

# Segurança da Rede

Seminário “A Internet e o consumidor”

PRO TESTE

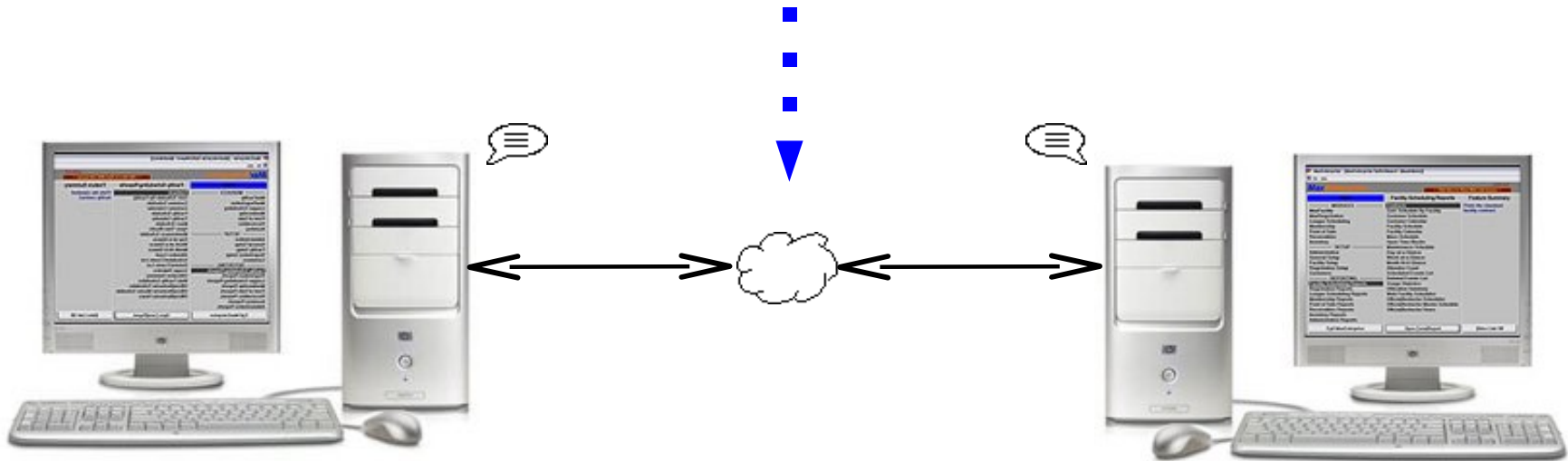
São Paulo, SP, Mar 2007

Prof. Pedro A. D. Rezende

[www.cic.unb.br/docentes/pedro/sd.htm](http://www.cic.unb.br/docentes/pedro/sd.htm)

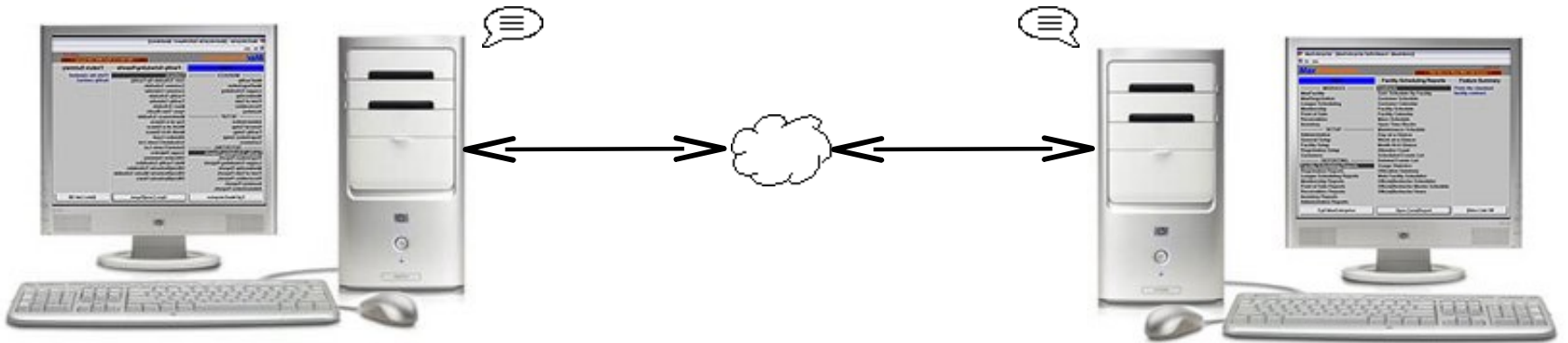
Ciência da Computação - Universidade de Brasília

# “a Rede”



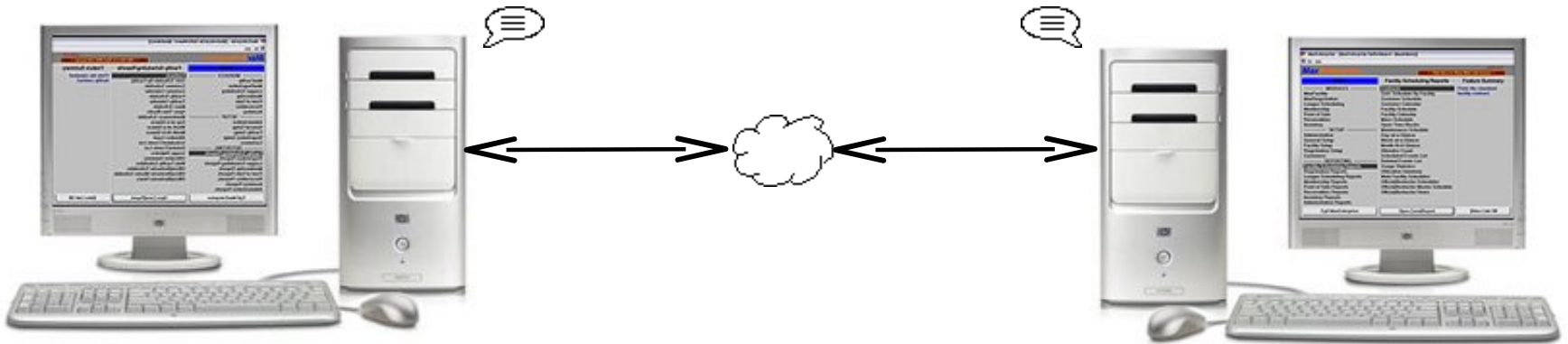
Uma nuvem de bits

# Segurança da Rede



Objetivo: cibercomunicação **robusta e descentralizada**

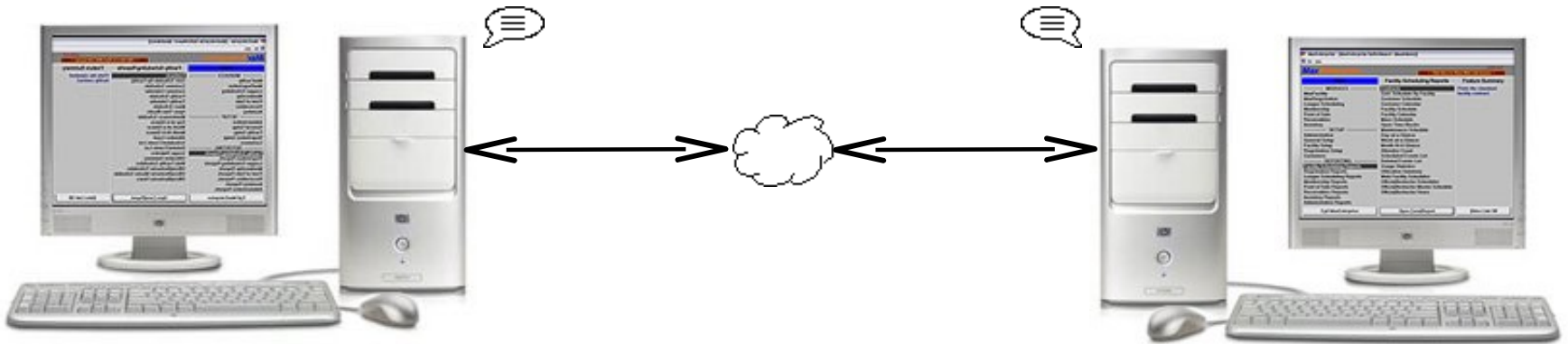
# Segurança da Rede



Objetivo: cibercomunicação robusta e descentralizada

Solução: **TCP-IP**.

