SVEUČILIŠTE U ZAGREBU

**FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA**

SEMINARSKI RAD

**SIGURNOST ALATA ZA VIDEOKONFERENCIJE**

Ema Popović

Zagreb, prosinac 2020.

Sadržaj

[Uvod 1](#_Toc58002052)

[1. Videotelefonija i videokonferencija 2](#_Toc58002053)

[2. Alati za videokonferencije 4](#_Toc58002054)

[2.1. Microsoft Teams 4](#_Toc58002055)

[2.2. Zoom 6](#_Toc58002056)

[2.3. Zaštita 7](#_Toc58002057)

[Zaključak 8](#_Toc58002058)

[Literatura 9](#_Toc58002059)

# Uvod

U današnje doba videokonferencija je postala primarni način interakcije u akademskom i poslovnom svijetu. Dostupnost kvalitetnih alata i sustava posljedica je mnogih tehnoloških inovacija prošlog i ovog stoljeća. Brzi Internet, novi softveri, kvalitetna računala i kamere postepeno su postali dostupniji javnosti. Pojavom koronavirusa potreba za kvalitetnim alatima za videokonferenciju se nepredvidivo povećala. Mnoge kompanije svjedočile su velikom porastu korisnika, ali time i većim prijetnjama. Dva često korištena alata za videokonferencije su Microsoft Teams i Zoom. Teams je i prije pandemije uživao raširenost u korporativnom svijetu zahvaljujući popularnosti Microsoft Officea, dok je Zoom tijekom 2020. godine ušao u svakodnevni rječnik i živote mnogih. Uz velik broj korisnika svaki alat se susreće i s velikim brojem problema vezanih uz zaštitu podataka. Svi imaju svoje mane i vrline, no nijedan nije siguran ako programeri, ali i korisnici nisu svjesni potencijalnih opasnosti.

# Videotelefonija i videokonferencija

Videotelefonija je tehnologija koja se bavi komunikacijom u stvarnom vremenu koristeći audiovizualne signale udaljenih korisnika.[1] Videokonferencija označava primjenu videotelefonije za službene i neslužbene sastanke grupa.

Prvi sustav za videokonferencije je 1970. godine predstavila američka telekomunikacijska kompanija AT&T. Ljudima je usluga bila omogućena u uredima ili vlastitom domu. Slanje signala se događalo analogno za kratke, a digitalno za duge udaljenosti, korištenjem iste tehnologije kao za telefoniju. Do kasnih 1990-tih videotelefonija se iz luksuza razvila u standardiziranu tehnologiju koja uz visoku kvalitetu i nisku cijenu nudi svoju uslugu cijelom svijetu. Za napredak je zaslužan razvoj mnogih tehnologija: video kodeka (koji nudi efikasniju kompresiju), jačih procesora i usluga Interneta s velikom propusnosti. Videokomunikacija postala je popularna 2000-tih godina uz pojavljivanje besplatnih usluga kao što su Skype i iChat. Uz niske cijene, pa i nisku kvalitetu, uvele su ovaj način komunikacije u javnu svijest.

U proteklih 10 godina videotelefonija je nastavila svoj razvoj, zahvaljujući napretku i popularnosti Interneta, te razvoju kamera pametnih mobitela i osobnih računala. Novi sustavi i softveri za videokonferencije omogućavaju prijenos kombinacije videa, zvuka, pa čak i crtanja po ekranu u stvarnom vremenu kroz sigurnu mrežu. Mnoge kompanije su počele i razvoj mobilnih verzija svojih sustava. Prijenos signala događa se putem digitalne ISDN i IP transmisije, što omogućava brzo slanje velike količine podataka generirane kamerama i mikrofonima. Ovakvi sustavi računaju na njihovo korištenje tijekom konferencija i time prijenos podataka velikog broja korisnika s različitih lokacija. Spomenuta tehnologija omogućuje dostupnost sastanaka na daljinu i smanjuje potrebu za putovanjem, što je korisno u gotovo svakoj branši. Prisutan je porast telemedicine kako bi invalidi, stariji i ljudi na dalekim lokacijama imali olakšani pristup zdravstvenim uslugama.[2] Tvrtke su također prihvatile ovu tehnologiju i koriste ju za udaljenje sastanke i konferencije. Videotelefonija igra veliku ulogu i u telekomunikaciji gluhih, nagluhih i nijemih ljudi, kojima je omogućena komunikacija znakovnim jezikom. U edukaciji videokonferencije pružaju mogućnost učenja s udaljenih lokacija, prilike za virtualnu suradnju, dovođenje gostujućih predavača i uvođenje tema koje nisu fizički dostupne. Kroz 2020. godinu potražnja za sustavima videokomunikacije drastično je porasla, uzrokovana pandemijom koronavirusa. U mnogim djelatnostima posao je postao opasan ili čak nemoguć bez videokonferencija i udaljenje komunikacije. Nastaju novi alati i mnoge kompanije prilagodile su postojeće proizvode novom opsegu korisnika.

