Introdução à Segurança da Informação

Mecanismos de Controle Parte II

Prof. Dr. Daniel Caetano

2021 - 1

Compreendendo o problema

- **Situação:** Clonagem de celular via aplicativos tem sido um problema cada vez mais frequente, envolvendo aplicativos como o WhatsApp, por exemplo.

Para quais tarefas "sensíveis" você usa seu celular no dia-a-dia?

Compreendendo o problema

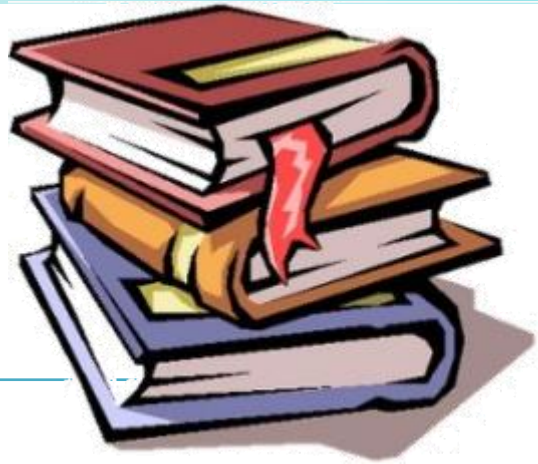
- **Situação:** Clonagem de celular via aplicativos tem sido um problema cada vez mais frequente, envolvendo aplicativos como o WhatsApp, por exemplo.

E se o seu celular for roubado ou perdido, o que você fará?

Objetivos

- Conceituar autenticidade e não repúdio
- Conhecer os principais mecanismos de identificação
- Conhecer os principais mecanismos de autenticação
- Conhecer os mecanismos adicionais de segurança no logon

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 6)
Biblioteca Virtual	Controles e Métodos de Defesa em Segurança da Informação – Cap 2 (páginas 29 a 39).
Material Didático	Gestão de Segurança da Informação, Caps 1 e 5
Material Adicional	http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf (TCU - Cap. 2) https://www.tre-ce.jus.br/videos/tse-saiba-o-que-e-biometria (TSE - O que é Biometria)

Autenticidade e Não-Repúdio

Problemas de Autenticidade

- **Ex.:** alguém sacar seu dinheiro em seu nome
  - "Personificação"
- Alguns outros problemas possíveis
  - Alguém enviar mensagem em seu nome
  - Alguém acessar um sistema em seu nome
  - Alguém visualizar documentos que só você deveria
  - Alguém interceptar mensagem destinadas a você
  - ...
- Como evitar?

Garantia de Autenticidade

- **Autenticidade:** sem adulterações
  - De usuário/pessoa
  - Do documento/autor.

- Autenticidade garantida por dois mecanismos
  - **Autenticação**: Partes são quem dizem ser
  - **Assinatura Digital**: Mensagem inalterada (inclui autoria)
    - Veremos mais sobre isso em breve!

Garantia de Autenticidade

- Requisitos da autenticidade:
  - Autenticação da origem
  - Autenticação do destino
  - Integridade da informação.

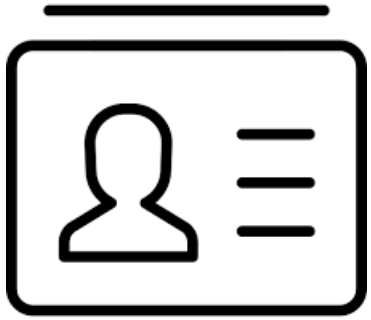
- Consequência: **não-repúdio**
  - Garantir a responsabilização dos envolvidos
- Para isso, é fundamental controle de acesso!

Retomando:

Mecanismo Lógico do Controle de Acesso

Controle de Acesso: Procedimento

- **Logon/Login**: dois processos básicos
  - Identificação**:** qual é o usuário e suas permissões
  - Autenticação**:** comprovar a identidade
- Ou seja: processo com pelo menos dois itens
  - **Identificação** + **Algo que usuário sabe ou tem**



  - **Usar mecanismos diferentes para cada um!**

Dificuldades Associadas ao Logon

- **Logon**: muito importante
  - Restringir as operações aos usuários permitidos
  - Registrar ações executadas
- Processo precisa ser resistente à “invasão”:
  - Praticamente todos podem ser contornados
- Limitar o número de tentativas

Mecanismos de Identificação

Mecanismos de Identificação

- Identificação
  - Objetivo: saber quem quer acessar
  - **Identificador** único para cada usuário (daí o nome!)
- Mecanismos comuns
  - Auto-declarado (username ou userid)
  - Uso de cartões de identificação
    - Cartões com código de barras / QR code
    - Cartões Inteligentes SmartCards / RFID
      - Certificados Digitais **(em breve!)**

Identificação Auto-Declarada

- O que é?
  - Uma sequência numérica ou alfanumérica.
- Como é feita?
  - O usuário digita seu identificador
- Vantagens (+) e Desvantagens (-)
  - \+ Solução mais barata
  - \+ Não tem “esquecer em casa” ou perder
  - \+ Em geral não requer hardware especializado
  - – Pode ser esquecida pelo usuário
  - – Facilmente transmitida ou copiada...

