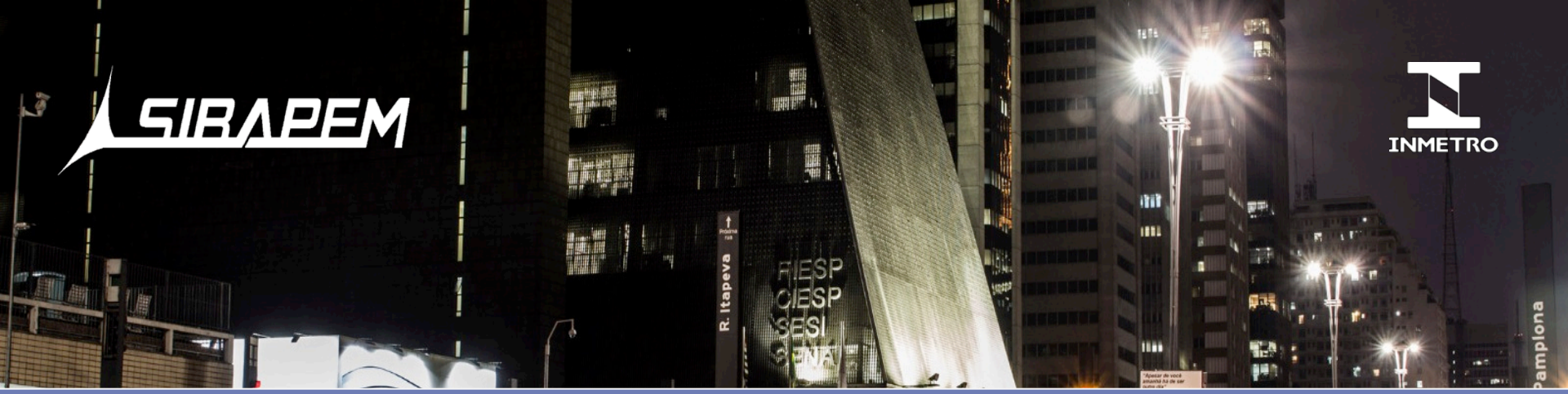


SCML/16

SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

Papel do Inmetro na Segurança e Confiança dos Novos Sistemas de Medição

Luiz Fernando Rust - Inmetro

#SCML2016

Agenda

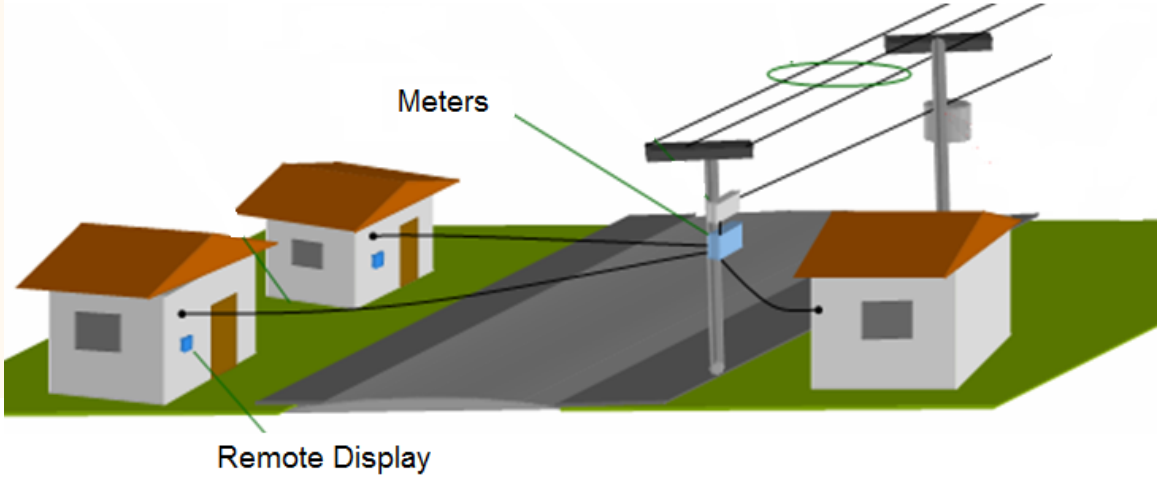
- Quem somos?
- Onde tudo começou
  - Metrologia legal
    - Aprovação de Modelo/Verificação - SMDEE
- O que Fazemos?
- Futuro
- Desenvolvimento de Competências
  - Áreas de pesquisa atuais
  - Projetos P&D

Quem Somos?

