C . E . S . A . R

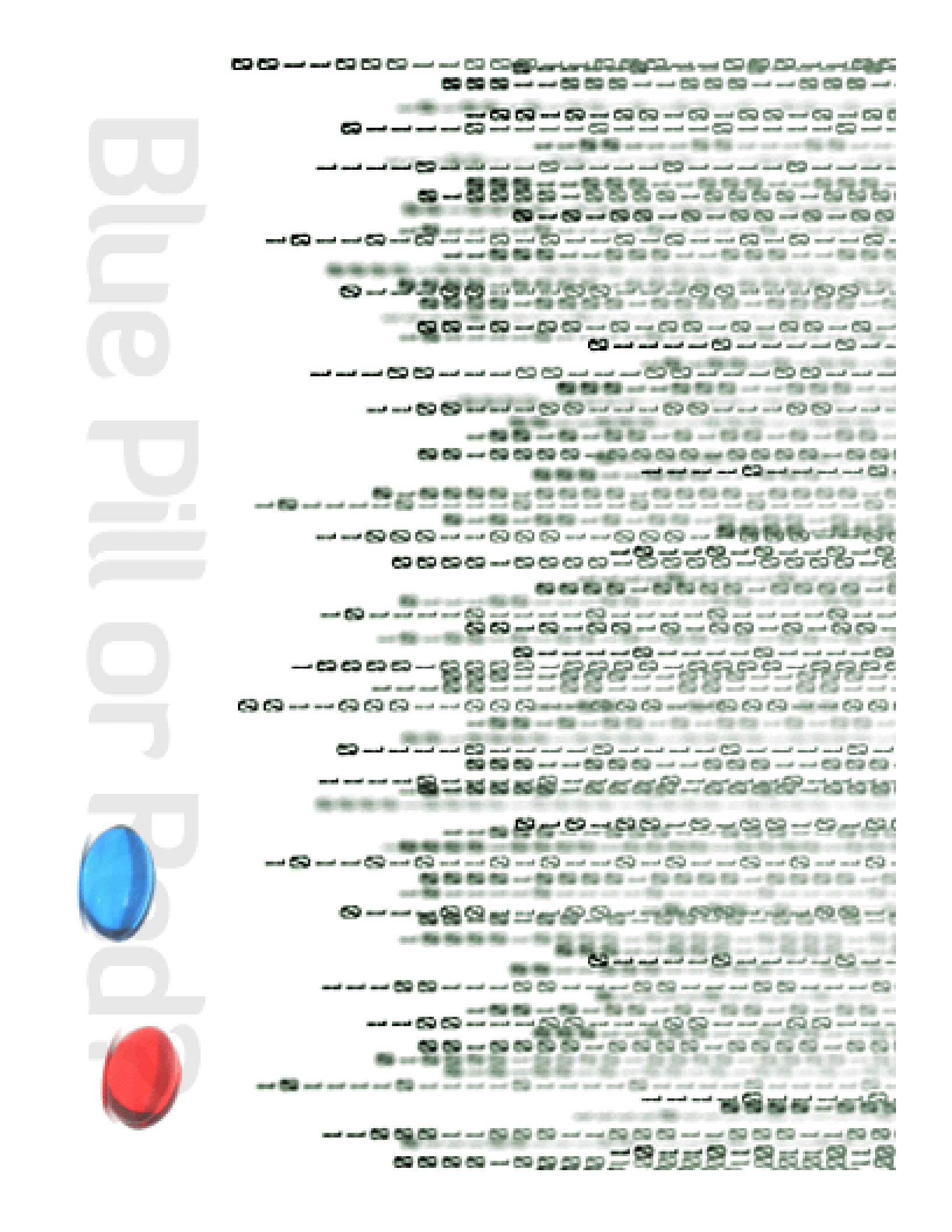
Instituto de Inovação com TIC

[Junho/ 2009]

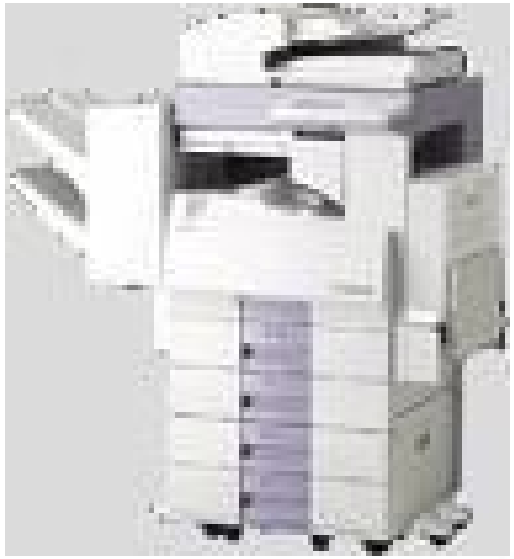
Segurança em aplicações WEB: A nova fronteira

