SCML/16

SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

Raphael Machado

Inmetro

#SCML2016

Segurança de Dispositivos Inteligentes: Especificação de Requisitos e Avaliação da Conformidade

Raphael Machado

Inmetro

#SCML2016

Agenda

- Requisitos de Segurança
- Avaliação da Conformidade
- Acreditação de Laboratórios
- Temas de Pesquisa
- Considerações finais

Sobre o palestrante

SCML/16
SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

- Pesquisador-Tecnologista em Metrologia e Qualidade, chefe substituto do Laboratório de Informática da Diretoria de Metrologia Científica do Inmetro
- Atuação desde 2008 com avaliações de segurança de dispositivos inteligentes (mais de uma centena de notas técnicas e relatórios de ensaio)
- D.Sc. Engenharia de Sistemas e Computação (PESC/COPPE/UFRJ, 2010)
- Bolsista de Produtividade em Pesquisa (CNPq/PQ-2)
- Jovem Cientista do Nosso Estado (FAPERJ)
- Mais de 80 artigos publicados em periódicos e anais de conferências
- Coordenador de mais de uma dezena de projetos de pesquisa e desenvolvimento (CNPq/FAPERJ/Finep)
- Docente permanente do PPGMQ-Inmetro e do PPGCC-CEFET/RJ

SCML/16
SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

Segurança da Informação e de Proteção de Software

Especficando Requisitos e Definindo Regulamentos

SIBRAPEM

INMETRO

Necessidade de requisitos de segurança

SCML/16
SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

- Dispositivos computacionais em todo lugar
  - Internet das coisas, computação ubíqua, e outras buzzwords
- Dispositivos computacionais controlando sistemas críticos
  - Smart grids, cyber-phisical systems, e outras buzzwords
- Diversos cenários de ataque, diversas motivações
  - Cyber-war, cyber-espionage, cyber-crime, cyber-fraud…
- Segurança quase nunca é vista como *feature* – geralmente, é custo:-(
  - Apenas quando uma falha ocorre
- Importante especificar claramente os requisitos de segurança
  - Especialmente quando o bem-estar da sociedade está envolvido

Ataques cibernéticos...

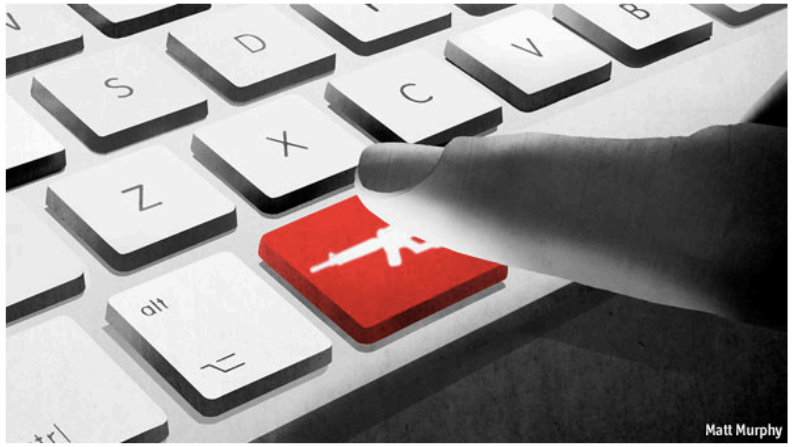
SCMU/16
SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

Cyberwar

War in the fifth domain

Are the mouse and keyboard the new weapons of conflict?

Jul 1st 2010 | From the print edition | Timekeeper | Like 561 | Tweet



AT THE height of the cold war, in June 1982, an American early-warning satellite detected a large blast in Siberia. A missile being fired? A nuclear test? It was, it seems, an explosion on a Soviet gas pipeline. The cause was a malfunction in the computer-control system that Soviet spies had stolen from a firm in Canada. They did not know that the CIA had tampered with the software so that it would "go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds," according to the memoirs of Thomas Reed, a former air force secretary. The result, he said, "was the most monumental non-nuclear explosion and fire ever seen from space."

ANNALS OF WAR

SEPTEMBER 17, 2012 ISSUE

THE SILENT STRIKE

How Israel bombed a Syrian nuclear installation and kept it secret.

BY DAVID MAKOVSKY

The Mossad extracted evidence of the nuclear site from the computer of a Syrian official.
PHOTOILLUSTRATION BY DAN WINTERS.

In the first days of March, 2007, agents from the Mossad, the Israeli intelligence agency, made a daring raid on the Vienna home of Ibrahim Othman, the head of the Syrian Atomic Energy Commission. Othman was in town attending a meeting of the International Atomic Energy Agency's board of governors, and had stepped out. In less than an hour, the Mossad operatives swept in, extracted top-secret information from Othman's computer, and left without a trace.

