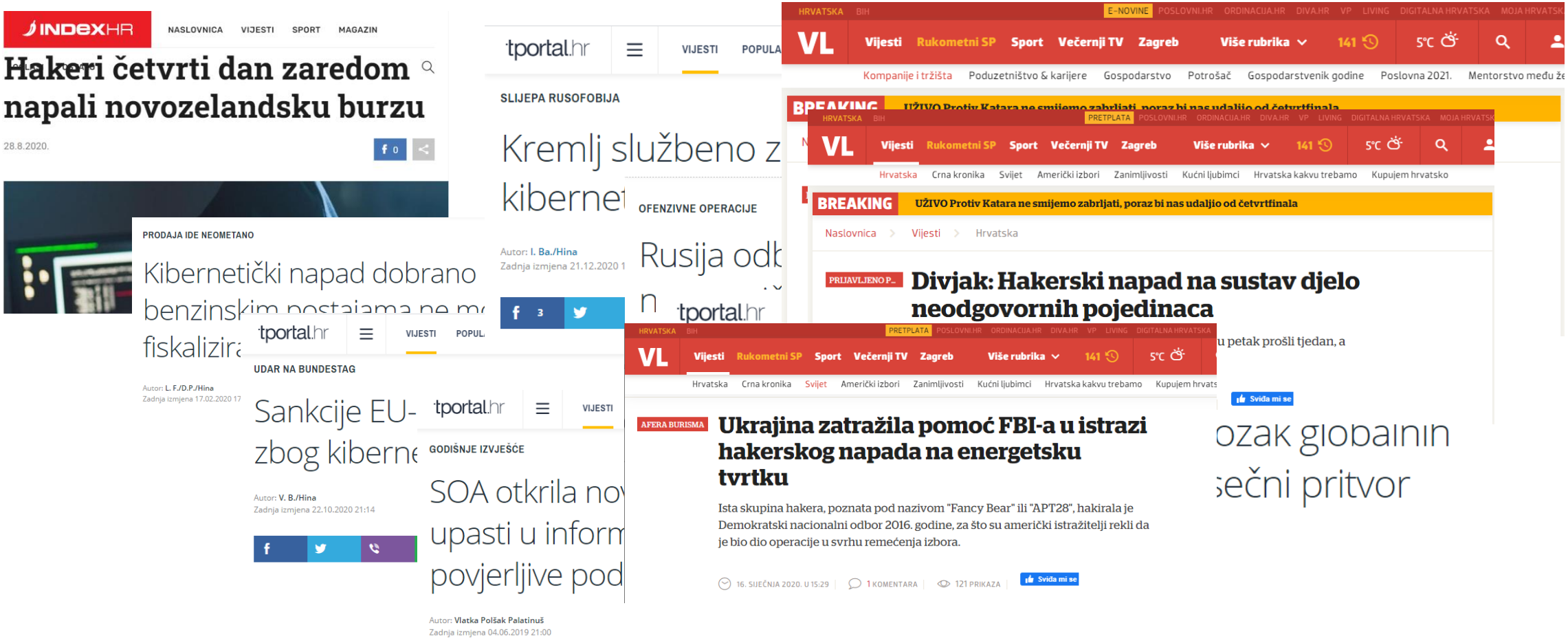
Sigurnost računalnih sustava

Uvod

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

Zašto sigurnost?



Što želimo postići s ovim predmetom?

- **Dati pregled sigurnosti i naučiti vas dovoljno da shvaćate probleme**
- To će Vam
  - Omogućiti razumijevanje informacija koje pronalazite na Internetu (uključivo novinske i druge članke)
  - Omogućiti razumijevanje potencijalnih opasnosti i nekih zaštita
  - Pomoći u profesionalnoj karijeri

Što je uopće sigurnost?

- Sigurnost se dovodi u vezu s „hakerima”, ali sigurnost je puno više od toga
  - Poneko to povezuje i sa kriptografijom
- Zadaća sigurnosti je učiniti sustave, procese, ljude otpornima na sve loše što im se može desiti zbog raznih manjkavosti
  - Ovo će nam biti privremena definicija
  - Prvenstveno nas zanima obrana, nećemo se baviti napadačkom stranom sigurnosti

S čime se područje sigurnosti bavi?

- U sigurnosti se prvenstveno bavimo sa zaštitom
  - Kako spriječiti da se nešto loše desi?
- Spriječavanje (između ostalog) uključuje
  - Razumijevanje manjkavosti sustava (aplikacija, tvrtka, …)
  - Ugrađivanje zaštita
  - Detekcija kada su zaštite zaobiđene
  - Utvrđivanje što se desilo te posljedice zaobilaska zaštita
  - Oporavak i sprečavanje sličnih događaja u budućnosti

Može li se izbjeći sigurnost?