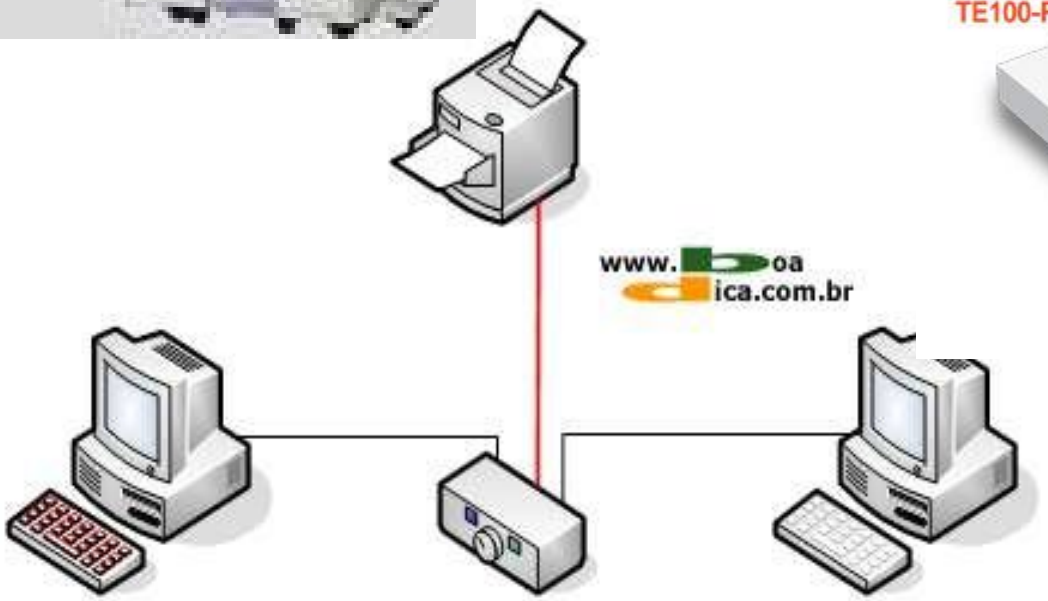
rodrigo.assad@cesar.org.br

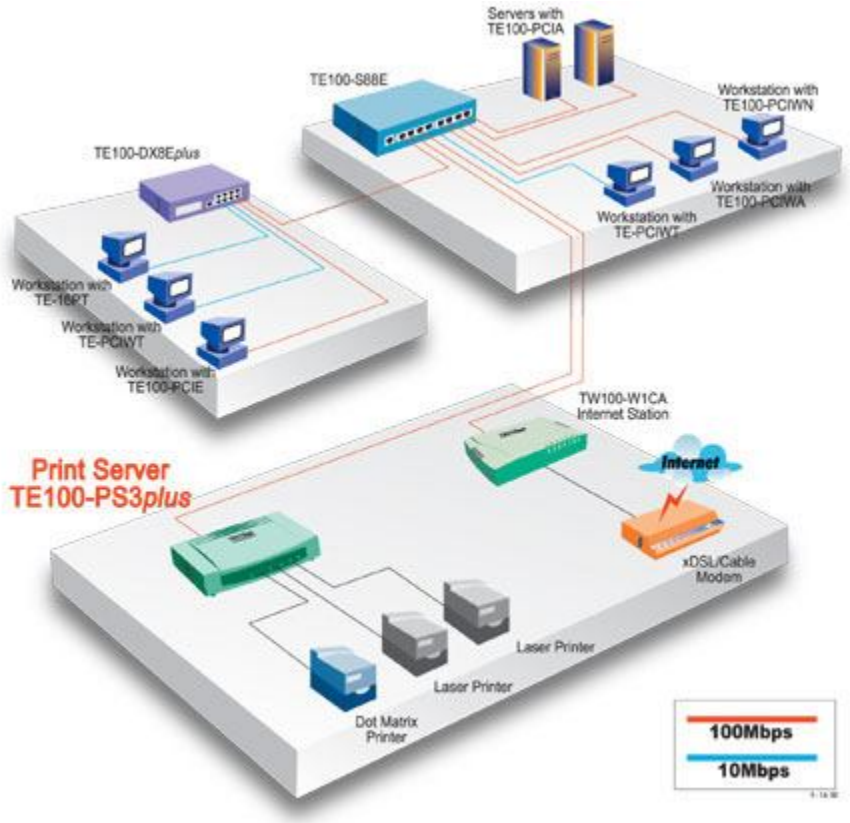

Não, obrigado!
Deus, vai me ajudar



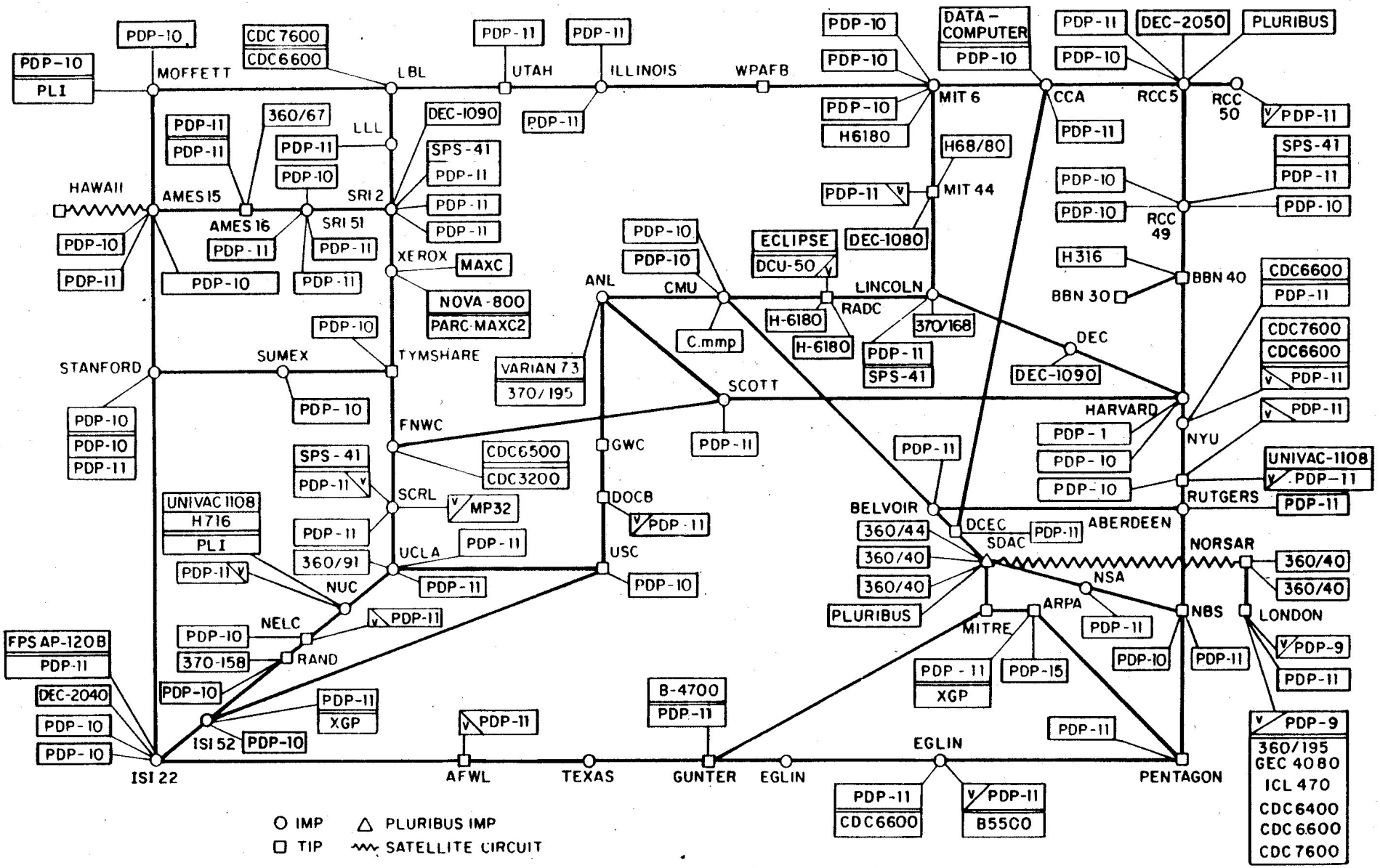
Redes de Computadores (Histórico)







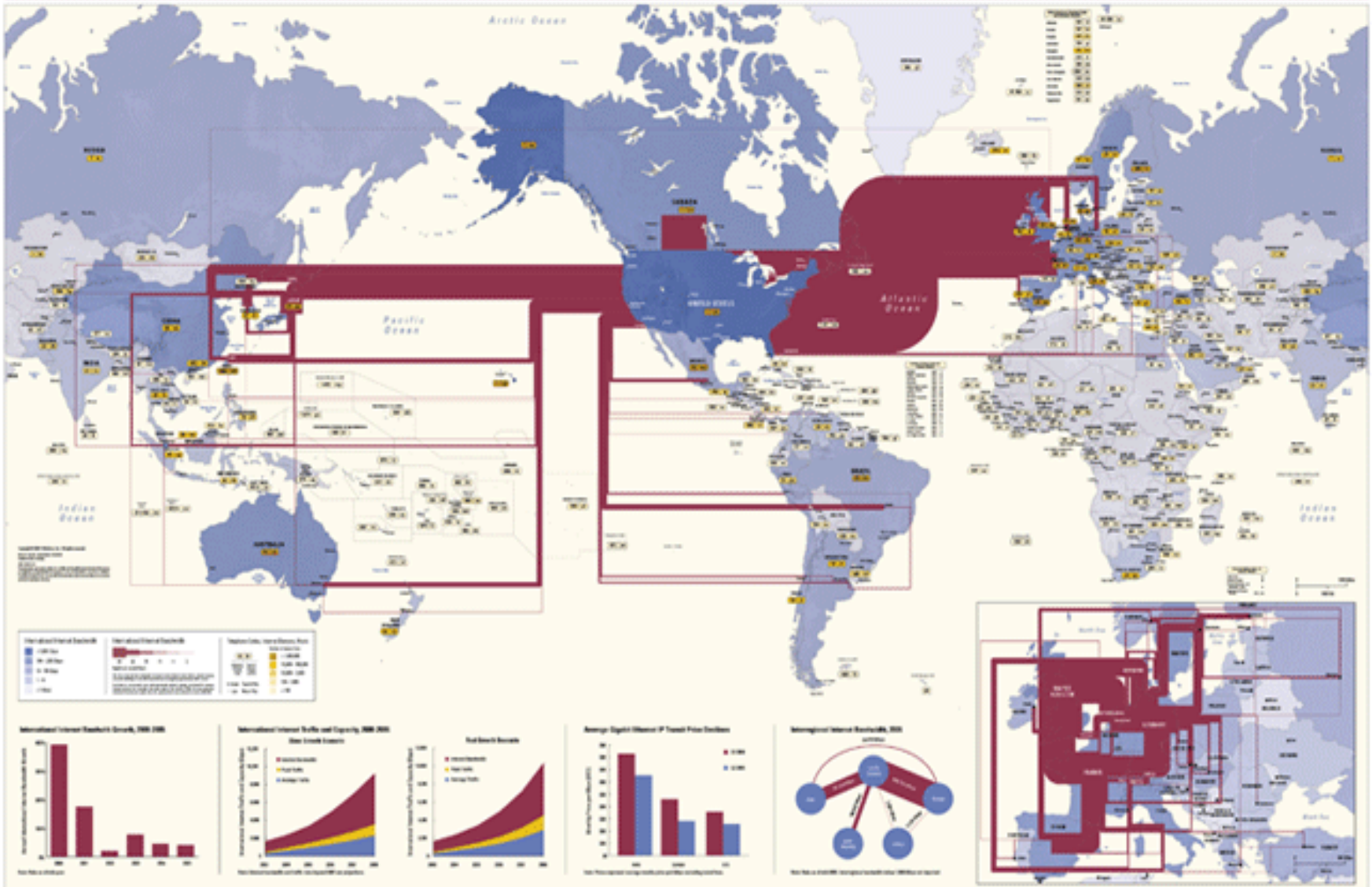
ARPANET LOGICAL MAP, MARCH 1977



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

Global Internet Map



Segurança de Redes (Histórico)

Robert Tappan

- O programa principal consistia em menos de 100 linhas de código em C
- 6.000 computadores infectados, só nos EUA, em 24 horas
- Efeitos:
  - Infecção
  - Sobrecarga
  - Incapacitação
  - http://pdos.csail.mit.edu/~rtm/

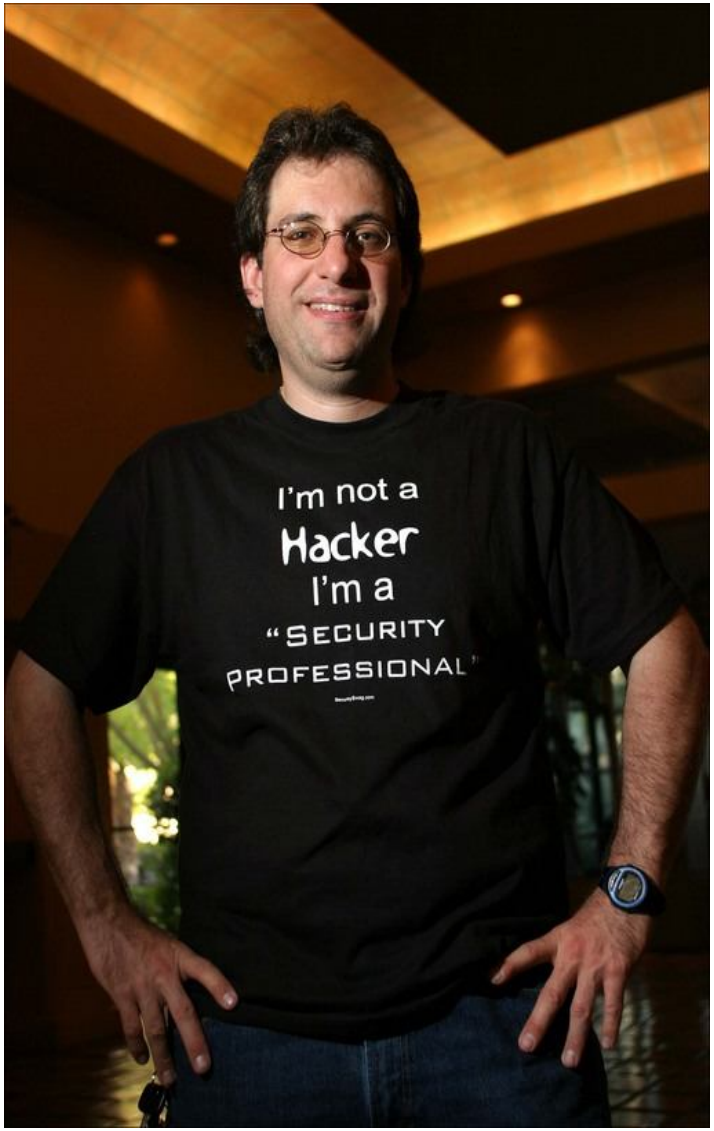
Segurança de Redes (Histórico)

Kevin Pulsen

- primeiro grande *hacker* da Internet
- Invadiu, entre outros,
  - a marinha americana,
  - diversas Universidades, como UCLA
- A partir daí, criou-se a lei americana contra “invasões” em redes
- Trabalhou posteriormente para o governo americano

Segurança de Redes (Histórico)

- Kevin Mitnick
  - O mais famoso de Todos
  - Foi Preso e já esta solto
  - Invadiu
    - FBI
    - Universidades
  - Seu ataque foi muito sofisticado e sem “solução” até os dias atuais



Administração de Redes

Perfil

“ Um bom administrador de redes sabe identificar, resolver e explicar qualquer problema que possa vir a acontecer em sua rede. Ele tem consciência de tudo o que acontece. “

Administração de Redes

- ***Recursos***
  - ***Sites***
    - ***www.usenix.org***
    - ***www.linux.org***
    - ***http://www.sun.com/bigadmin/***
    - ***www.microsoft.com***
    - ***www.google.com***
    - ***http://bhami.com/rosetta.html***

desGoverno do Brasil - (g) overnment of Brazil - finally owned? @#$@ - Netscape

File Edit View Go Communicator Help

b1Ow

...one s0ul, many minds...

BRASiL.GOV.BR bl0wn3d????????

h3h. 0h fuqn shee1t. th4 bl0w team 0wn3d my fuqn f4t 4zz!@#$#

mensagem do underground para voces.

