Popestritev predavanj o kibernetski varnosti z interaktivnimi računalniškimi simulacijami

Saša Divjak
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko
sasa.divjak@fri.uni-lj.si

Izvleček

Prispevek obravnava problem, kako narediti predavanja s področja kibernetske varnosti bolj zanimiva in razumljiva dijakom, študentom in udeležencem kakšnih izobraževalnih tečajev. Rešitev najde v simulacijah in animacijah, ki lahko vizualno ponazorijo dogajanja v računalniških mrežjih, na katera prežijo napadalci. Po kratkem vpogledu v sorodja dela se posveti kiberletom, to je spletnim aplikacijam, ki take simulacije predstavljajo. Delo prikazuje nekaj tipičnih simulacij in v grobem poda ozadje, ki omogoča tudi nadgradnjo z lastnimi primeri.

Ključne besede: Kibernetska varnost, računalniške simulacije, izobraževanje.

Enriching cyber security lectures with interactive computer simulations

Abstract

The paper deals with the problem of how to make lectures in the field of cyber security more interesting and comprehensible to pupils, students and participants of certain educational courses. The solution is found in simulations and animations that can visually illustrate the events in computer networks that attackers are lurking on. After a brief insight into similar solutions, the paper focuses on cyberlets, i.e. online applications that present such simulations. The paper presents some typical simulations and gives a rough background, which also allow for the development of own examples.

Keywords: Cyber security, digital simulations, education

1 UVOD

Običajna predavanja s pomočjo PPT prosojnic so lahko tudi dolgočasna in jih skušamo popestriti z različnimi vložki, kot so video, morda vmesna vprašanja s pomočjo glasovalnih aplikacij itd.

Eden od možnih pristopov je tudi uporaba različnih, po možnosti interaktivnih simulacij in poigritve predavanj.

Takšne, grafično podprte simulacije in animacije najdemo na primer na področju fizike, ki je za kaj takega zelo priročna veda. Med takimi rešitvami najdemo na primer fizlete [1] (angleško physlets), ki so bili v fizikalno področje usmerjeni spletni apleti. Najdemo jih v več svetovnih jezikih, tudi v slovenščini [2]. Danes jih seveda nadomeščajo istoimenske simulacije, tipično programirane z JavaScript. Seveda obstaja ogromno zelo kvalitetnih računalniških simulacij s področja fizike, a to ni fokus te predstavitve. Po analogiji s skovanko »physlets« lahko za področje kibernetske varnosti sestavimo besedo »cyberlets« (cyber applets), kar lahko prevedemo v kiberlete. Seveda na spletu najdemo tudi podobne skupine simulacij za druga naravoslovna področja (»mathlets« za matematiko [3], »chemlets« za kemijo [4],..)

2 SORODNA DELA

Simulacija kibernetskih napadov, imenovana tudi simulacija groženj, je nastajajoča varnostna tehnologija IT, ki lahko pomaga odkriti vrzeli, ranljivosti in napačne konfiguracije v naši varnostni infrastrukturi.

Simulacija nasprotnika je postopek posnemanja vedenja napadalca. Ponuja zmožnost testiranja odpornosti organizacije proti naprednemu napadalcu. Čeprav se nasprotnikova simulacija na prvi pogled sliši podobno kot avtomatizirano preskušanje vdorov, ta vrsta simulacije pokriva širši spekter varnostne infrastrukture: določanje različnih poti napada, ki bi jih lahko ubral nasprotnik, blaženje groženj in izbira primernih sanacijskih načrtov.

Simulacija se nanaša na zmožnost posnemanja tehnik, postopkov in taktik zlonamernih akterjev. Večina orodij in platform za simulacijo napadov zagotavlja avtomatsko ali polavtomatizirano sredstvo za pridobitev napadalčevega pogleda na žrtvino omrežje.

Obstaja kar nekaj platform oziroma orodij za pridobivanje potrditve resničnega varnostnega stanja v neki organizaciji [7]. Te rešitve so običajno komercialne, v večini primerov pa ponujajo le preizkusno verzijo. Nekatera sorodna orodja pas so odprtokodna.