# Segurança da Rede

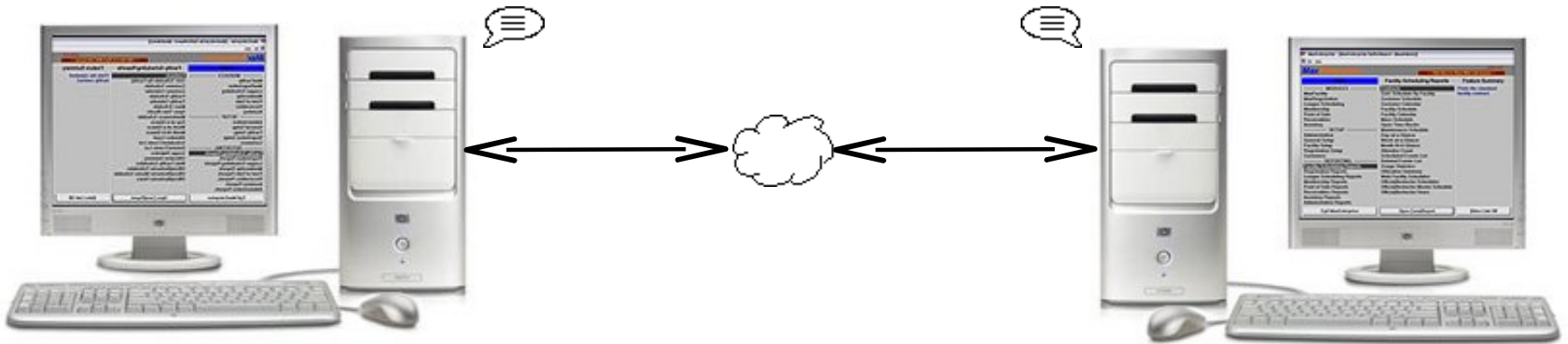


Objetivo: cibercomunicação robusta e descentralizada

Solução: TCP-IP.

Estratégia “best effort routing” em malha

# Segurança da Rede



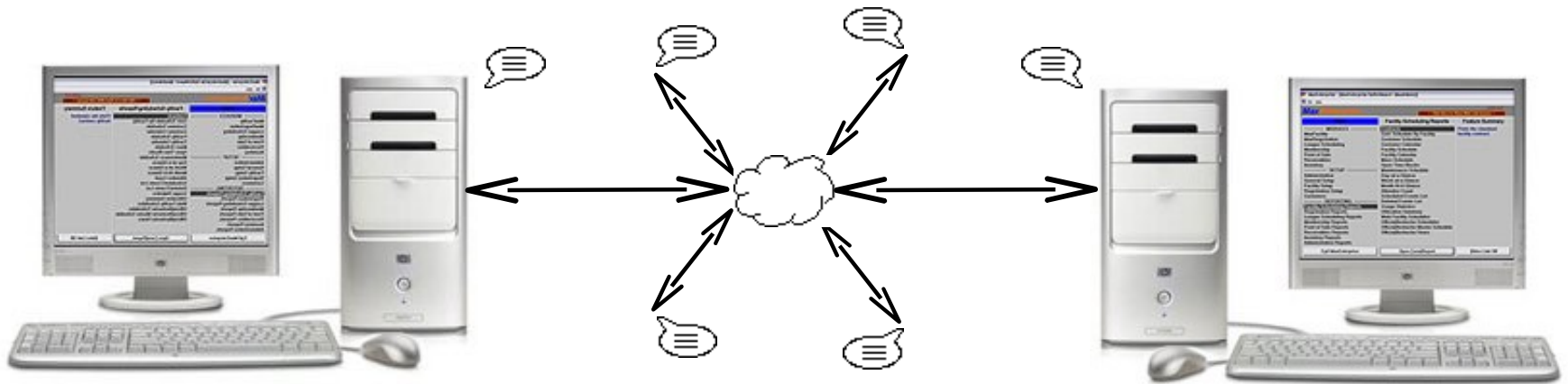
Objetivo: cibercomunicação robusta e descentralizada

Solução: TCP-IP.

Estratégia “best effort routing” em malha:

O tráfego segue por onde é possível, e mais fácil.

# Segurança da Rede

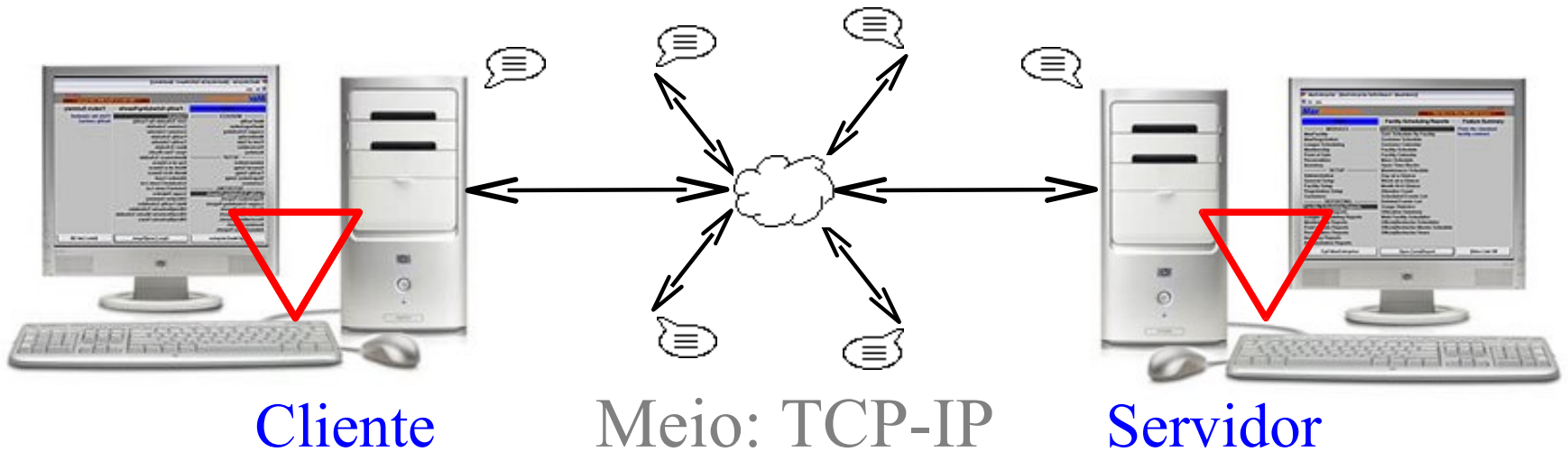


Meio: TCP-IP

Objetivo: Aplicações

1984: Roteamento se estabiliza (BGP4)

# Segurança da Rede

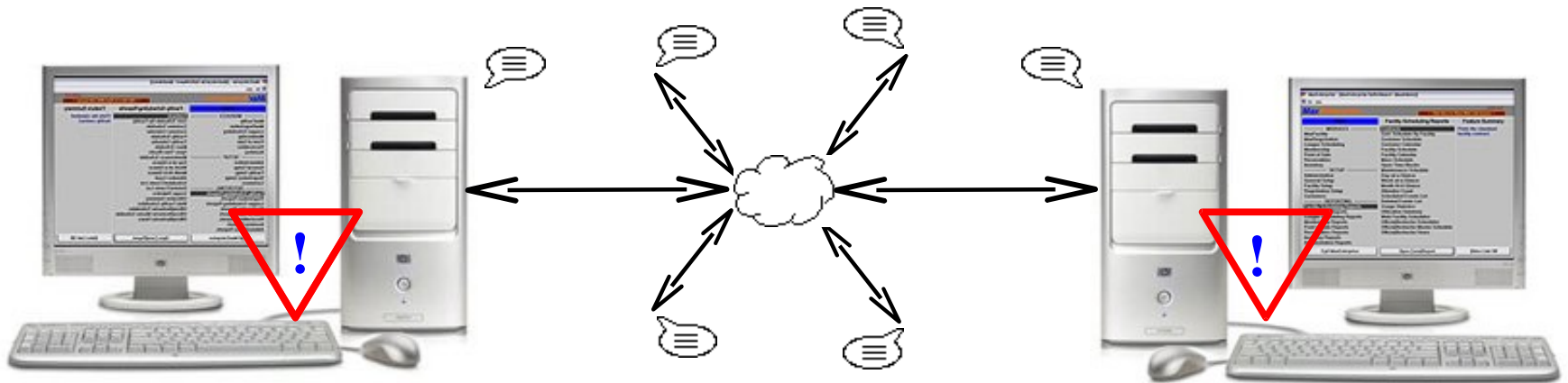


Meio: Aplicações

Objetivos: Eficiência, inovação e competitividade

1994: Internet “comercial”