# Alati za videokonferencije

Tradicionalne aplikacije za video pozive koriste komunikacijsku tehnologiju VoIP (eng. Voice over Internet Protocol). VoIP pretvara audio signal u digitalne podatke i prenosi ih preko internetske mreže.[3] Omogućava besplatno telefoniranje s računala na računalo i jeftiniju alternativu razgovora na telefon.

Na ovoj osnovi su razvijene i dvije aplikacije koje će se detaljnije promatrati, Microsoft Teams i Zoom. Audio i video podaci se konvertiraju u digitalni signal, optimiziraju i pošalju primatelju. Teams i Zoom dva su alata koja su stekla veliku popularnost i broj korisnika 2020. godine. Microsoft Teams se i prije pandemije često koristio u poslovne svrhe, te povezivao zaposlenike velikih tvrtki. Na računalu dolazi uz paket Microsoft Office, spreman za korištenje. Zoom se od gotovo nepoznatog alata ove godine pretvorio u jedan od najčešćih načina komunikacije. Intuitivan je i jednostavno ga mogu koristiti pojedinci u privatne i poslovne svrhe.

## Microsoft Teams

Microsoft Teams je platforma za poslovnu komunikaciju koju je razvio Microsoft u sklopu obitelji proizvoda Microsoft 365. Nudi pregled radnog prostora i kontakata, pohranu datoteka, integraciju s drugim aplikacijama, chat i videokonferencije.

Microsoft je najavio svoju novu platformu Teams u ožujku 2017. godine. Sredinom 2018. godine objavljena je besplatna verzija alata. Nudila je većinu postojećih mogućnosti, ali uz manji broj korisnika i manji kapacitet pohrane. Kroz protekle dvije godine gotovo je zamijenila Skype u poslovnim videokonferencijama. Prelazak s komunikacije uživo na onu putem Interneta zbog koronavirusa bila je pogodna za alat. Od ožujka do travnja 2020. alat je porastao s 44 milijuna na 75 milijuna dnevnih korisnika.[4]

Alat je baziran na mnogim Microsoftovim protokolima. Videokonferencija se realizira pomoću protokola MNP24 (eng. Microsoft Network Protocol version 24) umjesto SIP protokola. Koristi TCP pakete zaštićene TLS-om, što znači da su podaci u prijenosu nevidljivi bez odgovarajućeg privatnog ključa. Protokol postoji od 2014. godine od kada se primjenjuje i na Skype-u. Ako se računala ne mogu povezati na peer-to-peer način zbog vatrozida ili NAT usmjerivača, koristi se ICE tehnika (eng. Interactive Connectivity Protocol). Ona se koristi u umrežavanju kako bi računala mogla komunicirati što direktnije. ICE tehnika je najčešće korištena za VoIP, instant poruke i peer-to-peer komunikaciju jer je komunikacija pomoću centralnog poslužitelja znatno sporija.

Mnogi su napadi na podatke korisnika detektirani, no oni su često posljedica ljudskih pogreški i nemarnog upravljanja. Jedan od mogućih pristupa podacima korisnika je pomoću slanja maliciozne e-pošte. Pri prijavljivanju na Teams korisnikov klijent stvori privremene tokene koji pomažu pri autorizaciji i autentifikaciji. Napadač mora dobiti pristup jednoj od nekoliko Teams-ovih rizičnih poddomena. Nakon toga žrtvi šalje GIF e-poštom, koji nakon otvaranja preusmjerava na kompromitiranu poddomenu. Kroz ovo preusmjeravanje napadač dobiva pristup žrtvinom tokenu za autorizaciju. Uz posjedovanje jednog tokena napadač može pristupiti e-pošti žrtve, predstaviti se kao ona i poslati maliciozni GIF njezinim kontaktima.[5] Ovakav napad može ugroziti svakog korisnika Teams alata, time i cijele tvrtke i organizacije. Za sprječavanje napada Microsoft treba eliminirati rizične poddomene i nastaviti s razvojem sigurnosti. Još jedna mjera opreza bila bi promijeniti način autentifikacije korisnika pomoću tokena.

