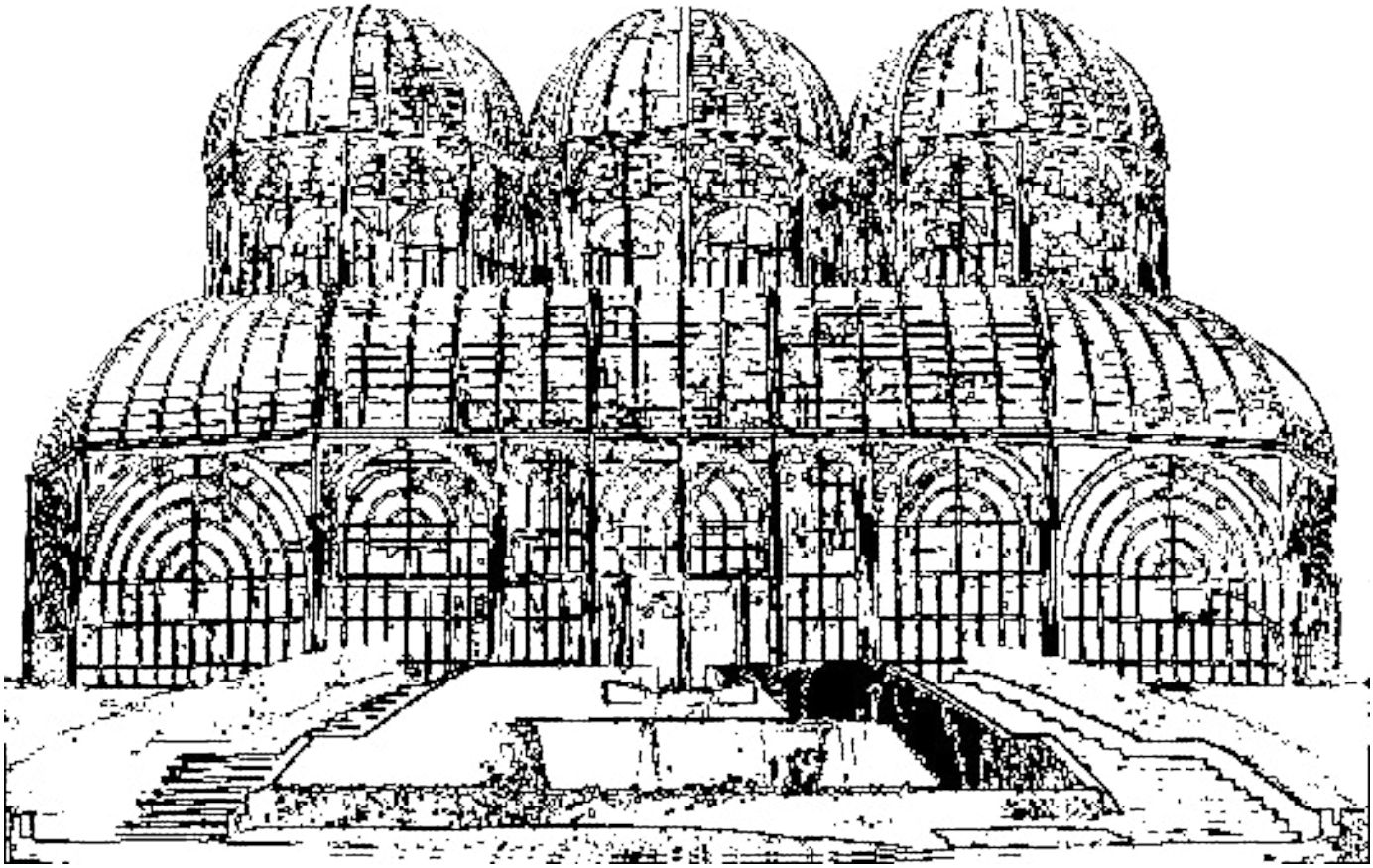


# SBSeg 2012 • Curitiba PR

XII Simpósio Brasileiro em Segurança da Informação
e de Sistemas Computacionais

Curitiba PR – 19 a 22 de Novembro de 2012
Centro de Convenções – Hotel Pestana

Organização
*Pontifícia Universidade Católica do Paraná – PUCPR*
*Universidade Federal do Paraná – UFPR*
*Universidade Tecnológica Federal do Paraná – UTFPR*

Promoção
*Sociedade Brasileira de Computação – SBC*

# Boas-vindas!

Sejam todos bem-vindos ao SBSeg 2012! Nesta 12ª edição, o simpósio conta com uma ampla gama de atividades. Além das sessões técnicas de apresentação de 28 artigos de pesquisa, serão ministrados 4 minicursos em tópicos recentes na área, duas palestras e dois tutoriais proferidos por especialistas internacionais, além da segunda edição do Concurso de Teses e Dissertações em Segurança (CTDSeg), que é realizado a cada dois anos. Também ocorrerão três workshops: a sexta edição do Workshop de Trabalhos de Iniciação Científica e de Graduação (WTICG), a segunda edição do Workshop de Gestão de Identidades Digitais (WGID), e o Workshop de Forense Computacional (WFC), que acontecerá pela primeira vez.

Desejamos a todos os participantes do SBSeg uma semana proveitosa e muito agradável. Aproveitem bem o simpósio e sua estadia em Curitiba!

Aldri dos Santos, UFPR
Altair Santin, PUCPR
Carlos Maziero, UTFPR
Coordenadores Gerais do SBSeg 2012

# Quadro Geral de Programação

<table>
<tr><th></th><th colspan="3">Seg 19/11/2012</th><th colspan="2">Ter 20/11/2012</th><th colspan="2">Qua 21/11/2012</th><th colspan="3">Qui 22/11/2012</th></tr>
<tr><td>08:00-08:30</td><td colspan="3">inscrições</td><td colspan="2">inscrições</td><td colspan="2">inscrições</td><td colspan="3">inscrições</td></tr>
<tr><td>08:30-10:00</td><td>MC1</td><td>WTICG</td><td>CTD</td><td>ST1</td><td>ST2</td><td>ST5</td><td>ST6</td><td>WFC</td><td>WGID</td><td>MC3</td></tr>
<tr><td>10:00-10:30</td><td colspan="3">coffee-break</td><td colspan="2">coffee-break</td><td colspan="2">coffee-break</td><td colspan="3">coffee-break</td></tr>
<tr><td>10:30-11:30</td><td rowspan="2">MC1</td><td rowspan="2">WTICG</td><td rowspan="2">CTD</td><td rowspan="2" colspan="2">PI1</td><td colspan="2">TI2</td><td rowspan="2">WFC</td><td rowspan="2">WGID</td><td rowspan="2">MC3</td></tr>
<tr><td>11:30-12:30</td><td colspan="2">PN2</td></tr>
<tr><td>12:30-14:30</td><td colspan="3">almoço</td><td colspan="2">almoço</td><td colspan="2">almoço</td><td colspan="3">almoço</td></tr>
<tr><td>14:30-15:15</td><td rowspan="2">MC2</td><td rowspan="2">WTICG</td><td rowspan="2">CTD</td><td colspan="2">TI1</td><td rowspan="2">ST7</td><td rowspan="2">ST8</td><td rowspan="2">WFC</td><td rowspan="2">WGID</td><td rowspan="2">MC4</td></tr>
<tr><td>15:15-16:00</td><td colspan="2">PN1</td></tr>
<tr><td>16:00-16:30</td><td colspan="3">coffee-break</td><td colspan="2">coffee-break</td><td colspan="2">coffee-break</td><td colspan="3">coffee-break</td></tr>
<tr><td>16:30-17:30</td><td rowspan="2">MC2</td><td rowspan="2">WTICG</td><td rowspan="2">CTD</td><td>ST3</td><td rowspan="2">AC</td><td rowspan="2" colspan="2">PI2</td><td rowspan="2">WFC</td><td rowspan="2">WGID</td><td rowspan="2">MC4</td></tr>
<tr><td>17:30-18:30</td><td>ST4</td></tr>
<tr><td>18:30-19:00</td><td colspan="3"></td><td colspan="2"></td><td colspan="2" rowspan="2"></td><td colspan="3" rowspan="3"></td></tr>
<tr><td>19:00-19:30</td><td colspan="3">Abertura</td><td colspan="2" rowspan="2">Reunião CESeg/SBC</td></tr>
<tr><td>19:30-21:00</td><td colspan="3">Coquetel</td><td colspan="2" rowspan="2">Jantar do Evento</td></tr>
<tr><td>21:00-23:00</td><td colspan="3"></td><td colspan="2"></td></tr>
</table>

**Legenda:**

- **WTICG** Workshop de Trabalhos de Iniciação Científica e de Graduação
- **WGID** Workshop de Gestão de Identidades Digitais
- **WFC** Workshop de Forense Computacional
- **CTD** Concurso de Teses e Dissertações em Segurança
- **MC*** Minicursos
- **ST*** Sessões técnicas SBSeg (artigos completos)
- **AC** Sessão técnica SBSeg (artigos curtos)
- **PI***, **PN*** Palestras Internacionais e Nacionais
- **TI*** Tutoriais Internacionais

## 19/11 Segunda-feira - Monday

# WTICG – Workshop de Trabalhos de Iniciação Científica e de Graduação (sala DC2)

[08:30-10:00] WTICG Sessão Técnica 1: Privacidade e Segurança em dispositivos móveis

- Uma estratégia para gerenciar o compartilhamento de recursos entre dispositivos móveis.
  *T. Bono, L. Martimiano (UEM)*
  *A intensificação do uso das redes sem fio tem elevado a quantidade de recursos que podem ser compartilhados entre os dispositivos móveis e, consequentemente, provocado um aumento do consumo dos recursos desses dispositivos. Assim, torna-se importante desenvolver uma estratégia que defina quais recursos devem ser compartilhados entre os usuários, considerando restrições de acesso às informações confidenciais e a capacidade do dispositivo, mantendo-o disponível para o usuário. Uma solução proposta para este cenário é a ontologia denominada PrOHand (Privacy Ontology for Handovers). Este artigo descreve a PrOHand, seu sistema de reputação e a aplicação desenvolvida para validar suas regras.*

- Computação distribuída com preservação de privacidade. *L. Pena, O. Coelho, J. Graaf (UFMG)*
  *Computação distribuída com preservação de privacidade se refere aos protocolos criptográficos utilizados para que duas partes se unam e realizem uma tarefa em comum. Este tipo de protocolo é muito importante para preservar a segurança em data mining e cloud computing, entre outros. Este artigo apresenta duas propostas de protocolos nessa área, uma para o cálculo do produto escalar de dois vetores e outra para a comparação de inteiros, ambas de forma segura e com preservação da privacidade das partes. Estas propostas foram estudadas e implementadas durante a execução do nosso trabalho de iniciação científica no Departamento de Ciência da Computação da UFM*

- Senhas descartáveis em dispositivos móveis para ambientes de Telemedicina.
  *T. Idalino, D. Spagnuelo (UFSC)*
  *Este trabalho é parte de um projeto que está sendo desenvolvido no Laboratório de segurança em Computação [LabSEC] da Universidade Federal de Santa Catarina [UFSC] em parceria com o Laboratório de Informática Médica e Telemedicina [LabTelemed] financiado pela Financiadora de Estudos e Projetos [FINEP]. Tem como objetivo implantar o uso de senhas descartáveis na Rede Catarinense de Telemedicina, através de uma versão melhorada do Google Authenticator e do uso do ASI-HSM como servidor de autenticação. Para a implantação na Telemedicina, propõe-se o uso de um serviço de autenticação desenvolvido também no LabSEC para abstrair a camada do HSM.*