- Moguće da nekoga od Vas sigurnost ne zanima
  - Vjerojatno se onda pitate zbog čega ovaj predmet?
- Nekoliko mogućih odgovora
  - Vi možete biti cilj napada
  - Sustav koji radite ili održavate može biti cilj napada
  - Komponenta koju radite ili održavate može biti cilj napada
- Zaključak: sigurnost se ne može izbjeći
  - Morate barem biti svjesni mogućih problema

Svrha predmeta

- Svrha predmeta je **upoznati sve studente** s problemima sigurnosti
  - Dobiti širok ali plitak uvid u sigurnost
  - Dovoljno znanja da znate koji su potencijalni problemi
  - Upoznati se s terminologijom kako bi mogli razgovarati s drugim ekspertima i ekspertima za sigurnost
- Za studente koje zanima sigurnost predmet daje temelje koji se produbljuju kroz druge predmete

Ishodi učenja

1. Objasniti osnovne pojmove i koncepte vezane uz računalnu sigurnost
2. Opisati vrste sigurnosnih prijetnji i napada te najčešćih načina obrana
3. Opisati svojstva često korištenih kriptografskih primitiva
4. Objasniti ulogu infrastrukture javnih ključeva i protokola TLS
5. Opisati mehanizme za zaštitu sigurnosti
6. Upoznati se s različitim područjima sigurnosti
7. Implementirati jednostavni napad na ranjivi sustav

Očekivano predznanje

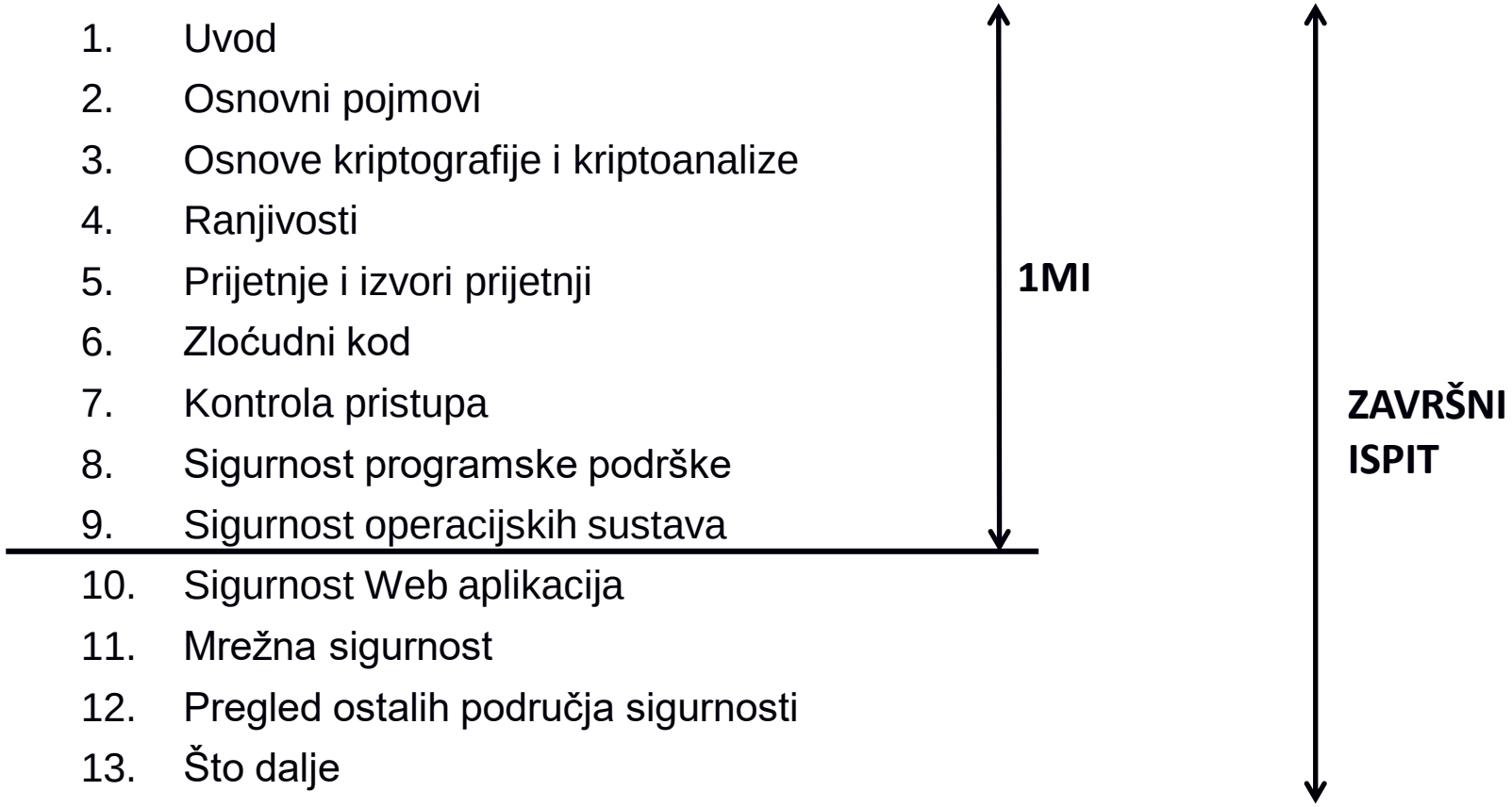
- Programiranje
- Arhitektura računala
- Operacijski sustavi
- Komunikacijske mreže
- Vjerojatnost
- Dobro dođe poznavanje Unix/Linux okruženja