- **DIMCI/DMTIC**
  - **Divisão de Metrologia em Tecnologia da Informação e TeleComunicações da Diretoria de Metrologia Científica**
  - **LAINF – Laboratório de Informática**
    - **8 servidores, 4 bolsistas (2 Inmetro, 2 PPGI/UFRJ)**
    - **7 doutores, 3 doutorandos (UFRJ), 1 mestrando, 1 graduando**
    - **3 bolsistas de produtividade em pesquisa do CNPq (dois PQ-2 e um PQ-1A)**
  - **Mestrado Profissional em Metrologia e Qualidade do Inmetro**

Onde Começou?

- 2008 - Metrologia Legal - SDMEE
  - Apreciação Técnica de Modelo
    - Avaliação da conformidade dos instrumentos de medição quanto às exigências legais, na fase de projeto, isto é de concepção do instrumento
      - ensaios de desempenho, desgaste acelerado perturbação
      - proteção contra manipulações



Controle de Software na apreciação de Modelo - SMDEE

Ineditismo do sistema SMDEE

Dificuldade de absorção dos requisitos iniciais
Portaria Inmetro nº 371

Amadurecimento dos padrões de metrologia legal relacionados a software embarcado
WELMEC 7.2: Software Guide – *Measuring Instruments Directive* 200/22/EC)
OIML D 31/2009: *General Requirements of Software Controlled Measuring Instruments - draft*

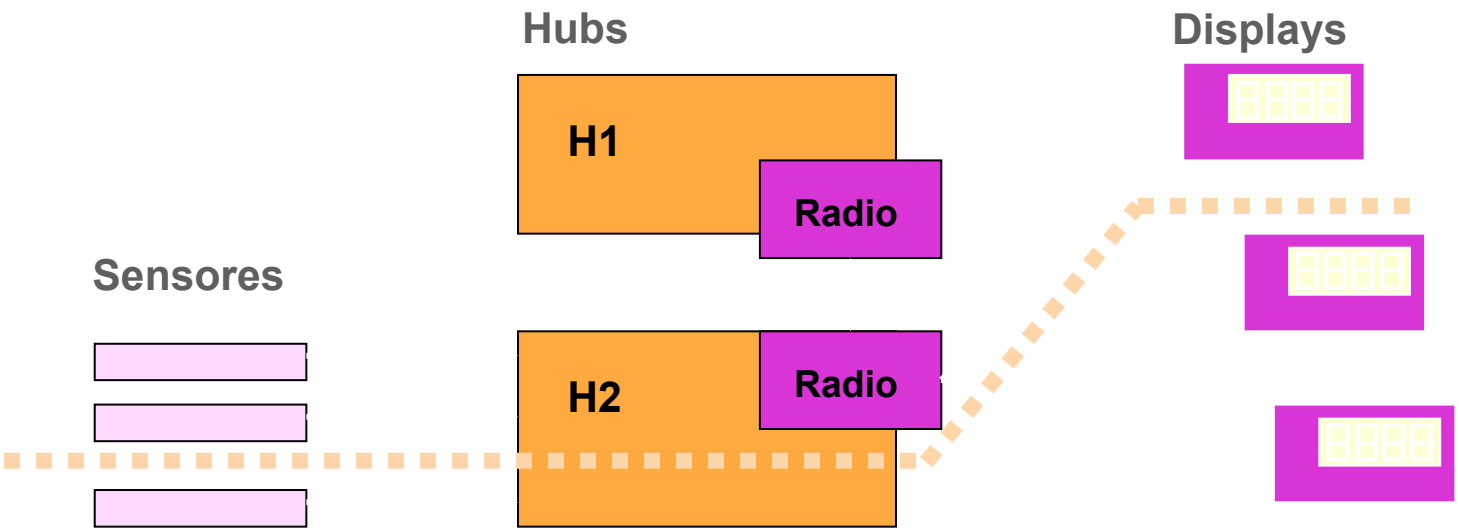
Detalhamento específico dos requisitos de software SMDEE
Portaria Inmetro nº 11 de 13 de janeiro de 2009

Características Básicas

- Entrega do código Fonte

- Legalmente relevante

  Todos os elementos envolvidos na captura, processamento e publicação do resultado ao consumidor pelo mostrador



Procedimentos para avaliação

Após disponibilização da documentação/produto

Análise da documentação

Procedimentos experimentais
cenários de testes funcionais na plataforma em aprovação

Inspeção visual do código fonte
busca de vulnerabilidades

Análise de fluxo do código fonte
aplicação de ferramentas automatizadas de "*tracking*" de variáveis relevantes
exemplo: constantes de calibração

O Que fazemos?

