THE DEVELOPER'S CONFERENCE

Trilha Segurança e Criptografia

Técnicas básicas de confidencialidade de dados em aplicações web

Jerônimo Fagundes da Silva

Especialista em Desenvolvimento de Software @KingHost

Quem sou eu?

THE DEVELOPER'S CONFERENCE

- Jerônimo Fagundes <jeronimo@jeronimofagund.es>
- Bacharel em Ciência da Computação pela UFRGS.
- Visitante no Programa de Pós Graduação em Computação da UFRGS na disciplina Computer Systems Security
- Trabalho com desenvolvimento de software voltado à web há mais de 15 anos.
- Já trabalhei com diferentes tecnologias, e sempre voltadas à web: HTML, JavaScript, CSS, PHP, MySQL, C, PostgreSQL, e ainda outras que não estou lembrando agora. :-D
- Atualmente trabalho como Especialista em Desenvolvimento de Software na KingHost em Porto Alegre-RS.

Sumário

THE DEVELOPER'S CONFERENCE

- Objetivo
- Motivação
- Conceito de Confidencialidade
- Arquitetura-exemplo e possíveis agentes
- Mecanismos
  - Controles de Acesso
  - Criptografia em Trânsito
  - Criptografia em Repouso
  - Criptografia de Ponta-a-Ponta
  - Privacidade Diferencial (menção honrosa)
- Conclusão

Objetivos

- Apresentar o conceito de confidencialidade
- Conscientizar sobre a existência de mecanismos para reforçar políticas de confidencialidade
- Mostrar que não há bala-de-prata ou solução all-in-one que resolva o problema apresentado

Motivação

THE DEVELOPER'S CONFERENCE

- Lei Geral de Proteção de Dados (LGPD)
  - Lei nº 13.709 de 14 de agosto de 2018
  - Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a **proteger os dados pessoais de acessos não autorizados**(…)
    - § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
  - Art. 47. Os agentes de tratamento (…) obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Motivação

THE DEVELOPER'S CONFERENCE

- General Data Protection Regulation (GDPR)
  - Art. 32 § 1. (…) the controller and the processor **shall implement appropriate technical** and organisational **measures to ensure** a level of **security** appropriate to the risk, including inter alia as appropriate:
    - (a) **the pseudonymisation and encryption of personal data**;
    - (b) the ability to ensure the ongoing **confidentiality**, integrity, availability and resilience of processing systems and services;

Motivação

THE DEVELOPER'S CONFERENCE

- Declaração Universal dos Direitos Humanos
  - Artigo XII. **Ninguém será sujeito à interferência em sua vida privada**, em sua família, em seu lar ou **em sua correspondência**, nem a ataque à sua honra e reputação. **Todo ser humano tem direito à proteção da lei contra tais interferências** ou ataques.