[10:30-12:30] WTICG Sessão Técnica 2: Algoritmos, Protocolos e Técnicas Criptográficas

- Modelagem e verificação formal de aspectos de tempo real do protocolo Kerberos.
  *B. Cremonezi, G. Pinto (UFJF)*
  *O protocolo de autenticação Kerberos utiliza timestamps dentro de mensagens criptografadas para prevenir ataques do tipo replay, permitindo que um servidor de aplicação possa distinguir mensagens novas de antigas. Assim, a disponibilidade do serviço se torna dependente dos tempos de cifragem e decifragem, e do acúmulo de mensagens no servidor. Neste trabalho, utilizamos o formalismo de Autômatos Temporizados e a ferramenta UPPAAL para modelar estes aspectos de tempo real do Kerberos. A modelagem permitiu a identificação de uma alteração no protocolo que o torna menos dependente daqueles fatores, aumentando a disponibilidade do serviço em situações onde muitos clientes tentam utilizar o servidor em um período curto de tempo.*

- Análise e implementação de um método para prover integridade a sistemas de banco de dados.
  *G. Becker, L. Perin, A. Silvério (UFSC), M. Carlos (Univ. London), R. Custódio (UFSC)*
  *Modificações não autorizadas a sistemas de banco de dados podem causar prejuízos para pessoas e organizações, sendo de extrema importância a garantia de sigilo e integridade a tais sistemas. Geralmente as aplicações utilizam os recursos disponibilizados por Sistemas Gerenciadores de Banco de Dados (SGBDs) para assegurar o sigilo e a integridade dos dados armazenados no SGBD. Entretanto, os SGBDs que provêm os recursos necessários para garantir o sigilo e a integridade dos dados possuem um custo muito elevado, muitas vezes inviável para organizações de médio e pequeno porte. Este trabalho analisa e implementa um método de verificação de integridade de dados, baseado no uso de Hash-based Message Authentication Code (HMAC), independente de SGBD. Os testes realizados mostram a eficiência do método. Em média, a sobrecarga de processamento para o cálculo e verificação do HMAC para um registro do banco de dados não ultrapassa 100% do tempo de execução de determinada operação.*

- Um protocolo criptográfico para controle de medicamentos.
  *B. Imhof, E. Santos, R. Custódio (UFSC)*
  *A falsificação de medicamentos é um problema em todo o mundo, e para resolver a rastreabilidade deste problema, o Governo Federal instituiu o Sistema Nacional de Controle de Medicamentos. A implantação completa deste novo modelo logístico, faz com que indústria, comércio e governo, precisem se adequar tecnologicamente, gerando demanda de ferramentas que consigam trabalhar de forma concomitante os aspectos de segurança da informação. A*

*contribuição deste trabalho é a formalização de um protocolo criptográfico que tem por objetivo garantir a integridade, autenticação e sigilo das informações referentes ao rastreamento dos medicamentos no Brasil.*

- Adaptações em um HSM para homologação na ICP-Brasil.
  *C. Cardozo, G. Welter, C. Dettoni Jr, A. Bereza Jr, R. Custódio (UFSC)*
  *A confiabilidade de uma ICP depende da segurança de suas chaves privadas. O HSM é um dispositivo que gerencia e protege chaves criptográficas, próprio para guardar as chaves privadas de uma ICP. HSMs também são utilizados em ICPs brasileiras. Para que um HSM possa guardar chaves privadas da ICP-Brasil, o dispositivo deve ser homologado pela ICP-Brasil. Este artigo descreve um conjunto de adaptações necessárias para que um HSM possa ser homologado na ICP-Brasil.*

[14:30-16:00] WTICG Sessão Técnica 3: Segurança em Sistemas

- Detecção de phishing em páginas Web utilizando técnicas de aprendizagem de máquina.
  *F. Cunha, E. Santos, E. Souto (UFAM)*
  *Este trabalho de pesquisa teve como objetivo desenvolver mecanismos para a detecção de phishing em páginas web. O phishing é uma forma de fraude eletrônica em que o criminoso, passando-se por uma entidade legítima, tenta convencer suas vítimas a fornecerem informações confidenciais como nomes de usuários e senhas. Foram utilizadas três técnicas de aprendizagem de máquina para realizar o processo de classificação: SVM, KNN e Regressão Logística. Durante o processo de pesquisa foram identificadas doze características que evidenciam a diferença entre páginas phishing e páginas legítimas. O classificador SVM obteve a maior taxa de acertos com 95,60%.*

- Desenvolvimento de roteiros laboratoriais de segurança computacional em ambientes virtualizados.
  *R. Ferreira, C. Westphall (UFSC)*
  *A segurança computacional é um fator fundamental para o bom funcionamento e sucesso das aplicações. Um treinamento de qualidade torna- se cada vez mais necessário para formar profissionais capacitados no cenário atual. Tendo em vista a presente dificuldade para a realização de aulas práticas de segurança computacional devido às limitações da infraestrutura disposta pelos ambientes acadêmicos, este trabalho propõe o uso de roteiros em ambiente virtual para a realização das atividades práticas de segurança, sem comprometer as instalações das máquinas físicas e o aprendizado do aluno devido a limitações de acesso.*

- CURUPIRA: uma solução para controle dos pais em navegadores Web.
  *D. Azulay, H. Cunha, E. Feitosa (UFAM)*
  *Este trabalho de pesquisa visa desenvolver uma solução de Parental Control para navegadores Web. Soluções de Parental Control (traduzindo do inglês, controle dos pais) tem como objetivo filtrar conteúdo, moderar o uso e controlar as atividades em qualquer ambiente que possa oferecer algum tipo de risco a algum usuário (especialmente crianças e adolescentes). Focando na segurança na Internet, as soluções de Parental Control são de suma importância para os pais poderem controlar e monitorar o acesso de seus filhos e também filtrar as informações que chegam aos mesmos. Utilizando técnicas de filtragem, aliada a uma interface de configuração simples e intuitiva, a solução proposta, denominada CURUPIRA, irá monitorar e controlar o acesso a Internet, de acordo com a definição de pais e responsáveis, evitando que crianças e/ou adolescentes sejam expostos a conteúdos considerados impróprios.*

[17:00-18:00] WTICG Sessão Técnica 4: Premiação e Encerramento do Workshop

## CTDSeg – Concurso de Teses e Dissertações em Segurança (sala DC3)

[09:00-10:00] CTDSeg – Teses de Doutorado

- Implementação eficiente em software de curvas elípticas e emparelhamentos bilineares.
  *D. Aranha (UnB), J. Hernandez (UNICAMP)*
  *O advento da criptografia assimétrica ou de chave pública possibilitou a aplicação de criptografia na forma de assinaturas digitais e comércio eletrônico. Dentre os vários métodos de criptografia assimétrica, a Criptografia de Curvas Elípticas destaca-se pelos baixos requisitos de armazenamento e custo computacional para execução. A descoberta relativamente recente da criptografia baseada em emparelhamentos bilineares permitiu ainda sua flexibilização e a construção de sistemas criptográficos com propriedades inovadoras. Porém, o custo computacional de sistemas baseados em emparelhamentos ainda permanece significativamente superior aos tradicionais, representando um obstáculo para sua adoção, especialmente em dispositivos com recursos limitados. As contribuições deste trabalho objetivaram aprimorar o desempenho de sistemas baseados em curvas elípticas e emparelhamentos bilineares e consistem em formulação e implementação eficientes de aritmética em corpos finitos em diversas plataformas computacionais; técnicas algorítmicas seriais e paralelas para aritmética em curvas elípticas e cálculo de emparelhamentos de interesse criptográfico. Estas contribuições permitiram obter significativos ganhos de desempenho e uma série de recordes de velocidade para o cálculo de diversos algoritmos criptográficos relevantes em arquiteturas modernas que vão de sistemas embarcados de 8 bits a processadores com 8 cores.*

- Criptografia de chave pública sem certificado. *D. Goya, R. Terada (USP)*
  *A criptografia de chave pública sem certificado (certificateless) é uma alternativa ao modelo convencional de criptografia assimétrica, pois a autenticação da chave pública ocorre implicitamente durante a execução dos protocolos, sem a necessidade de gerenciamento e distribuição de certificados digitais. Neste resumo de tese de doutorado, modelos formais de segurança para acordo de chave com autenticação sem certificado são aprimorados visando dois objetivos paralelos: (1) aumentar o nível de confiança que usuários podem depositar na autoridade geradora de chaves secretas parciais e (2) viabilizar protocolos que sejam eficientes computacionalmente e com propriedades de segurança relevantes. Para atestar que as melhorias efetuadas são praticáveis e possibilitam que os objetivos sejam alcançados, novos protocolos são propostos e provados seguros.*

[10:30-11:30] CTDSeg – Teses de Doutorado

- An orchestration approach for unwanted Internet Traffic identification.
  *E. Feitosa (UFAM), D. Sadok (UFPE)*
  *Current Internet traffic shows a varying mix of relevant and unwanted traffic. The latter is increasingly becoming harmful to network performance and service availability, while often taking up scarce precious network and processing resources. This paper presents some definitions of definitions of unwanted traffic and an approach to identify unwanted traffic based on orchestration. There are basically two main contributions to our work. First, we show that multiple specialized security modules benefit from an integrated and coordinated flow process. We also present a solution that generates new rules and produces inferences with a greater degree of certainty than the uncertainty generated by existing anomaly detectors. As proof of concept, we implement a prototype showing the effectiveness and accuracy of our proposal.*

- Análise de políticas de controle de acesso baseado em papéis com rede de Petri colorida.
  *E. Ueda, W. Ruggiero (USP)*
  *Controle de acesso é um tópico de pesquisa importante tanto para a academia quanto para a indústria. Controle de Acesso Baseado em Papéis (CABP) foi desenvolvido no início dos anos 1990, tornando-se um padrão generalizado para controle de acesso em vários produtos e soluções computacionais. Embora modelos CABP sejam largamente aceitos e adotados, ainda existem questões para responder. Um dos principais desafios de pesquisa em segurança baseada em papéis é determinar se uma política de controle de acesso é consistente em um ambiente altamente dinâmico. Nossa pesquisa visa preencher essa lacuna fornecendo um método para analisar políticas CABP com respeito a dois aspectos significativos: segurança e dinamismo envolvendo papéis, ações e objetos. Para este propósito, desenvolvemos um modelo de descrição e simulação de política usando rede de Petri colorida e CPN Tools. O modelo descreve e é capaz de simular vários estados CABP em um contexto de educação online típico. Usando este modelo, foi possível analisar o espaço de estados produzido pela rede de Petri colorida em um cenário dinâmico envolvendo a criação de novos papéis, ações e objetos. O resultado da análise de alcançabilidade da rede de Petri da política demonstrou que é possível verificar a consistência de políticas de controle de acesso considerando a dinamicidade de papéis, ações e objetos, e apontou vantagens de aplicabilidade da modelagem de políticas de segurança em ambientes distribuídos utilizando rede de Petri colorida.*