# Segurança “da Rede”



Cliente

Meio: TCP-IP

Servidor

A

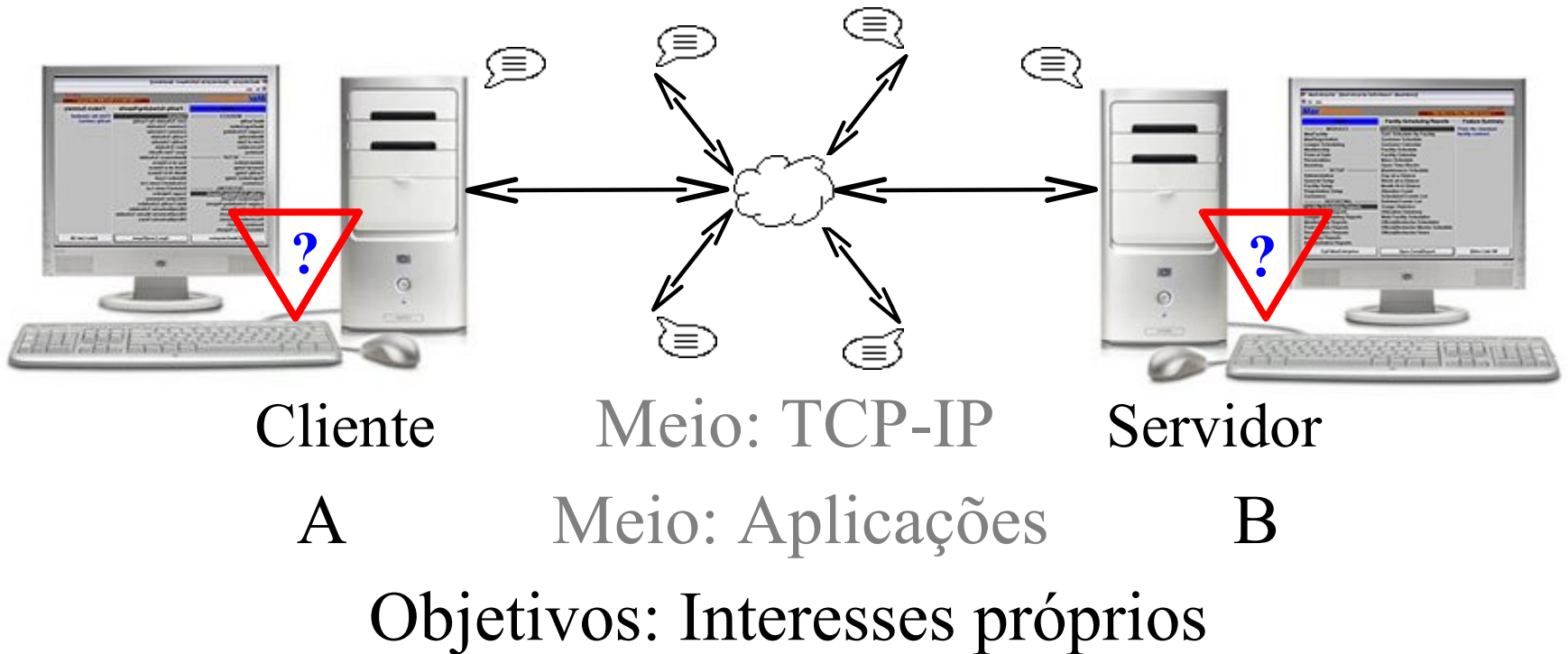
Meio: Aplicações

B

Objetivos: Interesses próprios

Hoje: Internet como infraestruturra.  
Interesses próprios buscam segurança **na** Rede

# Segurança “da Rede”



Hoje, Internet como infraestrutura **estratégica**:  
Como podem ser protegidos os interesses em cena?

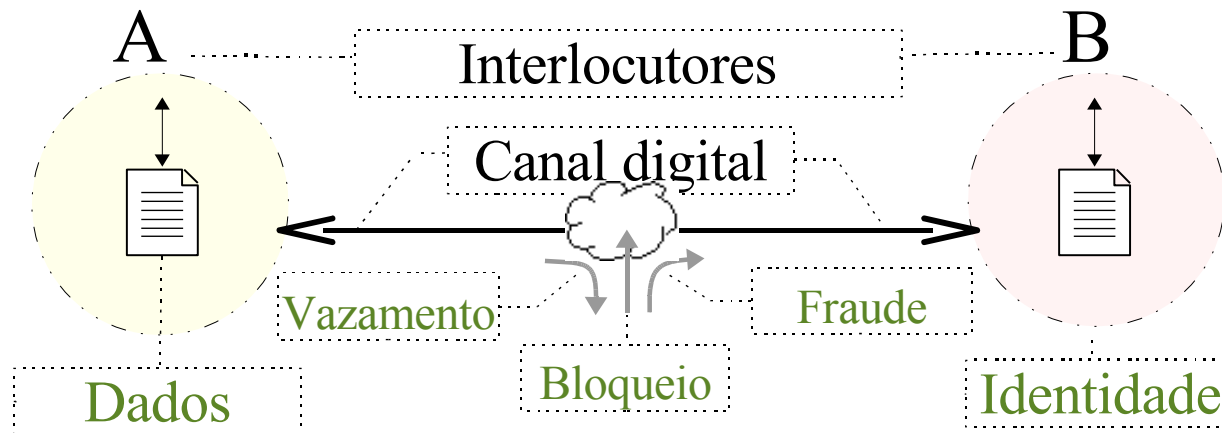
# Segurança d(os que estão n)a Rede



Quem são A e B?

Como são intermediados e protegidos seus interesses?

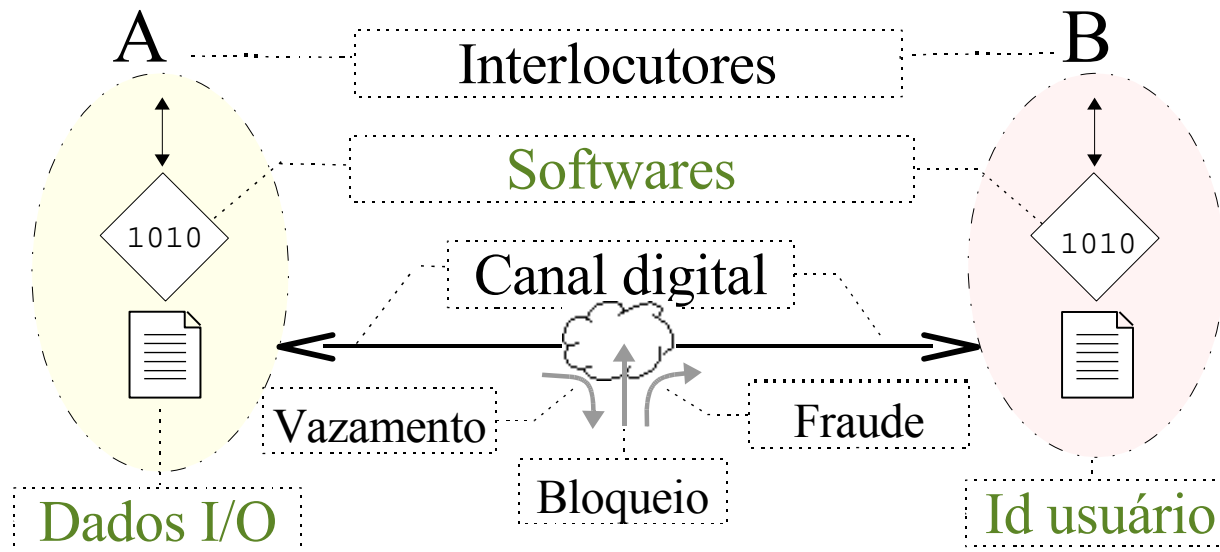
# Segurança na Rede



Como podem os interlocutores se identificar?

