Programação de jogos em rede

Marcelo Henrique dos Santos

www.marcelohsantos.com.br

Programação de jogos em rede

Aula 5:

Segurança

MARCELO HENRIQUE DOS SANTOS

Segurança

Ao conectar um computador a uma rede, é necessário que tome as providencias para se certificar que esta nova máquina conectada possa não vir a ser um “portão” que servirá de entrada de invasores, ou seja, de pessoas que estão mal intencionadas, procurando prejudicar alguém ou até mesmo paralisar a rede inteira.

Embora haja sistemas que conseguem fornecer um grau de segurança elevado, mesmo sendo bem configurado ainda estará vulnerável.

Segurança

Jogos em rede, como qualquer sistema complexo online, têm diversos pontos passíveis de ataque. A exploração de pontos fracos em jogos digitais pode trazer prejuízos para os jogadores, desenvolvedores e publicadores.

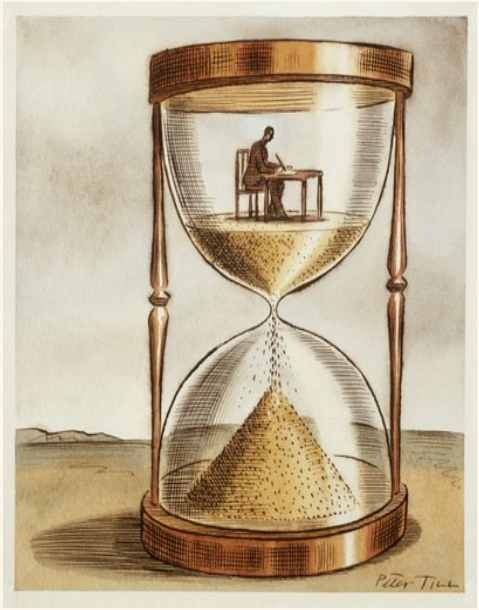
Ataques

Ataques

Um ataque, ao ser planejado, segue um plano de estratégia sobre o alvo desejado, e uma pessoa experiente em planejamento de ataque sempre traça um roteiro a ser seguido a fim de alcançar o objetivo.

Roteiro de um possível ataque

Um exemplo de roteiro organizado para atacar é exemplificado a seguir:

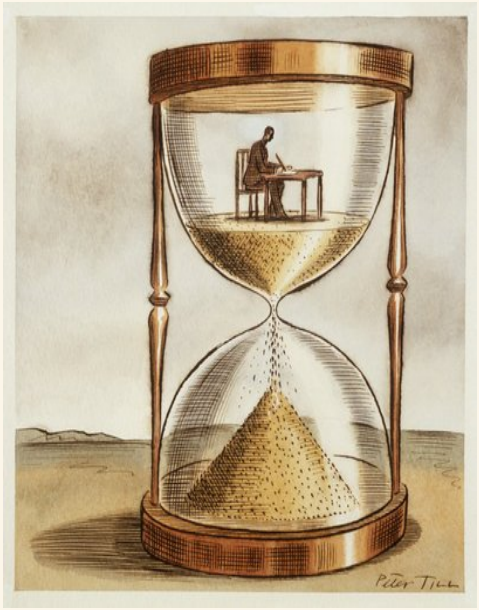


1. **Localizar o alvo desejado**;

2. **Concentrar o máximo de informações possíveis** sobre o alvo, geralmente utilizando alguns serviços da própria rede, ou até mesmo, ferramentas utilizadas na administração e gerenciamento da rede alvo;

Roteiro de um possível ataque

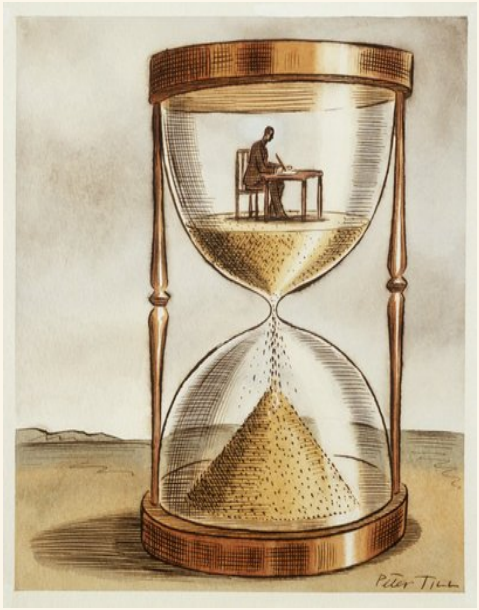
3. **Disparar o ataque sobre o alvo**, a fim de invadir o sistema, explorando a vulnerabilidade do sistema operacional, servidores e serviços oferecidos pela rede.



