ERK'95

Portorož, Slovenija, 25. – 27. september 1995

Zbornik
četrte Elektrotehniške in računalniške konference ERK'95

Proceedings of the Fourth
Electrotechnical and Computer Science Conference ERK'95

Zvezek B / Volume B

Računalništvo in informatika / Computer and Information Science
Umetna inteligenca / Artificial Intelligence
Robotika / Robotics
Razpoznavanje vzorcev / Pattern Recognition
Biomedicinska tehnika / Biomedical Engineering
Numerične metode / Numberical Methods
Študentski članki / Student Papers

Uredila / Edited by
Franc Solina, Baldomir Zajc

Slovenska sekcija IEEE / Slovenia Section IEEE

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

621.3(063)

ELEKTROTEHNIŠKA in računalniška konferenca (4 ; 1995 ; Portorož)
Zbornik četrte Elektrotehniške in računalniške konference ERK '95, 25. - 27. september 1995, Portorož, Slovenija. Zv. B / uredila Franc Solina in Baldomir Zajc. - Ljubljana : Slovenska sekcija IEEE, 1995

Besedilo slov. ali angl. - Na vzpor. nasl. str.: Proceedings of the Fourth Electrotechnical and Computer Science Conference ERK '95. - Vsebina na nasl. str.: Računalništvo in informatika ; Umetna inteligenca ; Robotika ; Razpoznavanje vzorcev ; Biomedicinska tehnika ; Numerične metode ; Študentski članki

ISBN 961-6062-07-7

1. Solina, Franc 2. Zajc, Baldomir. - I. Electrotechnical and Computer Science Conference (4 ; 1995 ; Portorož) glej Elektrotehniška in računalniška konferenca (4 ; 1995 ; Portorož). - II. ERK '95 glej Elektrotehniška in računalniška konferenca (4 ; 1995 ; Portorož)
52745472

Pri organizaciji Elektrotehniške in računalniške konference ERK'95
so sodelovala naslednja društva:

Društvo avtomatikov Slovenije,
Slovensko društvo za merilno-procesno tehniko (ISEMEC 95),
SLOKO–CIGRE,
Društvo za medicinsko in biološko tehniko Slovenije,
Društvo robotikov Slovenije,
Slovensko društvo za umetno inteligenco,
Slovensko društvo za razpoznavanje vzorcev,
Slovensko društvo za simulacijo in modeliranje.

Organizacijo konference in izdajo zbornika je finančno podprlo Ministrstvo za znanost in tehnologijo Republike Slovenije

Sponzorji: SMARTCOM, Ljubljana
HERMES SoftLab, Ljubljana
PROCOM, Kranj

Slovenska sekcija IEEE
Fakulteta za elektrotehniko in računalništvo
Tržaška 25, 61001 Ljubljana, Slovenija

Tisk: SOMARU d.o.o., Ljubljana

Zbornik četrte Elektrotehniške in računalniške konference ERK'95

25.–27. september 1995

Portorož, Slovenija

Zvezek B

Računalništvo in informatika
Umetna inteligenca
Robotika
Razpoznavanje vzorcev
Biomedicinska tehnika
Numerične metode
Študentski članki

Uredila

Franc Solina in Baldomir Zajc

Slovenska sekcija IEEE

Ljubljana • Slovenija

Načrtovanje varnih računalniških sistemov

Marko Hrček, Primož Krajnik, Franc Solina
Fakulteta za elektrotehniko in računalništvo
Univerza v Ljubljani
Tržaška 25, 61001 Ljubljana, Slovenija
Marko.Hrcek@snet.fer.uni-lj.si

Designing of Secure Computer Systems

Security is becoming an essential requirement of information networks. Every day, all over the world, computer systems are being broken into. Computer systems are vulnerable to many threats which can inflict various types of damage resulting in significant losses. The philosophy of open systems often makes them insecure and vulnerable to unauthorized access. This document provides an overview of WAN and Internet security-related problems, suggested solutions, firewalling, user authentication and network modeling. It is designed to assist in understanding the nature of system and network-related security problems.

