

# Introdução: Conceitos de Segurança Computacional



Prof. Roberto Rodrigues-Filho  
Dept. de Ciência da Computação (CIC)  
Universidade de Brasília (UnB)

- Cibersegurança é ESSENCIAL!
  - **Dados: o novo petróleo**
  - Nossas vidas dependem de sistemas digitais
  - Guerras são lutadas no ambiente digital
  - Segurança digital das empresas são essenciais



- Cibersegurança é ESSENCIAL!
  - Dados: o novo petróleo
  - **Nossas vidas dependem de sistemas digitais**
  - Guerras são lutadas no ambiente digital
  - Segurança digital das empresas são essenciais



- Cibersegurança é ESSENCIAL!
  - Dados: o novo petróleo
  - Nossas vidas dependem de sistemas digitais
  - **Guerras são lutadas no ambiente digital**
  - Segurança digital das empresas são essenciais



- Cibersegurança é ESSENCIAL!
  - Dados: o novo petróleo
  - Nossas vidas dependem de sistemas digitais
  - Guerras são lutadas no ambiente digital
  - **Segurança digital das empresas são essenciais**



EDIÇÃO D



Notícias ▾

Mais Que Cartão

Pesquisa e Relatórios

Idioma e região ▾



## DO MICRO AO MACRO

### Cresce número de ataques cibernéticos e os custos para empresas; veja como se proteger

Aumento dos ataques de extorsão evidencia a necessidade de maior segurança digital nas empresas

POR ALLAN RAVAGNANI

18.07.2024 07H00

Investimento em cibersegurança ainda não é prioridade para empresas, aponta Datafolha

- Cibersegurança é ESSENCIAL!
  - Dados: o novo petróleo
  - Nossas vidas dependem de sistemas digitais
  - Guerras são lutadas no ambiente digital
  - **Segurança digital das empresas são essenciais**

## NEGÓCIOS

### **Na mira de ataques cibernéticos, empresas de capital aberto ainda mostram vulnerabilidades**

Crimes cibernéticos devem causar um impacto de US\$ 10,5 trilhões na economia global; mais da metade das companhias listadas acredita que a falta de recursos e competências é o maior desafio

**exame.**

[Home](#) > [Economia](#)

### **Ataques cibernéticos geram perdas de US\$ 12 bi ao setor financeiro em duas décadas, diz FMI**

Número de incidentes mais que dobrou desde a pandemia e representa uma ameaça crescente à estabilidade financeira mundial



- Cibersegurança é ESSENCIAL!
  - Dados: o novo petróleo
  - Nossas vidas dependem de sistemas digitais
  - Guerras são lutadas no ambiente digital
  - **Segurança digital das empresas são essenciais**

 MENU

TECNOLOGIA E GAMES

22/06/2011 13h28 - Atualizado em 22/06/2011 15h29

## Site da Petrobras sai do ar; grupo hacker reivindica autoria de ataque

Página da instituição ficou indisponível a partir das 13h.  
Ataque foi reivindicado pelo grupo de hackers LulzSecBrazil.

[roberto.filho@unb.br](mailto:roberto.filho@unb.br)

- Cibersegurança é ESSENCIAL!
  - Dados: o novo petróleo
  - Nossas vidas dependem de sistemas digitais
  - Guerras são lutadas no ambiente digital
  - **Segurança digital das empresas são essenciais**

CRIMES VIRTUAIS • INTERNET

## Ataque hacker desvia cerca de R\$ 1 bi após invadir empresa que conecta instituições ao Pix

Recursos estavam em contas no Banco Central, que desligou do sistema fintech que administra troca de informações entre instituições

## KrebsOnSecurity Hit With Near-Record 6.3 Tbps DDoS

May 20, 2025

46 Comments

KrebsOnSecurity last week was hit by a near record distributed denial-of-service (DDoS) attack that clocked in at more than 6.3 terabits of data per second (a terabit is one trillion bits of data). The brief attack appears to have been a test run for a massive new Internet of Things (IoT) botnet capable of launching crippling digital assaults that few web destinations can withstand. Read on for more about the botnet, the attack, and the apparent creator of this global menace.



