

# Autenticação baseada em 2 fatores

Nelson Murilo

# Agenda

- Motivação
- Tipos de 2FA
- Ataques
- Soluções

# Motivação

- Vários bancos e sites estão usando autenticação com 2 fatores
- Vários usuários continuam tendo suas credenciais capturadas
- Por que?

# Fatores

- O que se sabe
- O que se tem
- O que se é

# Tipos

- OTP   
- Internet + SMS (Reverso)
- Ligação Reversa
- Biometria

# OTP



Gmail

<https://accounts.google.com/ServiceLogin?service=mail&continue=https://mail.google.com/mail/>

Google

One account. All of Google.

Sign in to continue to Gmail

Nelson Murilo  
nmurilo@gmail.com

.....

Sign In

Need help?

Sign in with a different account

One Google Account for everything Google



idgnow.com.br/internet/2015/04/21/adeus-senhas-paypal-quer-que-usuarios-tomem-comprimidos-de-acesso/

# Internet

# Adeus, senhas: PayPal quer que usuários tomem "comprimidos de acesso"

PC World / EUA 21 de abril de 2015 - 14h10

---

Segundo empresa de pagamentos, métodos externos como impressões digitais e escaneamento de íris são "antiquados".

---



70 Tweet

34 Share

45 Share

5 Share

g+1

Imprima

Mais +

Microsoft Azure



Falamos Hadoop

Java, Hive, Pig, LINQ, .NET

No Azure, o Hadoop fala

Teste grátis →

ÚLTIMAS NOTÍCIAS



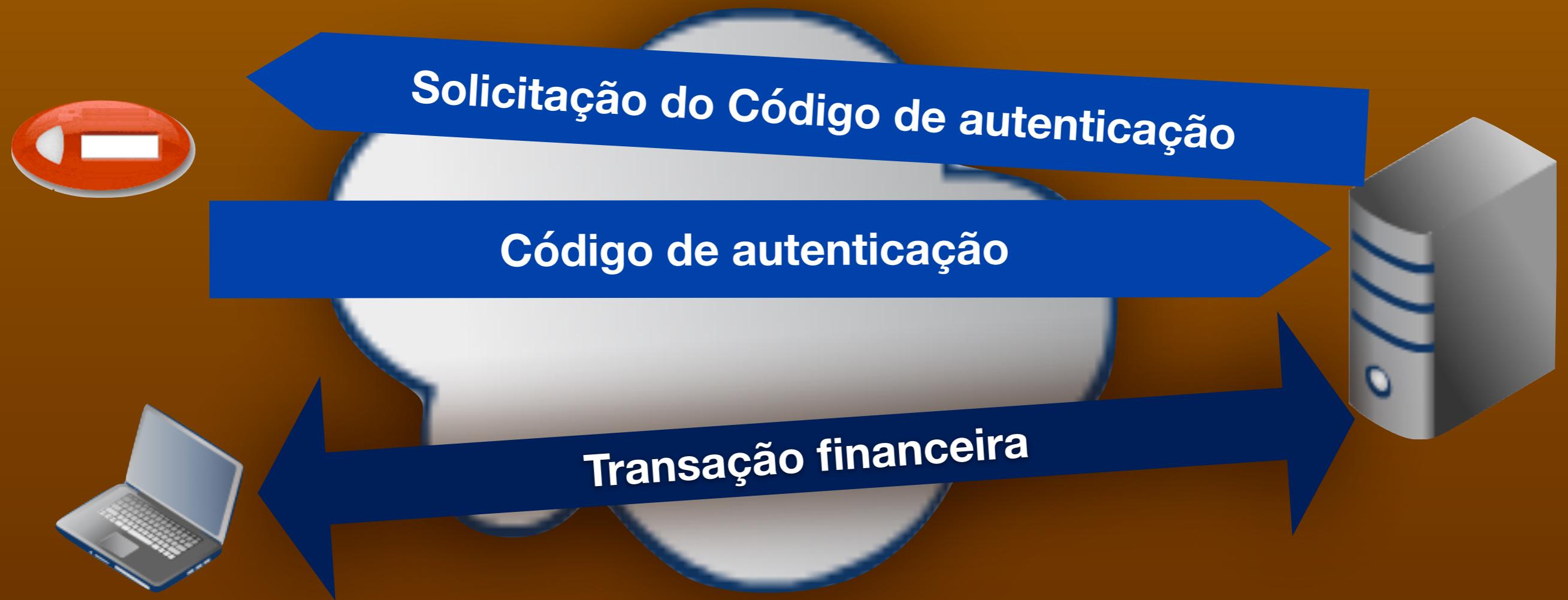
Justiça arquiva e libera uso de

Revogada liminar que proíbe Uber

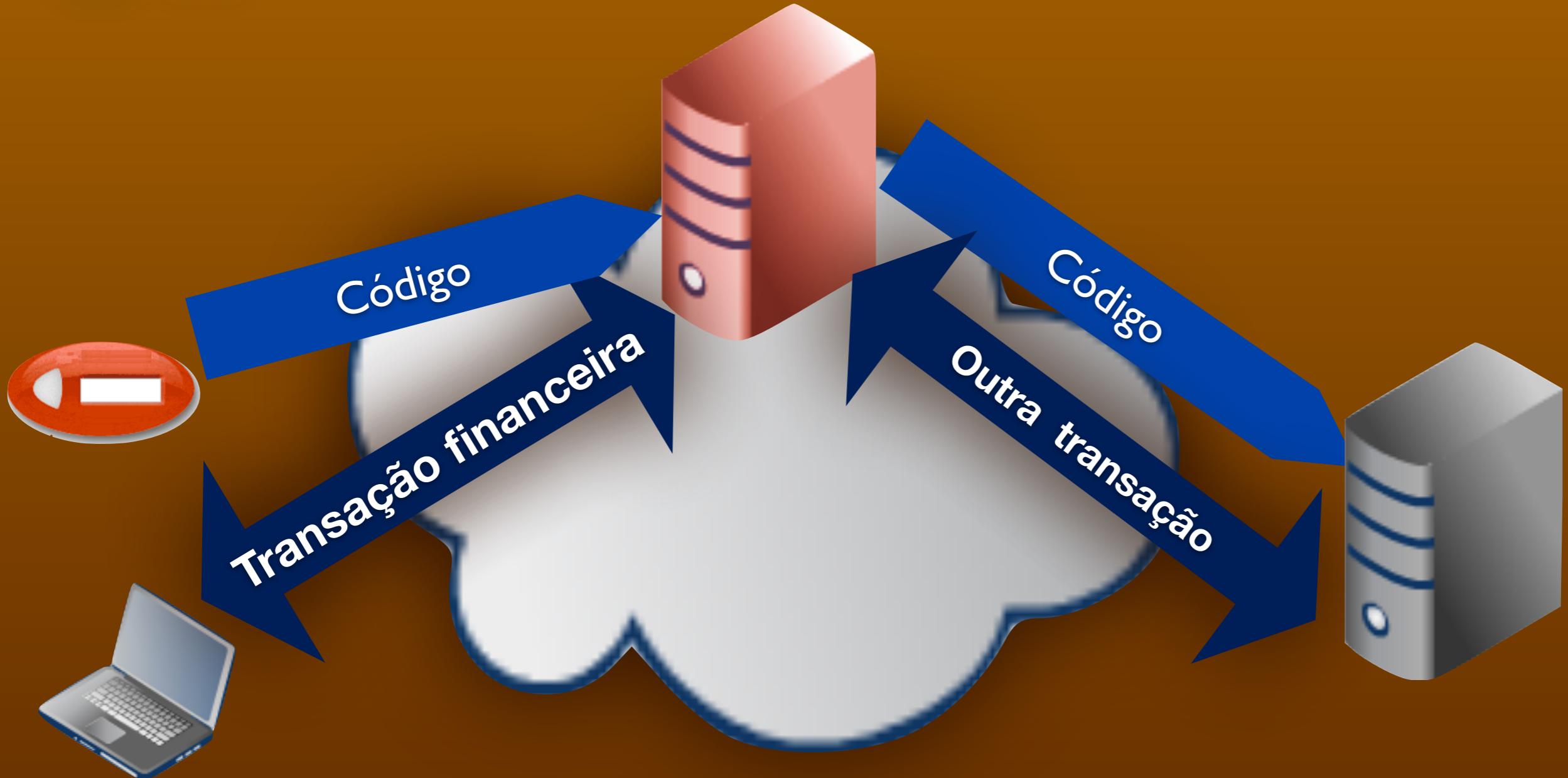


