Основни информации за курсот

Наслов на курсот: Инжинеринг на криптографски софтвер

Период на одржување: Септември 2016.

Цел на курсот: Курсот е посветен на најновите достигнувања за инжинеринг на софтвер за индустриски криптографски цели. Студентите ќе научат за имплементациски техники за отимизација на код за криптографски цели како и техники за отпорност на софтверски криптографски напади. Фокусот на курсот ќе бидат најсофистицираните модерни симетрични и асиметрични алгоритми, особено AES, Salsa20 и криптографски алгоритми базирани на елиптични криви. Техниките кои ќе се изучуваат на курсот се далеку над чисто наменски за овие алгоритми и се отшто корисни за оптимизација на (криптографски) софтвер за практична употреба.

Целна група слушатели: Курсот е наменет за студенти од додипломски и последипломски студии на Факултетот за информатички науки и компјутерско инженерство за кои е предвидено признавање на 2 кредити според ЕКТС. Курсот е отворен и за докторанти како и за надворешни и слушатели од други факултети кои ќе пројават интерес. За евентуално признавање на кредити за овие слушатели, тие самите би требало да спроведат постапка во соодветните институции.

Одговорни за спроведување на курсот: Ass. Prof. Peter Schwabe, доц. д-р Симона Самарџиска, м-р Панче Рибарски, м-р Христина Михајлоска

Предавач на курсот: Peter Schwabe, Digital Security Group, Radboud University, Nijmegen, Netherlands.

Администрација на курсот и оцена: Ass. Prof. Peter Schwabe, доц. д-р Симона Самарџиска
Одржување на вежби: м-р Панче Рибарски, м-р Христина Михајлоска

Форма на испитот: Изработка на практичен проект и негова евалуација која вклучува јавна одбрана

Работни часови:

- Предавања - 10 часа
- Практични вежби – 10 часа
- Самостојно учење и изработка на проект – 36 часа

Програма на курсот:

1. Вовед во оптимизација на софтвер
2. Имплементација на симетрични криптографски алгоритми (AES, Salsa20)
3. Аритмитика со повеќекратна прецизност
4. Алгоритми за множење со скалар
5. Криптографија со елиптични криви
6. Најлошите практики за крипто-инжинеринг

Цели на курсот: По завршување на курсот студентите ќе бидат способни да:

- Оптимизираат софтвер на асемблерско ниво
- Ги разбираат перформансите на софтверот
- Заштитат криптографски софтвер од напади базирани на девијации во времето за извршување на алгоритмот (timing attacks)

Кратка биографија на предавачот:

Петер Швабе е еден ов водечките експерти за оптимизација на сигурен код за криптографски потреби во светот. Докторирал на Техничкиот универзитет во Ајндховен, Холандија, под менторство на Тања Ланге и Даниел Бернштајн, во еден од најдобрите светски тимови за криптографија и безбедност. Во моментот е доцент на Радбауд универзитетот во Најмеген Холандија. Има издадено над 30 трудови на престижни криптографски конференции, а неговите трудови се цитирани над 1100 пати според Google Scholar. Бил член на програмскиот одбор на над 30 конференции од областа на криптографијата и криптографското инжинерство. Повеќе информации за предавачот може да најдете на неговата веб страна https://cryptojedi.org/peter/index.shtml.