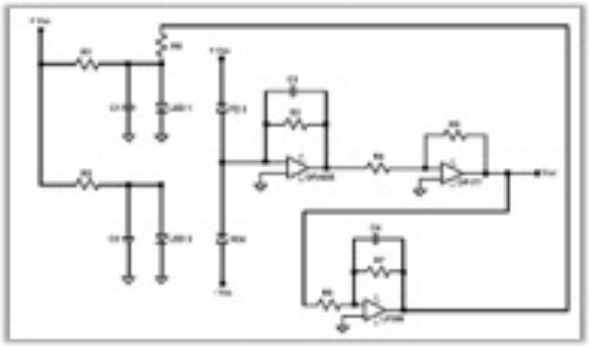
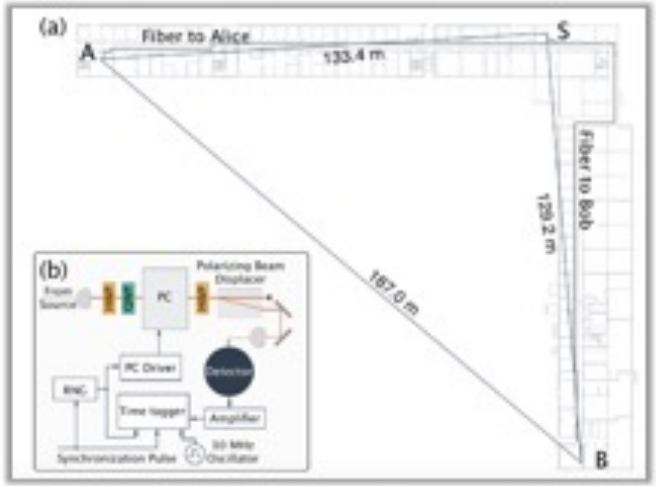
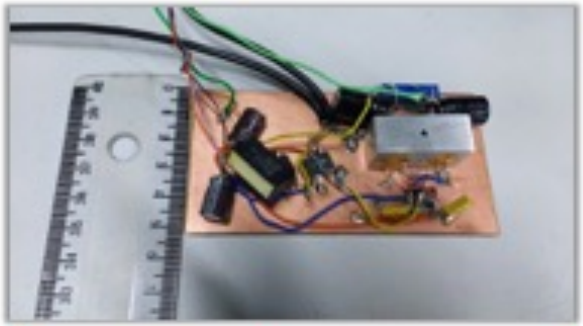
Temas de Pesquisa e Desenvolvimento

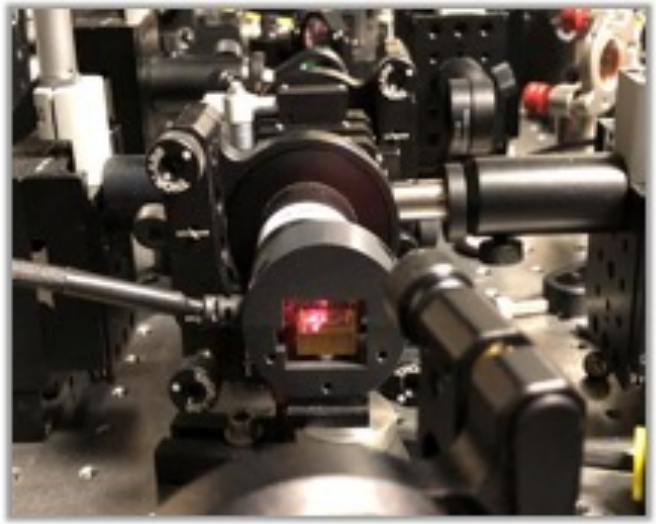
Testes de Aleatoriedade

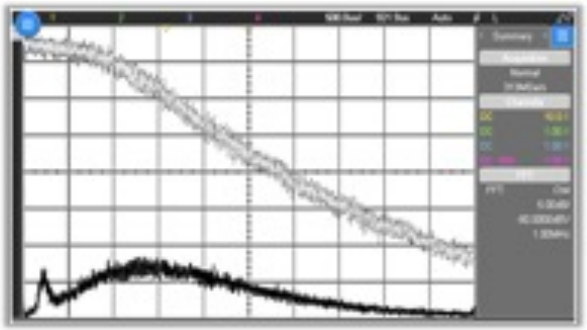
Estudo de Fontes de Aleatoriedade



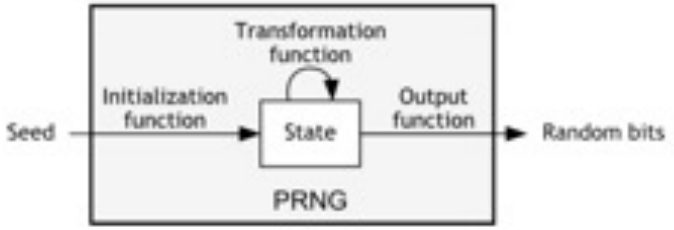




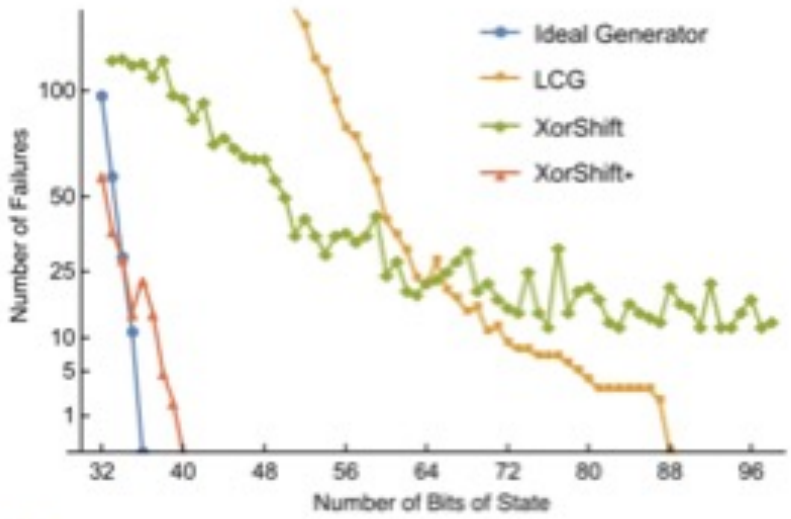




Caracterização da Aleatoriedade



Statistical test	*p-value*	*proportion*	*result*
Frequency	0.35048	47/50	pass
Block frequency	0.000123	47/50	pass
Cumulative sum	0.171867	47/50	pass
Longest runs	0.015598	47/50	pass
Rank	0.002374	50/50	pass
FFT	0.085587	47/50	pass
Non-overlapping template	0.085587	50/50	pass
Overlapping template	0.6163	49/50	pass
Random excursions variant	0.213309	48/50	pass
Serial	0.213309	50/50	pass
Linear Complexity	0.213309	49/50	pass



CEFET/RJ INMETRO uff

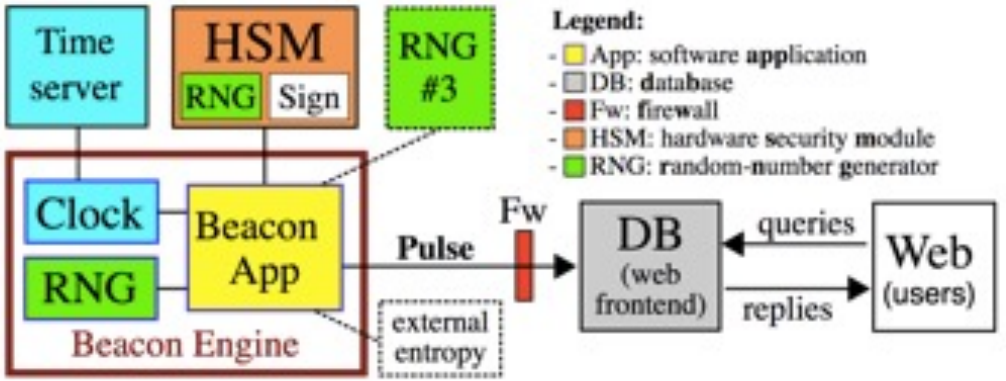
Randomness beacon: Disseminação e Aplicações

- Caracterização de fontes de entropia e RNGs
- Desenvolvimento de um sistema para distribuição beacons de aleatoriedade
- Pesquisa de protocolos de segurança baseados em beacons de aleatoridade