- Cibersegurança é ESSENCIAL!
  - Dados: o novo petróleo
  - Nossas vidas dependem de sistemas digitais
  - Guerras são lutadas no ambiente digital
  - Segurança digital das empresas são essenciais
- **SEGURANÇA DIGITAL - CIBERSEGURANÇA**



- Evolução da Segurança Computacional
  - **Antes dos computadores:** segurança física e administrativa
  - **Com a computação:** necessidade de ferramentas automáticas
  - **Com redes:** proteção de dados em transmissão
  - **Surgimento do termo:** Segurança de Redes / Segurança na Internet

- Segurança Computacional



- Segurança Computacional

“A proteção concedida a um sistema de informação automatizado com o objetivo de preservar a integridade, a disponibilidade e a confidencialidade dos recursos do sistema de informação (incluindo hardware, software, firmware, informações/dados e telecomunicações).” NIST95

- Segurança Computacional



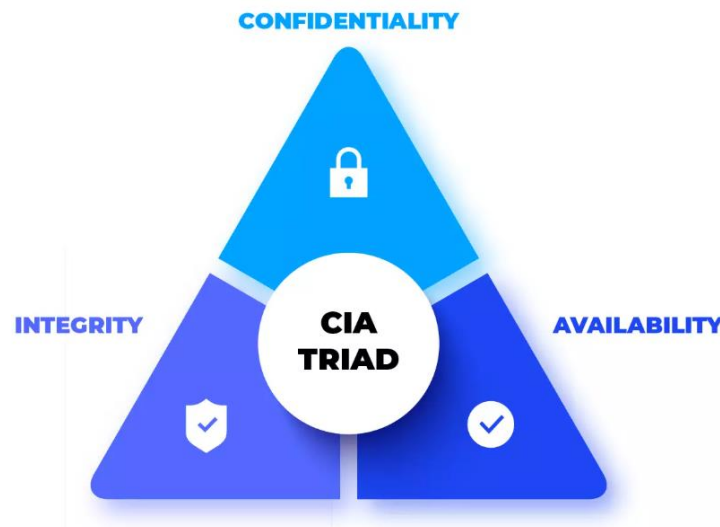
- Segurança Computacional

“A proteção concedida a um sistema de informação automatizado com o objetivo de preservar a **integridade**, a **disponibilidade** e a **confidencialidade** dos recursos do sistema de informação (incluindo hardware, software, firmware, informações/dados e telecomunicações).” NIST95



- Segurança Computacional
- Proteção a sistemas de informação automatizados para garantir:
  - Confidencialidade
  - Integridade
  - Disponibilidade
- Inclui hardware, software, dados, firmware e telecomunicações

- Segurança Computacional
  - **Confidencialidade**: restringir acesso e preservar privacidade
  - **Integridade**: evitar alteração ou destruição indevida
  - **Disponibilidade**: acesso confiável a sistemas



- Segurança Computacional
  - **Confidencialidade**: restringir acesso e preservar privacidade
  - **Integridade**: evitar alteração ou destruição indevida
  - **Disponibilidade**: acesso confiável a sistemas
  - **Autenticidade**: validar identidade, origem, confiabilidade
  - **Responsabilidade (Accountability)**: rastrear ações de entidades

- Segurança Computacional
  - **Política:** o que proteger (integridade, confidencialidade, e disponibilidade)
  - **Modelo de ameaça (threat model):** suposições (contra quem)
  - **Mecanismo:** software, hardware (implementa como proteger)

- Desafios de segurança
  1. Requisitos simples, mecanismos complexos
  2. Novos ataques exploram fraquezas inesperadas
  3. Serviços podem parecer contraintuitivos
  4. Onde aplicar mecanismos? Camadas e pontos da rede
  5. Gestão de chaves e segredos
  6. Atacante precisa de 1 falha; defensor precisa de 100%
  7. Benefícios pouco visíveis até falha ocorrer
  8. Necessidade de monitoramento constante
  9. Muitas vezes pensado como 'pós-projeto'
  10. Segurança pode ser vista como obstáculo à usabilidade

- Arquitetura OSI de Segurança (X.800)
  - O que é?
    - Organiza a segurança em redes de computadores de forma estruturada.
  - Define três elementos principais:
    - **Ataques de segurança** → ações que podem comprometer a informação.
    - **Serviços de segurança** → funções de proteção para defender contra ataques (ex.: autenticação, confidencialidade, integridade, não-repúdio, controle de acesso, disponibilidade).
    - **Mecanismos de segurança** → técnicas concretas que implementam os serviços (ex.: criptografia, assinatura digital, auditoria, roteamento seguro, firewall).