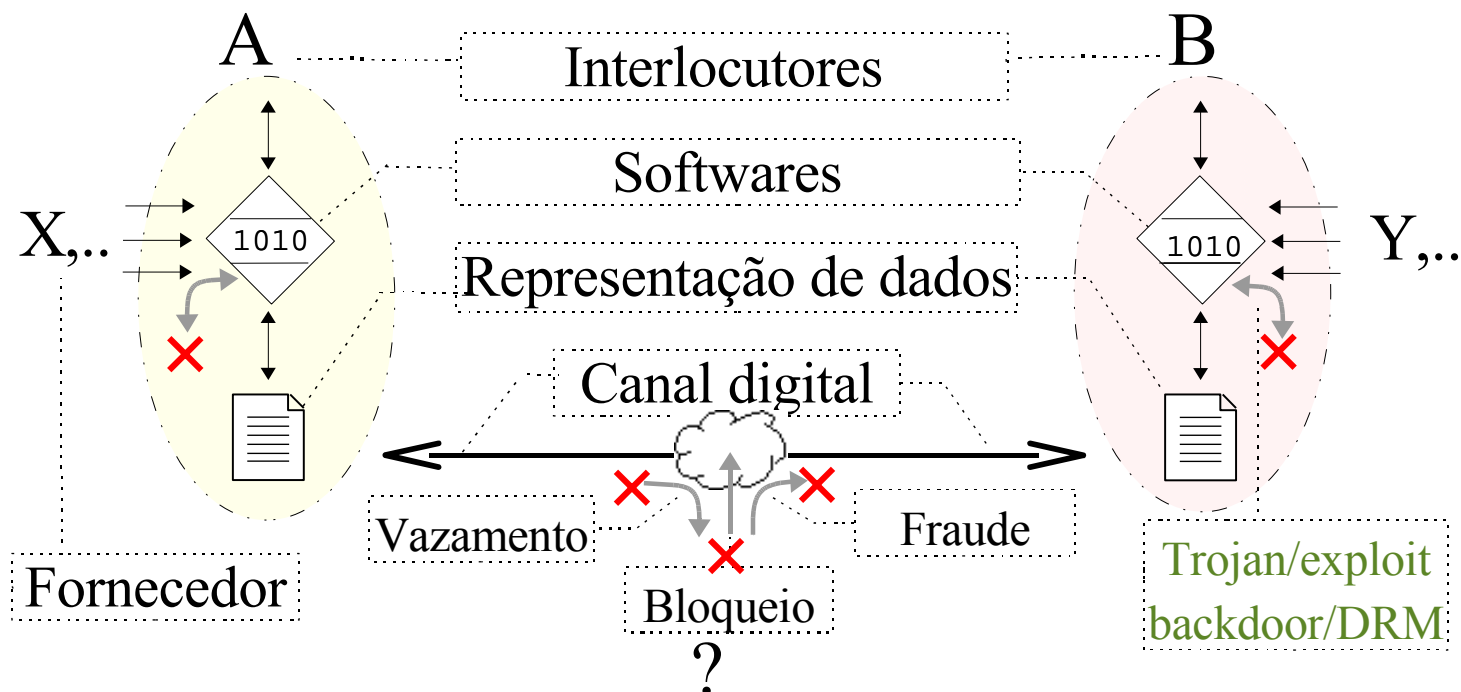
Como podem identificar interceptações?

# Segurança na Rede



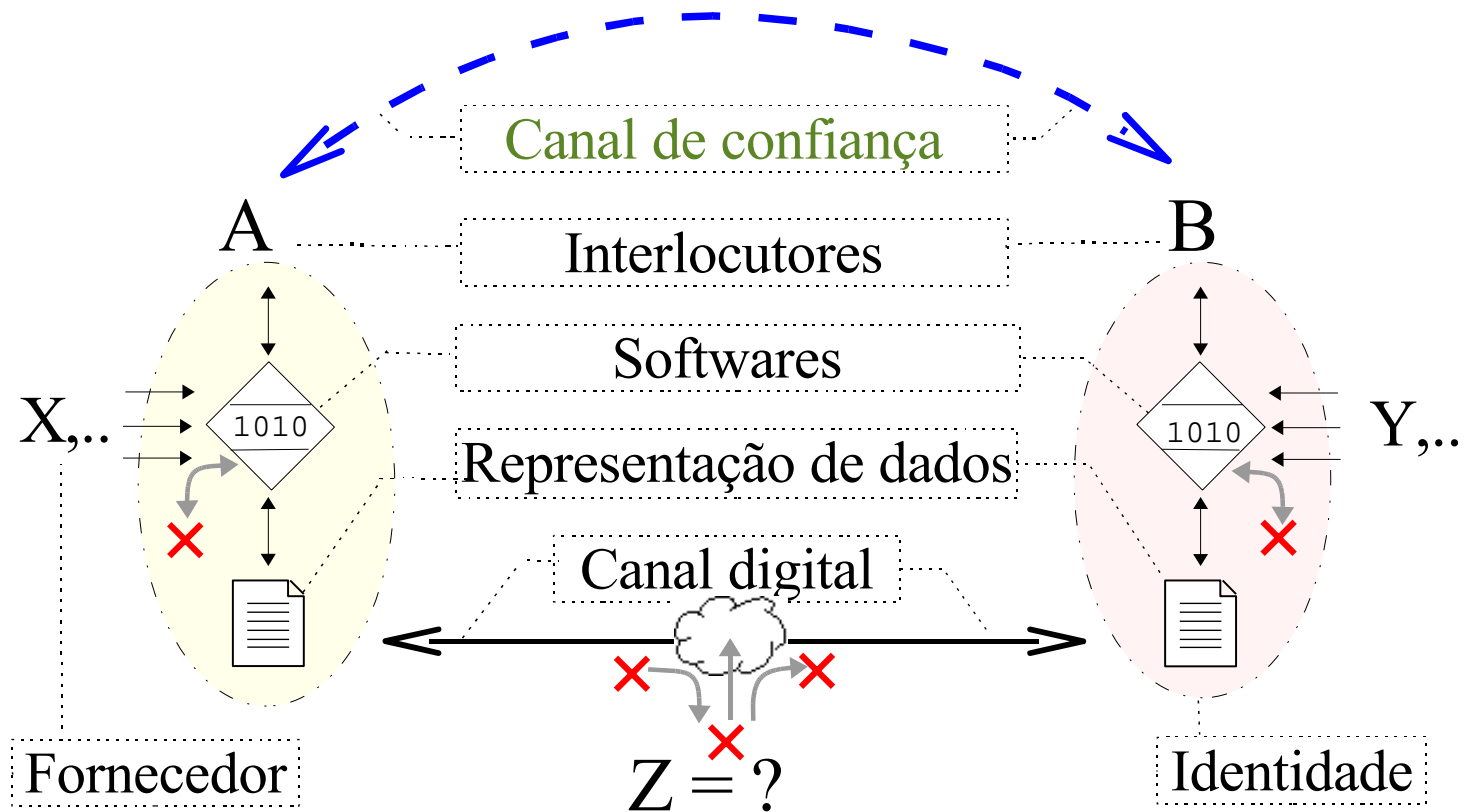
Como podem A e B controlar as intermediações?