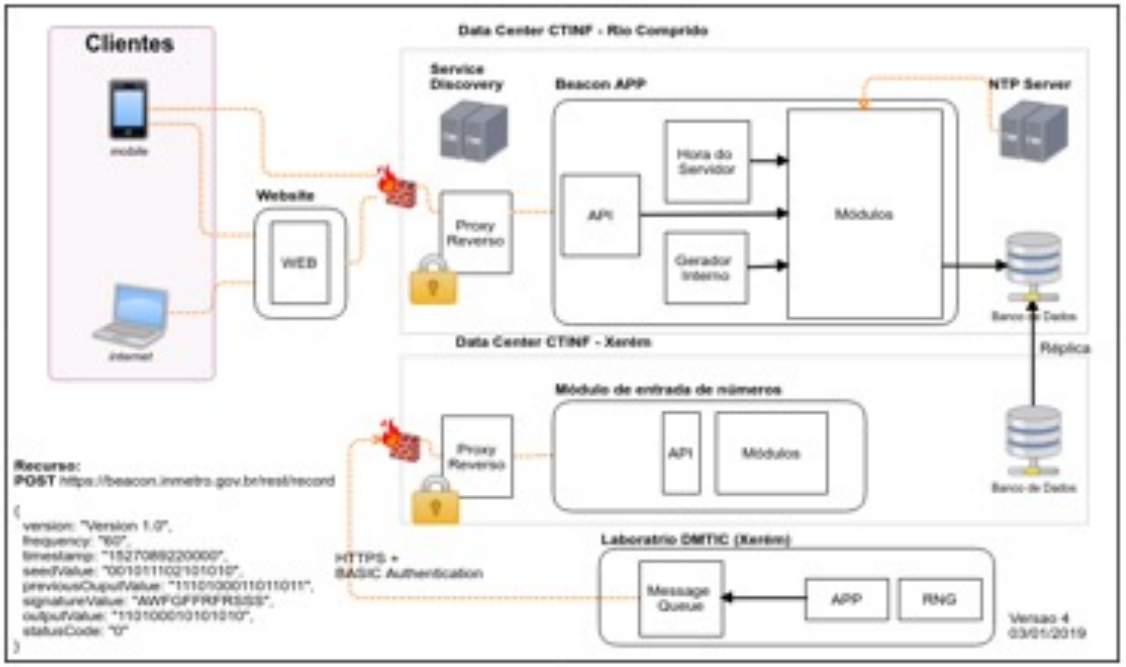
INMETRO

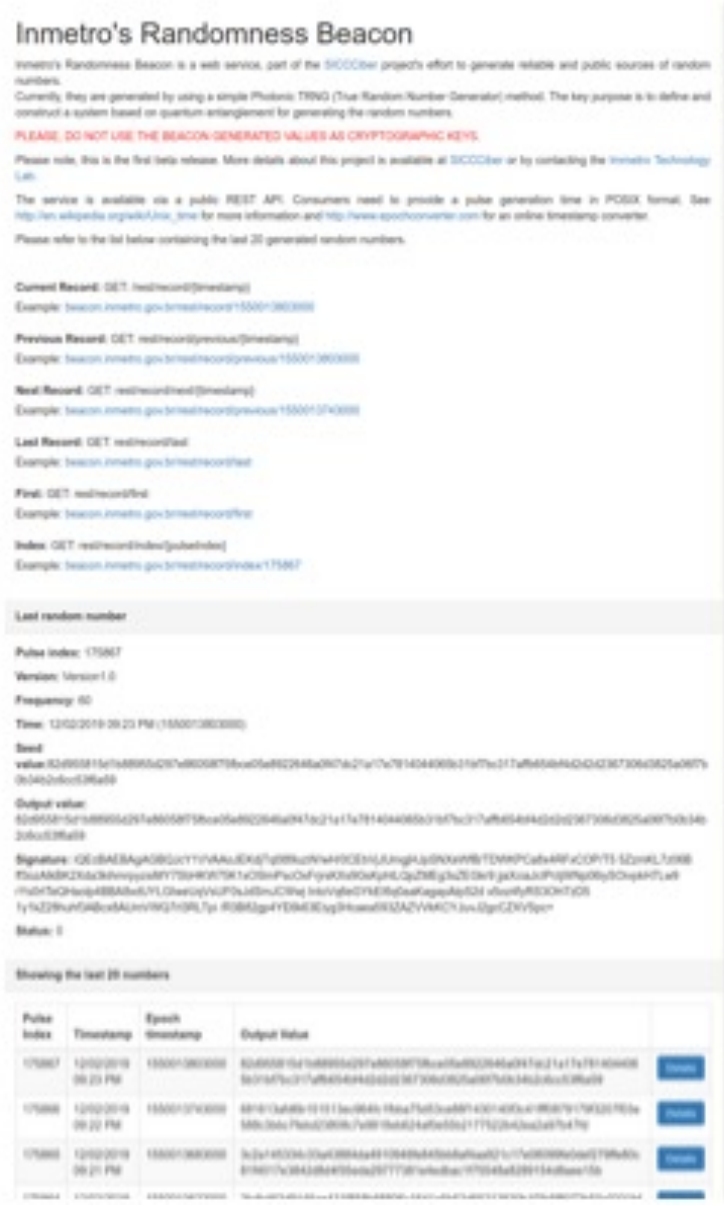
uff

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Randomness beacon: Disseminação e Aplicações





Inmetro's Randomness Beacon

Inmetro's Randomness Beacon is a web service, part of the SICCOBer project's effort to generate reliable and public sources of random numbers.
Currently, they are generated by using a simple Photonic TRNG (True Random Number Generator) method. The key purpose is to define and construct a system based on quantum entanglement for generating the random numbers.

PLEASE, DO NOT USE THE BEACON GENERATED VALUES AS CRYPTOGRAPHIC KEYS.

Please note, this is the first beta release. More details about this project is available at SICCOBer or by contacting the Inmetro Technology Lab.

The service is available via a public REST API. Consumers need to provide a pulse generation time in POSIX format. See http://en.wikipedia.org/wiki/Unix_time for more information and http://www.epochconverter.com for an online timestamp converter.

Please refer to the list below containing the last 20 generated random numbers.

Current Record: GET /rest/record/{timestamp}
Example: beacon.inmetro.gov.br/rest/record/1550013803000

Previous Record: GET /rest/record/previous/{timestamp}
Example: beacon.inmetro.gov.br/rest/record/previous/1550013803000

Next Record: GET /rest/record/next/{timestamp}
Example: beacon.inmetro.gov.br/rest/record/previous/1550013743000

Last Record: GET /rest/record/last
Example: beacon.inmetro.gov.br/rest/record/last

First: GET /rest/record/first
Example: beacon.inmetro.gov.br/rest/record/first

Index: GET /rest/record/index/{pulseIndex}
Example: beacon.inmetro.gov.br/rest/record/index/175867

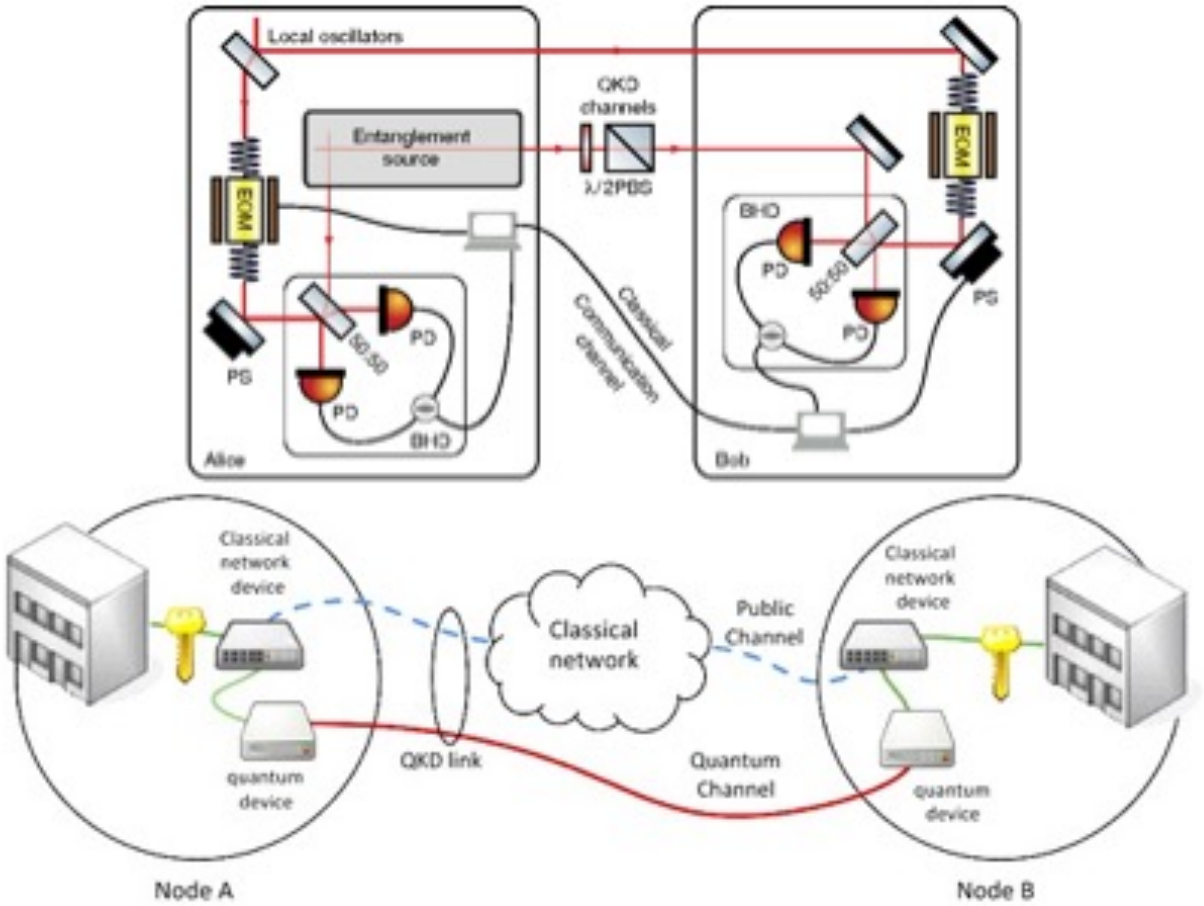
Last random number

Pulse index: 175867
Version: Version1.0
Frequency: 60
Time: 12/02/2019 09:23 PM (1550013803000)
Seed value: 82d9558 1fa01e88955d297e86058f758bca05a8922648a0f47dc21a17e7914044065b31bf7bc317af8d654644d2d2d367306d3625a99f7b0b462c6cc536a59
Output value: 82d9558 1fa01e88955d297e86058f758bca05a8922648a0f47dc21a17e7914044065b31bf7bc317af8d654644d2d2d367306d3625a99f7b0b346 2c6cc536a59
Signature: iQEcBAEBAgAGBQJcY1iVAAoJEKdj7qf99kuzNVwHYICEhVjUmgKJp5NXeWfBrTDWWPCa8v4RFxCOP/T5 SZpnxKL7z66B ff5uuMx8K2Xdx3kfvmyjyzxMY7S0HK9t75K1xO5mPscOvFrpvK0fu90eKpHL/QpZ9dEg3sZ503e9 jpKnaJcfPq9PlqO6y5OhqkkH7Lw9 r1s0rT5eQHwcip4BBA8w6JYLO0wnGqVnUP0eJx80mJCWaj hlnVrg8e01Y6E/8qDaaKagapAtp52d x6xoHfyR53OHTzQ5 1y1sZ2fkvnfZaBcx4AJmrVWQ7r0RL7px 4f0B6Zgp4YE6kE3EIyg3Hcaea5953AZVVAKC1Jxv J2grCZKV5pc=
Status: 0