Pesquisa do Li

# OTP

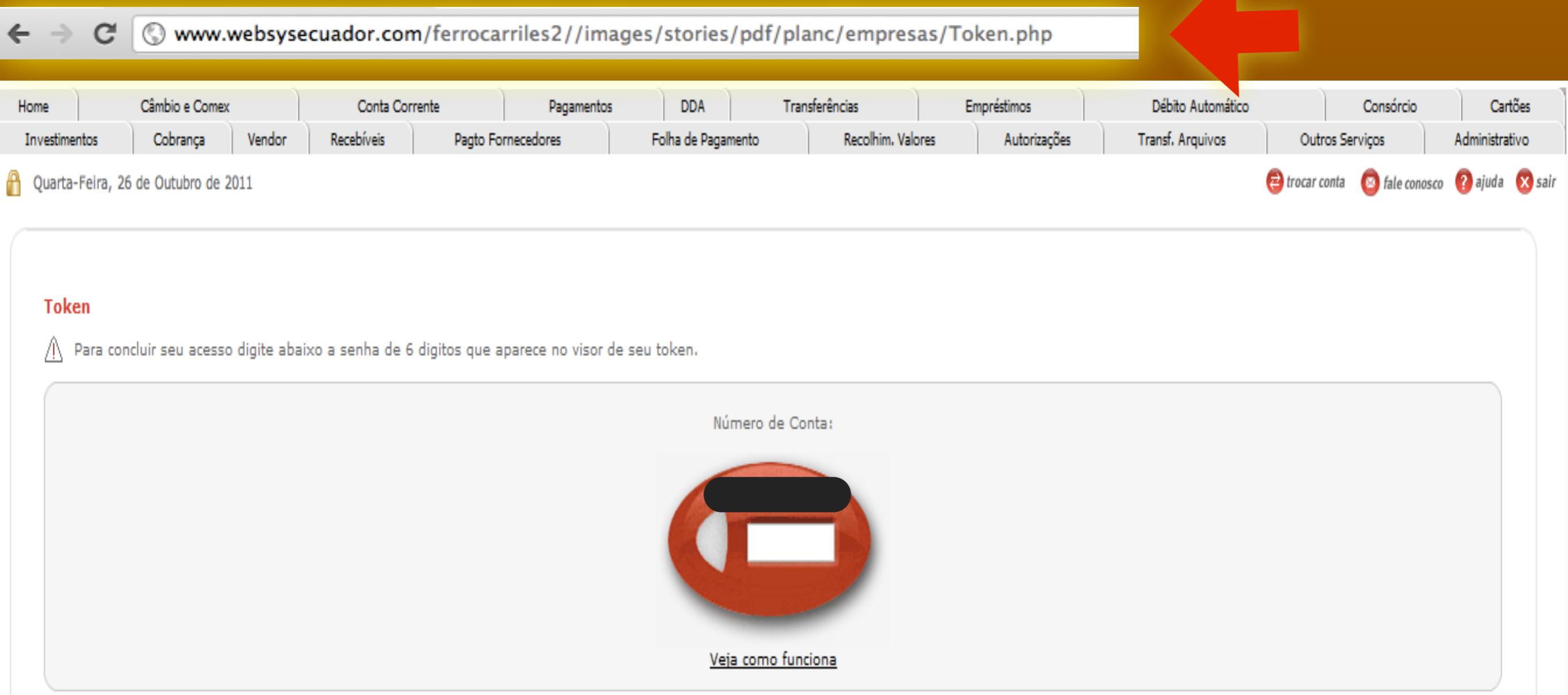


# OTP



Man in the middle attack

# Internet + Hard Token



www.websysecuador.com/ferrocarriles2//images/stories/pdf/planc/empresas/Token.php

Home Câmbio e Comex Conta Corrente Pagamentos DDA Transferências Empréstimos Débito Automático Consórcio Cartões

Investimentos Cobrança Vendor Recebíveis Pagto Fornecedores Folha de Pagamento Recolhim. Valores Autorizações Transf. Arquivos Outros Serviços Administrativo

Quarta-Feira, 26 de Outubro de 2011

[trocar conta](#) [fale conosco](#) [ajuda](#) [sair](#)

**Token**

Para concluir seu acesso digite abaixo a senha de 6 dígitos que aparece no visor de seu token.

