Requisitos de software para Medidores de Umidade de Grãos

Bruno Erthal

Pesquisadores-Tecnologista em Metrologia e Qualidade

Apresentação

- Contextualização
- Conceitos Básicos de Segurança de Software
- Segurança de Software em Medidores de Umidade e Grãos

Contextualização

Evolução do Instrumentos

Contextualização

Metrologia Legal

Contextualização

Inmetro especifica, insere requisitos de software e aprova modelos de MUG

- para assegurar adequada metrologia;
- para assegurar integridade do software aprovado;
- para avaliar segurança de TI.

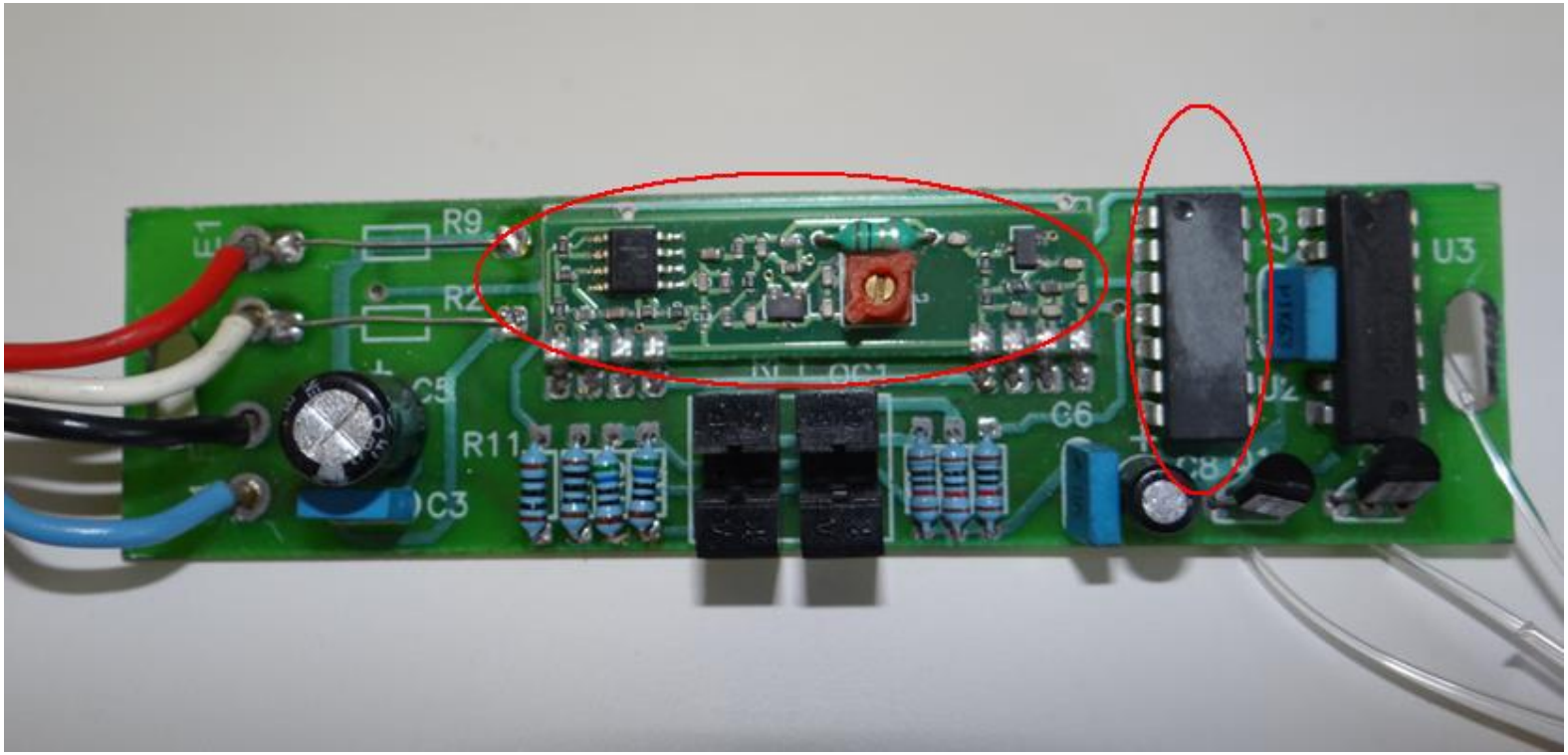
Contextualização

Escândalo de emissões da Volkswagen

Fraude intencional no software para burlar emissões de poluentes quando em modo de teste;