O invasor pode até mesmo
Abusar um pouco da sorte
Tentando adivinhar uma senha
na máquina alvo, fazendo combinações possíveis;

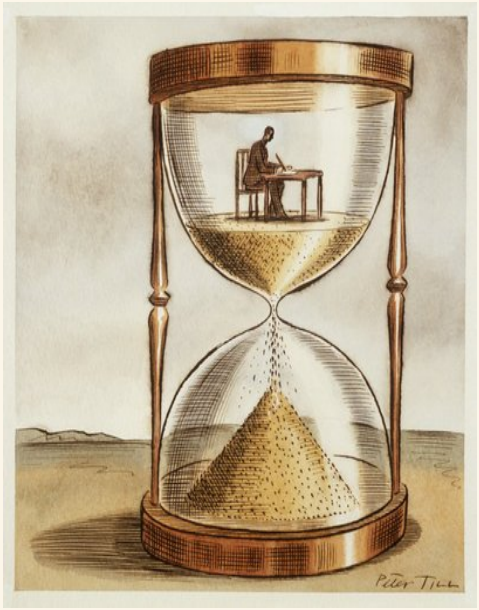
Roteiro de um possível ataque

4. **Não deixar pistas da invasão**, pois geralmente as ações realizadas pelos invasores são registradas no sistema alvo em arquivos de log, possibilitando que o administrador do sistema invadido possa vir a descobrir a invasão, a não ser que o invasor se preocupe em eliminar todos e quaisquer vestígios que o incriminem;



Roteiro de um possível ataque

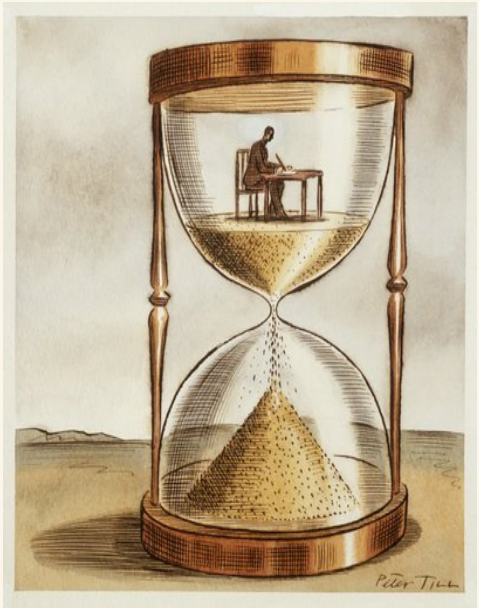
5. O invasor deve conseguir não somente senhas de usuários comuns, pois os privilégios destes usuários são limitados, não dando acesso a recursos mais abrangentes no sistema.



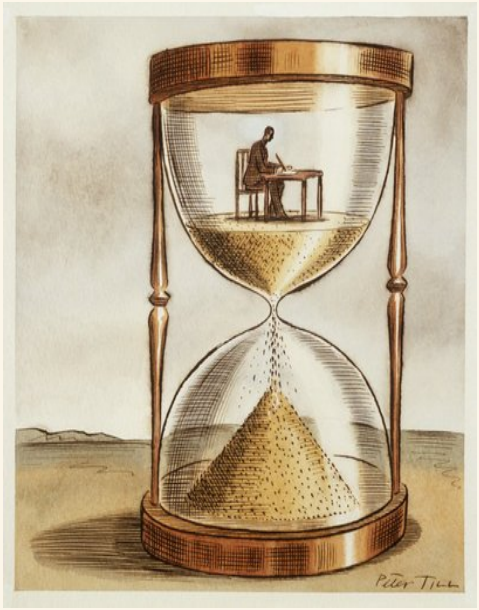
Com isso, é de grande importância que o invasor consiga **uma senha de administrador**, pois terá todos os recursos de gerenciamento do sistema disponíveis, para alterações e até mesmo gerar bug no sistema.