Taka orodja so namenjena tudi usposabljanju osebja v organizacijah, pa tudi za upravljanje kibernetske varnosti. Tako namen in tudi sposobnost takih orodij verjetno presegata potrebe, ki naj bi jih imeli pri poučevanju kibernetske varnosti v sklopu klasičnega izobraževanja tako v gimnazijah kot tudi na univerzitetnem nivoju. Večinoma so tudi zelo poglobljena. Kljub pomislekom, da so večinoma komercialna, lahko nudijo ideje, ki bi jih uporabili pri razvoju simulacij in animacij za popestritev naših predavanj. Zato naštejmo nekaj primerov:

Attack simulator [5]: Pri simulaciji kibernetskega napada organizacija posnema dejanski vdor v lastno omrežje, infrastrukturo in sredstva z uporabo orodij, taktik in postopkov znanih kibernetskih kriminalcev. Cilj simulacije je odkrivanje ranljivosti v obrambi organizacije, ki jih lahko odpravi varnostna ekipa, s čimer se zmanjša izpostavljenost napadom iz resničnega sveta.

FourCore Attack [6]: Simulacija vdora in napada, Prepoznavanje ranljivosti s posnemanjem resničnih poti napada, ki jih uporabljajo akterji groženj.

Firedrill [8]: firedrill je odprtokodna knjižnica podjetja FourCore Labs za preprosto izdelavo simulacij zlonamerne, izsiljevalske programske opreme. Zgradili so skupino štirih različnih simulacij napada, ki jih lahko uporabljamo in nadgrajujemo: simulacijo izsiljevalske programske opreme, simulacijo odkrivanja, obvod UAC in simulacijo vztrajnosti.

Infection Monkey [9]: Infection Monkey je odprtokodna platforma za simulacijo vdorov in napadov, ki nam pomaga preveriti veljavnost obstoječih kontrol in ugotoviti, kako lahko napadalci izkoristijo naše trenutne varnostne vrzeli v omrežju. Na voljo je vizualni prikaz zemljevid našega omrežja z vidika napadalca, z razčlenitvijo strojev, ki jih je Monkey uspel vdreti. Pride do okužbe naključnega računalnika in sledi samodejno odkrivanje varnostnega tveganja. Preizkusimo lahko različne scenarije:krajo poverilnic, ogrožanje naprav in druge varnostne napake.

CyberCIEGE [10]: CyberCIEGE pokriva široko paleto tem kibernetske varnosti. Igralci kupujejo in konfigurirajo računalnike in omrežne naprave, da so zahtevni uporabniki zadovoljni (npr. z zagotavljanjem dostopa do interneta), hkrati pa ščitijo sredstva pred različnimi napadi. Igra vključuje številne različne scenarije, od katerih se nekateri osredotočajo na osnovno usposabljanje in ozaveščanje, drugi pa na naprednejše koncepte varnosti omrežja.

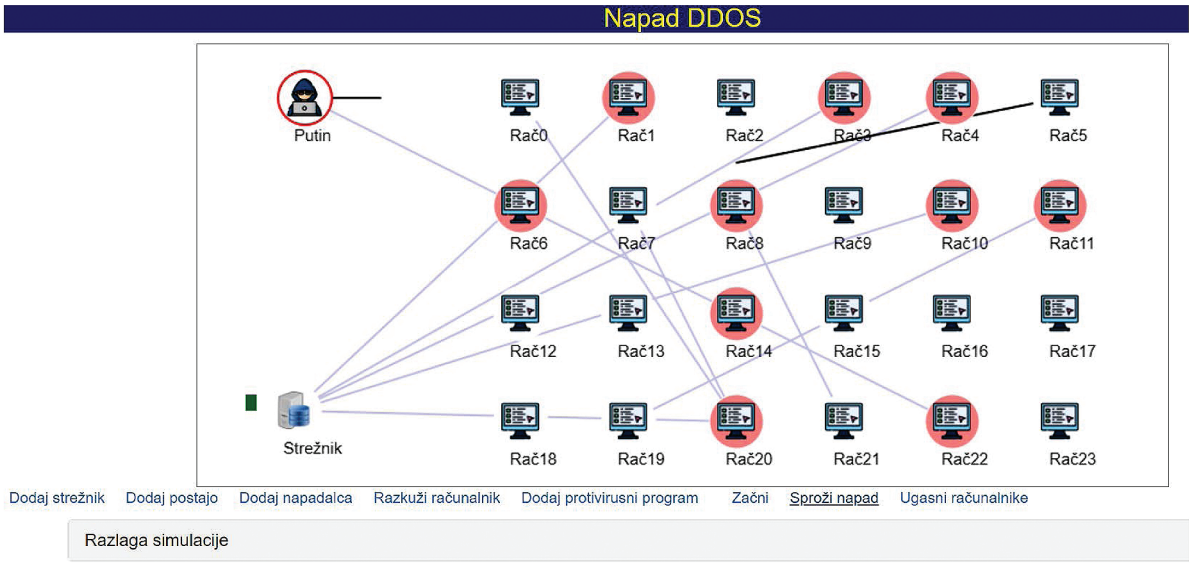
V nadaljevanju se bomo posvetili spletni aplikaciji, ki je enostavna in morda za dodatek pri predavanjih bolj primerna.