Predavanja

- Predavanja su obavezna
  - Neće biti popisivanja niti će se dijeliti bodovi s predavanja
  - Poželjno je postavljanje pitanja na predavanju i rasprava!
- Predavanja će biti u živo

Teme predavanja

1. Uvod
2. Osnovni pojmovi
3. Osnove kriptografije i kriptoanalize
4. Ranjivosti
5. Prijetnje i izvori prijetnji
6. Zlođudni kod
7. Kontrola pristupa
8. Sigurnost programske podrške
9. Sigurnost operacijskih sustava
10. Sigurnost Web aplikacija
11. Mrežna sigurnost
12. Pregled ostalih područja sigurnosti
13. Što dalje



Laboratorijske vježbe (1)

- 4 laboratorijske vježbe
- Način bodovanja i predaje
  - Za svaku vježbu postoji rok za maksimalan broj bodova
  - Nakon toga još jedan rok za predaju za **nula** bodova
  - Vježba se mora predati bez obzira nosi li još neke bodove ili ne
  - U jednom terminu moguće je predati najviše dvije vježbe

Laboratorijske vježbe (2)

- Zadatak studenta je da pravovremeno preda labos i uvjeri se da je to napravio na ispravan način. Ako netko preda neispravan labos, onda mu labos neće biti priznat!
  - Dešavalo se prošle godine da studenti predaju neispravne datoteke, labose s drugih predmeta, …
- Provjeravamo sličnost predanih labosa
  - Prepisan labos nosi poništenje labosa i prijavu stegovnom povjerenstvu

Teme laboratorijskih vježbi

1. Kriptografija ~ 6.3. – 19.3.
2. Autentifikacija – sigurnost lozinki ~ 27.3. – 10.4.
3. Sigurnost programske podrške ~ 1.5. – 14.5.
4. Mrežna sigurnost ~ 22.5. – 4.6.

Način polaganja predmeta

- Kontinuirano praćenje nastave
  - Predaja laboratorijskih vježbi
  - Pristup međuispitu i završnom ispitu
  - **Bliceva može biti ali se računaju kao bonus**
- Ispiti
  - Pristup pismenom ispitu
  - Usmeni ispit

Elementi ocjene na kontinuiranom praćenju

- Raspodjela bodova po komponentama

Laboratorijske vježbe	20%
Međuispit	40%
Završni ispit	40%

- Minimumi koje je potrebno ostvariti

Laboratorijske vježbe	min 20% (od 20% koliko nosi labosa)
Međuispit	min 40% (od 40% koliko nosi MI)
Završni ispit	min 40% (od 40% koliko nosi ZI)

Elementi ocjene na ispitima (1)

- Raspodjela bodova po komponentama

Laboratorijske vježbe	20%
Pismeni ispit	80%

- Minimumi koje je potrebno ostvariti

Laboratorijske vježbe	min 20% (od 20% koliko nosi labosa)
Pismeni ispit	min 50% (od 80% koliko nosi PI)

- **Postoji mogućnost usmenih ispita na pojednim rokovima. U tom slučaju bit ćete pravovremeno obaviješteni**