Showing the last 20 numbers

Pulse Index	Timestamp	Epoch timestamp	Output Value	
175867	12/02/2019 09:23 PM	1550013803000	82d9558 1fa01e88955d297e86058f758bca05a8922648a0f47dc21a17e7914044065b31bf7bc317af8d654644d2d2d367306d3625a99f7b0b462c6cc536a59	Details
175866	12/02/2019 09:22 PM	1550013743000	68161da8d8c10151bc9648c19daa75d53ca88f14301405ce1ff58797913f3337f03e 988c3bbc79ebd23808c7e9915e6624affe5f0b21775226453ea2ab7b47fd	Details
175865	12/02/2019 09:21 PM	1550013683000	3c2e145334c31ad08664ea4910949fa845fdc6affeed021c17e0f0899e0ee0379fe80c 81f4017e3843d8d4f05bda2f07773f01efbd0ac1f7554fa5289144dfaee150	Details

Quantum Key Distribution (futuro)



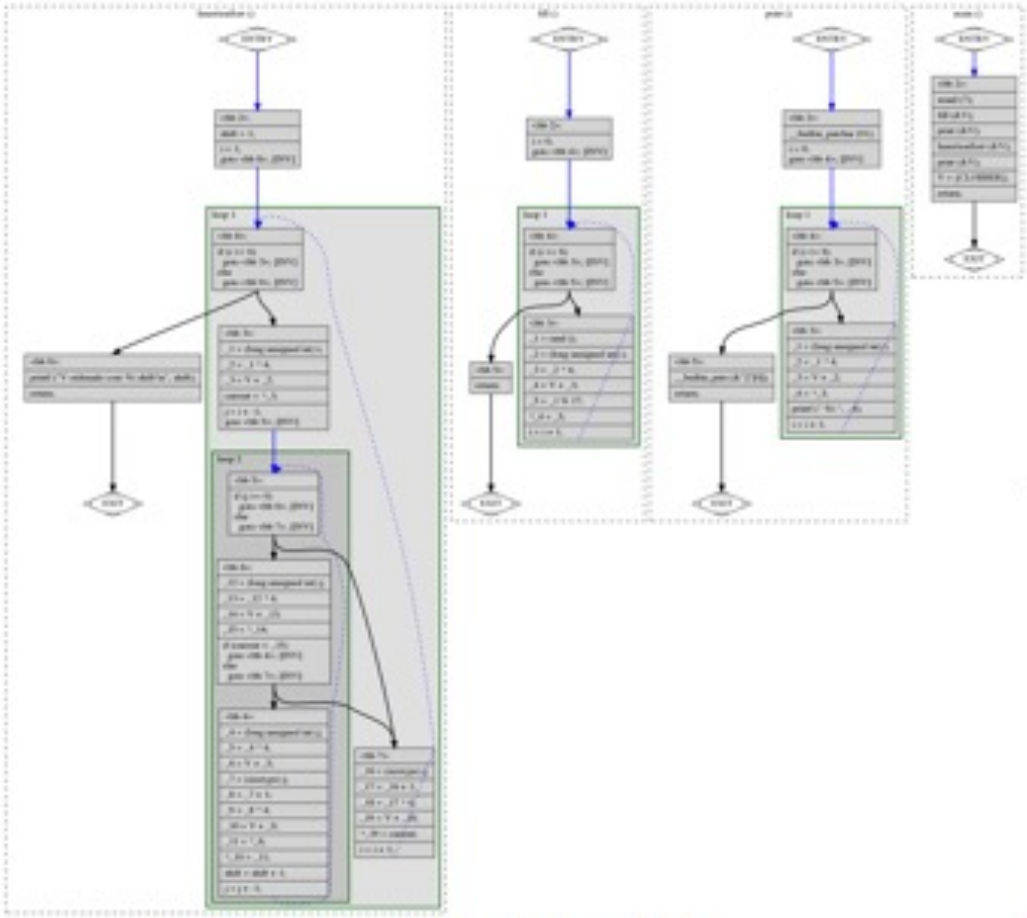
Tarefas e temas de pesquisa

- Alinhar o Beacon à versão 2.0 do padrão NIST
- Adaptar o Beacon a aleatoriedade verificável (VDF)
- Formalizar metodologia de análise de aleatoriedade
- Analisar fontes diversas de aleatoriedade
- Otimizar/testar circuitos de opto-detecção

Grafos de Programa para Análise e Proteção de Software

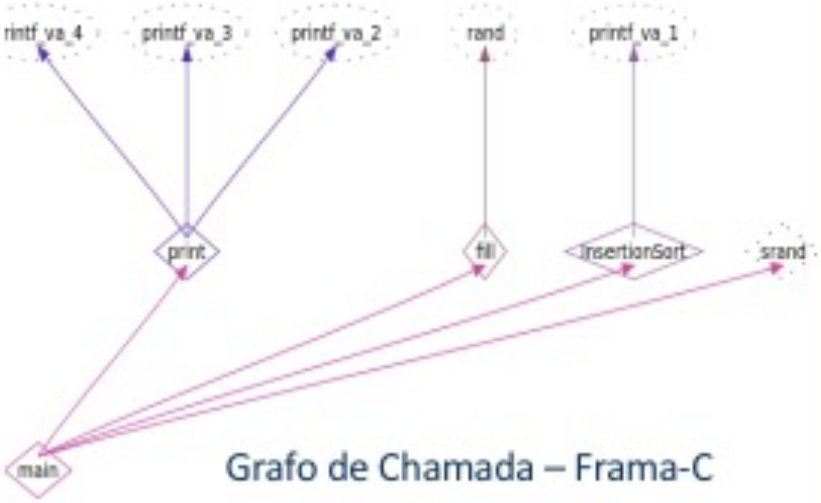
Análise Estática ”clássica” de Código Fonte