3 KIBERLETI

3.1 Razvoj kiberletov

V uvodu smo omenili fizlete predvsem zato, ker temeljijo na lastni, vendar odprtokodni platformi, ki je bila izhodišče za razvoj lastnih simulacij s področja kibernetske varnosti. Po zgledu fizletov smo razvili »kiberlete«, torej spletne računalniške animacije in simulacije, seveda grafično podprte, namenjene popestritvi predavanj in poučevanja na področju kibernetske varnosti.

Tako fizleti kot kiberleti so pisani v JavaScript. V obeh primerih je središče animacije knjižnica Animator.js, ki vsebuje kot razrede tipične gradnike s svojega problemskega področja. V primeru fizletov so to predvsem fizikalni delci, v primeru kiberletov pa so to računalniške komponente omrežja. Predvsem so to delovne postaje (stacionarni računalniki ali notesniki), pa strežniki. V primeru fizletov potekajo simulacije med spreminjanjem časa v inkrementih



Slika 1: **Simulacija porazdeljenega napada DDOS. Rdeče pobarvani računalniki so okuženi in delujejo v mreži BotNet**

dt, torej z oponašanjem sicer zveznega poteka pri fizikalnih pojavih. V primeru kiberletov pa v bistvu prehajamo od dogodka do dogodka. Več o ozadju kiberletov najdemo pri opisu njihove arhitekture.

Za boljše razumevanje delovanja kiberletov si najprej oglejmo en primer.

Primer take simulacije kaže slika 1, ki je utrinek iz računalniške upodobitve znanega porazdeljenega napada za zavračanje storitev (DDOS)

V tej simulaciji imamo mrežo delovnih postaj in en strežnik. Ena postaja pa je »posebna« in predstavlja napadalca. Simulacija začne s klikom na gumb »Začni«. Računalniki si začenjajo naključno pošiljati sporočila. In to na žalost počne tudi napadalec. Posebnost strežnika je, da na vsako sporočilo odgovori s svojim sporočilom (kar naj bi predstavljalo storitev, ki jo od njega pričakuje kličoči računalnik).

Sporočila napadalca pa so okužena. Prejemnik takega sporočila pordeči in odslej tudi sam s svojimi sporočili kuži svojo okolico. Sčasoma je tako na našem zaslonu čedalje več okuženih računalnikov.

V primernem trenutku kliknemo na link »Sproži napad«- Vsi okuženi računalniki začenjajo svoja sporočila usmerjati na napadeni strežnik, ki postaja preobremenjen (to kaže rast zelenega stolpca ob njem). To je le del tega scenarija.

3.2 Arhitektura kiberletov

Grobo zgradbo kiberletov prikazuje naslednji poenostavljen razredni diagram:

Glavni razred, Animator vsebuje podatke o sceni in njeni velikosti na spletni strani. Vsebuje tudi podatke o komponentah, ki to sceno sestavljajo. Poleg tega vsebuje metode za časovno krmiljenje simulacije oziroma animacije.

Objekti iz razreda Component imajo podatke o svojem položaju na sceni, o sliki, ki ta tak objekt predstavlja, o tipu (obliki) objekta ter o tem, ali je objekt fiksiran na scenu, ali pa ga lahko izbiramo in premikamo po sceni.

Objekti iz razreda Asset so v bistvu naprave, tipično računalniki ipd, ki jih uporabljamo v simuliranem okolju in jih primerno ščitimo.