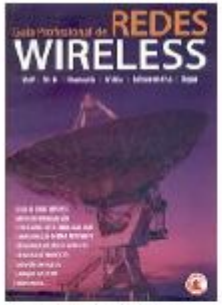
Oh yeah! Parece que nos chegamos ao topo! Ao topo do lixo, do estrume e da escoria que eh essa politicada brasileira! Da nojo de ver um site tao escroto como esse falando tantas mentiras para a massa brasileira. FHC fede, ACM fede, Brasilia fede, politicos em geral fedem! E a populacao, estagnada em suas casas assistindo a "REDEGLOBO", se conforma com a triste situacao na qual o Brasil esta enterrado. Eh o que o senhor queria nao eh FHC? Nao eh ACM? Nao eh isso

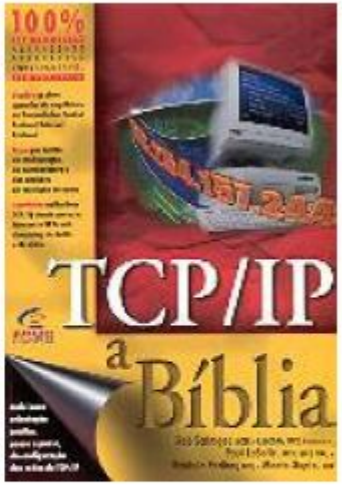
Document: Done

Segurança é um end-line

- Segurança em um “end line”
  - Mas o que é isso?
  - Não se discute segurança sem entender de
    - Arquitetura de Computadores, Sistemas Operacionais, Redes de computadores (protocolos de comunicação, Linguagem de programação, engenharia de software e Logica.

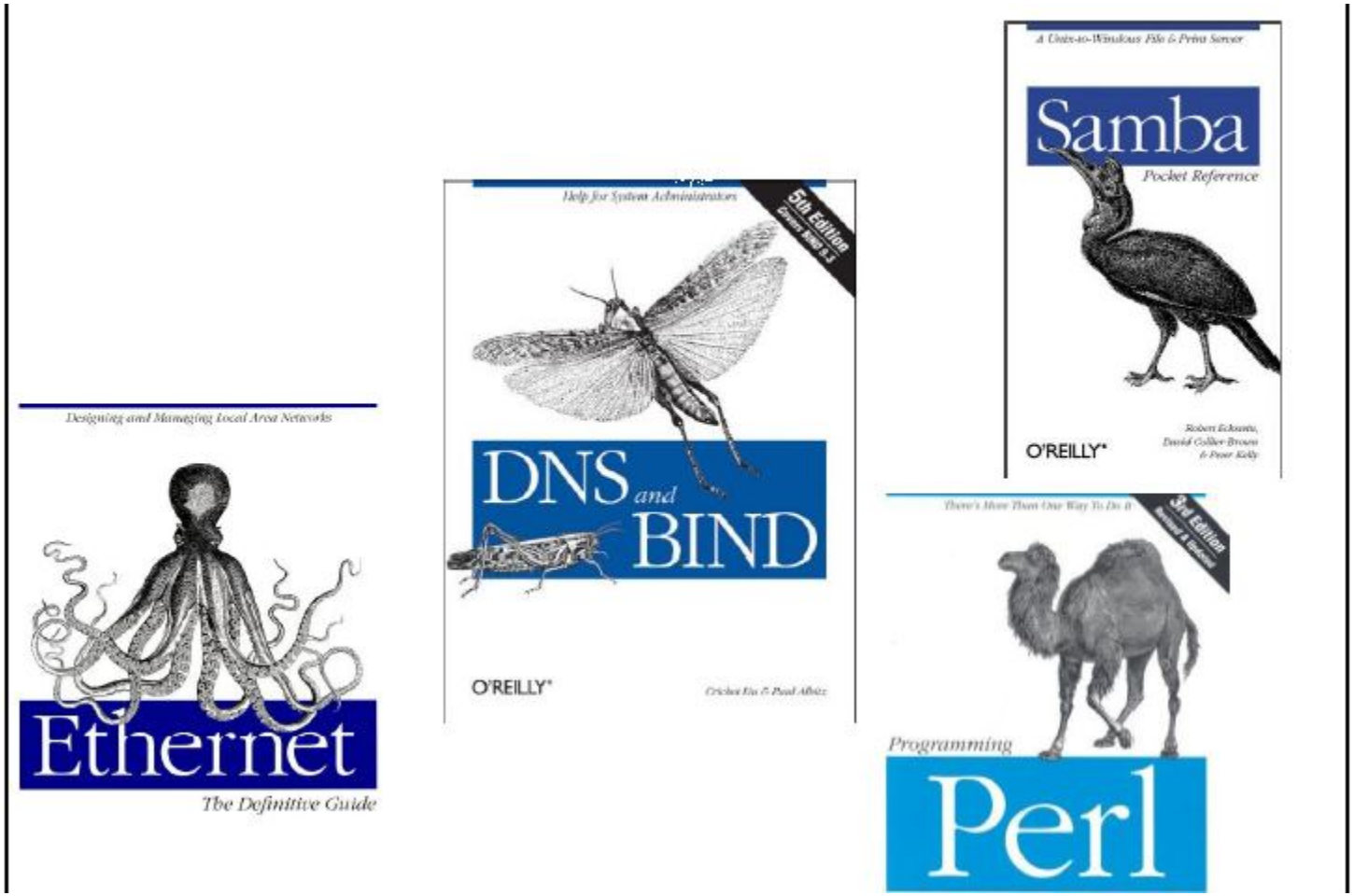
Então para o que querem ....





cesar.edu

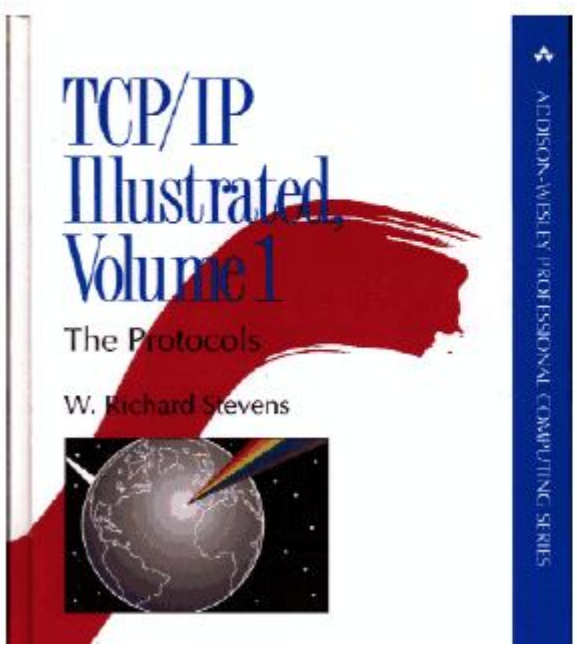
Então para o que querem ....



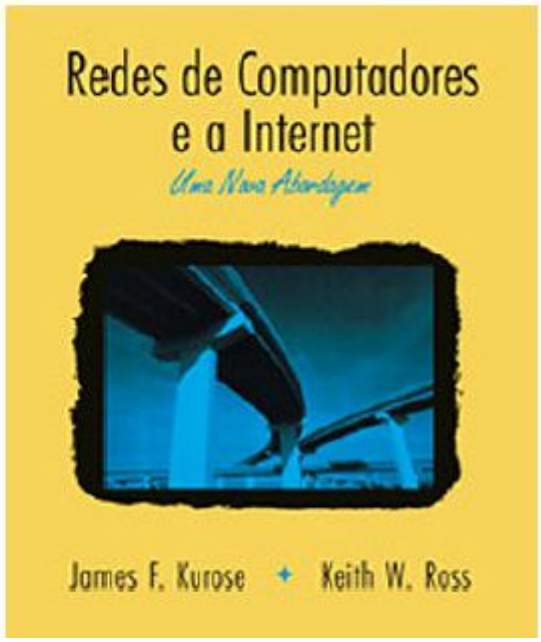
C.E.S.A.R

Então para o que querem ....

TCP/IP Illustrated
Volume 1
Stevens

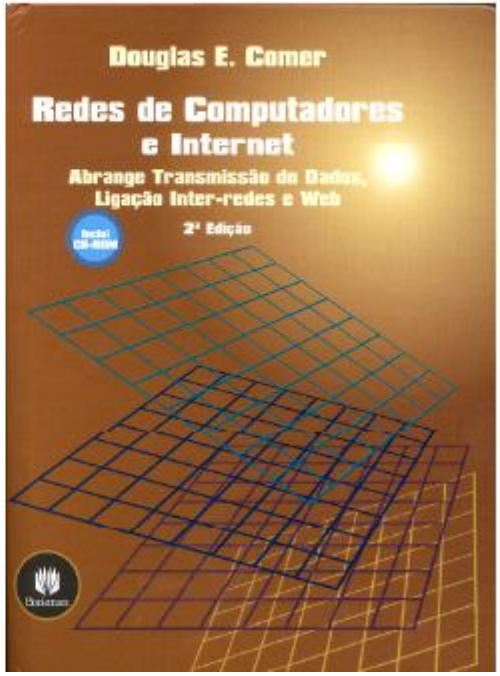


Redes de computadores
e a internet
Kurose



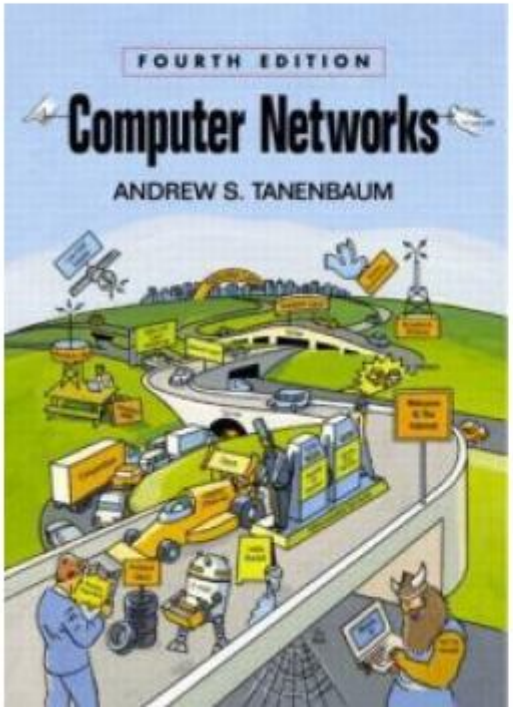
Então para o que querem ....

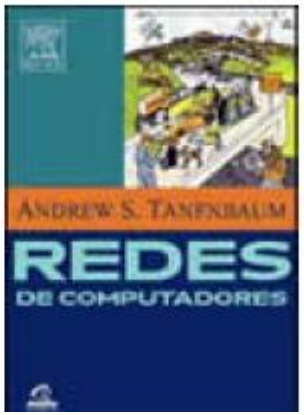
Douglas Comer
http://www.cs.purdue.edu/people/comer



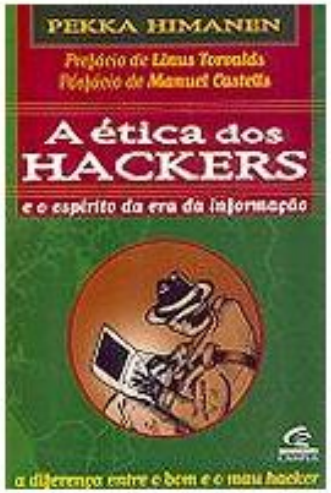
Então para o que querem ....