Grafos de Programa



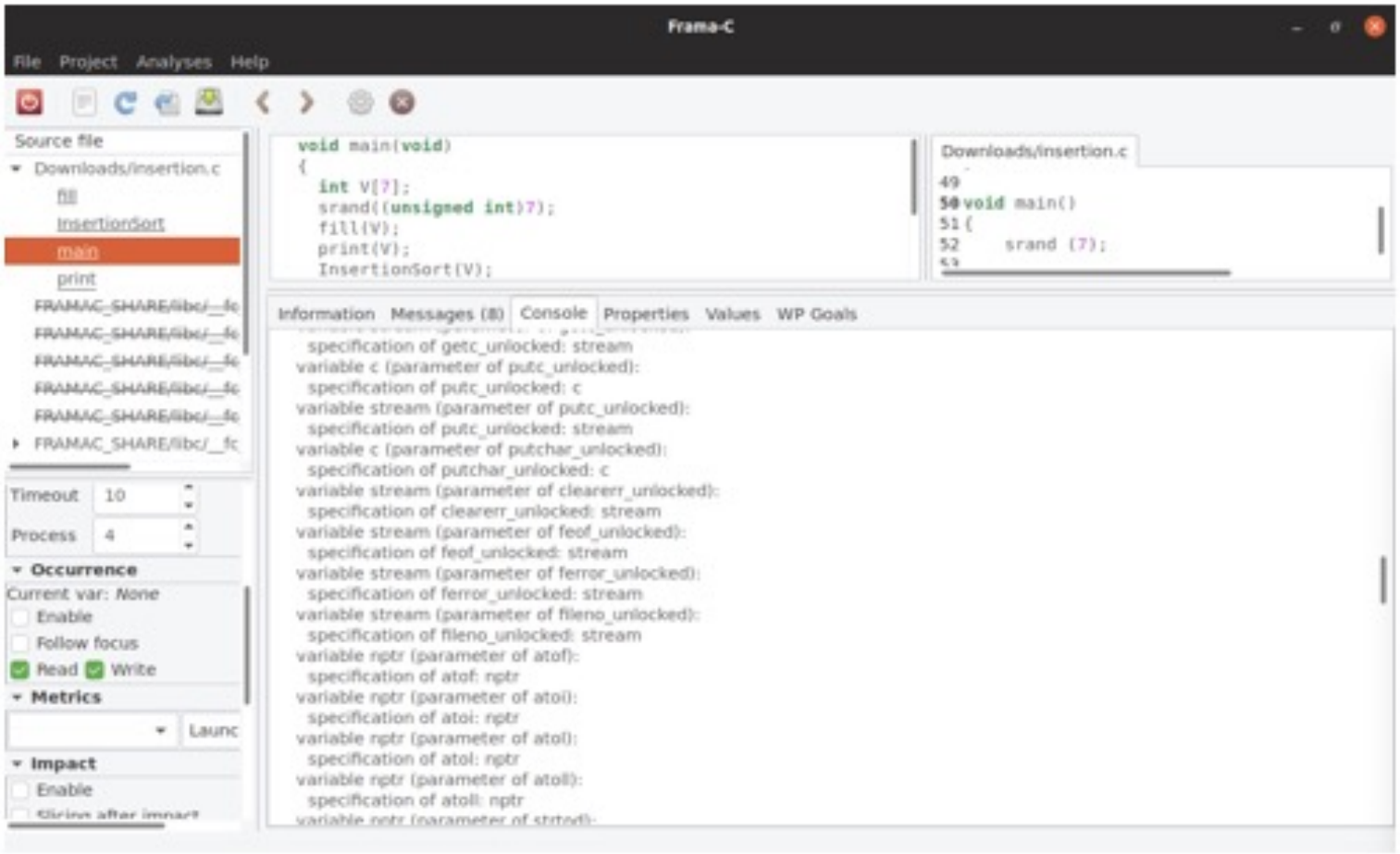
Grafo de Fluxo de Controle – GCC

Grafo de Chamada – LLVM

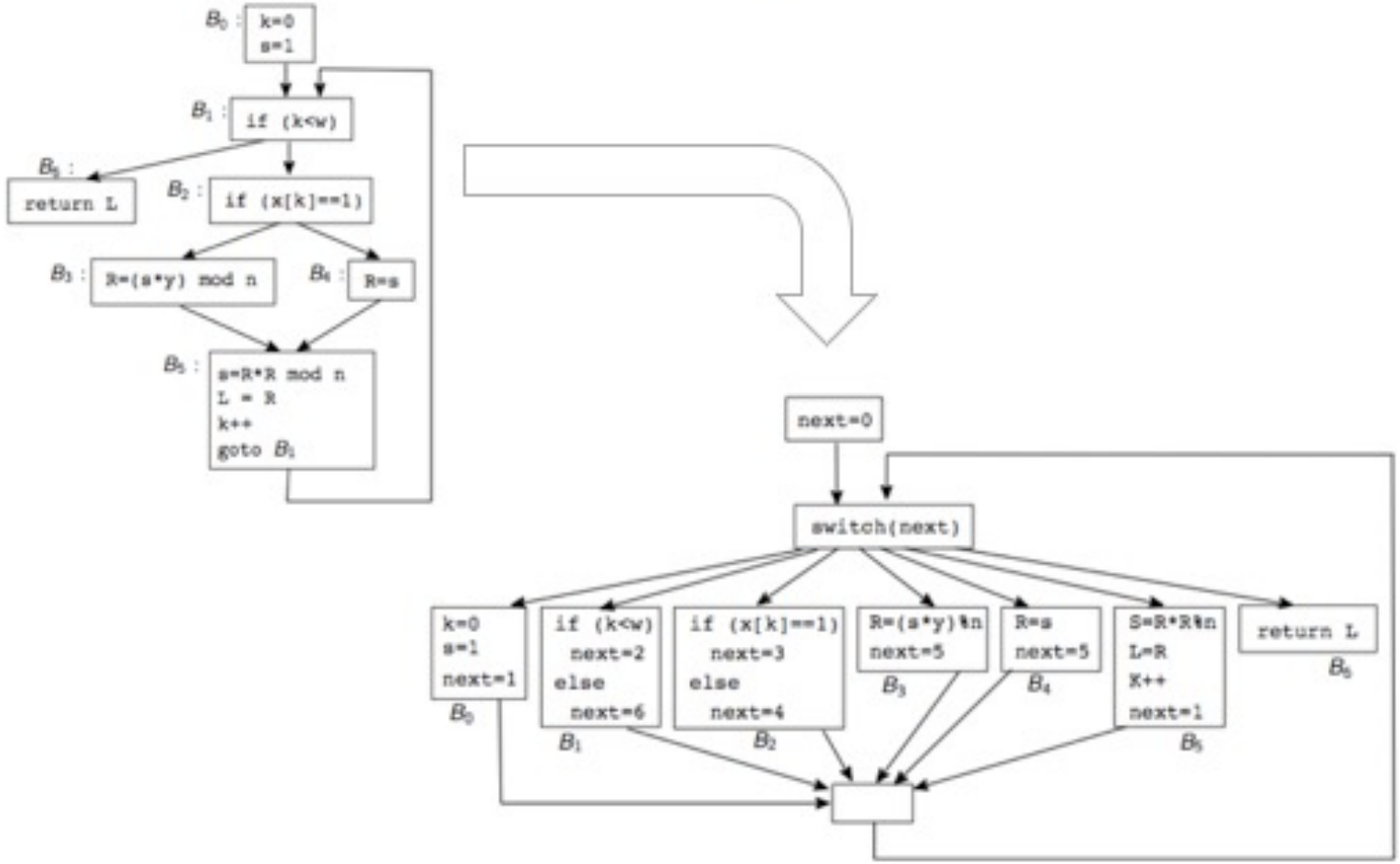


Grafo de Chamada – Frama-C

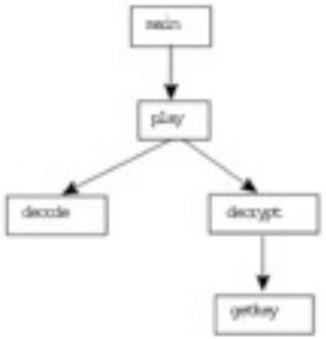
Análise de SW: Rastreamento de Variáveis

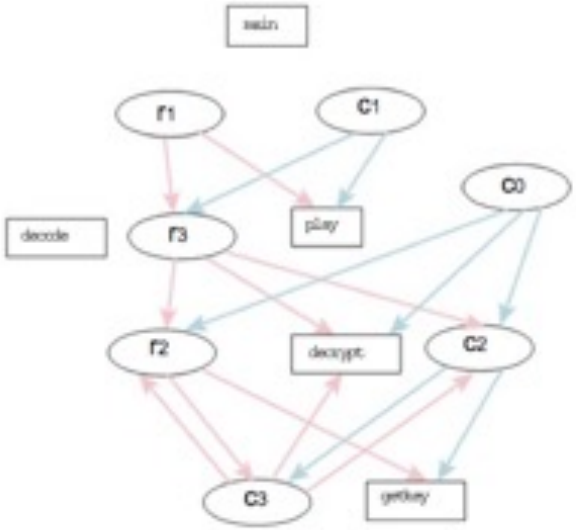


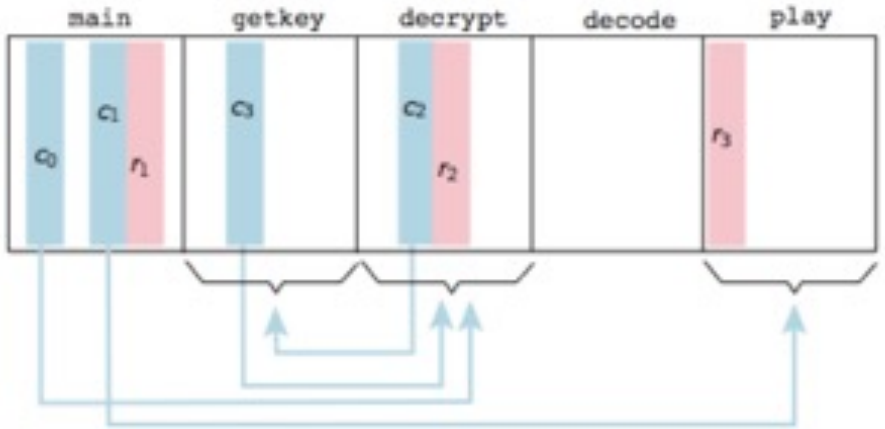
Proteção de SW: Ofuscação



Proteção de SW: Incorruptibilidade







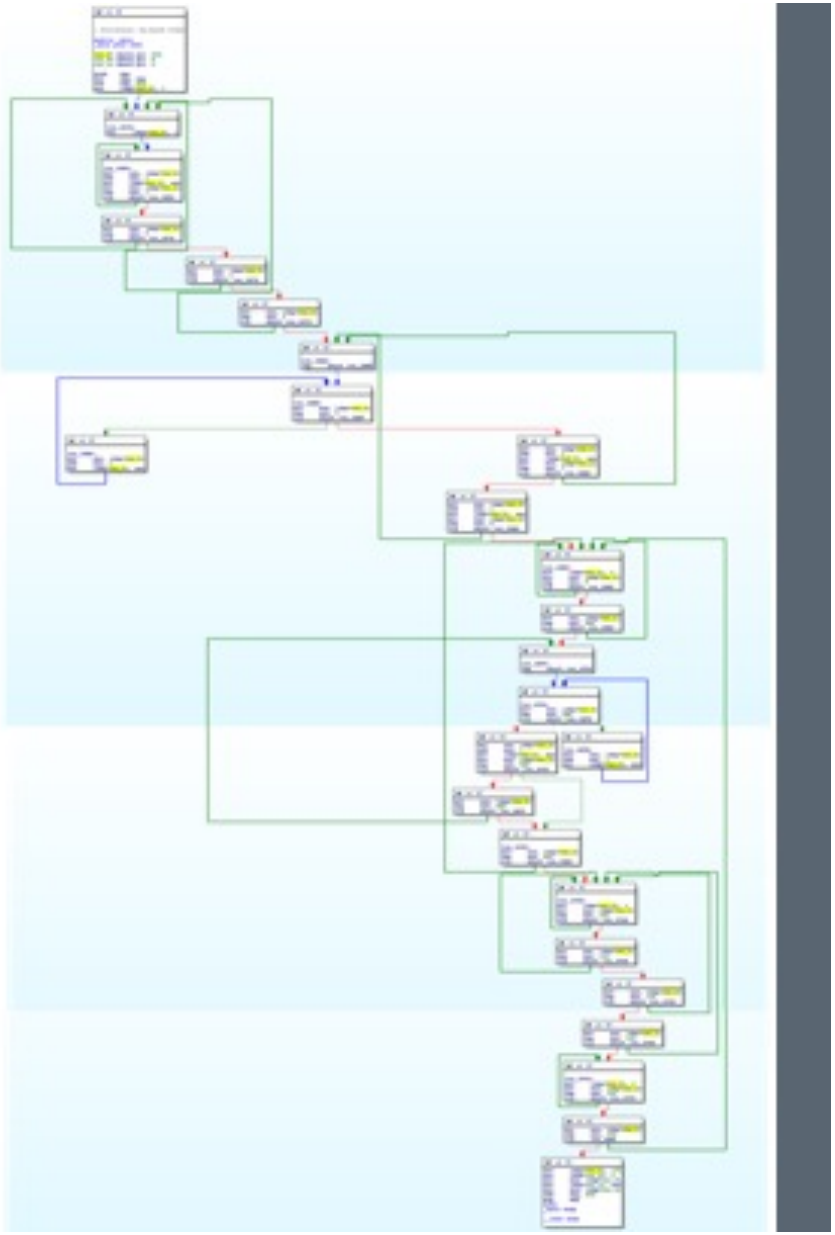
Proteção de SW: Marcas d'água

```
public void P(boolean S) {
    if (S)
        System.out.println("YES");
    else
        System.out.println("NO");
}

public void main (String args[]) {
    for (int i=1; i<args.length; i++) {
        if (args[0].equals(args[i])) {
            P(true);
            if (m4(3)<0)
                P(false);
            return;
        }
    }
    m3(-1);
    P(false);
}
```

```
public int bogus;
public int m4(int i) {
    i = i & 0x7BFF;
    bogus += 2;
    i -= i >> 2;
    do {
        if (i<-6)
            P(bogus<i);
        i = i >> 3;
        label: {
            if (++bogus <= 0) {
                i = i | 0x1000;
                m3(0);
                if ((bogus+=6)==0)
                    break label;
            }
            ++bogus;
            i = i * 88 >>> 1;
        }
        i = i | 0x4;
    } while (((bogus += 6)<0)
            && (m3(9)>=0) );
    bogus += 2;
    return i;
}
```

```
public int m3(int i) {
    i = i ^ i >> 0x1F;
    i = i / 4 * 3;
    do {
        i -= i >> 3;
        if((bogus += 11) <= 0)
            break;
```



Tarefas e temas de pesquisa

- Implementar e testar as várias metodologias de análise e proteção de software
- Desenvolver de novos métodos de análise e proteção de software
- Estudo de grafos de programas estruturados (para diversas definições de ”estruturado”)
- Usar grafos de programa para identificar ”plágio”
- Testar e comparar ferramentas SAST
- Construir bases de referência para SAST