# Segurança na Rede



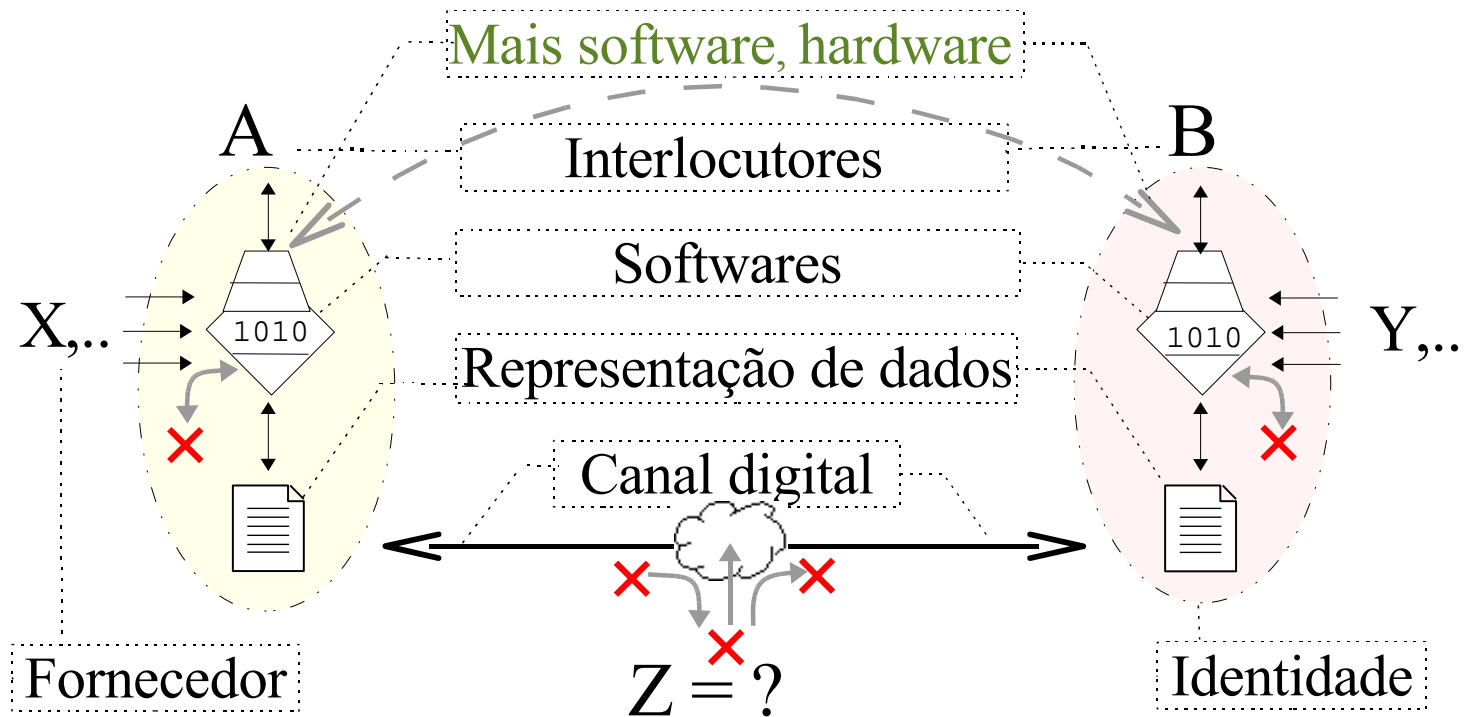
Como podem A e B assumir responsabilidades que intermediadores elidem? E os conflitos de interesse?

# Segurança na Rede



Não se pode prescindir dos **canais de confiança** que dão vida às relações sociais no mundo real

# Segurança na Rede



Quando se tenta substituir **relações de confiança** por produtos e consumo (mais camadas intermediadoras)...

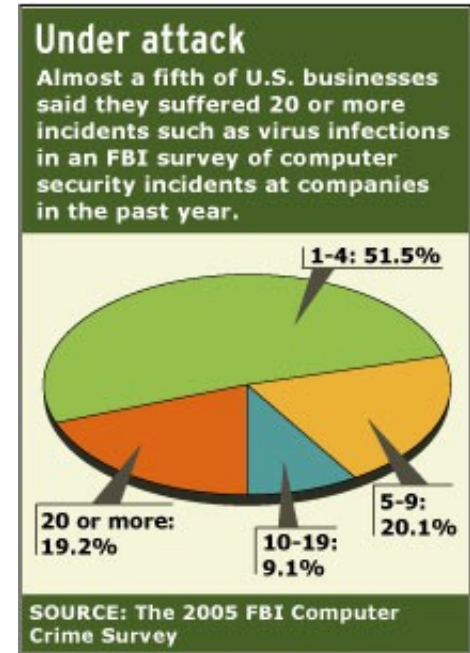
# (In)Segurança na Rede

## FBI report, jan 2006:

Pesquisa aponta que crimes relacionados à informática custaram ao *business* nos EUA mais de US\$ 67 bilhões em 2005.

64% dos respondentes sofreram incidentes, (ajustado para 20% do total de empresas)  
98.2 % usavam antivírus, 90.7 firewalls  
75% anti-spyware, 46% VPN, 23% IDS.  
86% sofreram ataques de vírus e trojans,  
80% de spyware; 44% ataques internos.

[http://news.com.com/2100-7349\\_3-6028946.html](http://news.com.com/2100-7349_3-6028946.html)



... **mais se gasta** com segurança, e **mais perdas** com incidentes de segurança ocorrem

# (In)Segurança na Rede

**Um exemplo** de controle geral de acesso a VPN:



Há quem usa controle por cartão ...

Controle externo de acesso por cartão bancário

# (In)Segurança na Rede

Um exemplo de (in)eficácia de controle geral de acesso a VPN:



Há quem usa controle por cartão ...

... e quem deixou de usar

Controle externo de acesso por cartão bancário oferece ponto fácil para instalação de chupa-cabras

# (In)Segurança na Rede

## Gartner report, 5 mar 2007:

Perda média por fraude de identidade mais que dobrou em 2006 nos EUA (média US\$3.257,00).

15 milhões de vítimas estimadas, 50% a mais que em 2005

<http://www.gartner.com/it/page.jsp?id=50191>



The screenshot shows a Gartner press release page. The main headline is "Gartner Says Number of Identity Theft Victims Has Increased More Than 50 Percent Since 2003". The sub-headline is "STAMFORD, Conn., March 5, 2007 --". The text of the release states: "Approximately 15 million Americans were impacted by some sort of identity theft-related fraud in the 12 months ending in early 2006, according to a survey by Gartner, Inc. These statistics represent more than a 50 percent increase since 2003 when the Federal Trade Commission (FTC) reported 9.9 million American adult identity theft victims." It also mentions that the average loss rose to \$2,237 in 2006, up from \$1,458 in 2003, and that the percentage of total consumers managed to recover dropped from 47 percent in 2005 to 44 percent in 2006. The release concludes by stating that "Fraudsters are exploiting Internet auctions, unregulated money transfer systems, the ability to manipulate online and consumer records, and other types of innovative schemes," and that "These findings are the result of an ongoing analysis at Gartner. The findings have also discovered the highest loss in the U.S. payments systems. Typically, the such loss are found among the free or more online businesses that accept online payments from consumers, and the consumer's libraries."

Quanto mais, em geral, se gasta com segurança mais perdas com incidentes de segurança ocorrem:

# (In)Segurança na Rede

**Gartner report, 5 mar 2007:**

*“Hackers are exploiting Internet auctions, nonregulated money transmittal systems, the ability to impersonate lottery contests, and other types of imaginative scams. The thieves have also discovered the weakest links in the U.S. payments systems”* said Avivah Litan, vice president at Gartner.



The screenshot shows a Gartner press release page. The main headline is "Gartner Says Number of Identity Theft Victims Has Increased More Than 50 Percent Since 2003". The sub-headline is "STAMFORD, Conn., March 5, 2007 --". The text of the release states: "Approximately 15 million Americans were impacted by some sort of identity theft-related fraud in the 12 months ending in early 2006, according to a survey by Gartner, Inc. These statistics represent more than a 50 percent increase since 2003 when the Federal Trade Commission (FTC) reported 8.9 million American adult identity theft victims." It also mentions that according to the Gartner survey of 5,000 online U.S. adults in August 2006, the average loss was \$1,237 in 2006, up from \$1,458 in 2003. At the same time, the percentage of total consumers managed to recover dropped from 47 percent in 2003 to 44 percent in 2006. The release concludes: "Thieves are exploiting Internet auctions, nonregulated money transmittal systems, the ability to impersonate lottery and contest sites, and other types of imaginative scams," said Avivah Litan, vice president and distinguished analyst at Gartner. "The thieves have also discovered the weakest links in the U.S. payments systems. Typically, the weak links are found among the line or more online businesses that accept online payments from consumers, and the consumer's libraries."