Número de Conta:



[Veja como funciona](#)

Em caso de dúvida entre em contato com a Superlinha - Atendimento Empresarial  
Capitais e Regiões Metropolitanas: 4004-2525 | Domínio localizado: 0800-702-2525

Man in the middle attack

## Invoeren rekening- en pasnummer

Neem het rekeningnummer en pasnummer over van uw pas.

rekeningnummer

pasnummer

Telefoonnummer

Onthoud mijn rekeningnummer en pasnummer.



## op uw e.dentifier2

- Controleer of uw pas is ingevoerd
- Druk op **1** Inloggen
- Toets uw pincode in
- Druk op **OK**
- Een response wordt getoond



## Invoeren response

Vul de response in

Klik op OK onder in het scherm.

OK

# OTP

Man in the middle attack



Manual ou Robô



Janela de ataque ~2 minutos



Troca da transação legítima pela  
do fraudador

# OTP

- Desvinculado da transação
- Man in the middle
- Man in the browser

# Internet + SMS (reverso)

## Uso:

- Identificação de computador
- Autenticação
- Confirmação de transação

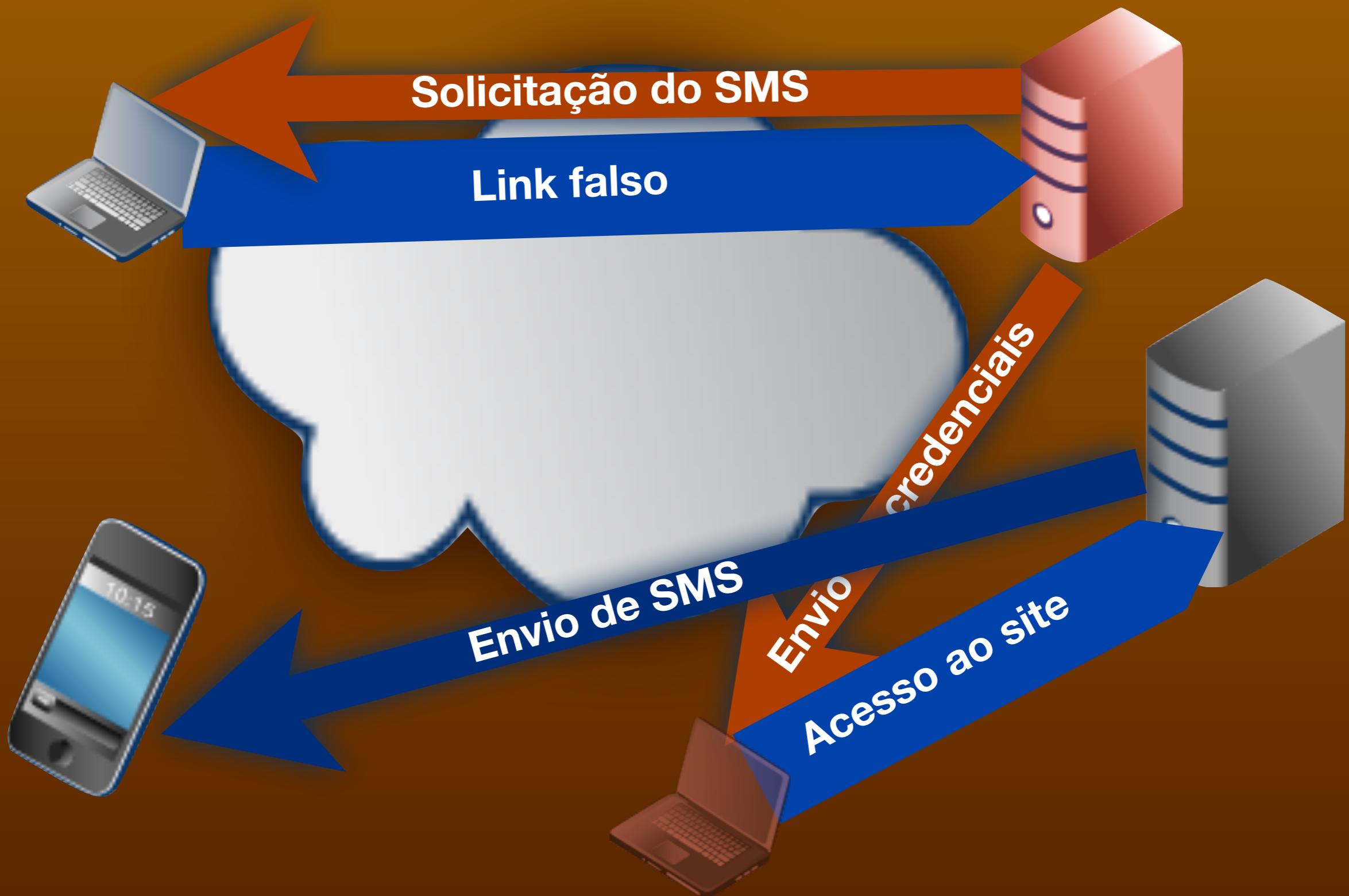
# Internet + SMS

- Man in the Middle
- Man in the Browser