[11:30-12:30] CTDSeg – Reunião do comitê de avaliação

[14:30-16:00] CTDSeg – Dissertações de Mestrado

- Segurança do bit menos significativo no RSA e em curvas elípticas.
  *D. Nakamura, R. Terada (USP)*
  *Na dissertação são apresentados algoritmos que conseguem inverter criptossistemas como o RSA fazendo uso de oráculos que predizem o LSB. Fizemos a implementação de dois desses algoritmos, identificamos parâmetros críticos e mudamos a amostragem do formato original. Com a modificação na amostragem conseguimos uma melhora nos tempos de execução. Nossos resultados indicam que não é válida a equivalência do nível de segurança comumente aceita de RSA-1024 = ECC-160.*

- Um esquema bio-inspirado para tolerância a má-conduta em sistemas de quórum apoiando serviços em MANETs. *E. Mannes, M. Nogueira, A. Santos (UFPR)*
  *Os serviços de operação de rede em MANETs, como localização de recursos e distribuição de informações de conectividade, devem ser confiáveis para oferecer apoio às aplicações. A confiabilidade e a disponibilidade desses serviços podem ser obtidas por meio de técnicas de gerência de dados, como a replicação por sistemas de quórum. Entretanto, os sistemas de quórum são vulneráveis a nós de má-conduta que intencionalmente não colaboram com as operações de replicação ou divulgam dados falsos a fim de prejudicar o funcionamento da rede. Para lidar com esses problemas, nós propomos e avaliamos um esquema bio-inspirado para a tolerância de nós egoístas e maliciosos em operações de replicação nos sistemas de quórum. Diferente de abordagens existentes, este esquema, chamado de QS2, é autônomo, distribuído e não requer o uso de mensagens extras. O QS2 foi aplicado diante de cenários realísticos de MANETs, e os resultados mostram que o QS2 provê uma confiabilidade dos dados acima de 90% mesmo diante de nós egoístas e maliciosos.*

- Assinatura digital Rabin-Williams sem randomização e com prova eficiente de segurança.
  *B. Magri, R. Terada (USP)*
  *Com o surgimento da criptografia de chave pública, muito esforço foi feito para a criação de protocolos de assinatura que fossem seguros contra indivíduos maliciosos. A família de protocolos de assinatura Rabin possui os recordes de velocidade de verificação da assinatura, chegando a ser até 100 vezes mais rápida do que o RSA. Este trabalho apresenta uma redução eficiente de segurança para uma variante do protocolo de assinatura Rabin descrito por Bernstein, onde não é necessário o uso de nenhuma função para geração de bits pseudo-aleatórios, o que torna o protocolo mais robusto. A redução apresentada é uma redução polinomial e eficiente do problema da fatoração de inteiros para o problema de quebrar o protocolo Principal Rabin-Williams B = 0.*

[16:30-17:30] CTDSeg – Dissertações de Mestrado

- Protocolos de acordo de chaves baseados em emparelhamentos para dispositivos móveis.
  *C. Okida, R. Terada (USP)*
  *Neste trabalho é descrito uma implementação em software, utilizando Criptografia de curvas elípticas e baseada em emparelhamentos bilineares para dispositivos móveis. Este trabalho possui foco na construção de um mecanismo provedor de segurança e integridade das informações sigilosas dos dados dos prontuários médicos trafegados em um canal inseguro. Utilizou-se um protocolo de acordo de chaves sem certificado mutuamente autenticado, sobre as curvas BN para atingir o nível de segurança desejado. Dentre as contribuições deste trabalho estão uma biblioteca escrita na linguagem Java para a implementação deste sistema e a implementação dos protocolos e do próprio sistema de segurança para os dispositivos móveis.*

- Mineração de dados para detecção de fraudes em transações eletrônicas.
  *J. Felipe Jr, W. Meira Jr. (UFMG)*
  *Com a popularização da Web, cresce o número de pessoas que a utilizam para realizar negócios e transações financeiras. Entretanto, essa popularização atrai a atenção de criminosos, aumentando o número de fraudes nesse cenário. As perdas financeiras chegam a bilhões de dólares por ano. Este trabalho propõe uma metodologia para detecção de fraude em pagamentos online baseado no processo de descoberta do conhecimento. Para avaliação, foi definido o conceito de eficiência econômica e aplicado em um conjunto de dados real de uma das maiores empresas latino-americanas de serviço de pagamentos eletrônicos. Os resultados mostram excelente desempenho na detecção de fraudes, com ganhos de até 46,46% em relação ao cenário atual da empresa.*

[17:30-18:30] CTDSeg – Reunião do comitê de avaliação

## Minicursos (sala DC1)

[08:30-10:00] e [10:30-12:30] Minicurso 1:

- Análise de vulnerabilidades em sistemas computacionais modernos: conceitos, exploits e proteções.
  *M. Ferreira, T. Rocha, G. Martins, E. Feitosa, E. Souto (UFAM).*
  *O crescimento da ocorrência de ataques cibernéticos tem elevado o interesse da comunidade científica e os investimentos de organizações na busca por novas soluções que sejam capazes de lidar com essas técnicas de invasão de sistemas computacionais. Entre essas técnicas, o desenvolvimento de exploits vem sendo destacado por diversos autores como uma das principais armas dos atacantes nas últimas décadas. Por esse motivo, o desenvolvimento desses artefatos tem sido incorporado também por analistas de segurança às metodologias de testes de penetração, como estratégia para prevenção de ataques, contribuindo para a pesquisa de novos mecanismos de defesa. Este capítulo fornece subsídios para o entendimento das técnicas de desenvolvimento de exploits e o seu emprego na construção de artefatos maliciosos efetivos no comprometimento de sistemas computacionais.*

[14:30-16:00] e [16:30-18:30] Minicurso 2:

- Introdução à segurança de dispositivos móveis modernos – um estudo de caso em Android.
  *A. Braga, E. Nascimento, L. Palma, R. Rosa (CpqD)*
  *Os dispositivos móveis, em particular os smartphones e os tablets, são os protagonistas de uma revolução silenciosa, caracterizada pelo uso de dispositivos com grande poder de processamento e conectividade em ambientes públicos e privados. A agregação de tais características à ampla difusão de dispositivos móveis trouxe uma série de ameaças, tornando necessário um estudo de novas técnicas e ferramentas de segurança. Este curso tem a finalidade de esclarecer estes assuntos, abordando os aspectos de segurança da informação relacionados aos dispositivos móveis modernos, exibindo ameaças e vulnerabilidades nesta temática, em particular na plataforma Android.*

**[19:00-19:30] Abertura Oficial do Simpósio (salas DC2+3)**

**[19:30-21:00] Coquetel de Abertura (Espaço Cultural David Carneiro)**

## 20/11 Terça-feira - Tuesday

## SBSeg – Sessões Técnicas

[08:30-10:00] Sessão Técnica 1: Virtualização (sala DC1+2)

- Redes virtuais seguras: uma nova abordagem de mapeamento para proteger contra ataques de disrupção na rede física.
  *R. Oliveira, L. Bays, D. Marcon, M. Neves, L. Buriol, L. Gaspary (UFRGS)*
  *Na virtualização de redes, roteadores e enlaces virtuais são alocados sobre uma infraestrutura de rede física. Tal característica representa uma vulnerabilidade a ataques de negação de serviço na rede física, visto que um único dispositivo físico comprometido afeta todos os virtuais sobrepostos. Trabalhos anteriores propõem a reserva de recursos sobressalentes. Apesar de funcional, esse tipo de solução agrega custo ao provedor da rede física. Neste artigo, propõe-se uma abordagem para alocação de redes virtuais que explora o compromisso entre a resiliência a ataques e a eficiência na utilização de recursos. A abordagem é separada em duas estratégias, uma preventiva e uma reativa. A primeira aloca enlaces virtuais em múltiplos caminhos do substrato, enquanto a segunda tenta recuperar a capacidade dos enlaces virtuais afetada por um ataque de negação de serviço subjacente. Ambas as estratégias são formuladas como problemas de otimização. Resultados numéricos demonstram o nível de resiliência a ataques propiciado pela abordagem e o baixo custo decorrente da mesma.*

- Um modelo para mapeamento ótimo de redes virtuais com requisitos de segurança.
  *L. Bays, R. Oliveira, L. Buriol, M. Barcellos, L. Gaspary (UFRGS)*
  *A virtualização de redes permite a criação de múltiplas instâncias de redes virtuais sobre uma única infraestrutura física. Devido à sua ampla aplicabilidade, tal técnica tem atraído grande interesse tanto de pesquisadores quanto de empresas importantes do segmento de redes de computadores. Apesar de esforços recentes (motivados principalmente pela busca de mecanismos para viabilizar a avaliação de propostas na temática Internet do Futuro) terem contribuído substancialmente para a materialização do conceito, nenhum preocupou-se em conciliar alocação eficiente de recursos e satisfação de requisitos de segurança (ex: confidencialidade). Ressalta-se que, no contexto de redes virtuais, a proteção de infraestruturas de rede compartilhadas constitui condição fundamental para seu uso em larga escala. Para abordar o referido problema, neste artigo propõe-se um modelo de alocação de redes virtuais que busca satisfazer o nível especificado de segurança e, ao mesmo tempo, otimizar a utilização dos recursos físicos. Os resultados obtidos demonstram que o modelo é capaz de alocar redes virtuais a um substrato físico de forma correta e ótima, minimizando custos de largura de banda para provedores de infraestrutura.*

- Uma arquitetura para auditoria de nível de serviço para computação em nuvem.
  *J. Bachtold, A. Santin, M. Stihler, A. Marcon Jr., E. Viegas (PUCPR)*
  *Este artigo apresenta uma arquitetura para auditoria multipartes de acordo de serviço (SLA) em computação em nuvem. São auditados o provedor de IaaS, contratante de IaaS (provedor de SaaS) e cliente de SaaS. O objetivo é auditar problemas internos e externos ao ambiente de nuvem de modo incontestável pelas partes. A proposta emprega inspetores (agentes de coleta para auditoria) e auditores independentes (terceiros), capazes de identificar desvios de SLA através de informações coletadas nos ambientes das partes. Os resultados mostram que é possível auditar e diagnosticar problemas na nuvem combinando informações das partes, com a autoria independente, inclusive evitando-se conflito de interesse dos inspetores.*

[08:30-10:00] Sessão Técnica 2: Criptografia e PKI (1) (sala DC3)

- Aprimoramento de esquema de identificação baseado no problema MQ.
  *F. Monteiro, D. Goya, R. Terada (USP)*
  *O problema MQ, que consiste em resolver um sistema de equações polinomiais multivariáveis quadráticas sobre um corpo finito, tem atraído a atenção de pesquisadores para o desenvolvimento de sistemas criptográficos de chave pública por ser (1) NP-completo, (2) não ter algoritmo conhecido de tempo polinomial para sua solução nem mesmo no modelo computacional quântico e (3) viabilizar primitivas criptográficas de interesse prático. Em 2011, Sakumoto, Shirai e Hiwatari apresentaram dois novos protocolos de identificação de conhecimento-zero baseados exclusivamente no problema MQ. O protocolo em 3 passos de Sakumoto et al. apresenta probabilidade de personificação de 2/3 em uma rodada. No presente artigo é proposto um protocolo aprimorado que reduz essa probabilidade para 1/2. O resultado é um protocolo que diminui a comunicação total necessária e requer um número menor de iterações para o mesmo nível de segurança.*

- Chi-square attacks on Block-Cipher based compression functions.
  *D. Freitas (UFSC), J. Nakahara Jr*
  *In this paper, we report on χ2 analyses of block-cipher based (cryptographic) compression functions. Our aim is not to find collisions nor (second) preimages, but to detect non-random properties that may distinguish a compression function from an ideal primitive such as a random oracle. We study some well-known single-block modes of operation*

