UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia e Certificação Digital
Primeira Aula

Prof. Frederico Sauer, D.Sc.

Construindo Alicerces: Apresentações

- Apresentação do Professor
- Apresentação do Curso
  - Conhecendo os objetivos
  - Conhecendo a bibliografia e conteúdos
  - Avaliações
  - Atividades Práticas
- Bibliografia
  - Criptografia e Segurança de Redes – 4ª edição – William Stallings – Ed. Pearson

Professor

- Prof. Frederico Sauer (Fred)
  - Mestre e Doutor UFRJ com dissertação e tese em Segurança e Gerenciamento de Redes
  - Professor Adjunto UEZO desde 2013
  - Professor Convidado FGV Management
  - Gerente de TI de 90 a 2010
  - Auditor de SegInfo na Marinha de 99 a 2010

Objetivos

- Preparar o profissional para a função de *Security Officer*
  - ISO 27001:2006
  - ISO 27002:2007
  - ISO 27005:2009
- Nas cadeiras → Associação dos conceitos com as práticas reais do mercado
- Importância da prática com as técnicas e ferramentas → diferencial de Mercado

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Vamos Trabalhar !

Aula 1 – “O Universo em Desencanto...”

Teoria: Fundamentos de Segurança

Prática: Algumas Ferramentas úteis

Características do Cenário Atual

- A área da SegInfo vive em permanente mutação
  - Recursos computacionais disponíveis
  - Novas ameaças
- A Informação como ativo da corporação
- As redes como elemento social, econômico e político das pessoas
- Onde há recursos de valor, há criminosos

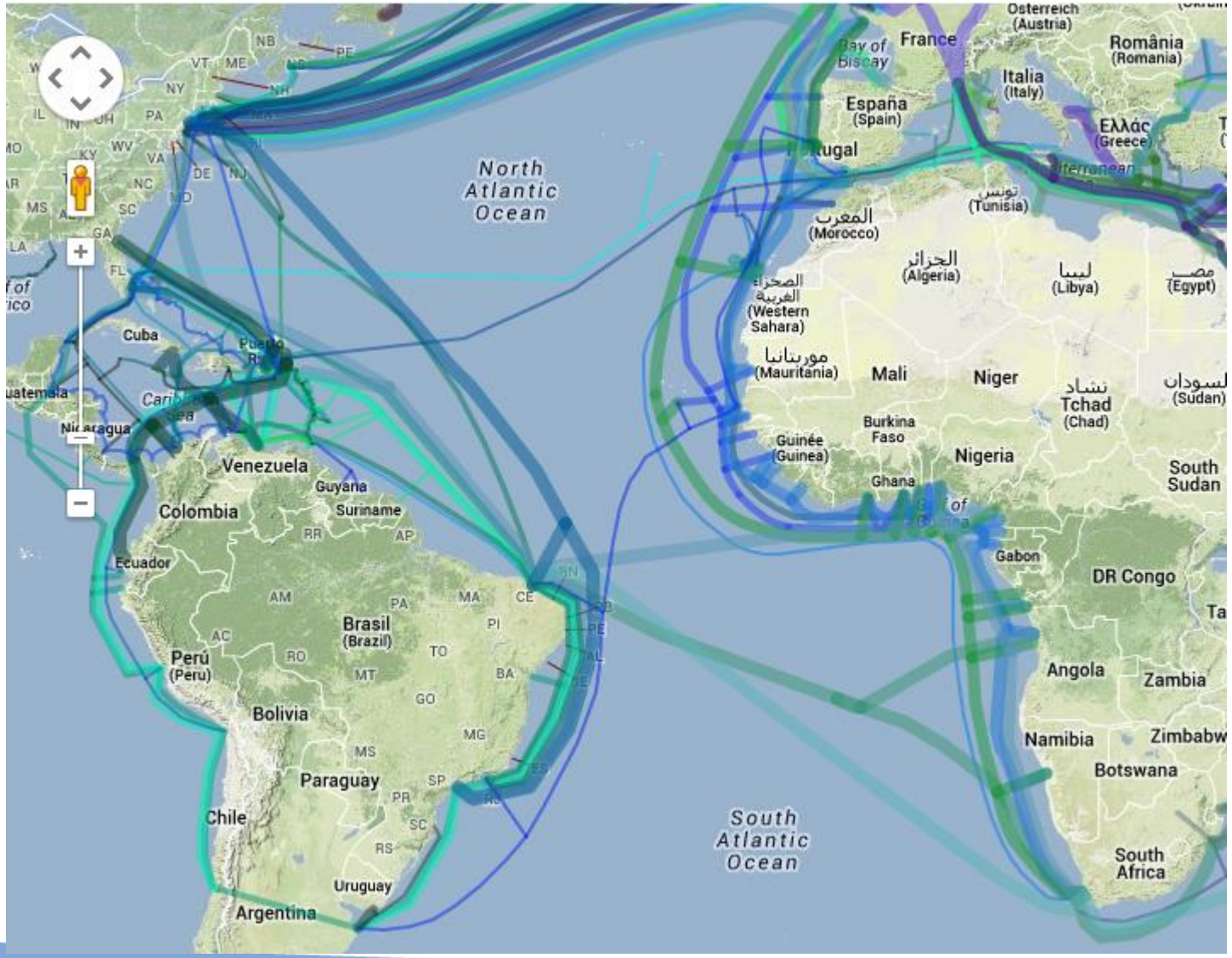
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Cyber War

- Palavras-chave:
  - Edward Snowden
  - NSA, FBI, CIA
  - Prism

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Como eles conseguem ?



