Kiberbiztonság – helyzetkép és kitekintés a jövőre

BUTTYÁN LEVENTE

BME, Hálózati Rendszerek és Szolgáltatások Tanszék

Jelen és jövő nagy vonalakban

Mára a kibertér mindennapi tevékenységünk színterévé vált, és függésünk az információs technológiáktól (azaz a számítógépes rendszerektől és az azokat összekötő hálózatoktól) kritikus mértékű. Sem a munkánkat, sem a magánéletünket nem tudjuk már elképzelni az internet és az azon keresztül elérhető szolgáltatások nélkül, és a fiatalabb generációkra ez még inkább igaz. Mindannyian tudjuk azonban, hogy ez a trend veszélyeket is jelent számunkra: informatikai rendszereink és az azok által kezelt adatok ki vannak téve a kibertér felől érkező támadásoknak. Rosszindulatú hekkerek próbálnak folyamatosan betörni rendszereinkbe, és ellopni vagy elérhetetlenné tenni adatainkat, hogy aztán eladják azokat vagy váltságdíjat követeljenek a visszaszolgáltatásukért.

A kiberbiztonság a fenti problémák megoldásával, enyhítésével foglalkozó terület. Egy informatikai rendszert biztonságosnak mondhatunk, ha az fel van készítve a kibertámadások elleni hatásos védekezésre és a rendszer üzemeltetője gondoskodik ennek a kellően védett állapotnak a folyamatos fenntartásáról is. A gyakorlati tapasztalat azt mutatja, hogy a biztonság elérése kihívásokkal teli feladat, és nem létezik tökéletesen védett rendszer. A nehézségek egyik forrása az, hogy – ellentétben azzal, amit maga a szó sugall – a kiberbiztonság megvalósítása nem kizárólag műszaki feladat. Ahogy azt Bruce Schneier, a terület egyik széles körben ismert szakembere megfogalmazta: „If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." A kiberbiztonság eléréséhez, a hatásos műszaki megoldások mellett, jól átgondolt üzemeltetési szabályokra és eljárásokra, valamint fizikai védelmi módszerek és eszközök alkalmazására is szükség van. Arról sem szabad megfeledkezni, hogy egy informatikai rendszernek részét képezik a felhasználók és a rendszert üzemeltető személyzet is, így foglalkozni kell az ő képzésükkel, biztonságtudatosságuk és lojalitásuk növelésével is. A nehézségek egy másik forrása, hogy e szerteágazó feladatokat egyenletes minőségben kell megoldani, a biztonság ugyanis olyan, mint egy lánc: a leggyengébb láncszem határozza meg az egész erősségét. Például hiába alkalmazzuk a legerősebb titkosítási eljárást, ha a felhasználóktól ki lehet csalni a titkos dekódoló kulcsot. Más megvilágításban: a támadónak elég egy kihasználható gyengeséget találni a rendszer védelmében, a rendszert üzemeltetőnek viszont minden nagy kockázatú fenyegetésre fel kell készülnie.

A fentiek tükrében nem csoda, hogy a kiberbiztonság, mint problémakör, évtizedek óta velünk van és a kérdést nem sikerült még „megoldanunk". Sőt, egy kicsit pesszimistább hozzáállással azt is mondhatnánk, hogy a kiberbiztonság stagnál, azaz az elmúlt 2-3 évtizedben semmilyen átütő eredményt nem tudtunk felmutatni. Mintegy 20 évvel ezelőtt, 2006 februárjában, az MIT Technology Reviews folyóiratban megjelent egy írás „The Internet is broken" címmel [1], mely azt állította, hogy „az Internet alapvető hibái milliárdokba kerülnek a cégeknek, akadályozzák az innovációt és veszélyeztetik a nemzetbiztonságot." Nos, ez ma sincs másként. A helyzet alapvetően nem javult: a kártékony programok (vírusok, férgek, trójaiak) nem tűntek el [2]; az informatikai rendszerekbe történő illetéktelen behatolás és az adatlopás mindennapos [3]; kritikus rendszereink ebben a pillanatban is éppen valamilyen elárasztásos (DDoS) támadás alatt állnak [4]. Mielőtt teljesen elszomorodnánk, érdemes persze mindezt perspektívába helyezni: jelenleg sokkal több informatikai rendszer működik és sokkal több adatot kezelünk, mint 20 évvel ezelőtt, és a sorozatos kibertámadások ellenére, a világ nagyjából mégis működik. Ez azonban csak annyit jelent, hogy a helyzet nem lett sokkal rosszabb sem, mint volt. A stagnálást jól illusztrálja, hogy míg a processzorok számítási kapacitása és a hálózatok sebessége több nagyságrenddel nőtt az elmúlt évtizedek során, és ennek következtében elképesztő új alkalmazások jelenhettek meg, addig a kiberbiztonság területén nem beszélhetünk ilyen mértékű javulásról vagy fejlődésről.

