Prime

CCS-A

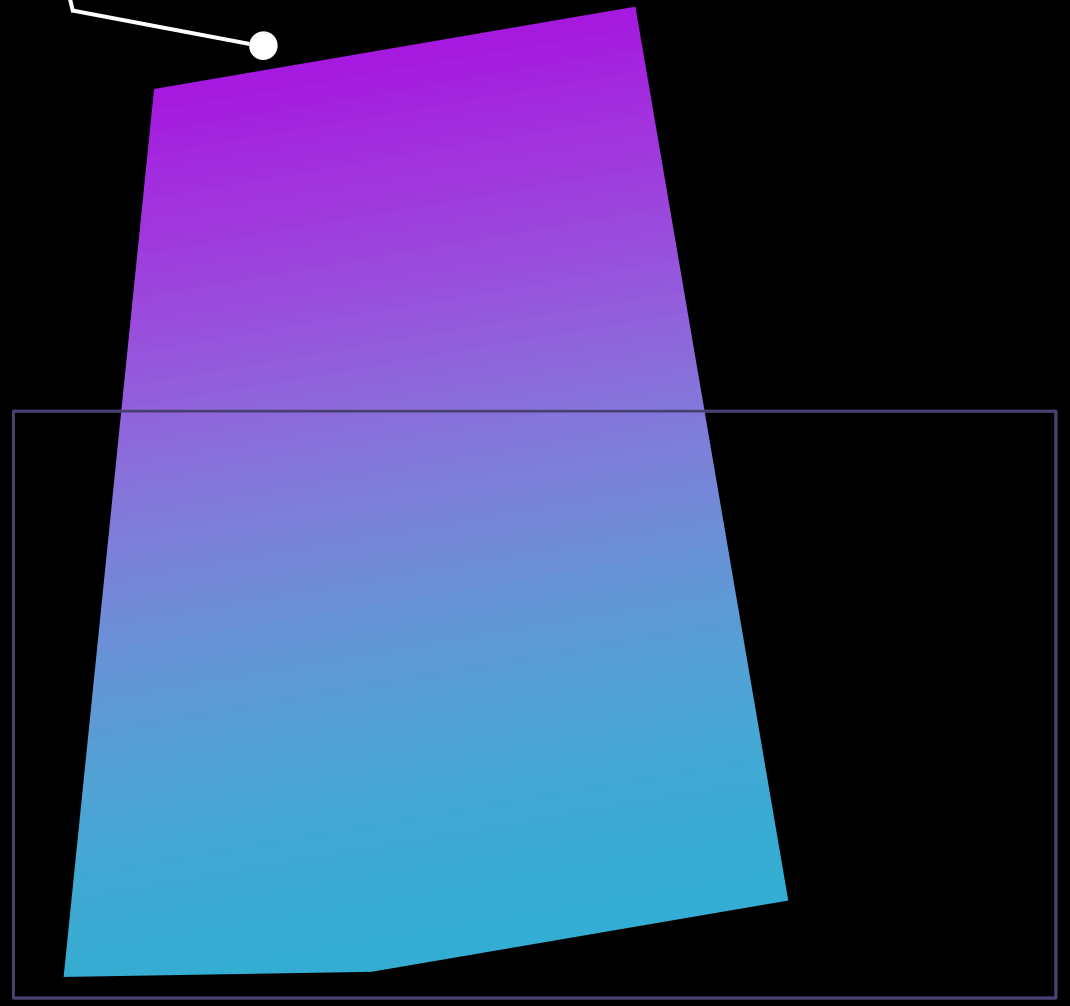
Tipos de Ataques Cibernéticos

Ataques de Senha

A autenticação de ID de usuário e senha pode ser atacada de diversas maneiras.

Esses ataques muitas vezes produzem resultados favoráveis para o invasor.

- Ocorrem devido ao usuário não seguir boas práticas de senha.



Pulverização

- Ataque que utiliza um número limitado de senhas e as aplica a um grande número de contas.
- Como ocorre:

Faz um teste em todas as contas.