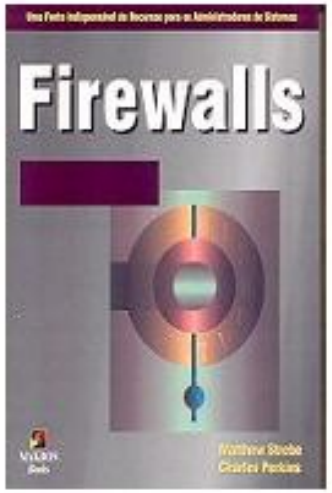
Andrew Tanenbaum
http://bugtraq.ru/library/underground/top.html

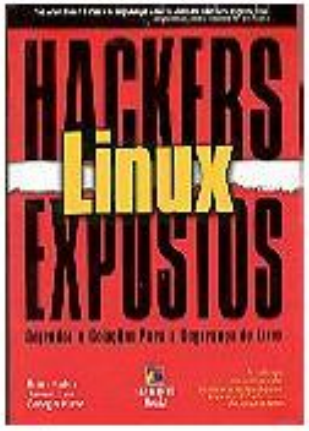


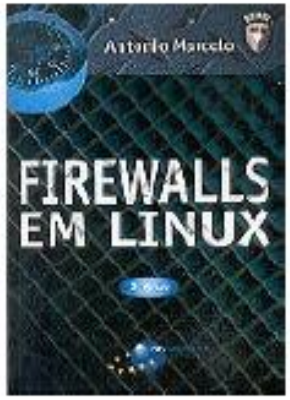


Então para o que querem ....

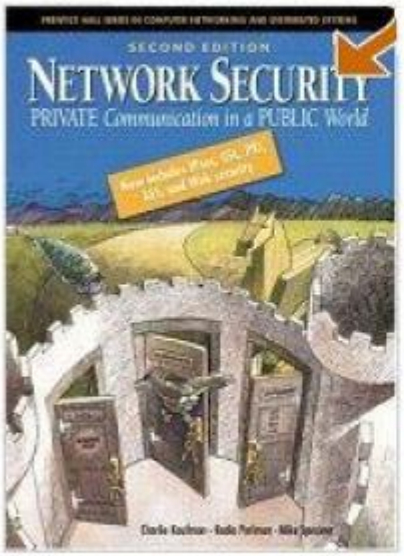


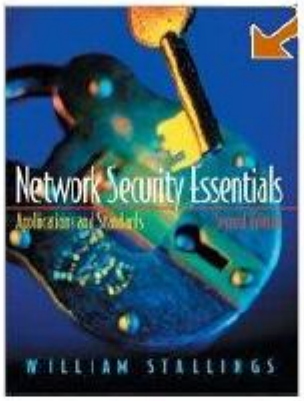


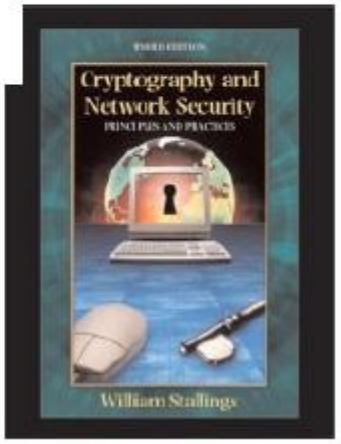




Então para o que querem ....

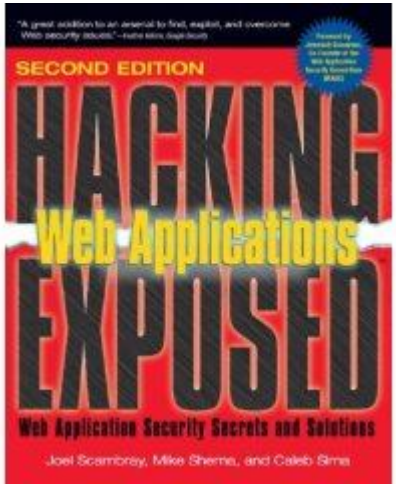


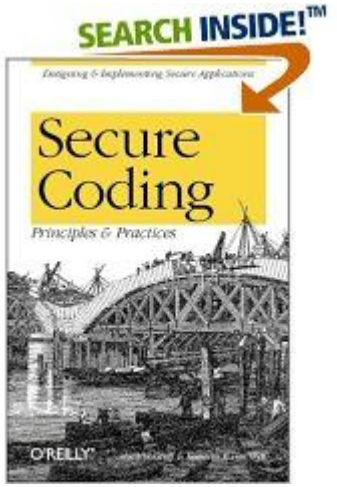


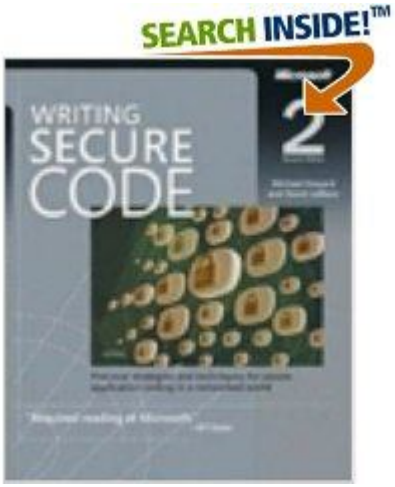


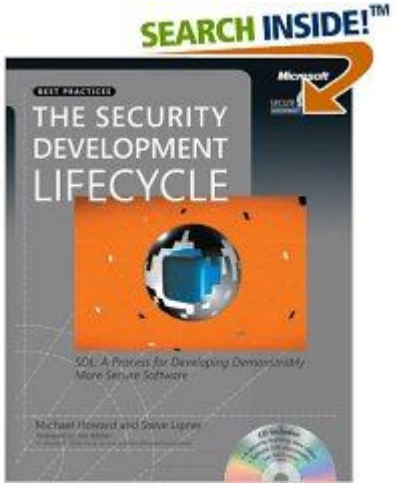
cesar.edu

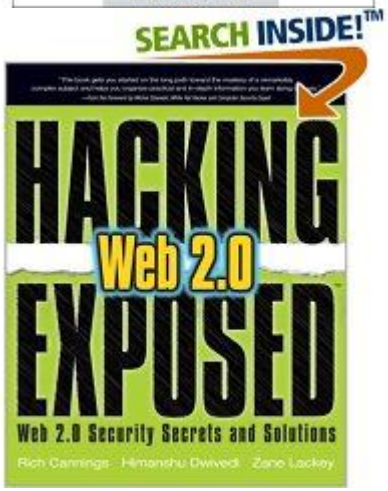
Então para o que querem ....









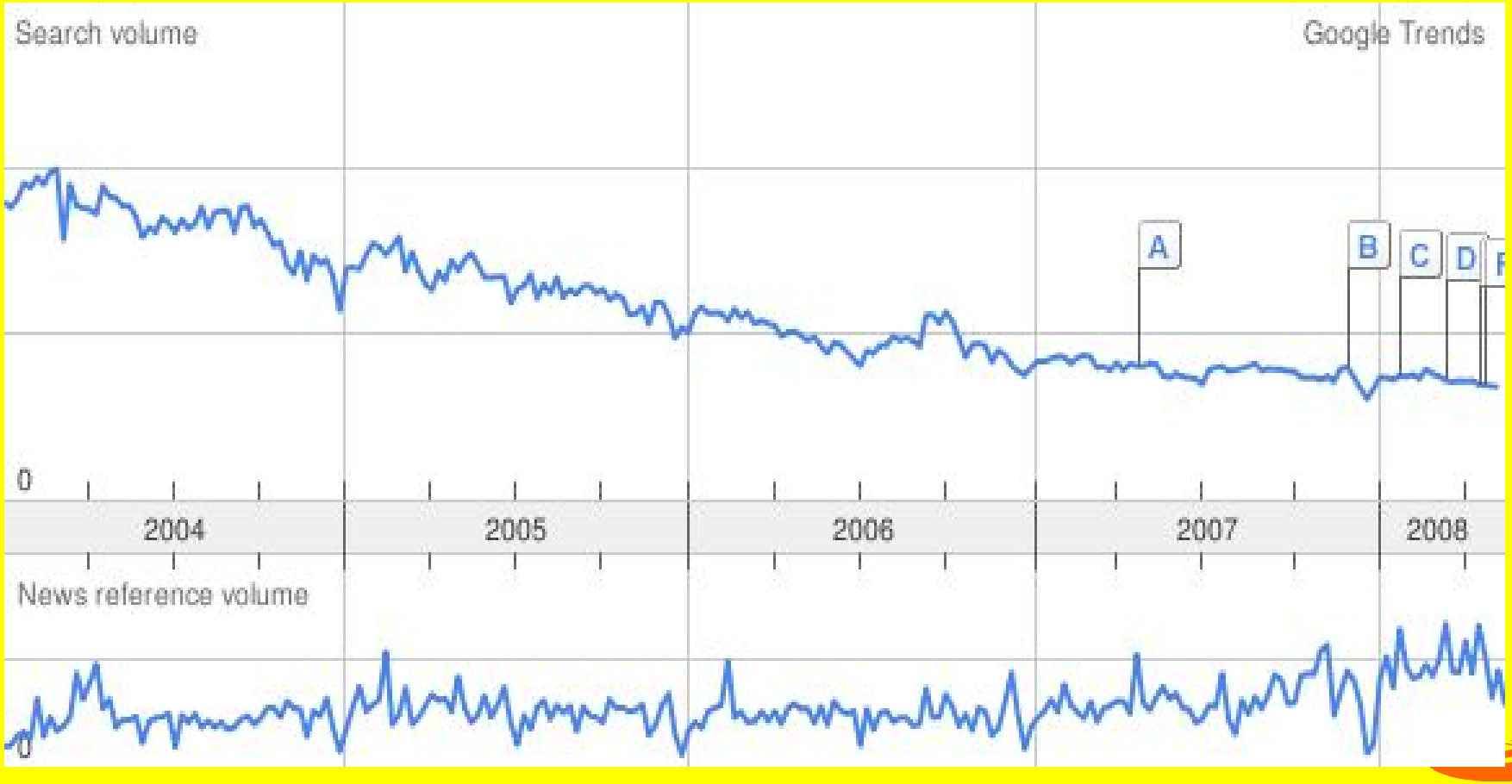


C.E.S.A.R

E como as coisas estão evoluindo ????

