CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnosni rizici web aplikacija za pristup elektroničkoj pošti

CCERT-PUBDOC-2008-12-238

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Pristup elektroničkoj pošti putem web aplikacija postaje sve popularniji, tim više što su korisnici u stalnom pokretu i bitno im je da mogu pristupiti svojim porukama elektroničke pošte s bilo kojeg računala povezanog na Internet. Sve je više pružatelja usluga besplatnih korisničkih računa elektroničke pošte. Osim toga, zbog velike konkurencije na području web mail servisa, sve više pružatelja usluga nudi veliki kapacitet za pohranu poruka elektroničke pošte. Osim običnih ljudi koji koriste web mail javnih pružatelja usluga elektroničke pošte (npr. Gmail, Yahoo! Mail, Hotmail), web mail servise koriste i tvrtke te sveučilišta koja posjeduju vlastite poslužitelje elektroničke pošte. Pri tome za pristup elektroničkoj pošti koriste neku od web aplikacija, kao što su Outlook i SquirrelMail. Iako web pristup sandučiću elektroničke pošte ima mnogo prednosti, postoji i mnogo sigurnosnih problema vezanih kako uz web mail aplikacije, tako i uz prijenos podataka između klijenta i poslužitelja. U nastavku slijedi opis web mail sustava, usluga i sigurnosti najpoznatijih web mail servisa te sigurnosni rizici korištenja web mail aplikacija. Osim toga, dane su preporuke za sigurno korištenje web mail usluga te za dodatno povećanje sigurnosti.

2. Elektronička pošta

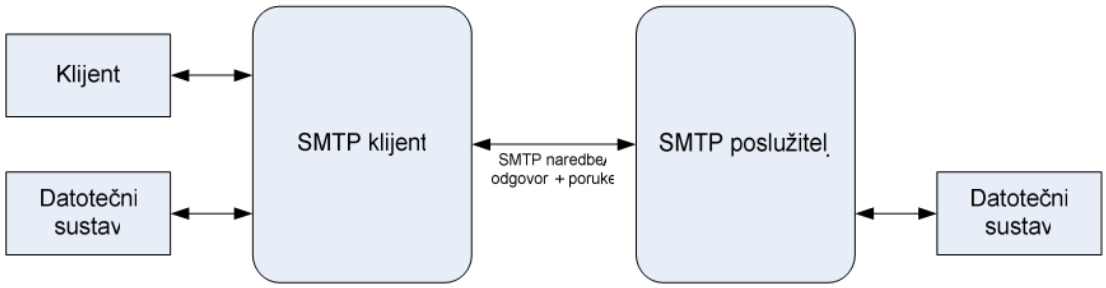
Komunikacija elektroničkom poštom postala je vrlo raširena i popularna te neophodna. Prema jednom istraživanju iz svibnja 2008. godine u svijetu ima oko 683 milijuna web mail korisnika od kojih svaki ima po nekoliko korisničkih računa elektroničke pošte te je aktivnih računa mnogo više, oko 1.2 milijarde. Rukovanje elektroničkom poštom uključuje primanje, sastavljanje i slanje poruka. Moderni sustavi elektroničke pošte temelje se na modelu „spremi-i-proslijedi" gdje poslužitelj elektroničke pošte prima i prosljeđuje ili sprema poruke. Sve što korisnik treba napraviti jest spojiti se na infrastrukturu elektroničke pošte sa svojeg računala. Prvi je sustav elektroničke pošte nastao 1966. godine. Podržavao je samo prijenos tekstualnih poruka koje su sadržavale isključivo ASCII znakove, no danas se mogu slati bilo kakvi podaci, kao što su multimedijalne datoteke.

Sustav elektroničke pošte koristi nekoliko protokola za prijenos elektroničke pošte, a oni su SMTP (eng. Simple Mail Transfer Protocol), POP3 (eng. Post Office Protocol version 3) i IMAP (eng. Internet Message Access Protocol). SMTP protokol se može koristiti za slanje i primanje elektroničke pošte, no kako je protokol ograničen u smislu sposobnosti da stavlja poruke u red na računalu koje ih prima, obično se koristi zajedno s POP3 ili IMAP protokolima. POP3 i IMAP protokoli omogućuju korisniku da poruke čuvaju na poslužitelju te da ih prenesu na lokalno računalo. Dakle, uobičajeno je koristiti SMTP protokol za slanje elektroničke pošte, a jedan od protokola, POP3 ili IMAP za primanje poruka elektroničke pošte. Prilikom slanja i primanja svaka se poruka elektroničke pošte stavlja u omotnicukoja sadrži podatke potrebne za prijenos poruke, kao što su odredišna adresa, prioritet, sigurnosna razina. Svaka se poruka sastoji od dva dijela: zaglavlja i tijela. U zaglavlju se nalaze podaci potrebni za rukovanje porukom tijekom njena prijenosa. Tijelo poruke je namijenjeno primatelju elektroničke pošte i ono ostaje nepromijenjeno tijekom prijenosa.

2.1. SMTP

SMTP (eng. Simple Mail Transfer Protocol) je komunikacijski standard za prijenos elektroničke pošte putem Interneta. Definiran je kao standard s oznakom RFC 821 (STD 10), i 2008. godine obnovljen s oznakom RFC 5321, koji opisuje ESMTP (eng. extended SMTP) standard.

Njegova je svrha osigurati pouzdan prijenos poruka elektroničke pošte. Pritom se koristi TCP komunikacijski kanal. Većina sustava za rukovanje elektroničkom poštom za slanje poruka koristi SMTP protokol, a za preuzimanje POP3 ili IMAP protokol. Slijedeća slika pokazuje rad SMTP protokola.



Slika 1. Način rada SMTP protokola

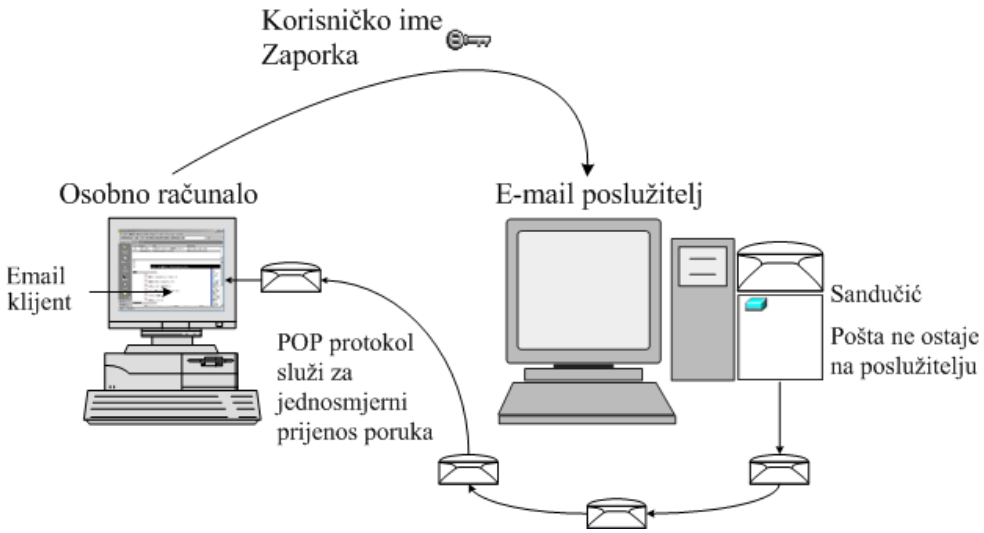
SMTP je jednostavan protokol kod kojega mogu postojati jedan ili više primatelja poruka. Prijenos poruke uključuje komunikaciju poslužitelja i klijenta u smislu postavljanja niza pitanja i primanja odgovora na postavljena pitanja. SMTP klijent može biti ili korisnička klijentska aplikacija (eng. Mail User Agent – MUA), ili poslužitelj za prijenos pošte (eng. Mail Transport Agent – MTA).

Elektronička se pošta putem Interneta prenosi tako da izvorišno računalo uspostavi TCP vezu na vrata (eng. port) 25 odlaznog poslužitelja elektroničke pošte. Osluškivanjem spomenutih vrata poslužitelj koji „razumije" SMTP prihvaća dolazne veze, preuzima poruke i sprema ih u odgovarajuće sandučiće dolazne pošte. SMTP je „gurajući" (eng. push") protokol koji ne može „povući" (eng. pull) poruke sa udaljenog poslužitelja na zahtjev. Za dohvaćanje poruka na zahtjev potrebno je koristiti POP3 ili IMAP.

2.2. POP3

POP3 (eng. Post Office Protocol 3) je protokol koji se koristi za primanje elektroničke pošte. Korisnik ne mora biti stalno spojen na Internet da bi dobio elektroničku poštu. Dovoljno je da se periodično spoji i upotrebom POP3 protokola poruke koje se nalaze na poslužitelju prebacit će na lokalno računalo. POP3 protokol osmišljen je tako da se poruke koje se nalaze na poslužitelju obrišu čim se prenesu na lokalno računalo, no neke primjene dozvoljavaju korisniku da izabere želi li ostaviti kopiju poruke na poslužitelju ili ne.

Kada korisnik pristupa elektroničkoj pošti preko klijentske aplikacije, kao što je Outlook Express, tada koristi POP3 protokol koji obavlja jednosmjerni prijenos poruka s poslužitelja na lokalno računalo. To je moguće vidjeti i na slijedećoj slici.



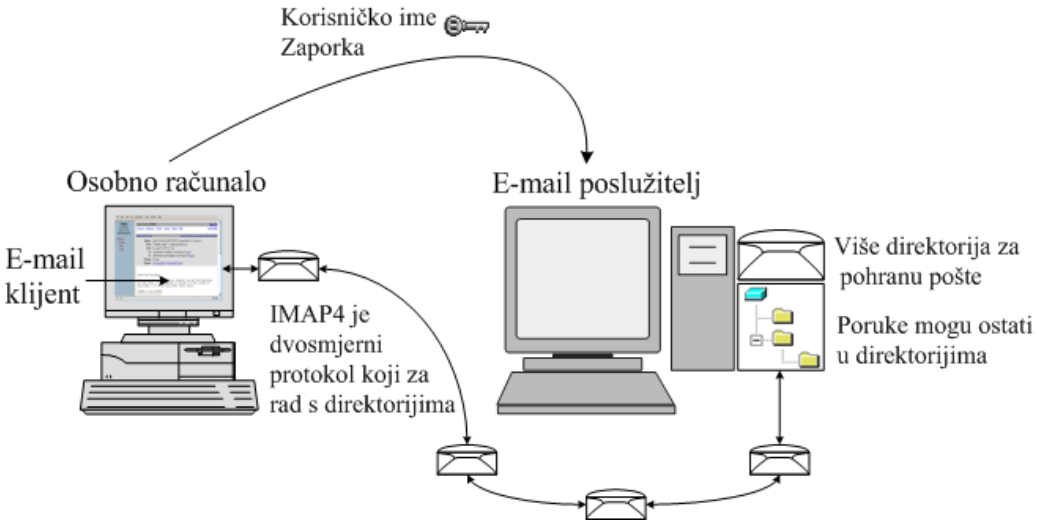
Slika 2. Pregled elektroničke pošte preko protokola POP3

2.3. IMAP

IMAP (eng. Internet Message Access Protocol) je protokol koji se uz POP3 koristi za primanje poruka elektroničke pošte. IMAP pruža korisniku više mogućnosti za primanje elektroničke pošte te omogućuje korisniku organizaciju direktorija na poslužitelju. IMAP protokol poznat je pod nazivom IMAP4 (inačica 4) i definiran je standardom RFC 3501.