- Por que é utilizado:

É útil quando o alvo é indefinido

Dá menos importância sobre quem terá a conta invadida.

- É o ponto de apoio necessário para um invasor entrar.

Dicionário

- Ataque que usa um programa de quebra de senha que utiliza uma lista de palavras do dicionário.
- Como funciona?
  - Os programas permitem a criação de várias regras para que o invasor combine novas senhas possíveis.
  - As regras podem ser definidas para substituir ou combinar palavras. s3cr3t
- Método usado por invasores habilidosos quando aplicado de maneira avançada.
- Consistem em uma tabela com letras e regras que geram novas senhas.

Força Bruta

- O programa de quebra de senha tenta todas as combinações de senha possíveis.
- O que influencia no tempo de ataque de força bruta:
  - 
    Comprimento da senha;
  - 
    Tamanho do conjunto de caracteres.
- Ocorre em dois níveis:
  - 
    Sistema (tentativa e erro de login);
  - 
    Lista de hashes.

Offline

Podem ser empregados para realizar comparações de hash com um arquivo de senha roubado.

Como realizar:

- Máquinas paralelas baseadas em GPU de alto desempenho para testar senhas em taxas muito altas.

Online

Ocorre em tempo real contra um sistema.

Características:

- O sucesso ou o fracasso são determinados pelo sistema sob ataque, e o invasor entra ou não;
- Tendem a ser fáceis de serem monitorados e são limitados pelo tempo de resposta e banda.

Tabelas Rainbow

- Tabelas pré-computadas ou valores de hash associados a senhas.
- **Melhor defesa:** *salted hashes*
  - Um salt é um conjunto aleatório de caracteres projetado para aumentar o comprimento do item que está sendo hashado.

Purotexto/Não-Criptografadas

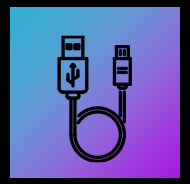
- Senhas de purotexto/não-criptografadas estão sujeitas a recuperação.
- **Ataques de senha de purotexto** são realizados contra problemas relacionados a cópias de senha.
- **Advanced Encryption Standard (AES) -** Permite que os administradores enviem senhas para contas locais por meio de preferências de *group policy*.
- Ferramentas de coleta de senhas de purotexto:
  - ProcDump;
  - Mimikats.

Ataques Físicos

Ocorrem quando um elemento físico, como uma unidade flash, é deixado sem querer para ser usado por um desconhecido.

Gatilho para ataques: dispositivos físicos.