*such as Davies-Meyer (DM), Matyas-Meyer-Oseas (MMO) and Miyaguchi-Preneel (MP), and double-block modes such as Hirose's, Tandem-DM, Abreast-DM, Parallel-DM and MDC-2. This paper shows how a weakness (χ2 correlation) in the underlying block cipher can propagate to the compression function via the mode of operation used in hash constructions. To demonstrate our ideas, we instantiated the block cipher underlying these modes with variable-round RC5, RC6 and ERC6 block ciphers.*

- Impossible-Differential attacks on block-cipher based hash and compression functions using 3D and Whirlpool. *D. Freitas (UFSC), J. Nakahara Jr*
  *In this paper, we analyze block-cipher-based hash functions, which means hash functions that use block ciphers as compression functions in a mode of operation, such as Davies-Meyer (DM), Matyas-Meyer-Oseas (MMO) and Miyaguchi-Preneel (MP), for instance. We use impossible differentials (ID) to distinguish the compression (or hash) function from an ideal primitive (a random oracle) by detecting a nonrandom behavior. We applied an ID analysis to an 8-round variant of the 3D block cipher used in MMO mode, as a compression function of a hypothetical hash function. This attack effectively improves upon the previously known distinguishing ID attacks on reduced-round 3D. We can also attack a hash function using 3D as compression function in DM mode. Finally, we attacked the compression function in Whirlpool with a 5-round W cipher in MP mode with 2^100 time and 2^64 memory.*

**[10:30-12:30] PI1 – Palestra Internacional 1 (sala DC1+2)**

Internet Monitoring via DNS Traffic Analysis . *Wenke Lee (Georgia Institute of Technology ).*
*In recent years miscreants have been leveraging the Domain Name System (DNS) to build Internet-scale malicious network infrastructures for malware command and control (C&C). In talk, I will describe our DNS traffic analysis work that aims to identify the C&C domains and hence the infected hosts, and gain insights into malware operations. First, I will describe Kopis, a system that passively monitors DNS traffic at the upper levels of the DNS hierarchy, analyzes global DNS query resolution patterns, and identifies domains likely associated with malware activities. Kopis has high detection rates (e.g., 98.4%) and low false positive rates (e.g., 0.3% or 0.5%). In addition, Kopis is able to detect new malware domains days or even weeks before they appear in public blacklists and security forums. For example, it discovered the rise of a previously unknown DDoS botnet based in China in 2010. Second, I will present a study of the DNS infrastructure used by mobile apps. Using traffic ob tained from a major US cellular provider as well as a major US non-cellular Internet service provider, we identified the DNS domains looked up by mobile apps, and analyzed information related to the Internet hosts pointed to by these domains. We found that the DNS infrastructure used by mobile apps is part of the infrastructure used by applications in non-cellular world; in other words, the mobile web is part of the Internet. We saw evidence that the criminals behind mobile malware may be the same as those behind botnets and malware in non-cellular world: about 48,098 hosts known to be associated with malicious activities are also pointed to by unknown (likely malicious) domains looked up by mobile apps. We found that the network characteristics of major, widespread mobile threats are very similar to those of non-cellular botnets. These findings that malicious mobile apps and non-cellular malware have commonalities in DNS infrastructure and network characteristics, and therefore, we should develop a DNS monitoring and reputation system for cellular carriers similar to the ones already developed for non-cellular ISPs.*

**[14:30-15:15] TI1 – Tutorial Internacional 1 (sala DC1+2)**

Internet Monitoring via DNS Traffic Analysis. *Wenke Lee (Georgia Institute of Technology).*
*In recent years miscreants have been leveraging the Domain Name System (DNS) to build Internet-scale malicious network infrastructures for malware command and control (C&C). In talk, I will describe our DNS traffic analysis work that aims to identify the C&C domains and hence the infected hosts, and gain insights into malware operations. First, I will describe Kopis, a system that passively monitors DNS traffic at the upper levels of the DNS hierarchy, analyzes global DNS query resolution patterns, and identifies domains likely associated with malware activities. Kopis has high detection rates (e.g., 98.4%) and low false positive rates (e.g., 0.3% or 0.5%). In addition, Kopis is able to detect new malware domains days or even weeks before they appear in public blacklists and security forums. For example, it discovered the rise of a previously unknown DDoS botnet based in China in 2010. Second, I will present a study of the DNS infrastructure used by mobile apps. Using traffic obtained from a major US cellular provider as well as a major US non-cellular Internet service provider, we identified the DNS domains looked up by mobile apps, and analyzed information related to the Internet hosts pointed to by these domains. We found that the DNS infrastructure used by mobile apps is part of the infrastructure used by applications in non-cellular world; in other words, the mobile web is part of the Internet. We saw evidence that the criminals behind mobile malware may be the same as those behind botnets and malware in non-cellular world: about 48,098 hosts known to be associated with malicious activities are also pointed to by unknown (likely malicious) domains looked up by mobile apps. We found that the network characteristics of major, widespread mobile threats are very similar to those of non-cellular botnets. These findings that malicious mobile apps and non-cellular malware have commonalit ies in DNS infrastructure and network characteristics, and therefore, we should develop a DNS monitoring and reputation system for cellular carriers similar to the ones already developed for non-cellular ISPs.*

**[15:15-16:00] PN1 – Palestra Nacional 1 (sala DC1+2)**

- Segurança em redes IPv6. *Antonio M. Moreiras (NIC.BR)*
  A migração do IPv4 para o IPv6 é uma realidade na Internet. Esta apresentação abordará de forma pragmática e realista as implicações relacionadas à segurança, nas redes IPv6. Existem muitos mitos em relação ao IPv6 ser mais seguro. A ausência de NAT e uma viabilidade melhor para o uso do IPSEC são exemplos de avanços que não devem ser desconsiderados. No entanto, também há vulnerabilidades: algumas comuns ao universo do IPv4, outras novas. No final, o nível de segurança obtido é basicamente o mesmo, com vulnerabilidades e técnicas de proteção similares, mas com diferenças que devem ser conhecidas e levadas em consideração.

[16:30-17:30] Sessão Técnica 3: Detecção e Prevenção de Ataques e Vulnerabilidades (1) (sala DC1+2)

- SDA-COG Sistema de detecção de ataques para rede de rádios cognitivos.
  *J. Filho (UFRJ), L. Rust, R. Machado (Inmetro), L. Pirmez (UFRJ)*
  *Este trabalho descreve um Sistema de Detecção de Ataques (SDA) para redes de rádios cognitivos a partir da integração dos métodos de detecção por Localização e por Reputação. O sistema é validado através de simulações que avaliam o desempenho do mesmo face aos ataques específicos de emulação do usuário primário (Primary User Emulation - PUE) e falso diagnóstico do sensoriamento do espectro (Sense Spectrum False Feedback - SSFF).*

- Detecção de variações de malware metamórfico por meio de normalização de código e identificação de subfluxos.
  *M. Cozzolino (DPF-Brasil), G. Martins (FUCAPI), E. Souto (UFAM), F. Deus (UnB)*
  *Este artigo apresenta uma metodologia capaz de identificar malware metamórficos. O código de um arquivo é submetido a um processo de normalização e subdividido em trechos de códigos (tokens) delimitados por mudanças de fluxo do programa. A combinação do identificador de cada token com os dois seguintes cria um conjunto de identificadores de fluxo, que são usados para medir a similaridades com um código de malware previamente mapeado. Os resultados obtidos mostram que a metodologia proposta é capaz de identificar com precisão a presença de códigos metamórficos.*

[17:30-18:30] Sessão Técnica 4: Criminalística (sala DC1+2)

- Identificação de autoria de documentos eletrônicos.
  *W. Oliveira Jr, E. Justino (PUCPR), L. Oliveira (UFPR)*
  *Entre as demandas das perícias forenses está a identificação da autoria de documentos eletrônicos. Compressores de dados e a Distância Normalizada de Compressão (NCD) são ferramentas que auxiliam o perito a executar esta tarefa. Estudou-se o desempenho destas ferramentas em uma base de dados com 3000 documentos eletrônicos em português, de 100 diferentes autores, e foram obtidas taxas médias de acerto superiores a 70%, indicando que esta técnica é promissora. Verificou-se, também, a influência da quantidade de documentos de treinamento no desempenho desta técnica.*

- Modelagem de aliciamento de menores em mensagens instantâneas de texto.
  *P. Santin, C. Freitas, E. Paraiso, A. Santin (PUCPR)*
  *As abordagens existentes na literatura não são modeladas para detecção do aliciamento sexual de menores, mas apenas fazem a descoberta do estágio de aliciamento numa comunicação entre o agressor e sua vítima. Além disto, mostram baixa eficiência em função do emprego de um perfil único para a descoberta dos estágios. Este artigo considera a descoberta dos estágios de aliciamento com o perfil do agressor e da vítima separadamente. Esta abordagem, baseada em avaliação estocástica (i.e. HMM), visa a modelagem individual de cada perfil para aumentar a eficiência da detecção. Os experimentos mostram taxas de acerto promissoras com resultados próximos a 91%.*

[16:30-18:30] Sessão Técnica de Artigos Curtos (sala DC3)

- Um modelo de segurança e privacidade para redes sociais móveis aplicadas à área da saúde.
  *J. Gonçalves, A. Teles, F. Silva (UFMA)*
  *Redes Sociais Móveis (RSM) consistem de uma estrutura social cujos membros se relacionam em grupos e a interação é feita através de dispositivos de computação portáteis com acesso a tecnologias de comunicação sem fio. Na área da saúde e possível aplicar o conceito de RSM para conduzir ações colaborativas relacionadas ao tratamento de pacientes e sua educação. Recentemente muitos middlewares para RSM foram propostos. Entretanto, os atuais middlewares de RSM estão em um estágio preliminar em relação a atender requisitos de segurança e privacidade. Esses últimos se tornam indispensáveis quando dados sensíveis são compartilhados, tais como em aplicações para saúde, onde os perfis dos pacientes e suas informações médicas são manipuladas. Este artigo apresenta um modelo de segurança e privacidade desenvolvido para aplicações de RSM focadas no domínio da saúde.*

- Identity management requirements in future Internet.
  *J. Torres (Univ. Paris 6), R. Macedo, M. Nogueira (UFPR), G. Pujolle (Univ. Paris 6)*
  *The characteristics of the Future Internet and the emerging technologies result in new requirements, in which user security issues are highlighted. Identity Management requirements are linked to the development of systems able to prevent unauthorized use of digital identities, information overload, and to enhance user privacy. This paper highlights the Identity Management requirements in Future Internet context, based on its characteristics. Security and privacy were identified as key factors since they determine the overall trustworthiness of a system in terms of confidentiality, integrity and availability. Further, we introduce a discussion, in which we present the relationship between the Identity Management requirements and a future Internet scenario.*

- IPSFlow – uma proposta de IPS distribuído para captura e bloqueio seletivo de tráfego malicioso em redes definidas por software. *F. Nagahama, F. Farias (UFPA), E. Aguiar (Univ Amazônia/SERPRO), E. Cerqueira, A. Abelém (UFPA), L. Gaspary (UFRGS)*
  *Os tradicionais sistemas de prevenção de intrusão (Intrusion Prevention Systems – IPS) possuem limitações em sua atuação. Quando operam no modo ativo, não possuem uma ampla cobertura na rede, e quando capturam tráfego espelhado, só bloqueiam o tráfego malicioso se atuarem em conjunto com equipamentos de rede do mesmo fabricante ou solução. Neste contexto, propomos neste artigo o IPSFlow, um framework de IPS para Redes Definidas por Software (Software Defined Networks - SDN) que, através do protocolo Openflow, possibilita a criação de um IPS com ampla cobertura na rede, permitindo a captura seletiva e o bloqueio automatizado de tráfego malicioso o mais próximo de sua origem, através da combinação dos resultados de diferentes técnicas de análise de tráfego.*