A múltból extrapolálva a jövő sem kecsegtet nagy reményekkel. A kiberbiztonság követi majd az aktuális technológiai trendeket és – az eddigiekhez hasonlóan – reagálni próbál a legfrissebb kihívásokra, legyenek azok a rendszerek jellemzőinek változásából származó kihívások vagy a támadási módszerek fejlődéséből származóak. Nem valószínű, hogy a kiberbiztonság ezen reaktív jellege megváltozna a jövőben. A nagyobb biztonság elérésének ugyanis magasabb a költsége, és ezt a plusz költséget csak akkor fizeti meg bárki, ha már nincs más választása. Azaz előbb az igény fog jelentkezni (pl. megnövekszik egy új fenyegetés kockázata), s ezt követi majd az arra adott válasz (pl. egy erősebb kódolási algoritmus kifejlesztése és bevezetése). Nem várható tehát olyan gyökeres fordulat, ami a kiberbiztonság problémakört teljes egészében megszünteti, vagy akárcsak a főbb problématerületek valamelyikét eltüntetné. 15 év múlva is küzdeni fogunk még a kártékony programokkal, köztük a zsaroló vírusokkal, a gyenge jelszavakkal, az adatlopással, és a különböző típusú megtévesztéses támadásokkal. Feltéve, hogy lesznek még informatikai rendszereink...

Ha nagyon távolról nézve nem is fog jelentősen változni a kiberbiztonság képe a jövőben, közelebbről tekintve a kiberbiztonság egy-egy részterületén minden bizonnyal tanúi leszünk innovatív új megoldások születésének. A teljesség igénye nélkül, a továbbiakban három olyan problématerületet mutatok be, ahol új kihívásokkal találkozunk és biztosan várható fejlődés a következő 15 évben.

Kiber-fizikai rendszerek kiberbiztonsága

A kiber-fizikai rendszerek folyamatos térhódításának vagyunk tanúi, és ez a trend várhatóan a jövőben is folytatódni fog. A kiber-fizikai rendszerek olyan rendszerek, melyekben beágyazott számítógépek felügyelnek és/vagy vezérelnek fizikai folyamatokat. Gondoljunk például egy modern autóra, amiben 40-50 beágyazott kontroller segíti a vezetést a jármű különböző részegységeinek (úgy, mint maga a motor, a kormány, a fékek, ...) felügyeletével. Hasonlóan, egy modern gyárban beágyazott számítógépek vezérlik a gyártósort, a futószalagokat és robotkarokat. Az élet minden területén egyre inkább megjelennek a beágyazott számítógépes rendszerek, melyek az eszközeinket és a környezetünket okosabbá, intelligensebbé teszik: okos otthonokban lakunk, intelligens közlekedési rendszereket használunk, okos városokban élünk majd. Ráadásul ezek a kiber-fizikai rendszerek ma már nem izoláltan működnek, hanem az internethez csatlakoznak és a „felhőbe" mentik az adataikat vagy azon keresztül nyújtanak különböző szolgáltatásokat.