Roteiro de um possível ataque

Instalar ferramentas que façam a captura de senhas de forma clandestina aos olhos do administrador, para isso existem programas que conseguem rodar em segundo plano sem que a vítima perceba, podendo ser colocados na pasta usada pela vítima;

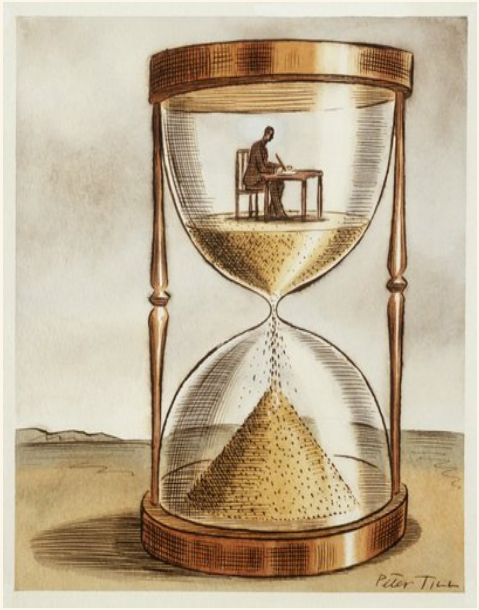


Roteiro de um possível ataque



6. **Criar caminhos alternativos de invasão**, logo que a administradora do sistema encontrar uma “porta aberta” que permita a invasão esta será fechada, mas se o invasor gerar outras maneiras de invadir o sistema, certamente terá outra chance de invasão, já que teve a preocupação de criar novas rotas alternativas;

Roteiro de um possível ataque



6. **Criar caminhos alternativos de invasão**, logo que a administradora do sistema encontrar uma “porta aberta” que permita a invasão esta será fechada, mas se o invasor gerar outras maneiras de invadir o sistema, certamente terá outra chance de invasão, já que teve a preocupação de criar novas rotas alternativas;

Políticas de Segurança

MARCELO HENRIQUE DOS SANTOS

Políticas de Segurança

As decisões relacionadas à segurança que você toma, ou não, sendo um administrador, em grande parte determinam o quão segura ou insegura sua rede é.

Você não pode tomar boas decisões sem determinar primeiro quais são **suas metas de segurança**.

Políticas de Segurança

Suas metas serão determinadas em grande parte pelos seguintes pontos chaves:

1. **Serviços oferecidos X Segurança provida**

Cada serviço oferecido aos usuários apresenta um próprio risco de segurança. Para alguns serviços, o risco excede em valor o benefício do serviço e o administrador pode escolher eliminar o serviço em lugar de tentar deixá-lo seguro.

Políticas de Segurança

2. **Facilidade de uso X Segurança**

O sistema mais fácil de usar permitiria acesso a qualquer usuário e não requereria senha; isso quer dizer, não haveria nenhuma segurança.

Políticas de Segurança

2. **Facilidade de uso X Segurança**

Requerer senhas torna o sistema um pouco menos conveniente, mas mais seguro. Requerer senhas geradas em dispositivos que as alteram toda vez que você se “loga”, faz o sistema até mesmo mais difícil para uso, mas muito mais seguro.

Políticas de Segurança

3. **Custo de segurança X risco de perda**

Existem muitos custos referentes à segurança: **monetário**, **desempenho e facilidade de uso**.

Políticas de Segurança

3. **Custo de segurança X risco de perda**

Também há muitos níveis de risco: **perda de privacidade** (a leitura de informação por indivíduos sem autorização), **perda de dados** (a corrupção ou deleção de informação) **e a perda de serviço**

Políticas de Segurança

3. **Custo de segurança X risco de perda**
(por exemplo, o preenchimento do espaço de armazenamento de dados, uso de recursos computacionais, e negação de acesso à rede).
Cada tipo de custo deve ser pesado contra cada tipo de perda.