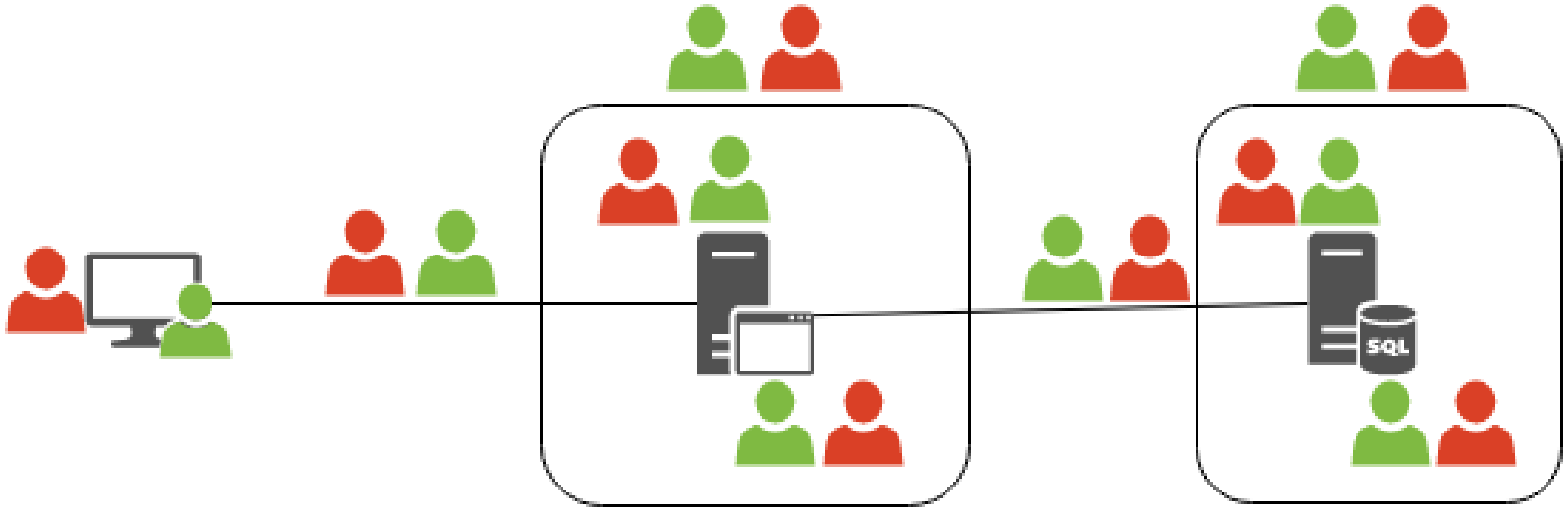
Conceito de Confidencialidade

THE DEVELOPER'S CONFERENCE

- ***"Confidentiality is the concealment of information or resources. (…) All the mechanisms that enforce confidentiality require supporting services from the system. The assumption is that the security services can rely on the kernel, and other agents, to supply correct data. Thus, assumptions and trust underlie confidentiality mechanisms."***
  BISHOP, Matt. Computer Security - Art and Science. Second Ed. Pearson Education, 2019.

Arquitetura-exemplo e possíveis agentes

THE DEVELOPER'S CONFERENCE



Mecanismos – Controles de Acesso

THE DEVELOPER'S CONFERENCE

Mecanismos – Controles de Acesso

THE DEVELOPER'S CONFERENCE

- Do sistema operacional
  - De serviços: **Pluggable Application Module (PAM)**

Vantagens	Desvantagens
Estabilidade	Administrador tem muito poder
Documentação	
Modularidade	

Mecanismos – Controles de Acesso

THE DEVELOPER'S CONFERENCE

- Do sistema operacional
  - De sistema de arquivos: **Ownership and Permissions (Linux)**

Vantagens	Desvantagens
Estabilidade	Administrador tem muito poder
Documentação	Manutenção
Facilidade de aplicar	

Mecanismos – Controles de Acesso

THE DEVELOPER'S CONFERENCE

- Do banco de dados - **MariaDB GRANT Statement**

Vantagens	Desvantagens
Estabilidade	Usuário com permissão GRANT tem muito poder
Documentação	Administrador do BD tem acesso total
Compartimentalização	
Fácil aplicação e manutenção	

Mecanismos – Controles de Acesso

THE DEVELOPER'S CONFERENCE

- Das APIs - **The OAuth 2.0 Authorization Framework (IEEE RFC 6749)**

Vantagens	Desvantagens
Suporte a linguagens (bibliotecas)	Necessário subir serviço de autenticação / autorização
Documentação	Cuidado com refino de permissões
	Administrador do serviço tem muito poder