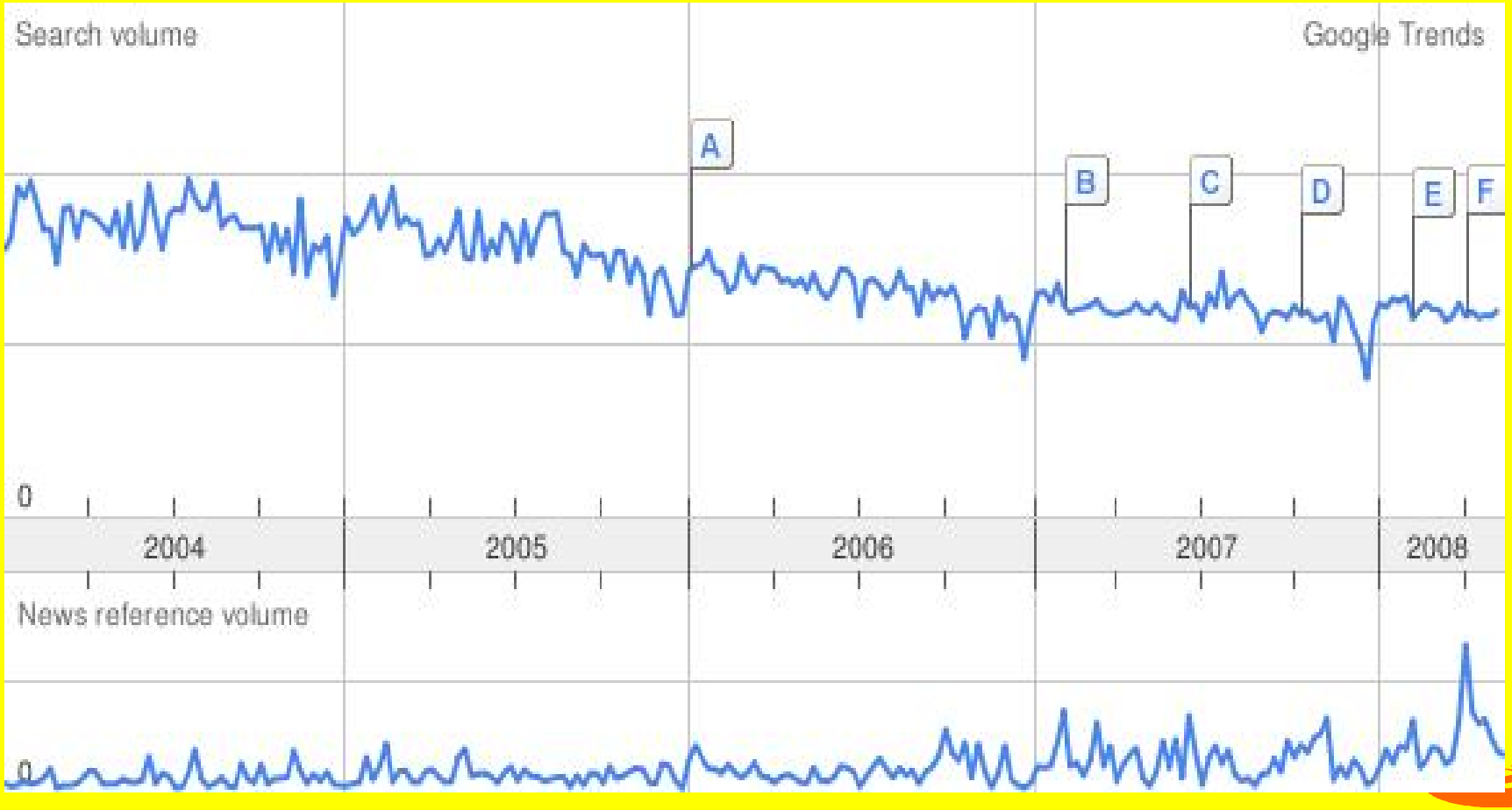
Atualmente duas grandes áreas

– Network security



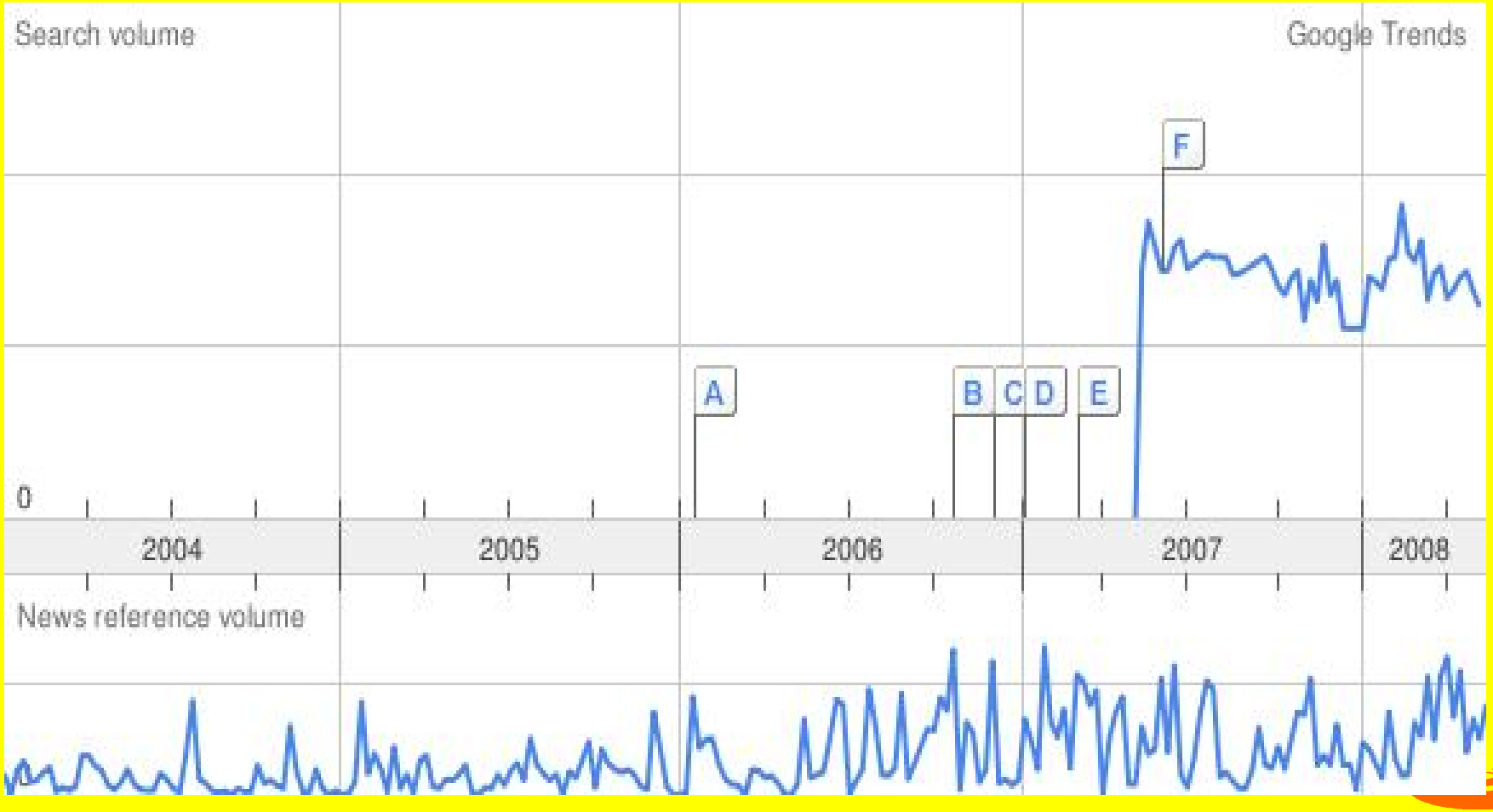
Atualmente duas grandes áreas

– Application security



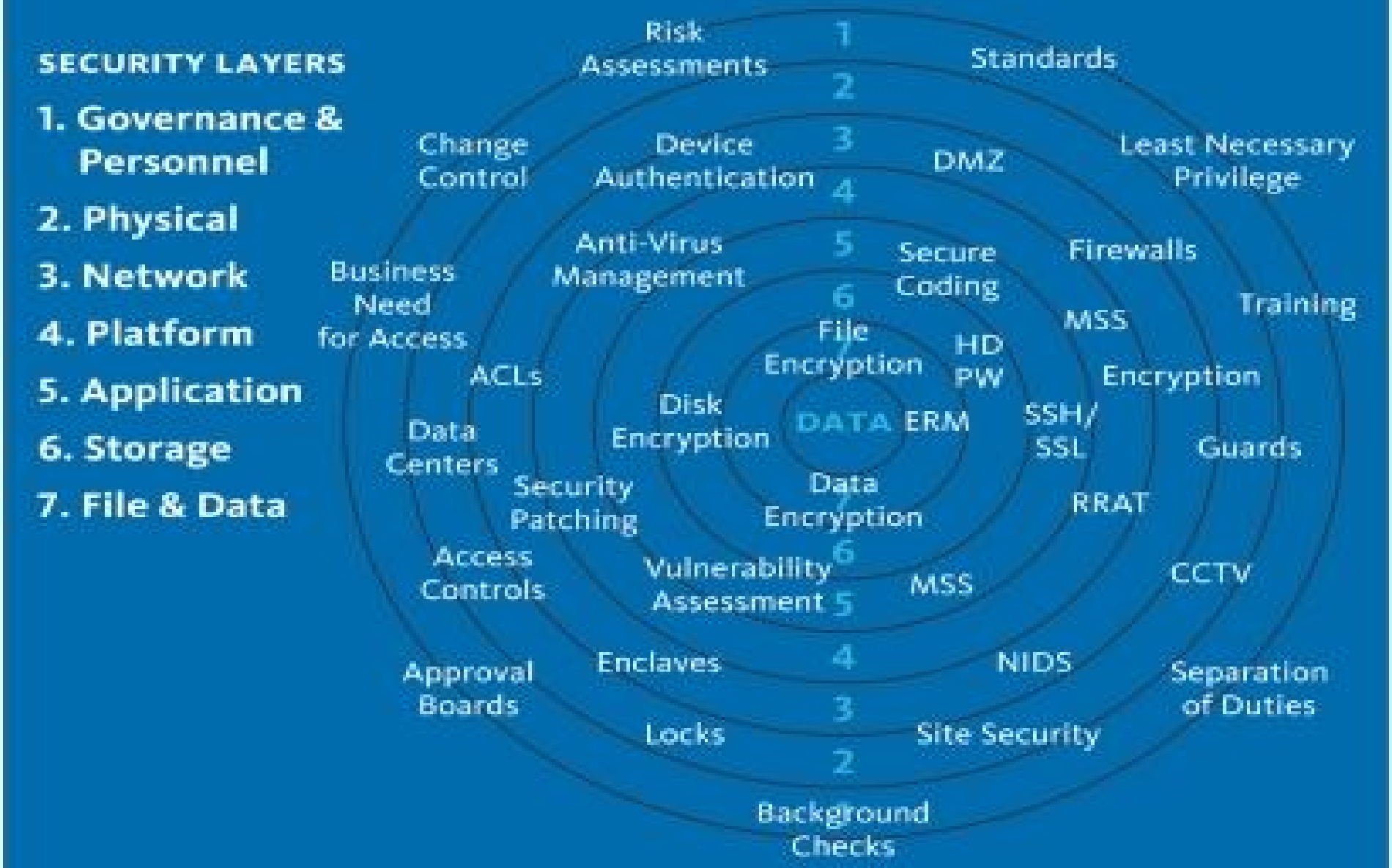