Contextualização

Exemplo de Fraude em Bomba de Combustível



Atributos básicos da segurança da informação

- Confidencialidade: propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação
- Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (Corrente, intermediária e permanente).
- Disponibilidade: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;
- Autenticidade: propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo;
- Irretratabilidade ou não repúdio: propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita;
- Conformidade: propriedade que garante que o sistema deve seguir as leis e regulamentos associados a este tipo de processo.

Função Hash

Uma função *hash* é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo (resumo), com as seguintes propriedades:

- Não é viável a partir de um código *hash* retornar ao bloco de dados original;
- Não é viável encontrar dois blocos que gerem o mesmo código *hash*.
- Qualquer alteração no dados devem gerar um *hash* completamente novo.

Exemplo função resto

A base para entender a função hash é o resto de uma divisão.

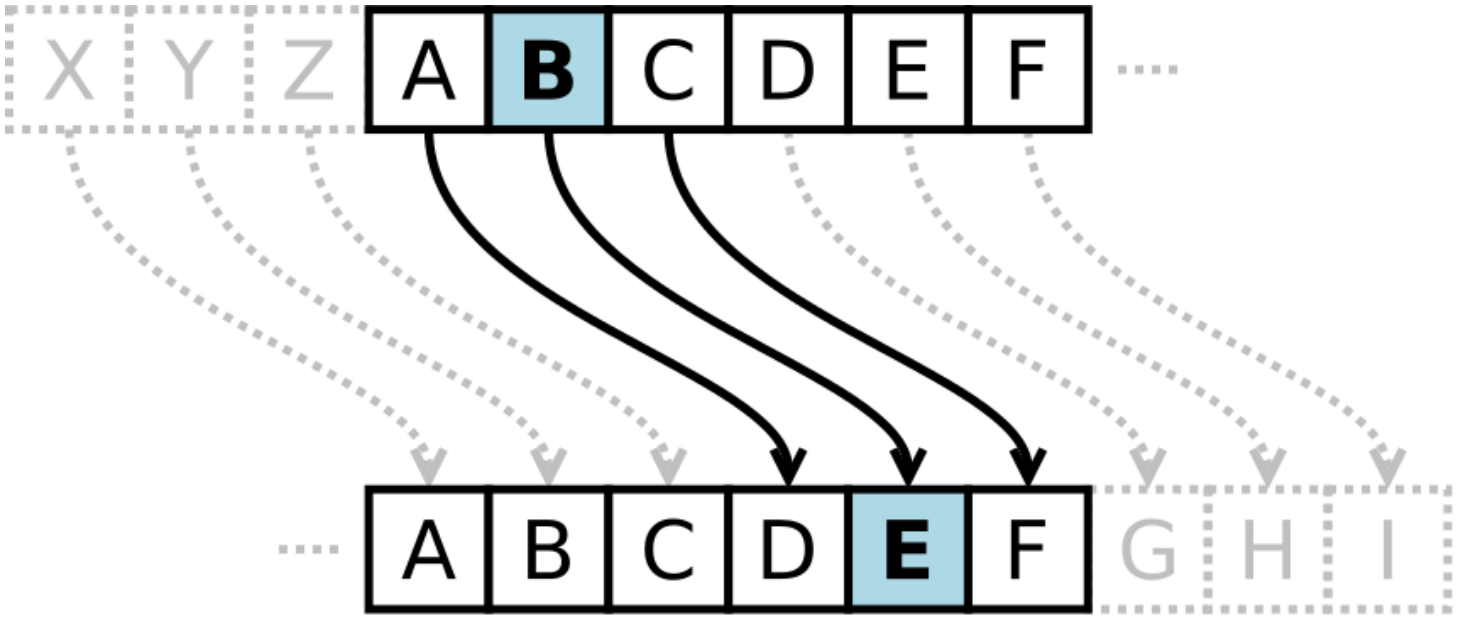
Contudo ela não pode ser usada pois viola a regra “Não é viável encontrar dois blocos que gerem o mesmo código *hash*.”

