O que interessa não é o servidor web
GTS 13 – São Paulo, Brasil

Luiz Eduardo DoS Santos

CISSP GISP GCIH CEH CWNE

Senior Security Engineer – Latin America

O que interessa não é (apenas) o servidor web
GTS 13 – São Paulo, Brasil

Luiz Eduardo DoS Santos

CISSP GISP GCIH CEH CWNE

Senior Security Engineer – Latin America

Who am I?

- That same guy.

Agenda

- Introduction
- Why are we here discussing this, now? (aka: infoSec)
- Beyond the web-server (the technical brief)
- Setting the stage
- Scenarios
- Conclusion
- Q&A

Introduction

Introduction

- Evolution
  - Internet focused on web services
  - Attacks
  - Mainstreaming

Web/ Internet

- ~20 years ago (give or take) people start using the www
- Mid 90s it start growing all over the place
- Late 90s all companies have a web presence
- y2k people actively using the internet for "everything"
- The bubble busted
- Who survived
- Web2.0, social networks, etc...

“useful” web services

- Internet banking
- e-commerce
- Stock trading
- .gov stuff
- b2b
- “i-commerce”

Attacks

- FUN
  - Defacement/ local attacks (server-side)
  - Network based (DoS)
  - Web services (via worms, affecting the network)
- Profit
  - "Infection" attacks (flash, players, etc)
    - Botnets, malware, etc
  - Stealing (confidential) data

Mainstreaming

- Web
- (useful) Services
- Web 2.0
  - Social Networks

Why are we here ?