- Avaliação do classificador Artmap Fuzzy em redes 802.11 com criptografia pré-RSN (WEP e WPA).
  *N. Araújo (UFMT), R. Oliveira (IFMT), A. Shinoda (UNESP), E. Ferreira, V Nascimento (IFMT)*
  *Nos últimos anos têm-se percebido um forte crescimento no uso da tecnologia sem fio 802.11 (Wireless LAN) e os mecanismos de segurança implementados pelas emendas IEEE 802.11i e IEEE 802.11w têm se mostrado pouco eficazes no combate a ataques contra a disponibilidade dos serviços da WLAN. Neste artigo avalia-se o desempenho do classificador ARTMAP Fuzzy na detecção de um grupo de ataques de negação de serviço (DoS) numa rede WLAN real com suporte a criptografia WEP e WPA. A rede neural ARTMAP Fuzzy foi escolhida pela sua capacidade de preservar o conhecimento anteriormente adquirido e adaptar-se a novos padrões de classificação. Os resultados obtidos demonstram que há a necessidade de uma metaheurística para fornecer parâmetros mais confiáveis para a execução do classificador e a seleção de atributos mais representativos do comportamento intrusivo existente nos ataques de DoS.*

- Arquitetura de sistema integrado de defesa cibernética para detecção de botnets.
  *S. Cardoso, R. Salles (IME-RJ)*
  *Este trabalho tem por objetivo apresentar uma proposta de arquitetura para um sistema de defesa cibernética capaz de detectar bots e bloquear a comunicação entre os bots e as botnets. também é proposto um algoritmo de detecção de bots baseado em grafos de relacionamento. Foram realizados experimentos por meio da análise de registros de consultas DNS com o objetivo de encontrar máquinas suspeitas de serem zumbis. Resultados preliminares mostram que os mecanismos empregados permitem filtrar os registros de DNS e identificar máquinas suspeitas de pertencerem a uma botnet.*

- Uma arquitetura para mitigar ataques DDoS em Serviços Web sob nuvem.
  *C. Menegazzo (UDESC), F. Bernardelli, F. Gielow, N. Pari, A. Santos (UFPR)*
  *Ataques de Distributed Denial of Service (DDoS) frequentemente são negligenciados por representarem apenas uma interrupção temporária no funcionamento normal de um sistema. Com o advento de paradigmas como a cloud, a mitigação deste tipo de ameaça com o acréscimo de recursos para as aplicações se torna viável, mas acarreta em um problema denominado economic DDoS. Este artigo apresenta uma proposta de arquitetura para a mitigação de ataques DDoS direcionados a uma aplicação hospedada em uma cloud. Tal arquitetura é baseada na instanciação de uma réplica da aplicação - operação simples em uma cloud - e no redirecionamento apenas de requisições legítimas a esta réplica. A arquitetura proposta não precisa identificar os clientes atacantes e, ainda assim, consegue filtrar apenas o tráfego legítimo sem a carga e possíveis erros decorrentes da necessidade de identificação.*

**[19:00-21:00] Reunião da Comissão Especial em Segurança da SBC (aberta aos sócios da SBC) (sala DC1+2)**

## 21/11 Quarta-feira - Wednesday

## SBSeg – Sessões Técnicas

[08:30-10:00] Sessão Técnica 5: Criptografia e PKI (2) (sala DC1+2)

- Segurança do bit menos significativo no RSA e em curvas elípticas.
  *D. Nakamura, R. Terada (USP)*
  *A segurança do bit menos significativo da chave secreta no Diffie- Hellman sobre Curvas Elípticas (e da mensagem no RSA) está relacionada à segurança de toda a chave (mensagem). Neste artigo são apresentados algoritmos que conseguem inverter os criptossistemas citados fazendo uso de oráculos que predizem o LSB. Fazemos a implementação de dois desses algoritmos, identificamos parâmetros críticos e mudamos a amostragem do formato original. Com a modificação na amostragem conseguimos uma melhora nos tempos de execução.*

- Universally composable committed oblivious transfer with a trusted initializer.
  *A. Pinto, A. Nascimento, B. David (UnB), J. Graaf (UFMG)*
  *Committed Oblivious Transfer (COT) is a two-party primitive that combines one-out-of-two oblivious transfer with bit commitment. In the beginning of COT, a sender is committed to bits b0 ,b1 and a receiver to a choice bit c. In the end, the receiver is committed to bc without learning anything about b1−c , while the sender learns nothing about c. This primitive implies secure multi-party computation assuming that a broadcast channel is available. In this paper, we introduce the first universally composable unconditionally secure committed oblivious transfer protocol based on a Trusted Initializer (TI), which pre-distributes data to the parties. Our protocol builds on simple bit commitment and oblivious transfer protocols, using XOR commitments to prove simple relations in zero-knowledge. Besides providing very high security guarantees, our protocols are significantly simpler and more efficient than previous results, since they rely on pre-computed operations distributed by the TI.*

- Cleaning up the PKI for long-term signatures.
  *M. Vigil (Tech Univ Darmstadt), R. Custódio (UFSC)*
  *In this paper we present a new approach for the conventional X.509 Public Key Infrastructures (PKI). Our goal is to reduce the effort to handle signatures in the long term. The novelty is that a Root CA reissues subordinate certificates of final users, but adjusting validity periods to exclude the periods after a revocation. The Root CA also authenticates timestamps. The result is the cleaned PKI, which is simpler than the conventional PKI because: a) there is no revocation; b) there is no intermediary Certification Authority; c) signatures are trustworthy as long as the used cryptographic algorithms remain secure. As benefits, we reduce the need of timestamps and consequently the demand for storage space and processing time to use signed documents.*

[08:30-10:00] Sessão Técnica 6: Mitigação e Tolerância a Ataques (sala DC3)

- Mitigando ataques de egoísmo e negação de serviço em nuvens via agrupamento de aplicações.
  *D. Marcon, M. Neves, R. Oliveira, L. Buriol, L. Gaspary, M. Barcellos (UFRGS)*
  *Na computação em nuvem, locatários consomem, sob demanda, recursos de hardware e software oferecidos por um provedor remoto. Entretanto, o compartilhamento da rede interna da nuvem por todos os locatários, aliado à falta de isolamento entre fluxos de dados decorrente do uso dos protocolos TCP e UDP, possibilita a ocorrência de ataques de egoísmo e negação de serviço. Os algoritmos de alocação atuais não impedem que a disponibilidade dos recursos de rede seja afetada por ataques. Este artigo propõe uma estratégia para a alocação de aplicações de locatários que visa mitigar o impacto de ataques de egoísmo e negação de serviço na rede interna da nuvem. A ideia chave, inédita na literatura científica, consiste no agrupamento de aplicações em infraestruturas virtuais considerando níveis de confiança mútua entre os locatários. Resultados de avaliações demonstram que a estratégia proposta é capaz de oferecer proteção contra ataques de egoísmo e negação de serviço com pouco ou nenhum custo extra.*

- Um esquema cooperativo para análise da presença de ataques EUP em redes ad hoc de rádio cognitivo. *J. Soto, S. Queiroz, M. Nogueira (UFPR)*
  *Nas redes ad hoc de rádio cognitivo, os usuários mal intencionados podem tirar proveito das funcionalidades da tecnologia de rádio cognitivo para realizar ataques de emulação de usuário primário (EUP). Nestes ataques, os usuários mal intencionados imitam as características dos usuários licenciados, visando obter prioridade no uso das bandas de radiofrequências licenciadas e ameaçando o funcionamento da rede. A fim de tratar deste problema, trabalhos na literatura utilizam critérios específicos para detecção de ataques EUP. Tais soluções, contudo, não consideram conjuntamente o uso de múltiplos e diferentes critérios que enriquecem o consenso de inferência sobre a presença de um ataque EUP na rede. Diante deste contexto, este trabalho apresenta INCA, um esquema de múltiplos critérios para análise cooperativa da presença de ataques EUP em redes ad hoc de rádio cognitivo. O esquema INCA é composto por duas fases. Na primeira, cada usuário não licenciado emprega múltiplos critérios para definir uma hipótese individual da presença dos ataques EUP. Na segunda, essas hipóteses são trocadas entre os seus vizinhos e cada usuário não licenciado calcula a probabilidade final da presença de um ataque EUP através do teorema de*

*Bayes. Os resultados de simulação mostram a melhoria e a eficácia da cooperatividade e do uso de múltiplos critérios quando aplicados simultaneamente.*

- Usando criptografia de limiar para tolerar clientes maliciosos em memória compartilhada dinâmica.
  *E. Alchieri (UnB), A. Bessani (Univ. Lisboa), J. Fraga (UFSC)*
  *Sistemas de quóruns Bizantinos são ferramentas usadas na implementação consistente e confiável de sistemas de armazenamento de dados em presença de falhas arbitrárias. Vários protocolos para implementação destes sistemas foram propostos para ambientes estáticos e, mais recentemente, também surgiram propostas de protocolos para ambientes dinâmicos. Um dos desafios na implementação desses sistemas em ambientes dinâmicos está na reconfiguração do conjunto de servidores devido a entradas e saídas arbitrárias de processos. Este trabalho vai além e apresenta protocolos que toleram a presença de clientes maliciosos em sistemas de quóruns Bizantinos dinâmicos, através do emprego de um mecanismo de criptografia de limiar que fornece a flexibilidade suficiente para operação nestes ambientes. Este mecanismo é utilizado para controlar as ações que clientes maliciosos podem executar contra o sistema. além disso, todos os protocolos apresentados são para sistemas assíncronos, não necessitando de nenhuma premissa temporal sobre o comportamento do sistema.*

**[10:30-11:30] TI2 – Tutorial Internacional 2 (sala DC1+2)**

Delivering New Platform Technologies. *George Cox (Intel Corporation).*
*Dreaming up a new technology is just the first of many steps in getting the technology developed, making it deployable, delivering it broadly into the market place, getting it widely enabled, and having it be effectively used. In this talk, we discuss this the various steps required to successfully carry out such a process using Intel's new RdRand/DRNG technology as an example.*

**[11:30-12:30] PN2 – Palestra Nacional 2 (sala DC1+2)**

Computação Forense: Pesquisas Atuais e Perspectivas.
*Itamar de Almeida Carvalho, Polícia Federal do Brasil.*
*A apresentação traz os principais desafios encontrados no trabalho dos peritos criminais, um panorama geral das pesquisas realizadas recentemente por estes profissionais e alguns desafios da área da Computação Forense.*

[14:30-16:00] Sessão Técnica 7: Segurança Baseada em Hardware e Controle de Acesso (sala DC1+2)

- A secure relay protocol for door access control.
  *H. Hüttel, E. Wognsen, M. Follin, M. Calverley, H. Karlsen, B. Thomsen (Aalborg University)*
  *Physical keys are easy to use but difficult to manage securely for large institutions. Digital replacements have been created, but dedicated hardware such as smartcards or RFID tags can have the same problems as physical keys. Several commercial products try to solve this by using the users' Bluetooth-enabled mobile devices as keys, but the built-in security of the Bluetooth standard is insufficient. Furthermore, to manage a varying set of users, such systems may require the door locks to be connected to the Internet which may require expensive infrastructure. We present a cryptographic protocol and a prototype implementation that solves these problems by letting door locks communicate with a central server using the Internet connections of the users' mobile devices. The protocol is specified formally in the applied π-calculus and security through secrecy and authenticity is verified using the cryptographic protocol verifier ProVerif. A prototype of the system is implemented for Android smartphones.*

