Falhas em Programas

Vinícius da Silveira Serafim
professor@serafim.eti.br

Erro, Falha e Defeito

- Erro
- Falha (PFLEEGER 2006, p. 100)
  - "O que o desenvolvedor vê"
  - Falha leva ao defeito
- Defeito (PFLEEGER 2006, p. 100)
  - Desvio da especificação do sistema
  - "O que o usuário vê"

Corrigindo falhas

- Qual é o melhor?
  - Um programa em que foram econtradas e corrigidas 100 falhas; ou
  - Um programa em que foram econtradas e corrigidas 20 falhas.
- Um programa com muitas falhas iniciais tende a ter muitas outras por serem descobertas. (PFLEEGER 2006, p. 100)

Patch

- "Torna o sistema mais inseguro pois frequentemente introduz novas falhas"
(PFLEEGER 2006, p. 100)
  - Foco na falha em si e não no seu contexto
  - Nem todos os efeitos da falha são conhecidos
  - Correção da falha causa outros problemas em outras partes do código
  - Correção inadequada por questões de

Falhas maliciosas, ou não

- Não maliciosas
  - Não há intenção de induzir uma falha
  - São acidentais, resultado de descuido
- Maliciosas
  - Propositais
  - Cuidadosamente elaboradas
- Independente do caso, temos que tratar seus efeitos (PFLEEGER 2006, p. 101)

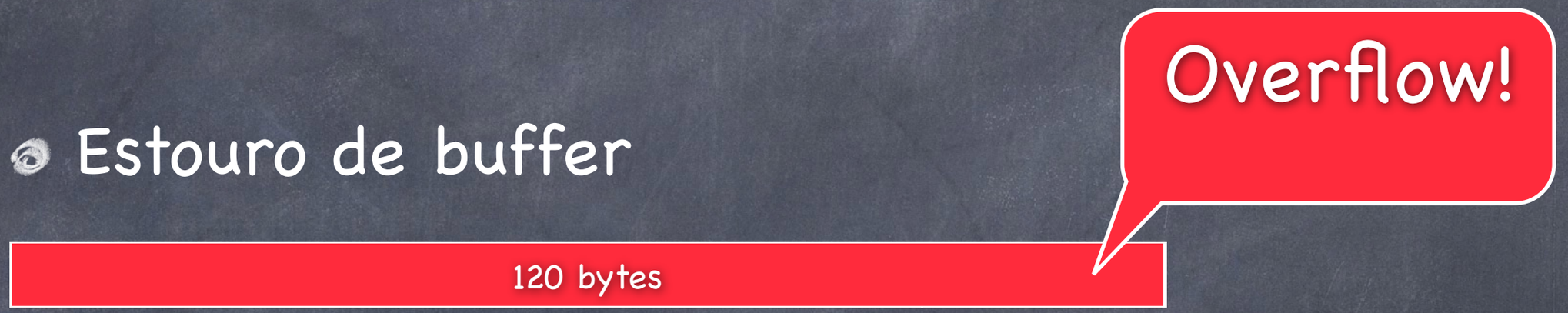
Para pensarmos

- "Erros humanos não intencionais são mais numerosos e causam muito mais estrago."
- "Falsas soluções de segurança impedem o progresso real na direção de programação mais segura." (GASSER 1988, em PFLEEGER, 2006 p. 102)
- "É quase impossível garantir que um programa faça precisamente o que seu projetista ou usuário esperam que faça e nada mais." (PFLEEGER 2006, p. 102)

Erros de programação não maliciosos

Buffer Overflow

- Estouro de buffer



- Em linguagem C

```
char buffer[100];


buffer[100] = ‘B’;

buffer[i] = ‘B’;
```

Buffer Overflow

- O que pode estar depois do buffer?
  - Dados ou código do usuário
  - Dados ou código do sistema
- O que o atacante pode fazer?

Mediação Incompleta

http://site.com/ordem.php?
prod=3928&qtd=10&preun=30&envio=sedex

http://site.com/ordem.php?
prod=3928&qtd=10&preun=15&envio=sedex

Mediação Incompleta

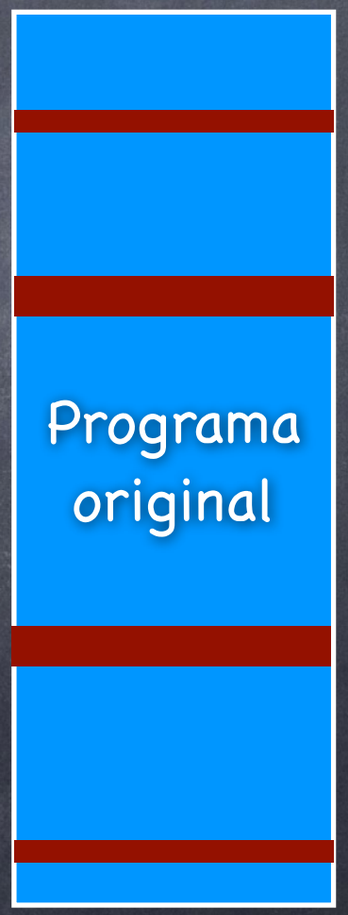
- Falha na checagem dos parâmetros recebidos do usuário ou de outras fontes não controláveis
  - Ausência de checagem
  - Checagem realizada apenas no lado do cliente (client-side). Ex.: JavaScript e campos escondidos ou bloqueados

Códigos Maliciosos Genéricos

Afetam usuários de sistemas de forma indiscriminada

Vírus

- Capaz de se autorreplicar
- Infecta programas não maliciosos



Porém não apenas programas

- Documentos
- Setor de boot dos discos
- Código residente em memória

Como encontrar um vírus?

