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 15,000.00

Description

Ve světě komunikací a honbě za bezpečím je potřeba mít k dispozici odborníky. Osoby znalé vzájemných vztahů a souvislostí. Jednou stranou mince je vhodná volba komunikačních protokolů či architektury, ale uvedená snaha může vyjít snadno naprázdno. Nevhodnou volbou metod se oslabí zabezpečení, umožní čtení či modifikace přenášených dat, nebo se jen sníží rychlost a promarní investice do infrastruktury. Je potřeba si uvědomit, že vaše data, případně data vašich zákazníků se přenáší veřejným prostorem a jedinou ochranou je vhodně zvolená kryptografie.
Zároveň je snahou uvedeného školení vhodně připravit techniky i na požadavky, kladené na ně zákonem o kybernetické bezpečnosti.

Toto školení pořádáme ve spolupráci s kryptologem Janem Dušátkem.

Cíle

Zvládnutí témat
• Restrikce kryptografie ve světě, základní zákony vztahující se ke kryptografii v CZ/SK
• Kryptografie, základní pojmy
• Hashe, přehled principů, používaných algoritmů, míra jejich bezpečnosti
• Generátory náhodných čísel, jejich význam a rozdělení
• Porovnání asymetrických a post-quantum asymetrických algoritmů, principy a porovnání rychlostí
• Porovnání nejznámějších symetrických algoritmů, jejich architektura, omezení daná konstrukcí, rozdíl
• mezi blokovými a proudovými šiframi
• Mody blokových šifer první generace, mody AE a AEAD - třetí a čtvrtá generace, mody pro práci s disky

Program

Program prvního dne
08:00 - 09:00 Prezence
09:00 - 10:00 Kryptologie a její limity dané lokálními zákony
10:00 - 13:00 Hashe, generátory náhodných čísel a asymetrické algoritmy
13:00 - 14:00 Oběd
14:00 - 17:00 Symetrické algoritmy, mody blokových šifer, architektura algoritmů a porovnání rychlostí
Program druhého dne
08:00 - 09:00 Volná diskuse
09:00 - 11:00 Implementace v hardware
11:00 - 13:00 Implementace v software - vrstva SSL
13:00 - 14:00 Oběd
14:00 - 15:00 Hardening aplikací
15:00 - 17:00 Další zajímavé aplikace v reálném životě

Termíny školení

Termíny školení na vyžádání, kontaktujte nás prosím

Dodatečné informace

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