Análise dinâmica de código

Cobertura de código para análise software e ensaios de proficiência

Biblioteca de cobertura de código

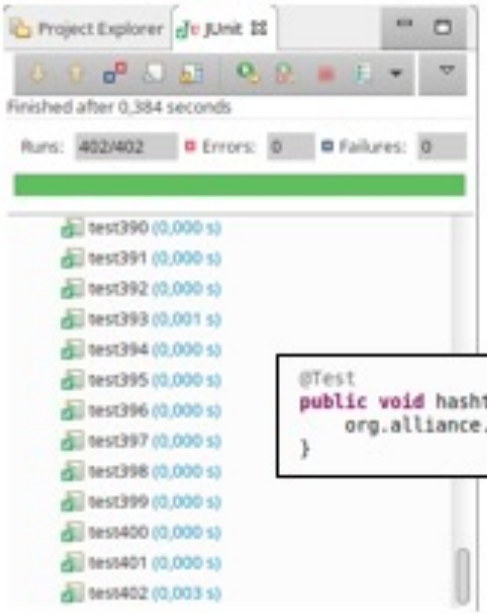
JaCoCo - linhas de código cobertas e não cobertas

```
    public void EVENT_addshare(ActionEvent a) throws Exception {
        Object[] pathParts = sharesTree.getSelectionPath().getPath();
        StringBuilder path = new StringBuilder();
        path.append(pathParts[1].toString());
        for (int i = 2; i < pathParts.length; i++) {
            path.append(pathParts[i].toString());
            path.append("/");
        }
        path.deleteCharAt(path.length() - 1);
        addNewSharePath(new File(TextUtils.makeSurePathIsMultiplatform(path.toString())));
    }

    private void addNewSharePath(File selectedDir) {
        if (selectedDir.exists() && selectedDir.isDirectory()) {
            String path = selectedDir.getAbsolutePath();
            for (int i = 0; i < shareListModel.getSize(); i++) {
                if (((Share) shareListModel.getElementAt(i)).getPath().equalsIgnoreCase(path)) {
                    return;
                }
            }
            Share share = new Share(path);
            share.setSgroupname(PUBLIC_GROUP);
            shareListModel.addElement(share);
        }
        while (removeDuplicateShare()) {
        }
        shareListHasBeenModified = true;
    }
```

JaCoCo - Visão geral de cobertura por classe

Element	Missed Instructions	Cov.	Missed Branches	Cov.
SharesWindow		68%		53%
SharesWindow new MouseAdapter() {...}		73%		50%
SharesWindow new KeyAdapter() {...}		22%		0%
SharesWindow new TreeExpansionListener() {...}		100%		91%
SharesListCellRenderer		100%		100%
SharesWindow new MouseAdapter() {...}		100%		75%
Total	292 of 1.183	75%	37 of 92	59%



Teste unitário para cobertura específica de código-fonte

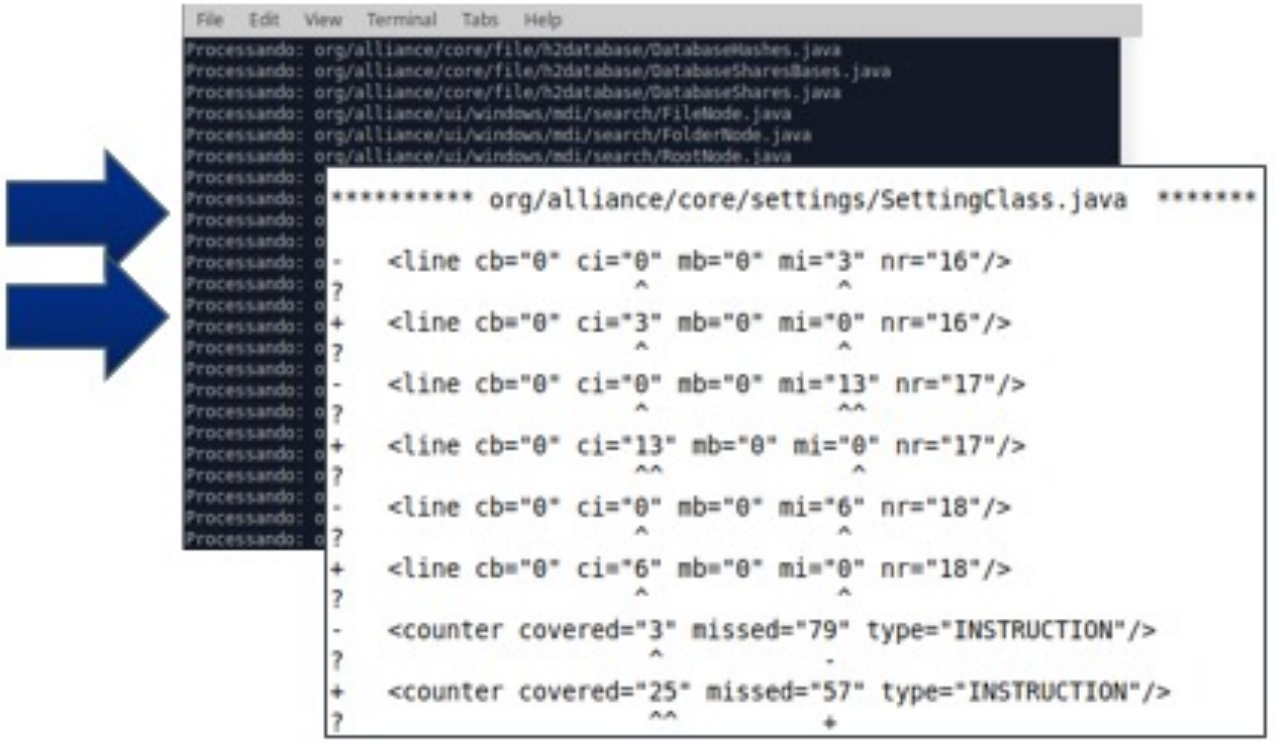
```
@Test
public void hashtest006() throws Throwable {
    org.alliance.core.file.hash.Hash hash1 = new org.alliance.core.file.hash.Hash("hiAA123456");
}
```

Hash.java

```
26
27    public Hash(String hash) {
28        this(Base64Encoder.fromBase64String(hash));
29    }
30
31    public Hash(byte[] hash) {
32        if (hash.length != HASH_SIZE) {
33            if (T.t) {
34                T.error("Incorrect hash size!!!");
35            }
36        }
37        this.hash = hash;
38    }
39
40    public byte[] array() {
41        return hash;
42    }
```

Exemplo do diff entre relatórios de cobertura (Inmetro x Laboratório)

Relatórios XML



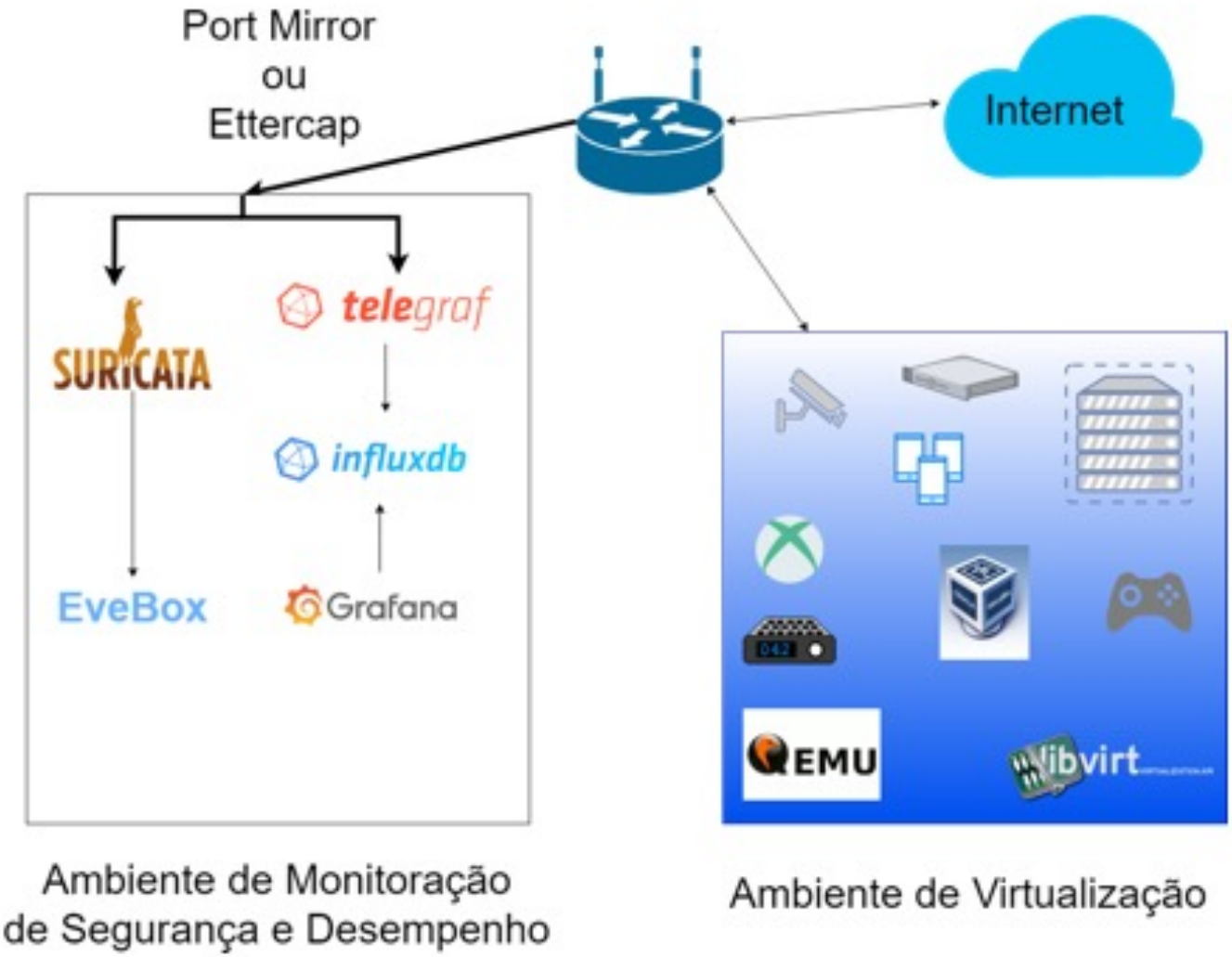
$$CC = \frac{|A \cap B| - |B - A|}{|A|}$$