Objekti iz razreda Person so uporabniki teh naprav. Njihove lastnosti vsebujejo podatke o njihovi strokovni in IT usposobljenosti, o njim dodeljenim napravam in o njihovih dovoljenjih.

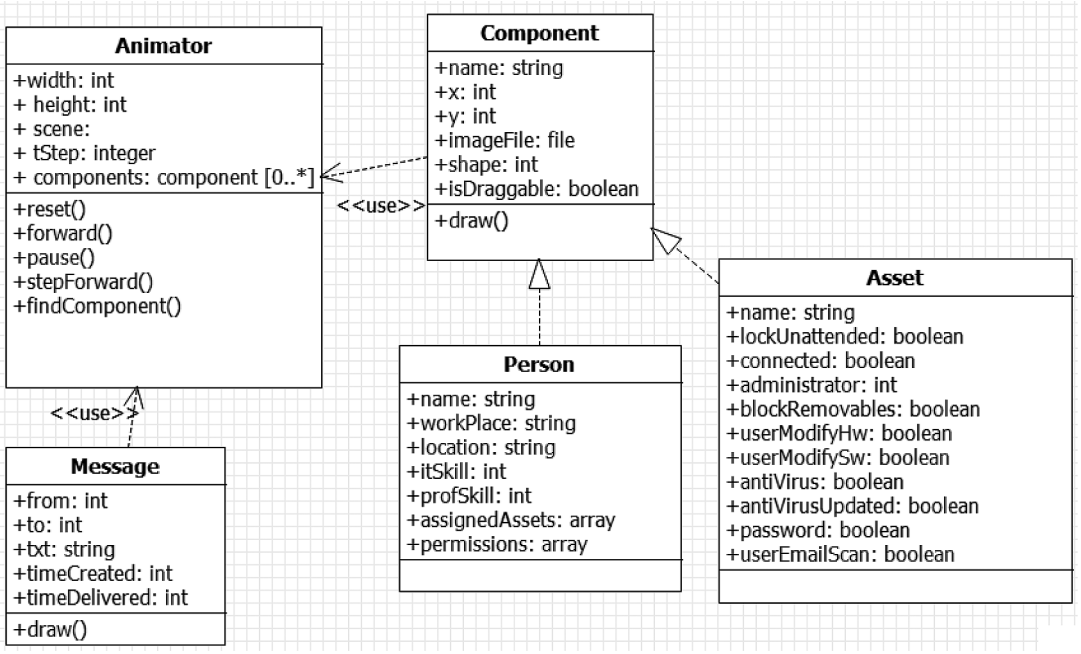
Objekti iz razreda Message vsebujejo podatke o sporočilih, ki potekajo od naprave do naprave.

To je osnovni koncept zgradbe kiberletov, ki pa se od primera do primera razlikujejo in so njihove dodatne značilnosti del JavaScript kode posamezne spletne strani.

3.3 Kaj še kiberleti omogočajo

V trenutni izvedbi so na voljo naslednje

- Širjenje okužbe po omrežju simulacije:
- Napad DDOS
- Napad moža v sredini
- Zaščiteni (šifrirani) kanali



Slika 2: **Poenostavljen razredni diagram kiberletov**

- Požarni zid
- Primerjava IDS in IPS
- Kerberos
- Internet stvari in kibernetska varnost
- Varnost v pisarni (ali manjšem podjetju)

Kiberlete najdemo na naslovu: http://sasa.musiclab.si/KIBERLETI/

V takih simulacijah lahko na »sceno« dodajamo različne komponente. Predvsem računalnike, ki so lahko v vlogi končnih delovnih postaj (tudi notesnikov) in strežnikov.

Računalniki se lahko okužijo, lahko jih tudi razkužimo in lahko jim dodajamo protivirusno zaščito. Računalnike lahko tudi vklapljamo ali izklapljamo. Dodajamo lahko nove strežnike, delovne postaje in tudi napadalce. Mrežo lahko (tudi med potekom simulacije) poljubno širimo.

Računalnike lahko izberemo s klikom miške in jih prestavljamo po zaslonu, morda zaradi boljšega pregleda.

V animacijah je sled sporočil običajno pobarvana modro, po koncu sporočila pa ostane še nekaj časa vidna svetlomodro. Simulacije kažejo vnaprej konfigurirano mrežo strežnikov, delovnih postaj (uporabniških računalnikov, notesnikov ipd) in napadalca.