Gasta-se **mal**, e atira-se no mensageiro  
da insegurança

# (In)Segurança na Rede

**Gartner report, 5 mar 2007:**

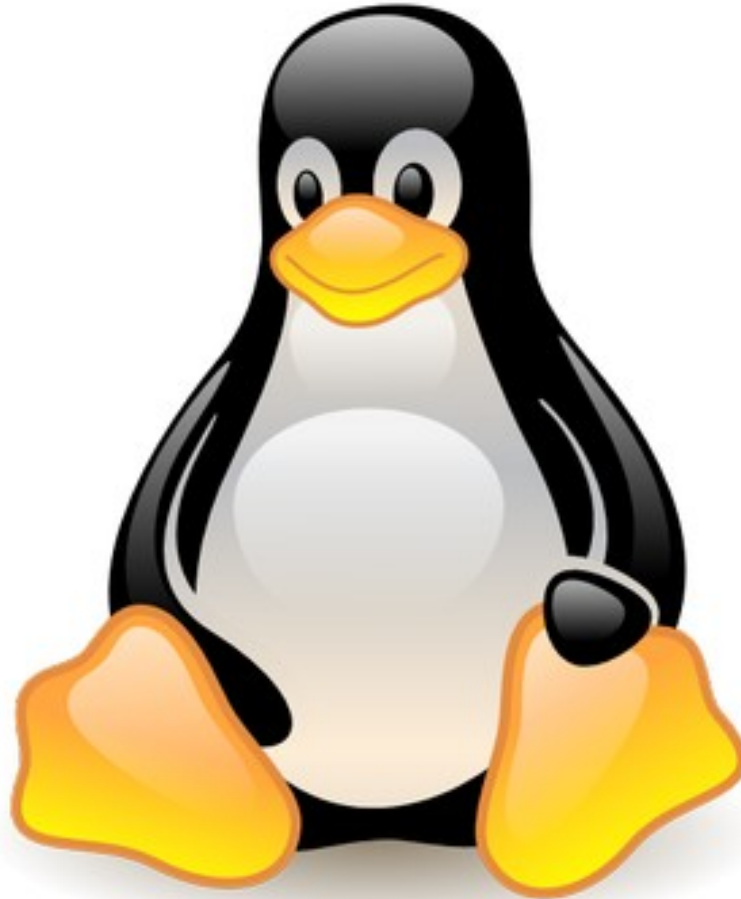
*“Hackers are exploiting Internet auctions, nonregulated money transmittal systems, the ability to impersonate lottery contests, and other types of imaginative scams. The thieves have also discovered the weakest links in the U.S. payments systems”* said Avivah Litan, vice president at Gartner.



The image shows a screenshot of a Gartner press release page. The main headline reads: "Gartner Says Number of Identity Theft Victims Has Increased More Than 50 Percent Since 2003". The text below the headline states: "Approximately 15 million Americans were impacted by some sort of identity theft-related fraud in the 12 months ending in early 2006, according to a survey by Gartner, Inc. These statistics represent more than a 50 percent increase since 2003 when the Federal Trade Commission (FTC) reported 8.9 million American adult identity theft victims." The page also includes a date stamp "STAMFORD, Conn., March 5, 2007" and a "2007 Press Release" label.

Gasta-se mal, e atira-se no mensageiro  
da insegurança (*hackers* = *thieves*?)

# (In)Segurança na Rede



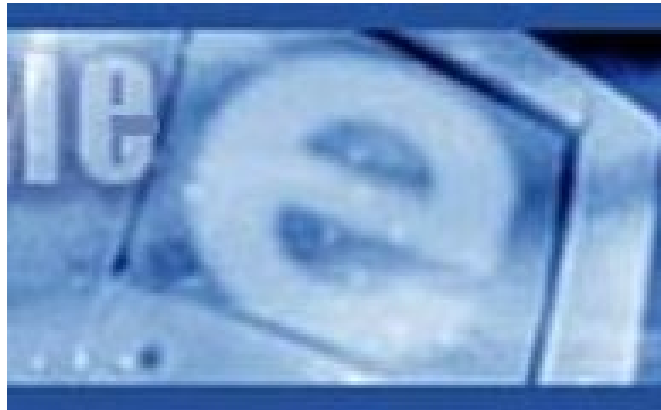
*Hackers fazem isso ...*

# (In)Segurança na Rede



... e isso, que roda em qualquer sistema  
e navega inquestionavelmente com mais segurança...

# (In)Segurança na Rede



... do que isso, que só roda em um sistema e já foi, devido à falta de segurança, condenado até pelo ...

# (In)Segurança na Rede

**Internetnews.com, jun 29, 2004:**

*US-CERT is warning Web surfers to stop using MS Internet Explorer.*

*"There are a number of significant vulnerabilities in technologies relating to the IE domain/zone security model, the DHTML object model, MIME-type determination, and ActiveX. It is possible to reduce exposure to these vulnerabilities by using a different Web browser."*

<http://www.kb.cert.org/vuls/id/713878>



The image shows a screenshot of a web page from the United States Computer Emergency Readiness Team (US-CERT). The page is titled "Vulnerability Note VU#713878" and describes a security issue with Microsoft Internet Explorer. The main heading is "Microsoft Internet Explorer does not properly validate source of redirected frame". The page includes a navigation menu on the left with links for "Vulnerability Database", "Search", "Publications", "Type/Status", "Home", "US Number", "CVE Status", "Open Policy", "Open Published", "Open Unpublished", "Security Advisories", "Other", and "How to Report". The main content area has an "Overview" section and a "1. Description" section. The "Description" section explains that IE uses a cross-domain security model to maintain separation between browser frames from different sources, designed to prevent code in one domain from accessing data in a different domain. It notes that the Local Machine Zone implicit zone for content that exists on the local computer, the content found on the user's computer, except that Internet Explorer can be used for its updates, is treated with a high level of trust. The description also mentions that the domain and user domain a URL exists in and what actions can be performed in that zone is made by the [Internet] Security Group.

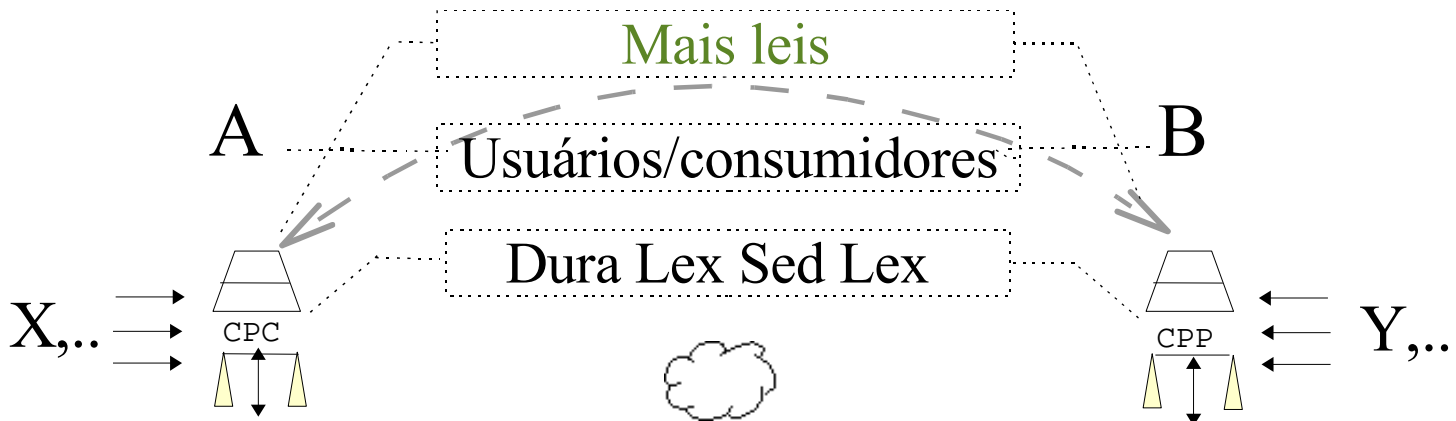
...United States Computer Emergency Readiness Team