Protokol se može koristiti za primanje elektroničke pošte kada je računalo stalno povezano na Internet te u slučaju kada nije. Klijentske aplikacije koje koriste IMAP u pravilu ostavljaju kopiju poruke elektroničke pošte na poslužitelju sve dok ju korisnik sam ne obriše. Također, podržava spajanje više korisnika istovremeno na isti sandučić elektroničke pošte. Mnoge primjene web mail servisa koriste IMAP4 protokol za primanje poruka elektroničke pošte s poslužitelja i njihov prikaz u web pregledniku.

Protokol IMAP4 ujedno prenosi poruke na klijentsko računalo i omogućava upravljanje direktorijima te olakšava organizaciju sandučića elektroničke pošte na poslužitelju. Kada se elektroničkoj pošti pristupa preko web mail aplikacije, korisnik poštu može čitati, pisati, slati i organizirati iz web preglednika s bilo kojeg računala spojenog na Internet, kao što prikazuje slika 3.



Slika 3. Pristup elektroničkoj pošti preko protokola IMAP4

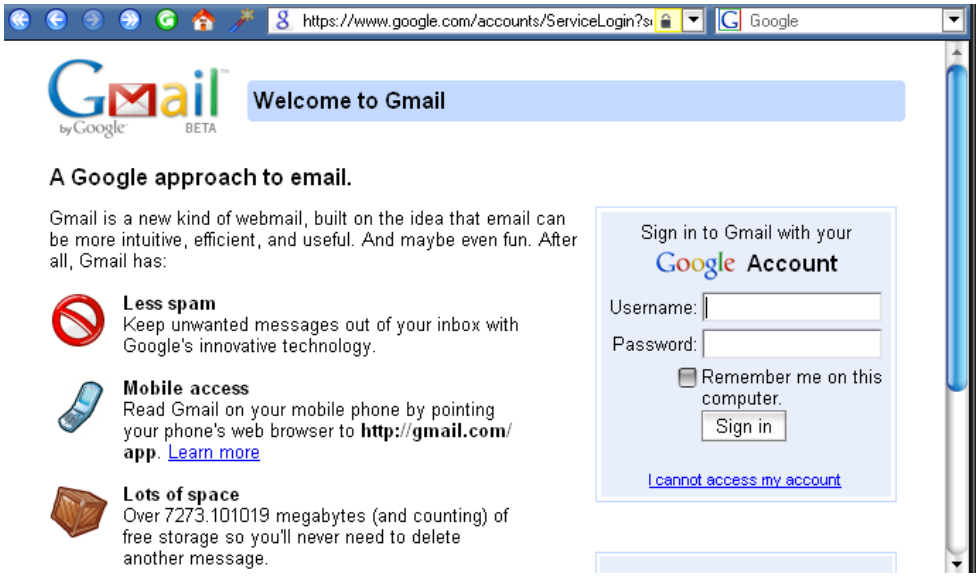
3. Web pristup sandučiću elektroničke pošte

Web mail, ili web pristup sandučiću elektroničke pošte, služi korisnicima kao sučelje za rukovanje porukama elektroničke pošte upotrebom web preglednika. Dakle, korisnik pristupa elektroničkoj pošti preko web aplikacije, umjesto preko klijenta elektroničke pošte (kao što su Microsoft Outlook, Mozilla Thunderbird i drugi). Najpopularniji web mail servisi su Gmail, Yahoo! Mail i Hotmail. Osim njih postoje i programski paketi koji korisnicima omogućuju postavljanje svojeg web mail poslužitelja i usluge, a neki od njih su Outlook Web Access (OWA), SquirrelMail, Horde IMP, itd.

Glavna prednost web mail servisa je mogućnost pristupa sandučiću elektroničke pošte s bilo kojeg računala povezanog na Internet. No glavna prednost može ujedno biti i velika mana zato što korisnik ne može pregledavati stare poruke kada nije povezan na Internet.

Korisnik svojoj elektroničkoj pošti može pristupiti putem web mail aplikacije ili preko klijenta elektroničke pošte instaliranog na njegovom računalu. Obično se pod izrazom „klijent elektroničke pošte“ smatra aplikacija postavljena na računalu korisnika koja se koristi za rukovanje elektroničkom poštom. Neki od takvih popularnih klijenata su Outlook Express, Mozilla Thunderbird, Eudora, itd. Ukoliko korisnik pristupa elektroničkoj pošti preko klijentske aplikacije, tada se poruke prenose u sandučić dolazne pošte i spremaju lokalno na računalu korisnika. Pri tome na poslužitelju može ostati kopija poruke spremljene na lokalno računalo. Zbog toga je poruke moguće čitati i ako je veza na Internet prekinuta. Nedostatak klijentske aplikacije za pristup elektroničkoj pošti je taj da nakon što je poruka primljena, nije joj moguće pristupiti s neke druge lokacije, odnosno s nekog drugog računala (osim ako nije ostavljena kopija poruke na poslužitelju). Glavni je nedostatak u tome da na nekom „stranom“ računalu treba podesiti parametre, pa i unijeti lozinke za čitanje pošte. Time se mijenjaju postavke izvornog korisnika računala, i iza nas ostavljamo naše podatke i iz poštanskog pretinca i o pristupu njemu. Osim toga, cijeli je proces spor.

Web mail servisi su se razvili upravo zbog potrebe korisnika da pristupaju elektroničkoj pošti s bilo kojeg računala, bilo gdje u svijetu. Prilikom upotrebe web mail usluga, poruke elektroničke pošte se ne prenose na lokalno računalo, već ostaju na poslužitelju. Nedostatak korištenja web mail aplikacija je i problem arhiviranja poruka. Mnoge tvrtke koje pružaju usluge web pristupa elektroničkoj pošti imaju ograničen prostor za spremanje poruka. Gmail je promijenio ovaj trend znatno povećavajući kapacitet prostora za spremanje poruka, no još je uvijek veliki broj web mail servisa koji omogućuju malo prostora (oko 5 do 10 MB) za spremanje pošte. Za pristup web mail servisu potrebno je svaki puta prijaviti se na sustav. Prijava na sustav uključuje upis korisničkog imena i zaporke te autentikaciju poslužitelja.



Slika 4. Web sučelje za prijavu na Gmail web mail poslužitelj

3.1. Povijesni razvoj web mail servisa

Prva web mail aplikacija imala je jednostavan naziv, WebMail i razvio ju je Luca Manunza sa Sardinije. Aplikacije je bila napisana u programskom jeziku Perl i objavljena je 1995. godine. 1997 godine Microsoft je uveo Hotmail kao uslugu web mail pristupa sandučiću te je postao jednim od popularnijih takvih aplikacija. Od tada su web mail servisi postali vrlo rašireni i popularni te su se počeli javljati pružatelji usluga web mail servisa kao što su kineski portal Sina te europski portali Voila.fr i GMX.de. Novi iskorak je napravio Google uvođenjem Gmail aplikacije 2004. godine. Google je uveo nove funkcionalnosti kao što su JavaScript izbornici, oglasi i ono najvažnije: veliki kapacitet pohrane poruka. Ova poboljšanja stimulirala su konkurenciju te su i ostali pružatelji web mail usluga morali poboljšati svoju web mail aplikacije, dodati nove funkcionalnosti te povećati kapacitet sa nekoliko MB na nekoliko GB za pohranu poruka elektroničke pošte.

Osim pružatelja web mail usluga, kao što su Gmail, Yahoo! Mail i ostali, razvijeni su i programski paketi kojima korisnici mogu stvoriti vlastiti web mail poslužitelj. Također sve više pružatelja Internet usluga počelo je pružati i web pristup sandučiću elektroničke pošte.

3.2. Programski paketi za web pristup elektroničkoj pošti

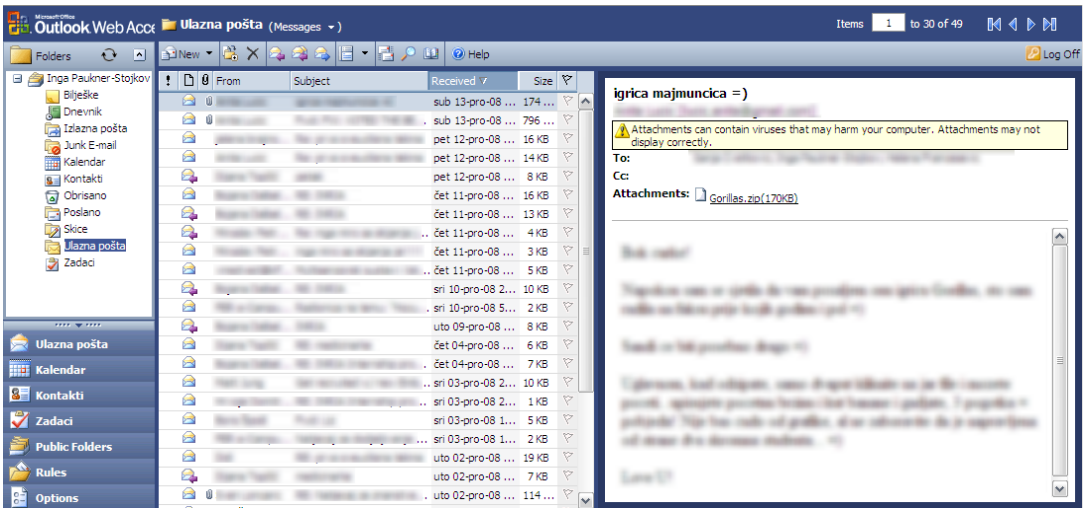
Razvijeni su i web mail programski paketi koji omogućuju stvaranje web mail poslužitelja. Poznati su takvi komercijalni i programski paketi otvorenog koda, a neki od poznatijih su:

- Outlook Web Access,
- Open WebMail,
- Horde IMP te
- SquirrelMail.

Mnoga sveučilišta i tvrtke koriste takve programske pakete te imaju svoje web mail poslužitelje kojima se može pristupiti preko web preglednika.

3.2.1. Outlook Web Access

Outlook Web Access (OWA) je web mail servis koji krajnjim korisnicima pruža web pristup sandučiću elektroničke pošte. Pri tome sandučić elektroničke pošte se nalazi na poslužitelju na kojem je postavljen programski paket Microsoft Exchange Server, inačice 2003 i 2007. OWA i Microsoft Exchange Server su aplikacije koje zajedno čine web mail sustav. Takav sustav obično postavljaju tvrtke, sveučilišta i škole. Web sučelje klijentskog dijela sustava, OWA, ima izgled korisničkog sučelja programa Microsoft Outlook, kao i njegove funkcionalnosti.