Ex. 242429484982/10 = 2

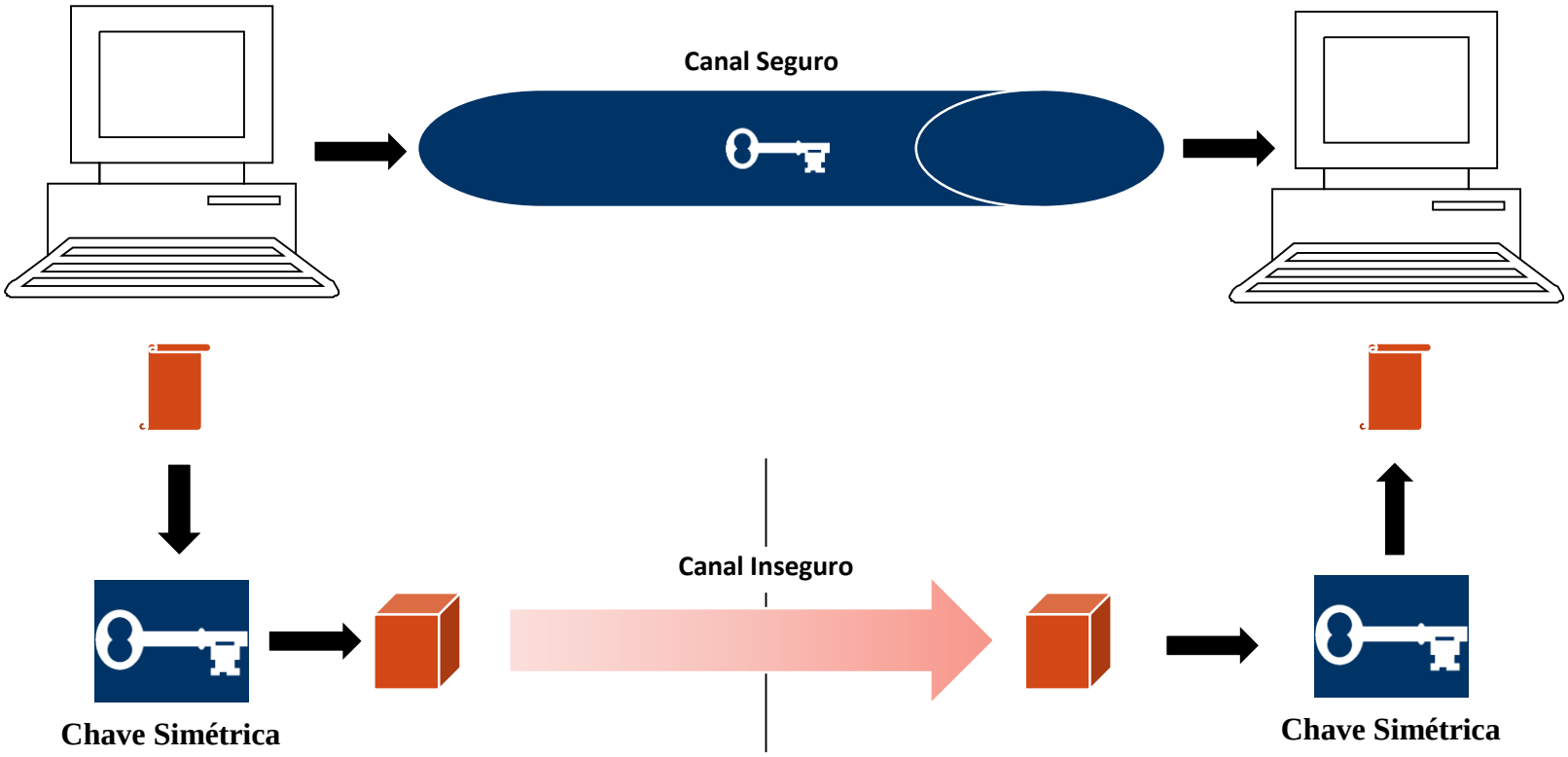
Funções Criptograficas

- Código
  - O algoritmo é o segredo
- Cifra
  - O algoritmo é conhecido
  - A chave é o segredo