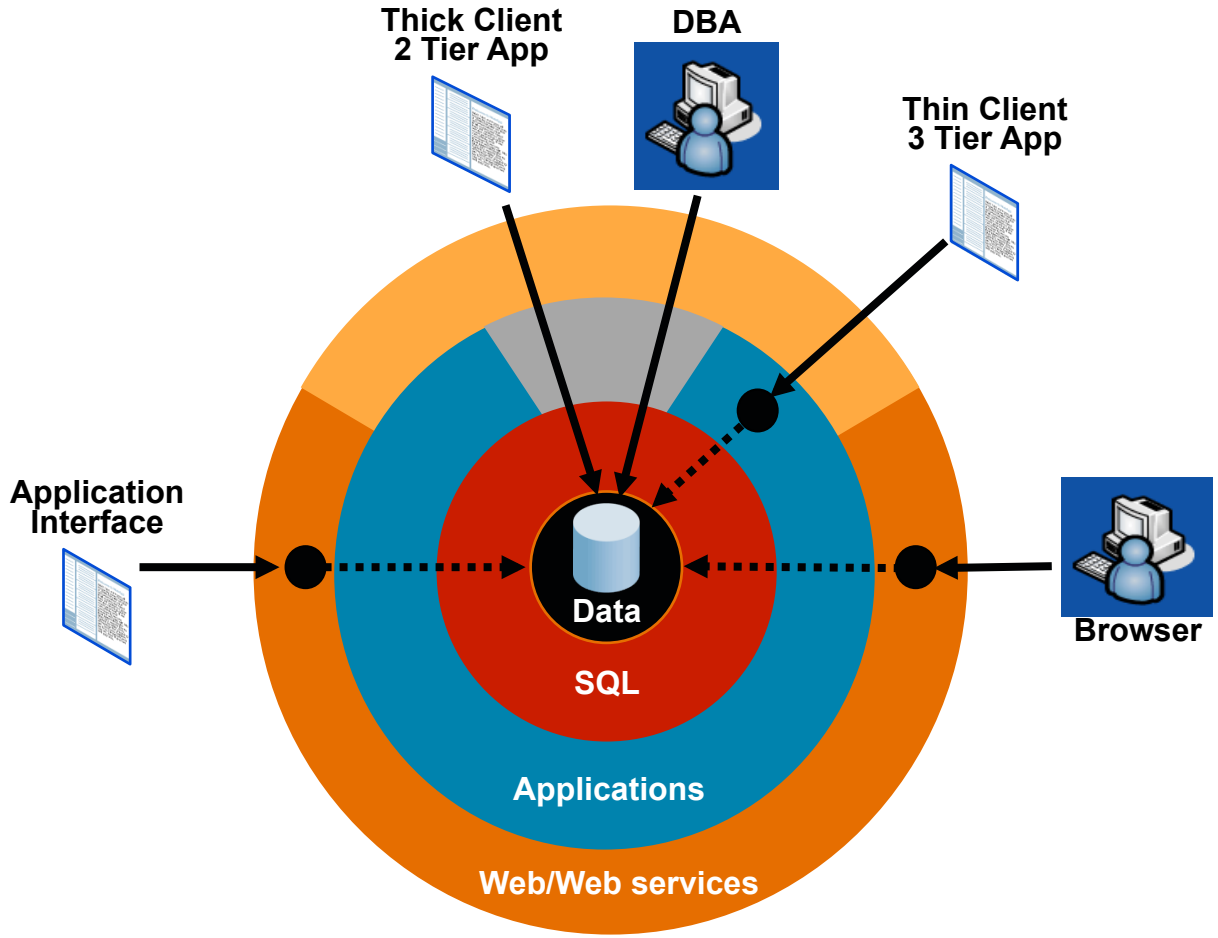
InfoSec

- Information Security

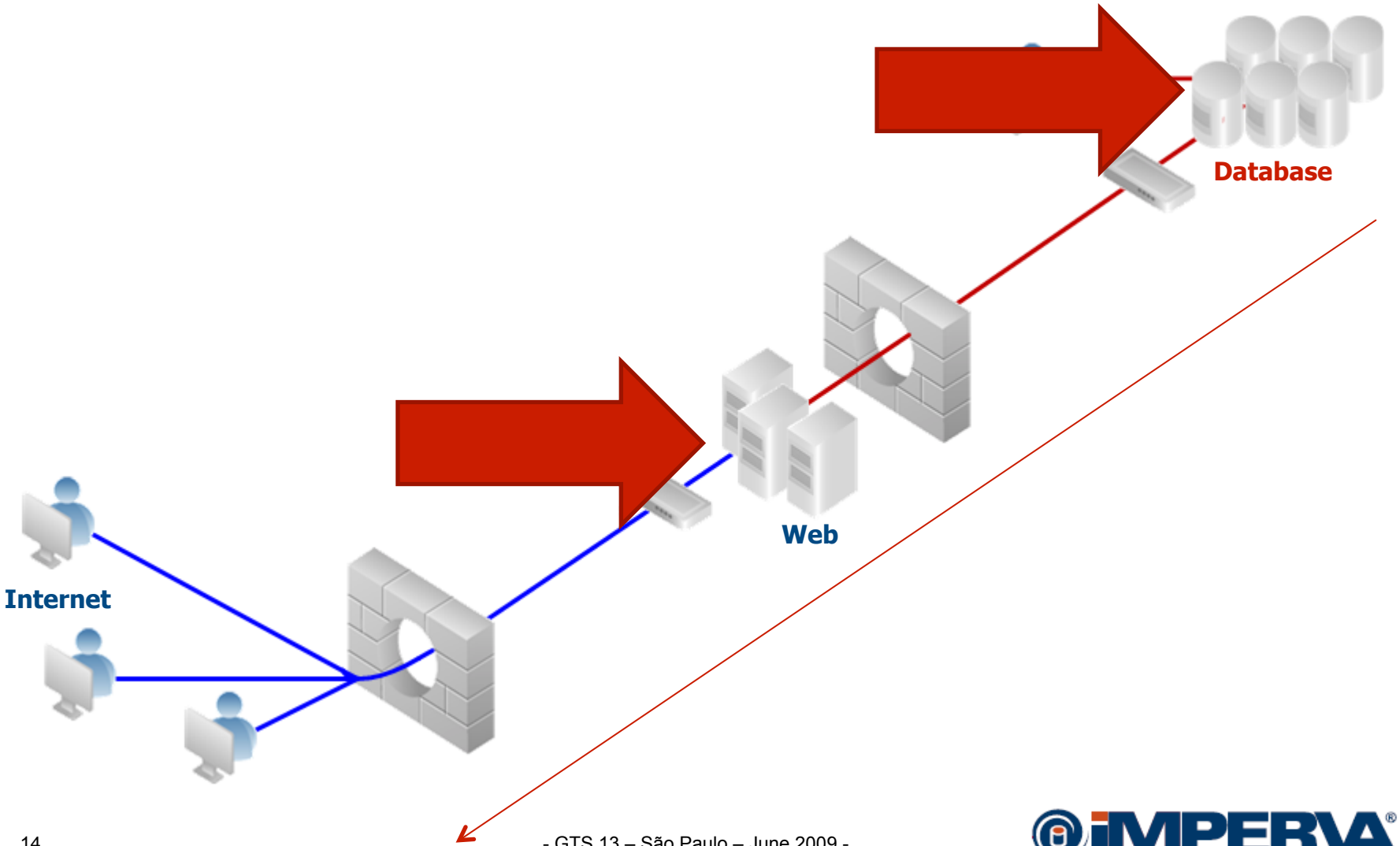
  "**Information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction." from wikipedia

- What information is important though?

