Hardwarová bezpečnost

Zobrazit rozvrh

Kód	Zakončení	Kredity	Rozsah	Jazyk výuky
BI-HWB.21	Z,ZK	5	2P+2C	česky

Garant předmětu:
Jiří Buček

Přednášející:
Jiří Buček

Cvičící:
Jiří Buček, Ondřej Staníček, Martin Šutovský

Předmět zajišťuje:
katedra informační bezpečnosti

Anotace:

Předmět se zabývá hardwarovými prostředky pro zajištění bezpečnosti počítačových systémů včetně vestavných. Jsou probírány principy funkce kryptografických modulů, bezpečnostních prvků moderních procesorů a ochrany paměťových médií pomocí šifrování. Studenti získají znalosti o zranitelnostech HW prostředků, včetně analýzy postranními kanály, falšování a napadení hardwaru při výrobě. Studenti budou mít přehled o technologiích kontaktních a bezkontaktních čipových karet včetně aplikací a souvisejících témat pro vícefaktorovou autentizaci (biometrii). Studenti porozumí problematice efektivní implementace šifer.

Požadavky:

základy počítačové bezpečnosti a kryptografie, programování

Osnova přednášek:

1. HW kryptografické moduly, úložiště klíčů.
2. Bezpečnostní prvky architektur procesorů.
3. Čipové karty a tokeny: Architektury a systémy.
4. Čipové karty a tokeny: Autentizační protokoly.
5. Čipové karty a tokeny: RFID, Near Field Communication.
6. Metody útoky postranními kanály (odběrová analýza, časový útok, elektromagnetická analýza).
7. Algoritmy šifrování paměťových médií, úvod do polynomiální aritmetiky.
8. Efektivní implementace šifer, šifra AES.
9. Fyzicky neklonovatelné funkce.
10. Generátory skutečně náhodných a pseudonáhodných čísel.
11. Úvod do biometrických metod identifikace.
12. Bezpečnost vestavných zařízení, zranitelnosti moderních procesorů.
13. Důvěryhodný návrh hardware, hardwarové trojské koně.

Osnova cvičení:

1. Úvod do programování čipových karet Java Card
2. Nahrátí appletu na kartu, úkol na PIN
3. Hashovací operace, komunikace s PC
4. Digitální podpis na čipové kartě
5. Základy diferenciální analýzy spotřeby
6. Počítání s polynomy (seminář)
7. Jednoduchá implementace AES-128
8. Optimalizace AES pro 32bitovou platformu
9. Akcelerace AES pomocí dedikovaných instrukcí AES-NI
10. Testování AES na mikrokontroléru ARM
11. Dokončování úloh na AES
12. Analýza odpovědí obvodu PUF

Cíle studia:

Studijní materiály:

1. Mangard S., Oswald E., Popp T. : Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer, 2007. ISBN 387308571.

2. Tuyls P., Skoric B., Kevenaar T. : Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting. Springer, 2007. ISBN 1846289831.

3. Bhunia S., Tehranipoor M. : Hardware Security: A Hands-on Learning Approach. Morgan Kaufmann, 2018. ISBN 9780128124772.

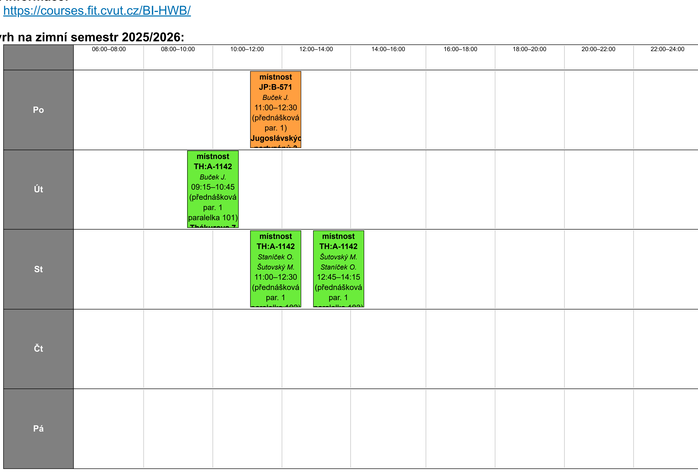
4. Rankl W., Effing W. : Smart Card Handbook (4th Edition). John Wiley & Sons, 2010. ISBN 978-0-470-74367-6.

Poznámka:

This course is presented in Czech.

Další informace:
https://courses.fit.cvut.cz/BI-HWB/

Rozvrh na zimní semestr 2025/2026:



Rozvrh na letní semestr 2025/2026:
Rozvrh není připraven

Předmět je součástí následujících studijních plánů:

- Bc. specializace Informační bezpečnost, 2021 (PS)
- Bc. specializace Manažerská informatika, 2021 (volitelný předmět)
- Bc. specializace Počítačová grafika, 2021 (volitelný předmět)
- Bc. specializace Počítačové inženýrství, 2021 (volitelný předmět)
- Bc. program, pro fázi studia bez specializace, 2021 (VO)
- Bc. specializace Webové inženýrství, 2021 (volitelný předmět)
- Bc. specializace Umělá inteligence, 2021 (volitelný předmět)
- Bc. specializace Teoretická informatika, 2021 (volitelný předmět)
- Bc. specializace Softwarové inženýrství, 2021 (volitelný předmět)
- Bc. specializace Počítačové systémy a virtualizace, 2021 (volitelný předmět)
- Bc. specializace Počítačové sítě a Internet, 2021 (volitelný předmět)
- Bc. specializace Informační bezpečnost, 2024 (PS)
- Bc. program, pro fázi studia bez specializace, 2024 (VO)
- Bc. specializace Manažerská informatika, 2024 (volitelný předmět)
- Bc. specializace Počítačová grafika, 2024 (volitelný předmět)
- Bc. specializace Softwarové inženýrství, 2024 (volitelný předmět)
- Bc. specializace Webové inženýrství, 2024 (volitelný předmět)
- Bc. specializace Počítačové sítě a Internet, 2024 (volitelný předmět)
- Bc. specializace Počítačové inženýrství, 2024 (volitelný předmět)
- Bc. specializace Počítačové systémy a virtualizace, 2024 (volitelný předmět)
- Bc. specializace Umělá inteligence, 2024 (volitelný předmět)
- Bc. specializace Teoretická informatika, 2024 (volitelný předmět)
- Bc. specializace Počítačová grafika s vynecháním BI-SVZ (volitelný předmět)

Platnost dat k 2. 12. 2025