

Florianópolis - SC, 5 e 6 de março de 2001

## **Anais do WSeg'2001**

**Workshop em Segurança de Sistemas Computacionais**

Evento integrante do

**SCTF'2001 - Simpósio de Computação Tolerante a Falhas**

O Wseg'2001 é uma promoção conjunta do

*Programa de Pós-Graduação em Informática Aplicada  
Pontifícia Universidade Católica do Paraná*

e do

*Departamento de Automação e Sistemas  
Universidade Federal de Santa Catarina*

Com o apoio da *SBC - Sociedade Brasileira de Computação*

## **Apresentação**

A segurança é uma característica essencial para o funcionamento confiável e robusto dos sistemas de informação, juntamente com os aspectos de tolerância a falhas e confiabilidade. O funcionamento de nossa sociedade depende de forma inegável e irreversível dos sistemas de informação. Um exemplo contundente dessa dependência é a realização de eleições totalmente informatizadas. A expansão explosiva da Internet, aliada à ampla cobertura da mídia sobre a ação de *crackers* e ataques de *vírus* e *worms*, leva a uma grande expectativa do público em relação à construção de sistemas seguros.

A segurança de sistemas computacionais é uma área de pesquisa científica e tecnológica em franca expansão atualmente, suscitando o surgimento de vários focos de debates, englobando diferentes grupos de pesquisas e temas específicos.

O WSeg'2001 - *Workshop em Segurança de Sistemas Computacionais* - realizado no contexto do IX SCTF - *Simpósio Brasileiro de Computação Tolerante a Falhas*, tem por principal objetivo atuar como um espaço para a apresentação de pesquisas e atividades relevantes na área de segurança de sistemas de informação, integrando a comunidade brasileira de pesquisadores e profissionais atuantes nessa área. A aceitação do evento surpreendeu os organizadores: foram submetidos 32 artigos, dos quais 19 foram selecionados para apresentação. É um ótimo resultado, sobretudo tratando-se de uma primeira edição.

Este evento tem o apoio da Sociedade Brasileira de Computação (SBC) e está sendo organizado pelo Programa de Pós-Graduação em Informática Aplicada da Pontifícia Universidade Católica do Paraná (PUCPR) e pelo Departamento de Automação e Sistemas (DAS) da Universidade Federal de Santa Catarina (UFSC). Ficam aqui registrados nossos agradecimentos a todos aqueles que contribuíram para sua realização.

Prof. Carlos Maziero (PPGIA/PUCPR)

Em nome das comissões de Programa e de Organização do Wseg'2001

## **Comissão de Programa**

Adriano Mauro Cansian	UNESP
Carla Merkle Westphall	LCMI/UFSC
Carlos Maziero	PPGIA/PUCPR, Coordenador
Carlos Westphall	INE/UFSC
Clovis Torres Fernandes	IEC/ITA
Edgard Jamhour	PPGIA/PUCPR
Edson Moreira	ICMC/USP
Elias Duarte Jr	DI/UFPR
Joni Fraga	DAS/UFSC
Michael Stanton	IC/UFF
Noemi Rodriguez	DI/PUC-Rio
Paulo Lício de Geus	IC/Unicamp
Raul Weber	INF/UFRGS
Ricardo Dahab	IC/Unicamp

## **Comissão Organizadora**

Carlos Maziero	PPGIA/PUCPR, Coordenador
Frank Siqueira	DAS/UFSC
Joni Fraga	DAS/UFSC
Lau Cheuk Lung	DAS/UFSC
Mauro Borchardt	PPGIA/PUCPR

## **Revisores dos artigos**

Adriano Mauro Cansian	Antônio José dos Santos Brandão
Carla Merkle Westphall	Carlos B. Westphall
Carlos Maziero	Clovis Torres Fernandes
Diego de Assis Fernandes	Edgard Jamhour
Edson Moreira	Eduardo Souza Machado da Silva
Elias P. Duarte Jr	Francisco Figueiredo
Francisco Gomes Milagres	Jansen Carlo Sena
Joni Fraga	Luis M. Cáceres Alvarez
Marcello Milanez	Marcelo Abdalla dos Reis
Mauro Borchardt	Mauro César Bernardes
Michael Stanton	Michelle Silva Wangham
Noemi Rodriguez	Paulo Lício de Geus
Rafael Rodrigues Obelheiro	Raul Weber
Ricardo Dahab	Wagner T. Watanabe