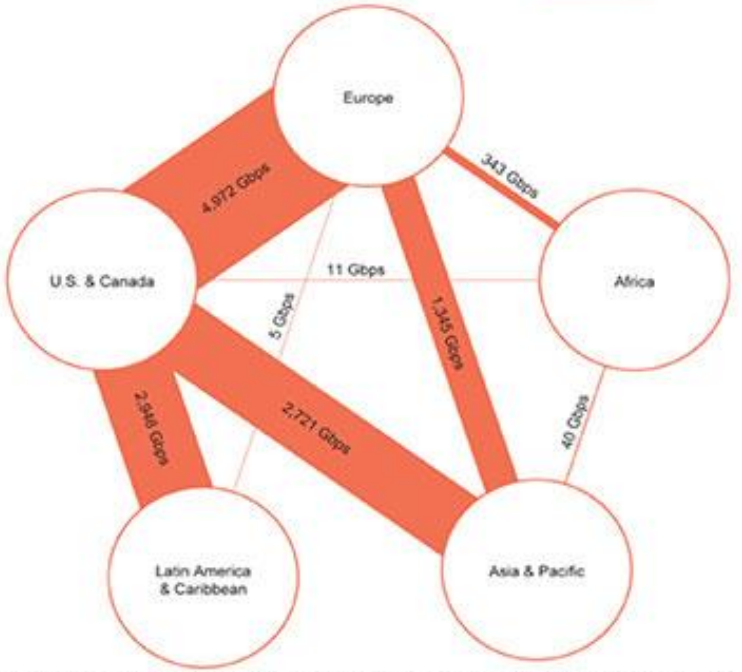
Didaticamente...

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



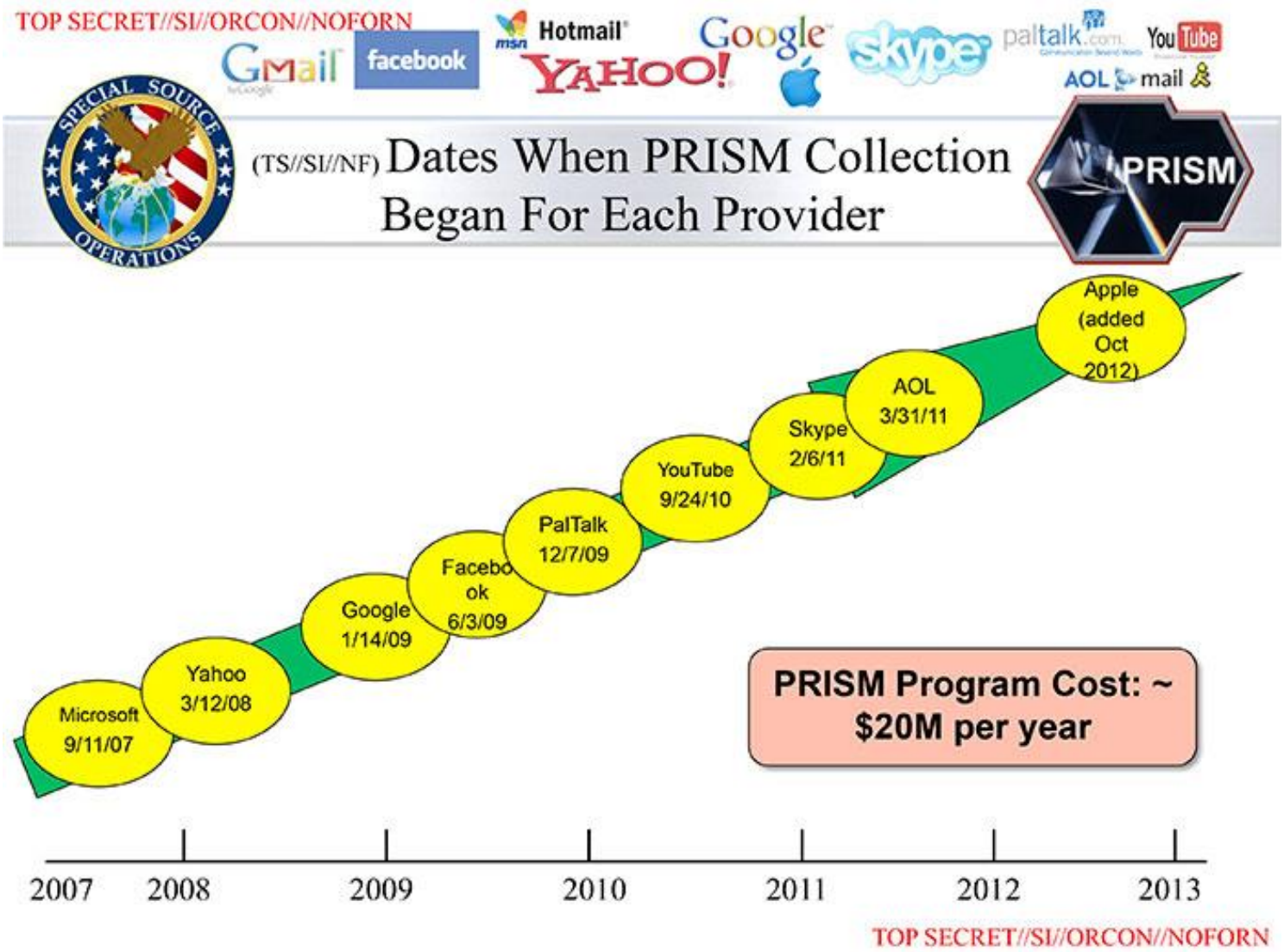
International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