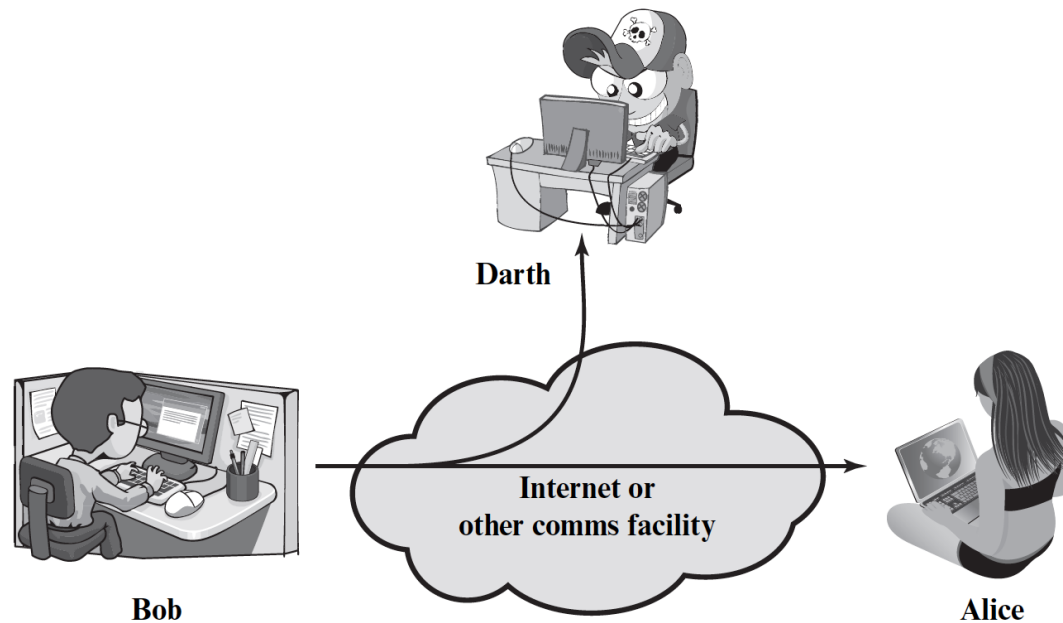


- **Tipos de ataques:**
  - Passivos
  - Ativos



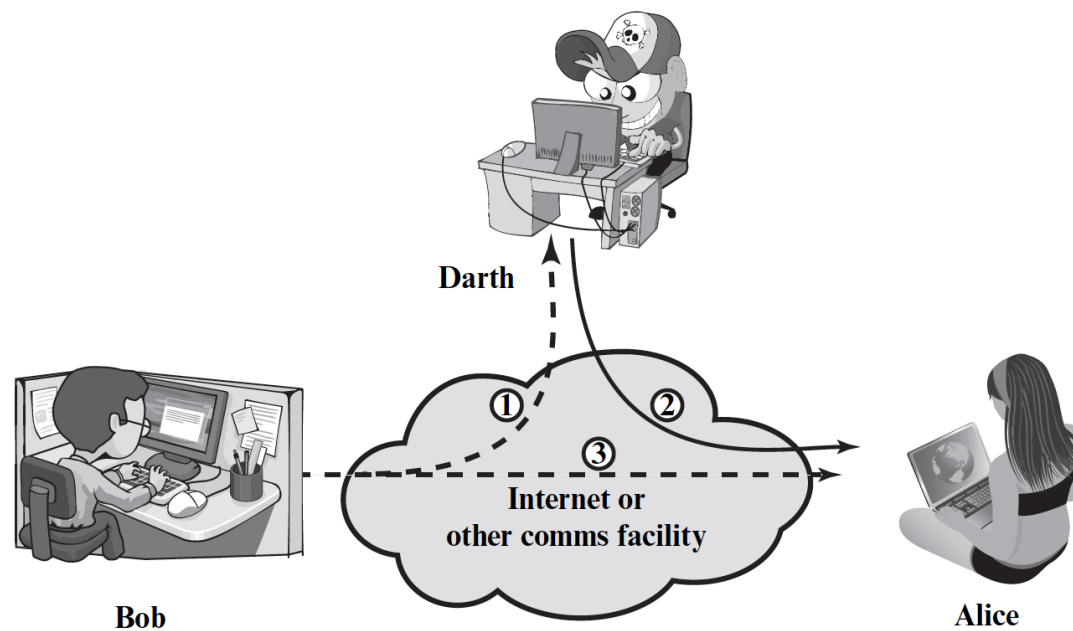
- **Tipos de ataques:**

- **Passivos:** escuta, análise de tráfego (difíceis de detectar, prevenção via criptografia)