Delovne postaje med seboj komunicirajo s sporočili. Posebnost strežnikov je, da na vsako prejeto sporočilo (zahtevek) pošljejo odgovor (izvedejo storitev, svoje sporočilo) .

Napadalci so tudi računalniki, ki pa le pošiljajo sporočila, ne morejo pa jih prejemati (so uporabnikom omrežja neznani)

Med kiberleti najdemo tudi simulacijo drugih pojavov, vezanih na kibernetsko varnost: napad moža

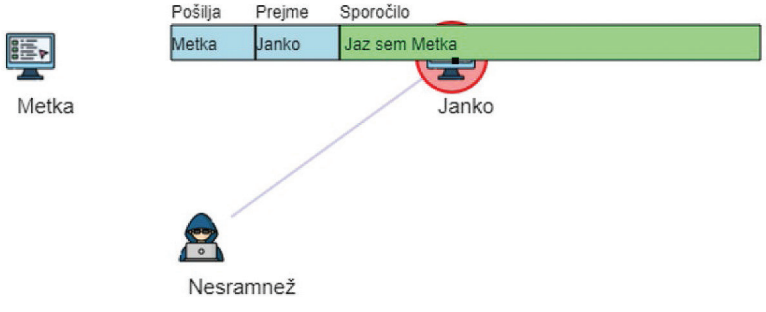


Figure 3: **Utrinek iz simulacije napada moža v sredini.**

Figure 4: **Utrinek iz simulacije šifriranih kanalov.**

v sredini, prenos podatkov preko šifriranih kanalov, vloga požarnega zidu in še kaj.

Naslednji zgled je na primer napad moža v sredini, kot ga kaže slika 3

Gre le za utrinek s simulacije, saj je celotna animacija bolj zgovorna. Napadalec je prestregel komunikacijo med Jankom in Metko in se v sporočilu Janku pretvarja, da je Metka. V resnici je format sporočila bolj zapleten. V tej simulaciji pa je napadalec spremenil glavo sporočila (in tudi samo besedilo), v katerem sta med drugim tudi podatka o pošiljatelju in prejemniku sporočila.

Pa še en utrinek iz simulacije šifriranih, torej zaščitenih kanalov. Prikazuje ga slika 4.

V tej simulaciji si Janko in Metka najprej izmenjala javna ključa. Nato pa si pošiljata sporočila, ki pa ga lahko vsakdo dešifrira le s svojim privatnim ključem. Uporabljeno je bilo resnično asimetrično šifriranje v JavaScript.

Med bolj kompleksimi simulacijami najdemo simulacijo pisarne (ali manjšega podjetja), ki mora z vidika kibernetske varnosti skrbeti za stanje svoje zaupnosti, celovitosti in razpoložljivosti. Na voljo ima zaposlene in računalniško opremo s svojimi lastnostmi, pa tudi politiko varovanja. Spodnja slika kaže utrinek s take simulacije, v okviru katere prihaja do različnih dogodkov, na primer poskusa vdora v strežnik, kraje podatkov ipd.

Kiberleti se ne izognejo niti bolj sodobni problematiki, kot je na primer kibernetska varnost pametnega doma, pametnega vozila ali oseb, opremljenih s pametnimi napravami, Spodnja slika kaže utrinek s take animacije.