Políticas de Segurança

Suas metas devem ser comunicadas aos envolvidos no projeto de desenvolvimento do game através de um conjunto de regras de segurança, chamadas **"política de segurança"**.

Políticas de Segurança

Suas metas serão determinadas em grande parte pelos seguintes pontos chaves:

Suas metas devem ser comunicadas aos envolvidos no projeto de desenvolvimento do game através de um conjunto de regras de segurança, chamadas **"política de segurança"**.

Definição dos Planos de Segurança

Pós-graduação em Games - Programação e Produção
Programação de jogos em rede
MARCELO HENRIQUE DOS SANTOS

Definição dos Planos de Segurança

- Uma lista dos serviços de rede que serão oferecidos;
- Quais áreas da organização proverão os serviços;
- Quem terá acesso a esses serviços;
- Como será provido o acesso;
- Quem administrará esses serviços; etc.

Protegendo os Serviços

Um ataque próspero em um destes serviços pode produzir desastres de grandes proporções;

- Serviço de Nomes;
- Serviço de Senhas/Chaves;
- Serviço de Autenticação/Proxy;
- Transferência de Arquivos;

Exemplo de ataques em jogos em rede

Inserção de Bots

MARCELO HENRIQUE DOS SANTOS

Inserção de Bots

Jogos em tempo real normalmente exigem do jogador, além do raciocínio para definição da estratégia, reflexos.

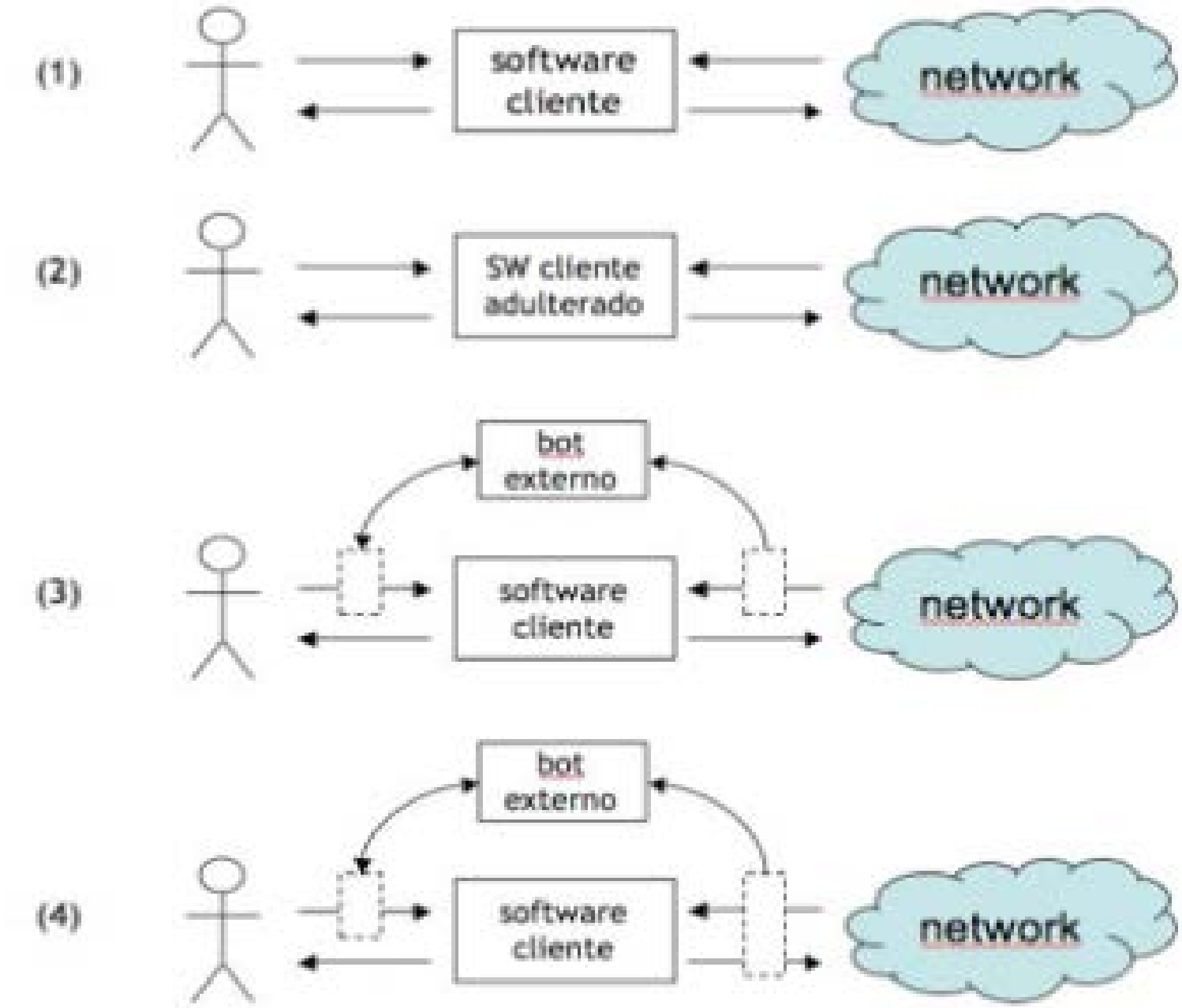
Esta é a **oportunidade** ideal para se trapacear com agentes artificiais “inteligentes”, os chamados Bots.

