Bezpečnostní slabiny software pro spolupráci ve virtuální realitě

Martin Vondráček

Virtuální realita (VR) je rozšiřující se oblast, která nachází stále více oblastí využití. VR dnes slouží nejen k zábavě, ale využívá se k průmyslovým aplikacím, výzkumu a vývoji, ale také k sociální interakci. Komunikační aplikace pro VR nachází využití i pro firemní jednání kde si takové aplikace můžeme představit jako podstatně rozšířenou formu telekonference. Avšak se zaváděním nových technologií přichází i nová bezpečnostní rizika. Aktuální výzkum kybernetické bezpečnosti VR z USA odhalil slabiny v komunikační aplikaci Bigscreen a v platformě Unity. Potenciální útočníci tak byli schopní nejen odposlouchávat mikrofony, ale dokonce vytvořit botnet ovládnutých počítačů.

Využití VR v podnikovém prostředí

V posledních letech se virtuální realita stává dostupnější i pro běžné uživatele. Ke zprovoznění virtuálního prostředí si lze dnes pořídit komerční produkty jako například Oculus Rift, HTC Vive, Sony PlayStation VR, nebo nám dokonce může stačit levná krabička na připevnění chytrého telefonu k očím.

Firmy již zavádí VR také do vzdělávání zaměstnanců. „Virtuální kurzy jsou obecně vhodné pro firmy, kde je klasické školení nemožné nebo nákladnější. Hodí se například pro trénink servisních úkonů v nepřetržitých provozech v chemickém průmyslu, nebo k nácviku výrobních postupů na výrobních linkách," jak uvedli například ve svém článku v IT Systems p. Mjartan a p. Bronis. „Z jednoho centra můžete školit zaměstnance po celém světě," vysvětlují význam VR pro efektivní fungování firem.

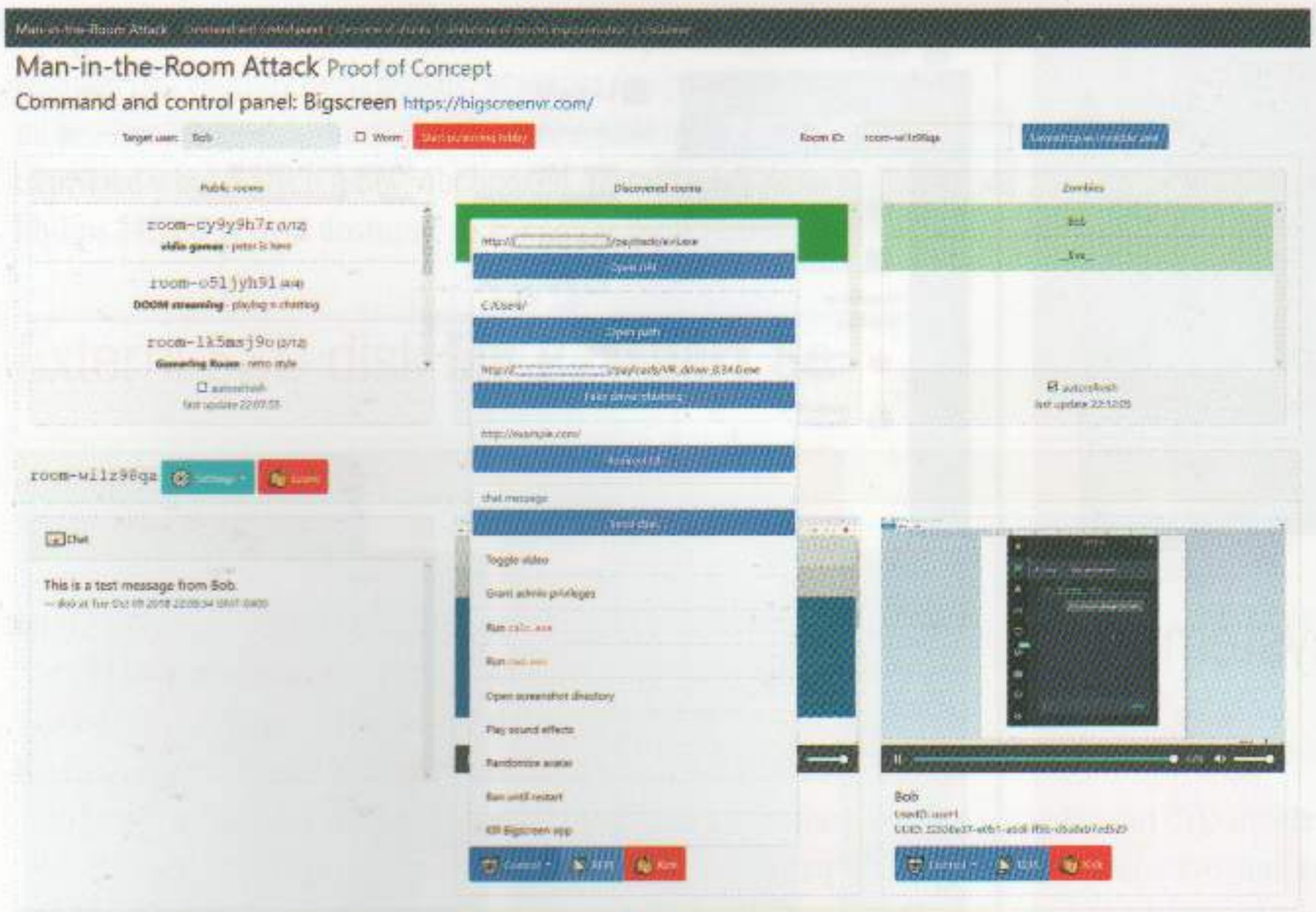
Výzkumná skupina UNHcFREG působí na University of New Haven. Její výzkumníci se zaměřují zejména na vzdělávání, forenzní vědy a bezpečnost v oblasti moderních technologií. To ostatně napovídá i celý název této skupiny, který zní University of New Haven Cyber Forensics Research & Education Group / Lab. V oblasti kybernetické bezpečnosti se výzkumné aktivity skupiny zaměřují na řadu aktuálních témat jako je například internet věcí, kryptoměny, nositelná zařízení a nyní právě virtuální realita. V rámci forenzních aktivit se zajímají například o to, jaké stopy po sobě zanechávají programy a jaké užitečné informace je možné zjistit z analyzovaných systémů pro účely pátrání po zločincích v kyberprostoru. Při bezpečnostní analýze postupují tak, že na odhalené bezpečnostní slabiny upozorňují odpovědné společnosti, aby mohly být chyby opraveny. Taková bezpečnostní analýza pak zahrnuje postupy podobné reálnému hackingu, ale dodržováním procesu responsible disclosure vědci pomáhají dělat technologie bezpečnější.