Tarefas e temas de pesquisa

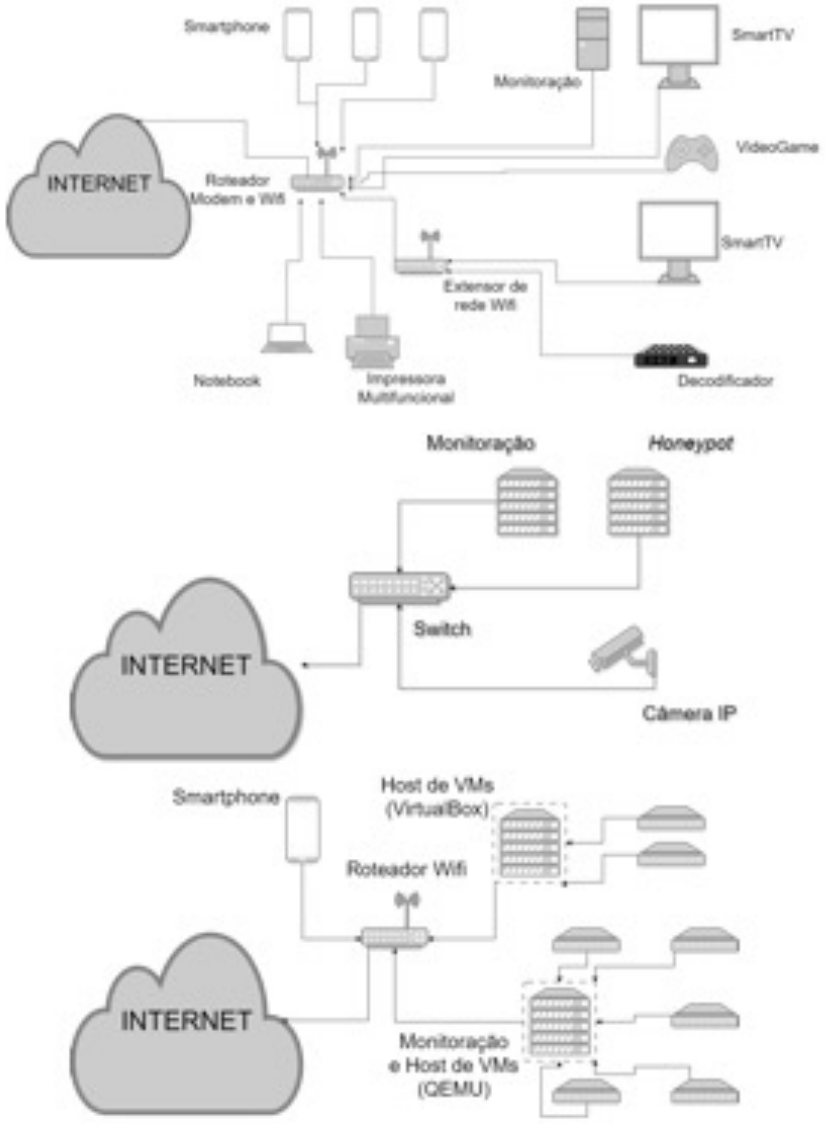
- Incluir aspectos de segurança no PEP
  - cobertura de código em funcionalidades relacionadas a segurança
  - testes que demandam exploração de falhas e vulnerabilidades
- Desenvolver modelos de PEP p/ produtos específicos
  - IDS/IPS/FW/etc.
- Automatizar e aumentar confiança com blockchains

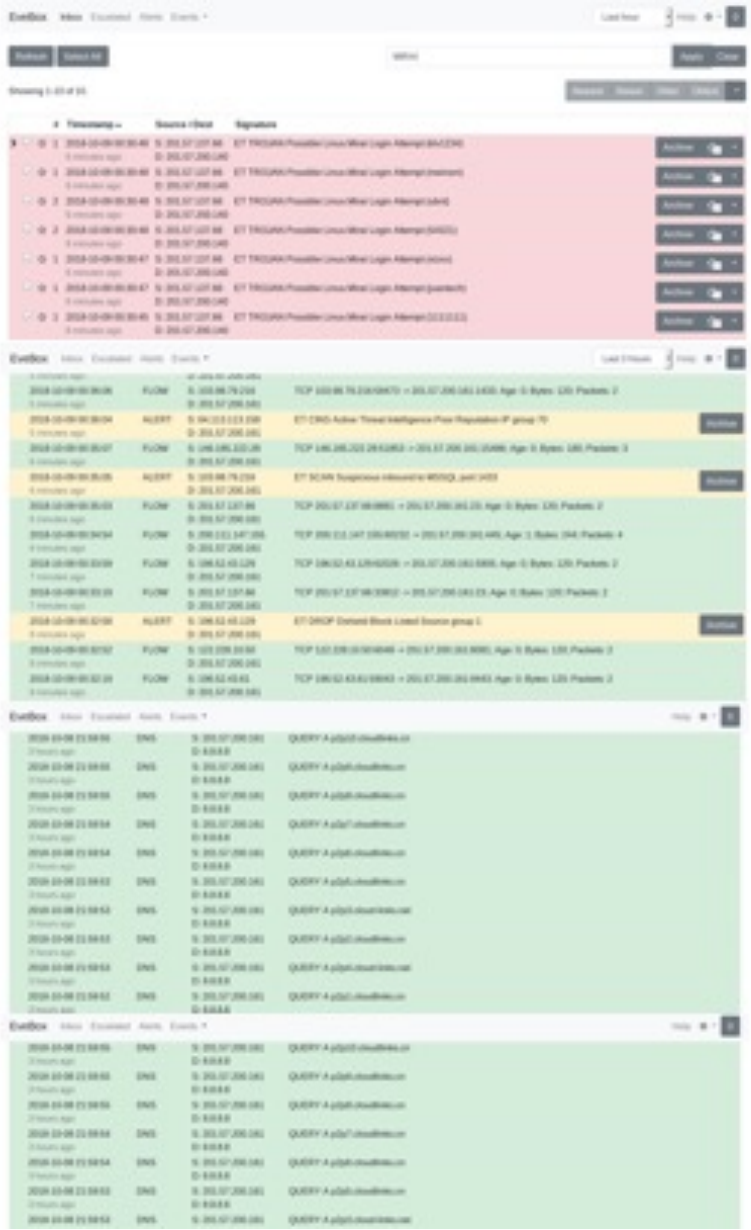
Testes de Caixa Preta em Ambientes Virtualizados

BlackBox TestBox - Arquitetura



BlackBox TestBox – Ensaios





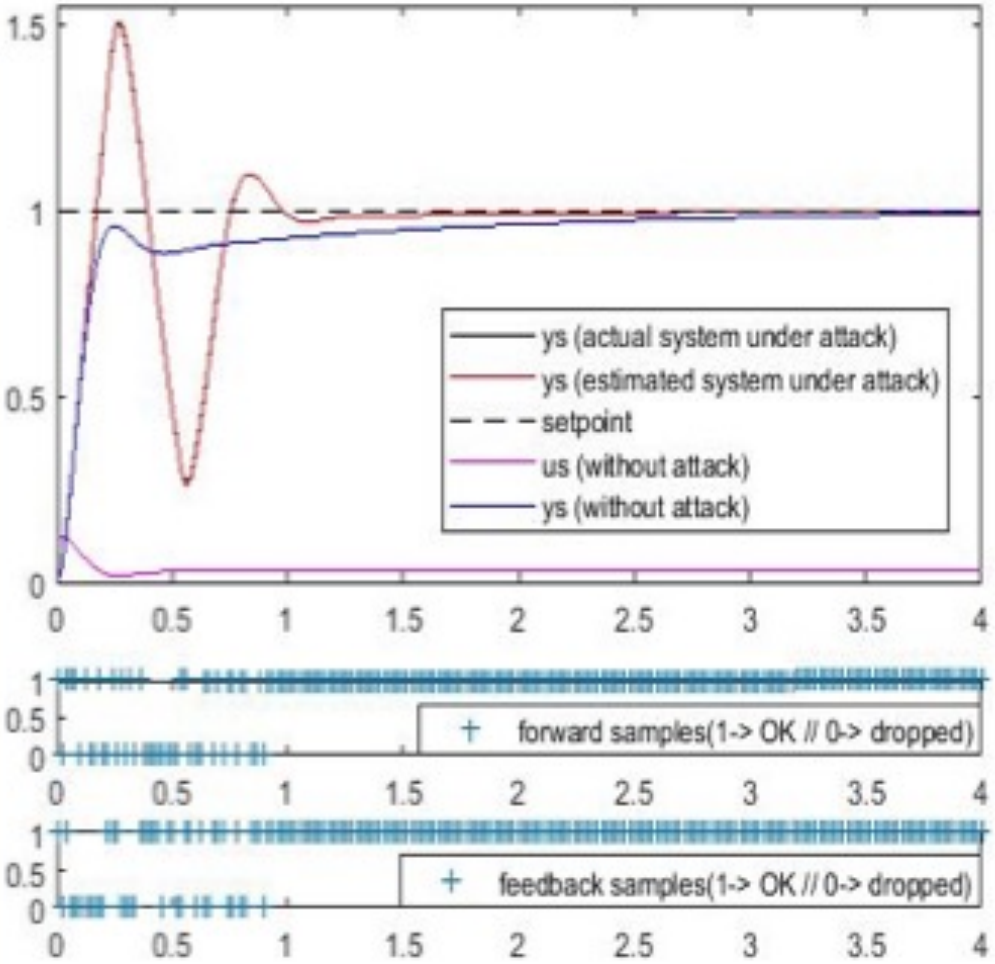
BlackBox TestBox – Monitoramento de Desempenho

Tarefas e temas de pesquisa

- Definição de metodologias para testes comportamentais
- Desenvolvimento de métodos de inteligência artificial para detecção de anomalias
- Identificação de vulnerabilidades em aplicações