Inserção de Bots

Dentre as maneiras de fazer um agente de software responder no lugar do jogador estão:

1. Adulteração do software-cliente;

2. Espionagem no input que o software-cliente recebe pela rede e geração de sinais nas interfaces de mouse e teclado (sinais que o software-cliente recebe do jogador).


(1)
software cliente
network
(2)
SW cliente adulterado
network
(3)
bot externo
software cliente
network
(4)
bot externo
software cliente
network

Exemplo de ataques em jogos em rede

Falsificação de identidade

MARCELO HENRIQUE DOS SANTOS

Falsificação de identidade

No mundo online, como não se vê a pessoa propriamente, torna-se aparentemente fácil mentir a identidade.

Quase todos os sistemas online que se preocupam com identidade hoje tem um padrão de identificação que envolve senhas.

Alguns sistemas mais sofisticados pedem uma composição de algo que a pessoa conhece (senha) com algo que ela possui (um cartão, por exemplo), como os sistemas de banco.

Exemplo de ataques em jogos em rede

Sequestro de sessão

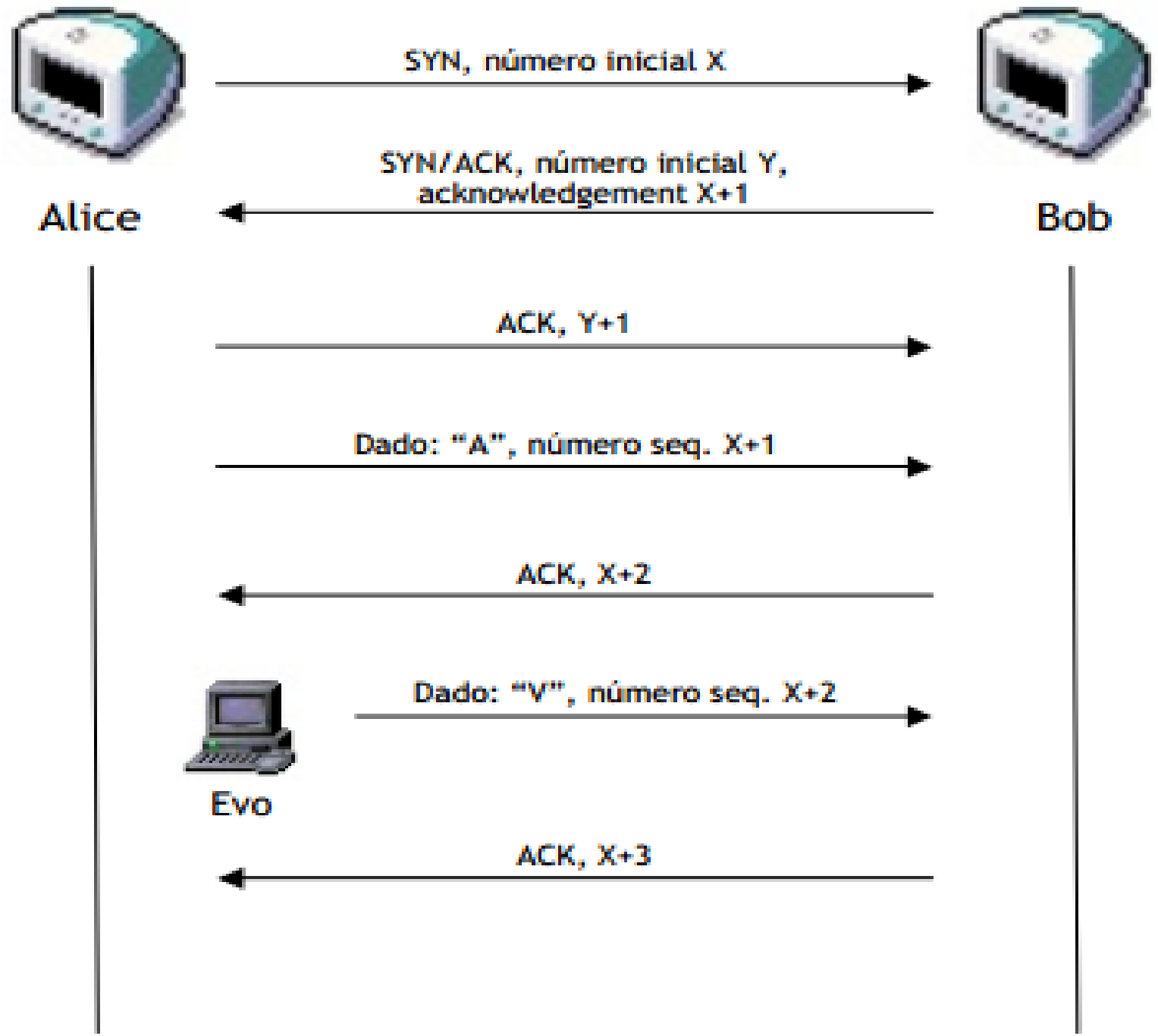
MARCELO HENRIQUE DOS SANTOS

Sequestro de sessão

Uma das maneiras de se passar por alguém no mundo online é sequestrando uma sessão.

E como se Alice telefonasse a Bob e, de repente, Evo tomasse o telefone da mão de Alice.