- Início
  - Metrologia Legal
    - Apreciação Técnica de Modelo
      - Medidores Elétricos, Umidade, Tora,
      - Bombas de combustível (Cadeado Inteligente – Patente)
      - MotoTaxi
  - Hoje
  - Serviço
    - Avaliação de segurança de equipamentos e dispositivos inteligentes
  - Desenvolvimento de novos requisitos/ensaios para novos programas
  - Nucleação de laboratórios
  - Apoio a Sociedade (Consultoria)
  - Pesquisa correlata para ampliação de competências

- **Exemplos**

  - **Registro de Ponto Eletrônico (Regulador MTE)**
    - Participação no Desenvolvimento do RTQ (Requisitos + Ensaios)
    - Avaliação de Requisitos não funcionais

  - **Equipamentos de Certificação Digital (Regulador ITI)**
    - Participação no grupo de trabalho para atualização dos MCT's
    - Acreditação de laboratórios

  - **Serviço de Avaliação de Produto de Software – números:**
    - 11 modelos de SDMEE, com a emissão de 32 notas técnicas
    - 13 modelos de REP, com a emissão de 25 notas técnicas
    - 9 modelos de med. energia, com a emissão de 14 notas técnicas
    - 5 modelos de simulador de pista, com a emissão de 19 notas técnicas
    - Outros medidores: taxímetro, volume de madeira...

Notas técnicas 2015 – Avaliação da segurança

Número NT		Atividade/Fabricante	Descrição
15_01	REP	REP Dimep	Documentação do REP - PRINTPOINT 111- DIMEP 06 de janeiro de 2015.
15_02	REP	REP Madis	Documentação do REP - EVO - MADIS 06 de janeiro de 2015.
15_03	REP	REP Henry	Registrador Eletrônico de Ponto modelo SI fabricante Henry, processo 045495/2014.
15_04	ME	ME Elster	Documentação dos medidores de energia AI050 2G e AI052 2G do Fabricante Elster Medição de Energia Ltda., recebida em 12 de janeiro de 2015.
15_05	REP	REP Topdata	Documentação do REP - Inner Rep Plus - TOPDATA, 14 de janeiro de 2015.
15_06	REP	REP Trix	Documentação do BIO REP-200, fabricante TRIX de 13 de janeiro de 2015.
15_07	REP	REP Topdata	Documentação do REP - Inner Rep Plus - TOPDATA, 26 de janeiro de 2015.
15_08	ME	ME Nansen	Documentação do Medidor - KS 70 - Nansen 12 de janeiro de 2015.
15_13	REP	REP Control ID	Documentação do REP - iDClass Mult S - Control ID, 20 de janeiro de 2015.
15_14	REP	REP Henry	Registr… …o 045495/2014.
15_15	REP	REP Rotec Relógios	Docum… …o de 2015.
15_16	REP	REP Biometrus	Docum… …15.
15_17	REP	REP Velti	Docum…
15_21	REP	REP Control ID	Docum…
15_22	ME	ME Landis+Gyr	Docum… …evereiro de 2015.
15_23	ME	ME Landis+Gyr	Docum… …o de 2015.
15_24	ME	ME Elster	Documentação do Medidor de Energia Elétrica Elster - A152 TB e A1052 TB- 12 de janeiro de 2015.
15_25	ME	ME Nansen	Documentação do Medidor - KS 70 - Nansen 18 de março de 2015.
15_26	Simulador Pista	Simulador Pista ETM	Avaliação de simulador de pistas – ETM
15_27	REP	REP Henry	Registrador Elejrôníco de Ponto modelo Compacto SI fabricante Henry,' "processo 52600,.045495/2014-44.,'.,
15_28	Simulador Pista	Simulador Pista Universal Maquinas	Avaliação de simulador de pístas-- UniversalMaquinas
15_29	ME	ME Elster	Documentação do Medidor de Energia Elétrica Elster - A152 TB eAI052'TB-17 de abril de 2015.
15_30	REP	REP Topdata	Documentação do REP -.Inner Rep Plus - TOPDATA, 10 de.março de 2015.
15_31	REP	REP Control ID	Documentação do REP - IDCLASS =Control !D~ 20 de' março de 2015 .
15_32	ME	ME Elster	Documentação dos medidores de energia A1050 2G e A1052 2G do Fabricante Elster Medição de Energia Ltda., recebida em 17 de abril de 2015.
15_33	Outros		Regulamentos Técnicos Metrológicos anexos às Portarias Inmetro 586/2012 e 520/2014 e Regulamento Técnico da Qualidade anexo à Portaria Inmetro 595/2013.
15_34	REP	REP Enterplak	Documentaçãodo REP ~IPOINTLINE":RWTech-Enterplák, 30 de abril 'de 201S
15_35	Simulador Pista	Simulador Pista Mequivel	Av~liação de simuladordepístas'> Mequível
15_36	Simulador Pista	Simulador Pista Moss do Brasil	Avaliação de -simulador de pistas r Moss do.Brasil
15_37	REP	REP Trix	Trix
15_38	ME	ME Weg	Documentação dos medidores de energia elétrica modelos SMW100, SMW200, SMW200i, SMW300 e SMW300i, recebida em 8 de junho de 2015.
15_39	ME	ME Nansen	Documentação do Medidor - K,S70 - Nanseü 17 de abril de '2015.