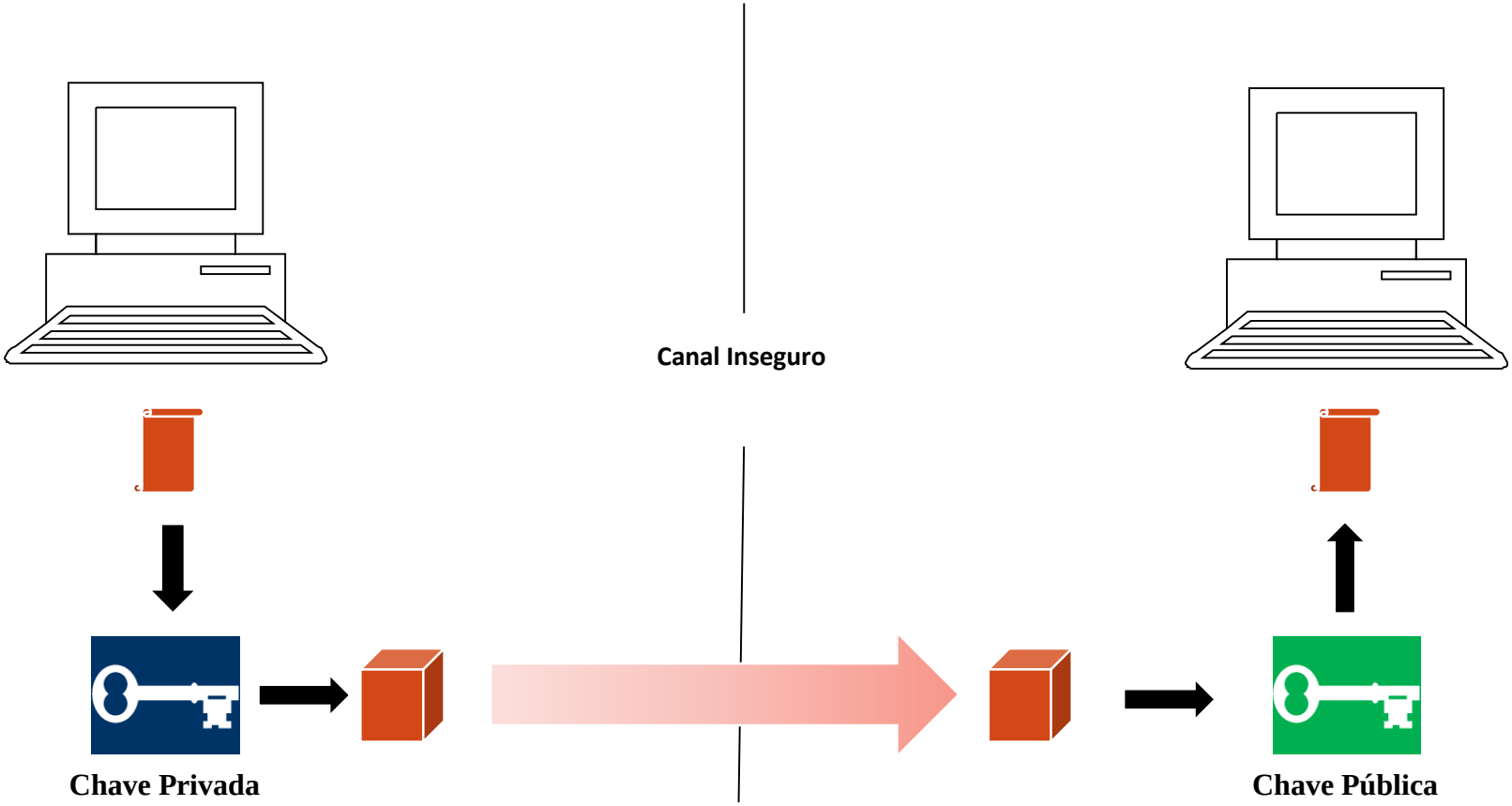
Crifra de César



Conceito de criptografia simétrica



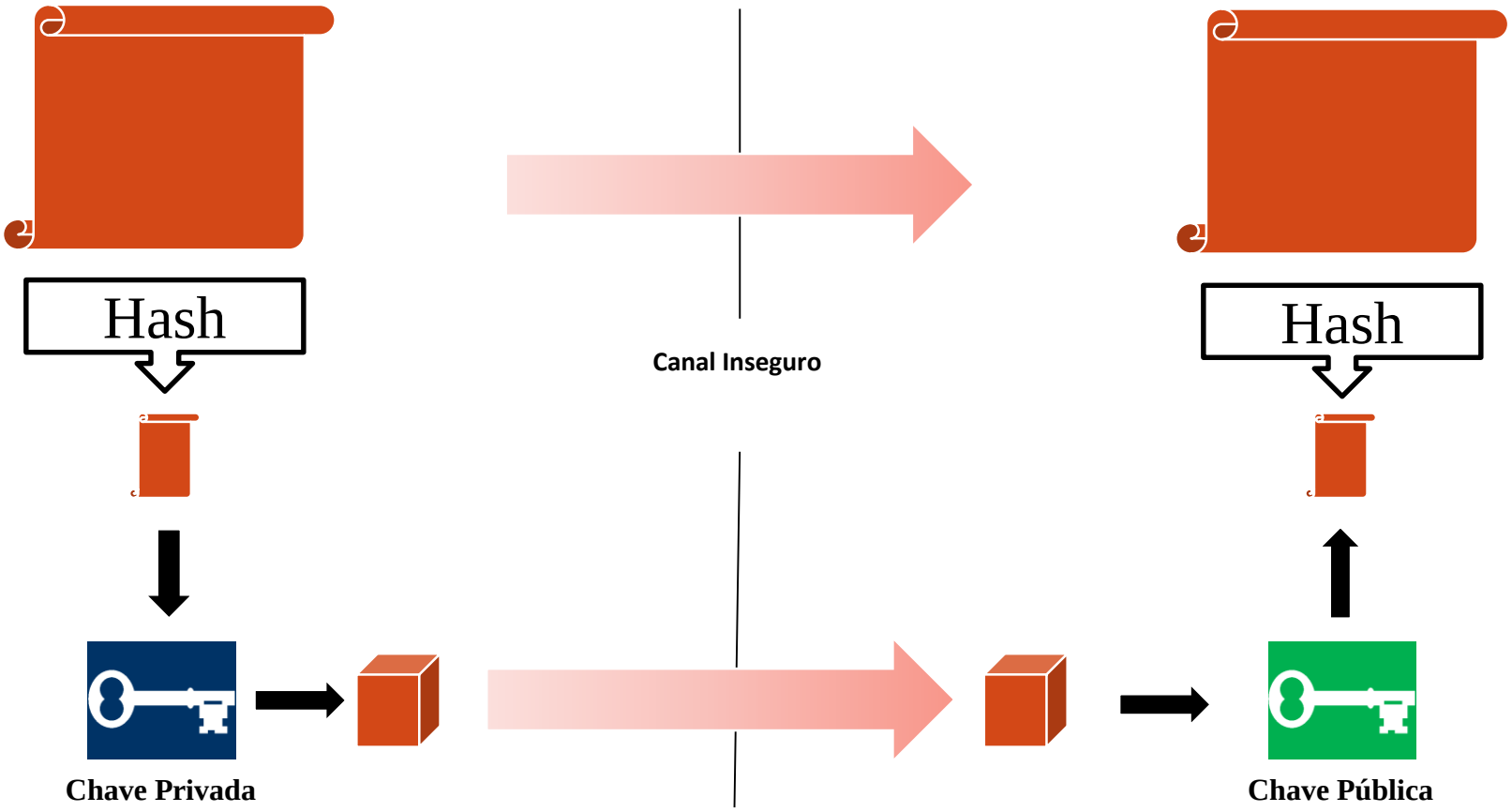
Conceito de criptografia assimétrica



Assinatura Digital

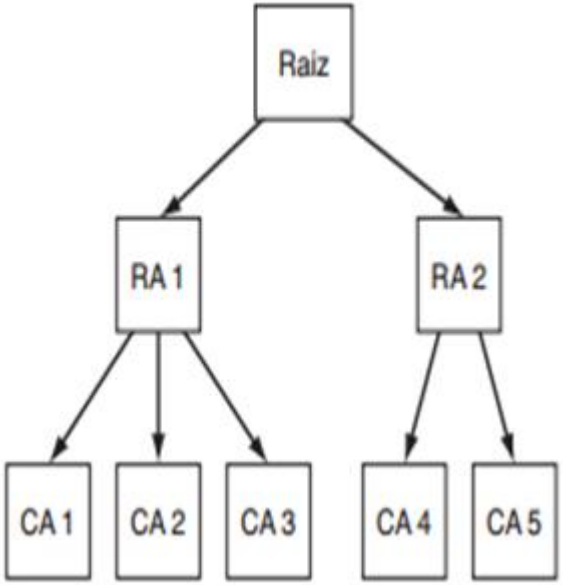
- Integridade dos dados
- Autenticidade dos dados
- Criptografia Assimétrica
- Função Hash
- Implementações
  - *Hardware*
  - *Software*