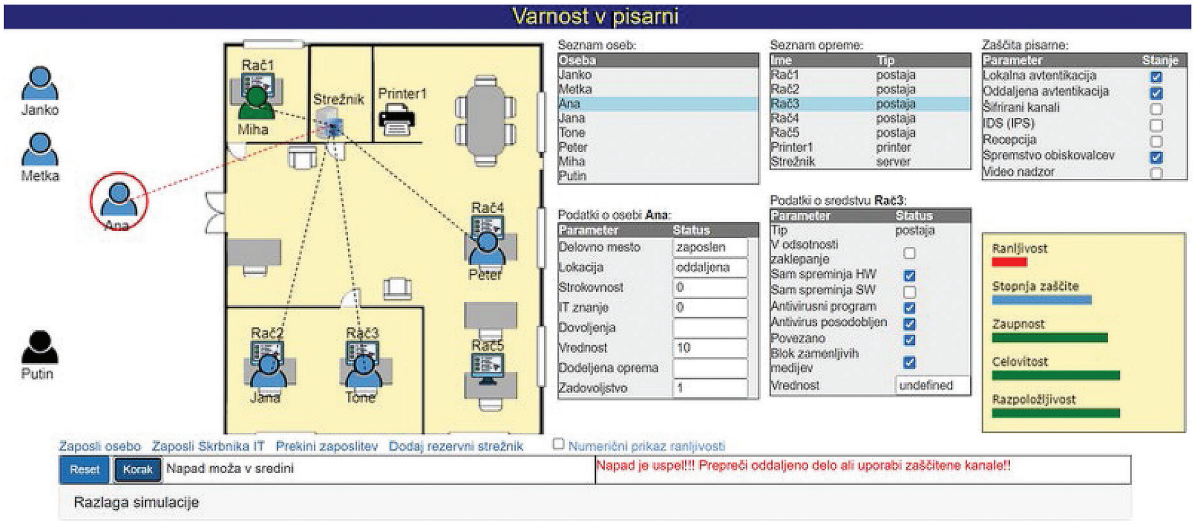


Figure 5: **Simulacija kibernetske varnosti v pisarni ali manjšem podjetju**

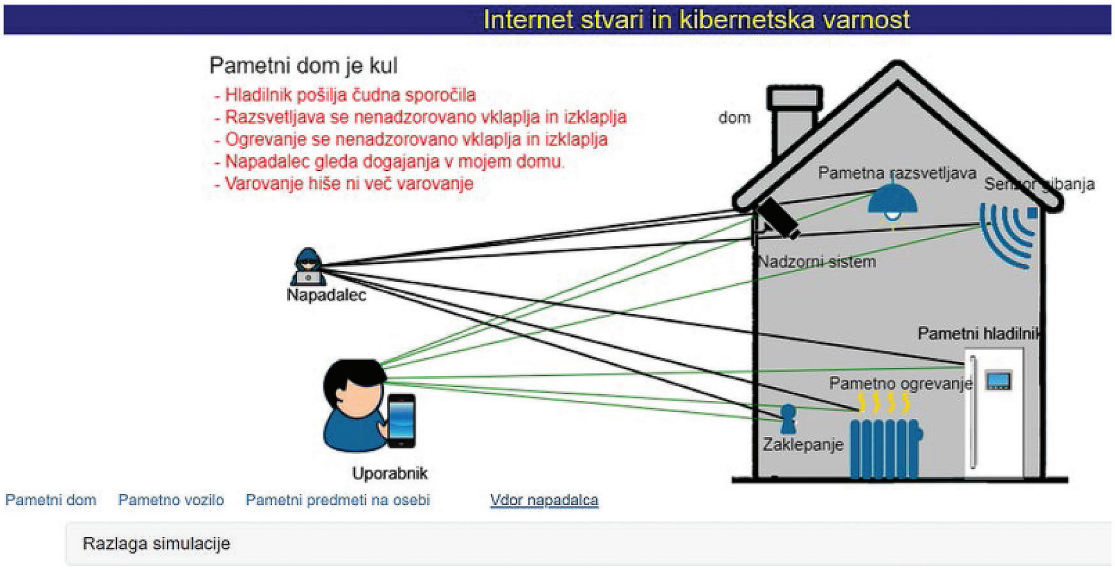


Figure 6: **Internet stvari in kibernetska varnost**

3.4 Razvoj novih kiberletov

Jedro kiberletov je zasnovano modularno in objektno usmerjeno tako, da si lahko izkušen računalnikar tudi sam izmišlja sorodne scenarije in sam sestavlja svoje simulacije. Seveda mora imeti za kaj takega primerno predznanje HTML in JavaScript.

Trenutna, še razvojna različica se nahaja na prej omenjenem naslovu. Celotna koda skupaj z vsemi JavaScript datotekami in slikami je zaenkrat prosto dostopna in seveda brezplačna pri avtorju. Zanjo velja licenca »CopyLeft«.

4 Zaključki

Kiberleti so uporabni tudi v sklopu spletnih učnih gradiv, saj so pisani v JavaScript in HTML. Že v trenutni obliki predvidevajo dvojno uporabo: Pri odprtju take strani je sama razlaga simulacije skrita. To je bolj primerno za predavanja, kjer kažemo le simulacijo. S klikom pa se razpre razlaga simulacije, kar je primerno bodisi pri pripravi predavatelja bodisi pri samoučenju.