Cyberwar

The meaning of Stuxnet

A sophisticated "cyber-missile" highlights the potential—and limitations—of cyberwar

Sep 30th 2010 | From the print edition | Timekeeper | Like 265 | Tweet

IT HAS been described as "amazing", "groundbreaking" and "impressive" by computer-security specialists. The Stuxnet worm, a piece of software that infects industrial-control systems, is remarkable in many ways. Its unusual complexity suggests that it is the work of a team of well-funded experts, probably with the backing of a national government, rather than rogue hackers or cyber-criminals (see article). It is designed to infect a particular configuration of a particular type of industrial-control system—in other words, to disrupt the operation of a specific process or plant. The Stuxnet outbreak has been concentrated in Iran, which suggests that a nuclear facility in that country was the intended target.

SIBRAPEM

INMETRO

Fraude...

Regulação “inteligente”

[…] in favor of “smart regulation” of some aspects of cyber security […] The smart part was the idea of government regulators specifying goals, rather than micromanaging by dictating means. (Richard Clarke, CyberWar)

- Especificar objetivos, não soluções: “escolha possível”
  - Vantagem: mantém a liberdade de criação de desenvolvedores (independência de tecnologia)
  - Desvantagem: não é evidente quando uma solução é aceitável; regras do jogo tornam-se mais nebulosas
- Qual a responsabidade do desenvolvedor por não-conformidade?
- Qual a responsabidade do usuário-proprietário por eventual falha?

Requisitos de segurança

- **Requisitos de aplicação – funcionalidades**
- Controle de acesso e identificação de usuários
- Integridade de dados e software
- Responsabilidade/irrefutabilidade
- Disponibilidade
- Confidencialidade/privacidade

Requisitos de segurança

- Requisitos de aplicação – funcionalidades
- **Controle de acesso e identificação de usuários**
- Integridade de dados e software
- Responsabilidade/irrefutabilidade
- Disponibilidade
- Confidencialidade/privacidade

Requisitos de segurança

- Requisitos de aplicação – funcionalidades
- Controle de acesso e identificação de usuários
- **Integridade de dados e software**
- Responsabilidade/irrefutabilidade
- Disponibilidade
- Confidencialidade/privacidade

Requisitos de segurança

- Requisitos de aplicação – funcionalidades
- Controle de acesso e identificação de usuários
- Integridade de dados e software
- **Responsabilidade/irrefutabilidade**
- Disponibilidade
- Confidencialidade/privacidade

Requisitos de segurança

- Requisitos de aplicação – funcionalidades
- Controle de acesso e identificação de usuários
- Integridade de dados e software
- Responsabilidade/irrefutabilidade
- **Disponibilidade**
- Confidencialidade/privacidade

Requisitos de segurança

- Requisitos de aplicação – funcionalidades
- Controle de acesso e identificação de usuários
- Integridade de dados e software
- Responsabilidade/irrefutabilidade
- Disponibilidade
- **Confidencialidade/privacidade**

Avaliação da Conformidade e Certificação de Segurança

Como garantir que um dispositivo atende a requisitos de segurança.

Desafio da avaliação da conformidade

SCML/16
SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

- Avaliação de segurança ainda não é perfeitamente objetiva
  - Existe “zona cinza”, especialmente se não são especificadas soluções aceitáveis
- Avaliação de segurança busca “caso de falha”
  - “Engenhosidade” na busca por falhas
  - “Experiência” do avaliador é relevante
  - Ensaio apenas evidencia não-conformidade

Tipos de ensaio

- Consistência de documentação, software e hardware
- Análise de documentação (arquitetura de segurança)
- Análise estática de código fonte (garantia de projeto)
- Análise estática de código binário
- Análise dinâmica de software
- Testes de funcionalidade
- Testes de hardware (não-invasivos/semi-invasivos/invasivos)
- Testes de segurança
- Testes de criptografia…

Testes de criptografia/arquitetura

SCML/16
SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

- Identificação dos casos de uso de criptografia
- Segurança por obscurantismo
- Algoritmos criptográficos vulneráveis
- Primitivas criptográficas incorretas
- Algoritmos não-criptográficos para funções de dispersão
- Algoritmos não-criptográficos para pseudo-aleatoriedade
- Reutilização de nonce
- Chave criptográfica de tamanho inadequado
- Fonte de entropia/aleatoriedade inadequada

SCML/16
SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

Infraestrutura de avaliação da conformidade

Acreditando laboratórios e reconhecendo competências

SIBRAPEM

INMETRO

Importância de uma rede de laboratórios

SCML/16
SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

- Especialização da atividade de avaliação de segurança
  - Elevado volume de avaliações
  - Velocidade na evolução das metodologias
  - Necessidade de independência e imparcialidade
- Demanda de avaliação por diversos setores da sociedade
  - Governo (Regulador, Compras públicas)
  - Empresas (Segurança dos sistemas internos, Gestão de aquisição)
  - Sociedade civil (privacidade), judiciário (forense) etc.
- Fomentar competência em Segurança deve ser ação de Estado

Desafio da acreditação de laboratórios

SCML/16
SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

- Ensaios de Segurança ainda não são completamente “sistemáticos”
- Aspectos mais relevantes da 17025
  - **Métodos**
  - **Recursos humanos**
- Outros aspectos
  - Condições ambientais (segurança física)
  - Equipamentos