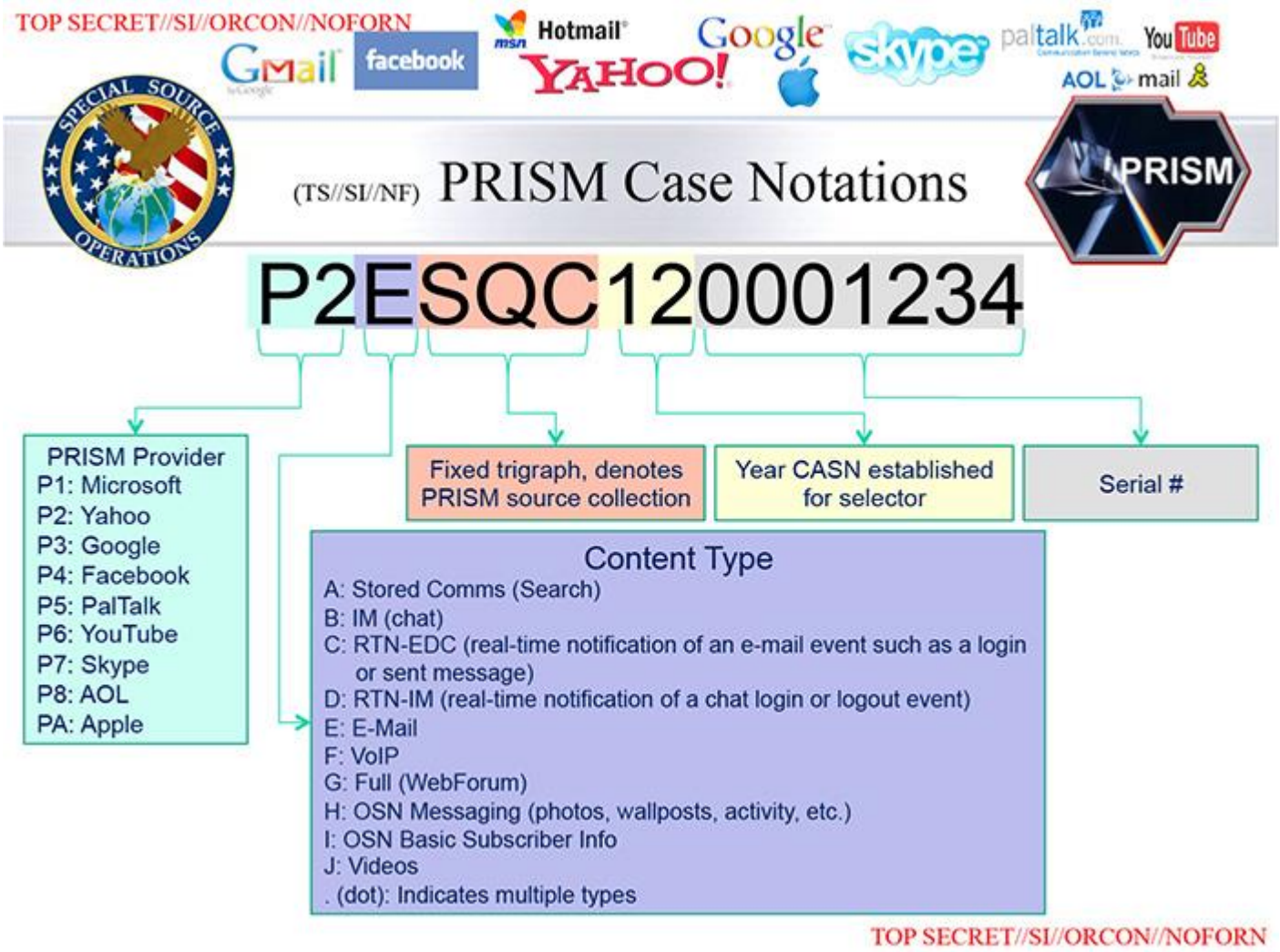
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Quando começaram ?



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

O que eles vêem ?