Čeprav so navedene simulacije bolj ali manj preproste, lahko služijo popestritvi predavanj o kibernetski varnosti. Kot je pri takih simulacijah značilno, niso vse primerne za vsa možna pedagoška okolja. Tako so verjetno večinoma pretirane za uporabo na srednješolskem nivoju, vsaj kar se tiče predmeta Informatika v klasičnih gimnazijah. V srednjih šolah s področja računalništva pa bi bile lahko koristne. Tudi na univerzitetnem nivoju so uporabne. Ker so odprtokodne in prosto dostopne omogočajo pa tudi nadgradnjo v obliki seminarskih nalog.

Zanimiva je tudi misel, da bi kiberlete nadgradili z možnostjo vključevanja vanje preko drugih, v omrežje navezanih računalnikov. Po analogiji s spletnimi mnogouporabniškimi igricami bi lahko uvedli nekakšne sodelavne simulacije. Tako bi lahko bila taka mnogouporabniška izkušnja še bolj realistična.

5 LITERATURA

[1] Wolfgang Christian, Mario Belloni, Anne Cox, Melissa Dancy: Physlets; https://www.physport.org/curricula/physlets/
[2] Saša Divjak: Fizika s fizleti; http://sasa.musiclab.si/fizleti/
[3] MIT mathlets; https://mathlets.org/
[4] Chemlets (chemistry applet animations): https://lead.mst.edu/mathscicon/chemistry/chemlets/
[5] Cyber Security Awareness Training with Automated Phishing Simulations; https://attacksimulator.com/
[6] FourCore ATTACK Security Control Validation, https://fourcore.io/
[7] Hardik Manocha: Top 10 Awesome Open-Source Adversary Simulation Tools; https://fourcore.io/blogs/top-10-open-source-adversary-emulation-tools
[8] firedrill: A malware simulation harness; https://github.com/FourCoreLabs/firedrill
[9] Simulate, Validate, and Mitigate with the Infection Monkey; https://www.akamai.com/infectionmonkey
[10] CyberCIEGE: https://nps.edu/web/c3o/cyberciege
[11] Saša Divjak: Kibernetski napadi; http://sasa.musiclab.si/KIBERLETI/
[12] Kennedy Mwangi: Implementing Public Key Cryptography in JavaScript; https://www.section.io/engineering-education/implementing-public-key-cryptography-in-javascript/

▪

Saša Divjak je zaslužni profesor Univerze v Ljubljani, Fakultete za računalništvo in informatiko. Bil je Vodja odseka za avtomatiko, robotiko in biokibernetiko in kasneje načelnik oddelka za elektroniko na Institutu Jozef Stefan, pomočnik direktorja Iskre Delte, prodekan za raziskovalno delo na Fakulteti za elektrotehniko in računalništvo, prodekan za raziskovalno delo na Fakulteti za računalništvo in informatiko, dekan na Fakulteti za računalništvo in informatiko Univerze v Ljubljani , gostujoči profesor na Fakulteti za informatiko Univerze v Vidmu, Predstojnik Katedre za programsko opremo na Fakulteti za računalništvo in informatiko v Ljubljani. Predsednik Slovenske sekcije IEEE. Predstojnik Laboratorija za računalniško grafiko in multimedije na Fakulteti za računalništvo in informatiko, odgovoren za več projektov s področja multimedijskih tehnologij, Predsednik računalniške sekcije v sklopu slovenskega društva IEEE, član Izvršnega odbor ACM Slovenija, Senior member IEEE. Predsednik mednarodnega združenja CoLoS (Conceptual learning of Science). Predsednik generalne skupščine mednarodnega združenja HSci (Hands on Science), član in predsednik Evropske akademije znanosti (www.eurasc.org). Nosilec več projektov, predvsem s področja simulacije in avtomatizacije različnih tehnoloških procesov. Koavtor programske opreme prvih slovenskih robotov, sodelavec na italijanskem izobraževalnem projektu »Tovarne prihodnosti«. Nosilec več domačih in mednarodnih projektov s področja multimedijskih tehnologij v izobraževanju.