Sigurnost računalnih sustava

Osnovni pojmovi i uvod u sigurnost

doc. dr. sc. Ante Đerek
doc. dr. sc. Stjepan Groš
izv. prof. dr. sc. Miljenko Mikuc
izv. prof. dr. sc. Marin Vuković

Što znači „sigurno” i „sigurnost”?

- Lozinke su sigurne
  - Moraju biti poznate samo ovlaštenom sustavu ili osobi
- Web stranice tvrtke su sigurne
  - Trebaju biti poznate svima, ali ne smiju biti neovlašteno mijenjane
- Poslužitelj je siguran
  - Na poslužitelju smiju raditi samo ovlaštene osobe, ne smiju se koristiti neovlaštene aplikacije, ne smije biti neovlaštenih izmjena i mora biti na raspolaganju korisnicima
- Tvrtka je sigurna
  - Njeni sustavi su sigurni i na raspolaganju korisnicima

Dakle, što je sigurnost?

- Na temelju prethodnih primjera možemo zaključiti kako je pojam sigurnosti ovisan o kontekstu
  - Može se odnositi na podatke, aplikacije, sustave, …
- Čak i za isti objekt može značiti različite stvari
  - Podaci u jednom slučaju ne smiju biti poznati svima (lozinke), a u drugom moraju (Web stranice, odnosno njihov sadržaj)
- S obzirom na tu složenost pojma sigurnost morat ćemo pronaći odgovarajuću definiciju koja uzima u obzir kontekst

Definicija sigurnosti

- Niz je mogućih definicija sigurnosti, mi ćemo se u sklopu ovog predmeta držati sljedeće definicije

  *Sigurnost je **kontinuirani proces** čijim provođenjem se osigurava određeno **stanje** (sustava, podataka/informacija). Željeno stanje je definirano **zahtjevima**.*
- Kada su zahtjevi ispunjeni, kažemo da je sustav (alternativno podatak/informacija) sigurna.
  - Ako neki od zahtjeva nije ispunjen, kažemo da se desio **incident**, odnosno, da je **narušena sigurnost**.
  - Reći da je nešto nesigurno ne znači da se desio incident
  - Zahtjeve moramo definirati prije nego započnemo raspravljati o sigurnosti
  - Zahtjevi su kontekstno ovisni, odnosno, ovise o specifičnoj situaciji

Temeljni sigurnosni zahtjevi

- povjerljivost (engl. confidentiality), tajnost (engl. secrecy)
  - podaci/informacije moraju biti dostupne samo ovlaštenim entitetima
- cjelovitost, integritet (engl. integrity)
  - jamstvo da su podaci/informacije poslane, primljene ili pohranjene u izvornom i nepromijenjenom obliku
- raspoloživost (engl. availability)
  - informacije moraju biti raspoložive, a sustavi i usluge u operativnom stanju, usprkos mogućim neočekivanim i nepredvidljivim događajima
    - primjerice nestanku struje, prirodnim nepogodama, nesrećama i zlonamjernim napadima

Neki dodatni sigurnosni zahtjevi

- U skup mogućih zahtjeva dodaju se još autentičnost i neporecivost
  - Međutim nisu toliko prihvaćeni kao prethodna tri
- Autentičnost (engl. authenticity)
  - potvrda identiteta korisnika; ovjera vjerodostojnosti (autentifikacija) sudionika komunikacije; ovjera izvora podataka
- Neporecivost (engl. non-repudiation)
  - sudionici ne mogu poreći akciju u kojoj su sudjelovali, npr. nemogućnost naknadnog odricanja slanja, odnosno primanja, poruke

Sigurnosni zahtjevi: podaci vs. sustavi

- Sigurnosni zahtjevi odlično odgovaraju podacima
- Kod sustava ipak nije tako jednostavno
  - Primjerice, što znači zahtjev tajnosti kada je u pitanju računalo?
    - Da se ne zna da to računalo postoji? Da su podaci na računalu tajni – koji podaci na računalu?
  - Što je s tajnošću kada su u pitanju tvrtke?
  - Slična pitanja se mogu postaviti i za druge sigurnosne zahtjeve
- U praksi, za složene sustave se sigurno stanje ne opisuje samo sa temeljnim sigurnosnim zahtjevima

Prijetnje i ranjivosti

- Da bi se desio incident (narušila sigurnost) moraju postojati dva preduvjeta: **ranjivost** i **prijetnja**
  - Ranjivost (engl. vulnerability) je pogreška ili slabost u dizajnu sustava, implementaciji, upotrebi ili upravljanju koja se može iskoristiti za narušavanje sigurnosti sustava ili informacije.
  - Prijetnja (engl. threat) je bilo koja okolnost ili događaj koji ima potencijal narušiti sigurnost sustava ili informacije
- Napad je realizacija namjerne prijetnje