Az előnyeik mellett, a kiber-fizikai rendszerek kiberbiztonsági kockázatokat is hordoznak: az őket alkotó beágyazott számítógépek hasonló módon megtámadhatók, mint a hagyományos számítógépek. Egyre erősödő trend például a beágyazott eszközök kártékony programmal történő fertőzése valamilyen hálózati kapcsolaton keresztül, majd a fertőzött eszközökből nagy méretű botnetek létrehozása [5], melyeket a támadók háttér infrastruktúraként használhatnak az interneten elérhető szolgáltatások támadása során [6]. A támadók dolgát speciális keresőmotorok segítik (pl. a Shodan [7] szolgáltatás), melyek internet kapcsolattal rendelkező, potenciálisan sérülékeny beágyazott eszközöket keresnek automatizált módon. A legnagyobb problémát – és egyben a legérdekesebb kihívást – azonban az jelenti, hogy a kiber-fizikai rendszereket ért kibertámadásoknak akár fizikai hatása is lehet! Ez jobb esetben csak anyagi károkat okoz majd (pl. tönkremegy egy robotkar egy gyárban), rosszabb esetben azonban környezetkárosító vagy akár emberéletet követelő balesethez is vezethet (pl. egy kompromittált önvezető autó közúti balesetet okoz). Ezért az elkövetkezendő években, a kiberbiztonság egyik meghatározó alkalmazási területe a kiber-fizikai rendszerek védelme lesz.

Poszt-kvantum kriptográfia

Egy másik erősödő trend a kvantumtechnológia fejlődése: kormányzatok és nagyvállalatok fektetnek dollármilliárdokat kellően nagy, a gyakorlatban is használható kvantumszámítógépek fejlesztésébe [8]. Az, hogy pontosan mire is lesznek jók ezek a számítógépek még nem teljesen világos, de egy alkalmazási terület biztosan nagy reményekkel kecsegtet: a gyakorlatban jelenleg használt publikus kulcsú kriptográfiai algoritmusok (pl. az RSA és az elliptikus görbe alapú kriptográfiai eljárások) feltörhetők lesznek egy nagy, kriptográfiailag releváns (azaz több tízezer kvantum-bites) kvantumszámítógép segítségével [9]. Bár egy ilyen kvantumszámítógép építése még több évtizedes kutatást és fejlesztést igényelhet, a problémával már most foglalkoznunk kell a „harvest now, decrypt later" támadások lehetősége miatt. Arról van szó, hogy bizonyos (pl. kormányzatok által támogatott) támadók folyamatosan, nagy mennyiségben rögzíthetnek számukra potenciálisan érdekes titkosított hálózati forgalmakat, és tárolhatják ezeket mindaddig, amíg rendelkezésre nem áll egy nagy kvantumszámítógép, amivel aztán feltörhetővé válik minden korábban rögzített titkosított forgalom [10].

Felmerülhet a kérdés, hogy egyáltalán lehetséges-e olyan új publikus kulcsú kriptográfiai algoritmust tervezni, ami ellenáll a kvantumtámadásoknak, vagy a kvan-

tumszámítógéppel minden jelenlegi és jövőbeli publikus kulcsú séma feltörhető? Szerencsére úgy tűnik, hogy a fenti kérdésre a válasz megnyugtató, azaz vannak olyan nehéz matematikai problémák, melyekre nem létezik polinom idejű megoldás sem hagyományos, sem kvantumszámítógépen [11], és ezek némelyikére építhető hagyományos számítógépen is futtatható publikus kulcsú titkosítás vagy digitális aláírás algoritmus. Az ilyen algoritmusok tervezésével és elemzésével foglalkozó területet nevezik „poszt-kvantum kriptográfiának", és ez jelenleg a kriptográfia egyik legaktívabb területe. Most születnek azok az új ötletek, melyek a jövőbeli publikus kulcsú kriptográfiai algoritmusok alapjául szolgálnak. Az amerikai National Institute of Standards and Technology (NIST) már meg is kezdte az új poszt-kvantum sémák szabványosítási folyamatát [12]. A várakozás azonban az, hogy az átállás az új poszt-kvantum algoritmusokra még akár 10-12 évet is igénybe vehet, ezért a NIST 2035-öt tűzte ki a teljes poszt-kvantum átállás céldátumának. Ezalatt az idő alatt még sok minden történhet: jelenlegi jelölt algoritmusokról kiderülhet, hogy mégsem biztonságosak, új jelöltek léphetnek a színtérre, és akár még korábban nehéznek vélt matematikai problémákról is kiderülhet, hogy mégsem olyan nehezek. A mérnököknek pedig óriási feladat lesz az új algoritmusok biztonságos integrálása a meglévő rendszerekbe, és egy olyan átmeneti időszak lehetővé tétele, melyben hibrid módon egyszerre fogunk hagyományos és poszt-kvantum kriptográfiát használni.