Serviço interativo

- # Outras atuações

  - Apoio à DMEL: Regulamentos Técnicos Metrológicos e Avaliação de Software
  - Apoio à DCONF: Elaboração de diversos Programas de Avaliação da Conformidade e Consultoria (MEC, ENEM, MTE, ITI, VLT, LED, Planejamento)
    - MTE: sistemas de registro de ponto
    - ITI: revisão dos Manuais de Condutas Técnicas para a avaliação de produtos ICP-Brasil
    - MEC/FNDE: avaliação de notebooks e tablets para alunos
    - ENEM: avaliação do sistema de rastreamento das provas
    - Avaliação do sistema de Sorteio da Caixa Econômica
    - Regulamento VLT
    - Receita Federal: Avaliação do sistema de autenticação para selos de bebidas
  - Apoio à CGCRE
    - Organismos de Inspeção
      - Veículos de transporte de produtos perigosos
      - Conversão para Gás
  - .....

Futuro

Redes Inteligentes

- Internet das coisas
- Sistemas Ffísico-Cibernéticos

Modernização de serviços prestados
implica
Infra-estrutura avançada de medição

Medidores inteligentes

- Eletrodomésticos inteligentes
- Novos sensores e atuadores
- Aplicativos

Com

- **Segurança**
- **Interoperabilidade**

3 Pilares

- **Normalização**
- **Metrologia**
- **Avaliação da Conformidade**

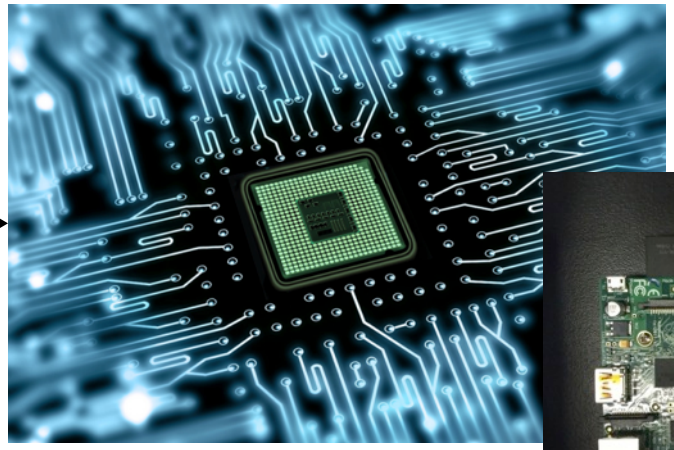
Desenvolvimento de Competências

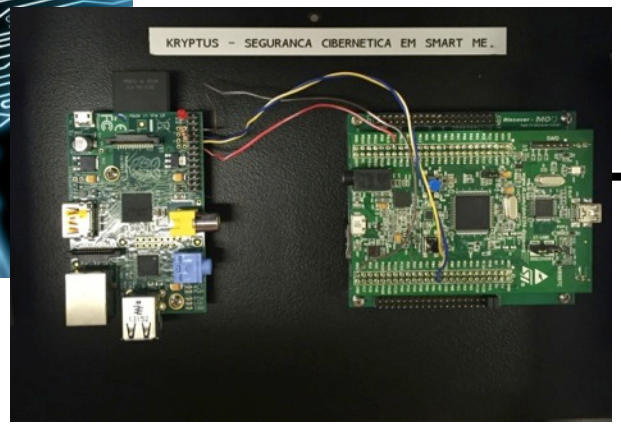
- **Áreas de Pesquisa**
  - Smart Grid (Cooperação em com o NIST)
    - mecanismos de autenticação baseados em atraso
    - protocolos de distribuição de msg para Unidades de Medição Fasorial
  - Mecanismos de forense
    - Logs seguros
      - Garantir a detecção de manipulação das entradas de log
  - Autenticação por Assinatura Cinética
      - Sensoriamento confiável para crash tests
  - Análise de software
    - Transposição de ferramentas de análise em x86 para ARM
      - Falhas não Intencionais
        - Falhas de Programação
      - Programação Intencional
        - Detecção de códigos não-executados, códigos maliciosos
  - Técnicas computacionais para controle de fraudes
    - Controle de Emissão de Gases
    - Markov (para modelar processo de auditoria)
    - Benford, Inlier detection (função recompensa)

