ЗАШТИТА ПОДАТАКА

Садржај

- Наставници
- Циљ предмета
- Програм предмета
- Начин извођења наставе
- Начин полагања испита
- Литература

Наставници

- Предавања:
- проф. др Зоран Јовановић,
  доц. др Жарко Станисављевић,
  доц. др Павле Вулетић
- zoran@rcub.bg.ac.rs,
  zarko@etf.bg.ac.rs,
  pavle.vuletic@etf.bg.ac.rs
- Консултације после часова или заказати

Наставници

- Вежбе:
- ас. мастер Маја Вукасовић
- majav@etf.rs
- Консултације после часова или заказати

Циљ предмета

- Упознавање студената са основним концептима заштите података. Разумевање основа криптографије и сигурносних протокола. Упознавање са ризицима у мрежном окружењу и упознавање са свим нивоима на којима мере заштите треба да буду уведене.
- Студенти ће стећи знања о начинима за одвраћање, детекцију, спречавање и неутралисање нарушавања сигурности.

Садржај предмета

- Расположивост, аутентикација, ауторизација, тајност, интегритет и контрола приступа
- One-Time-Pad, Алгоритми тока (RC4), блоковски алгоритми (DES, AES), асиметрични алгоритми (Diffie-Hellman, RSA), хеш функције (MD-5, SHA)
- Аутентикационе апликације, управљање кључевима, сигурне Web конекције, електронско плаћање
- Пасивни напади, активни напади, малициозни програми
- Denial of Service
- Мрежне баријере
- ...

Програм предмета

- СИМЕТРИЧНИ АЛГОРИТМИ ШИФРОВАЊА
- ШИФРОВАЊЕ ПОМОЋУ ЈАВНОГ КЉУЧА И ХЕШ ФУНКЦИЈЕ
- АПЛИКАЦИЈЕ ЗА БЕЗБЕДНОСТ У РАЧУНАРСКИМ МРЕЖАМА
- ЗАШТИТА РАЧУНАРСКИХ СИСТЕМА

Симетрични алгоритми шифровања

- Класичне технике шифровања
- Основни концепти блоковских алгоритама шифровања
- Стандард за шифровање података (DES)
- Напредни стандард за шифровање података (AES)
- Додатна разматрања код симетричних шифара (поверљивост,...)

Шифровање помоћу јавног кључа и хеш функције

- Шифровање јавним кључем и RSA алгоритам
- Управљање кључевима (Diffie-Hellman)
- Аутентикација порука и хеш алгоритми
- SHA (Secure Hash Algorithm)
- Дигитални потпис и аутентикациони протоколи

Апликације за безбедност у рачунарским мрежама

- Апликације за аутентикацију (Kerberos, X.509, …)
- Заштита електронске поште (PGP, S/MIME)
- Заштита у рачунарским мрежама (IP Security)
- Заштита на интернету (SSL, ...)

Заштита рачунарских система

- Уљези (детекција, управљање шифрама, ...)
- Злонамерни програми (вируси, …)
- Firewall
- Заштита информационих система коришћењем улога

Начин извођења наставе

- Предавања
- Вежбе
- Лабораторијске вежбе (само на основним студијама)

Начин полагања испита

- Основне студије (ИР и ОЕ):
  - Лаб. вежбе – 15%
    - важе једну школску годину
  - Пројекат – 20%
    - брани се у првом року
    - важи једну школску годину
  - Колоквијум – 40%
    - важи у првом року
  - Испит
    - у првом року 30%
    - у осталим роковима интегрално 65%

Начин полагања испита

- Основне студије (СИ):
  - Лаб. вежбе – 15%
    - важе једну школску годину
  - Пројекат – 20%
    - брани се у првом року
    - важи једну школску годину
  - Колоквијум 1 – 20%
    - важи у првом року
  - Колоквијум 2 – 20%
    - важи у првом року
  - Испит
    - у првом року 30%
    - у осталим роковима интегрално 65%

Начин полагања испита

- Мастер студије:
  - Семестрални рад – 15%
    - важи једну школску годину
  - Пројекат – 20%
    - брани се у првом року
    - важи једну школску годину
  - Колоквијум – 40%
    - важи у првом року
  - Испит
    - у првом року 30%
    - у осталим роковима интегрално 65%

Начин полагања испита

- Коначна оцена се формира на основу броја освојених поена на следећи начин:
- 91<=X<100 – оцена 10
- 81<=X<90 – оцена 9
- 71<=X<80 – оцена 8
- 61<=X<70 – оцена 7
- 51<=X<60 – оцена 6
- 50 и мање – студент није положио испит

Литература

- Слајдови са предавања и вежби на српском језику
- Књига: „*William Stallings: Cryptography and Network Security*“ четврто издање