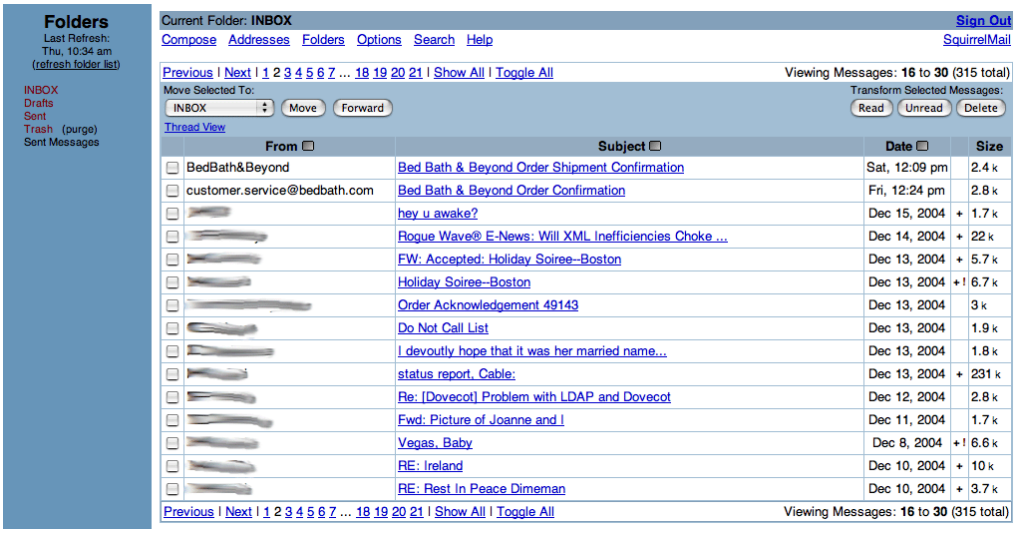


Slika 5.OWA korisničko sučelje

OWA se koristi, osim za pristup elektroničkoj pošti i za rukovanje kalendarom, kontaktima, zadacima i drugim sadržajima. Također OWA nudi pristup dokumentima pohranjenim na Microsoft SharePoint stranicama i mrežnim dijeljenim datotekama. OWA je prva web aplikacija koja je koristila XmlHttpRequest za slanje HTTP zahtjeva s klijentske strane. Komponenta XmlHttpRequests je kasnije postala sastavni dio AJAX tehnologije.SquirrelMail

3.2.2. SquirrelMail

SquirrelMail je kao i OWA sustav za rukovanje elektroničkom poštom. Sastoji se od klijentske web aplikacije i programa koji se postavlja na poslužitelja. Sustav je razvijen programskim jezikom PHP i kompatibilan je s većinom web preglednika. SquirelMail koristi „plugin“ arhitekturu za dodatke koji se mogu priključiti osnovnoj aplikaciji.



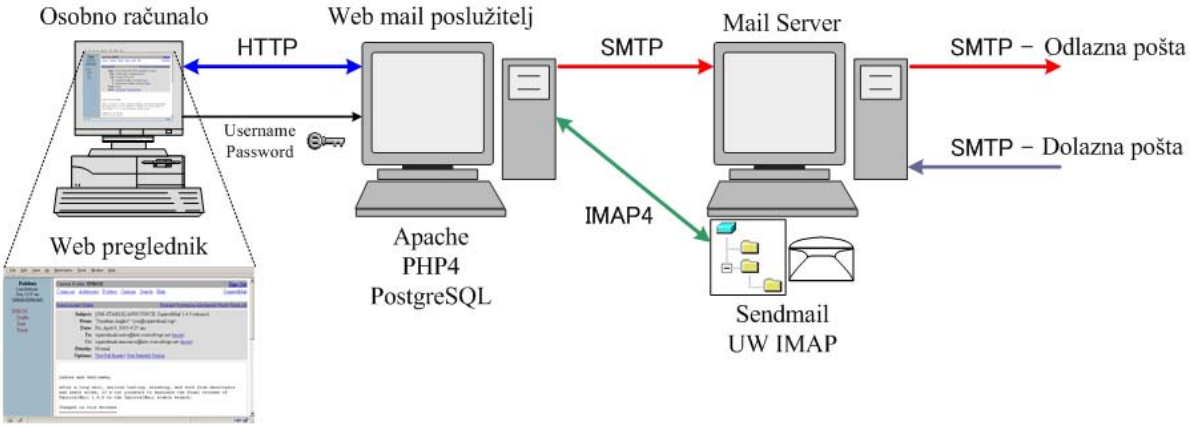
Slika 6. Web sučelje aplikacije SquirrelMai*l*

3.3. Primjer načina rada web mail servisa

Web mail servis koristi SMTP i IMAP4 standarde te pruža osnovne funkcionalnosti za rukovanje elektroničkom poštom:

1. Komunicira s korisničkim računalom preko web preglednika.
2. Autentikacija se obavlja prilikom prijave na sustav za što je potrebno imati korisničko ime i odgovarajuću zaporku. Uspješnom autentikacijom korisniku je omogućen pristup sandučiću elektroničke pošte.
3. Korisnik čita poštu iz svog sandučića prikazanog u sučelju web preglednika.
4. Korisnik može odabrati poruku i prikazati ju.
5. Korisnik sastavlja poruku u sučelju web preglednika i šalje ju na poslužitelja preko HTTP protokola te dalje preko SMTP protokola (slika 4)

Na slici 4. web mail poslužitelj i poslužitelj elektroničke pošte su odvojeni, iako obje funkcije može obavljati jedan fizički poslužitelj. Sendmail je MTA koji podržava različite metode prijenosa poruka, a UW IMAP je fleksibilna poslužiteljska implementacija protokola IMAP.



Slika 7. Pregled web sandučića elektroničke pošte preko web mail aplikacije

3.4. Prednosti i nedostaci web pristupa elektroničkoj pošti

Prednosti:

- Omogućuje pristup elektroničkoj pošti s bilo kojeg računala spojenog na Internet. Dok god korisnik zna svoje korisničko ime i zaporku može pristupiti web mail servisu preko web preglednika. Web mail je prema tome prikladan korisnicima koji su u pokretu ili mnogo putuju. Osim toga, poruke su pohranjene na poslužitelju pa nema potrebe za brigu o organizaciji poruka na samo jednom računalu.
- Radi s bilo kojim pružateljem Internet usluga te nema potrebe za promjenom adrese poslužitelja elektroničke pošte kada korisnik promijeni pružatelja Internet usluga. Osim toga neki pružatelji Internet usluga dozvoljavaju da se isključivo njihov poslužitelj koristi kao odlazni te blokiraju uobičajena vrata 25 (eng. port).
- Sve tvrtke koje nude usluge web mail servisa pružaju korisniku mogućnost pretraživanja poruka elektroničke pošte. Korisnik može poslati upit za traženje određenog izraza ili u zaglavlju poruke (adresa, naslov itd.) ili u sadržaju poruke. Način pretraživanja elektroničke pošte obično je učinkovitiji od onog koji postoji u klijentskim aplikacijama na lokalnom računalu.
- Sve više pružatelja web mail usluga omogućuje korisniku veliki kapacitet pohrane elektroničke pošte (npr. Gmail neprekidno povećava kapacitet za pohranu pošte; trenutni je kapacitet oko 7 GB). Zbog toga nema potrebe koristiti ograničene resurse osobnog računala.

Nedostaci:

- Za pristup elektroničkoj pošti potrebno je imati vezu na Internet. U današnje doba to nije problem zbog pouzdanih pružatelja Internet usluga. Međutim, ukoliko se korisnik nalazi u području gdje je pristup Internetu nepouzdan, postoji rizik da neće moći pristupiti svojem računu, a time i porukama elektroničke pošte.
- Čak se i najbolje održavanim web mail sustavima događa da je zbog npr. nestanka struje pristup elektroničkoj pošti onemogućen. No takvi su događaji vrlo rijetki i obično su vrlo dobro medijski popraćeni. A to za korisnika znači da će problem biti brže otklonjen.
- Može se dogoditi da se sve pohranjene poruke elektroničke pošte obrišu. Ipak, u praksi se to ne događa zbog legalne odgovornosti (svaki pružatelj usluga sklapa ugovor s korisnikom prije nego mu dozvoli stvaranje korisničkog računa) i velikog budžeta tvrtki koje nude web mail usluge te će poruke elektroničke pošte biti bolje zaštićene od gubitka ili oštećenja podataka nego da se nalaze na osobnom računalu.
- Većinu web mail servisa sponzoriraju različite tvrtke koje se oglašavaju u web mail aplikacijama. Zbog toga postoji i veća mogućnost dobivanja neželjenih poruka elektroničke pošte (eng. SPAM). Međutim, postoji velik broj korisnika web mail usluga, a time i velik broj žrtava koji mogu primati neželjenu elektroničku poštu.
- Djelomično narušavanje privatnosti poruka. Pružatelji web mail usluga imaju slobodan pristup elektroničkoj pošti svojih klijenata. Gmail na primjer koristi sadržaj poruka kako bi ustanovili koje reklame da prikazuju korisnicima prilikom pristupanja elektroničkoj pošti. Sve poznatije tvrtke provode politiku privatnosti (korisnika upućuje u način upotrebe njegovih podataka vezanih uz elektroničku poštu i korisnički račun) te ju korisnik prilikom otvaranja računa treba prihvatiti.
- Kod otvaranja korisničkog računa elektroničke pošte moguće je da korisnik neće dobiti željeni oblik adrese elektroničke pošte. Zbog velikog broja korisnika postoji i velika vjerojatnost da su sve za korisnike poželjne adrese elektroničke pošte već zauzete te ona adresa koju korisnik odabere može zvučati neprofesionalno (npr. ime.prezime44000@gmail.com).

Iz ove je usporedbe moguće uočiti da je popis nedostataka dulji od popisa prednosti, no to su sve manji nedostaci. Većina korisnika smatra da su nabrojane prednosti sasvim dovoljni razlozi za upotrebu web mail usluga.

3.5. Gmail

Gmail je besplatni web mail servis tvrtke Google. Podržava POP3 i IMAP4 standarde za prijenos elektroničke pošte. Gmail je nastao 1. travnja 2004. godine i sve do 2007. godine za stvaranje korisničkog računa za pristup elektroničkoj pošti korisnici su morali dobiti pozivnicu. Gmail je još uvijek u beta fazi, odnosno u fazi ispitivanja i ima na desetke milijuna korisnika.

U početku je kapacitet pohrane poruka elektroničke pošte bio 1GB, što je bilo mnogo više u odnosu na 2 do 4MB, koliko je nudila konkurencija. Web mail servis svojim korisnicima trenutno besplatno pruža 7250 MB prostora za pohranu poruka. Taj prostor se neprekidno povećava (uz stopu rasta 353.9 KB po danu). Ukoliko korisnik želi još više prostora za pohranu, Google nudi od 10GB do 400GB dodatnog prostora uz naknadu od 20 do 500 američkih dolara godišnje. Aplikacija koristi AJAX tehnologije i pokrenuta je na poslužitelju s operacijskim sustavom Linux.

Gmail je jedinstven po svojem karakterističnom korisničkom sučelju orijentiranom pretraživanju i pregledu poruka sličnom Internet forumu. Korisnici imaju mogućnost pretraživati poruke prema parametrima koje sami odrede putem sučelja *Advanced search*. Neki od parametara prema kojima mogu pretraživati poruke su proizvoljni izrazi, pošiljatelj poruke, datum poruke, itd. Osim toga, postoji mogućnost filtriranja poruka u smislu raspoređivanja u različite kategorije. Korisnik može spomenutu mogućnost iskoristiti za filtriranje poruka prema zaglavlju, sadržaju poruke ili privitku poruke.