Cabo USB (Universal Serial Bus) Malicioso

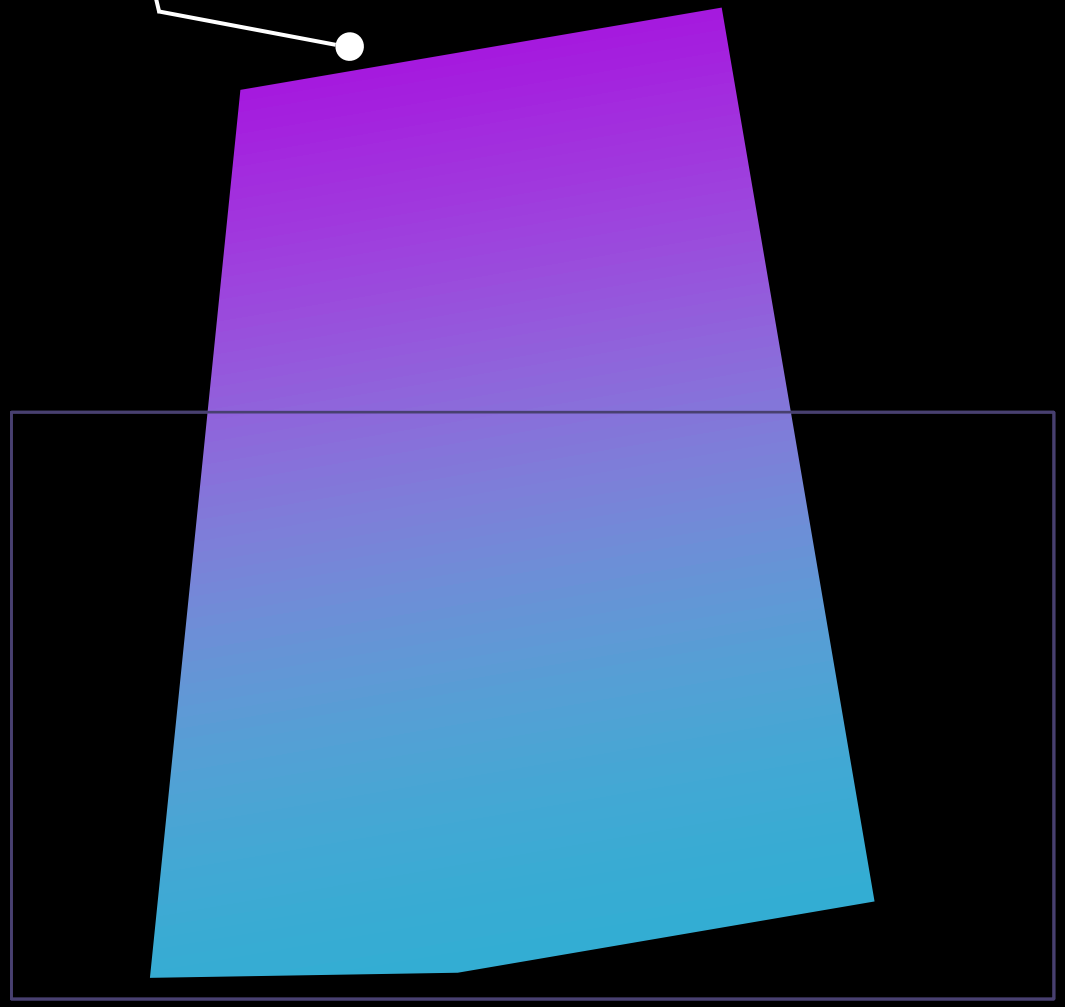


Um cabo USB pode ter componentes eletrônicos embutidos.

- Cabos USB podem entregar malware às máquinas:
  - **Exemplo:** USBHarpoon. Usado como carregador de bateria de celular ou um USB normal, que permite comandos ocultos.

Flash Drive Maliciosos

- Dispositivos USB maliciosos já foram usados para enganar usuários, conectando-os em sua máquina e dando acesso para uma pasta importante.
- Exemplo de ataque com Flash Drive: queda do USB.
- Problemas de segurança grave:
  - Ativar o Autorun ou Autoplay.



Clonagem de Cartão

Caso alguém tenha a posse física do seu cartão de crédito, é possível copiar as informações contidas na tarja magnética.

Método eficiente contra clonagem: cartões inteligentes.

- **Obs:** um cartão sem contato com a máquina também pode ser clonado.
- NFC (Por aproximação), com ataques semelhantes ao sistema de pedágio sem parar.

Skimming

- Dispositivos de skimming – Usados para interceptar um cartão de crédito.
- Características:
  -  Coletam todas as informações de um chip magnético do cartão.
- Falha de defesa: bloquear recursos de segurança de um cartão inteligente.

Skimming

Fonte: Tecmundo – Google Imagens.

Inteligência Artificial Adversária (IA)

Inteligência Artificial (IA)

Representa modelos complexos para simular funções do cérebro.