Obr. 1: Aplikace Bigscreen se používá nejen k zábavě, ale také k produktivitě a k soukromým jednáním. Zdroj: https://bigscreenvr.com/press/

Zabezpečení komunikační aplikace pro VR — Bigscreen

Tým ve složení Martin Vondráček, Peter Casey a Ibrahim Baggili provedl analýzu zabezpečení technologií pro VR se zaměřením na aplikace určené mj. k virtuálním schůzkám a komunikaci. Řada takových aplikací je nyní dostupná zdarma, těší se velké popularitě a vedou tvrdý boj s konkurencí o získání uživatelů. V tomto prostředí se bohužel řada vývojářských společností zaměřuje hlavně na vydání produktů na trh co nejdříve a na přidávání nových funkcí, které by zaujaly uživatele a tím potenciální zákazníky. Často tak nezbývá čas věnovat pozornost dostatečnému zabezpečení uveřejněných produktů. A přitom právě u sociálních a komunikačních aplikací je kritické zajistit důvěrnost.

Aplikace Bigscreen umožňuje nejen samotné setkání a komunikaci ve VR, ale také ovládání počítače uvnitř virtuálního prostoru. Díky tomu je možné například vést firemní poradu a diskutovat nad důležitými dokumenty, nebo společně ve VR používat jiné počítačové programy. Aplikace funguje na principu virtuálních místností, kdy 3D model a vzhled lze vybrat od zasedací místnosti přes balkón mrakodrapu, virtuální kinosál až po táborák uprostřed lesa. Virtuální místnosti v aplikaci Bigscreen jsou buď veřejné, nebo privátní. Každý uživatel má svou 3D postavu a pomocí sensorů se jeho pohyb a akce přenáší do virtuální místnosti. Pomocí ovladačů v rukou a VR brýlí se pak uživatelé naprosto ponoří do virtuálního prostředí. Aplikace Bigscreen



Obr. 2: Pro demonstraci závažnosti objevených zranitelností výzkumníci vytvořili i command-and-control server (na obrázku), ze kterého bylo možné provádět jednotlivé útoky a ovládat celý botnet. Zdroj: Archiv Martina Vondráčka

byla ve verzi Beta uveřejněna v roce 2016 a má přes 500 000 uživatelů.