SIBAPEM

INMETRO

Notícias do *front*

- Já existem Programas de Avaliação da Conformidade em Segurança da Informação que prevêem avaliação por laboratórios privados
  - Registrador Eletrônico de Ponto
  - Equipamentos da ICP-Brasil
  - Sistema de contagem de passageiros (transporte público)
- Já existem laboratórios privados atuando na área
- Pelo menos uma dúzia de laboratórios privados com competência e interesse em atuar na área

Papel do Inmetro

SCML/16
SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

- Gerir a rede de laboratórios, buscando sua sustentabilidade
- Estimular o uso de um arcabouço comum (normalizado) de requisitos e metodologias de avaliação da conformidade
- Fomentar o desenvolvimento de recursos humanos e competências
- Desenvolver pesquisas (básicas e aplicadas) em Segurança
- Aprimorar metodologias de avaliação de segurança
- Ser uma “referência” para os laboratórios
  - Auditorias
  - Treinamento
  - Intercomparações
  - Disponibilização de padrões...

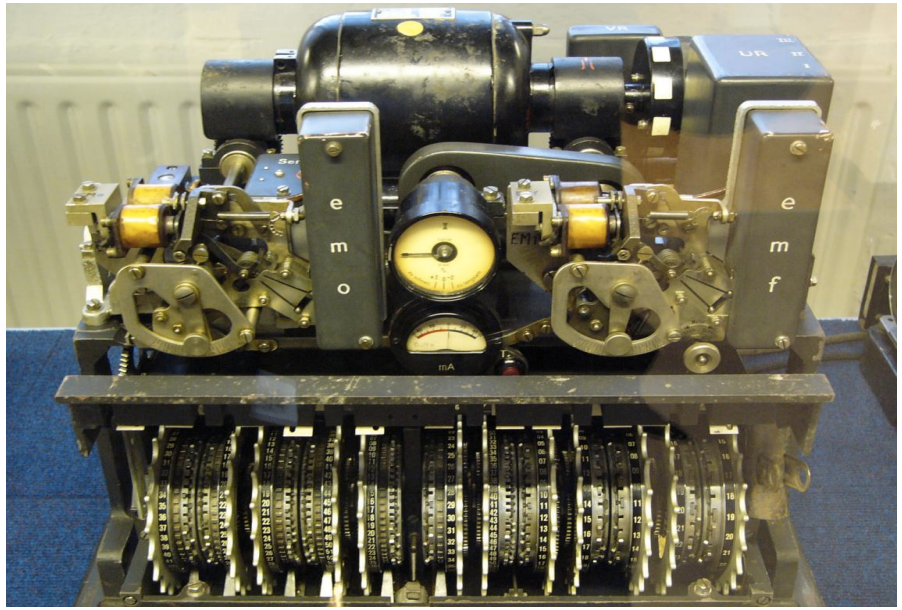
Temas de pesquisa

Mantendo-se alinhado às tendências

Criptografia e arquiteturas de segurança

SCML/16
SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

- Quão seguros são os atuais algoritmos (padrões) criptográficos
- Quais modelos de ataque são plausíveis
  - Criptografia quântica ?
  - Dados massivos ?
  - …