Características comuns de um ataque com IA:

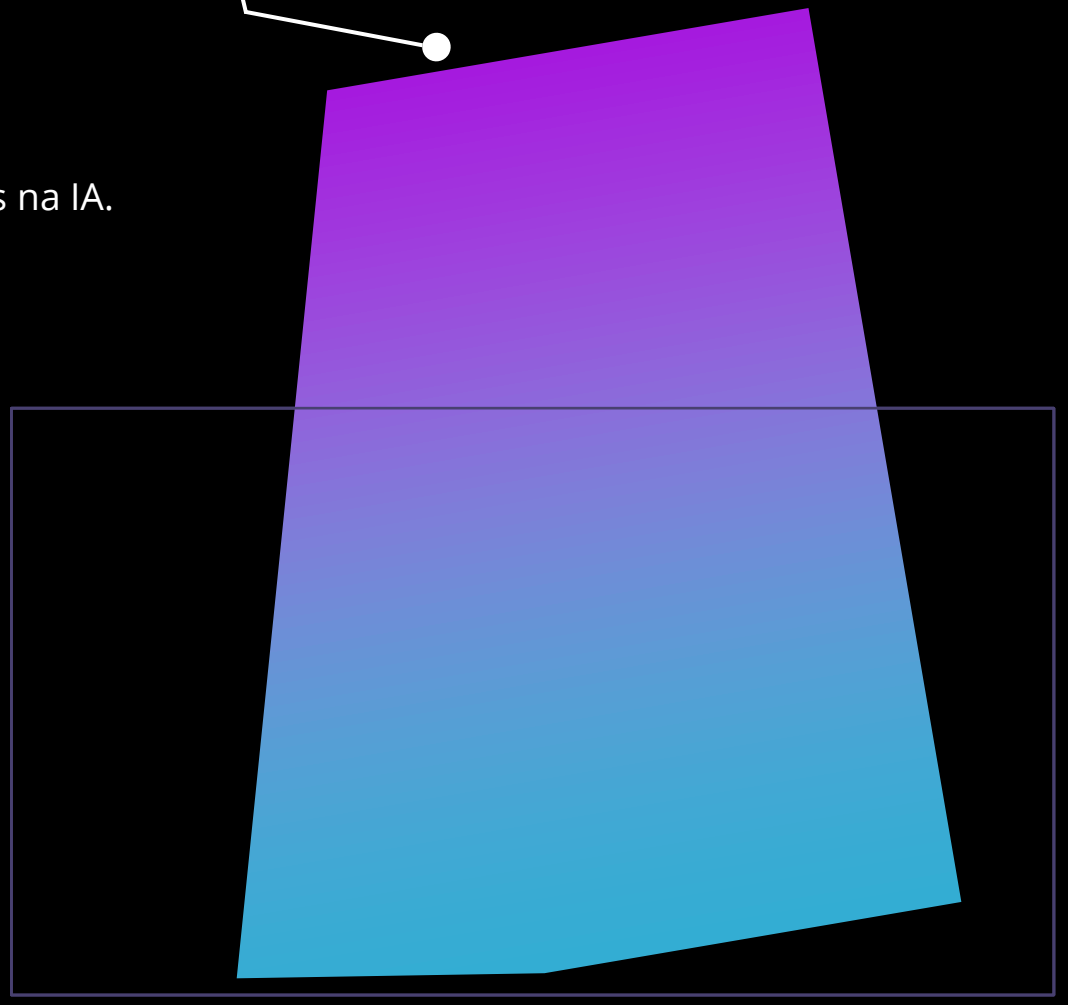
Podem ser usadas para invadir sistemas;

Inteligência Artificial Adversária;

Phishing em grande quantidade.

Dados de Treinamento Contaminados Para Aprendizado de Máquina (ML)

- O **aprendizado de máquina (ML)** é uma das técnicas usadas na IA.
- **Ponto fraco do ML:**
  - Dependência do conjunto de treinamento de dados.
- **Cuidados com o ML:**
  - Um conjunto ruim de dados pode oferecer alguns vieses (gaps) de segurança.
  - Cada atualização pode manchar o conjunto de dados.



Segurança dos Algoritmos de Aprendizado de Máquina

É preciso ficar de olho no algoritmo de aprendizado.

Invasores podem criar conjuntos de dados que passem pelo algoritmo de ML.

Fundamental para a segurança:
cuidar dos parâmetros.