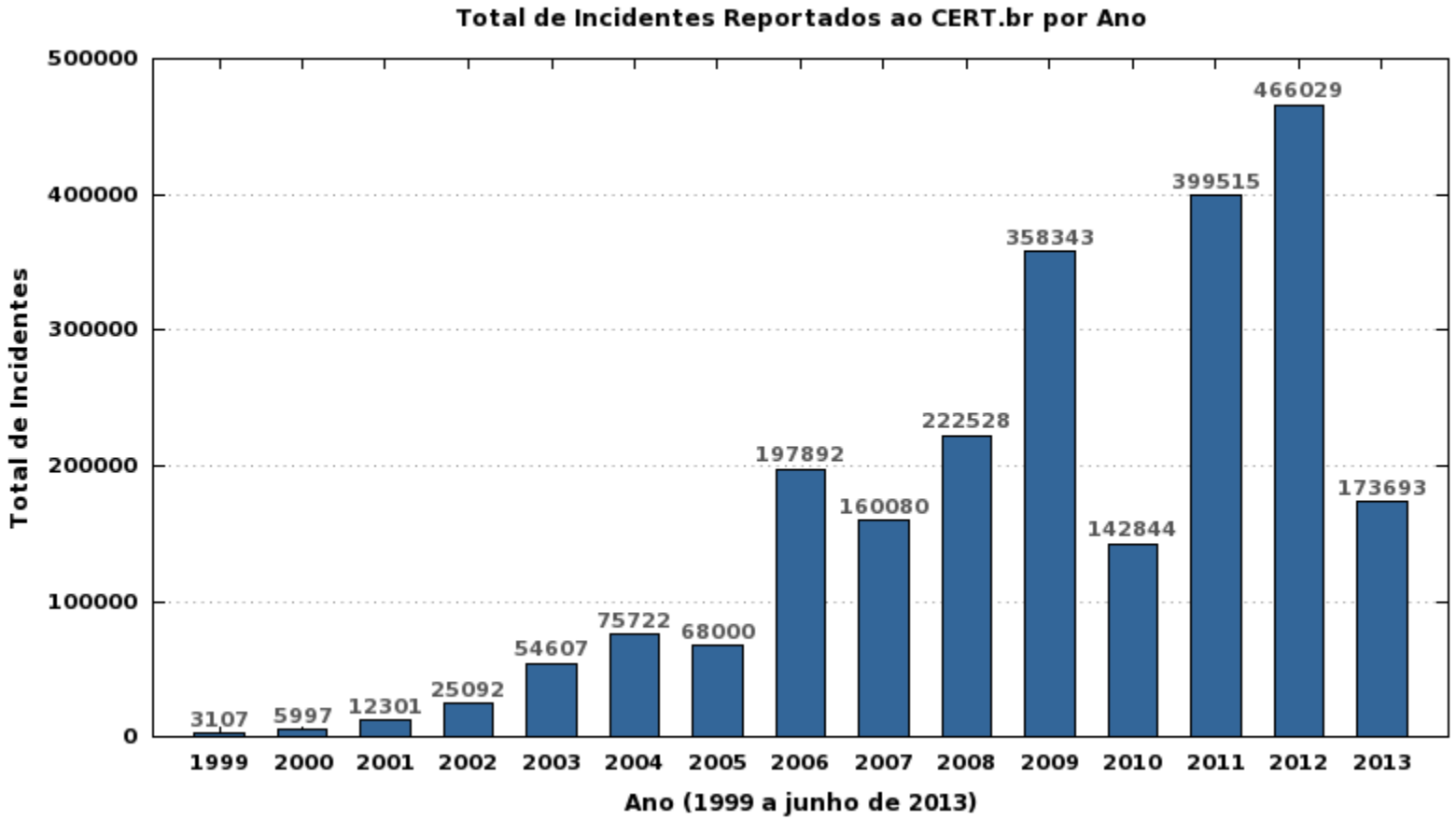
Por que chegaram a este ponto ?

- Richard A. Clarke – “Cyber War” (2010)
  - “Many nations can use cyber war against us and do great damage. The existence of a cyber war gap may tempt some nation to attack the United States” (pg. 149)

Nation	Cyber Offense	Cyber Dependence	Cyber Defense	Total
U.S.	8	2	1	11
Russia	7	5	4	16
China	5	4	6	15
Iran	4	5	3	12
North Corea	2	9	7	18

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

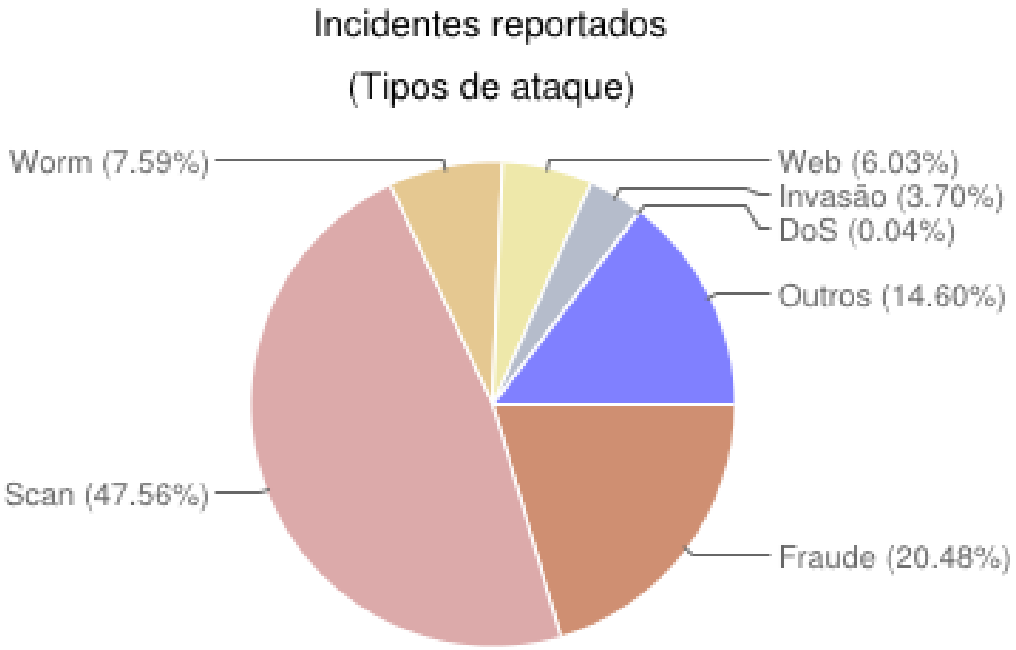
Algumas Estatísticas Locais



- Qual é a sua análise destes dados ?