- Modified Current Mask Generation (M-CMG): an improved countermeasure against differential power analysis attacks.
  *D. Mesquita (UFU), H. Besrour, M. Mohsen, T. Rached (Monastir University)*
  *It has been demonstrated that encryption device leaks some information, which can be exploited by various attacks such as differential power analysis (DPA). To protect an Advanced Encryption Standard (AES) implementation from DPA without any modification of the cryptographic algorithm, we can use the Current Masking Generation (CMG). The CMG countermeasure consists of stabilizing the power consumption, but it presents some limitations concerning temperature variations and the Early effect. The goal of this paper is to update the CMG to address these problems, evolving to the Modified-Current Masking Generation (M-CMG).*

- Uma arquitetura de segurança para medidores inteligentes – verificação prática de dados de energia multitarifada. *S. Câmara (UFRJ), R. Machado (Inmetro), L. Pirmez (UFRJ), L. Rust (Inmetro)*
  *Medidores de energia elétrica tornaram-se equipamentos complexos, por outro lado, seu correto funcionamento ainda e questionável e o esforço envolvido na aprovação de novos modelos aumentou imensamente. Objetivando estabelecer confiança no medidor inteligente, este artigo propõe uma arquitetura de segurança baseada em um autenticador de consumo. Este autenticador é gerado por um dispositivo seguro, localizado no módulo de medição, usando o esquema ECPVS. Nossa abordagem considera diferentes cenários de energia multitarifada e apresenta três técnicas de composição da mensagem contida no autenticador. Nossas preocupações incluem o tamanho total desta mensagem e os dados necessários para validação do consumo em cada faixa de preço.*

[14:30-16:00] Sessão Técnica 8: Detecção e Prevenção de Ataques e Vulnerabilidades (2) (sala DC3)

- Avaliação da sensibilidade de preditores de suavização exponencial na detecção de ataques de inundação. *N. Silva, R. Salles (IME)*
  *Este artigo analisa a sensibilidade de preditores de suavização exponencial usados para detectar ataques distribuídos de negação de serviço (DDoS). Comparou-se a capacidade de detecção de dois preditores (EWMA e Holt-Winters) com diferentes configurações e cenários. Foi verificado o desempenho através das taxas de falsos positivos e falsos negativos gerados. Foi inserido ataques em traces reais do MAWILab e em amostras reais de tráfego de backbone da RNP com o intuito de realizar simulações de ataques com diferentes volumes de inundação. As simulações mostram que a otimização de parâmetros dos preditores trazem melhores resultados.*

- Análise de métodos de aprendizagem de máquina para detecção automática de spam hosts. *R. Silva (UNICAMP), T. Almeida (UFSCar), A. Yamakami (UNICAMP).*
  *Web spamming é um dos principais problemas que afeta a qualidade das ferramentas de busca. O número de páginas web que usam esta técnica para conseguir melhores posições nos resultados de busca é cada vez maior. A principal motivação são os lucros obtidos com o mercado de publicidade online, além de ataques a usuários da Internet por meio de malwares, que roubam informações para facilitar roubos bancários. Diante disso, esse trabalho apresenta uma análise de técnicas de aprendizagem de máquina aplicadas na detecção de spam hosts. Experimentos realizados com uma base de dados real, pública e de grande porte indicam que as técnicas de agregação de métodos baseados em árvores são promissoras na tarefa de detecção de spam hosts.*

- Dynamic detection of address leaks. *G. Quadros, R. Martins, F. Pereira (UFMG)*
  *An address leak is a software vulnerability that allows an adversary to discover where a program is loaded in memory. Although seemingly harmless, this information gives the adversary the means to circumvent two widespread protection mechanisms: Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP). In this paper we show, via an example, how to explore an address leak to take control of a remote server running on an operating system protected by ASLR and DEP. We then present a code instrumentation framework that hinders address disclosure at runtime. Finally, we use a static analysis to prove that parts of the program do not need to be instrumented; hence, reducing the instrumentation overhead. We claim in this paper that the combination of the static and dynamic analyses provide us with a reliable and practical way to secure software against address leaks.*

**[16:30-18:30] PI2 – Palestra Internacional 2 (sala DC1+2)**

Solving The Platform Entropy Problem. *George Cox (Intel Corporation)*.
*This talk will present the need for entropy in Cryptography and the problem of generating adequate streams in hardware, highlighting some recent attacks to software-based implementations. I go on with TRNG, a breakthrough that made a hardware implementation viable, and present DRNG, Intel's implementation available through the RdRand instruction, and how the module can be embedded on processor designs. Finally, I also show performance results in terms of throughput, response time and reseed frequency.*

**[19:30-23:00] Jantar do Simpósio (Churrascaria Batel Grill, Av. Nossa Sra. Aparecida, 84)**

## 22/11 Quinta-feira - Thursday

## WFC – Workshop de Forense Computacional (sala DC1)

[08:30-09:00] Palestra: Paulo Batimarchi - IFIP – *International Federation on Intellectual Property* (Latin America) – São Paulo – SP

[09:00-10:00] WFC Sessão Técnica 1

- Metodologia para análise forense de imagens digitais utilizando sensor pattern noise.
  *A. Nascimento, L. Torres, V. Ramos, J. Alencar-Neto (RASTRU)*
  *Este artigo propõe uma metodologia baseada no princípio da divisibilidade do problema em análise forense. A proposta tem como foco delinear um fluxo de trabalho para os experimentos utilizando o Sensor Pattern Noise no uso forense. A metodologia possui três etapas: (i) Aquisição e Armazenamento das Imagens, (ii) Extração de Atributos e (iii) Processo de Decisão. Na primeira etapa propomos um modelo entidade-relacional para este fim. Em seguida, foram levantadas as principais técnicas de extração de atributos. A terceira etapa refere-se aos métodos de decisão e classificação largamente utilizados. Por fim, apresentamos as considerações finais e próximos passos.*

- Além do óbvio: a análise forense de imagens e a investigação do conteúdo implícito e explícito de fotografias digitais. *T. Carvalho, E. Silva, F. Costa, A. Ferreira, A. Rocha (UNICAMP)*
  *Atualmente, torna-se cada vez mais comum a utilização de ferramentas para manipulação de imagens e vídeos. Tais ferramentas facilitam a criação de alterações em documentos, enganando a percepção de observadores quanto a semântica desses documentos. Apesar de existirem alterações consideradas inocentes (como uma correção de brilho), existem aquelas consideradas maliciosas como, por exemplo, operações de cópia e colagem e composição. Neste trabalho, discutimos os principais desafios tratados no cenário forense de autenticação de documentos digitais como imagens e vídeos, bem como as nossas mais recentes contribuições nesse contexto.*

[10:30-11:00] Palestra: Demetrius Gonzaga, Delegado de crimes virtuais de Curitiba (NUCIBER PR)

[11:00-12:00] WFC Sessão Técnica 2

- Identificação da origem de imagens com zoom utilizando sensor pattern noise. *L. Torres (RASTRU, UFAL), A. Nascimento, V. Ramos, J. Alencar-Neto (RASTRU), A. Frery (UFAL)*
  *Este artigo apresenta uma abordagem para identificar o dispositivo de origem de imagens com zoom através do Sensor Pattern Noise. O padrão de cada câmera é obtido com a extração do ruído residual de n-imagens, sobre os quais são aplicados operadores estatísticos, média e mediana, para a obtenção da respectiva fingerprint. Um limiar adaptativo é obtido a partir da correlação de m-imagens de treinamento, oriundas da mesma câmera investigada, com as fingerprints. Por fim, validamos a proposta aplicando a mesma correlação entre a imagem investigada e a fingerprint de cada câmera, concluindo que tal imagem pertence a uma dada câmera caso o coeficiente de variação esteja entre os limiares definidos para o dispositivo. Os resultados desta abordagem foram satisfatórios, tendo sido obtida uma acurácia de 100% na maioria dos casos discutidos neste artigo.*

- Content-based filtering for video sharing social networks. *E. Valle (UNICAMP), S. Avila, F. Souza (UFMG), M. Coelho (UFMG, EPCAR), A. Araújo (UFMG)*
  *In this paper we compare the use of several features in the task of content filtering for video social networks, a very challenging task, not only because the unwanted content is related to very high-level semantic concepts (e.g., pornography, violence, etc.) but also because videos from social networks are extremely assorted, limiting the use of a priori information. We propose a simple method, able to combine diverse evidence, coming from different features and various video elements (entire video, shots, frames, keyframes, etc.). We evaluate our method in two social network applications, related to the detection of unwanted content — pornographic videos and violent videos. Using challenging test databases, we show that this simple scheme is able to obtain good results, provided that adequate features are chosen. Moreover, we establish the use of spatiotemporal local descriptors as critical to the success of the method in both applications.*

[12:00-12:30] Palestra: Angelo Volpi – Tabelião do 7º. Tabelionato Volpi em Curitiba – PR

[14:30-15:00] Palestra: Leandro Bissoli – Escritório Patrícia Peck Pinheiro – Advogados Especialistas em Direito Digital – São Paulo – SP

[15:00-16:00] Apresentações técnicas – Instituto Nacional de Criminalística – Departamento de Policia Federal – Brasília – DF

[16:30-17:00] WFC Sessão Técnica 3

- Identificação de autoria offline em documentos manuscritos.
  *A. Amaral (CESUMAR), C. Freitas (PUCPR), F. Bortolozzi (CESUMAR)*
  *O objetivo deste trabalho é apresentar o estado da arte relacionado à identificação de autoria offline em documentos manuscritos. Para tanto, foram analisados os seguintes elementos de cada abordagem estudada: granularidade e características extraídas para o processo de identificação, base utilizada para validação dos experimentos de identificação, algoritmo de classificação utilizado e taxa de reconhecimento. Pode-se observar que abordagens que utilizam características texturais (em nível de documento) apresentam taxas muito elevadas, no entanto exigem um alto poder computacional. Enquanto que as abordagens que realizam manipulação direta, ou seja, pixel a pixel da imagem, exigem menos recursos computacionais, mas possuem taxas de acerto com valores reduzidos.*

[17:00-17:30] Palestra: Luiz Rodrigo Grochocki - Perito Oficial Criminal da Polícia Científica do Estado do Paraná – Setor de Computação Forense

[17:30-18:00] WFC Sessão Técnica 4:

- Aplicação de observação de pessoas em computação forense. *W. Schwartz (UFMG)*
  *Um dos principais objetivos do monitoramento automático de ambientes é a extração de informações a respeito de atividades desempenhadas pelos humanos de modo a detectar interações entre agentes e identificar padrões de comportamentos que sejam suspeitos. Para que as atividades sejam analisadas, um conjunto de problemas, tais como detecção e identificação dos agentes na cena, rastreamento ao longo do tempo, possivelmente entre câmeras distintas, reconhecimento de ações individuais, precisa ser resolvido. Tais problemas compõem o domínio de aplicações denominado observação de pessoas, responsável pela análise de imagens e vídeos contendo humanos. Este trabalho descreve os conceitos do domínio de observação de pessoas, discute seus desafios e visa estabelecer algumas relações entre problemas deste domínio com a área de computação forense. Finalmente, abordagens escaláveis para o problema de reconhecimento de faces e reidentificação de pessoas serão apresentadas.*