Mecanismos – Controles de Acesso

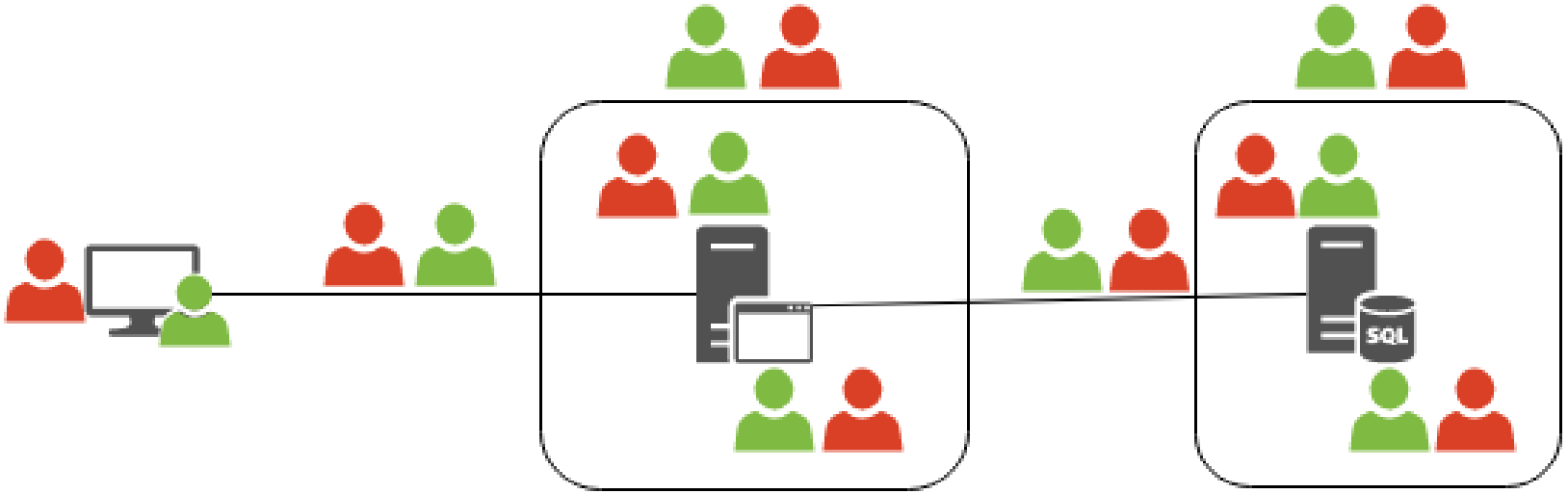
THE DEVELOPER'S CONFERENCE

- De rede – **Firewall** (IPv4 e IPv6!)

Vantagens	Desvantagens
Estabilidade	Se topologia for complexa, difícil administrar
Documentação	Se atacante está na rede autorizada, passa
Só autorizados tem acesso	Administrador do serviço tem muito poder

Mecanismos – Controles de Acesso

THE DEVELOPER'S CONFERENCE



Mecanismos – Criptografia em Trânsito

THE DEVELOPER'S CONFERENCE

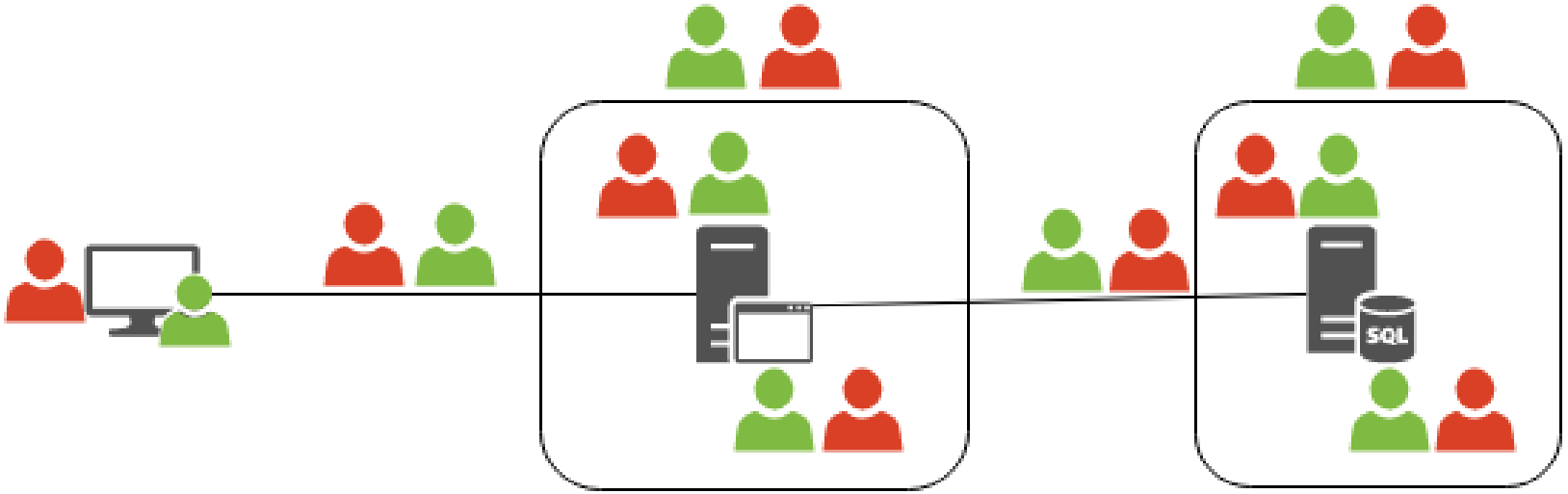
Mecanismos – Criptografia em Trânsito

THE DEVELOPER'S CONFERENCE

- **The Transport Security Layer (TLS) Protocol Version 1.3 (IEEE RFC 8446)**
- **HTTP over TLS (HTTPS) (IEEE RFC 2818)**