Slika 8. Filtriranje poruka kod Gmail-a

Gmail prepoznaje pristigle poruke prema naslovu i grupira ih u „razgovore" nalik razgovorima na forumu. Poruke koje imaju isti naslov prikazuju se na ekranu jedna za drugom kao stog s tim da je najnovija poruka na dnu stoga.

Programeri stalno dodaju nove mogućnosti u Gmail aplikaciju i daju ih korisnicima na ispitivanje. Ako se novi dio aplikacije često koristi, ostaje u programu, u suprotnom se miče. Jedna od novih mogućnosti koje se trenutno ispitivaju je Gmail Labs. Mogućnost omogućuje korisnicima da označe poruke u smislu pripadnosti nekoj od proizvoljnih kategorija.

Za razliku od konkurentskih web mail servisa, Gmail ne dozvoljava svojim korisnicima pregled veličine poruka elektroničke pošte niti razmještanje poruka (npr. abecedno po naslovu).

Kontakti, odnosno adrese elektroničke pošte s kojih korisnik dobiva poruke ili na koje ih šalje spremaju se i ažuriraju automatski. Osim toga, korisnik može prebaciti kontakte iz različitih aplikacija pokrenutih na lokalnom računalu, kao što su Microsoft Office Outlook, Mozilla Thunderbird, Eudora, ili ih može prebaciti s nekog drugog web mail računa (Hotmail, Yahoo! Mail).

3.5.1. Sigurnost web mail servisa Gmail

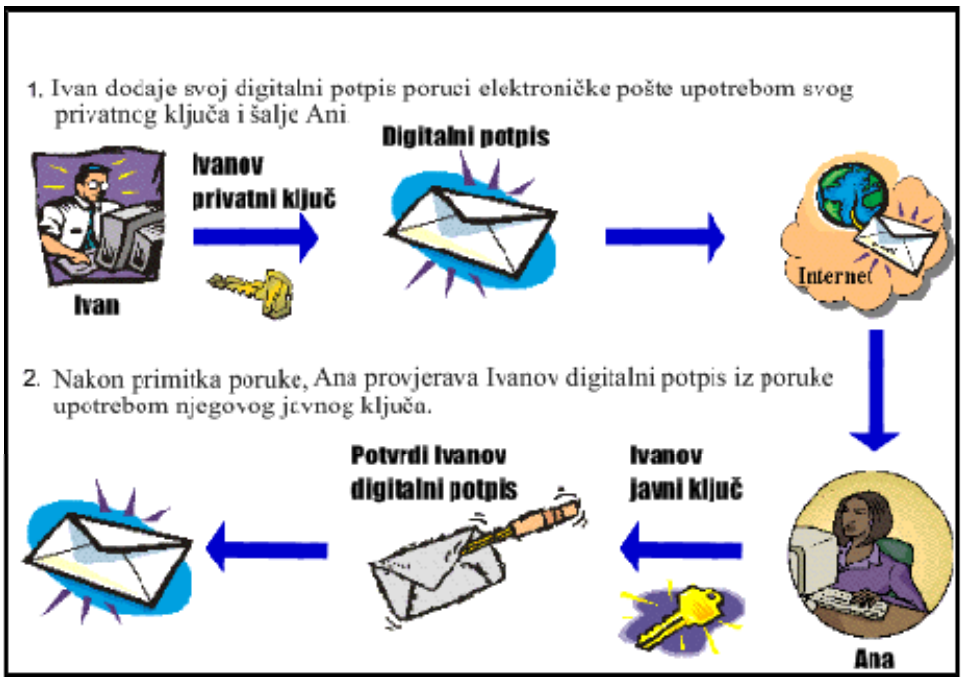
Prema tvorničkim postavkama Gmail aplikacija koristi nekriptiranu vezu za dohvat korisničkih podataka. Veza se kriptira samo prilikom prijave na sustav. Međutim, korisnik može proizvoljno koristiti HTTPS (eng. Hypertext Transfer Protocol over Secure Socket Layer) protokol te na taj način uspostaviti sigurnu vezu. Upotrebom sigurne veze smanjuje se rizik krađe korisnikovih podataka (kao što su kontakti) koji se prenose u tekstualnom obliku kao JavaScript podaci u izvornom kodu stranice. Od srpnja 2008. godine korisnici mogu odabrati mogućnost da Gmail aplikacija koristi isključivo HTTPS pristup. Postavljanje ove mogućnosti sprečava mogućnost krađe podataka. Prijenos poruka u tom slučaju je zaštićen jer se za u komunikaciji koristi TLS (eng. Transport Layer Security) protokol. Kada se poruka šalje s Gmail poslužitelja klijentskoj aplikaciji na lokalnom računalu ona se ipak ne šalje putem TLS protokola. TLS protokolom se šalje samo ako korisnik to izričito odredi u nekoj od mogućnosti. Tako da se u nekom trenutku poruka elektroničke pošte šalje u nekriptiranom obliku što ju čini ranjivom na različite vrste napada kao što su: prisluškivanje, promjena sadržaja poruka, izmišljanje poruka te lažno predstavljanje. IP adrese korisnika koji se prijave na Gmail aplikaciju maskiraju se u svrhu zaštite. Tako napadači ne mogu vidjeti s koje se IP adrese korisnik prijavio na sustav.

Gmail nudi filtriranje neželjene elektroničke pošte (eng. SPAM). Sustav automatski briše poruke označene kao neželjene nakon 30 dana. Korisnici ne mogu isključiti sustav za filtriranje elektroničke pošte. Zanimljiv je podatak da se oko 75% poruka poslanih na Gmail račune označava kao neželjena pošta.

Sve poruke koje stižu ili se šalju putem Gmail aplikacije automatski se skeniraju antivirusnim programima. Korisnik ne može prenijeti sadržaj privitka na lokalno računalo ukoliko se skeniranjem ustanovi da privitak može ugroziti sigurnost korisnikovog računala. Uz to, ako privitak odlazne poruke sadrži virus, Gmail aplikacija ne dozvoljava slanje takve poruke. Također, nije dozvoljeno slati i primati privitke koje sadrže izvršne datoteke ili arhive s istima.

Ako korisnik pošalje poruku samom sebi, ili ju pošalje na tzv. mailing listu na kojoj se nalazi i njegova adresa, poruku neće dobiti. To znači da napadači ne mogu imitirati korisnika i slati mu opasan sadržaj.

Gmail koristi digitalni potpis tvrtke Yahoo! za autentikaciju poslanih poruka. Sustav koji se koristi je *DomainKeys* i namijenjen je verifikaciji DNS naziva pošiljatelja elektroničke pošte te očuvanju integriteta poruke. Digitalni se potpis dodaje zaglavlju poruke. Poslužitelj koji prima poruku preuzima javni ključ pošiljatelja preko DNS sustava te potvrđuje potpis.



Slika 9. Digitalni potpis kod poruka elektroničke pošte

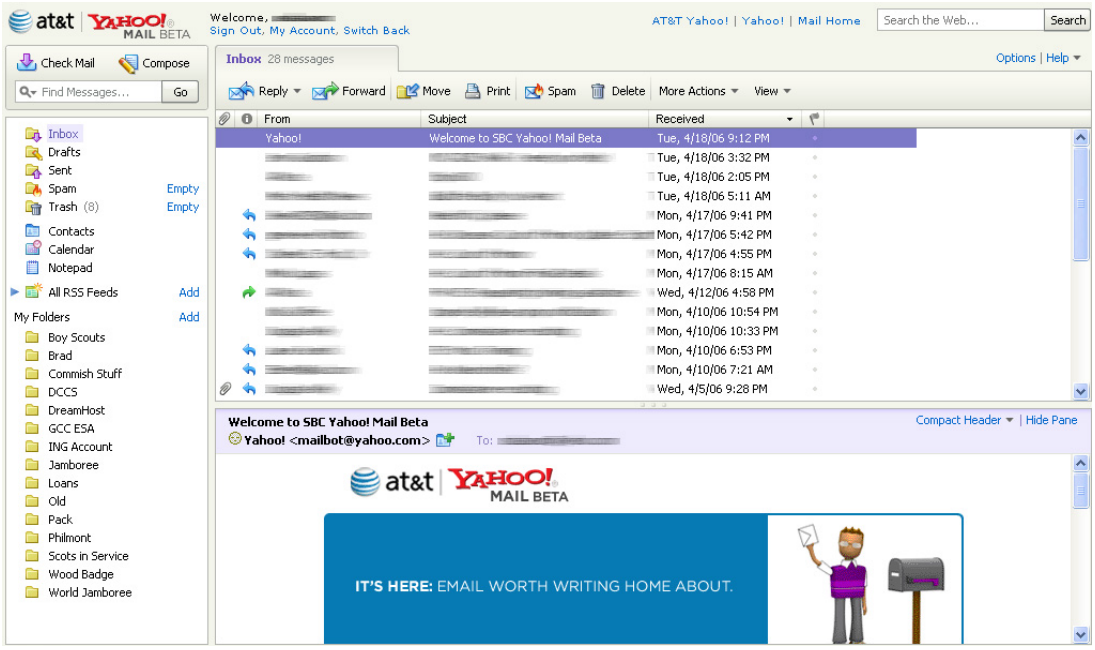
3.5.2. Privatnost poruka

Google automatski skenira poruke elektroničke pošte u svrhu dodavanja reklamnog sadržaja. Bilo je mnogo rasprave da spomenuti postupak narušava privatnost poruka te da može predstavljati sigurnosni problem. Iako sve poruke obrađuje računalni program, privatnost poruka elektroničke pošte je smanjena. Uz to, poruke koje su korisnici drugih web mail servisa poslali na Gmail adresu se također skeniraju u već spomenutu svrhu, iako ti korisnici nisu pristali na poštivanje politike privatnosti koju nameće Gmail. Ipak, isti se sustav za pregled poruka za oglašavanje reklamnog sadržaja koristi i u svrhu uklanjanja neželjene elektroničke pošte.

Još je jedan problem vezan uz privatnost poruka, a to su: politika o roku čuvanja podataka i povezivanje podataka s drugim podacima dostupnim tvrtki Google. Google može kombinirati podatke o korisniku iz poruka elektroničke pošte s informacijama o njegovim navikama pretraživanja Interneta. Nepoznato je koliko dugo se takve informacije čuvaju i na koje se načine mogu iskoristiti (npr. dati na korištenje vladinim agencijama). Nekoliko je civilnih organizacija tražilo da se ukine Gmail servis dok se ne razriješe spomenuti problemi privatnosti podataka. Poznato je također da Google čuva ostatke kopija obrisanih poruka i korisničkih računa te da je potrebno više od šezdeset dana da se obrišu s poslužitelja.