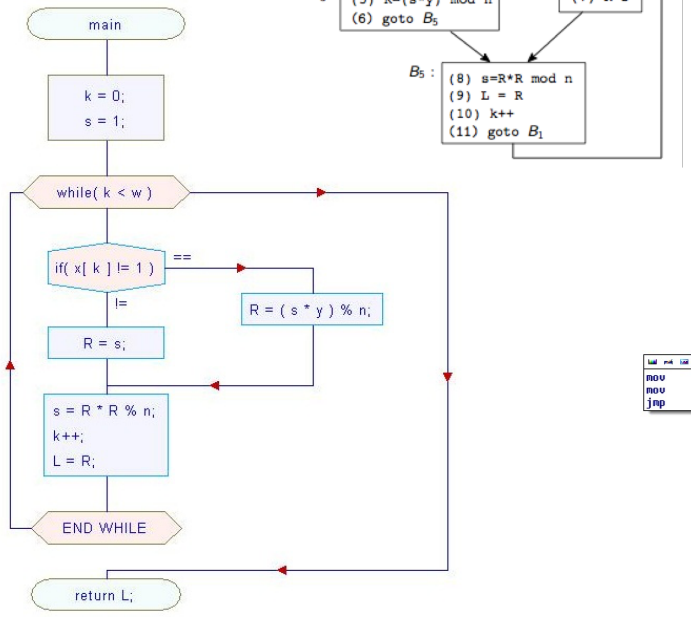


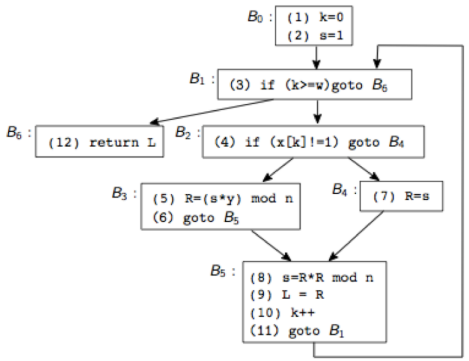
SIBAPEM

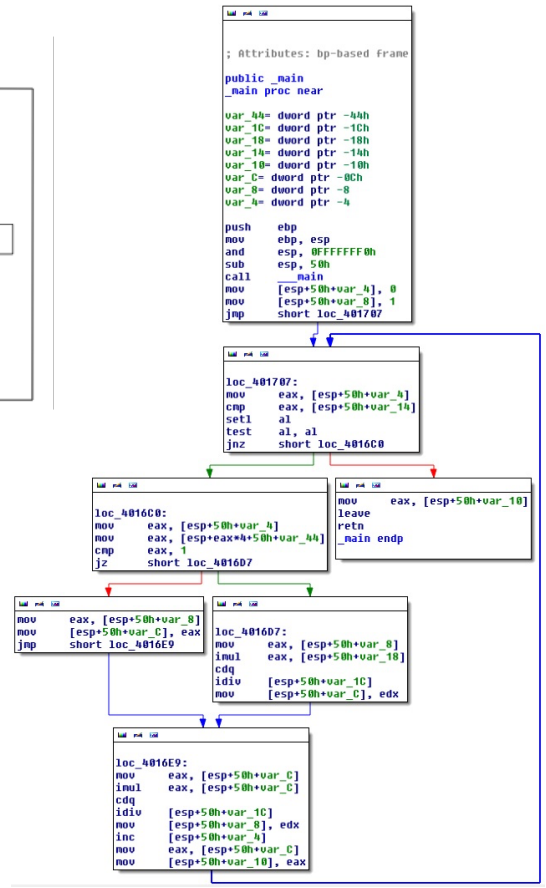
INMETRO

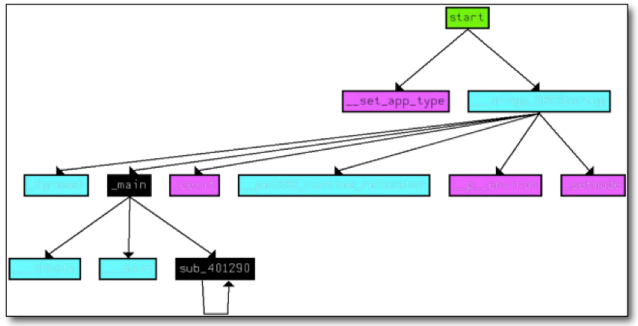
Análise de código

- Como garantir o comportamento de um software a partir de seu código?