Identificação Auto-Declarada

- Vantagens (+) e Desvantagens (-) (cont.)
  - Algumas vezes pode ser “adivinhada”
  - Fácil ter mais de um acesso simultâneo

- Cuidados especiais
  - Pedir que os usuários não anotem
    - Menos ainda o com o mecanismo de autenticação
  - Se for numérico, adotar dígito verificador
    - Evitar erros de digitação e bloqueios desnecessários

Identificação por Cartões

- O que é?
  - Um cartão que contém o identificador do usuário.
- Como é feita?
  - O usuário passa o cartão em um dispositivo
- Variações
  - Cartões com código de barras
  - Cartões com código QR
  - Cartões com RFID
  - Cartões inteligentes (*smartcards*)

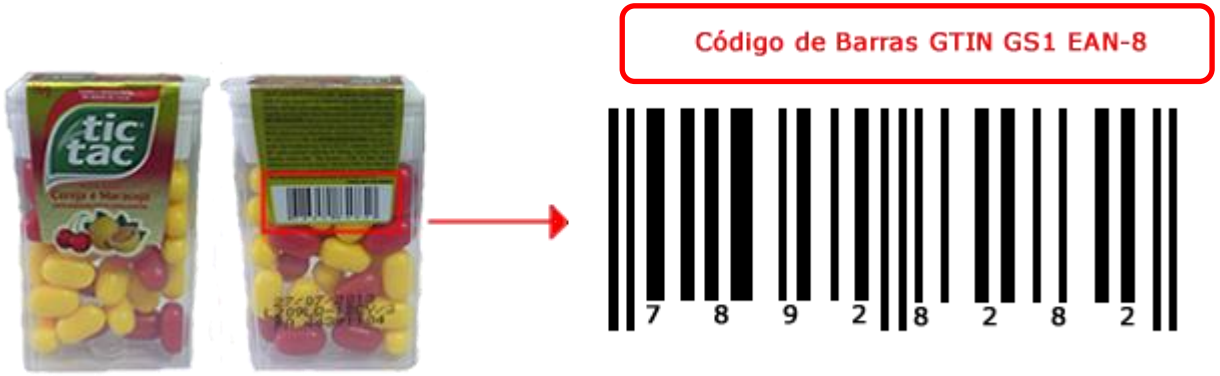
Identificação: Código de Barras

- Como funciona?
  - Leitura óptica

3805565154

Identificação: Código de Barras

- Como é a conversão?
  - Existem vários padrões de codificação



  - Mais comuns
    - UPC (EUA)
    - EAN (Europa e Brasil)

EAN-13

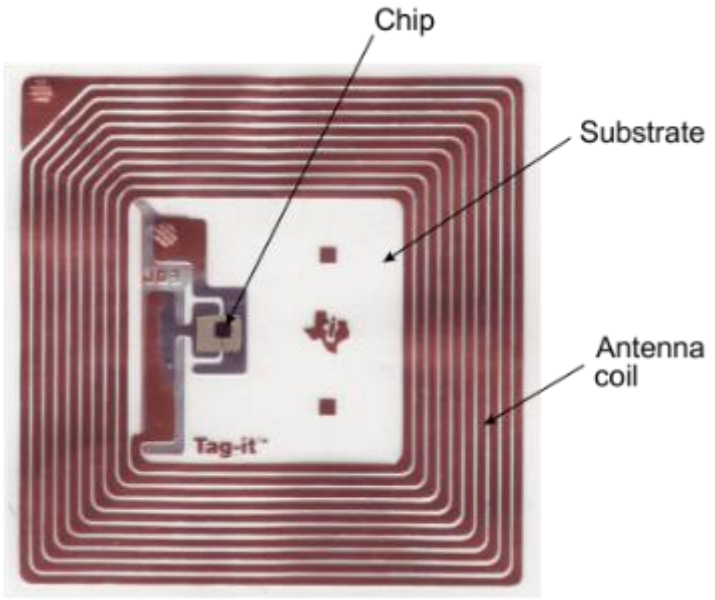
Identificação: Código QR

- Código *Quick Response*
  - Informações mais complexas
    - Que não cabem em um código de barras...
    - como textos, imagens, *fingerprints*...