Segurança de Sistemas Industriais em Rede

Ataque baseado em perdas de pacotes



INMETRO

UNIVERSITÀ DEGLI STUDI DI BRESCIA

UFF

Segurança de Sistemas Elétricos

INMETRO

UNIVERSITÀ DEGLI STUDI DI BRESCIA

uff

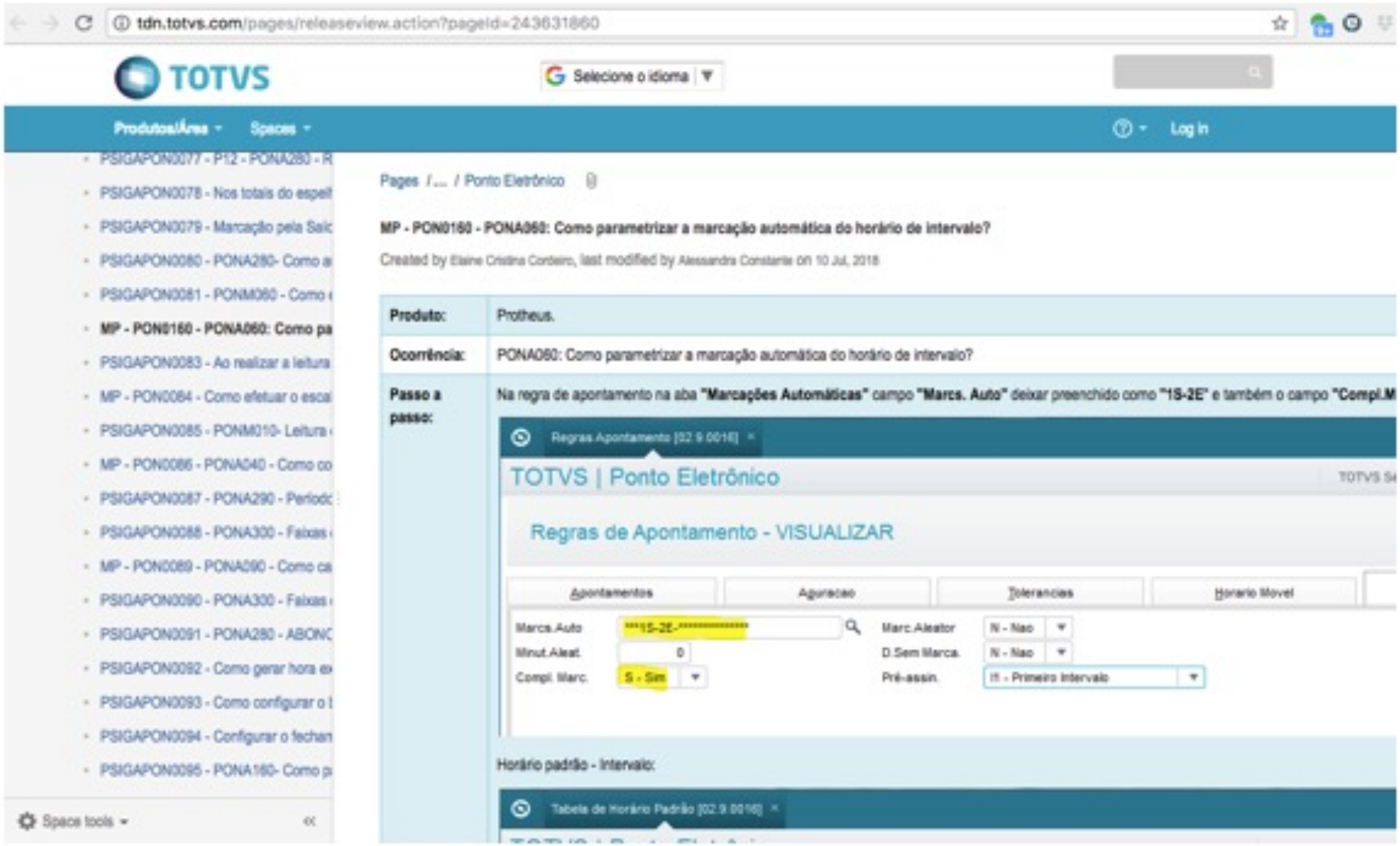
Tarefas e temas de pesquisa

- Estudo de novos modelos de ataque
- Estudo de novos tipos de sistemas de C&A
- Estudo de novos algoritmos de identificação
- Implementação de setups de teste

Análise de Riscos Cibernéticos em Aplicações Específicas e em Infraestruturas Críticas

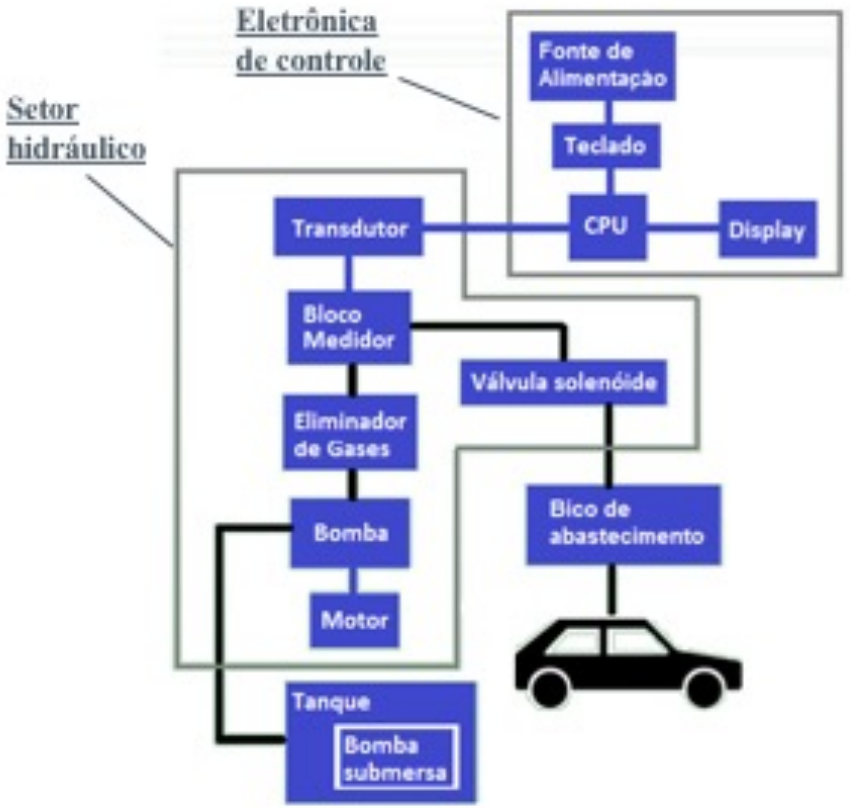
Registradores Eletrônicos de Ponto

Registradores Eletrônicos de Ponto

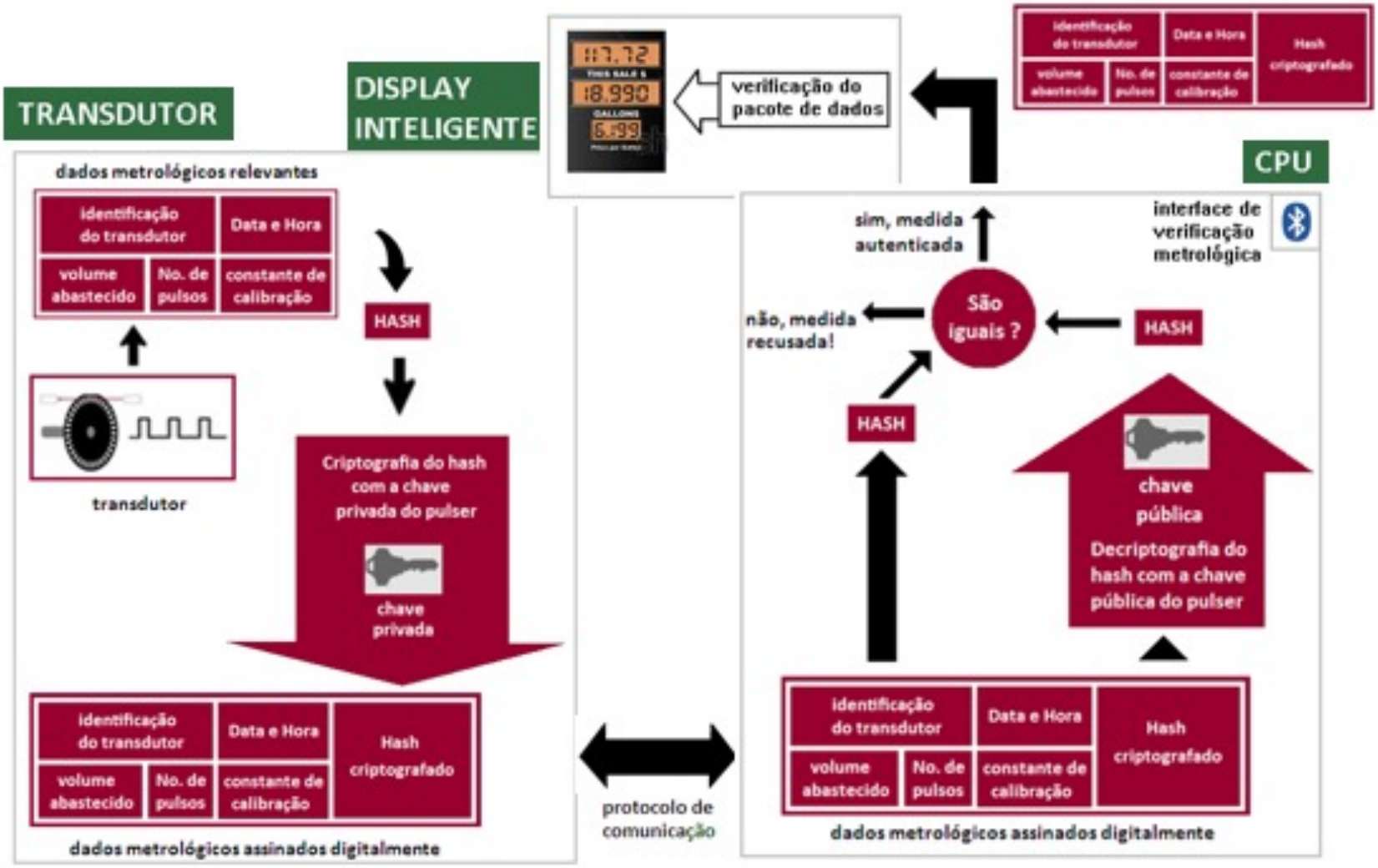


Bombas Medidoras de Combustível

Bombas Medidoras de Combustível



Bombas Medidoras de Combustível



Bombas Medidoras de Combustível

ITI
Instituto Nacional de Tecnologia da Informação

MAIS ACESSADOS

- CAR
- Credenciamento
- Navegadores
- Repositório
- Verificador

ASSUNTOS

- Auditoria ICP-Brasil
- Certificado Digital
- Comitê Gestor
- Consulta Pública
- Fiscalização
- Homologação
- ICP-Brasil
- Legislação
- Publicações Técnicas

Certificado Digital ICP-Brasil será usado para combater fraudes na venda de gasolina

Publicado: Sexta, 06 de Julho de 2018, 13h01 | Última atualização em Segunda, 09 de Julho de 2018, 16h55

Um novo tipo de certificado digital no padrão da Infraestrutura de Chaves Públicas Brasileiras – ICP-Brasil foi anunciado durante o 16º Certforum - Fórum de Certificação Digital. No painel "Certificado digital nas bombas de gasolina", o assessor técnico da presidência do ITI, Ruy Ramos, explicou que a novidade será destinada a objetos metrológicos aprovados pelo Inmetro.