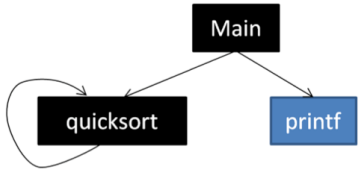




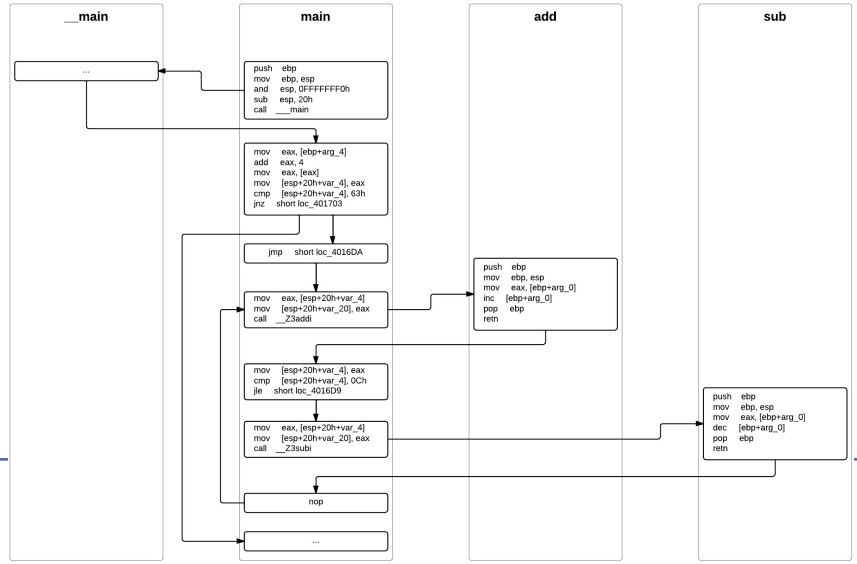




Código Binário



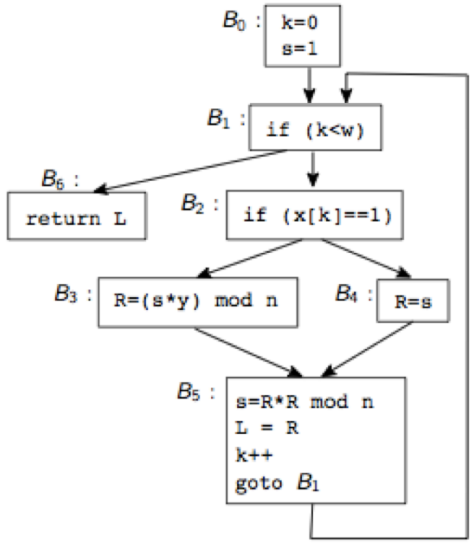
Código Fonte

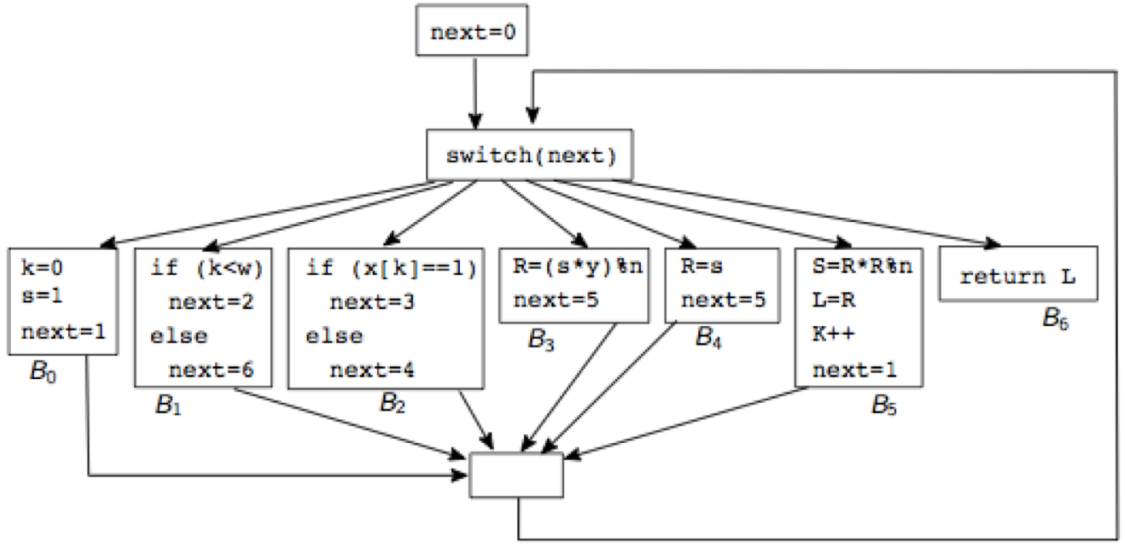


Ofuscação de código

- Como dificultar o entendimento do código de um software

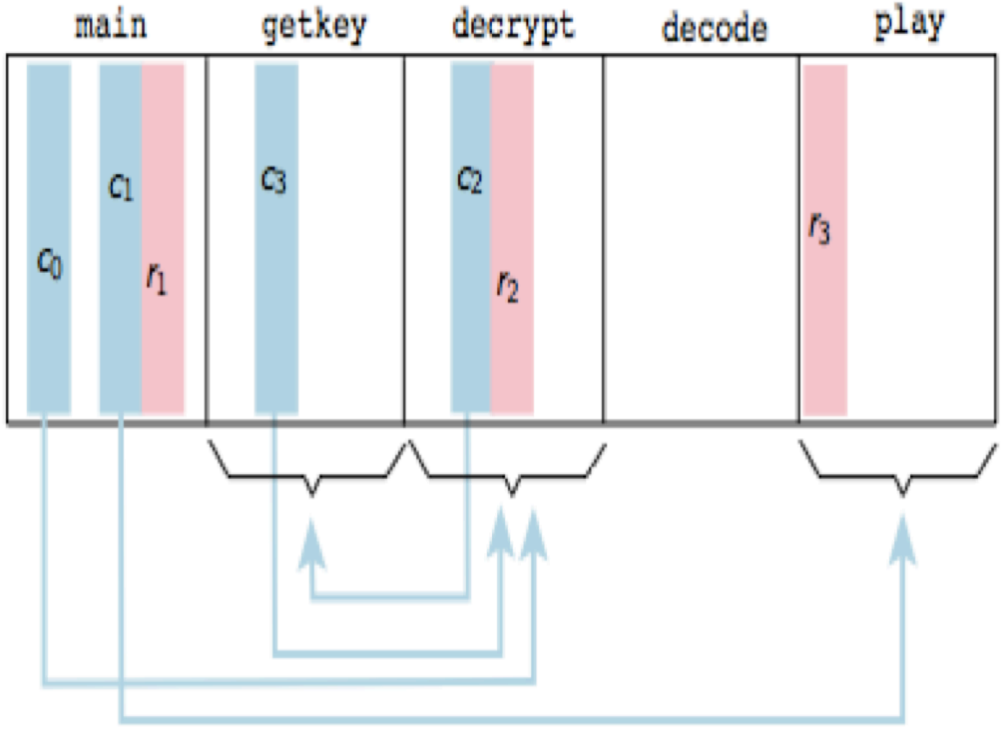
```
int modexp(int y,int x[],
           int w,int n) {
   int R, L;
   int k = 0;
   int s = 1;
   while (k < w) {
      if (x[k] == 1)
         R = (s*y) % n;
      else
         R = s;
      s = R*R % n;
      L = R;
      k++;
   }
   return L;
}
```