Rizik

- Vrlo čest pojam u sigurnosti
  - Ali nije specifičan za sigurnost! S rizicima se susrećete u svakodnevnom životu.
  - Rizici se koriste u upravljanju sigurnošću – omogućavaju rangiranje problema!
- Mnoštvo je definicija rizika, ali mi ćemo reći da je to **očekivani gubitak** koji nastaje kao posljedica prijetnje, vjerojatnosti ostvarenja prijetnje, štete i ranjivosti.
  - Mogu biti kvantitativni (recimo, 1 – 5) ili kvalitativni (Niski, Srednji, Visoki)
  - Rizici su kontekstno osjetljivi!
    - Nije isto koristite li neku aplikaciju vi ili, primjerice, predsjednik neke države

Načini na koje postižemo sigurnost

- Pojedinu zaštitu koju primjenjujemo kako bi postigli sigurnost nazivamo kontrola (engl. control)
- Sve kontrole su razvrstane u tri velike grupe:
  - Fizičke kontrole
    - Kamere, zaštitari, blindirana vrata, …
  - Tehničke kontrole (alternativno, sigurnosni mehanizmi)
    - Kriptografija, vatrozidi, sustavi za detekciju napada, antivirusi, …
  - Administrativne kontrole
    - Politike, pravilnici, itd.
    - Različiti propisi kojima definiramo što znači biti siguran, kako se ljudi moraju ponašati, kako uređaji moraju biti podešeni, …

Sigurnost je sustavsko pitanje

- Sigurnost se ne može riješiti u jednoj komponenti
  - Dodavanje kriptografije ne rješava problem
  - Vatrozid (firewall) neće riješiti problem
  - Antivirus neće također riješiti problem
- Sigurnost komponente je bitna, ali u konačnici komponente su dio sustava
  - U interakcijama se također javljaju ranjivosti
- Kako bi bili sigurni morate voditi o svemu računa
  - Obrana u dubinu (engl. defense in depth)

Područja primjene sigurnosti (1)

- Informacijska sigurnost (engl. information security)
  - sigurnost informacija
  - u fokusu i informacije na papiru, u nekom registratoru i slično
- Kibernetička sigurnost (engl. cyber security)
  - sigurnost **kibernetičkog prostora** i njegov utjecaj na stvarni/fizički svijet
  - nešto “unutar” računala, potrebna je određena razina složenosti da kibernetički prostor postane problem
    - Dovoljnu složenost kibernetičkog prostora je omogućio Internet i primjena ICT-ja u upravljačkim sustavima
  - Interdisciplinarno područje – uključuje sociologiju, psihologiju, ekonomiju, pravo, vojne znanosti, obavještajni rad, itd.

Područja primjene sigurnosti (2)

- Mrežna sigurnost
  - Sigurnost komunikacije (podaci tijekom prijenosa) i komunikacijskih sustava
- Računalna sigurnost (engl. computer security)
  - Sigurnost računalnog sustava
- Aplikacijska sigurnost (engl. application security)
  - Sigurnost aplikacije tijekom dizajna, razvoja te upotrebe

Područja primjene sigurnosti (3)

- Sigurnost upravljačkih sustava
  - Vrlo široko područje u kojoj je osnovni zahtjev raspoloživost, ne tajnost
  - Upravljački sustavi kontroliraju fizičke procese
  - Njihovom manipulacijom moguće je napraviti fizičku štetu te čak ozlijediti i čovjeka
  - O upravljačkim sustavima ovisi kritična infrastruktura!
- Sigurnost računarstva u oblaku (engl. cloud security)
  - Sigurnost sustava i informacija u računalnom oblaku

Podjela sigurnosti (1)

- Podjela na ofenzivnu i defenzivnu sigurnost
  - Ofenzivna sigurnost – bavi se napadačkim aspektima
  - Defenzivna sigurnost – bavi se obrambenim aspektima
- Neki dijelovi su zajednički
  - Alati koji se koriste za napad, mogu se koristiti i za obranu
  - I jedna i druga se dijele na razine: tehničku, taktičku, operativnu, stratešku

Podjela sigurnosti (2)

- Podjela na tehničku, taktičku, operativnu i stratešku sigurnost
  - Tehnička – direktno vezano uz tehničke aspekte
  - Taktička – povezivanje više tehničkih aspekata u jednu cjelinu
  - Operativna – povezivanje više taktičkih aspekata u jednu cjelinu
    - Ta jedna cjelina se naziva **operacija**
  - Strateška – definira smisao i svrhu, iz nje proizlazi operativna razina (operacije)

Sigurnost i privatnost

- Sigurnost i privatnost nisu isti pojmovi
- Privatnost je pravo pojedinca na kontrolu nad vlastitim osobnim podacima
  - Privatnost se odnosi na pojedinca, tajnost na podatke
  - Narušavanje sigurnosti ne znači nužno i narušavanje privatnosti
    - Primjerice, brisanje podataka narušava raspoloživost i potencijalno integritet, ali ne i privatnost
  - Poboljšanje sigurnosti ne znači nužno i poboljšavanje privatnosti
    - Primjerice, praćenje svih zaposlenika radi zaštite (sigurnosti) tvrtke kosi se sa privatnošću pojedinaca
- Na Internetu je vrlo bitno pitanje privatnosti!