Atualmente duas grandes áreas

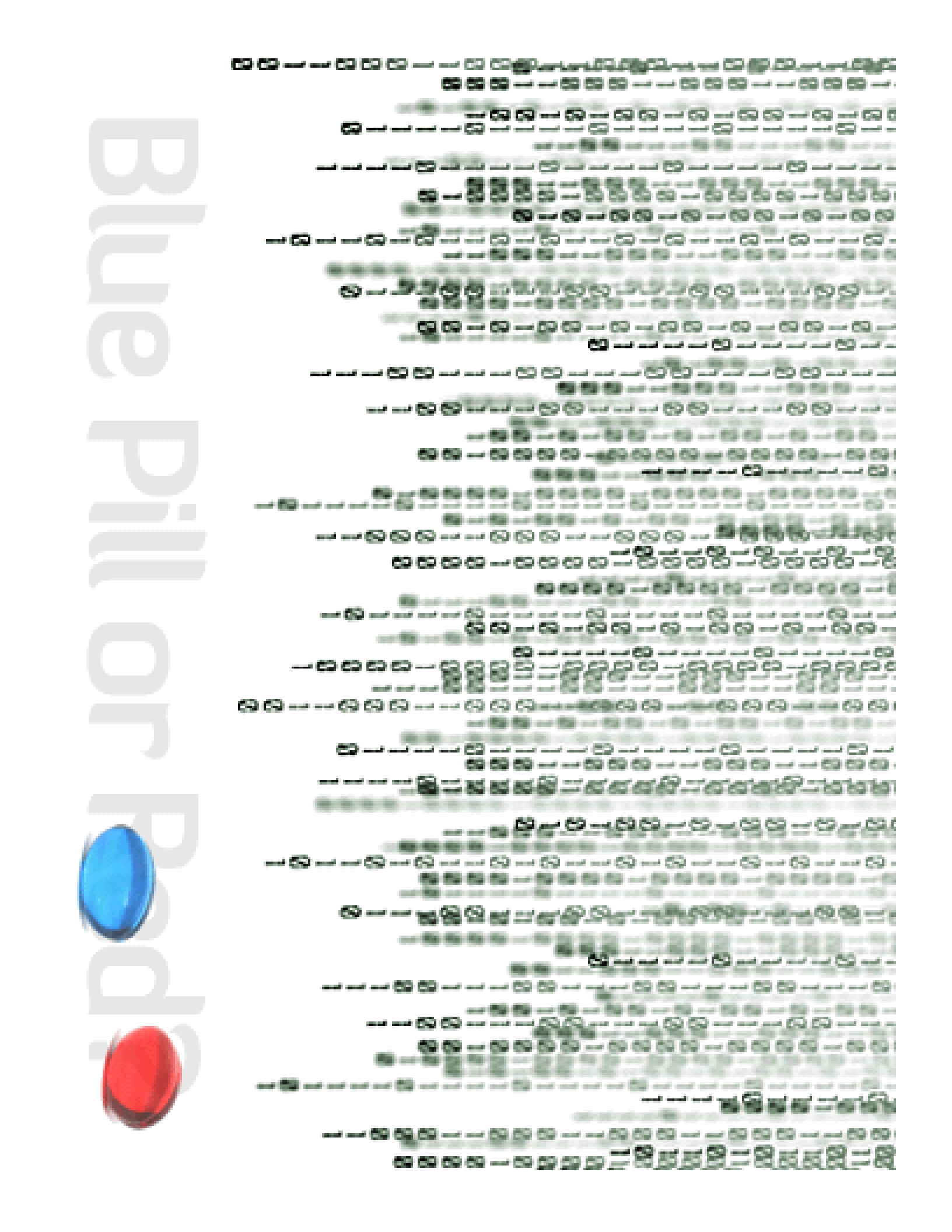
– Web Application security

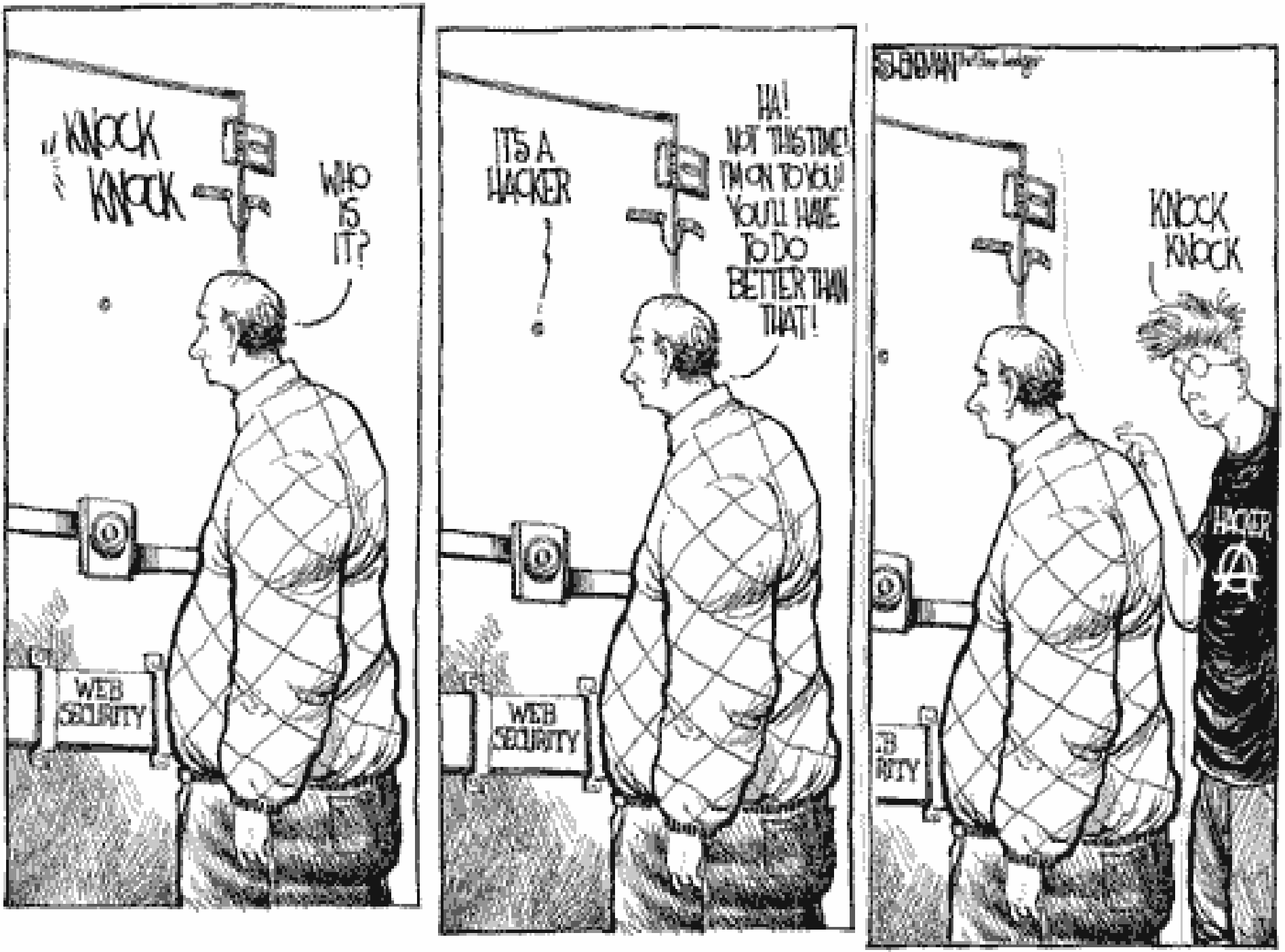


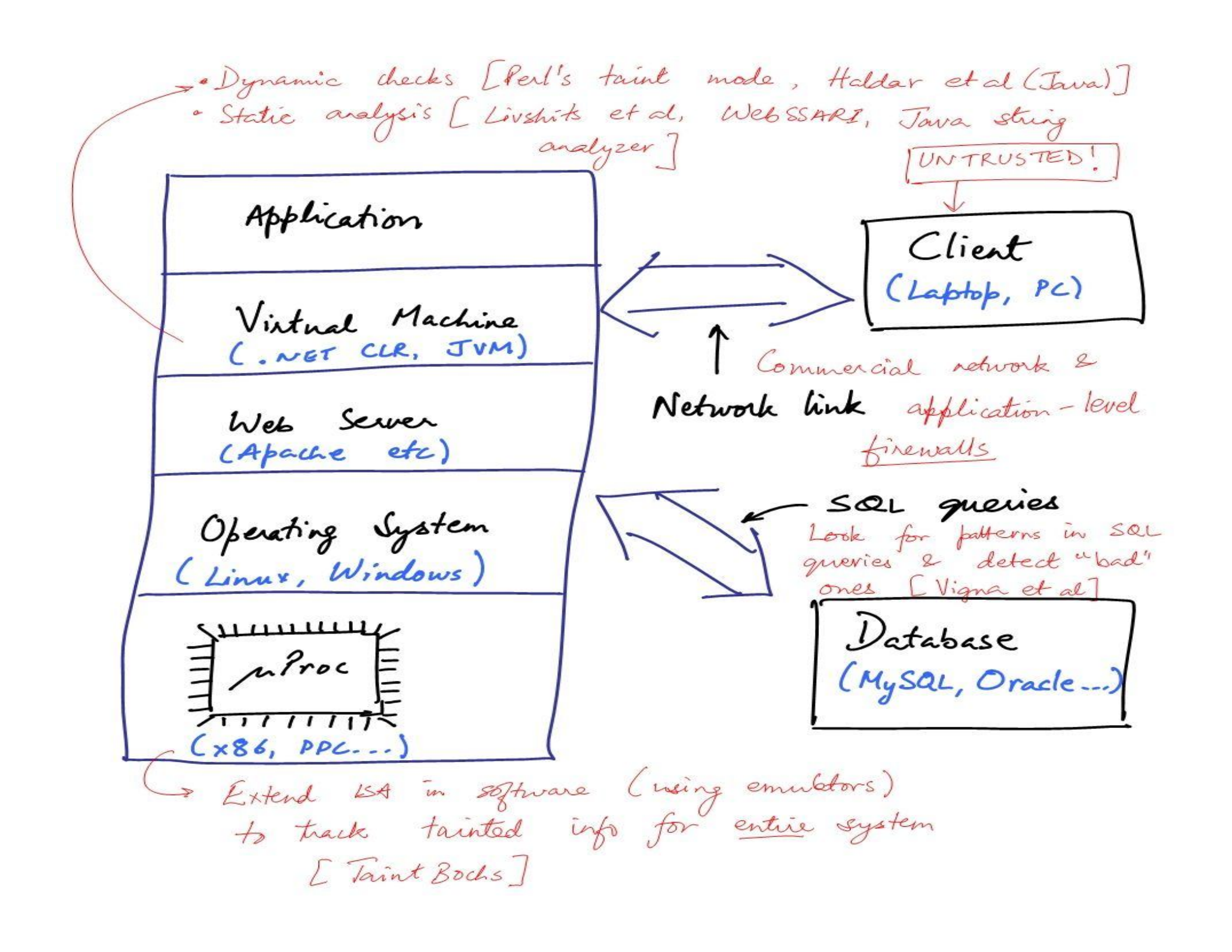
Em aplicações WEB !!!