## Conteúdo

### Criptografia

- pág *Incorporação de Certificados SPKI/SDSI ao Protocolo SSL*  
Cristian Ferreira de Souza / Luiz Antônio da Frota Mattos  
UnB - Universidade de Brasília
- pág *Substituição Homofônica utilizando Códigos de Huffman Canônicos*  
José Rodrigues Fernandes , Ruy Luiz Milidiú , Claudio Gomes de Mello  
Universidade Católica de Petrópolis (UCP), Pontifícia Universidade Católica  
(PUC-Rio), Instituto Militar de Engenharia (IME)
- pág *Uma proposta para avaliação de criptossistemas implementados em software baseados em curvas elípticas*  
Arnaldo Jorge de Almeida Jr. Marco Aurélio Amaral Henriques  
Universidade Estadual de Campinas - UNICAMP

### Detecção de intrusão

- pág *Um Sistema de Detecção de Intrusão projetado para usuário final*  
André Fischer e Vinicius G. Ribeiro  
UNILASALLE e UFRGS/UNILASALLE/ULBRA
- pág *O Sistema de Detecção de Intrusão Asgaard*  
Rafael Saldanha Campello, Raul Fernando Weber, Vinicius da Silveira  
Serafim, Vinicius Gadis Ribeiro  
Instituto de Informática, PPGC, Universidade Federal do Rio Grande do Sul
- pág *Verificação da integridade de arquivos no kernel do sistema operacional*  
Mauro Borchardt, Carlos Maziero  
Programa de Pós-Graduação em Informática Aplicada - PUCPR

### Firewalls

- pág *Intelligent Sentinell Agent*  
Eduardo Leiva Correa  
PUC/RS
- pág *Um Linux Reduzido para Sistema de Firewall*  
José de Ribamar Braga Pinheiro Júnior, Sidy Ould Ehmety  
Universidade Federal do Maranhão
- pág *Acesso remoto em firewalls e topologia para gateways VPN*  
Francisco José Candeias Figueiredo, Paulo Lício de Geus  
Universidade Estadual de Campinas - UNICAMP
- pág *Certificação de Firewalls*  
Daniel Ribeiro Brahm, Sandro Antônio Fernandes, João Avelino Bellomo Filho  
Universidade Católica de Pelotas

## **Segurança em Comércio Eletrônico**

- pág *Segurança em Aplicações de Comércio Eletrônico Baseadas em Agentes Móveis*  
Daniel Rodrigues Ambrosio, MSc. Mauro César Bernardes, Stênio Firmino Pereira Filho e Dr.Edson dos Santos Moreira Universidade de São Paulo

## **Segurança em sistemas eleitorais**

- pág *Critérios para Avaliação da Segurança do Voto Eletrônico*  
Amílcar Brunazo Filho  
Diretor Técnico da TD Tecnologia Digital Ltda
- pág *Auditoria de Sistemas Eleitorais: o Caso São Domingos*  
Evandro Luiz de Oliveira , Cláudio Andrade Rego  
Centro Federal de Educação Tecnológica de Minas Gerais - CEFET-MG
- pág *Forense Computacional: Aspectos legais e Padronização*  
Célio Cardoso Guimarães, Flávio de Souza Oliveira, Marcelo Abdalla dos Reis, Paulo Lício de Geus  
Universidade Estadual de Campinas - UNICAMP

## **Autenticação e autorização**

- pág *Beyond Parasitic Authentication*  
Lucas de Carvalho Ferreira , Ricardo Dahab  
IC/Unicamp e Webmind Inc
- pág *Autorização e controle de acesso para o prontuário eletrônico do paciente em ambientes abertos e distribuídos: uma proposta de modelo e arquitetura*  
Gustavo H. M. B. Motta, Sérgio S. Furuie, Fabiane B. Nardon, Marco A.Gutierrez e Marcos Yamaguti  
Instituto do Coração, Hospital das Clínicas, Faculdade de Medicina da USP

## **Ferramentas e técnicas**

- pág *Dolt4Me: a tool for automating administrative tasks on Windows NT networks*  
Alessandro Augusto, Célio Guimarães, Paulo Lício de Geus  
Universidade Estadual de Campinas - UNICAMP
- pág *SCOM: Scan de Portas de Comunicação Remotas*  
Stéphany Moraes Martins Cláudio de Castro Monteiro  
ULBRA - Universidade Luterana do Brasil
- pág *Aplicando Ataques de Dicionário no protocolo Kerberos do Windows 2000*  
Marcus Cunha Granado  
Instituto de Computação - UNICAMP