3.6. Yahoo! Mail

Yahoo! Mail je jedna od popularnih web aplikacija za pristup elektroničkoj pošti. Nastala je 1997. godine i ima oko 260 milijuna korisnika. Trenutno Yahoo! nudi dvije inačice Yahoo! Mail aplikacije, jednu čije korisničko sučelje ima izgled sličan klijentskoj aplikaciji Outlook Express i koristi AJAX tehnologije te jednu koja koristi statički web i ima naziv Yahoo! Mail Classic. Prva spomenuta web aplikacija ima naziv New Yahoo! Mail i razvijen je 2007. godine. 2008. godine Yahoo! nudi svim svojim korisnicima neograničen kapacitet pohrane poruka elektroničke pošte. Ova je odluka odgovor na konkurenciju.



Slika 10. New Yahoo! Mail

Osim besplatnih web mail aplikacija Yahoo! nudi i usluge vezane uz web mail koje se plaćaju. Usluga ima naziv Yahoo! Mail Plus i ima različite dodatne mogućnosti, kao što su slanje deset privitaka po poruci, arhiviranje poruka elektroničke pošte za pristup kada korisnik nije povezan na Internet i dr.

New Yahoo! Mail korisničko sučelje slično je klijentskim aplikacijama na lokalnom računalu te nudi mogućnost prikaza poruka elektroničke pošte u karticama, RSS obavijesti, prebacivanje poruka u datoteke mišem, napredno pretraživanje, integraciju s kalendarom i aplikacijom Yahoo! Messenger za instant komunikaciju, itd.

Yahoo! Mail je kompatibilan s web preglednicima Internet Explorer 7, Firefox (sve inačice) i Safari, dok neke funkcionalnosti ne rade u web pregledniku Opera.

Yahoo! je u web aplikaciju dodao i zabavni sadržaj, tzv. Uskršnje jaje (eng. Easter egg) pod nazivom „Subject-O-Matique“. Uskršnja jaja, u informatičkom smislu, su namjerne skrivene poruke ili elementi u objektima kao što su filmovi, knjige, CD, DVD, računalni programi, web stranice ili računalne igre. Subject-O-Matique prikazuje slučajne poruke u naslovu kada korisnik klikne na područje za upis naslova.

Ukoliko se korisnik ne prijavi na svoj korisnički račun u roku od četiri mjeseca, račun se deaktivira. Korisnik si može dodati alternativnu adresu elektroničke pošte (eng. alias) na svoj račun elektroničke pošte.

Osim podrške za pristup elektroničkoj pošti za privatne korisnike Yahoo! Mail pruža uslugu i za poslovne tvrtke. Ova usluga nije besplatna i ima naziv Yahoo! Business Email koji stoji 34.95 američkih dolara godišnje i nudi dodatne mogućnosti. Neke od tih mogućnosti su neograničeni kapacitet pohrane poruka elektroničke pošte, posebno prilagođene adrese elektroničke pošte, vodeća antivirusna i anti-spam zaštita te još mnoge druge..

3.6.1. Sigurnost

Kao i svaki moderni web mail servis, i Yahoo! Mail je izložen pošiljateljima neželjene elektroničke pošte koji se lažno predstavljaju kao pružatelji web mail usluga te u svojim porukama korisnika često navode da na primjer potvrdi svoj korisnički račun. Kada korisnik sijedi web poveznicu (eng. link) kako bi potvrdio svoj račun, zapravo otvara vrata pošiljateljima neželjene pošte da šalju još više takvih poruka. Ako pošiljatelj neželjene pošte ima Yahoo! korisnički račun, njegov račun se briše. Yahoo! ima politiku da uklanja sve korisničke račune koji su povezani s aktivnostima slanja neželjene pošte bez upozorenja. Mehanizam kojim provjerava slanje nepoželjne poštene sYahoo! drži u tajnosti. Također, korisnici za koje je utvrđeno da šalju nepoželjnu pošti gube kontakt s bilo kojim drugim Yahoo! uslugama koje su vezane uz njihovo korisničko ime.

Od 2004. godine Yahoo! digitalno potpisuje odlaznu poštu DomainKeys sustavom koji digitalni potpis stavlja u zaglavlje poruke.

Kako bi se spriječila zlouporaba Yahoo! Mail servisa, 2002. godine uvedeni su filtri koji mijenjaju određene riječi koje bi napadači mogli iskoristiti za XSS (eng. Cross-site scripting) napade. Tako su riječi, koje su zapravo ključne riječi JavaScript programskog koda, zamijenjene nekim drugim istog značenja. Neke od tih riječi su „Mocha" koja je promijenjena u „espresso", „expression" se mijenja u „statement" te riječ „eval", koja se najbolje može zlouporabiti, promijenjena je u „review". Kao posljedice ovih promjena kod pretraživanja poruka elektroničke pošte moguće je naići na besmislene pojmove kao što su „prreviewent" umjesto „prevalent", „reviewuation" umjesto „evaluation" i drugi. Zbog očite nepraktičnosti 2006. godine navedene su zamjene izbačene te se na ključne riječi koje napadači mogu zlouporabiti dodaje kao prefiks donja crta („_"). Postavljanje prefiksa sprečava napadače da umetnu štetni kod u HTML stranicu.

Kao dodatnu zaštitu korisnika svaki se privitak poruka elektroničke pošte pregledava antivirusnim programom i to prilikom zahtjeva za prijenos privitka na lokalno računalo.

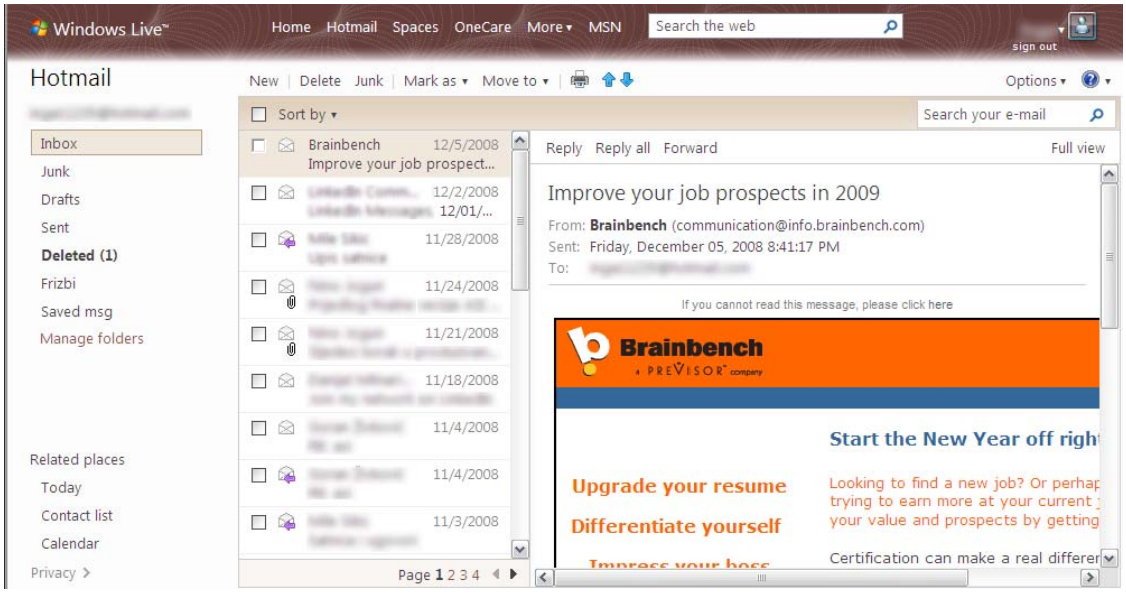
3.7. Hotmail

Hotmail je besplatni web mail servis tvrtke Microsoft i dio je sustava Windows Live. Hotmail je pokrenut 1996., a Microsoft ga je kupio 1997. Godine. Hotmail je jedan od prvih web mail servisa uopće. Windows Live Hotmail pruža korisnicima kapacitet od 5 GB za pohranu poruka elektroničke pošte. Web aplikacija za pristup elektroničkoj pošti koristi AJAX tehnologije, i pruža mogućnosti integracije s programom za instant dopisivanje - Windows Live Messenger, kalendarom, adresarom, itd. Preko 260 milijuna ljudi koristi Hotmail za web pristup elektroničkoj pošti.

Kao i većina modernih web mail servisa, Hotmail je kompatibilan s web preglednicima Internet Explorer i Mozilla Firefox. Neke od mogućnosti uključuju navigaciju po stranici isključivo upotrebom tipkovnice, napredno pretraživanje poruka, filtriranje poruka, organizaciju poruka elektroničke pošte u direktorije, automatsko nastavljanje adresa elektroničke pošte prilikom upisa u polje primatelja, grupiranje kontakata, unos i iznos kontakata u obliku CSV datoteka, uklanjanje neželjene elektroničke pošte, antivirusnu zaštitu te potporu za različite jezike.

Kao i Yahoo! Mail Hotmail korisniku pruža mogućnost izbora između dvije inačice web aplikacije. Jedna inačica ima izgled temeljen na prvotnoj MSN Hotmail aplikaciji, dok alternativna web aplikacija ima napredno korisničko sučelje nalik onom klijentske aplikacije Microsoft Outlook

.



Slika 11. Hotmail

Osim uobičajenih elemenata web aplikacija za pristup elektroničkoj pošti, korisnik aplikaciju Hotmail može koristiti i za slušanje glazbe i glasovne pošte. Korisnici mogu stvarati direktorije i u njih osim poruka elektroničke pošte spremati i fotografije te različite osobne podatke.

Za pristup elektroničkoj pošti s lokalnog računala potrebno je platiti 19.95 američkih dolara godišnje. Za ovu uslugu koristi se WebAV protokol koji dozvoljava prijenos elektroničke pošte na lokalno računalo preko klijentske aplikacije kao što su Eudora, Outlook Express i Mozilla Thunderbird. Za pristup elektroničkoj pošto na Hotmail računu korisnici koji imaju instaliran Outlook (inačicu 2003 ili 2007) mogu preuzeti besplatni program Microsoft Office Outlook Connector, koji mora proći verifikaciju aplikacijom Office Genuine Advantage. Za prijenos pošte koristi se DeltaSync protokol.

3.7.1. Sigurnost

Sigurnosni elementi koje sadrži web aplikacija Hotmail uključuju:

- antivirusno ispitivanje programom Trend Micro,
- SMTP autentikaciju,
- heurističko prepoznavanje phishing poruka,
- otkrivanje mailing lista.

Rizične poruke Hotmail tretira tako da ne dozvoljava njihovo otvaranje ili pregled privitka sve dok korisnik ne zahtijeva suprotno. Spomenuta je sigurnosna mjera postavljena kako bi se smanjila mogućnost phishing napada.

Tijekom razvoja web mail servisa Hotmail se povezao s autentikacijskom aplikacijom Passport tvrtke Microsoft, što je prouzročilo mnoge sigurnosne probleme. Aplikacija je dozvoljavala prijavu na sustav svima koji bi kao zaporku upisali riječ „eh". Propust je ispravljen.