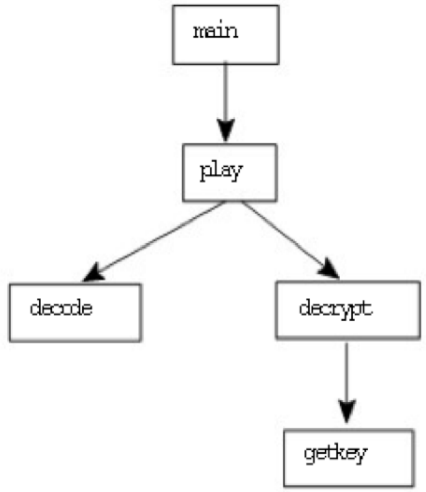


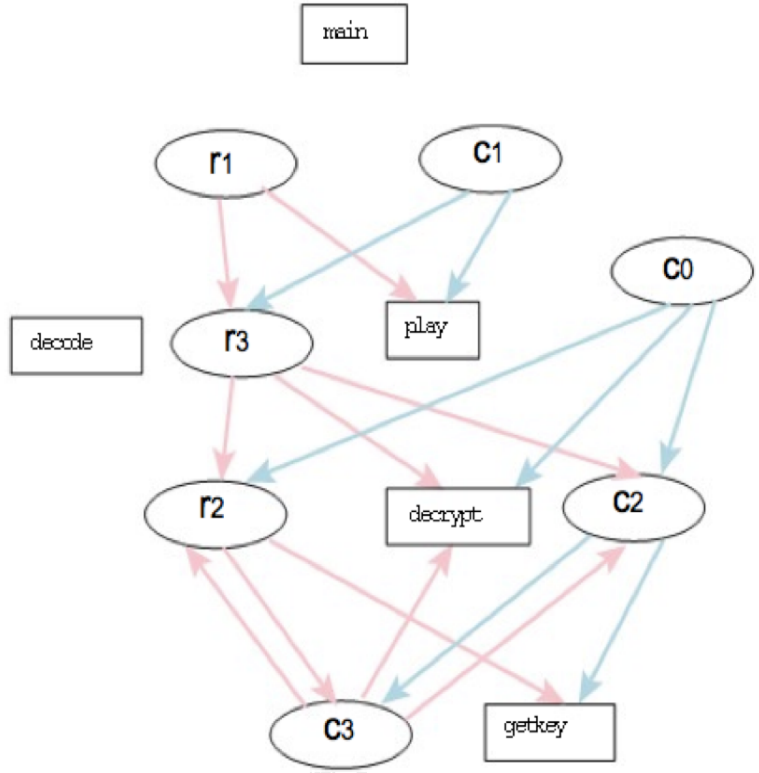


Incorruptibilidade de software

- Garantindo que o software se recupera de adulterações



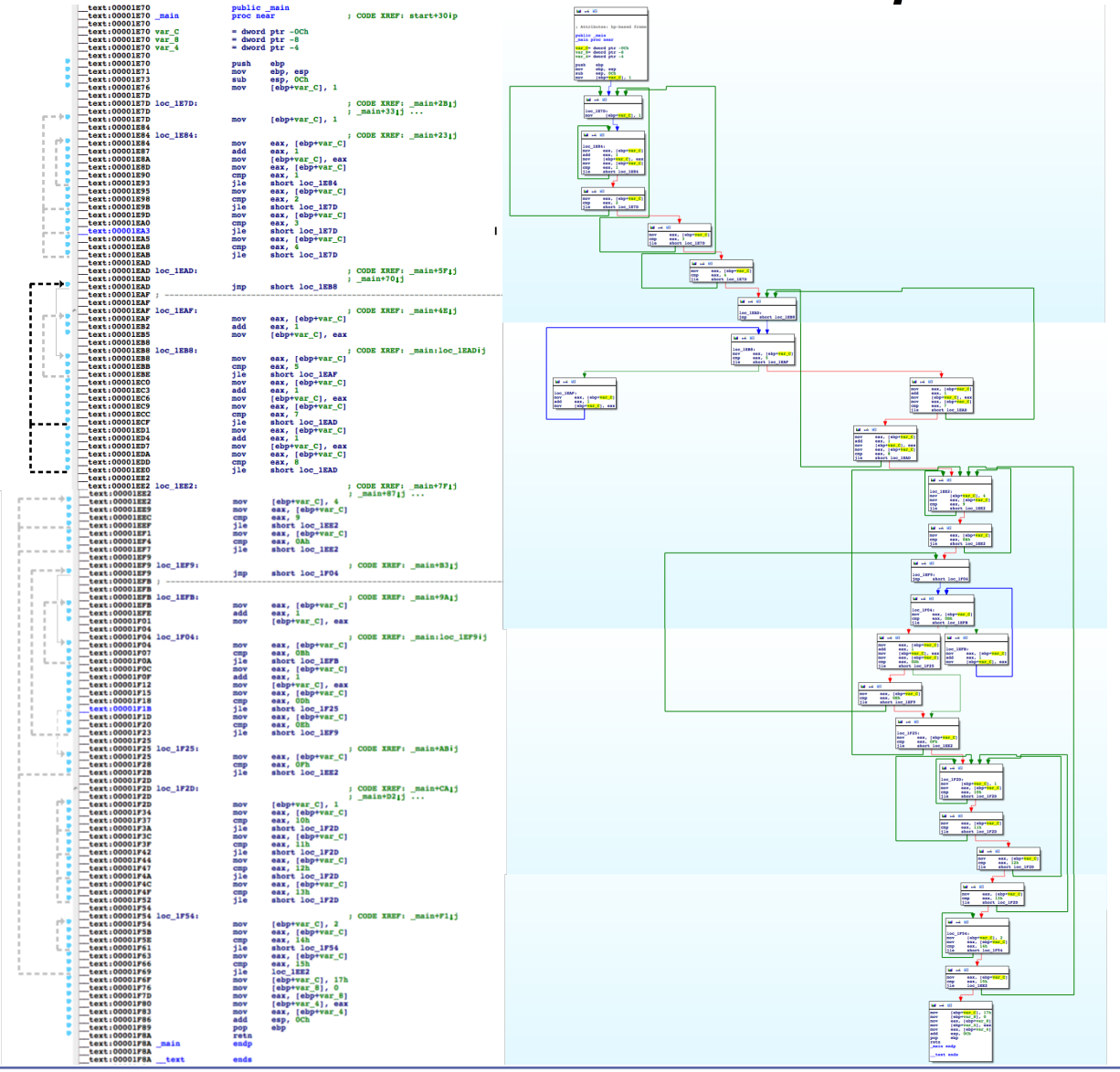




Marcas d'água

- Imersão de informação em software
- Proteção da propriedade intelectual

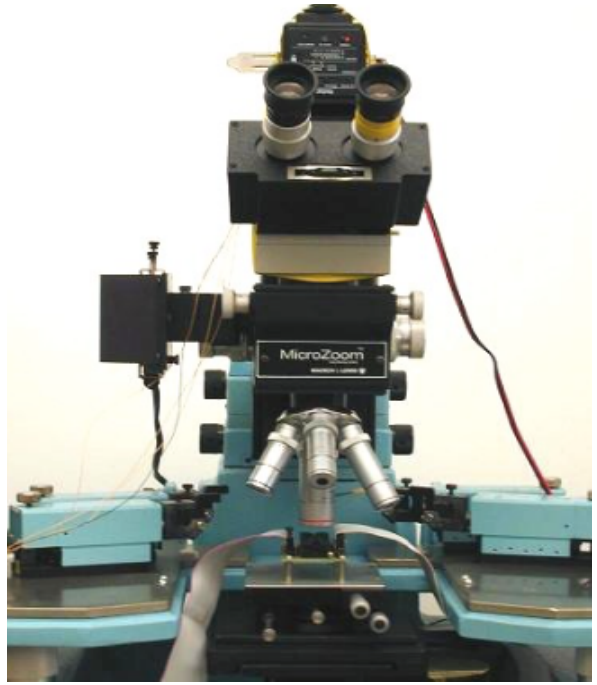
```
CodecMaceio3.py – /Users/vigusmao/Dropbox/UFRJ/Problemas/Presentes/Watermarking/ReedSolomon/CodecMaceio3.py

watermark = [None] * 4

*Python Shell*

Please type the key (<enter> to quit): 198765
B = 110000100001101101 (n = 18)

Watermark:

      1<<  1<<    |  1<<    |  6<<  6<<    |   6<<      |  11<<            |          13<<  11<<  11<<      |       |
   1--->2--->3--->4--->5--->6--->7--->8--->9--->10--->11--->12--->13--->14--->15--->16--->17--->18--->19--->20
                                                        >>15        >>17

Testing decoding procedure...
Retrieved key = 198765
Watermark decoded successfully.

========================================

Please type the key (<enter> to quit): 198765
B = 110000100001101101 (n = 18)

Watermark:

      1<<    |    |  3<<    |  6<<    |    |   8<<      |  11<<            |          15<<  13<<            |       |
   1--->2--->3--->4--->5--->6--->7--->8--->9--->10--->11--->12--->13--->14--->15--->16    17--->18--->19--->20
                                                        >>15        >>17              >>20

Testing decoding procedure...
Retrieved key = 198765
Watermark decoded successfully.

========================================

Please type the key (<enter> to quit): 198765
B = 110000100001101101 (n = 18)

Watermark:

      1<<  1<<    |  1<<    |  6<<  6<<  1<<     |      |  11<<  10<<  10<<  10<<          |       |       |
   1--->2--->3--->4--->5--->6--->7--->8--->9--->10--->11--->12--->13--->14--->15--->16--->17--->18--->19--->20
                                                                          >>18        >>20

Testing decoding procedure...
Retrieved key = 198765
Watermark decoded successfully.

========================================
```

