Enterprise Computing Solutions - Education Services

NABÍDKA ŠKOLENÍ

Prosím kontaktujte nás zde

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: training.ecs.cz@arrow.com
Phone: +420 597 488 811

Základy kryptografie

Kód:	DÉLKA:	CENA:
OTH_CRYPT	16 Hours (2 DENNÍ)	Kč bez DPH 18,000.00

Description

Požadavky na bezpečnost se neustále zvyšují. Kryptografie je důležitým stavebním kamenem, ale bezpečnost není jen kryptografie. Bohužel, úroveň porozumění tomuto tématu a dalším, souvisejícím tématům, je na velice nízké úrovni.

Cíle

Cílem kurzu je základní porozumění klasické kryptografii, její historii a vývoji. V rámci tohoto kurzu je účastník seznámen s důležitostí náhodnosti a nepředvídatelnosti. Na toto téma je navázáno vysvětlení hash funkcí a následně klasických symetrických algoritmů. Zde je součástí rozbor základních proudových a blokových šifer. V rámci asymetrických algoritmů jsou vysvětlovány algoritmy, které tvořily po téměř 40 let jádro soudobé počítačové bezpečnosti, zajišťovaly domluvu na klíčích a digitální podpis.
Co se můžete naučit

Filozofické otázky související s kryptografií
Historie kryptografie
Co znamená entropie, náhodnost a nepředvídatelnost
Hashe, přehled principů, přehled používaných algoritmů, míra jejich bezpečnosti
Symetrické algoritmy (blokové, blokové v proudovém módu, proudové)
Generace módů blokových šifer a jejich užití
Lehká kryptografie
Asymetrické algoritmy pro výměnu klíčů a digitální podpis
Porovnání a metody digitálního podpisu
Krátký přehled zajímavých směrů vývoje:
- MultiParty Computation, Zero Knowledge Protokoly
- Homomorfní kryptografie
- Post-kvantová kryptografie a kvantová kryptografie
Standardizace v oblasti kryptografie
Základní implementace v hardware

Vstupní znalosti

- znalosti středoškolské matematiky
- zkušenosti se správou systémů
- základní znalosti počítačové bezpečnosti

Program

Den 1

- Etické otázky a restrikce v kryptografii
- Historie kryptografie
- Kryptografie, základní pojmy
- Generátory náhodných čísel, jejich význam a rozdělení
- Hashe, přehled principů, přehled používaných algoritmů, míra jejich bezpečnosti
- Symetrické šifrování, historie a rozdíl mezi blokovými a proudovými šiframi
- Symetrické blokové algoritmy a módy jejich operací
- Lehká kryptografie (Lightweight cryptography)

Den 2

- Asymetrické šifrovací algoritmy, principy a porovnání

- Algoritmy pro digitální podpis, principy a porovnání
- Algoritmy pro slepý podpis, ukázka pro Schnorrův algoritmus
- Přehled současného vývoje a seznámení se s termíny:
  - MultiParty Computation, Zero Knowledge Protokoly a Atribute Based Encryption
  - Homomorfní kryptografie
  - Post-kvantová kryptografie a přehled algoritmů
  - Kvantová kryptografie
- Standardizace
- Schopnosti ASIC a FPGA
- Porovnání vlastností CPU a používané instrukce

Termíny školení

Termíny školení na vyžádání, kontaktujte nás prosím

Dodatečné informace

Školení je možné zajistit na míru. Kontaktujte nás pro bližší informace.