Inicialmente, o novo certificado digital estará presente nas bombas de gasolina, mas poderá ser aplicado em outros equipamentos, como balanças e relógios medidores de energia elétrica. Avindo de parceria entre as duas entidades, o principal objetivo desse novo certificado é coibir fraudes ocorridas na venda de combustíveis.

De acordo com dados da Federação das Indústrias do Estado de São Paulo – Fiesp, o prejuízo pode chegar a R$ 200 bilhões apenas ao governo do estado de São Paulo por causa das fraudes em diversos setores da economia. Segundo explicitou o presidente do Inmetro Carlos Augusto de Azevedo, esta parceria com o ITI representa apenas o início do uso da certificação digital em conjunto com a metrologia neste combate. Azevedo disse que optou-se inicialmente pelas bombas de gasolina por elas serem um dos objetos mais fraudados no país.

Os palestrantes indicaram que a fraude metrológica se torna uma burla fiscal, problema grave para todo o país. Eles afirmaram que o papel dos institutos é justamente impedir que esses problemas aconteçam. "Esta união entre a certificação digital e Inmetro é um plano pioneiro do Brasil, ação histórica e projeto de vanguarda no mundo", afirmou o presidente do Inmetro. Este novo modelo de certificado digital para dispositivos ou objetos metrológicos deverá ter validade de 10 anos, requisição assinada por certificado do fabricante, hardware criptográfico certificado pelo Inmetro, entre outras características técnicas.

Segurança do Poder Marítimo

Poder Naval

Marinha Mercante

Infraestrutura Hidroviária

Abrangência do Poder Marítimo

Indústria Naval

Indústria Bélica Naval

Indústria da Pesca

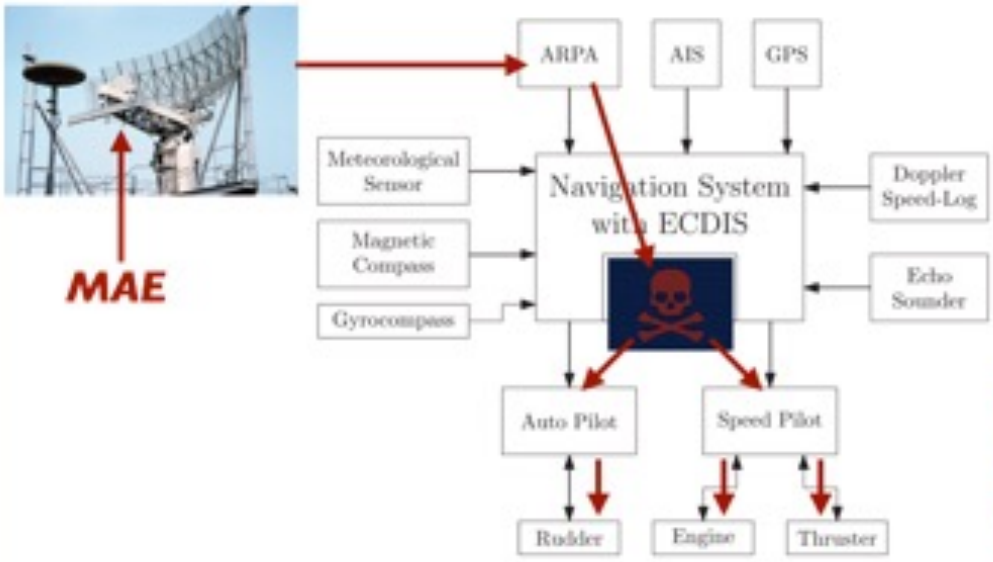
Meios de exploração do mar, leito e subsolo

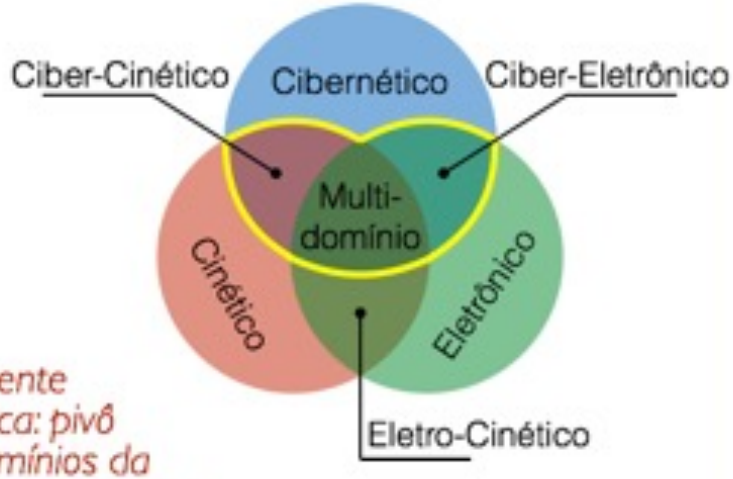
INMETRO

uff

Segurança do Poder Marítimo

› Inmetro + CIAW (MB) + EGN (MB)
  - Caracterização de vulnerabilidades em sistemas cibernéticos e híbridos do Poder Marítimo;
  - Estudo de políticas para mitigar vulnerabilidades.





Componente cibernética: pivô entre domínios da guerras eletrônica e cinética.

* de Sá, A. O., Machado, R. C. S., Almeida N. N. "O Encontro da Guerra Cibernética com as Guerras Eletrônica e Cinética no Âmbito do Poder Marítimo", Revista da Escola de Guerra Naval (aceito para publicação)

Tarefas e temas de pesquisa

- Análise de riscos e desenvolvimento de modelos de ataque em aplicações críticas

Monitoramento/sensoriamento por meio de redes oportunísticas orientadas a interesse

Monitoramento/sensoriamento por meio de redes oportunísticas orientadas a interesse

Coleta:
- Temperatura
- Umidade
- Presença

Geração:
- timestamp

Registro:
- eventos

Coleta de dados sensoriamento (Raspberry Pi)

Transporte de dados (drone)

Servidor

Base de dados com logs de eventos

UFRJ

INMETRO

Monitoramento/sensoriamento por meio de redes oportunísticas orientadas a interesse

Tarefas e temas de pesquisa

- Análise de segurança da comunicação com o Drone
- Estudo de protocolos de roteamento em redes ad-hoc com nós móveis
- Desenvolvimento de aplicações ”inteligentes” com base em sensoriamento

Blockchains para aplicações de Metrologia, Qualidade e Segurança

Rede Blockchain de Metrologia e Qualidade

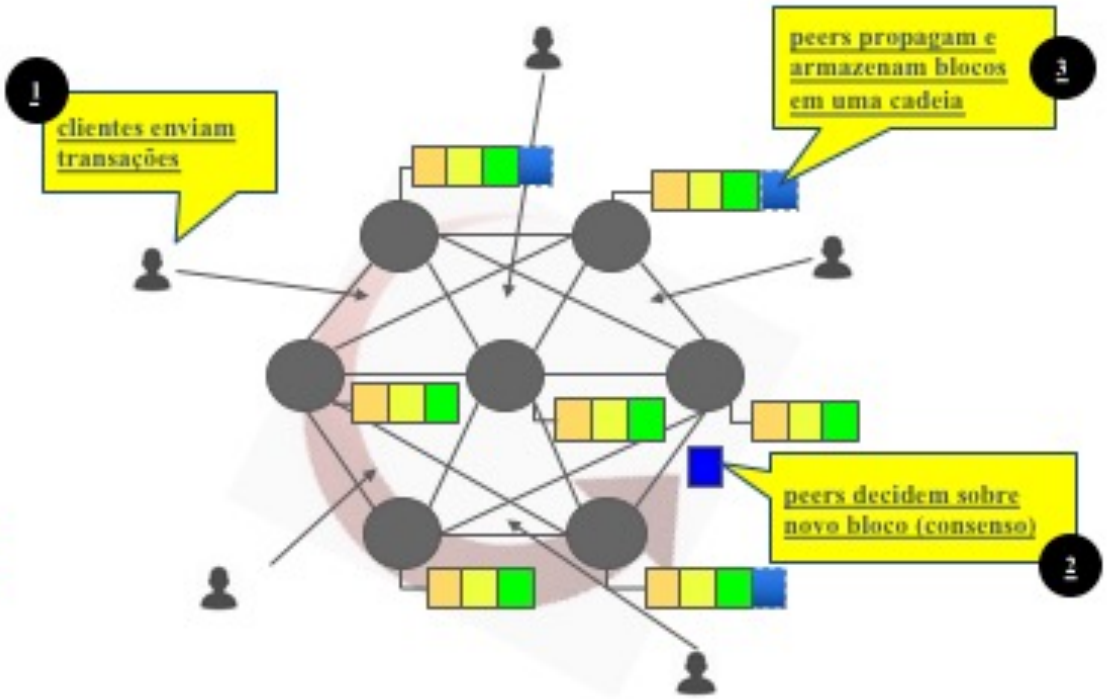
INMETRO

PTB
Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin

Ciências ULisboa
LASIGE

UFRJ

LabNet



PUCPR

NMIJ

uff
Instituto de Computação

IRD

Tarefas e temas de pesquisa

- Implementar nó IC/UFF na rede de blockchains
- Desenvolver aplicações baseadas em blockchains