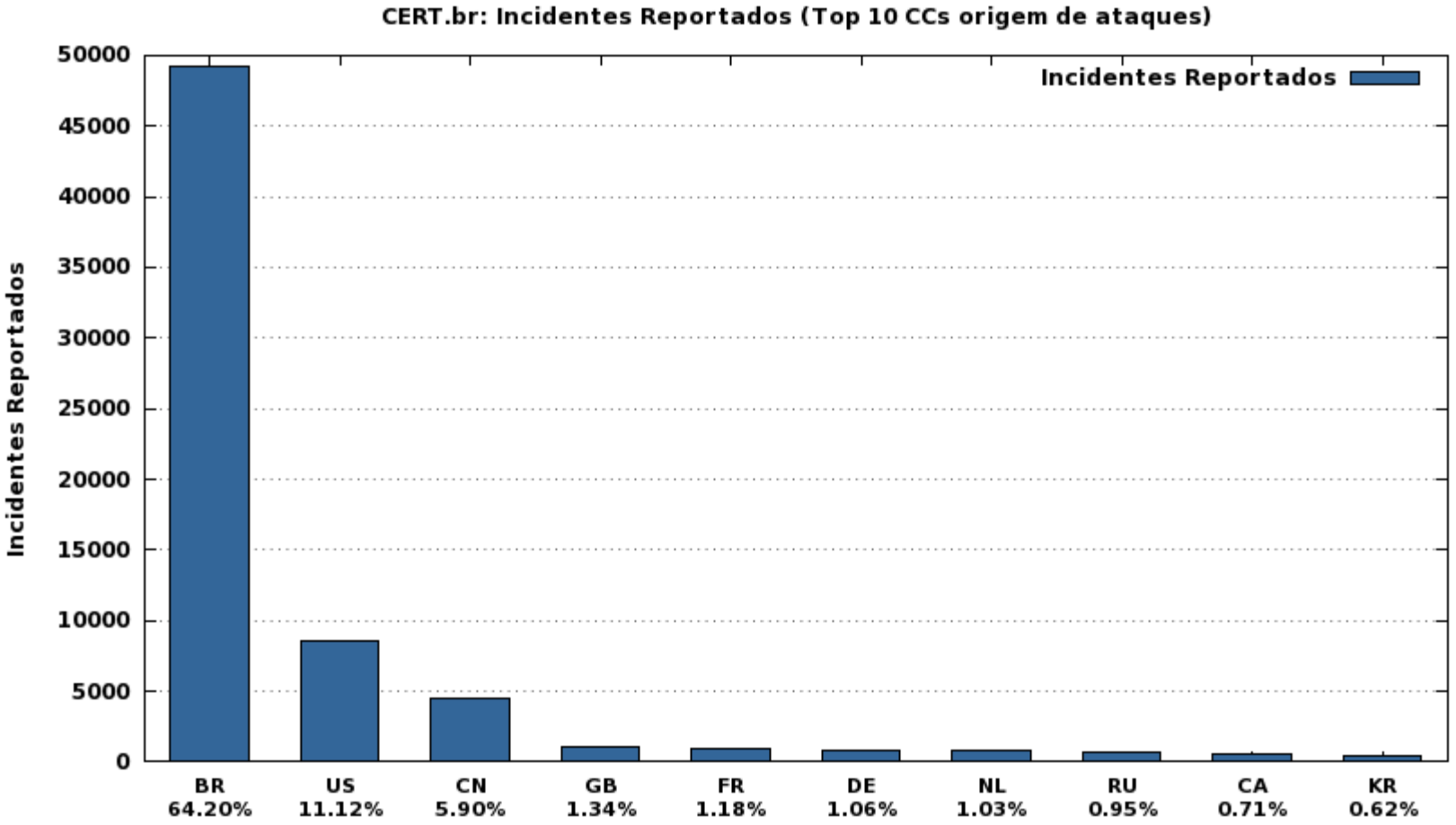
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Mais Estatísticas



- Escaneamentos e fraudes no top. Por que ?