[18:00-18:30] Mesa Redonda

## WGID – Workshop de Gestão de Identidades Digitais (sala DC2)

[08:30] Abertura

[08:30-10:00] Sessão Técnica de Artigos Convidados

- Um survey sobre ferramentas para single sign-on. *H. Nogueira, D. Santos, R. Custódio (UFSC)*
  *Existem muitas ferramentas de gestão de identidades que permitem o Single Sign-On (SSO) e o agrupamento de provedores de identidades e serviços na forma de federações. Este trabalho descreve e compara algumas dessas ferramentas. As ferramentas que fizeram parte do estudo foram: OAuth, CoSign, OpenID, OneLogin, OpenAM, JOSSO, WebAuth, CAS e BrowserID. O estudo comparativo foi resultado do trabalho feito por um grupo de alunos do curso de Ciência da Computação da Universidade Federal de Santa Catarina (UFSC) no primeiro semestre de 2012. Todas as ferramentas foram instaladas, configuradas e avaliadas.*

- A framework for secure single sign-on. *B. David, A. Nascimento, R. Tonicelli, R. Sousa Jr (UnB)*
  *Single sign-on solutions allow users to sign on only once and have their identities automatically verified by each application or service they want to access afterwards. There are few practical and secure single sign-on models, even though it is of great importance to current distributed application environments. We build on proxy signature schemes to introduce the first public key cryptographic approach to single sign-on frameworks, which represents an important milestone towards the construction of provably secure single sign- on schemes. Our contribution is two-fold, providing a framework that handles both session state across multiple services and granular access control. The intrinsic centralized access control functionality adds no additional cost to the single sign on protocol while providing an easy way to manage access policies and user rights revocation. Moreover, our approach significantly improves communication complexity by eliminating any communication between services and identity providers during user identity and access permission verification. Relying on simple primitives, our methods can be easily and efficiently implemented using standard cryptography APIs and libraries. We base our constructions on standard cryptographic techniques and a threat model that captures the characteristics of current attacks and the requirements of modern applications. This is the first approach to base single sign-on security on proxy signatures.*

- Geração de certificados digitais a partir da autenticação federada Shibboleth.
  *M. Wangham (UNIVALI), E. Mello (IFSC), D. Böger, J. Fraga (UFSC), M. Guérios (Inohaus)*
  *O framework Shibboleth é a infraestrutura de autenticação e autorização mais empregada para constituição de federações acadêmicas, possibilitando que usuários, através de um navegador web, acessem serviços disponibilizados pela federação usufruindo do conceito de autenticação única. O Shibboleth faz uso do padrão SAML, porém, nem todas as aplicações usadas pela comunidade acadêmica operam com credenciais SAML ou não são web. Diversos projetos surgiram para interligar o Shibboleth com a tecnologia de autenticação comumente usada em grids, as credencias X.509, permitindo assim a conversão de credenciais SAML em certificados digitais. O presente trabalho descreve e compara duas abordagens para geração de certificados X.509, a partir da autenticação federada Shibboleth. Uma abordagem está vinculada ao provedor de serviços e a outra ao provedor de identidades. Por fim, as abordagens propostas são comparadas com os projetos relacionados.*

[10:30-12:00] Palestra Nacional 1:

- Certificação Digital no Brasil.
  *Renato Martini, Diretor Presidente do Instituto Nacional de Tecnologia da Informação (ITI)*

[12:00-12:30] Apresentação dos Projetos do Programa de Gestão de Identidades (PGId) da RNP

- Um Levantamento de Métodos para Autenticação com Múltiplos Fatores.
  *Orientador: Jeroen van de Graaf, UFMG. Bolsista: Dayana Spagnuelo, UFSC*

[14:30-16:00] Apresentação dos Projetos do Programa de Gestão de Identidades (PGId) da RNP

- Integração de OpenID e Oauth a uma Infraestrutura de Autenticação Baseada em Shibboleth/SAML.
  *Orientador: Marco Aurélio Henriques, UNICAMP. Bolsista: Mateus Lara, UNICAMP*
- Gestão de Identidade em Redes Definidas por Software.
  *Orientadora: Débora Christina Saade, UFF. Bolsista: Edelberto Franco Silva, UFF*
- Adaptação do Sistema de Gerenciamento de Dados e Aplicações Científicas do SINAPAD para Controle de Acesso Federado.
  *Orientador: Antônio Tadeu Azevedo Gomes, LNCC. Bolsista: Vivian Medeiros, LNCC*

[16:30-18:00] Palestra Nacional 2:

- Gestão de Identidades da Geração que Vive na Nuvem.
  *Paulo Pagliusi, Diretor da Cloud Security Alliance – Chapter Brazil.*

[18:00-19:00] Painel:

- Impacto das Novas Tecnologias de IdM na Comunidade Acadêmica.
  *Noemi de La Rocque Rodriguez (Moderadora, PUC-Rio), Ricardo F. Custodio (LabSEC/UFSC), Jean Carlo Faustino (RNP) e Leandro Marcos de Oliveira Guimarães (RNP)*

[19:00-19:30] Encerramento

## Minicursos (sala DC3)

[08:30-10:00] e [10:30-12:30] Minicurso 3:

- Segurança em redes centradas em conteúdo: vulnerabilidades, ataques e contramedidas.
  *I. Ribeiro, F. Guimarães, J. Kazienko, A. Rocha, P. Velloso, I. Moraes, C. Albuquerque (UFF)*
  *As Redes Centradas no Conteúdo (Content-Centric Networking), ou simplesmente CCN, simplificam a solução de determinados problemas de segurança relacionados a arquitetura TCP/IP. Atualmente, para se prover a autenticidade e a integridade dos dados compartilhados na rede, faz-se necessário garantir a segurança do repositório e do caminho que os dados devem percorrer até o usuário final. Além disso, a contínua eficácia dos ataques de negação de serviço praticados contra a Internet atual sugere a necessidade de que a própria infraestrutura da rede forneça mecanismos para mitigá-los. Por outro lado, o modelo de comunicação da CCN é focado no conteúdo em si e não em sua localização física. Este capítulo apresenta uma visão geral da arquitetura CCN e como os seus mecanismos mitigam os problemas de segurança tradicionais. São abordados os ataques e possíveis contramedidas propostas na literatura, além de indicar seus desafios e perspectivas futuras.*

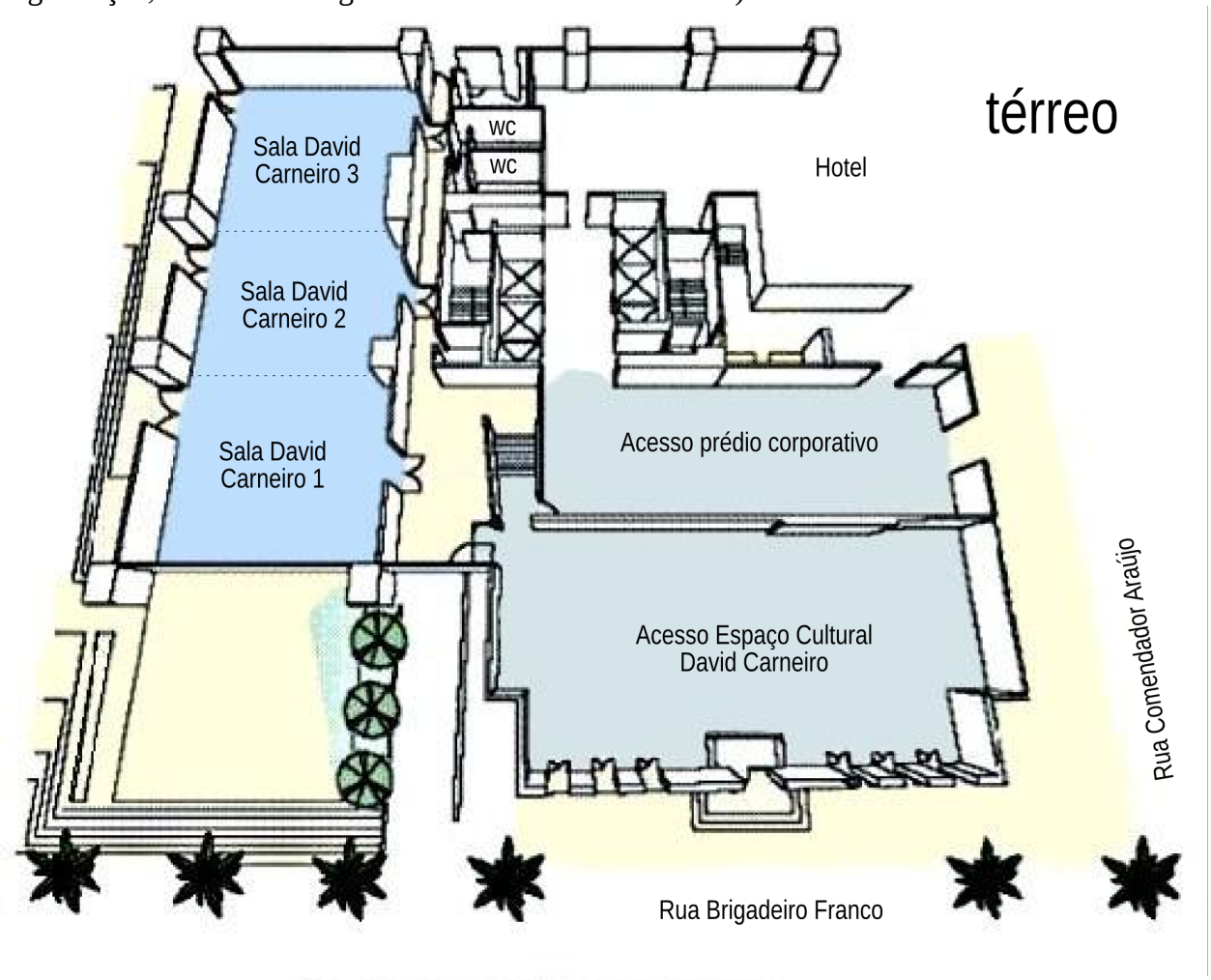
[14:30-16:00] e [16:30-18:30] Minicurso 4:

- *Encriptação homomórfica. E. Morais, R. Dahab (UNICAMP)*
  *Em 1978, Rivest, Adleman e Dertouzos [RAD78] sugeriram a construção de homomorfismos secretos - privacy homomorphisms - como forma de prover um mecanismo de proteção para computação sobre dados sigilosos. O problema permaneceu em aberto até recentemente, quando em 2009 Craig Gentry [Gen09a] o resolveu sugerindo a utilização de reticulados ideais na construção de um criptossistema completamente homomórfico. Infelizmente a proposta de Craig Gentry não é suficientemente eficiente para ser usada na prática, mas inúmeros trabalhos têm contribuído para que a eficiência dos algoritmos se torne cada vez maior. Neste minicurso serão estudados os esquemas recentemente propostos por Craig Gentry, apresentando o estado da arte e analisando os problemas que ainda precisam ser resolvidos.*