# (In)Segurança na Rede



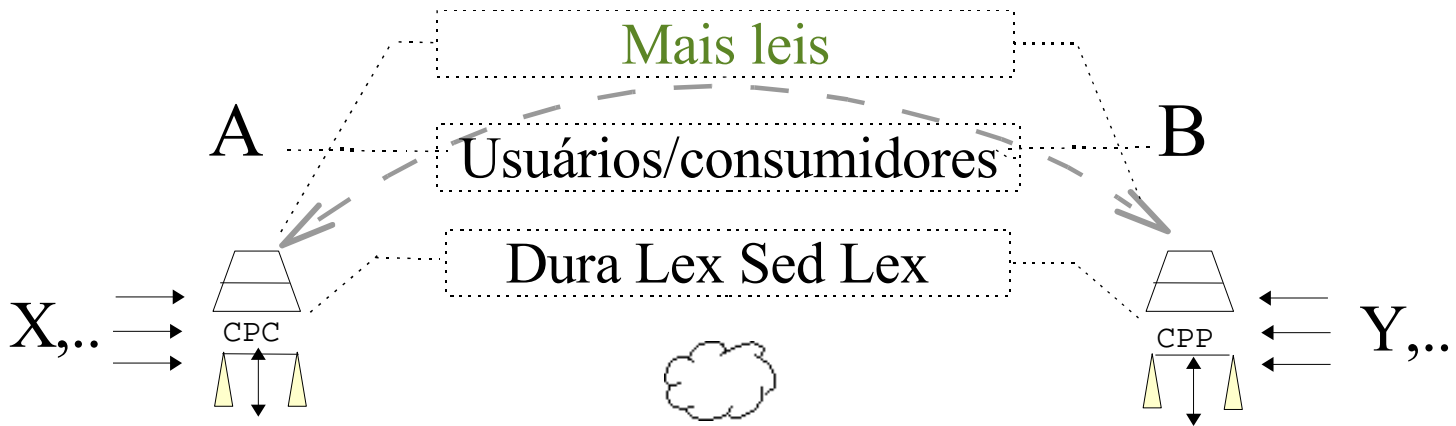
Nesse cenário, como **reagem** os que querem controlar ou se apoderar da nuvem de bits?

# (In)Segurança Jurídica com a Rede



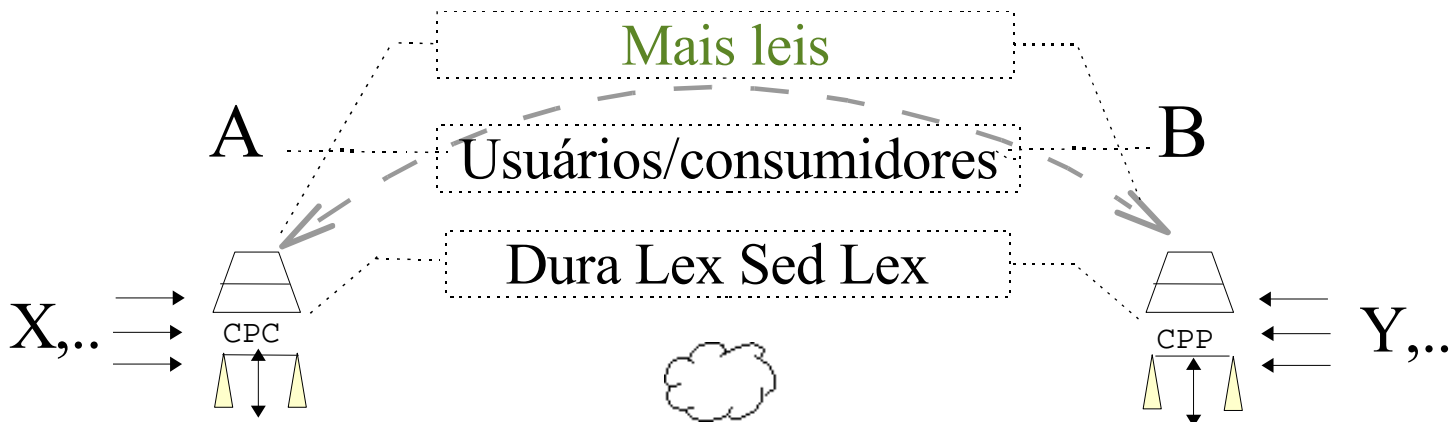
Reagem **com fúria legiferante**

# (In)Segurança Jurídica com a Rede



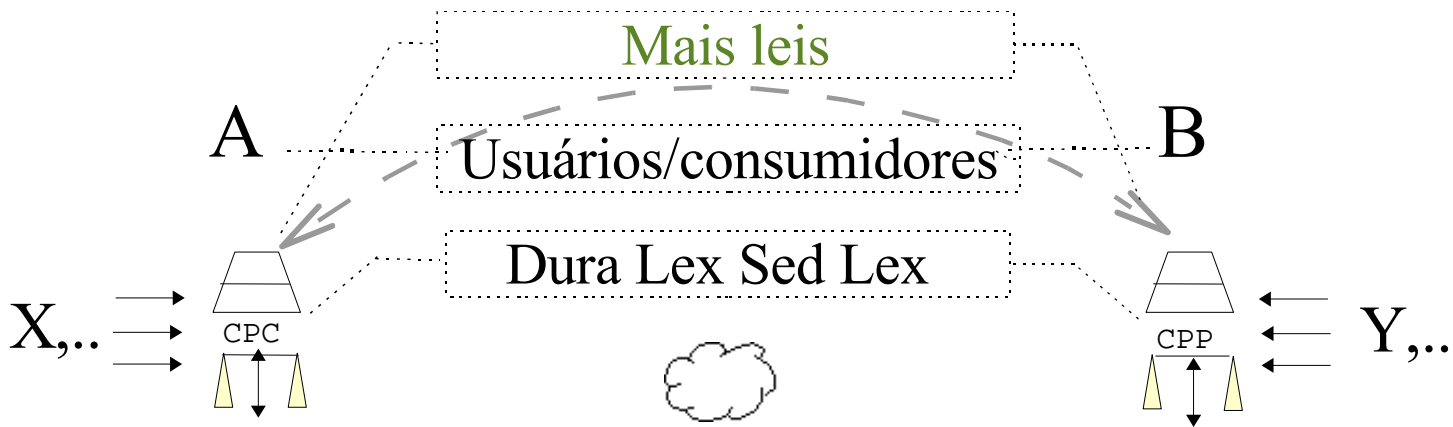
- Com novas leis por excessão, centradas em condutas aberrantes

# (In)Segurança Jurídica com a Rede



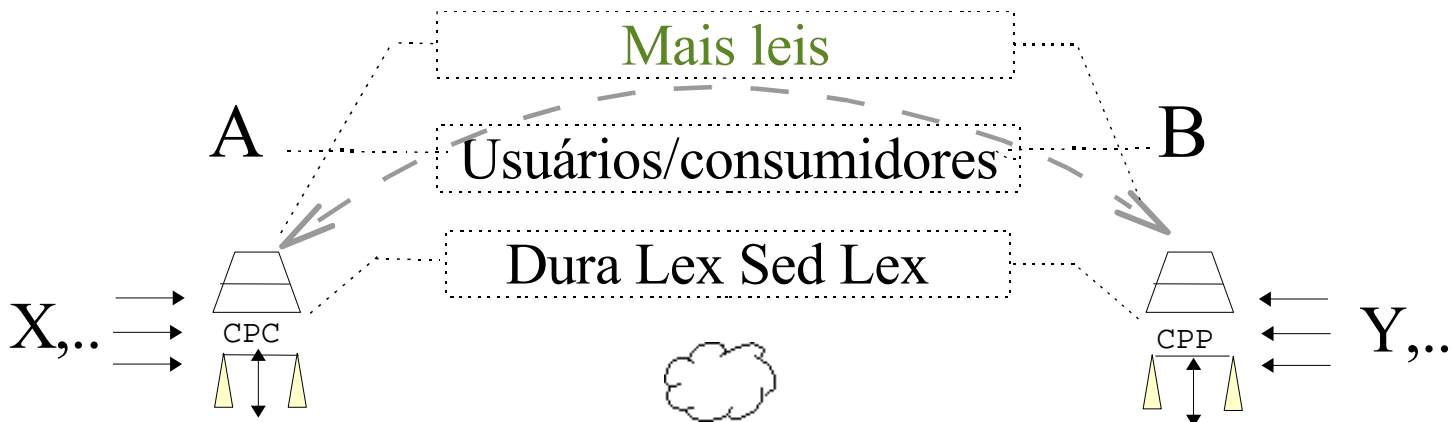
- Com novas leis por excessão, centradas em condutas aberrantes
- Com novos tipos penais em aberto, imprecisos e subjetivos