Áreas de Pesquisa (cont.)

- Desenvolvimento de Hardware Seguro
  - Facilitar Avaliação de Software

Requisitos de software
verificação de integridade, carga de software,
Proteção de parâmetros relavantes, controle de acesso





Projeto P&D Ceron/Eletrobras

2013 - 2015

Avaliado com 4,5 em 5 pela ANEEL

Verificação de integridade

Proteção de Software

Rastreabilidade de Software

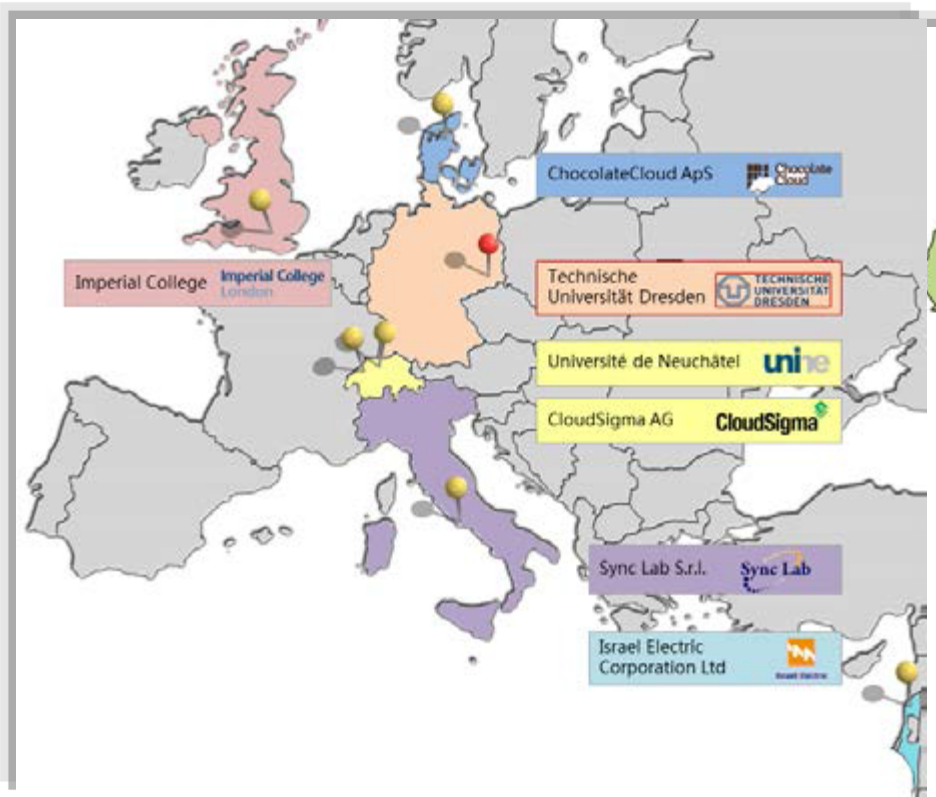
Ferramentas para avaliação de Software (vulnerabilidades)

Componentes especializados para controle metrológico

INMETRO
Ministério do Desenvolvimento, Indústria e Comércio Exterior
GOVERNO FEDERAL BRASIL PÁTRIA EDUCADORA

SECURECLOUD - SECURE BIG DATA PROCESSING IN UNTRUSTED CLOUDS – H2020

- Starting 01/2016
- Development of a secure cloud platform
- Evaluate the platform with the help of privacy- and security-enhanced big data demonstrators in the area of smart grid including smart metering
  - Consortium brings together 14 organisations (7 from Europe, 7 Brazil): Universities, Research centers, Industrial partners