(a) Passive attacks

- **Tipos de ataques:**
  - **Ativos:** replay, modificação de mensagens, negação de serviço



(b) Active attacks

- **Princípios Fundamentais de Projeto**

- Economia de mecanismo
- Padrões (default) seguros
- Mediação completa
- Design aberto
- Separação de privilégios
- Menor privilégio
- Menor mecanismo comum
- Aceitabilidade psicológica

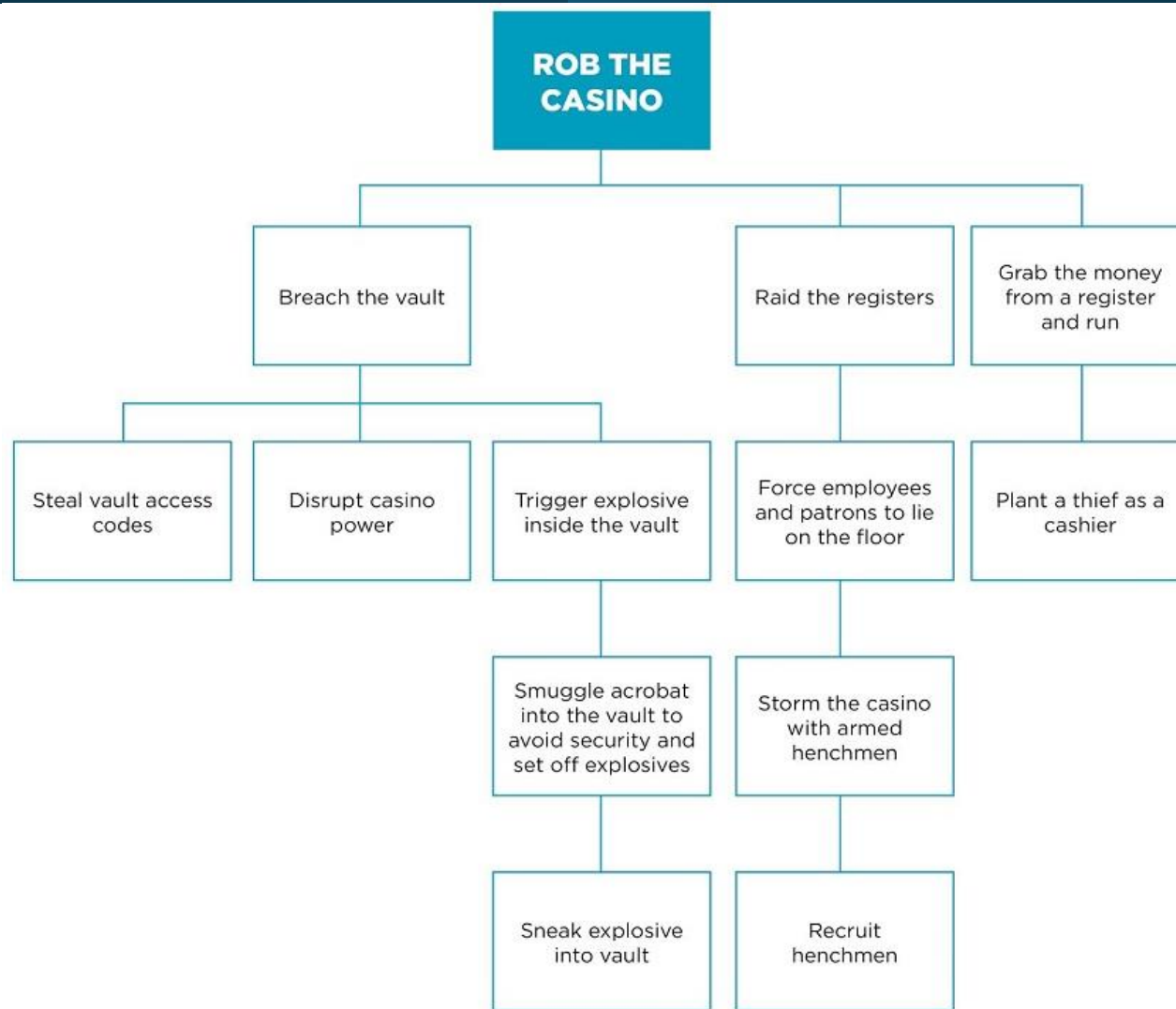


- **Superfície de ataques**
  - **Rede:** protocolos, portas abertas...
  - **Software:** falhas em aplicações/sistemas
  - **Humanos:** engenharia social, erro, insiders