MI – a kétélű kard

S végül ebből a kitekintésből nem hagyhatjuk ki a Mesterséges Intelligencia (MI) potenciális hatásait a kiberbiztonságra. Ezen a területen az MI kétélű kardként jelenik meg: egyrészt a gépi tanulás és a legújabb generatív modellek segítségével hatásosabb biztonsági mechanizmusokat hozhatunk létre és hatékonyabbá válhat rendszereink biztonságos üzemeltetése; másrészt az új MI technikákat a támadók is sikerrel alkalmazhatják hatásosabb támadások kivitelezésére és rosszindulatú tevékenységük hatékonyságának fokozására.

Gépi tanulási modelleket már most is alkalmazunk kártékony programok és támadási mintázatok észlelésére, és a jövőben várhatóan egyre több feladatot oldunk majd meg ezekkel a modellekkel. Az MI segíteni fog a repetitív feladatok elvégzésében: a közeljövőben várhatóan MI-alapú asszisztensek segítik majd a biztonsági műveleti központokban ülő elemzők és a rendszerek penetrációs tesztelését végző szakemberek munkáját, míg egy kicsit távolabbi jövőben akár az is elképzelhető, hogy ezen feladatok megoldása nagy részben automatizálttá válik.

Ugyanakkor, a gépi tanulásnak megvannak a saját biztonsági problémái, mint például a tanító adatok szennyezése (poisoning) [13], kiskapuk (backdoor) elhelyezése [14], vagy az ellenséges minták (adversarial samples) lehetősége [15]. Ezek kihasználásával a támadók manipulálni tudják a gépi tanulási modellek viselkedését, predikciós képességeit. A generatív modelleknek szintén vannak biztonsági problémáik, például a jailbreaking [16] és a prompt injection [17]. Az elkövetkező évtizedek nagy kihívása lesz a robusztus MI technikák kifejlesztése, melyek a fenti – és más hasonló – támadásoknak ellenálló modelleket eredményeznek.

A támadó oldal is masszívan kihasználja majd az MI adta lehetőségeket. A generatív modellek nagyszerűen alkalmazhatók például a felhasználók megtévesztésében, kártékony programok fejlesztésében, és új támadási stratégiák kidolgozásában. Az MI segítségével a jövőben automatizálhatóvá válik majd a sérülékenységek keresése és kihasználása, és a támadók hatékonysága olyan mértékben növekedhet, hogy azzal már nem lehet lépést tartani, csakis valamilyen MI-vel támogatott védekezési módszer segítségével. Hogy ez a spirális út hova vezet majd, azt nehéz megjósolni.

Hivatkozások

[1] https://www.technologyreview.com/2006/02/15/229667/the-internet-is-broken/
[2] https://www.ibm.com/blog/malware-history/
[3] https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
[4] https://www.netscout.com/ddos-attack-map
[5] https://iotsecurityfoundation.org/iot-botnets-might-be-the-cybersecurity-industrys-next-big-worry/
[6] https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/
[7] https://www.shodan.io/
[8] https://www.newyorker.com/magazine/2022/12/19/the-world-changing-race-to-develop-the-quantum-computer
[9] https://www.techtarget.com/searchdatacenter/feature/Explore-the-impact-of-quantum-computing-on-cryptography
[10] https://techmonitor.ai/hardware/quantum/harvest-now-decrypt-later-cyberattack-quantum-computer
[11] https://en.wikipedia.org/wiki/BQP
[12] https://csrc.nist.gov/projects/post-quantum-cryptography
[13] https://defence.ai/ai-security/data-poisoning-ml/
[14] https://defence.ai/ai-security/backdoor-attacks-ml/
[15] https://datascientest.com/en/adversarial-examples-definition-and-importance-in-machine-learning
[16] https://www.techopedia.com/what-is-jailbreaking-in-ai-models-like-chatgpt
[17] *https://www.techtarget.com/searchsecurity/tip/Types-of-prompt-injection-attacks-and-how-they-work*