Upozorenje: postoje i druge „sigurnosti”

- Kada u informacijsko-komunikacijskim tehnologijama koristimo pojam „sigurnost” tada mislimo na neke od sigurnosti navedene na prethodnim slajdovima
- ALI, pojam „sigurnosti” je vrlo širok i uključuje neka područja koja nemaju veze s IKT sigurnošću
  - Geopolitička sigurnost, vojna sigurnost, fizička sigurnost, itd.
  - Zaključak je: pazite kad pričate s nekim tko nije u IKT-u da ne dođe do zabune

Sigurnost i „safety”

- Na hrvatskom jeziku *security* i *safety* se isto prevode
  - Ali to nisu isti pojmovi, iako između njih postoji preklapanje (u svojstvu raspoloživosti)
- “Safety” je karakteristika sustava da neće prouzročiti štetu (posebno fizičku)
  - „Safety” je temeljna karakteristika koja se traži od upravljačkih sustava

Stručnjak za sigurnost vs. inženjer

- Inženjeri grade sustave
  - Pri tome se inženjeri drže zadanih ograničenja
- Stručnjaci za sigurnost razmišljaju kako se može naštetiti sustavu
  - Traže koja su ograničenja i ispituju što će se desiti ako se ta ograničenja prekrše!

Sigurnost košta!

- Kako bi se sustav učinio sigurnim potrebno je uložiti resurse i vrijeme – to košta
- Svijest još nije na toj razini da se sigurnost tretira kao dodana vrijednost
  - Za razliku od funkcionalnosti koju će svatko prepoznati kao potencijalnu prednost nad konkurencijom!
- Iz tog razloga sigurnost se ne uzima u obzir, ili ako treba štedjeti prva je na listi za odstrel
  - OSIM ako netko vanjski ne inzistira na sigurnosti – klijent/korisnik, regulator

Čovjek kao osnovni izvor problema

- Temeljni izvor problema u sigurnosti je **čovjek**
- Sve proizlazi iz ljudske nesavršenosti – **svi** pravimo greške
  - I oni koji se bave sigurnošću, kao i svi računarci – samo treba biti strpljiv
  - Pokušava se napraviti alate koji će ispraviti ljudske pogreške – ali daleko smo od rješenja
- Nažalost, ne možemo očekivati da će se ljudi promijeniti i možemo očekivati probleme u doglednoj budućnosti

Stražnja vrata u sustave (engl. backdoor)

- Stražnja vrata su svojstvo sustava da omogućava pristup nekome tko ne bi smio imati pristup
- Ugrađuju se namjerno i slučajno
  - Slučajno: Primjerice, nakon testiranja ostane nekakva funkcionalnost koja se nađe na produkcijskim sustavima
- Stalni su pokušaji nametanja regulative koja bi proizvođače prisilila da ugrađuju stražnja vrata u sustave
  - Problem je što stražnja vrata mogu otkriti i zloupotrijebiti i napadači

Prikriveni kanali (engl. covert channel)

- Komunikacijski kanal kojim se prenose podaci, a da toga nisu svjesni vlasnici ili legitimni korisnici sustava u kojemu se kanal javlja
- Prikrivene kanale koriste napadači kako bi mogli komunicirati, a da ne budu primijećeni
- Primjeri prikrivenih kanala
  - Echo request/reply poruke omogućavaju smještaj podataka
    - Informacija se može kodirati i u duljinu Echo request/reply poruka
  - Razrješavanje imena koja ne postoje, ali nose u sebi kodiranu informaciju

Sporedni kanal (engl. side channel)

- Komunikacijski kanal kroz koji prolaze dodatne informacije
  - Ne želimo da se te informacije otkriju potencijalnom napadaču
  - Kanal je posljedica načina na koji rade, ili su implementirani, sustavi
- Primjeri sporednih kanala
  - Razlika u potrošnji električne energije
  - Implementacija algoritama koji kroz vremenske odnose otkrivaju implementacijske detalje ili skrivene tajne
  - Vremena pristupa priručnoj memoriji u mikroprocesorima

Povjerenje i povjerljiv(ost)

- Povjerenje (engl. trust, trustworthy, trustworthiness) je pojam vezan uz ljude, ali i sustave
  - Čim je nešto vezano uz ljude, tada se dotiče psihologije i sociologije!
- Moguća definicija: povjerenje znači *informirano oslanjanje na karakter, sposobnost, snagu, istinu nekoga ili nečega*
- Povjerenje se može ostvarivati ili graditi na razne načine (npr. reputacija, provjere podataka)
- **Uvijek vjerujete nečemu – to je neizbježno!**

CTF natjecanja

Hvala!