Chyby v zabezpečení umožnily ovládnout počítače uživatelů

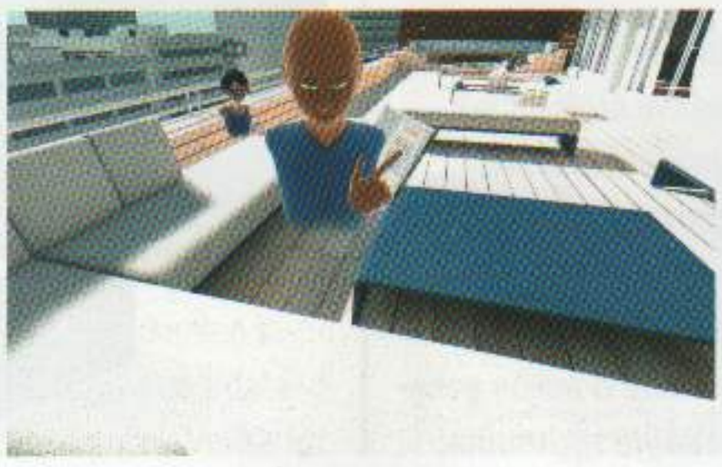
Bezpečnostní analýzu prováděli výzkumníci v jednotlivých fázích a iterativně. Výzkumný projekt zahrnoval metody penetračního testování a reverzního inženýrství proprietárních protokolů i samotné aplikace. Týmu se podařilo odhalit kritické bezpečnostní zranitelnosti v aplikaci Bigscreen a platformě Unity, které by potenciálním útočníkům umožnily:

Odposlouchávat mikrofon a sledovat obrazovku počítačů obětí při používání aplikace bez jejich vědomí. Tato zranitelnost se týkala i privátních místností. Pokud by se uvnitř napadené uzavřené místnosti probíraly soukromé informace a sdílely důvěrné fotky nebo dokumenty, potenciální útočník by je získal.

Získat kontrolu nad počítači obětí a distribuovat malware. Spojením bezpečnostních chyb v aplikaci Bigscreen a objevené chyby v platformě Unity bylo možné přes internet ovládnout počítač uživatelů, kteří si aplikaci i jen spustili. Potenciální útočníci tak mohli spouštět libovolné programy, otevírat soubory a procházet složky na disku. Tímto útokem bylo možné na počítač oběti stáhnout a spustit malware.

Vytvořit botnet a škodlivého červa ve VR, který přenášel infekci mezi jednotlivými uživateli. Výzkumníci našli způsob, jak bylo možné zranitelnosti zneužít k vytvoření počítačového červa. Po napadení uživatele škodlivý kód ovládne jeho aplikaci Bigscreen a připojí se k útočníkovi na jeho command-and-control server. Aplikace napadená červem je pod kontrolou útočníka a je tak součástí jeho botnetu. Každý uživatel aplikace Bigscreen, který je napadený tímto červem, pak při setkání s jiným uživatelem ve virtuálním prostoru předává nákazu červa dál. Botnet se tak mohl velmi rychle a nepozorovaně rozšířit po komunitě aplikace Bigscreen.

Obr. 3: Nový kyberútok Man-in-the-Room v prostředí aplikace Bigscreen. Uživatel Bob (pohled vlevo) si myslí, že je ve virtuální místnosti sám. V soukromé místnosti je ale i útočník (pohled vpravo), který je pro ostatní neviditelný. Zdroj: prostředí aplikace Bigscreen



Nový kybernetický útok Man-in-the-Room

Po odhalení uvedených zranitelností se výzkumníci zaměřili ještě na zabezpečení samotného virtuálního prostoru. S využitím předchozích útoků byli schopni získat přístupové údaje k soukromým místnostem. Následně se jim podařilo odhalit další slabinu, která umožnila, aby byl některý účastník virtuální místnosti pro ostatní skrytý. Tím se týmu ve složení Vondráček, Casey a Baggili podařilo vytvořit kyberútok s novými dopady na soukromí. Potenciální útočníci by tak byli schopni přistoupit do libovolné uzavřené soukromé místnosti a být přitom neviditelní. Útok Man-in-the-Room umožňuje se skrytě pohybovat po virtuální místnosti, přitom vidět a slyšet veškeré dění.

Zodpovědné nahlášení a opravení odhalených chyb

Při odhalení popsaných bezpečnostních chyb v aplikaci Bigscreen a v platformě Unity kontaktovali výzkumníci relevantní společnosti a předali jim technické detaily zranitelností včetně možností jejich zneužití. Podle procesu responsible disclosure byly výsledky výzkumu neveřejné než obě společnosti provedly nápravu chyb. Týmu výzkumné skupiny UNHcFREG z americké University of New Haven se tak podařilo zmírnit rizika pro více než půl milionu uživatelů aplikace Bigscreen a pro uživatele aplikací, na které se vztahovala chyba v platformě Unity.

Zavedení technologií pro VR v rámci podnikové sféry může představovat velký přínos, zefektivnění stávajících procesů a zejména snížení nákladů. Jak výsledky tohoto výzkumu ukazují, je však vždy potřeba důkladně zvážit bezpečnostní rizika spojená s novými a neotestovanými technologiemi. Bezpečnostní slabiny v neprověřených produktech mohou způsobit únik citlivých informací nebo ohrozit IT systémy firem.

Martin Vondráček

Autor článku a popisovaného výzkumu v současné době dokončuje magisterské studium na Fakultě informačních technologií Vysokého učení technického v Brně. Kromě kybernetické bezpečnosti se věnuje počítačovým sítím a vývoji software. Na University of New Haven působil v závěru léta 2018 jako Visiting Scholar.