Elementi ocjene na ispitima s usmenim

- Raspodjela bodova po komponentama

Laboratorijske vježbe	20%
Pismeni ispit	70%
Usmeni ispit	10%

- Minimumi koje je potrebno ostvariti za pristup pismenom ispitu i prolazak pismenog ispita

Laboratorijske vježbe	min 20% (od 20% koliko nosi labosa)
Pismeni ispit	min 50% (od 50% koliko nosi PI)

- **Za prolaz ispita je potrebno ostvariti minimum 50% ukupnog broja bodova**

Bodovne granice za oba načina polaganja

Dovoljan (2)	50
Dobar (3)	63
Vrlo dobar (4)	75
Izvrstan (5)	88

Istaknuti studenti

- Najbolje studente generacije ističemo na Web stranicama predmeta
  - https://www.fer.hr/predmet/srs/istaknuti_studenti
    - Stranica je javno dostupna
- Na kraju semestra dobijate mail kako bi dali privolu da se vaše ime objavi
  - Ako ne date privolu, ne objavljujemo ništa!

Predavači

doc. dr. sc. Ante Đerek
ante.derek@fer.hr

izv. prof. dr. sc. Stjepan Groš
stjepan.gros@fer.hr

izv. prof. dr. sc. Miljenko Mikuc
miljenko.mikuc@fer.hr

izv. prof. dr. sc. Marin Vuković
marin.vukovic@fer.hr

Konzultacije

- Nema fiksnih termina konzultacija, sve je u dogovoru s predavačima
- **Za sva pitanja, uključivo konzultacije, koristiti mail srs@fer.hr**
  - Ako trebate konzulatacije, u poruci navedite da želite konzultacije, iz kojeg dijela gradiva i zašto želite konzultacije
- Konzultacija nema dva dana prije ispita, međuispita, odnosno završnog ispita

Literatura (1)

- Slajdovi će biti dostupni na stranicama predmeta
- Tijekom semestra, vezano uz specifične teme, dobijat ćete još literature
- Za izradu laboratorijskih vježbi također ćete dobivati literaturu

Literatura (2)

- Prošlogodišnja predavanja su dostupna na YouTube kanalu
  - OPREZ: Moguće su određene izmjene ove godine
- Od knjiga, jedina literatura koju preporučamo je

  Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin, Second Edition by Paul C. van Oorschot. Springer, 2021. 2e ISBN: 978-3-030-83410-4 (hardcopy), 978-3-030-83411-1 (eBook)

  http://people.scs.carleton.ca/~paulv/toolsjewels.html

Neki izvori informacija (1)

- Stručne konferencije
  - BlackHat **USA**/EU/Asia/Israel [www.blackhat.com]
  - DefCon [www.defcon.org]
- Znanstvene konferencije
  - ACM Conference on Computer and Communication Security
  - USENIX Security
  - IEEE Symposium on Security and Privacy

Neki izvori informacija (2)

- Blogovi
  - Krebs On Security, Schneier on Security, A Few Thoughts on Cryptographic Engineering
  - Symantec, Microsoft, FireEye, Kaspersky, …
- Organizacije, udruge i certifikacije
  - SANS, ISACA, ISC2, MITRE
  - Honeynet organization
- Twitter

Etička pitanja

- Nerazumnim korištenjem stvari koje naučimo na ovom predmetu potencijalno kršimo etička načela i zakonske i druge propise
  - Naravno, ovo vrijedi i za one stvari koje ne učimo
- Primjerice
  - Izrada virusa je protuzakonita
  - Skeniranje, kao i svaki drugi pristup resursima bez privole vlasnika je protuzakonit u mnogim državama svijeta, pa i u Hrvatskoj

Kazneni zakon RH

Članak 266, stavak 1

Tko neovlašteno pristupi računalnom sustavu ili računalnim podacima, kaznit će se kaznom zatvora do jedne godine.

Članak 267, stavak 1

Tko onemogući ili otežа rad ili korištenje računalnog sustava, računalnih podataka ili programa ili računalnu komunikaciju, kaznit će se kaznom zatvora do tri godine.

Članak 268, stavak 1

Tko neovlašteno u cijelosti ili djelomično ošteti, izmijeni, izbriše, uništi, učini neuporabljivim ili nedostupnim ili prikaže nedostupnim tuđe računalne podatke ili programe, kaznit će se kaznom zatvora do tri godine.

Članak 269, stavak 1

Tko neovlašteno presretne ili snimi nejavni prijenos računalnih podataka, uključujući i elektromagnetsku emisiju računalnog sustava, ili drugome učini dostupnim tako pribavljene podatke, kaznit će se kaznom zatvora do tri godine.

Hvala!