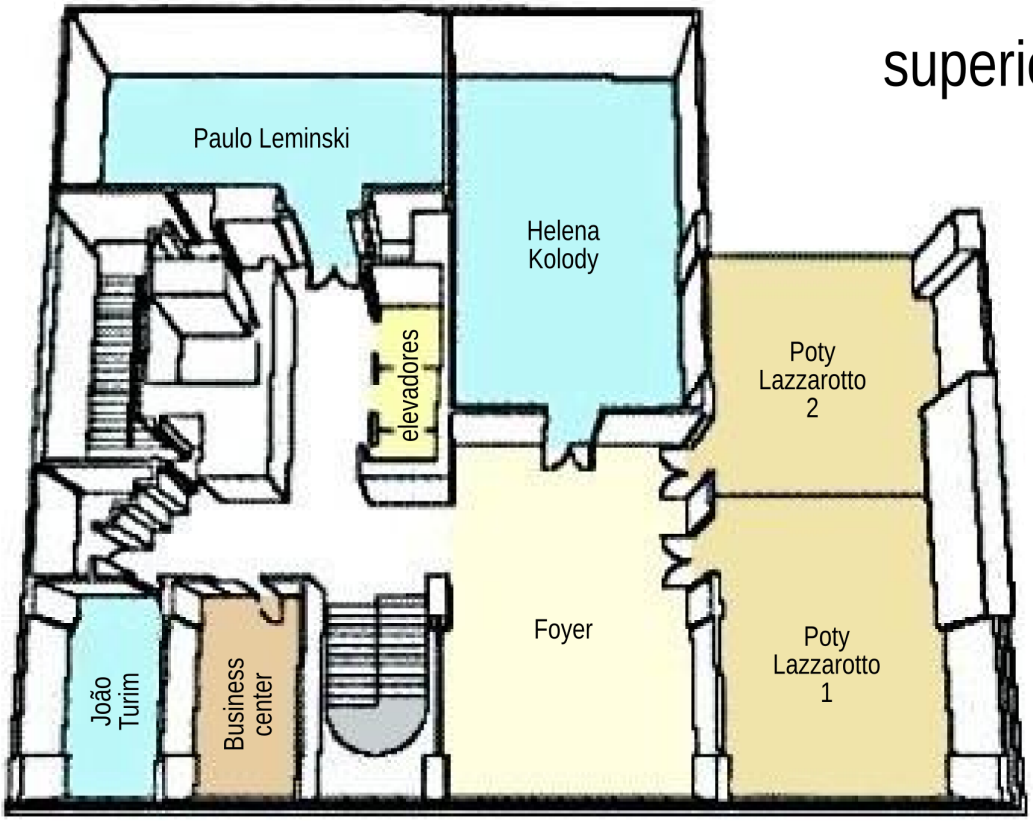
# Centro de Convenções do Hotel Pestana

(na programação, “Sala DC1” significa “Sala David Carneiro 1”)

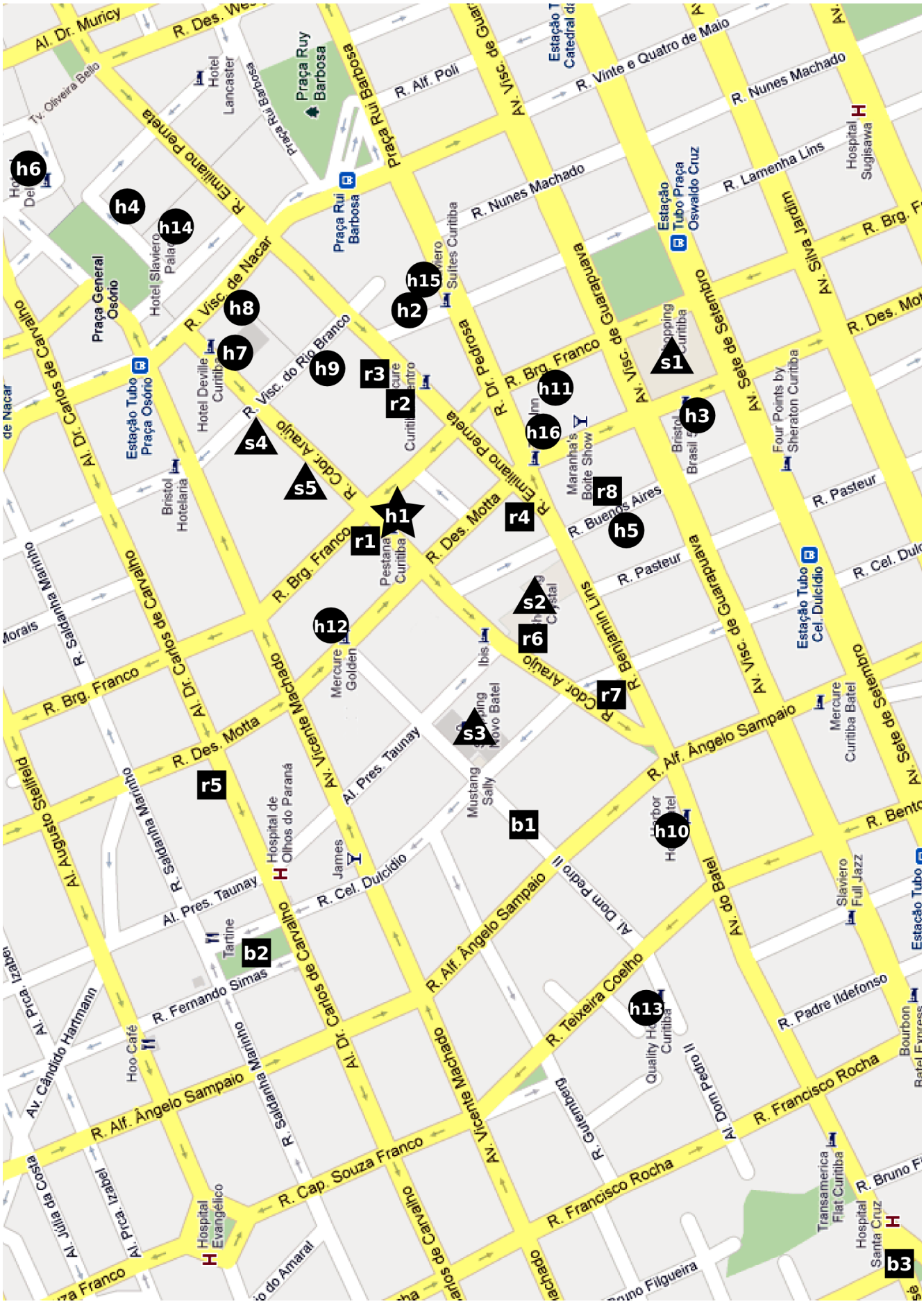
térreo




superior



# Mapa da região do evento



## Hotéis

★h1 **Hotel Pestana: Rua Comendador Araújo, 499 (41 3017-9900) (local do evento)**
● h2 Blue Tree Towers: Rua Lamenha Lins, 71 (41 3017-1090)
● h3 Bristol Brasil 500: Rua Desembargador Motta, 1499 (41 3021-1500)
● h4 Centro Europeu Tourist: Praça General Osório, 61 (41 3021-9900)
● h5 Confiance Batel: Rua Buenos Aires, 316 (41 3223-6962)
● h6 Del Rey: Rua Desembargador Ermelino Leão, 18 (41 2106-0099)
● h7 Deville Curitiba: Rua Comendador Araújo, 99 (41 3883-4777)
● h8 Deville Rayon: Rua Visconde De Nacar, 1424 (41 2108-1100)
● h9 Duomo Park Hotel: Rua Visconde do Rio Branco, 1710 (41 3221-1900)
● h10 Harbor Hotel Batel: Avenida do Batel, 1162 (41 3523-5800)
● h11 Ibis Curitiba Batel: Rua Brigadeiro Franco, 2154 (41 3595-2450)
● h12 Mercure Curitiba Golden: Rua Desembargador Motta, 2044 (41 3322-7666)
● h13 Quality Hotel Curitiba: Alameda Dom Pedro Il, 740 (41 2103-4000)
● h14 Slaviero Palace Hotel: R. Sen. Alencar Guimarães, 50 (41 3017-1000)
● h15 Slaviero Suítes Aspen: Rua Dr. Pedrosa, 208 (41 3323-3968)
● h16 Tulip Inn Batel: Rua Benjamin Lins, 513 (41 3028-5000)

## Centros Comerciais

▲s1 Shopping Curitiba
▲s2 Shopping Cristal
▲s3 Shopping Novo Batel
▲s4 Shopping Omar
▲s5 Mercadorama (supermercado)

## Restaurantes

■ r1 Comenda Grill (buffet por quilo)
■ r2 Tropilha Grill Churrascaria
■ r3 Avenida Paulista Pizza Bar
■ r4 Restaurante Scavolo (massas)
■ r5 Giotto Pizzaria
■ r6 Pizza Hut
■ r7 Taisho Batel (japonês)
■ r8 Porcini Trattoria (italiano)
▲s* As praças de alimentação dos *Shoppings*

## Bares - vida noturna

■ b1 vários na Alameda Dom Pedro II
■ b2 vários na Praça de Espanha
■ b3 vários na Alameda Bispo Dom José

## Cervejas especiais

Curitiba tem sido vista como uma das capitais que mais produzem cervejas artesanais, contando com 14 micro-cervejarias, além de uma cervejaria-escola. As cervejas curitibanas já conquistaram vários prêmios nacionais e internacionais. Sugestão de lugares para degustar nossas cervejas locais:

- **Asgard**: Rua Brigadeiro Franco, 3388 – Rebouças
- **Cervejaria da Vila**: Rua Mateus Leme, 2631 – Centro Cívico
- **Clube do Malte**: Rua Desembargador Motta, 2200 – Centro
- **Hop' N Roll**: Rua Mateus Leme, 950 – Centro Cívico
- **Templo da Cerveja**: Rua Cel. Dulcídio, 775 – loja 3 – Batel

# Utilidades

**Telefones de emergência**

- SAMU (pré-atendimento clínico): 192
- SIATE (pré-atendimento a trauma): 193
- Bombeiros: 193
- Defesa Civil: 199
- Polícia Civil: 197
- Polícia Militar: 190
- Guarda Municipal de Curitiba: 153
- Polícia Federal: 194

**Transportes**

- Ônibus executivo Aeroporto: (41) 3381 1326, http://www.aeroportoexecutivo.com.br
- Taxi: (41) 3376-7676, 3352-5252, 0800 41 1411, 0800 41 4646, 0800 41 4141

**Turismo**

- BWT Operadora (agência do evento): 3043-2233, http://www.bwtoperadora.com.br
- Portal da Prefeitura (ônibus, horários de atrações, etc): 156
- Linha de ônibus turística: http://www.urbs.curitiba.pr.gov.br/PORTAL/linha_turismo
- Agenda Cultural: http://www.fundacaoculturaldecuritiba.com.br

**Saúde**

- Hospital São Vicente. Av. Vicente Machado, 401 (41 3111-3000)
- Hospital Santa Casa de Misericórdia, Praça Rui Barbosa, 694 (41 3320-3500)
- Hospital Evangélico de Curitiba, Alameda Augusto Stellfeld, 1908 (41 3240-5000)
- Hospital Vita Batel, Rua Alferes Ângelo Sampaio, 1896 (41 3883-8400)
- Hospital Sugisawa Ltda, Avenida Iguaçu, 1236 (41 3259-6500)

**Bancos**

- Há um Banco 24 Horas no subsolo do hotel Pestana (estacionamento)
- Caixas automáticos nos shoppings.
- Rua Comendador Araújo (Banco do Brasil, Caixa Econômica, Itaú, Bradesco, HSBC, ...)

## Promoção


## Organização




## Apoio