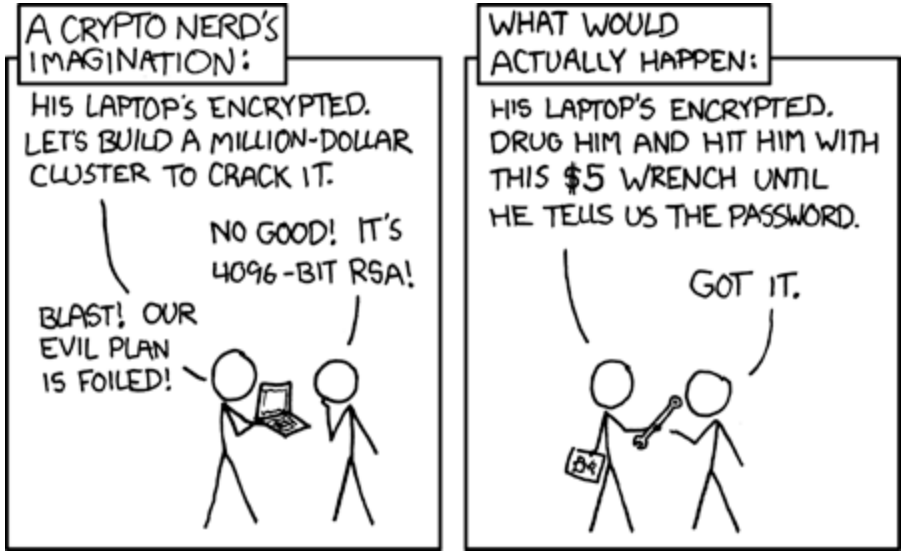
Vantagens	Desvantagens
Ilegibilidade em trânsito	Pessoas com acesso ao servidor conseguem ler
Somente par cliente X servidor vê aberto	Requer autoridades certificadoras

Mecanismos – Criptografia em Trânsito



Mecanismos – Criptografia em Repouso

THE DEVELOPER'S CONFERENCE



Mecanismos – Criptografia em Repouso

THE DEVELOPER'S CONFERENCE

- No sistema de arquivos – **LUKS**

Vantagens	Desvantagens
Facilidade	Uma vez aberta, acessível a qualquer um
Protege todos os arquivos da partição	Administrador é o portador da chave

Mecanismos – Criptografia em Repouso

THE DEVELOPER'S CONFERENCE

- No banco de dados – **MariaDB Encryption Functions**

Vantagens	Desvantagens
Facilidade	Simétrica: chave precisa ser enviada ao banco
Algoritmos estado-da-arte	Administrador do BD/servidor pode ver senha