Reduzir superfície = reduzir pontos exploráveis

## • Árvores de Ataque

- Raiz: objetivo do atacante
- Nós: sub-objetivos
- Folhas: técnicas concretas





# Árvores de Ataque

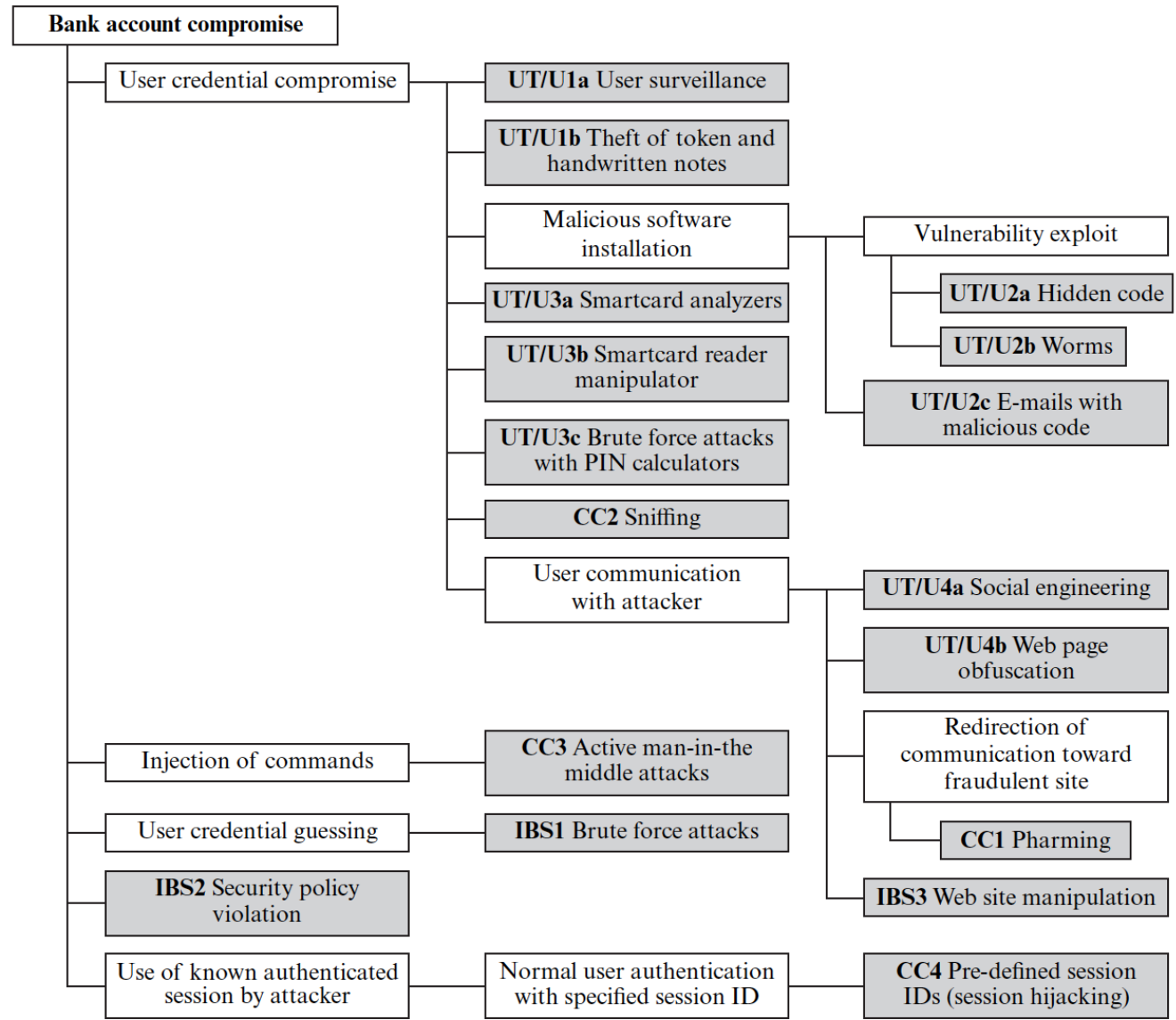


Figure 1.4 An Attack Tree for Internet Banking Authentication