3.8. Sigurnost web aplikacije Outlook Web Access

Sustav Outlook Web Access i Excange Server imaju mogućnost naprednog postavljanja sigurnosti. Omogućuju postavljanje nekoliko autentikacijskih metoda:

- standardna – uključuje autentikaciju Integrated Windows (koristi sažetak - hash i autentikacijski sustav Kerberos), Digest (koristi MD5 sažetak) i Basic (koristi 64 bitno kriptiranje).
- na temelju formi (eng. Forms based) – stvara stranicu za prijavu na aplikaciju OWA te koristi cookie datoteke za spremanje kriptiranih korisničkih podataka prilikom prijave na sustav

Uz ove osnovne mogu se koristiti i slijedeće:

- ISA Server forme – omogućuje sigurno objavljivanje OWA poslužitelja upotrebom poslužiteljskih pravila objavljivanja. Također dozvoljava postavljanje autentikacije putem web formi te nadzor privitaka elektroničke pošte
- Pametne kartice i autentikcija putem certifikata – certifikati se mogu nalaziti ili na klijentskom računalu ili na pametnoj kartici. Autentikacija preko certifikata korsti EAP (eng. Extensible Authentication Protocol) i TLS (eng Transport Layer Security) protokole. Klijent i poslužitelj jedno srugome dokazuju svoje identitete.
- RSASecureID – program za autentikaciju koji se temelji na dvo-faktorskoj autentikacji: zaporci (nešto što korisnik zna) i autentikatoru (program ili sklop koji generira autentikacijski kod svakih 30 do 60 sekundi)

OWA u tvorničkim postavkama ima postavljenu upotrebu digitalnih certifikata. Digitalni certifikat ima dvije uloge:

- autenticira da je identitet onoga koji ga pruža valjan
- štiti razmijenjene podatke od krađe i lažiranja

Za dodatnu sigurnost moguće je podesiti klijentsku stranu da koristi provjerene certifikate (eng. trusted certificates), certifikate koje izdaje provjereni autoritet (eng. third-party certificqation authority – CA) ili infrastrukturu Windows Public Key. Autentikacija se može postaviti posebno za svaki dio sustava elektroničke pošte, kao i za protokole koji se koriste.

Kako bi se zaštitila komunikacija OWA nudi mogućnost postavljanja SSL (eng. SEcure Scokets Layer) protokola. SSL se koristi za komunikaciju između klijenta i poslužitelja. digitalni se certifikati koriste i za stvaranje SSL kriptiranog komunikacijskog kanala.

Kada korisnik otvara privitke upotrebom web aplikacije OWA, sadržaj se privitka sprema u priručnu memoriju (eng. cache) web preglednika. Kada se korisnik odjavi od računala, privitak se još uvijek nalazi u priručnoj memoriji. Dakle neki drugi korisnik se može prijaviti na računalo i pregledati sadržaj priručne memorije. Ako su se u privitku nalazili osjetljivi korisnički podaci, taj drugi korisnik ih može ukrasti.

Ako se korisnik ne odjavi nakon upotrebe OWA, neki drugi korisnik može jednostavno pregledati povijest posjeta web stranica u web pregledniku i upasti u sjednicu korisnika koji se nije odjavio.

3.9. Sigurnost web aplikacije SquirrelMail

SquirrelMail podržava nekoliko metoda autentikacije koje koriste MD5 sažetak. Moguće je koristiti različite metode za svaki od protokola IMAP i SMTP. Po tvorničkim postavkama kod autentikacije se koristi 64-bitno kriptiranje.

SquirrelMail se može povezati na IMAP i SMTP poslužitelje preko TLS protokola. Od inačice 1.5.1 korisnik ima mogućnost i ključne riječi STARTTLS za pokretanje zaštićene SSL veze između dva poslužitelja preko SMTP protokola

Osim ugrađenih sigurnosnih elemenata, administrator može priključiti u aplikaciju i dodatne sigurnosne elemente. Jedan od njih je Timeout User. Ova aplikacija štiti korisnika koji se zaboravi odjaviti od sustava od štetnih posljedica. U ovakvoj situaciji napadač bi mogao upravljati sandučićem elektroničke pošte, međutim Timeout User to ne dozvoljava. Naime, dodatak zaboravljivog korisnika odjavi nakon nekog vremena. U dodatku se nalazi i dio koji briše sjedničke podatke tako da korisnika štiti i od krađe sjednice ukoliko se zaboravi odjaviti sa sustava.

Kako bi pružili što bolju zaštitu korisnicima tvrtka koja je dizajnirala SquirrelMail ima posebnu stranicu na kojoj korisnici mogu prijaviti sigurnosne propuste. U zadnje vrijeme posljednji je prijavljeni propust vezan uz XSS ranjivost. Objavljen je u prosincu 2008. godine u obliku sigurnosne preporuke s CVE oznakom CVE-2008-2379.

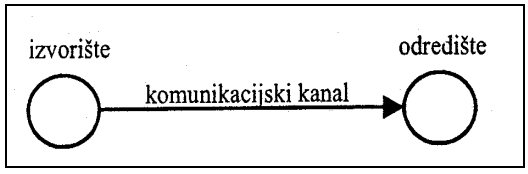
4. Sigurnosni rizici

Prva stvar koju treba imati na umu prilikom upotrebe Interneta u bilo koju svrhu jest da je sve što korisnik radi rizično. Na primjer korisnik može biti žrtva phishing napada, zatim može kliknuti na poveznicu koju je napadač postavio kako bi ukrao korisničke podatke itd. Sigurnosni rizici besplatnih web mail servisa su ujedno i oni rizici koje korisnik prihvaća prilikom otvaranja bilo koje stranice na Internetu. Iako web mail servisi uglavnom koriste kriptiranu komunikaciju, to ne znači da je elektronička pošta potpuno sigurna od zlouporabe. Poruke se prenose raznovrsnim otvorenim i nesigurnim komunikacijskim putovima gdje se pristup do tih putova ne može fizički zaštititi. Prema tome svaki zlonamjerni napadač može narušiti sigurnost komunikacijskog sustava. U web mail sustavu sve se informacije prenose porukama te je osnovni problem komunikacijskog sustava zaštita poruka, odnosno zaštita komunikacijskog kanala.

4.1. Problemi zajednički svim web mail sustavima

4.1.1. Vrste napada

Najbolje je prikazati vrste napada modelom u kojem je izvorište informacija povezano s odredištem komunikacijskim kanalom.



Slika 12. Model komunikacije

U slučaju web mail sustava, izvorište i odredište se nalaze u različitim računalima raspodijeljenog sustava. Pojedine vrste napada na različite načine narušavaju sigurnost sustava.

- **Prisluškivanje** – najjednostavniji način napada na sigurnost. Napadač može čitati poruke koje su namijenjene nekom drugom te na taj način doći do osjetljivih informacija. Ovakvim napadom djeluje se na povjerljivost informacija.
- **Prekidanje** – napadač svojim djelovanjem može prekinuti komunikacijski kanal te na taj način narušiti raspoloživost informacija.
- **Promjena sadržaja poruka** – napadač može prekinuti komunikacijski kanal i lažno se predstavljajući kao izvorište promijeniti sadržaj poruke te tako narušiti integritet podataka.
- **Izmišljanje poruka** – napadač može uspostaviti komunikacijski kanal s odredištem i lažno se predstavljajući kao izvorište slati izmišljene poruke ili snimljene stare poruke. Kao i promjena sadržaja poruka narušava se integritet ili besprijekornost podataka.
- **Lažno predstavljanje** – napadač se predstavlja kao neki drugi korisnik (primjerice provalivši u tuđi korisnički račun)

Nekoliko je elemenata web mail sustava koje napadač može zlouporabiti. Većina web mail aplikacija koristi AJAX tehnologije, čije elemente napadač može iskoristiti za zlouporabu servisa. Osim toga, napadač može prisluškivati sjednice i krađom sjednica pristupiti web mail računima, pregledavati, mijenjati ili slati poruke elektroničke pošte lažno se predstavljajući. Uz to napadač može izvesti i phishing napad te prouzročiti različite probleme korisniku web mail servisa.

4.1.2. XSS napad

XSS (eng. Cross-site scripting) je napadačka tehnika koja prisiljava web aplikaciju da korisniku proslijedi zlonamjerni izvršni kod, koji se zatim učitava i izvršava u korisnikovom web pregledniku. Štetni programski kod najčešće je pisan u programskom jeziku JavaScript, ali napadač ga može stvoriti i upotrebom nekog drugog programskog jezika kojeg podržava korisnikov web preglednik (HTML, VBScript, ActiveX, Java i Flash). XSS ranjivost se javlja uslijed nepravilne provjere ulaznih podataka web aplikacije. Svaka web stranica koja omogućuje korisniku unos nekih podataka potencijalno sadrži XSS ranjivost pa tako i web mail aplikacija.

Kada napadač uspješno iskoristi XSS ranjivosti i podmetne zlonamjerni programski kod za pokretanje u korisničkom web pregledniku , kod će se izvršavati unutar tzv. sigurnosne zone web aplikacije. Koristeći ovu privilegiju, napadač može čitati ili promijeniti osjetljive podatke dostupne web pregledniku. Ova se napadačka tehnika može iskoristiti za krađu korisničkih računa (krađa cookie datoteka), krađu sjednica, usmjeravanje web preglednika na neke druge lokacije, ili prosljeđivanje štetnog sadržaja od strane web aplikacije. Osim toga, XSS napadi ugrožavaju povjerljivi odnos između korisnika i web aplikacije.

Upotreba AJAX tehnologija za stvaranje funkcionalnijeg i atraktivnijeg korisničkog sučelja znači i povećanu složenost sustava klijent-poslužitelj. Ukoliko AJAX aplikacija koristi programski kod JavaScript za komunikaciju s poslužiteljem, kod se mora prenijeti s poslužitelja na klijentsko računalo u izvornom (nekriptiranom) obliku. Dakle, sve što korisnik treba napraviti je pogledati izvorni kod web stranice i vidjet će kako aplikacija funkcionira. Iako je moguće zamaskirati programski kod tako da je na prvi pogled nečitljiv, napadači svejedno mogu iskoristiti transparentnost koda za pribavljanje informacija o načinu rada određenog dijela aplikacije. Uvođenjem AJAX tehnologija u web aplikacije otvorile su se nove mogućnosti zlouporabe XSS ranjivosti. JavaScript podržava objektno orijentirane tehnike programiranja te sadrži mnogo ugrađenih objekata, ali i dozvoljava stvaranje korisničkih objekata. Slijedeći kod prikazuje stvaranje novog objekta:

```
New Object()
ili
message = {from : "marko@primjer.com",
           to : "pero@zrtva.com",
           subject : "Ovdje staviti zlonamjerni kod",
           body : "Tekst poruke elektroničke pošte",
           showsubject : function(){document.write(this.subject)}};
```

Ovaj kod služi za stvaranje poruke elektroničke pošte koja sadrži sva potrebna polja. JavaScript objekt može sadržati podatke, ali i metode, što napadač može iskoristiti za izvođenje XSS napada. Ako napadač umetne zlonamjerni kod u polje *subject* i pošalje takvu poruku, tada primatelj poruke postaje žrtva XSS napada.

4.1.3. Krađa sjednica

Krađa sjednica je oblik napada gdje napadač zloupotrebljava sjednički ključ (eng. session key) u svrhu dobivanja pristupa podacima ili uslugama računalnog sustava. Krađa sjednica se odnosi na krađu „magičnih“ cookie datoteka koje se koriste za autentikaciju korisnika na udaljenom poslužitelju. HTTP cookie datoteke, koje održavaju korisničke sjednice na mnogim web stranicama, napadači mogu lako ukrasti što može imati drastične posljedice za žrtvu napada.