Our engagements in SecureCloud

- **Task 1.1**
  - Definition of use cases and requirements (M1-M9; TUD, CC, SYNC, IEC, CS, LACTEC, UFCG, UTFPR, UNIFEI, COPEL, CAS, INMetro)

- **Task 5.3**
  - Test and validation of secure applications for privacy-sensitive data (M1-M24; UTFPR, TUD, CC, SYNC, IEC, CS, LACTEC, UNIFEI, CAS, INMetro)

- **Task 5.4**
  - Tests and validation of applications with strict QoS requirements (M11-M36; UFCG, TUD, IMP, UniNE, CC, SYNC, IEC, CS, LACTEC, UTFPR, COPEL, CAS, INMetro)

- **Produção científica e tecnológica**

  - **Produção científica**
    - **15 artigos publicados em periódicos em 2015**
    - **Diversas participações em conferências, comitês de programas (3 SBSeg 2016), bancas de avaliação...**

  - **Produção tecnológica**
    - **Uma patente depositada (cadeado inteligente) e uma patente em elaboração (marca d'água em software)**

  - **Principais eventos organizados**
    - **Workshop NIST- Inmetro on Cybersecurity - 2014**
    - **ISSISP'2015, WRAC+'2015 (SBSeg 2015)**

Conclusões

- **O Inmetro já está naturalmente envolvido com segurança cibernética devido suas ações de controle metrológico legal, e**

- **Pode contribuir com a gestão dos mais diversos programas de avaliação da conformidade necessários para a garantia dos aspectos de segurança e interoperabilidade em aplicações para Internet da Coisas e Sistemas Físicos-Cibernéticos.**

INMETRO
Ministério do Desenvolvimento, Indústria e Comércio Exterior
GOVERNO FEDERAL BRASIL PÁTRIA EDUCADORA

Muito obrigado pela atenção

www.inmetro.gov.br
lfrust@inmetro.gov.br

Publicações

2016

Multicast Delayed Authentication For Streaming Synchrophasor Data in the Smart Grid
IFIP SEC 2016 (31th IFIP TC-11 SEC 2016 International Information Security and Privacy Conference), May 30th till June 1st 2016 at Ghent, Belgium.

2015

A Decentralized Damage Detection System for Wireless Sensor and Actuator Networks.
IEEE Transactions on Computers

A Dynamic and Context-aware Security System for Shared Sensor Networks
International Journal of Distributed Sensor Networks

Methods to Protect Cryptographic Keys on Safety-Critical Systems
WSEAS Transactions on Information Science and Applications

Hiding Cryptographic Keys of Embedded Systems
9th International Conference on Computer Engineering and Applications

Ensuring energy efficiency of power quality applications in smart grids through a framework based on wireless sensor and actuator networks
International Wireless Communications & Mobile Computing Conference (IWCMC)

SensorWatermark: scheme of software watermark using code obfuscation and tamper-proofing for WSN

2014

Software Analysis and Protection For Smart Metering
NCSL International Measure – The Journal of Measurement Science

Publicações (cont.)

SBSEG 2014

- Protocolo para transferência parcial de conhecimento e sua aplicação à verificação segura de marcas d'água
- A randomized graph-based scheme for software watermarking
- Detecção de Dados Suspeitos de Fraude em Organismos de Inspeção Acreditados
- Segurança no Sensoriamento e Aquisição de Dados de Testes de Impacto Veiculares
- Esquema de Estruturação SbC-EC para Log Seguro

Energy footprint framework: A pathway toward smart grid sustainability.
IEEE Communications Magazine (Print), v.51, p. 50-56, 2013.

A consumption authenticator based mechanism for Time-Of-Use smart meter measurements verification.
Applied Mechanics and Materials, v. 241-244, p. 218-222, 2013.

A tight bound for exhaustive key search attacks against message authentication.
Informatique Théorique et Applications (Imprimé), v. 46, p. 000, 2013.

Program Matching through Code Analysis and Artificial Neural Networks.
International Journal of Software Engineering and Knowledge Engineering , v. 22, p. 1-17,

Software Evaluation of Smart Meters within a Legal Metrology Perspective: A Brazilian Case.
IEEE PES Conference on Innovative Smart Grid Technologies Europe, 2010, Gothenburg.

Traceability of Executable Codes using Neural Networks
Information Security Conference, 2010, Boca Raton. 2010.

Program Equivalence using Neural Networks.
5th International ICST Conference on Bio-Inspired Models of Network, Information, and Computing Systems, 2010,Boston.