Osim samih GIF-ova, mnogi napadači preusmjeravaju žrtvu na lažne ekrane za prijavu u svrhu otkrivanja korisničkog imena i lozinke. Novi napadači vrlo su pažljivi i profesionalni. Ne šalju obavijesti i uzbune koje sliče stvarnima, već zatraže dodatnu prijavu ili unos podataka na novoj stranici. Odredišne stranice izgledaju identično stvarnima, sa slikama i tekstom kopiranim iz stvarnih alternativa. Registriraju i nove domene kako bi izgledale kao sigurni izvori. Korisnici su postali naviknuti na obavijesti davatelja usluga, pa poruka koja traži prijavu u drugu Microsoft aplikaciju (npr. Microsoft SharePoint) ne izgleda sumnjivo. Microsoftovi podaci s Teamsa skupljaju se u SharePointu svakog korisnika i pristup njima može rezultirati velikom štetom. Već do početka svibnja zabilježeno je 50,000 korisnika koji su bili izloženi ovakvom napadu.[6] O prevarama putem e-pošte je potrebno dobro educirati zaposlenike, pogotovo kada ljudi rade iz domova i većinski komuniciraju putem Interneta.

Iako je Microsoft velika i razvijena tvrtka, sigurnost alata nije zadaća samo njih, već i svakog pojedinog korisnika. Nepažnja može dovesti do odavanja privatnih podataka korisnika i cijele organizacije. Pomoću pristupa jednom računu može se pristupiti drugima, ali i poslati lažne informacije koje mogu dovesti do gubitka tajnosti i financijske štete.

## Zoom

Zoom je alat za videotelefoniju koji je razvila američka tvrtka Zoom Video Communications. Koristi se za videopozive, ima mogućnost prijenosa video i audio signala, te chat.

Tvrtka Zoom Video Communications objavila je alat Zoom već krajem 2012. godine sa sjednicama u kojima je prisustvovalo maksimalno 15 ljudi. Alat se razvijao uz suradnju i pokroviteljstvo različitih tvrtki. Do 2020. godine nije ušao u svijest šire javnosti. Prosječni broj dnevnih korisnika narastao je od 10 milijuna u prosincu 2019. godine godine do preko 300 milijuna u travnju 2020. godine. Njegova jednostavnost i funkcionalnosti besplatne verzije privukli su mnoge pojedince i mala poduzeća.

Alat je kompatibilan s mnogim operacijskim sustavima, uključujući Windows, Linux, macOS i Android. Ima jednostavno sučelje i relativno lako se koristi, što je privuklo ljude koji se ne razumiju u tehnologiju. Nude se opcije sastanka jedan na jedan, grupnog sastanka, dijeljenja ekrana i snimanja sastanaka. Besplatna verzija omogućava sastanke s do 100 istovremenih sudionika i s vremenskom granicom od 40 minuta.

Neke od sigurnosnih značajki su mu sastanci zaštićeni lozinkom, autentifikacija korisnika i nasumično odabrani ID-jevi. Moguć je način u kojem su sudionici smješteni u čekaonicu dok ih domaćin ne odluči primiti u sastanak. Domaćin također može ukloniti sudionike i onemogućiti dijeljenje ekrana.[7] Od lipnja 2020. godine potpuno (end-to-end) šifriranje uvedeno je za korisnike koji plaćaju, a od listopada je ponuđeno i besplatno. Zoom koristi AES 256 GCM šifriranje toka podataka. AES (eng. Advanced Encryption Standard) je američki državni standard za šifriranje i pripada porodici simetričnih blok šifri. 256 označava da je ključ korišten za šifriranje veličine 256 bitova. Za streaming medija koristi ključ veličine 128 bitova. GCM je algoritam šifriranja dizajniran kako bi osigurao autentičnost i povjerljivost podataka.

Mnoge ranjivosti su uočene u alatu kroz godine. U studenome 2018. godine otkriveno je da se neautentificirani napadač može uključiti u komunikaciju pomoću UDP poruka. Takav pristup omogućava napadaču da ukloni korisnike iz sastanka, lažira poruke i dobije pristup dijeljenom ekranu.[8] Tvrtka je ubrzo dodala zakrpu koja je popravila sigurnost. U srpnju 2019. godine pronađena je zero-day ranjivost prisutna na macOS-u. Bilo koja stranica mogla je natjerati macOS korisnika da se pridruži Zoom pozivu, s uključenom kamerom, bez odobrenja. Pri pokušaju deinstalacije alat bi se automatski opet instalirao u pozadini. Nakon žalbi od javnosti ranjivost je uklonjena. Na Internetu se također javljaju programi instalateri koji u sebi skrivaju zlonamjerni softver. Ako korisnik nije pažljiv i skine instalater s neslužbene stranice, može neželjenom softveru dati pristup svojim podacima. Kroz 2020. godinu pronađen je veći broj sigurnosnih problema, ali tvrtka brzo popravlja neispravnosti i uklanja rizične značajke. Osim uvođenja potpunog šifriranja formirali su CISO vijeće, rade s trećom stranom koja testira sigurnost i savjetuju se sa stručnjacima. Korisnici trebaju imati na umu svoje postavke, prihvaćati sastanke samo s poznatima i provjeravati izvore alata i informacija.

