوزه‌ها شامل الگوهای جدید حمله ، پاسخ خودکار به نفوذ و مجموعه داده‌ها و آزمایشگاه‌ها هستند.

الگوهای جدید حمله

حملات فعلی بر سیستم‌های VR به طور اصلی بر روی بهره‌برداری از تحریکات بصری تمرکز دارند. با این حال، پژوهشگران باید به آسیب‌پذیری‌های معرفی شده از طریق جنبه‌های صوتی، لمسی و بویایی و همچنین سطح حمله نیز نگاه کنند. آنها همچنین باید حملاتی را که از شباهت رفتاری بهره می‌برند و کاربر به واسطه قانون عملکرد فرضی فریب داده می‌شود را نیز مورد مطالعه قرار دهند.

پاسخ خودکار به نفوذ

تحقیقات فعلی در زمینه روشهای دفاع سایبری در این حوزه به طور اصلی درباره تدابیر پیشگیرانه برای احراز هویت و حفظ حریم خصوصی، از جمله ارزیابی ریسک سایبری، بوده است. هنوز هیچ کاری مربوط به پاسخ به یک نقض امنیتی انجام نشده است. پژوهشگران می‌توانند همچنین توصیه‌های عملیاتی به کاربر و عملیات خودکار توسط سیستم را مورد پژوهش و تحقیق قرار دهند.

ایجاد مجموعه داده‌ها و آزمایشگاه‌ها

پیشرفت در امنیت سایبری VR به دلیل عدم وجود مجموعه داده‌های عمومی در مورد رفتار عادی و حمله، و همچنین عدم دسترسی به آزمایشگاه‌ها محدود شده است. توسعه یک آزمایشگاه برای انجام تحقیقات سایبری VR نیاز به تلاش و ترکیب مهارت‌های توسعه VR و سایبری است که به طور معمول در یک گروه تحقیقاتی یکسان یافت نمی‌شود.

نتیجه‌گیری

واقعیت مجازی به عنوان یک فناوری جدید نیست، اما تنها در چند سال گذشته نقش برجسته‌تر آن باعث جذب توجه جامعه تحقیقاتی امنیت سایبری شده است. به همین دلیل، ما تنها در حال حاضر شروع به درک تهدیدات سایبری مختلفی هستیم که با پذیرش گسترده آنها همراه است. تا به تازگی، تقریباً تمام تحقیقات مرتبط بر روی احراز هویت کاربر بود که در آن فرض بر این بود که جلوگیری از استفاده بدون احراز هویت کافی است برای مقابله با بخش عمده چالش. این در حال تغییر است زیرا تحقیقات جدید نشان می‌دهد که چگونه حملات مختلفی در VR انجام می‌شود. ما یک طبقه‌بندی را به عنوان یک روش برای ارائه دید کلی از چشم‌انداز تهدید سایبری VR ارائه دادیم و این در عوض به ما کمک کرد تا جنبه‌های استفاده از VR را که هنوز توسط دفاع‌های موجود پوشش داده نشده‌اند، شناسایی کنیم. در نهایت، ما مثالهایی را ارائه دادیم که در تحقیقات آتی امنیت سایبری VR مفید خواهد بود.

منابع

[1] Casey, P., Baggili, I., Yarramreddy, A., 2019. Immersive virtual reality attacks and the human joystick. IEEE Trans. Dependable Secure Comput..

[2] Al Arafat, A., Guo, Z., Awad, A., 2021. VR-spy: a side-channel attack on virtual key-logging in VR headsets. In: Proceedings of the IEEE Virtual Reality and 3D User Interfaces (VR). IEEE, pp. 564–572.

[3] Gulhane, A., Vyas, A., Mitra, R., Oruche, R., Hoefer, G., Valluripally, S., Calyam, P., Hoque, K.A., 2019. Security, privacy and safety risk assessment for virtual real-ity learning environment applications. In: Proceedings of the 16th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, pp. 1–9.

[4] Valluripally, S., Gulhane, A., Hoque, K.A., Calyam, P., 2021. Modeling and defense of social virtual reality attacks inducing cybersickness. IEEE Trans. Dependable Secure Comput..

[5] Maloney, D., Freeman, G., 2020. Falling asleep together: what makes activities in social virtual reality meaningful to users. In: Proceedings of the Annual Sympo-sium on Computer-Human Interaction in Play, pp. 510–521.

[6] Falchuk, B., Loeb, S., Neff, R., 2018. The social metaverse: battle for privacy. IEEE Technol. Soc. Mag. 37 (2), 52–61.

[7] John, B., Jörg, S., Koppal, S., Jain, E., 2020. The security-utility trade-off for iris au-thentication and eye animation for social virtual avatars. IEEE Trans. Vis. Com-put. Graph. 26 (5), 1880–1890.

[8] Pfeuffer, K., Geiger, M.J., Prange, S., Mecke, L., Buschek, D., Alt, F., 2019. Behavioural biometrics in VR: identifying people from body motion and relations in virtual reality. In: Proceedings of the CHI Conference on Human Factors in Computing Systems, pp. 1–12.

[9] Iskander, J., Abobakr, A., Attia, M., Saleh, K., Nahavandi, D., Hossny, M., Nahavandi, S., 2019. A K-NN classification based VR user verification using eye movement and ocular biomechanics. In: Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (SMC). IEEE, pp. 1844–1848.

[10] Sutherland, I., 1965. The ultimate display.

[11] Market, V., 2020. Virtual reality market with COVID-19 Impact analysis by offer-ing (hardware and software), technology, device type (head-mounted display, gesture-tracking device), application (consumer, commercial, enterprise, health-care) and geography - global forecast to 2025.

[12] Aliman, N.-M., Kester, L., 2020. Malicious design in AIVR, falsehood and cybersecu-rity-oriented immersive defenses. In: Proceedings of the IEEE International Con-ference on Artificial Intelligence and Virtual Reality (AIVR). IEEE, pp. 130–137.