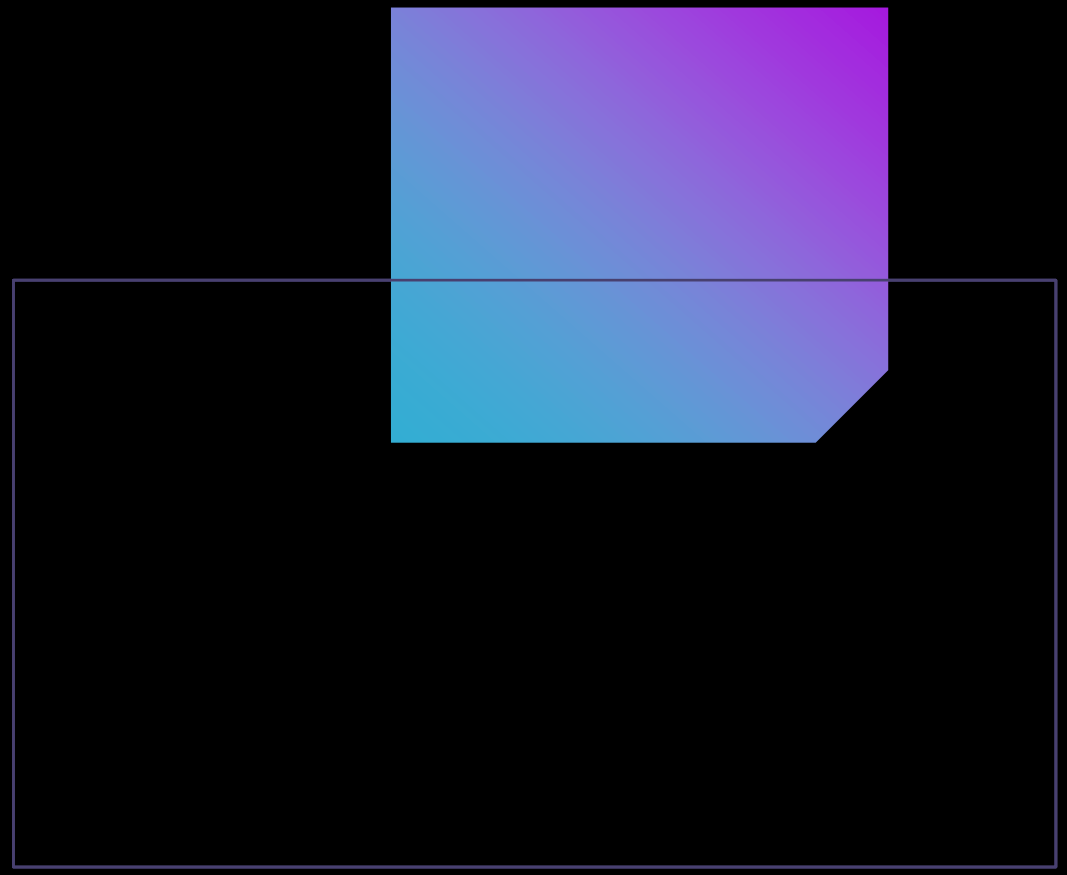
Ataques à Cadeia de Suprimentos

- **Uma rede de fornecedores que fornece o material para que algo seja construído.**
- **Cadeia de suprimentos na TI:**

A cadeia de suprimentos do computador fornece uma peça.