- Assinatura do vírus
  - Um padrão particular no seu código
  - Um padrão de armazenamento
  - Um padrão de execução
- Vírus polimórficos
  - Trocam sua aparência
  - Códigos equivalentes ou mesmo cifrados

O que um vírus pode fazer?

- "O dano é limitado apenas pela criatividade do autor do vírus." (PFLEEGER 2006, p. 126)

Para pensarmos (PFLEEGER 2006, p. 126)

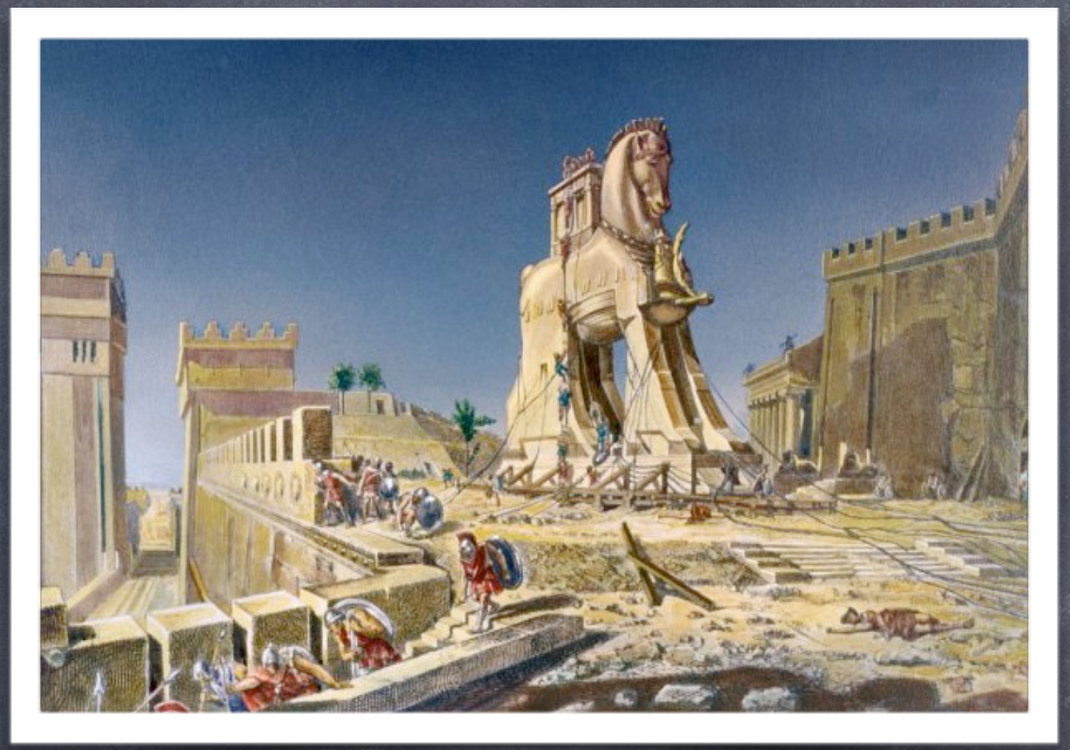
- "Vírus afetam somente sistemas Microsoft Windows." ✖
- "Vírus podem modificar arquivos escondidos ou somete-leitura." ✔
- "Vírus só se espalham por discos ou e-mails." ✖
- "Vírus não podem infectar hardware." ✔ ✖

Outros códigos maliciosos

- Worm (verme)
  - Se espalha pela rede e existe de forma independente de um outro arquivo ou programa
- Rabbit (coelho)
  - Vírus ou Worm que se autorreplica sem limite

Outros códigos maliciosos

- Cavalo-de-tróia



- Bomba lógica

Códigos Maliciosos Especializados

Escritos com um objetivo específico e especificamente para um sistema, uma aplicação

Trapdoor ou Backdoor

- "Um ponto de entrada não documentado"
- Muito usado por desenvolvedores
  - E depois de esquecidos vão parar em ambiente de produção
- Algumas vezes deixados intencionalmente
  - Visando uma futura manutenção
  - Ou visando acesso não autorizado

RootKits

- Um programa ou conjunto de programas
- Realiza atividades como
  - Esconder processos não autorizados
  - Esconder arquivos de um invasor
- O RootKit intercepta e filtra os resultados dos comandos do sistema

Keylogger

- Capturar o que é digitado no teclado
- Programa ou Hardware
- Às vezes é instalado pelo atacante em seu próprio computador

Outros códigos maliciosos

- Ilusões da Interface
- Man-in-the-Middle
- Escalada de privilégios