No telefone isso seria engraçado, porque Evo teria que imitar a voz de Alice e talvez Bob percebesse. A voz ao telefone funciona como uma assinatura. No mundo online, como nem sempre se assina cada mensagem (porque isso pode custar caro), o sequestro de sessão é menos perceptível.


SYN, número inicial X
SYN/ACK, número inicial Y,
acknowledgement X+1
Alice
Bob
ACK, Y+1
Dado: "A", número seq. X+1
ACK, X+2
Dado: "V", número seq. X+2
Evo
ACK, X+3

Exemplo de ataques em jogos em rede

Escuta clandestina (grampo)

MARCELO HENRIQUE DOS SANTOS

Escuta clandestina (grampo)

Instalar uma escuta clandestina no PC de um jogador adversário pode revelar login, senha e permitir a falsificação de identidade.

A escuta pode ser instalada de várias formas. Há vírus e cavalos de tróia criados especialmente para isto, mas a escuta também pode ser instalada em locais por onde a informação trafega aberta.

Exemplo de ataques em jogos em rede

Escuta dos dados enviados e recebidos pela aplicação cliente

MARCELO HENRIQUE DOS SANTOS

Escuta dos dados

Em jogos que não adotam mecanismos seguros de conexão, pode-se obter informação observando os dados que trafegam pela interface de rede.

Neste caso, a aplicação, em vez de modificar o jogo, terá que funcionar conjuntamente com o jogo, prestando atenção nos estados do game e mostrando ao jogador.

Escuta dos dados