Web mail servisi obično dozvoljavaju korisniku da mijenja zaporku i podatke korisničkog računa. Prijenos podataka između klijenta i poslužitelja može, ali i ne mora biti kriptiran. Prilikom prijave na sustav korisnik treba upisati svoje korisničko ime i zaporku u za to predviđena polja. Također, prijenos podataka može biti kriptiran, ali i ne mora. Kako se korisnik ne bi morao stalno prijavljivati na sustav, mnoge web stranice koriste sjedničke cookie datoteke. Spomenute datoteke sadrže podatke koje je poslužitelj poslao klijentu prilikom prijave na sustav s ciljem potvrde identiteta, odnosno autentikacije. Ukoliko napadač uspije ukrasti cookie datoteku, može sam slati zahtjeve lažno se predstavljajući kao korisnik čiju je autentikaciju ukrao. Dakle, napadač uopće ne treba znati korisničko ime, niti zaporku kako bi neovlašteno pristupio žrtvinom web mail računu. Ako ukradena cookie datoteka nema rok trajanja, napadač ima neograničen pristup web mail računu korisnika čiju je sjednicu ukrao.

Krađa sjednica nije ograničena samo na cookie datoteke, već na bilo kakvu komunikaciju u kojoj dvije strane razmjenjuju ključeve. Velika je opasnost od krađe podataka ako komunikacija nije kriptirana.

Poznate su tri metode za izvođenje napada krađom sjednica. To su:

1. **Fiksacija sjednice** – napadač postavlja sjedničku identifikacijsku varijablu na neku vrijednost koja mu je poznata, na primjer pošalje poruku elektroničke pošte s poveznicom koja sadrži određenu vrijednost. Napadač sada samo treba čekati dok se korisnik ne prijavi na sustav.
2. **Krađa sjednice presretanjem paketa (eng. Session sidejacking)** – napadač krade pakete koji se šalju između klijenta i poslužitelja te na taj način prati mrežni promet. Među ukradenim paketima nalazi se i sjednička cookie datoteka. Mnoge web stranice koriste SSL kriptiranje na stranicama za prijavu kako bi spriječili da napadači preuzmu zaporku, ali ne koriste zaštitu za stranice kojima korisnik pristupa nakon prijave. Spomenuta situacija omogućuje napadačima da presreću i čitaju sve podatke poslane poslužitelju. S obzirom da se među podacima nalazi i sjednička cookie datoteka, napadač ju može iskoristiti za lažno predstavljanje.
3. **XSS napad** – napadač prevari korisnika te mu podmetne zlonamjerni programski kod za pokretanje. Pri tome zlonamjerni kod između ostaloga kopira sjedničke cookie datoteke i šalje napadaču.

4.1.4. Phishing

Phishing je metoda napada kojom napadač slanjem lažnih poruka pokušava doći do osjetljivih korisničkih podataka kao što su korisničko ime, zaporka, podaci o kreditnoj kartici, itd. Napadač svoju poruku maskira tako da se doima vjerodostojno. Primjer jedne takve poruke elektroničke pošte koja je kružila elektroničkom poštom dana je u nastavku:

```
Dear Account User,

This Email is from webmail user Customer Care and we are sending it
to every webmail User Accounts Owner for safety. we are having
congestions due to the anonymous registration of accounts so we are
shutting down some accounts and your account was among those to be
deleted.

Due to the congestion in all webmail users and removal of all unused
Accounts, Webmail would be shutting down all unused Accounts, You
will have to confirm your E-mail by filling out your Login
Information below after clicking the reply button, or your account
will be suspended within 24 hours for security reasons.

* Username: …….
* Password: …….
* Date of Birth: ……..
* Country Or Territory: …….

Your response should be sent to admin manager Email :
customercare.xxxxxxx@gmail.com

Warning!!! Account owner that refuses to update his/her account after
two weeks of receiving this warning will lose his or her account
permanently.

Regard,
Customer Care Of Webmail Team
```

Slika 13. Primjer phishing poruke

Ako korisnik nasjedne na ovakvu prevaru napadač će dobiti korisničko ime i zaporku svoje žrtve. Napadač ovakvim napadom dobiva potpuni administratorski pristup korisničkom računu žrtve. U

sadržaju poruke primatelja se upozorava da će se njegov korisnički račun zatvoriti ukoliko ne pošalje svoje korisničko ime, zaporku, datum rođenja i mjesto u kojem živi na navedenu adresu elektroničke pošte. Ovom prijevarom zlonamjerni napadači nagovaraju korisnika da otkrije osjetljive podatke. Ovakve poruke korisniku trebaju odmah biti sumnjive. Poruka u primjeru odnosi se na neki neodređeni web mail servis. No češće su poruke elektroničke pošte koje napadači maskiraju kao da su poslane od nekog poznatog web mail servisa, kao što je Yahoo!. Osim toga, poruka u primjeru sugerira da postoji neki glavni nadzornik za sve web mail usluge na Internetu, što nije istina. Štoviše vrlo je malo vjerojatno da će web mail servis kojeg korisnik koristi tražiti da mu šalje svoje osobne podatke putem poruke elektroničke pošte.

4.2. Prijavljeni propusti u najpoznatijim web mail servisima

Iako najpoznatiji web mail servisi, Gmail, Yahoo! Mail i Hotmail imaju mnogo sigurnosnih mjera zaštite, često su izloženi napadima. Zlonamjerni napadači ne prežu pred ničime i ničiji korisnički račun nije siguran. Koliko god sigurnosne mjere štite korisnike, napadači će uvijek biti jedan korak ispred i pronaći načina kako da ih zaobiđu. U nastojanju da stanu na kraj zlonamjernim napadačima, svi poznatiji web mail servisi imaju blogove na kojima objavljuju otkrivene napade te primijenjene zakrpe. U nastavku slijedi par zanimljivih primjera napada na najpoznatije web mail servise.

4.2.1. Gmail

U svojim počecima Gmail je imao mnogo problema sa sigurnosti sustava. Nisu postojale dovoljne sigurnosne mjere te je napadač mogao dobiti potpuni pristup korisničkim računima. Napadači su iskoristili XSS ranjivosti web stranice www.google.com ili su otkrili sadržaj datoteka koje su bile pohranjene na poslužitelju. Datoteke su uključivale i poruke elektroničke pošte te pohranjene kontakte trenutno prijavljenog korisnika. Ovu su opasnu i štetnu ranjivost vrlo brzo uklonili zbog toga što se brzo proširila Internetom. Od tada pa do danas nisu prijavljeni veći propusti, a najčešći oblik napada je phishing. Posljednji phishing napad u kojemu su napadači koristili lažnu google adresu prijavljen je u studenom 2008. godine. Napadači su poslali posebno oblikovane poruke elektroničke pošte te mamili korisnike da otkriju svoje podatke, kao što su korisničko ime i zaporka. U prijevari su poticali žrtve da posjete lažnu web stranicu „google-hosts.com“. U slučaju uspješne zlouporabe, napadači su prikupili podatke potrebne za prijavu na korisnički račun te prilikom pristupa elektroničkoj pošti imali sve ovlasti kao i korisnik čiji su podaci ukradeni. U slučaju opisane prijevare napadač je mogao postaviti filtre tako da se njemu prosljeđuju poruke od pružatelja domenskih usluga na web-u.

Osim ovih službeno prijavljenih napada, na Youtube stranicama moguće je naći mnogo načina kako preuzeti korisničke podatke. Kao što je upotreba raznih alata za razbijanje zaporki i krivotvorenje adresa elektroničke pošte. No, treba i te napade uzeti s rezervom, jer sigurno među njima također ima prijevara.

4.2.2. Yahoo! Mail

Posljednji napad na Yahoo! Mail prijavljen je u listopadu 2008. godine. Napadači su iskoristili XSS ranjivost kako bi pristupili korisničkim računima elektroničke pošte. XSS ranjivost je otkrivena u domeni hotjobs.yahoo.com i napadači su ju iskoristili za ubacivanje i pokretanje posebno oblikovanog, maskiranog JavaScript koda koji je potajno krao sjedničke cookie datoteke. Nakon što je napadač uspješno sakupio spomenute datoteke, mogao je tada preuzeti nadzor nad Yahoo! korisničkim računom žrtve te bilo kojom drugom Yahoo! uslugom za koju je potrebna autentikacija. Ranjivost je uklonjena, ali napadači stalno otkrivaju nove metode napada i na Internetu se stalno pojavljuju novi alati za narušavanje sigurnosti korisničkih podataka. Jedan takav novi alat je CookieMonster, čija je namjena rukovanje cookie datotekama koje su stvorili web preglednici za operacijski sustav Windows. Omogućuje stvaranje popisa cookie datoteka koji se žele brisati te ima mogućnost za otkrivanje cookie datoteka za posebno odabrane web stranice.

Zanimljiv napad na Hotmail sustav prijavljen je 2001. godine kada su napadači otkrili da se bilo tko može prijaviti na njihov korisnički račun. Poruke su se zatim mogle dohvaćati sa bilo kojeg drugog hotmail računa putem posebno oblikovane URL adrese. Ta je URL adresa sadržavala korisničko ime i valjani broj poruke tuđeg računa. Osnovni URL koji se koristio u napadu izgledao je ovako:

```
http://pv2fd.pav2.hotmail.msn.com/cgi-bin/saferd?
_lang=EN&hm___tg=http%3a%2f%2f64%2e4%2e36%2e250%2fcgi
%2dbin%2fgetmsg&hm___qs=%26msg%3dMSGXXXXXXXXX%
2e(X)X%26start%3d1%26len%3d99999999999%26login%
3dUSERNAME%26domain%3dhotmail%2ecom
```

U primjeru zlonamjernog URL zapisa je USERNAME korisničko ime računa u koji se želi provaliti, a XXXXXXXXX devetero znamenkasti broj poruke te (X)X je drugi broj između 0 i 59.

Zbog jednostavnosti napada vrlo brzo su novine i web stranice na Internetu objavile metodu napada te je na desetke tisuća napadača krenulo u pohod na Hotmail. Prije nego što je primijenjena zakrpa otkriveni su milijuni korisničkih računa u koje je bilo provaljeno u razdoblju između 1. i 21. kolovoza 2001. godine.

Još jedan zanimljiv napad dogodio se u veljači 2008. godine kada su zlonamjerni korisnici uspjeli prevariti Hotmail-ov program CAPTCHA. Svi korisnici Interneta upoznati su s potpuno automatiziranim javnim Turingovim testom (eng. Completely Automated Public Turing) kojim se utvrđuje razlika između računala i ljudi na Internetu. CAPTCHA je brza metoda koja provjerava je li osoba koja se prijavljuje za neku uslugu zaista osoba ili bot. Obično su to slike sa izobličenim, jedva prepoznatljivim slovima i brojevima koje korisnik mora upisati u za to predviđeno polje. Do sada je sustav uspijevao usporiti zlonamjerne botove, međutim prijavljeno je da se CAPTCHA koja se koristi za Hotmail, može prevariti za manje od šezdeset sekundi. Nekoliko tjedana kasnije otkriveno je da je i CAPTCHA koju koristi Gmail također probijena.