Mecanismos – Criptografia em Repouso

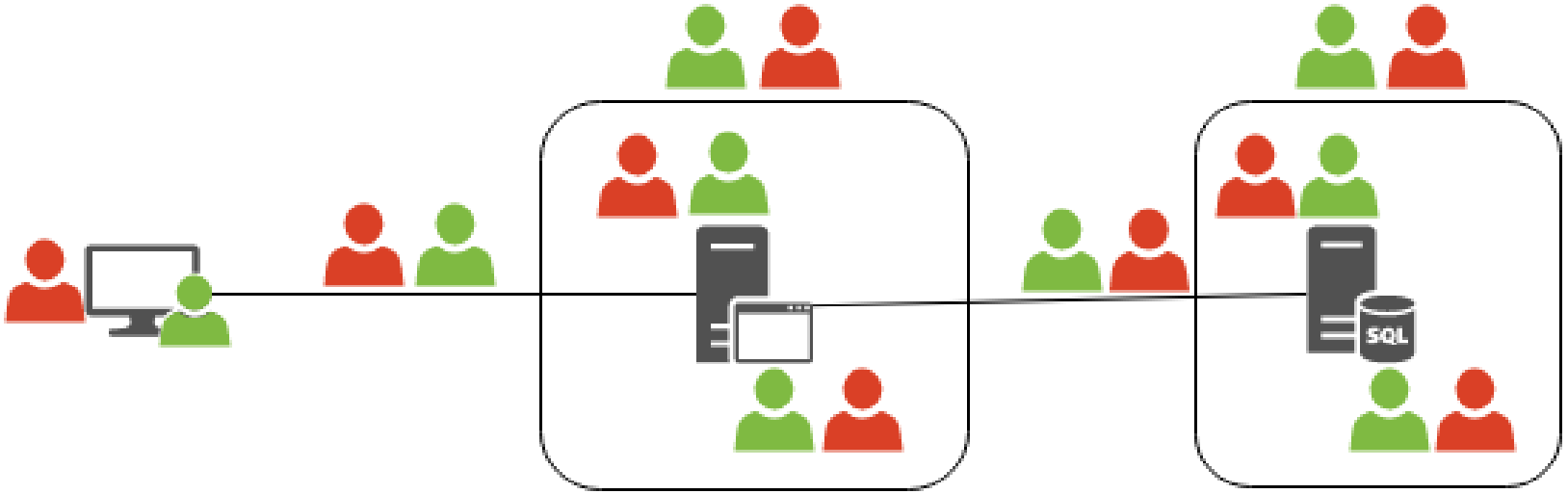
THE DEVELOPER'S CONFERENCE

- Na aplicação – **PHP: OpenSSL – Manual**

Vantagens	Desvantagens
Facilidade	Administrador do servidor de aplicação pode ver senha
Algoritmos estado-da-arte	Impossibilita operações sobre dados no banco
Servidor de BD nunca recebe a chave	