# (In)Segurança Jurídica com a Rede



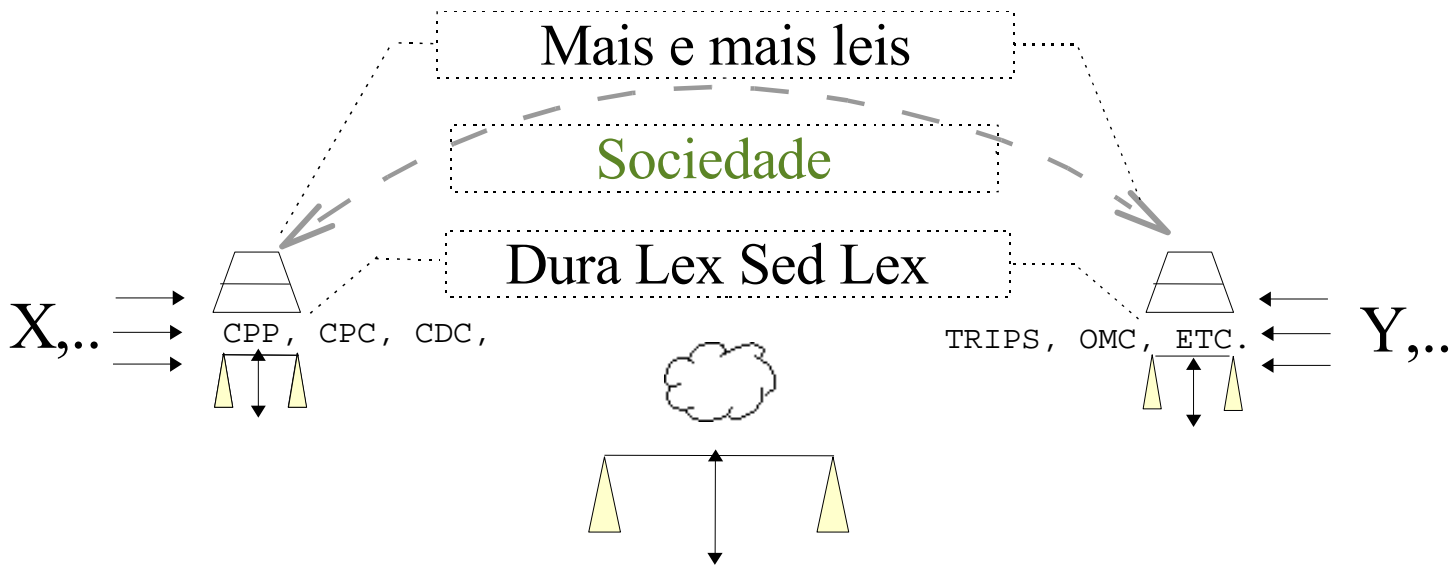
- Com novas leis por excessão, centradas em condutas aberrantes
- Com novos tipos penais em aberto, imprecisos e subjetivos
- Com isenção de responsabilidade subsidiária a fornecedores intocáveis

# (In)Segurança Jurídica com a Rede



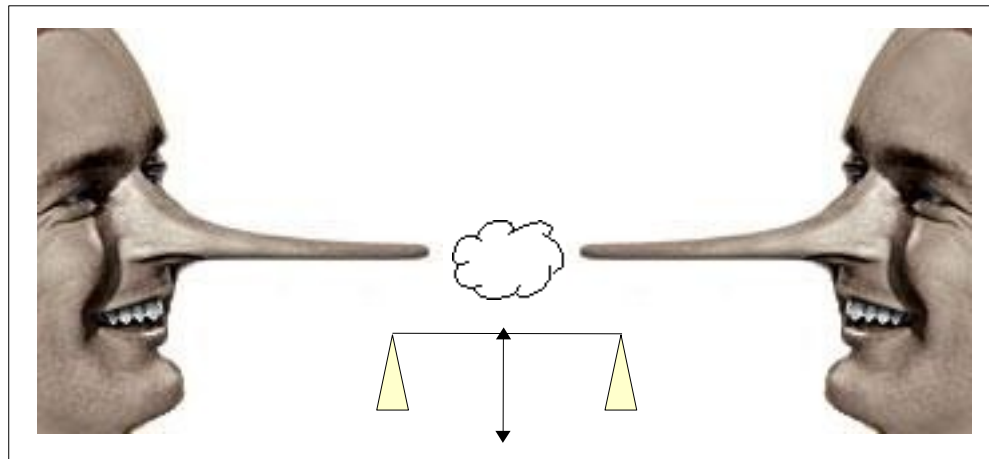
- Com novas leis por excessão, centradas em condutas aberrantes
- Com novos tipos penais em aberto, imprecisos e subjetivos
- Com isenção de responsabilidade a fornecedores intocáveis
- Com penas desproporcionais, critérios frouxos de admissibilidade ou inversão do ônus de prova, **tentando** compensar as dificuldades naturais de se legislar sobre o virtual

# (In)Segurança Jurídica com a Rede



Nesse cenário, qual o maior **risco sistêmico** que corre a sociedade?

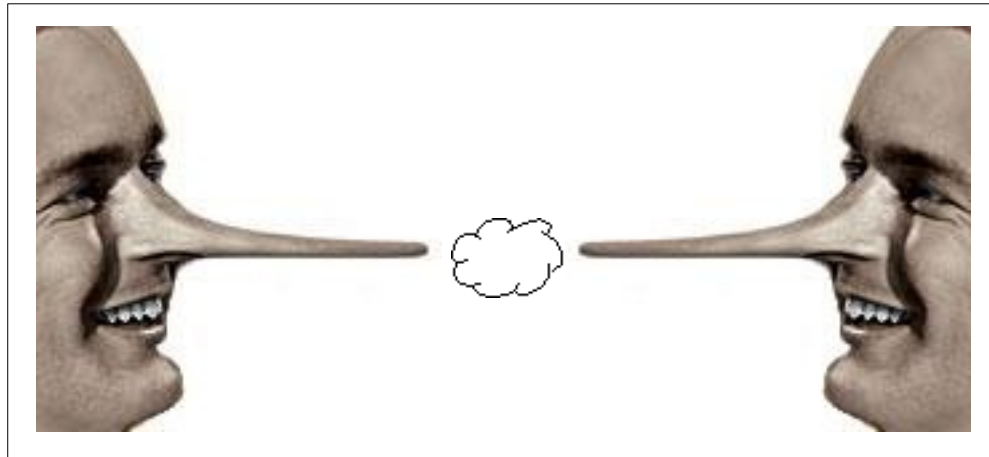
# Erosão do Direito com a (contribuição da) Rede



*"Seria mais apropriado chamar o . . . . de Corporatismo porque ele é a fusão do Estado com o poder corporativo."*

???

# Instabilidade Política com a Rede



*"Seria mais apropriado chamar o **Facismo** de Corporatismo porque ele é a fusão do Estado com o poder corporativo."*

Benito Mussolini <http://en.wikipedia.org/wiki/Corporatism>

# O cenário das guerras virtuais

Liberdade ao conhecimento  
vs. Liberdade ao capital

## Mundo dos Símbolos