5. Korištenje web mail servisa

5.1. Preporuke za korištenje web mail servisa

Upotreba web mail servisa vrlo je praktična jer korisnik može svojoj elektroničkoj pošti pristupiti sa bilo kojeg računala povezanog na Internet. Međutim, korisnik samim time što posjeduje web mail korisnički račun, omogućava da njegovi podaci budu izloženi zlouporabi. Zbog toga je dobro proučiti koje sve sigurnosne mjere primjenjuju web mail servisi. Poznati web mail servisi kao što su Gmail, Yahoo! Mail i Hotmail otvorili su blogove posebno namijenjene prijavi neželjene pošte te napada.

Korisnici uvijek moraju biti na oprezu kako bi se zaštitili od phishing napada. Osim toga, potrebno je paziti i na sadržaj privitaka koji se šalju porukama elektroničke pošte. Svima bi trebala postati navika provjeravanje sumnjivih poveznica (eng. link) preko besplatnih skenera na webu, kao što je LinkScanner na Explabs.com. Također korisnike se potiče na kopiranje poveznica izravno u web preglednik ukoliko ju žele slijediti. Prilikom stvaranja zaporke preporuča se korištenje više od sedam znakova koji mogu biti velika ili mala slova, brojevi te određeni posebni znakovi (primjer „dobre“ zaporke: *ST3k6sw&9e!u*). Osim toga, dobro je postaviti rok trajanja na zaporku, na primjer na sedam mjeseci.

Edukacija korisnika je osnova svake sigurnosne politike i vrlo je važno da svaki web mail sustav ima ugrađenu tehnologiju koja omogućava provođenje sigurnosnih mjera.

Napadači često koriste ranjivosti web preglednika kako bi izveli svoje napade na web mail usluge te je preporučljivo da korisnici redovito instaliraju novo objavljene zakrpe i inačice te na taj način smanje mogućnost zlouporabe.

Google na primjer upozorava svoje korisnike da u svrhu zaštite za prijavu na korisnički račun koriste isključivo stranicu https://www.google.com/accounts.

5.2. Dodatna zaštita

Web mail dozvoljava promet paketima upotrebnom standarda HTTP te HTTPS veza, što čini web mail servise metom različitih mreža botova koji koriste ugrožena računala za slanje neželjene elektroničke pošte ili virusima zaražene poruke. Dobro postavljeno proxy računalo može spriječiti takve napade kriptiranjem poruka i analiziranjem web mail prometa.

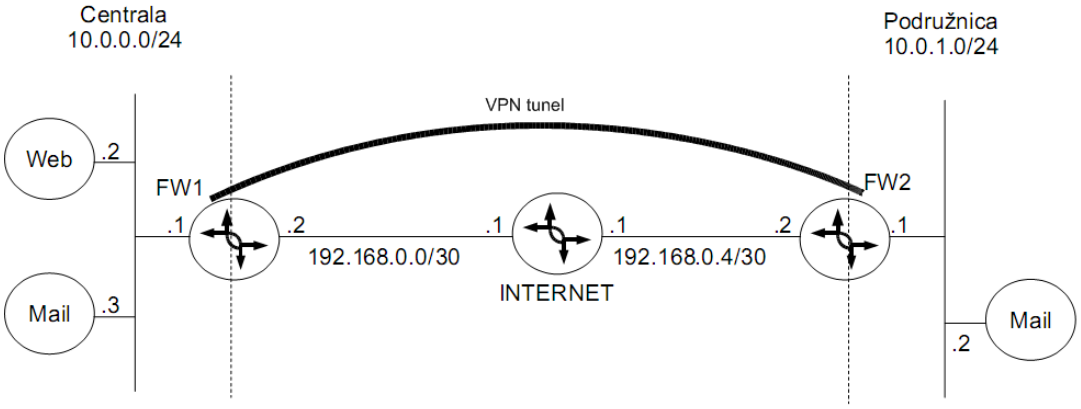
5.2.1. HTTPS

Upotreba HTTPS standarda umjesto HTTP također može poboljšati sigurnost web mail sjednice. HTTPS nije zaseban protokol već kombinacija uobičajene HTTP interakcije preko kriptirane SSL (eng. Secure Sockets Layer) ili TLS (eng. Transport Layer Security) veze. Upotreba HTTPS standarda pruža dostatnu zaštitu od prisluškivanja, ali mogući su napadi s čovjekom u sredini (eng. man-in-the-middle), koji uključuju presretanje prometa. HTTPS URL može koristiti točno određena TCP vrata, a pretpostavljeni broj TCP vrata je 443. Web stranice koje koriste HTTPS veze obično imaju certifikate koji jamče da je onaj koji ga posjeduje zaista onaj kojim se predstavlja.

5.2.2. VPN

Osim HTTPS standarda, korisnici se mogu zaštititi upotrebom VPN (eng. Virtual Private Network) računalnih mreža. U virtualnoj privatnoj mreži (VPN) podaci se između lokacija šalju javnim Internetom, ali se osigurava da usmjernici (eng. router) na tim lokacijama komuniciraju isključivo jedan s drugim. Dobiva se iluzija privatne mreže. Tri su osnovne primjene virtualnih privatnih mreža, a to su pristup udaljenom računalu, povezivanje lokalnih mreža preko Interneta te preko Intraneta. Komunikacija između računala zaštićena je kriptiranjem, odnosno za slanje paketa koristi se IPsec protokol. IPSec je protokol, koji podržava siguran prijenos podataka preko IP mreže. IPSec podaci su organizirani u posebne enkapsulirane pakete. Takvi se paketi prilikom slanja kriptiraju kriptografskim algoritmom dogovorenim između dvije strane IP tunela. Sakriven je ne samo sadržaj, nego i adrese pošiljatelja i primatelja.

Na slici je prikazan najčešći način upotrebe VPN-a. Dvije lokalne mreže povezane su VPN kanalom u jedinstvenu cjelinu. Na slici su s FW1 i FW2 označeni usmjernici koji povezuju centralu i podružnicu s Internetom, ali ti usmjernici istovremeno imaju i funkciju vatrozida. Osim usmjernika prikazani su i bitni servisi u privatnoj mreži – web i mail poslužitelji. Na slici su označene i IP adrese koje pripadaju pojedinoj mreži te adrese sučelja.



Slika 14.VPN

IP paketi koji se razmjenjuju između računala na krajevima VPN kanala su kriptirani i nečitljivi ostalim korisnicima Interneta. Unutar lokalnih mreža koje se ovim putem povezuju paketi su dekriptirani i čitljivi računalima članovima mreže. Ovakva se veza zbog svojih karakteristika naziva i VPN IP tunel, a sam postupak spajanja - IP tuneliranje. Poopćeno, tuneliranje je pojam koji označava da se u podatkovnim jedinicama jednog sloja prenose paketi tog ili nižih slojeva.

Osnovna prednost VPN tunela je što se njegovom upotrebom po cijeni pristupa javnoj mreži (Internetu) omogućava sigurna razmjena podataka sa korisničkih računala iz dvije ili više udaljenih mreža kao da se one nalaze na istoj lokaciji, i spojene su u lokalnu mrežu.

6. Zaključak

Kako raste popularnost web pristupa sandučiću elektroničke pošte, tako se povećava i opasnost od zlouporabe. Postoji mnogo načina na koje napadači mogu ugroziti sigurnost korisnikove elektroničke pošte. Neke od metoda zlouporabe uključuju iskorištavanje XSS ranjivosti, krađa sjednice te phishing napade. Najpoznatiji web mail servisi nude različite mjere sigurnosti, no napadači uvijek smišljaju nove načine iskorištavanja ranjivosti web mail aplikacija. Osim što poruke elektroničke pošte mogu zlouporabiti napadači, upitna je i privatnost podataka prema politici privatnosti koju korisnici prihvaćaju prilikom stvaranja korisničkih računa elektroničke pošte. Korisnici mogu smanjiti opasnost od napada ukoliko su oprezni prilikom otvaranja poruka elektroničke pošte te ukoliko slijede preporuke za sigurno rukovanje elektroničkom poštom. Edukacija korisnika je osnova svake sigurnosne politike i vrlo je važno da svaki web mail sustav ima ugrađenu tehnologiju koja omogućava provođenje sigurnosnih mjera. Sve web mail tvrtke neprekidno rade na poboljšanju sigurnosti web mail servisa. Rastom konkurencije web mail servisi će u budućnosti nuditi sve više funkcionalnosti orijentiranih personalizaciji funkcionalnosti. Također rast će i kapacitet prostora za pohranu poruka elektroničke pošte sve dok svi web mail servise neće nuditi neograničen kapacitet. Što se tiče sigurnosti, vječna trka napadača s novim načinima ugroze i proizvođača programskih rješenja definitivno će biti još izraženija i kompleksnija. Ono što se može svakog korisnika savjetovati jest da se pravovremeno informira o potencijalnim opasnostima te sluša savjete stručnjaka za računalnu sigurnost.

7. Reference

[1] http://www.sahughes.net/papers/squirrelmail/jcmi2003/, funkcioniranje web mail servisa

[2] http://en.wikipedia.org/wiki/Webmail, o web mail servisima

[3] http://googleonlinesecurity.blogspot.com/2008/11/gmail-security-and-recent-phishing.html, Gmail Security Blog

[4] http://www.governmentsecurity.org/archive/t12454.html, Gmail sigurnosna ranjivost

[5] http://antispam.yahoo.com/, Yahoo Security

[6] http://www.theregister.co.uk/2008/10/27/yahoo_xss_vuln/, Yahoo! XSS napad

[7] http://arstechnica.com/news.ars/post/20080415-gone-in-60-seconds-spambot-cracks-livehotmail-captcha.html, Hotmail CAPTCHA ranjivost

[8] http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1313468,00.html, Preporuke za sigurno korištenje web mail servisa

[9] http://www.ditii.com/2008/04/20/windows-live-hotmail-security-tips/, Preporuke za sigurno korištenje web mail servisa

[10] http://www.hoax-slayer.com/webmail-account-phishing-scam.shtml, web mail phishing napadi

[11] http://en.wikipedia.org/wiki/Https, HTTPS

[12] Mreže računala, materijali za laboratorijske vježbe 2006

[13] http://en.wikipedia.org/wiki/Gmail, Gmail

[14] http://en.wikipedia.org/wiki/Yahoo!, Yahoo!

[15] http://en.wikipedia.org/wiki/Hotmail, Hotmail

[16] http://en.wikipedia.org/wiki/Session_hijacking, krađa sjednica

[17] http://arstechnica.com/news.ars/post/20080201-report-google-mail-vulnerable-to-sidejacking-despite-ssl.html, Gmail sidejacking

[18] http://www.gordano.com/kb.htm?q=1450, STARTTLS

[19] http://technet.microsoft.com/en-us/library/aa997437.aspx, OWA

[20] http://www.squirrelmail.org/index.php, SquirrelMail

[21] http://www.itfacts.biz/people-check-e-mail-5-times-a-day-on-average/3429, IT facts

[22] http://www.itfacts.biz/683-mln-e-mail-users-worlwide-130-bln-e-mails-sent-daily/3428, IT facts 2

[23] http://en.wikipedia.org/wiki/IMAP, IMAP

[24] http://en.wikipedia.org/wiki/Pop3.POP3