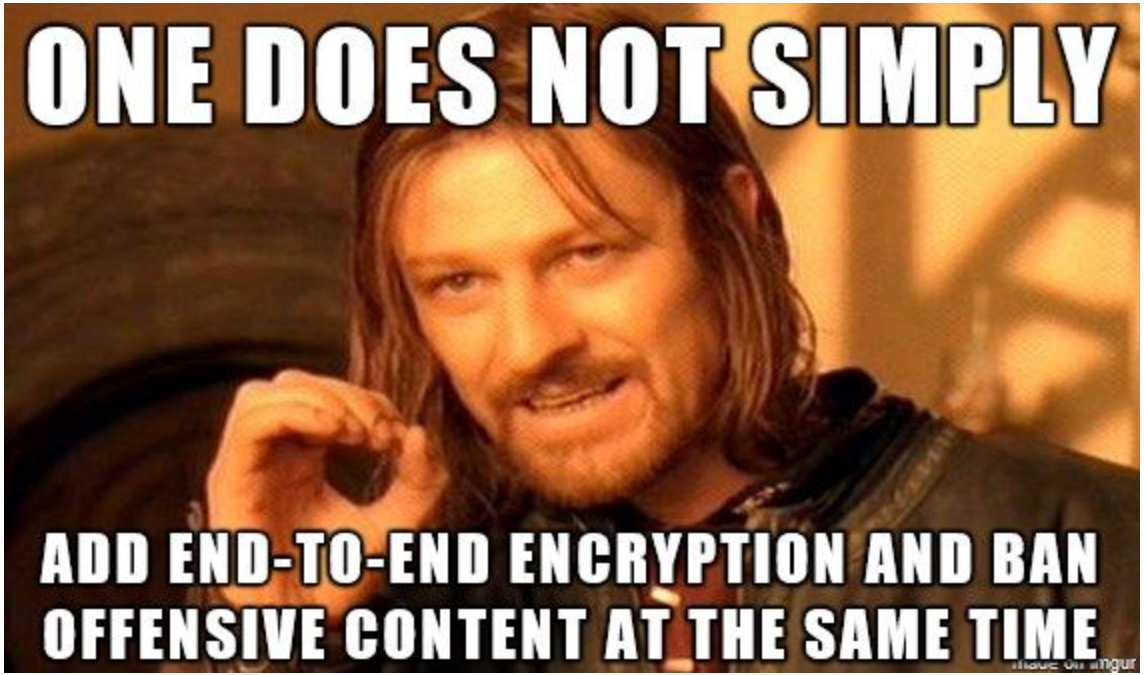
Mecanismos – Criptografia em Repouso

THE DEVELOPER'S CONFERENCE



Mecanismos – Criptografia de Ponta-a-Ponta

THE DEVELOPER'S CONFERENCE



Mecanismos – Criptografia de Ponta-a-Ponta

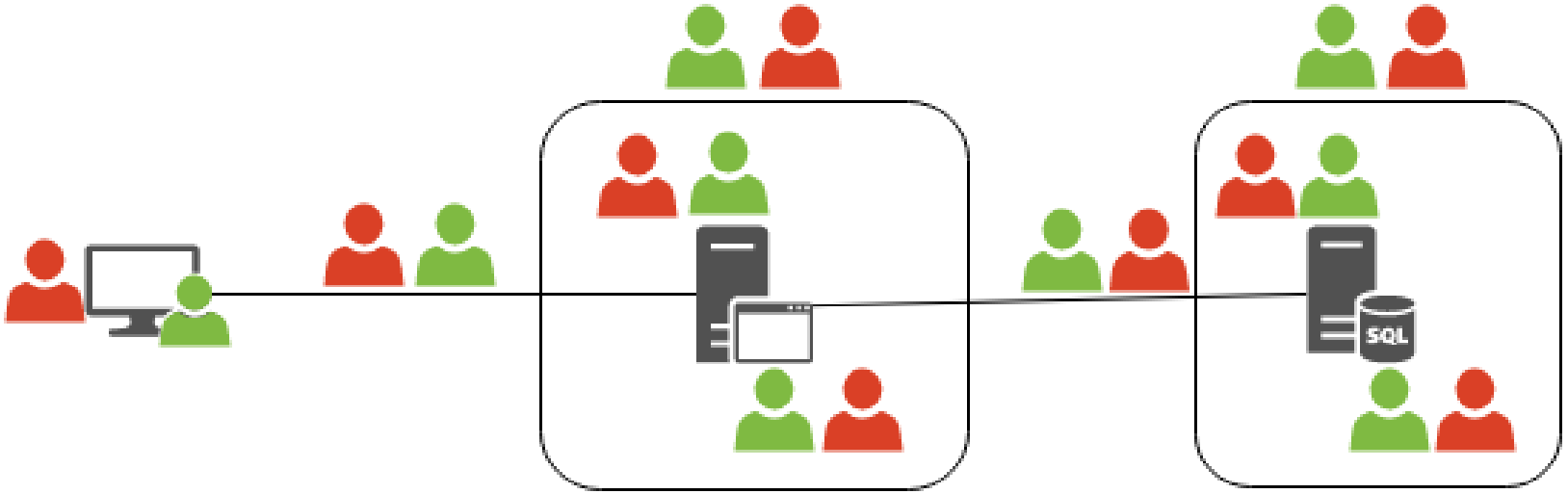
THE DEVELOPER'S CONFERENCE

- **Signal Protocol Technical Information**
- **OpenPGP.js**

Vantagens	Desvantagens
Somente o usuário final tem acesso ao dado aberto	Impossibilita operações do lado servidor

Mecanismos – Criptografia de Ponta-a-Ponta

THE DEVELOPER'S CONFERENCE



Mecanismos – Privacidade Diferencial (menção honrosa)

THE DEVELOPER'S CONFERENCE

- ***"(...) an algorithm is said to be differentially private if by looking at the output, one cannot tell whether any individual's data was included in the original dataset or not."*** - Differential Privacy. Harvard University Privacy Tools Project.

Vantagens	Desvantagens
Identidade do usuário preservada	Os dados ainda existem e são acessíveis pelo administrador, ainda que "sujos"
	Difícil aplicar
	Degradação da privacidade

Conclusão

- Cada técnica/mecanismo tem vantagens e desvantagens
- Necessário realizar a modelagem de ameaças (threat model) e avaliar os riscos e custos envolvidos
- Necessário avaliar quais operações a aplicação deve realizar sobre os dados, e quais serão realizadas no lado servidor ou no lado cliente
- Não há bala-de-prata: cada aplicação é diferente, e cada usuário é diferente

Agradecimentos

THE DEVELOPER'S CONFERENCE

- Mateus Schmitz
- Morvana Bonin
- Rodrigo Hahn
- Rodrigo Paris

Obrigado!

THE DEVELOPER'S CONFERENCE

jeronimo@jeronimofagund.es