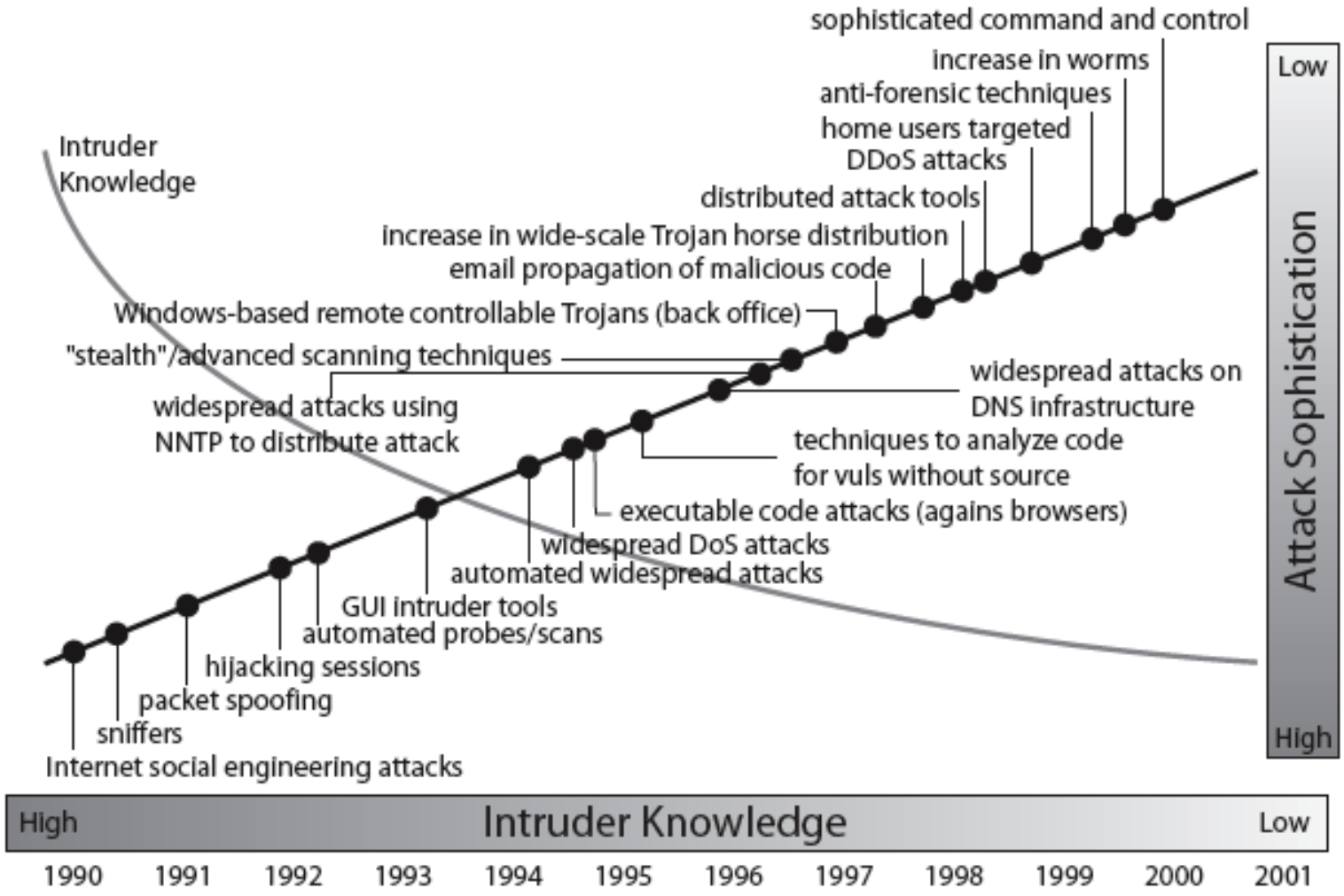
Questões Estratégicas



- Por que americanos e chineses ?

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Nível de Expertise do Intruso



Source: CERT

Elementos Essenciais

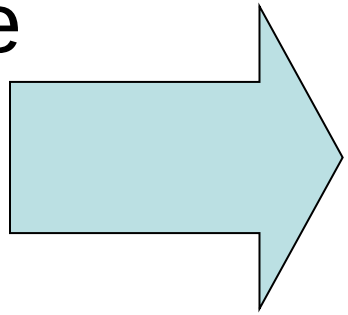
- Elementos do Risco à Segurança da Informação:
  - Vulnerabilidades
  - Ameaças
  - Impactos
  - Mecanismos de Segurança

$$R = \frac{V \times A \times I}{M}$$

- Para tratar os Riscos, os mecanismos são implementados de acordo com a classificação da informação

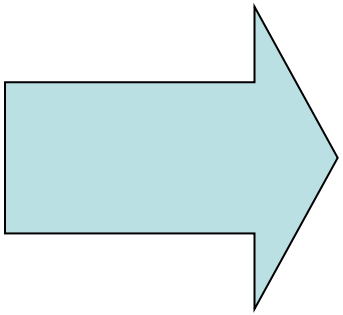
Serviços de Segurança

- Confidencialidade
- Integridade
- Disponibilidade



Base Normativa

- Autenticidade
- Legalidade
- Controle de Acesso
- Irretratabilidade (não-repúdio)



Sox, CVM, etc

X.800 ITU-T

MECANISMOS DE SEGURANÇA ESPECÍFICOS

Podem ser incorporados à camada de protocolo apropriada a fim de oferecer alguns dos serviços de segurança OSI.

Cifragem

O uso de algoritmos matemáticos para transformar os dados em um formato que não seja prontamente decifrável. A transformação e subseqüente recuperação dos dados depende de um algoritmo e zero ou mais chaves de criptografia.

Assinatura digital

Dados anexados a (ou uma transformação criptográfica de) uma unidade de dados que permite que um destinatário da unidade de dados comprove a origem e a integridade da unidade de dados e proteja-se contra falsificação (por exemplo, pelo destinatário).

Controle de acesso

Uma série de mecanismos que impõem direitos de acesso aos recursos.

Integridade de dados

Uma série de mecanismos utilizados para garantir a integridade de uma unidade de dados ou fluxo de unidades de dados.

Troca de informações de autenticação

Um mecanismo com o objetivo de garantir a identificação de uma entidade por meio da troca de informações.

Preenchimento de tráfego

A inserção de bits nas lacunas de um fluxo de dados para frustrar as tentativas de análise de tráfego.

Controle de roteamento

Permite a seleção de determinadas rotas fisicamente seguras para certos dados e permite mudanças de roteamento, especialmente quando existe suspeita de uma brecha de segurança.

Certificação

O uso de uma terceira entidade confiável para garantir certas propriedades de uma troca de dados.

MECANISMOS DE SEGURANÇA PERVASIVOS

Mecanismos que não são específicos a qualquer serviço de segurança OSI ou camada de protocolo específica.