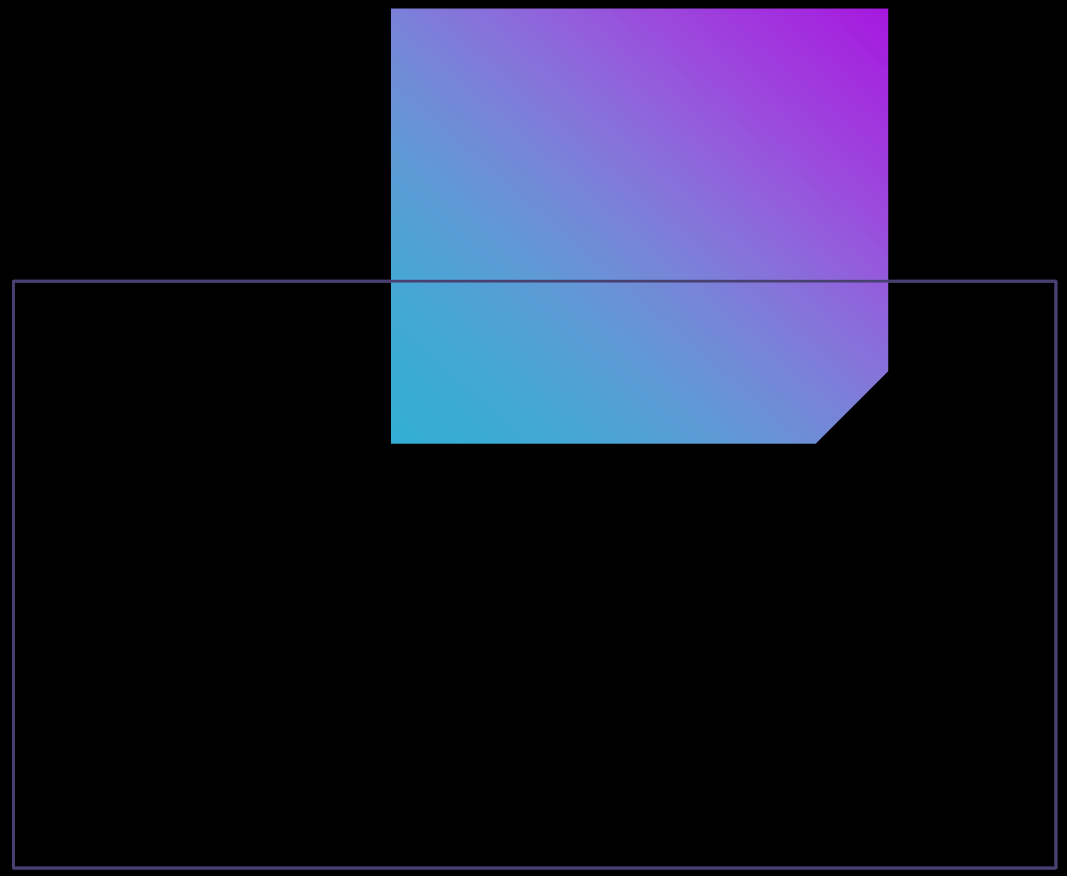
No caso de um programa, programadores e bibliotecas fazem parte dessa cadeia.

Peças de suprimentos podem ter vulnerabilidades.



Ataques Baseados na Nuvem vs. No Local

- É preciso escolher um fornecedor de nuvem com uma solução de segurança que faça parte do pacote.
- Cuidados:
  - Nem todos os fornecedores têm o mesmo nível de proteção;
  - Adotar a nuvem não garante segurança;
  - É preciso definir a segurança que deseja.



Ataques Criptográficos

- **Ataques criptográficos**
  Atacam o sistema de criptografia.

- **É projetado para tirar proveito de duas fraquezas específicas:**

  - A confiança inabalável de pessoas pela criptografia;
  - Fraquezas algorítmicas que podem ser exploradas pelo atacante.

Ataque de Aniversário

Tipo especial de ataque de força bruta.

Como funciona:

- Paradoxo de aniversário;
- Equação:

  $1,25k^{1/2}$, (com k = conjunto de valores possíveis);
- Esse mesmo cálculo se aplica a senhas de um grupo fechado.

Ataque de Colisão

Onde duas entradas diferentes produzem a mesma saída de uma função hash.

Como funciona:

- Manipulação de dados;
- Um invasor tem a chance de criar um arquivo com conteúdo visível alterado, porém com hashes idênticos.

Downgrade

Transport Layer Security/Secure Sockets Layer (TLS/SSL)
Uma especificação de conjunto de cifras pode ser empregada.

O invasor força o uso de uma conexão de rede entre dois sistemas com uma criptografia mais fraca.

O invasor aproveita a criptografia menos segura para realizar a quebra de comunicação.

OBRIGADO!

OUTROS TIPOS DE
ATAQUES CIBERNÉTICOS