- Como funciona?
  - Leitura óptica...
    - Como um “Código de Barras Bidimensional”

Identificação: RFID

- *Radio Frequency IDentification*
  - Informações bem mais complexas
  - Uma evolução do código de barras
- Como é feito?
  - Microeletrônica: chip que guarda informações
  - Antena / Indutor
- Como funciona?
  - Indução + RF
  - Leitura à distância
    - Problema?



Identificação: *Smartcard*

- Cartão Inteligente
  - Informações bem mais complexas
  - Similar ao RFID, mas requer contato
- Como é feito?
  - Microeletrônica: chip que guarda informações
  - Contatos expostos

Identificação por Cartões

- Vantagens (+) e Desvantagens (-)
  - + Mais difícil copiar / clonar
    - *Smartcard* > RFID > QR / Código de Barras
  - + Mais difícil "adivinhar" para construir um
  - + Dificulta mais de um acesso simultâneo
  - – Mecanismo mais caro: **requer** hardware
  - – Pode ser perdido ou esquecido em casa
  - – Pode ser emprestado.
- Cuidados especiais
  - – Código de barra e QR: devem ser ocultos!
  - – Cartão deve ser branco, sem indicações
    - Nunca usar o próprio crachá para isso!

Mecanismos de Autenticação

Mecanismos de Autenticação

- Autenticação
  - Objetivo: provar que o usuário é quem ele diz ser
  - Comprovar **autenticidade/autoria do acesso**
- Mecanismos comuns
  - Senhas
  - Cartões
  - *Tokens*
  - Biometria

Autenticação por Senha

- O que é?
  - Uma sequência de caracteres
- Como é feita?
  - O usuário digita sua senha
- Vantagens (+) e Desvantagens (-)
  - \+ Solução mais barata
  - \+ Não tem “esquecer em casa” ou perder
  - \+ Em geral não requer hardware especializado
  - – Pode ser esquecida pelo usuário
  - – Facilmente transmitida ou copiada...

Autenticação por Senha

- Vantagens (+) e Desvantagens (-) (cont.)
  - Algumas vezes pode ser “adivinhada”
  - Pode ser usada em mais de um local/sistema.
- Cuidados especiais
  - Não usar senhas curtas (menos de 6 dígitos)
  - Misturar letras, números e símbolos
  - Não anotar... Menos ainda com a identificação

Autenticação por Cartão

- O que é?
  - Um cartão que contém uma senha ou *chave*.
- Como é feita?
  - O usuário passa o cartão em um dispositivo
- Variações
  - Cartões com código de barras
  - Cartões com código QR
  - Cartões com RFID
  - Cartões inteligentes (*smartcards*)

Autenticação por Cartão

- Vantagens (+) e Desvantagens (-)
  - \+ Mais difícil copiar / clonar
  - \+ Permite uso de senhas/chaves mais complexas
  - \+ Dificulta mais de um acesso simultâneo
  - – Mecanismo mais caro: **requer** hardware
  - – Pode ser roubado, perdido ou esquecido em casa
  - – Pode ser emprestado.

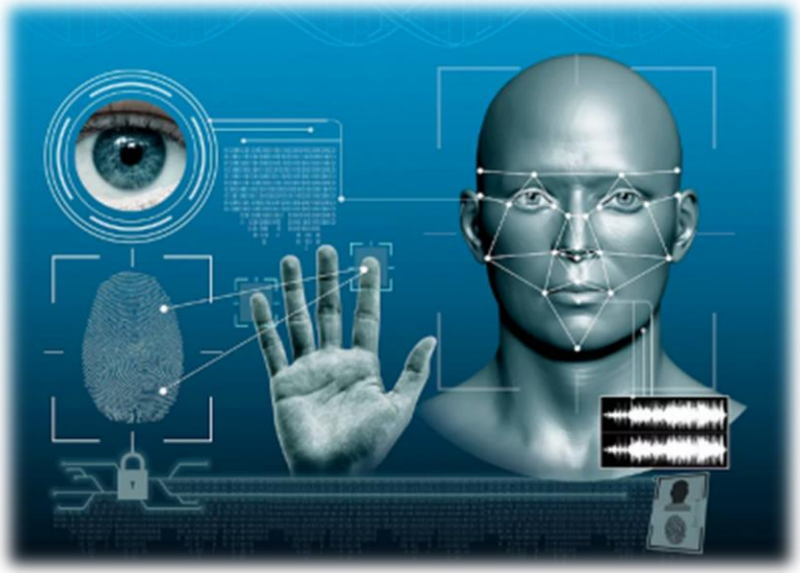
- Cuidados especiais
  - – Mesmos da identificação
  - – Não usar quando a identificação é feita pelo mesmo cartão: dois mecanismos diferentes!