Funcionalidade confiável

Aquela que é considerada como sendo correta em relação a alguns critérios (por exemplo, conforme estabelecido por uma política de segurança).

Rótulo de segurança

A marcação vinculada a um recurso (que pode ser uma unidade de dados) que nomeia ou designa os atributos de segurança desse recurso.

Detecção de evento

Detecção de eventos relevantes à segurança.

Registros de auditoria de segurança

Dados coletados e potencialmente utilizados para facilitar uma auditoria de segurança, que é uma revisão e exame independentes dos registros e atividades do sistema.

Recuperação de segurança

Lida com solicitações de mecanismos, como funções de tratamento e gerenciamento de eventos, e toma medidas de recuperação.

Disponibilidade – Considerada um serviço a ser anexado a cada mecanismo.

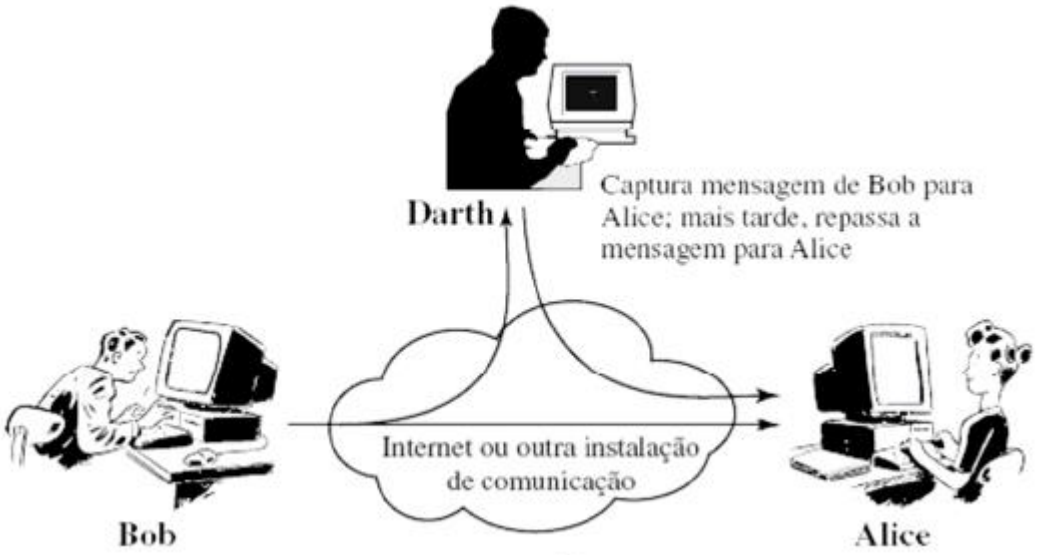
Ataques - Ameaças

- Formas de obter vantagens causando impactos
- As ações de segurança buscam sempre lidar com o risco da ocorrência destes ataques
  - Mitigar
  - Manter
  - Transferir
  - Eliminar
- Evento x Incidente de Segurança