Conceito de criptografia assimétrica

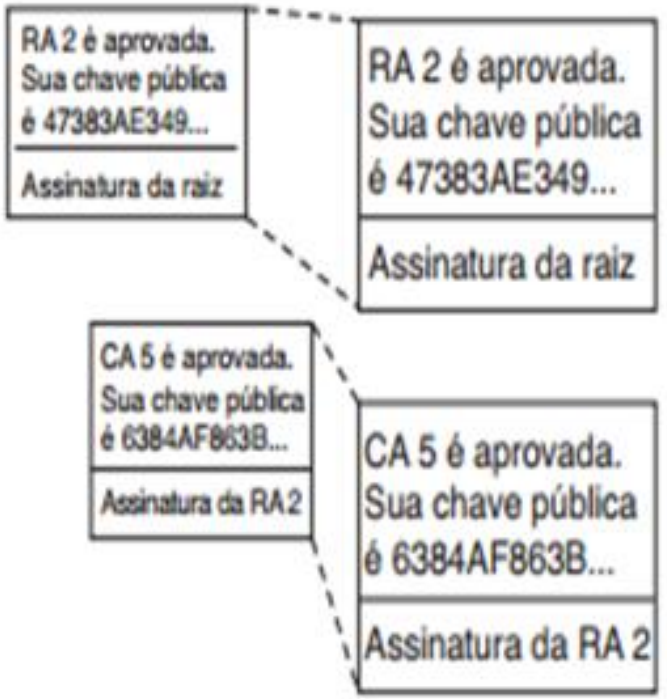


Certificado Digital / PKI

PKI hierárquica



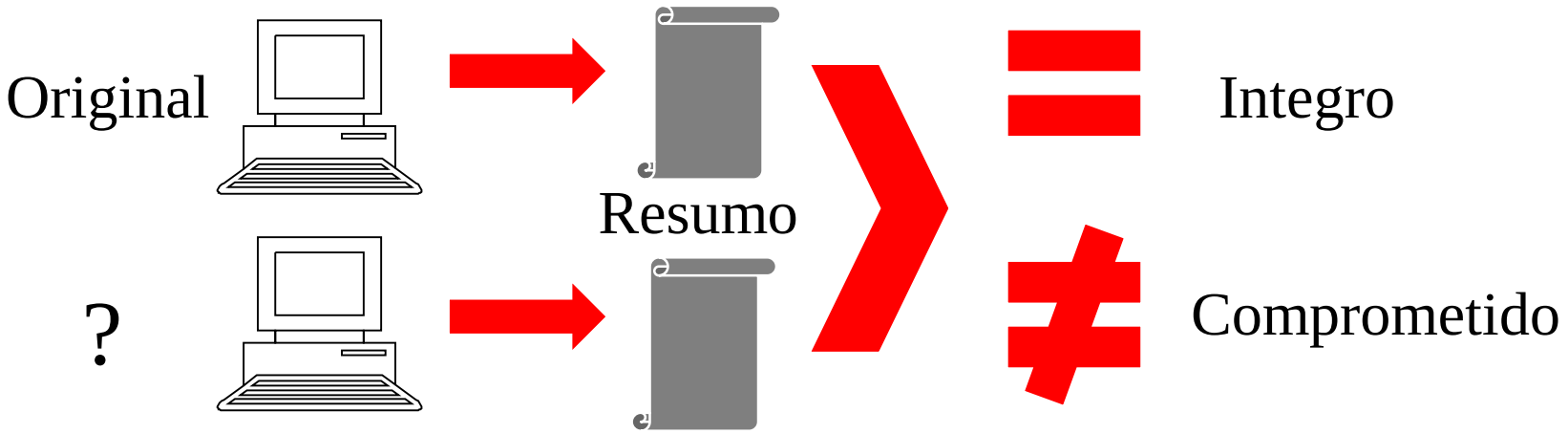
Cadeia de certificados



Fonte: Tanenbaur

Verificação de Integridade

- Metodogia sugerida para proteger a propriedade intelectual do software
- A verificação de Integridade de um software é realizada comparando o resultado da função hash (resumo) do código original com o do código a ser verificado.
- Se os resultados (resumos) forem iguais o código pode ser considerado integro.



Fator Aleatório

Para evitar ataques em que a resposta seja calculada previamente é necessário que seja fornecido um parâmetro aleatório ao instrumento, duas metodologias são possíveis:

- Semente aleatória – É fornecido ao instrumento um número que irá compor os dados a serem cifrados pela função hash.
- Faixas aleatórias – São fornecidos faixas de endereços aleatórios e o hash é calculado apenas sobre estas.

Carga de software legalmente relevante

- Atualização do *software* sem rompimento de lacres
- Deve ser prevista na aprovação de modelo.
- A autenticidade do *software* deve ser verificada através de uma assinatura digital feita pelo Inmetro.
- O par de chaves para a assinatura digital é gerado durante a aprovação de modelo.

Procedimento para geração de Assinatura Diigital

- Solicita chave pública ao Inmetro
- Grava chave publica do Inmetro no *firmware*
- Envia *firmware* ao Inmetro
- Recebe assinatura do Inmetro

*Se a chave pública não ficar gravada no firmware os dois primeiros passo podem ser pulados.

Proteção e atualização dos parâmetros de configuração

- Todos os parâmetros que fixam as características legalmente relevantes do medidor de umidade de grão devem ser protegidos contra modificações não autorizadas.
- As modificações das constantes de calibração devem ser previamente autorizadas pelo Inmetro, sendo o Inmetro responsável por assinar digitalmente os novos parâmetros.
- O software do medidor de umidade de grão somente pode efetuar mudanças em constantes de calibração após verificação (validação) da assinatura digital do Inmetro.

Requisitos em discussão

- Protocolo unificado
  - Permite usar uma única ferramenta para fazer verificação de integridade, leitura de logs etc.
- PKI – Metrológico
  - Permite dar rastreabilidade para as chaves dos instrumentos

Fim

Obrigado!

Contato:

Bruno Erthal– beabreu@inmetro.gov.br