Monitoring & Protecting Data



The Typical Web Scenario



Web Attacks

- SQL Injection
- XSS
- Cookie Poisoining
- Session-Hijacking
- Command Injection
- Web Worms
- ...

- Reality, very very important, but that would be a whole new talk...

Setting the stage


AWARENESS

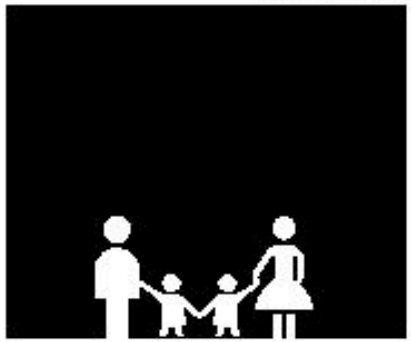
The Different Scenarios

- Aka: “explicando com maçãs”
- Nothing new, but, maybe part of the day-to-day activities we just assume are safe or just learned not to care about
- ... Or not realize it’s about database security

29/08/2008 - 10h12

PF apura venda de senha para rede de dados

ANDRÉ CARAMANTE
da **Folha de S.Paulo**



Senhas de acesso ao Infoseg, sistema federal responsável pela interligação dos bancos de dados de todos os órgãos de segurança pública do país, são vendidas atualmente por aproximadamente R$ 2.000 na região da rua Santa Ifigênia, no centro de São Paulo.

A Abin (Agência Brasileira de Inteligência) e a Polícia Federal investigam quem vende e quem compra as senhas que, a partir de qualquer computador conectado à internet, permitem consultar dados cadastrais e sigilosos dos cidadãos.

A rede Infoseg é controlada pela Senasp (Secretaria Nacional de Segurança Pública), órgão do Ministério da Justiça. Além de guardar dados sigilosos sobre qualquer cidadão, a rede tem informações sobre todas as empresas com sede no território nacional -inclusive nomes e endereços de seus donos ou responsáveis.

Dados como CPF, RG, endereços residenciais e comerciais, e-mails, telefones, título de eleitor, carteira nacional de habilitação, placas de carros e até registros de armas estão disponíveis na rede.

O Ministério da Justiça, órgão responsável pela Senasp e pela Infoseg, as polícias Civil e Militar de todos os Estados, os Ministérios Públicos Estaduais e o Federal, a Receita Federal, o Judiciário, a Abin e a PF também usam a base de dados para realizar suas investigações.

Ontem, o telejornal "SBT Brasil" exibiu reportagem na qual mostrou como conseguiu comprar por

Scenario 3 = Internet Banking

Scenario 4 = The ISP and the Bank

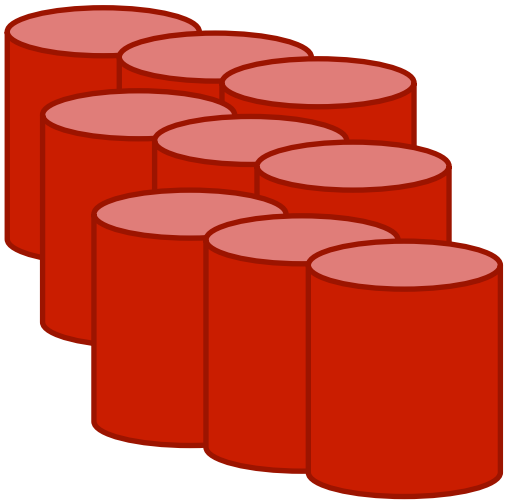
Scenario 5 = The Happy Call Center Rep

For sure?

Database Servers

DBA(s)

Shipping Dept



Sales Dept

Marketing Dept

Customer Services

Technical Support

Always there

New factor

Company Credibility, really?

- Would you stop using a site that got pwn3d?

Profit = Money? (always?)


Comcast
YouTube
facebook
YAHOO!

Cloud Computing / Outsourcing

Corporate Espionage

Conclusion (leading to solutions?)

- Provider side:
  - Avoid/ eliminate bad business practices
  - Enforce policies (like, no user/dba credential sharing)
  - (try to) solve internal abuse
  - Bring the security maturity from the perimeter to the internal net
  - (smart) DiD, not only throwing boxes in the net
  - Test your infrastructure, servers, etc, for security
- Customer side
  - Analyse risks involved before taking decisions on providers
  - Analyse what you do as a mortal user on the internet
  - Take brand-damaging seriously

Until "Visite a Nossa Cozinha" for InfoSec

IMPERVA®

Questions?

Muito Obrigado

Luiz Eduardo DoS Santos
le<at>imperva.com