Figure 4: Layers of Defense for Data Protection






KNOCK KNOCK
WHO IS IT?
WEB SECURITY
IT'S A HACKER!
HA! NOT THIS TIME! I'M ON TO YOU! YOU'LL HAVE TO DO BETTER THAN THAT!
WEB SECURITY
KNOCK KNOCK
HACKER


• Dynamic checks [Perl's taint mode, Haldar et al (Java)]
• Static analysis [Livshits et al, WebSSARI, Java string analyzer]
UNTRUSTED!
Application
Virtual Machine
(.NET CLR, JVM)
Web Server
(Apache etc)
Operating System
(Linux, Windows)
μProc
(x86, PPC...)
Client
(Laptop, PC)
Commercial network & application-level firewalls
Network link
SQL queries
Look for patterns in SQL queries & detect "bad" ones [Vigna et al]
Database
(MySQL, Oracle...)
Extend ISA in software (using emulators) to track tainted info for entire system
[Taint Bochs]

Introdução

- Os ataques a serviços de rede estão se tornando muito sofisticados
- A criatividade humana não para
- Mas o que faltava?
  - APLICAÇÕES!!! Mas será que é possível?
- Atualmente a maioria dos BUG's reportados estão em aplicações
- Application Security != Network Security
- Não se esqueçam: Quem provê acesso aos dados? As aplicações !!!

Lendas Urbanas

- Não há problemas
  - Até que a aplicação seja comprometida
- Erros de runtime não são problemas (tratamento de erros)
  - Exponham informações relevantes
  - Consumam todo recurso do servidor
- Web Services não são vulneráveis
  - Quase nunca testados e raramente segurança é considerada

- Solução
  - Testes de penetração. São caros !!!

Pesquisas

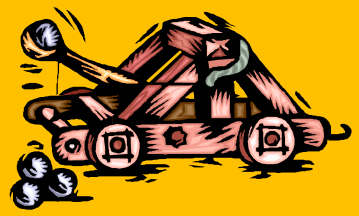
- Gartner
  - **75%** dos ataques acontecem no nível das aplicações
  - Em caso de falha no sistema provavelmente os desenvolvedores são três vezes mais culpados do que os administradores de sistemas
- NIST
  - **92%** das vulnerabilidades estão no nível das aplicações

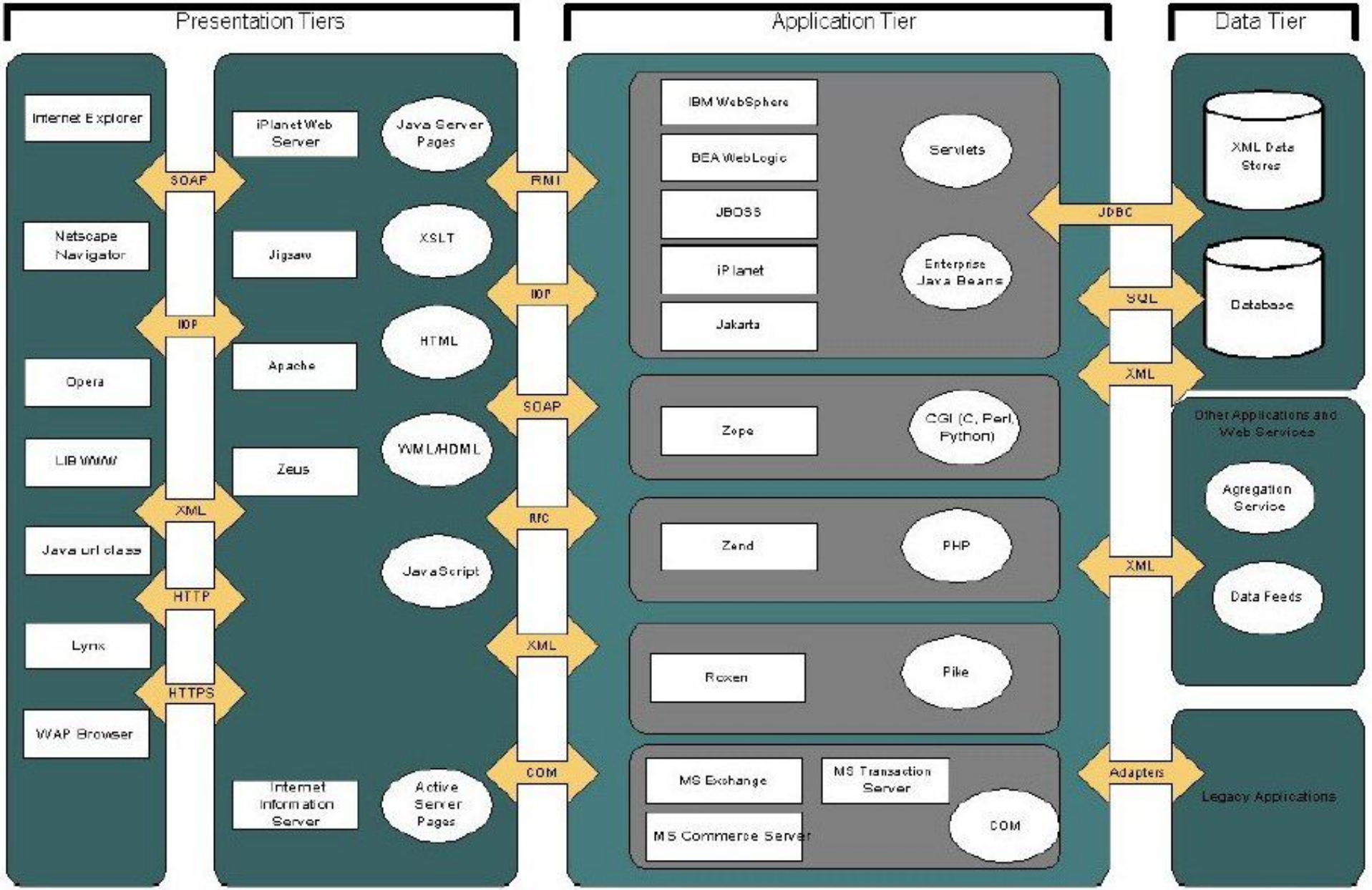
cesar.edu

Objetivo

- Nosso foco será demonstrar estes BUG's de forma prática
- Para nos proteger temos que entender das táticas e armas no nosso inimigo
- Temos que ter nossas armas

para nos defender !!!




Presentation Tiers
Application Tier
Data Tier
Internet Explorer
Netscape Navigator
Opera
LIB WWW
Java url class
Lynx
WAP Browser
SOAP
IIOP
XML
HTTP
HTTPS
iPlanet Web Server
Jigsaw
Apache
Zeus
Internet Information Server
Java Server Pages
XSLT
HTML
WML/HDML
JavaScript
Active Server Pages
RMI
IIOP
SOAP
RPC
XML
COM
IBM WebSphere
BEA WebLogic
JBOSS
iPlanet
Jakarta
Servlets
Enterprise Java Beans
Zope
CGI (C, Perl, Python)
Zend
PHP
Roxen
Pike
MS Exchange
MS Transaction Server
MS Commerce Server
COM
JDBC
SQL
XML
XML
Adapters
XML Data Stores
Database
Other Applications and Web Services
Agregation Service
Data Feeds
Legacy Applications

Testes

Metodologias

- Atualmente existem algumas metodologias de testes de segurança como:
  - OWASP Testing Guide
  - OSSTMM
  - ISSAF
  - NIST

OWASP

- OWASP Testing Guide é baseado na SDLC, e tem por objetivo prover um framework para adoção de testes de segurança nas empresas. Divide-se em cinco fases:
  - Antes do Desenvolvimento começar
  - Durante a Definição e Desing
  - Durante o Desenvolvimento
  - Durante a Implantação
  - Manutenção

cesar.edu

OSSTMM

cesar

OSSTMM 2.1.

Open-Source Security Testing Methodology Manual

Created by Pete Herzog

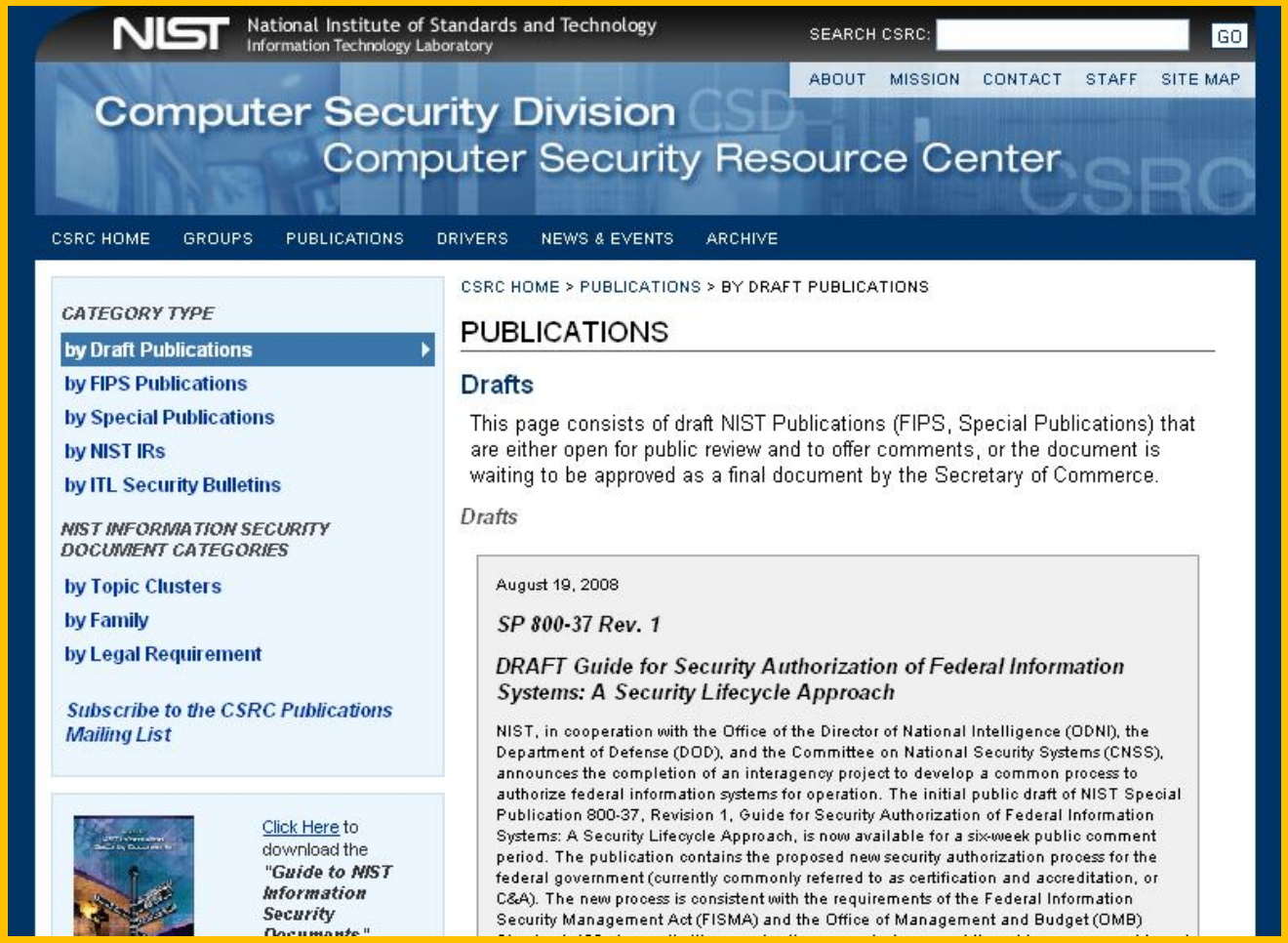
OSSTMM

- OSSTMM do inglês Open-Source Security Testing Methodology Manual, oferece uma metodologia formal para uma auditória operacional de segurança, métricas, regras para uma análise lógica e imparcial e um padrão de relatório de certificação para segurança.