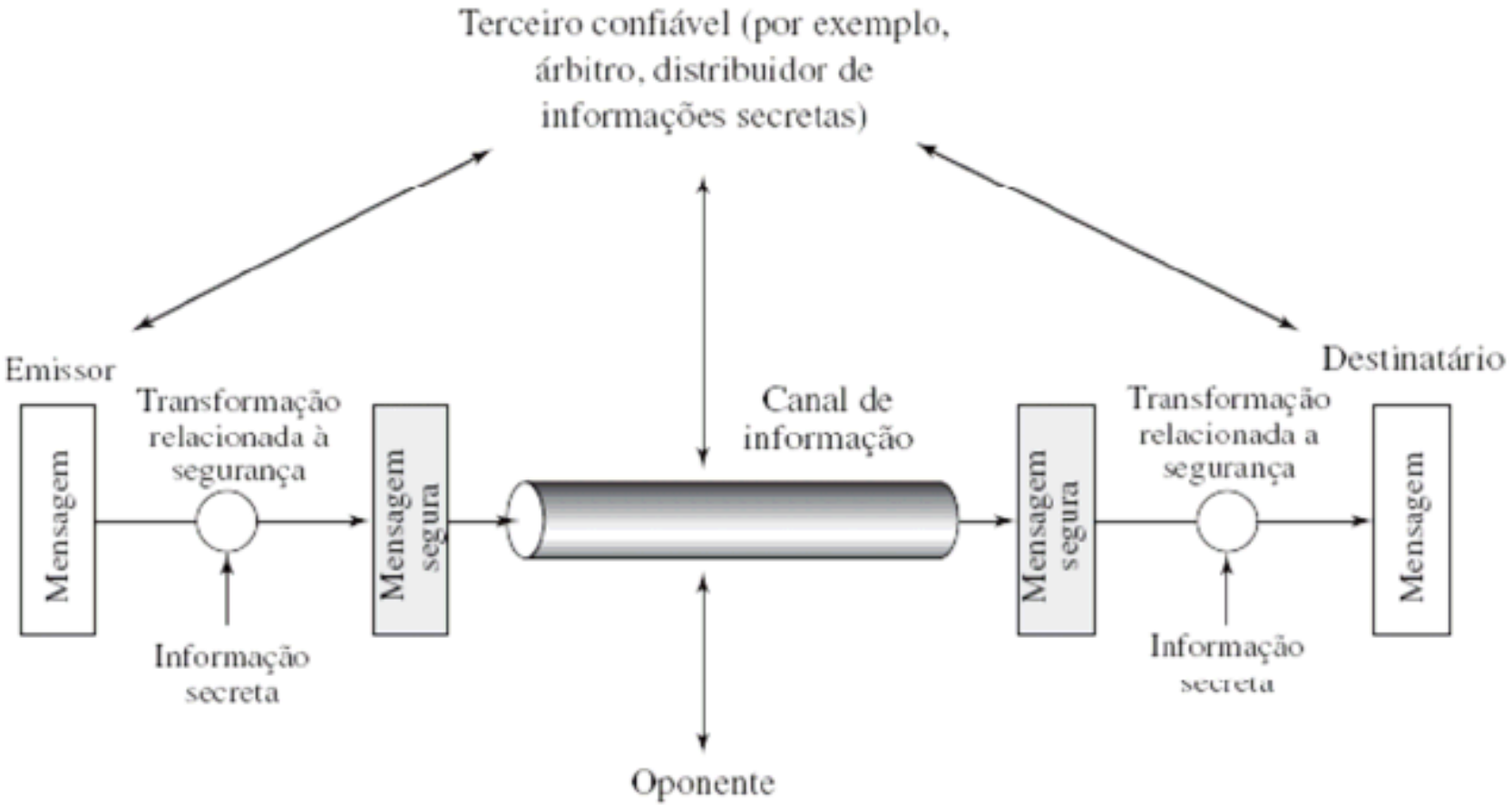
Taxonomia dos Ataques

Passivo

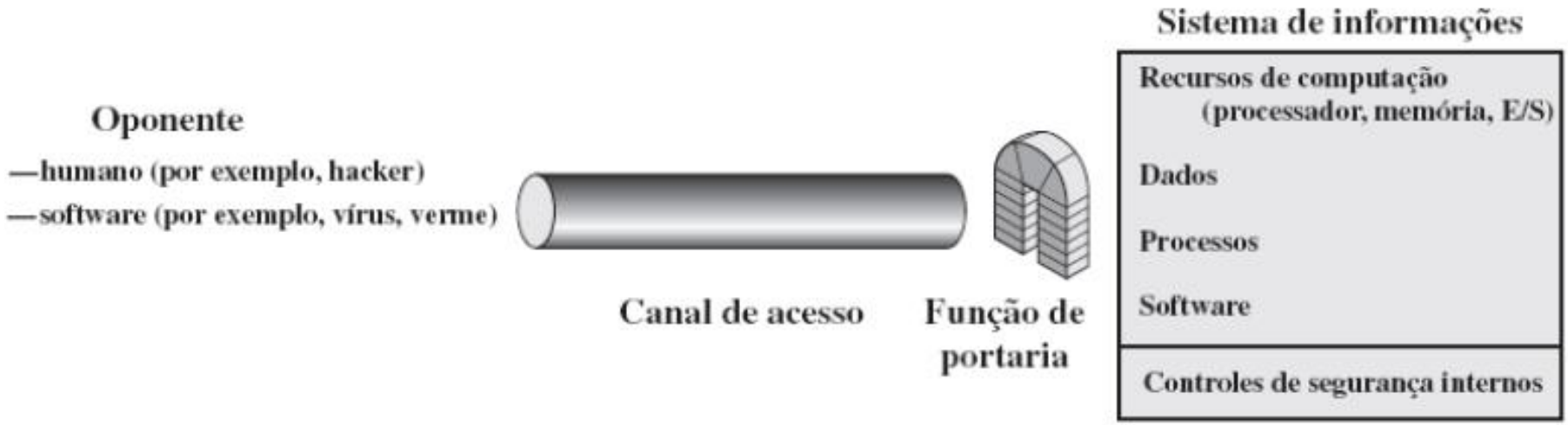
Ativo



Modelo de Segurança



Segurança no Acesso



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

TCP/IP – Por que é tão vulnerável ?

- Nascido no meio acadêmico
- Principal meta foi a tolerância a falhas
  - *r-utilities, telnet*
- Protocolos padronizados e disponíveis
- Sockets – transparentes para o usuário
- Ainda tem coisa pior:
  - NetBIOS/NetBEUI
  - SMB/CIFS

Algumas Potenciais Falhas

- Serviços acessíveis por portas
- *Three-way handshake*

$$
\begin{aligned}
C \rightarrow S: &\quad SYN(\mathrm{ISN}_C) \\
S \rightarrow C: &\quad SYN(\mathrm{ISN}_S), ACK(ISN_C) \\
C \rightarrow S: &\quad ACK(\mathrm{ISN}_S) \\
C \rightarrow S: &\quad \text{data}
\end{aligned}
$$

and/or

$$
S \rightarrow C: \quad \text{data}
$$

$$
\begin{aligned}
X \rightarrow S: &\quad SYN(\mathrm{ISN}_X), SRC = T \\
S \rightarrow T: &\quad SYN(\mathrm{ISN}_S), ACK(\mathrm{ISN}_X) \\
X \rightarrow S: &\quad ACK(\mathrm{ISN}_S), SRC = T \\
X \rightarrow S: &\quad ACK(\mathrm{ISN}_S), SRC = T, nasty - data
\end{aligned}
$$

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Algumas Potenciais Falhas

- Ataques no roteamento
- Uso do ICMP
  - Redirect
  - ICMP errors (DoS)
- Email
- DNS
- Na prática, worms e trojans facilitam as coisas

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Conheça suas vulnerabilidades !

- Netstat - ?
- NMAP
- MBSA