Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií

Ústav počítačových systémov a sietí FIIT STU v Bratislave

vás pozýva na odborný seminár

Správa kľúčov v distribuovanom prostredí

ktorý sa koná dňa

20. apríla 2006 o 13:00

v zasadačke FIIT STU – D 220

prednášať bude

PaedDr. Ladislav HURAJ (KI FPV UMB)

externý doktorand FIIT STU, ktorý na túto tému vypracoval dizertačnú prácu

Anotácia:

V sieťach typu ad-hoc a v ďalších vysokodistribuovaných a decentralizovaných prostrediach sú na riadenie prístupu používané autorizačné certifikáty. Navyše je možné delegovať práva uvedené v certifikáte iným používateľom. Autorizačný certifikát udeľuje entite prístupové práva. Entita potom môže prístupové práva vymenované v certifikáte delegovať ďalším používateľom (vrátane práva na ďalšie delegovanie) a takýmto spôsobom vytvoriť reťazec certifikátov. Reťazec certifikátov môže byť dlhý a môžu vznikať pri overovaní ťažkosti.

Implentovaný reťazcový certifikát zlepšuje časovú zložitosť verifikácie reťazca certifikátov. Implentovaný reťazcový certifikát (IChC) si môžeme predstaviť ako certifikát celého reťazca certifikátov. Verifikácia IChC vyžaduje iba konštantný počet kryptografických operácií, oproti klasickému overovaniu reťazca certifikátov (počet kryptografických operácií je úmerný počtu zreťazených certifikátov).

Na seminári bude stručne uvedená nova koncepcia certifikátov IChC s dôrazom na zlepšenie výkonnosti pri ich overovaní. A to nielen iba pre veľmi dlhé reťazce certifikátov, ale aj pre veľmi krátke, obsahujúce iba štyri zreťazené certifikáty je prístup IChC efektívnejší ako klasický prístup. Navyše budú v sieťach typu ad-hoc so sytémom ručiteľov ukázané všeobecné služby schémy IChC certifikátov a budú demonštrované vnútorné pohľady do konfigurovania takýchto bezpečnostných služieb.

Ilkovičova 3 812 19 Bratislava Tel.: 02/654 29 502 Fax: 02/654 20 587 lhudec@fiit.stuba.sk
http://www.fiit.stuba.sk