ISSAF

- ISSAF do inglês Information System Security Assessemt Framework, que tem como objetivo prover um único ponto de referencia para avaliação da segurança.

NIST


NIST National Institute of Standards and Technology
Information Technology Laboratory
SEARCH CSRC:
GO
ABOUT MISSION CONTACT STAFF SITE MAP
Computer Security Division
Computer Security Resource Center
CSRC HOME GROUPS PUBLICATIONS DRIVERS NEWS & EVENTS ARCHIVE
CATEGORY TYPE
by Draft Publications
by FIPS Publications
by Special Publications
by NIST IRs
by ITL Security Bulletins
NIST INFORMATION SECURITY DOCUMENT CATEGORIES
by Topic Clusters
by Family
by Legal Requirement
Subscribe to the CSRC Publications Mailing List
Click Here to download the "Guide to NIST Information Security
CSRC HOME > PUBLICATIONS > BY DRAFT PUBLICATIONS
PUBLICATIONS
Drafts
This page consists of draft NIST Publications (FIPS, Special Publications) that are either open for public review and to offer comments, or the document is waiting to be approved as a final document by the Secretary of Commerce.
Drafts
August 19, 2008
SP 800-37 Rev. 1
DRAFT Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach
NIST, in cooperation with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS), announces the completion of an interagency project to develop a common process to authorize federal information systems for operation. The initial public draft of NIST Special Publication 800-37, Revision 1, Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach, is now available for a six-week public comment period. The publication contains the proposed new security authorization process for the federal government (currently commonly referred to as certification and accreditation, or C&A). The new process is consistent with the requirements of the Federal Information Security Management Act (FISMA) and the Office of Management and Budget (OMB)

Testes

- Agora faça seu checklist
  - O que fazer?
  - O que testar?
  - Como fazer?

  - São as resposta que queremos. Vamos começar por .....

AQUI

Primeiros Passos

- Elicitar e documentar os requisitos de segurança
- Mapear e entender as vulnerabilidades associadas a cada requisito de segurança
- Utilizar Checklist para verificar possíveis falhas de código
- Testes funcionais
- Testes Automáticos

Em Aplicações WEB

Elicitando Requisitos

- Esta sendo elaborado um guia que lista os requisitos de segurança web;
- Cada requisito é composto por uma breve explicação, técnicas utilizadas para implementação, e as vulnerabilidades associadas.

Guia

- O Guia vem responder as seguintes perguntas:
  - Qual o meio que será utilizada para o sistema?
  - Qual a solução utilizada?
  - Quais vulnerabilidades precisam ser mitigas?
  - Qual a ação para mitigar?
  - Qual a linguagem a ser utilizada?
  - Impactos da escolha arquitetural, frameworks e componentes?

Template

- Primeiro passo é identificar o objetivo do grupo de requisitos:
  - **Controle de Acesso:** *O subsistema de segurança agrupará as funcionalidades relativas à acessibilidade dos usuários às funções do sistema, é formado pelos módulos abaixo descritos.*

Template

- Segundo passo é identificar o requisito:
  - **[RNF001] Identificação e autenticação Externo:** *Tem por objetivo solicitar ao usuário a digitação de um login alfa e uma senha encriptografada pelo algoritmo<<verificar o algoritmo utilizado>> após ser digitada, previamente cadastrada, efetuando, desta forma, a autenticação do mesmo. Nesta funcionalidade, o sistema determinará a permissão ou a negação de acesso ao Sistema*

Template

- Terceiro passo é identificar prioridades, dependências e impacto:
  - ***Prioridade:*** *Alto*
  - ***Requisitos dependentes:*** RF003 – Desenvolver a interface de login do sistema
  - ***Impacto:*** Baixo, pois os requisitos de performance não são requeridos

Template

- Quarto passo é identificar as vulnerabilidades associadas:

Vulnerabilidade	Mitigação	Impacto
Adivinhar senhas	Política de senha	Usabilidade
Repasse de senhas	Criar uma cultura de segurança na empresa	N/A
Ataque de força bruta	Bloqueio de acesso,	Disponibilidade (pode derrubar o servidor)
Ignorando o esquema de autenticação [33A]	Autenticação de sessões, seguir normas e padrões de segurança no código	Performance
Diretório de transferência / Inclusão de arquivos [33A]	Validar os arquivos incluídos, verificar permissão de acesso aos arquivos	Performance

CheckList

- Faça um checkList com todos os pontos que precisam ser checados na sua aplicação web. Existe arquivos com checklist completos disponibilizados na internet um deles é:
- http://download.microsoft.com/documents/uk/msdn/security/The%20Developer%20Highway%20Code.pdf

cesar.edu

Vulnerabilidades

- URL Manipulation
- SQL Injection
- XSS

C.E.S.A.R

URL Manipulation

- Ferramentas:

SQL Injection

cesar.edu

SQL Injection

- Ferramentas

WSTOOL *(Web vulnerable scanner tool)*

Chorizo! by MAYFLOWER

SQL Inject Me 0.3.0
by Security Compass

dotDefender ™

SQLNINJA
...a SQL Server injection & takeover tool

Web Application Security Project (W.A.S.P.)

cesar

XSS Cross Site Scripting

SQL Injection

- Ferramentas

WSTOOL *(Web vulnerable scanner tool)*

O que estamos fazendo?

ESPECIALIZAÇÃO EM

SEGURANÇA DA INFORMAÇÃO EM ENGENHARIA DE SOFTWARE

TEORIA, TECNOLOGIA E APLICAÇÕES

"CADA 1.000 LINHAS DE CÓDIGO EMBUTEM 15 DEFEITOS DE SEGURANÇA. PORTANTO, NUMA APLICAÇÃO TÍPICA DE 200 MIL LINHAS, EXISTIRÃO 3.000 DEFEITOS DE SEGURANÇA!" *(Ministério da Defesa Americano)*

Para corrigir a parte defeituosa identificada no código é preciso que analistas e programadores conheçam o sistema, tenham sido treinados em segurança e sigam uma metodologia que garanta o desenvolvimento de aplicações seguras. Nosso objetivo é desenvolver estas competências.

INÍCIO DAS AULAS: 19 de junho de 2009
DURAÇÃO: 12 meses (disciplinas + monografia)

HORÁRIOS: Sex- 19h00 às 22h15 | Sáb - 08h00 às 13h00
LOCAL: C.E.S.A.R (Recife Antigo)

Formas de Pagamento:
(por quantidade de parcelas)

INSCRIÇÃO: R$ 45,00
À VISTA: R$5.625,00

NÚMERO DE PARCELAS	PERCENTUAL DE DESCONTO	VALOR DA PARCELA	VALOR TOTAL
1 + 14	–	R$375,00	R$5.625,00
1 + 12	5	R$411,05	R$5.343,75
1 + 9	8	R$517,50	R$5.175,00
1 + 6	10	R$726,58	R$5.086,80

Descontos para grupos:
(por quantidade de alunos, cálculo base valor de R$5.625,00)

QUANTIDADE DE ALUNOS	PERCENTUAL DE DESCONTO
GRUPO DE 03	5%
GRUPO DE 06	10%
GRUPO COM MAIS DE 09	15%

OBJETIVO:
Promover a habilidade de entender e aplicar aspectos fundamentais para o desenvolvimento de Software Seguro.

PÚBLICO-ALVO:
O curso destina-se a gestores e profissionais do setor de TIC - Tecnologia da Informação e Comunicação, com formação superior, que desejam se especializar na área de Segurança com enfoque na construção de sistemas seguros. Também está direcionado a estudantes diplomados em cursos de Graduação em Ciências Exatas que buscam aprofundar-se em tópicos avançados na área de Segurança e Redes de Computadores.

c e s a r cesar.edu

Acesse o site e inscreva-se:
www.cesar.edu.br/siesta.html
(81) 3425 .4700


Instituto Nacional para Engenharia de Software - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://www.ines.org.br/
posgraduacao mauricio de nassau
Mais visitados Real Internet Banking intranet Oraculo(suporte) ::We... ABN AMRO Asset Man... MirrerDesk Bem-vindo ao Gmail Traffic Analysis for 4 --... Login 0180s.com - Media Pla...
CS155 Co... FSM - Pós ... Category:... Chamada ... String enc... SSS 2009 Submarino... JSON - Pes... A200 - Gab... The largest... Programaç... Institu...
Instituto Nacional de Ciência e Tecnologia para Engenharia de Software
ines
Home Sobre Missão Laboratórios Pesquisadores Objetivos Metas Log in
Buscar
INES submete 22 pedidos de bolsas de pós-graduação à CAPES (0)
Publicado em June 3rd, 2009 Uncategorized
A CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) realizou uma chamada no âmbito do Edital Programa Institutos Nacionais de Ciência e Tecnologia para bolsas de pós-graduação (mestrado, doutorado, doutorado sanduiche e pós-doutorado). Os alunos contemplados receberão as bolsas a partir de 01/07/2009. O INES pediu um total de 22 bolsas, sendo 14 de mestrado, 1 de doutorado, 5 de doutorado sanduiche e 2 de pós-doutorado. Os candidatos às bolsas são alunos de 5 programas de pós-graduação orientados por pesquisadores do INES. Agora é torcer e aguardar o resultado.
Dissertação de Mestrado Premiada - VII CTDQS - SBQS 2009 (0)
CALENDÁRIO
June 2009
M T W T F S S
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
« May
ines_inct
10 Followers
LOGIN
FOLLOW
INES submete 22 pedidos de bolsas de pós-graduação (mestrado, doutorado, sanduiche e pós-doutorado) à CAPES.
Arquivos
June 2009
May 2009
March 2009
January 2009
December 2008
Categorias
Notícias (22)
Sobre o Instituto (9)
Trabalhos em eventos (5)
Uncategorized (13)
Instituições envolvidas
CESAR
UFPE
Leu s3.amazonaws.com
Tor desabilitado

Pesquisa !!!

- Doutorando professor Silvio Meira
- Colaborador Professor Ruy Queiroz
- 6 Alunos de mestrado
- 4 Alunos de especialização

- Mais 8 bolsas vindo .....

Referências

- http://www.owasp.org/
- http://www.isecom.org/osstmm/
  - Open-Source Security Testing Methodology Manual
- Web Application Disassembly with ODBC Error Messages
- JavaOne 2005
  - Strategies for Securing Java™ Technology Code
  - Web Services Security Attacks in Action
  - 9 Ways to Hack a Web App
- Advanced SQL Injection In SQL Server applications
- Advanced Cross Site Scripting
- CROSS-SITE TRACING (XST)
- SQL Injection Signatures Evasion

F I M

rodrigo.assad@cesar.org.br