## Zaštita

Za sigurnost s korisničke strane se moraju njegovati dobre prakse korištenja Interneta. Mnogi korisnici s prosječnim znanjem o tehnologiji ne pridržavaju se svih aspekata sigurnosti na Internetu. Računaju da će ih davatelji usluga zaštititi. Ipak, osoba kao korisnik Internet mora razviti medijsku pismenost, znati sama zaključivati u potencijalno opasnim situacijama. Ne smije se slijediti svaku poveznicu, potrebno je razmisliti o okolnostima i provjeriti izvor. Također je potrebno pratiti kakva dopuštenja se daju stranicama kojima se pristupa i čitati pravila korištenja. Instalateri alata i resursi trebaju se prihvaćati samo od provjerenih i službenih stranica tih resursa.

Programeri alata kao što su Microsoft Teams i Zoom moraju postaviti sigurnost kao prioritet pri stvaranju softvera. Sve ranjivosti se moraju uklanjati kad god su otkrivene. Sigurnost bi trebala biti jednakog prioriteta bez obzira na (ne) plaćanje za usluge. Mnogi alati za videokonferencije imaju problema s prisluškivanjem i autentifikacijom. Ovo su veliki problemi, promet na alatima se povećava svaki mjesec i potrebno je zaposliti kvalificirane ljude kao pomoć. Potrebno je provoditi šifriranje podataka tijekom komunikacije. Moderatori trebaju kontrolirati lažne web stranice kako bi korisnici imali pristup istinitim informacijama. Provjeru sigurnosti treba obavljati neovisni stručnjak sigurnosti kako ne bi došlo do previda određenih ranjivosti. Korisnicima se trebaju pružiti sve potrebne informacije o sigurnosti i trebaju biti obavezne za čitanje, inače će ih većina korisnika preskočiti. Primjer velikog rasta korisničke baze ove godine pokazuje da se treba voditi briga i o skalabilnosti alata kako bi korisnici uvijek bili sigurni.

# Zaključak

Videokonferencija u 2020. godini jedan je od najčešćih i najsigurnijih načina komunikacije s većim brojem ljudi. Alati korišteni u ovu svrhu dosežu neplanirani vrhunac broja korisnika. Problem nastaje u većem broju napadača koji proizlazi iz situacije. Različiti alati imaju različite razine sigurnosti, ali nijedan nije posve siguran. Programerima zaštita podataka ne smije biti samo naknadna misao u razvoju proizvoda. Šifriranje podataka, zapošljavanje stručnjaka i održavanje točnosti dostupnih informacija nužni su za pravilno održavanje sigurnosti. Korisnici moraju razviti medijsku pismenost i uzeti u obzir moguće napadače. Potrebno je provjeravati integritet izvora podataka i informirati se o načinima zaštite. Sigurnost je proces te u njemu moraju sudjelovati i programeri i korisnici.

# Literatura

1. McGraw-Hill, McGraw-Hill Concise Encyclopedia of Engineering. Videotelephony. 2002.
2. Videophone Scheme Could Provide ‘Virtual Care’ for Elderly Residents. Europe Intelligence Wire, Aberdeen Press & Journal. 2006.
3. VOIP – Internet Telefonija, <https://franz-net.hr/voip-internet-telefonija/> datum pristupa: 3. 12. 2020.
4. Tilley, A. Microsoft takes on Zoom and Slack in a Battle for Your Work Computer. 2. 6. 2020. <https://www.wsj.com/articles/microsoft-aims-to-dominate-technology-at-work-starting-with-those-video-calls-11591108757> datum pristupa: 4. 12. 2020.
5. Tsarfati, O. Beware of the GIF: Account Takeover Vulnerability in Microsoft Teams. 27. 4. 2020. <https://www.cyberark.com/resources/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams> datum pristupa: 4. 12. 2020.
6. Winder, D. Beware This New Microsoft Teams Password Hacking Threat To 75 Million Users. 2. 5. 2020. <https://www.forbes.com/sites/daveywinder/2020/05/02/beware-this-new-microsoft-teams-password-hacking-threat-to-75-million-users/#da60e5f2fbc6> datum pristupa: 4. 12. 2020.
7. Osborne, C. Zoom Security: Your meetings will be safe and secure if you do these 10 things. 22. 4. 2020. <https://www.zdnet.com/article/make-sure-your-zoom-meetings-are-safe-by-doing-these-10-things/> datum pristupa: 4. 12. 2020.
8. CVE-2018-15175 Detail. 9. 10. 2019. <https://nvd.nist.gov/vuln/detail/CVE-2018-15715> datum pristupa: 4. 12. 2020.