1. Uvod

Podatkovna revolucija je prinesla odprte računalniške sisteme. Komunikacija z računalniki ni več pogojena lokacijsko, mogoča je povezava iz oddaljenih krajev preko omrežja ali ustreznih klicnih linij. Odprtost je približala računalnike množicam uporabnikov, po drugi strani pa zagotavlja tudi precejšnjo mero anonimnosti. Filozofija odprtih sistemov predstavlja v tem smislu določene težave[1].

Danes so računalniški sistemi praviloma povezani v neko omrežje. Začne se s povezavo računalnika ali delovne postaje v lokalno računalniško omrežje. Povezave se širijo preko velikih razdalj v omrežja širšega obsega (WAN). Posledica medomrežnih povezovanj (internetworking) je veliko število uporabnikov, s tem pa se poveča tudi število vsiljivcev, ki si iz takšnih ali drugačnih razlogov prizadevajo nepoblaščeno vstopiti v računalniške sisteme. Škoda, ki jo pri tem povzročijo, je lahko precejšnja. Da bi zmanjšali ranljivost računalniških sistemov je zato potrebno sprejeti določene ukrepe in omejitve.

2. Ranljivost

Računalniški sistemi so se v preteklosti izkazali kot ranljivi. Napadom so podlegli celo dobro varovani sistemi vladnih in vojaških organizacij. Ranljivost je lahko posledica napak v programski opremi in varnostnih mehanizmih. Pri tem igra zelo pomembno vlogo človeški dejavnik.

Računalniške sisteme varujemo pred:

- uničenjem in namerno povzročeno škodo,
- zaporo strežbe (denial of service attacks),
- nelegitimno uporabo resursov s strani nepooblaščenih oseb.

Dejavniki ranljivosti v računalniških sistemih:

- ***vohunjenje in prisluškovanje*** - prenos podatkov med vozlišči medomrežnih povezav večinoma poteka v nešifrirani obliki. Na ta način je mogoče s pomočjo ustrezne programske in aparaturne opreme prisluškovati komunikacijskim kanalom (npr. izmenjavi elektronske pošte, podatkovnim prenosom in celo uporabniško vtipkanim geslom, ki v večini primerov nezavarovano potujejo preko omrežja);
- ***pomanjkanje politike varovanja*** - mnogo računalnikov je (pogosto nenamenoma) v omrežje povezano preveč odprto (npr. več mrežnih servisov kot je to potrebno). Pogosto ni izdelana politika varovanja za določen računalniški sistem, ni opredeljeno kaj storiti v določeni situaciji in kako ravnati v kritičnih trenutkih;
- ***zahtevna konfiguracija*** - upravljanje omrežja, sistemska administracija in konfiguracija sistemske programske opreme je, kljub prijaznim uporabniškim vmesnikom in zgledno dokumentacijo, zapleten proces ob katerem lahko hitro pride do neljubih napak;
- ***ranljivost TCP/IP servisov*** - komunikacijski protokol TCP/IP je bil razvit s ciljem, da se zgradi "mreža vseh mrež" (Internet). Internet povezuje več omrežij, kjer se poleg TCP/IP-ja uporabljajo še drugi protokoli. Vendar pa je prav TCP/IP najbolj razširjen, saj predstavlja osnovo porazdeljenih sistemov in odprtih sistemov nasploh. Hitra uveljavitev TCP/IP protokola je posledica koristnih osnovnih servisov, ki jih nudi uporabniku (prenos datotek, elektronska pošta, virtualni terminal, ipd). V zvezi z omenjenimi servisi se z varnostnega stališča pojavljajo določene težave. Problematični so lokalni mrežni servisi, kot so NIS, NFS, TFTP in t.i. r-servisi (servisi, ki omogočajo uporabo brez postopka avtorizacije npr. `rlogin`, `rsh`, ipd.). V

[1] Pojma varnost in odprtost se medsebojno izključujeta. Varni sistemi so praviloma zaprti, izmenjevanje informacij je otežkočeno. Primer zelo odprtega sistema je omrežje Internet, ki pa je z varnostnega stališča neobvladljivo, saj je enostavno preveliko.