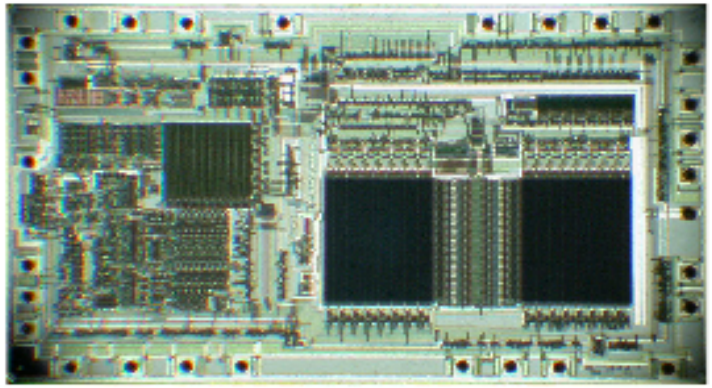


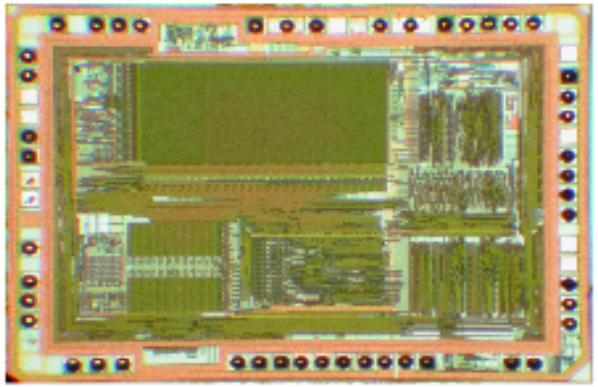
Segurança por hardware

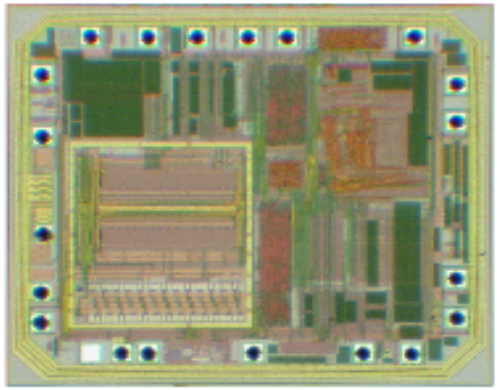
SCML/16
SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL

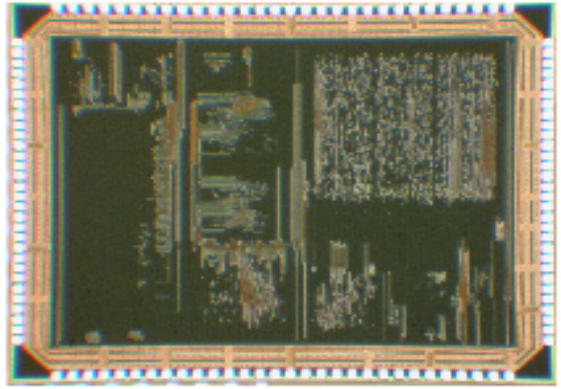
- Quão bem o hardware protege chaves criptográficas e outros segredos
- É possível modificar o software embarcado por meio de ataques de hardware?
- Ataques invasivos, semi-invasivos e invasivos
- Questão da cadeia de suprimentos




MC68HC705P6A, 1 µm


PIC16F77, 0.5 µm


MSP430F1121A, 0.35 µm


XAP Springbank, 0.18 µm

SIBAPEM

INMETRO

Considerações finais

Preparando-se para o almoço

WRAC+

- WRAC+ : Workshop de Regulação, Avaliação da Conformidade e Certificação de Segurança
- Satélite do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)
- Objetivo: discutir os diversos aspectos da avaliação da conformidade na área de Segurança da Informação e de Sistemas Computacionais.
- Público: Reguladores, Organismos de Certificação, Laboratórios, Governo, Academia e Indústria

SIBAPEM

INMETRO

Próximos passos

- Regulamentos com requisitos de Segurança da Informação
  - Regulamentos técnicos próprios
  - Atuação junto a outros órgãos de governo
- Metodologias de avaliação de Segurança
  - Pesquisa e desenvolvimento de métodos
  - Desenvolvimento e especificação de padrões
- Laboratórios atuando em Segurança da Informação
  - Auditorias
  - Treinamento
  - Intercomparações

Obrigado!

Raphael Machado

rcmachado@inmetro.gov.br

SCML/16

SEGURANÇA CIBERNÉTICA EM METROLOGIA LEGAL