Autenticação por Token

- O que é?
  - Um dispositivo que gera senhas temporárias
- Como é feita?
  - Sequência de números associada a usuário e hora
- Vantagens (+) e Desvantagens (-)
  - \+ Mais difícil copiar / clonar
  - \+ Senha muda o tempo todo, não previsível
  - – Menos barato: **requer** hardware (pode ser celular)
  - – Pode ser roubado, perdido ou esquecido em casa
  - – Pode ser emprestado.

Autenticação por Biometria

- O que é?
  - Uso de características físicas ou comportamentais
- Como é feita?
  - Aparelho lê a característica ou comportamento
- Tipos comuns de biometria:
  - Leitura de digitais
  - Leitura de retina
  - Reconhecimento facial
  - Reconhecimento de voz
  - Leitura de gestos.



Autenticação por Digital

- O que é?
  - Leitura dos padrões de desenho de um dos dedos
    - Variante: leitura da palma da mão
- Como é feita?
  - Captura de imagem
  - Captura termal
  - Ultrassom
  - Capacitiva.
- Considerada uma das mais seguras
  - Mas qualidade depende da tecnologia

Autenticação por Retina

- O que é?
  - Leitura dos padrões da retina
    - Variante: leitura da íris
- Como é feita?
  - Captura de imagem.

- Considerada bastante segura
  - É, porém, menos confortável
  - Retina muda com a morte do indivíduo.

Autenticação por Reconh. Facial

- O que é?
  - Leitura dos padrões do rosto
- Como é feita?
  - Captura de imagem
  - Captura termal
  - Ultrassom.

- Considerada, no geral, fraca
  - Bastante prática
  - Qualidade depende muito da tecnologia e da I.A.

Autenticação por Reconh. de Voz

- O que é?
  - Leitura dos padrões da voz e fala
- Como é feita?
  - Gravação de som

- Considerada, no geral, fraca
  - Simples, mas um pouco inconveniente
  - Qualidade depende muito da tecnologia e da I.A.
    - Mas mesmo as melhores são “fracas”.

Autenticação por Gestos

- O que é?
  - Leitura de padrões de comportamento
- Como é feita?
  - Gravação de vídeo (visível ou termal)
  - Leitura de dispositivo de toque.
- Considerada, no geral, fraca
  - Relativamente prática, porém fraca
    - Se outra pessoa vê,
      costuma ser fácil de “copiar”

Autenticação por Biometria

- Vantagens (+) e Desvantagens (-)
  - \+ Não dá para esquecer ou perder
  - \+ Dificulta a cópia e os acessos simultâneos
  - – Em geral **requer** hardware especializado
  - – Tecnologia mais cara e delicada
  - – São comuns os falsos positivos e negativos
    - Variabilidade do indivíduo (acidentes, doenças...).
- Cuidados especiais
  - – Tecnologia compatível com a segurança
    - Em especial, garantir a "vida" do elemento lido

Mentimeter

Mecanismos de Melhoria da Identificação/Autenticação

Mecanismos Adicionais

- Adições à Identificação e Autenticação
  - Objetivo: ampliar a segurança
  - Mecanismos de **naturezas diferentes** e...
  - Fatores adicionais
    - Identificador + algo sabido + algo possuído

- Mecanismos comuns
  - Restrição de Equipamentos
  - Autenticação em 2 Fatores.

Restrição de Dispositivos

- O que é?
  - Restringir o uso a determinados dispositivos
- Como é feita?
  - Dispositivo é registrado...
  - ...e checado a cada operação.

- Vantagens (+) e Desvantagens (-)
  - \+ Exigir acesso físico ou posse do dispositivo
  - – Limita o acesso e o uso do recurso
  - – Em geral exige recurso de rede.

Autenticação em Dois Fatores

- O que é?
  - Restringir o uso a quem tem acesso comprovado por outros meios
- Como é feita?
  - Após a autenticação básica...
  - Código enviado para outro serviço.

- Vantagens (+) e Desvantagens (-)
  - \+ Requer acesso a outro sistema com autenticação
  - – Limita o acesso e o uso do recurso
  - – Em geral existe recurso de rede.

ATIVIDADE

Atividade

- Grupos – 15 minutos
  - Conforme canais do Teams
- Assista ao vídeo: **https://bit.ly/33OOPIe**
- Discuta com seu grupo e identifique:
  - Qual a importância da implantação de biometria no processo eleitoral?
  - Quais os princípios de segurança da informação atendidos?

ENCERRAMENTO

Resumo e Próximos Passos

- Não-repúdio
  - Essencial e exige autenticação
- Mecanismos de Identificação x Autenticação
- Aprimoramento
  - Mecanismos distintos, dois fatores...
- **Pós Aula**: Aprenda Mais, Pós Aula e Desafio!
  - No padlet: https://padlet.com/djcaetano/seguranca

- Controle de Acesso a Recursos Compartilhados
  - Controle de permissões de usuário

PERGUNTAS?