- Man in the Mobile

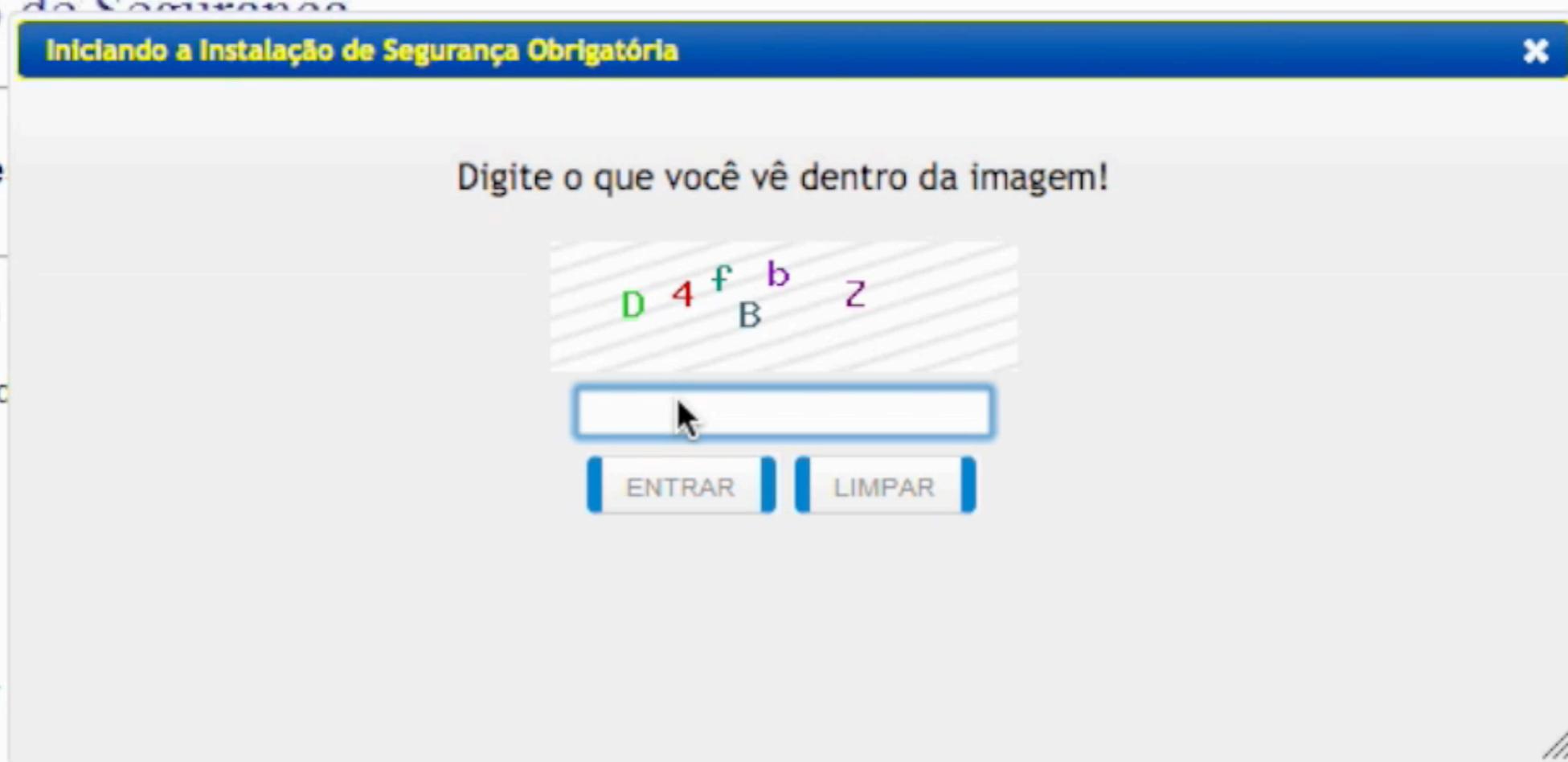
# Internet + Celular



# Internet + Celular

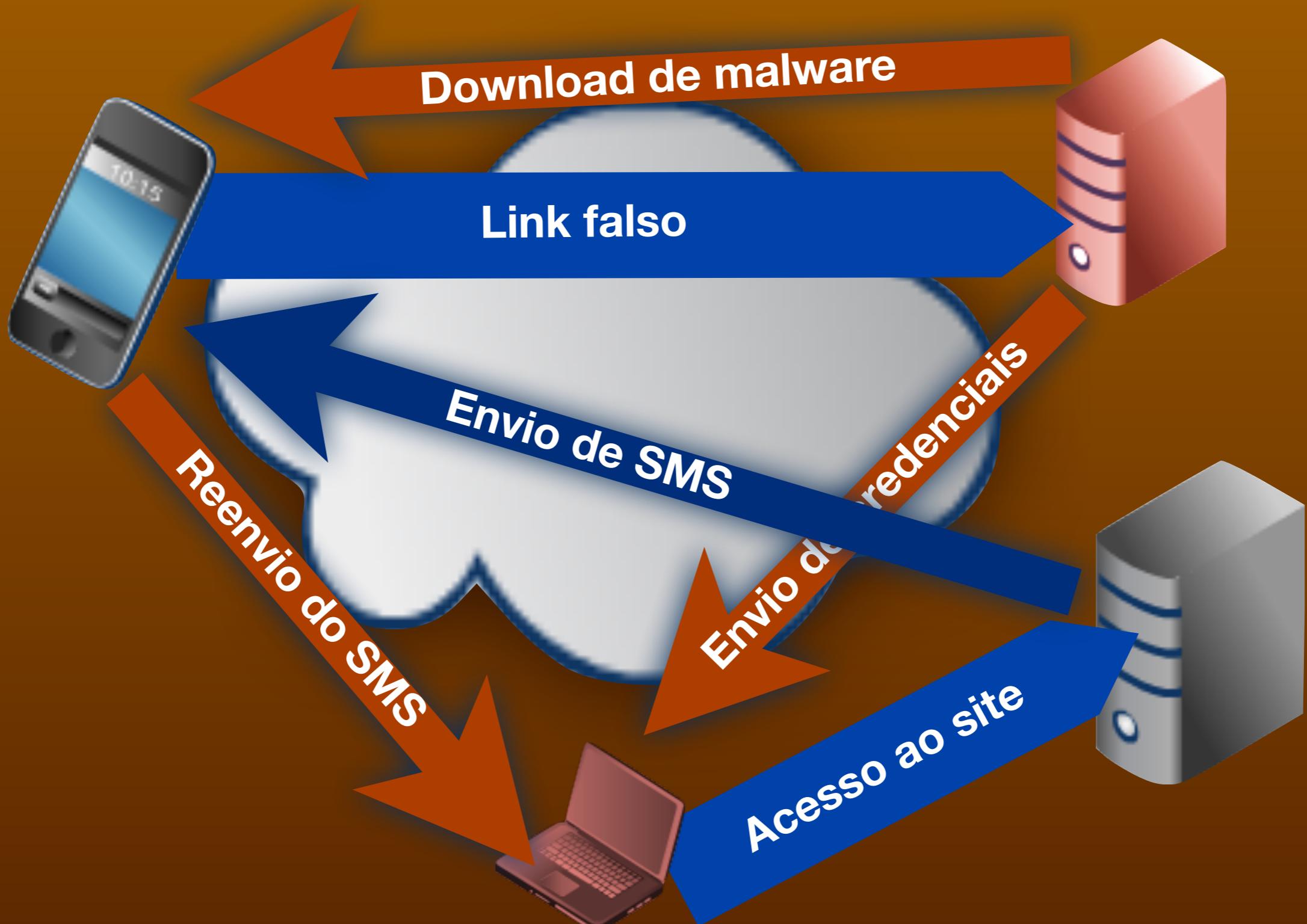


# Internet + Celular



overno): 3003-0500 (capitais e regiões que dispõem do serviço 3003), 0800-729-0500 (demais localidades)

# Internet + Celular



# Internet + Celular

Man in the middle attack



On-line ou Robô



Janela de ataque ~1 dia



Acesso com as credenciais  
do usuário

# OTP

# Google

## 2-Step Verification

You normally use a Security Key, but must use a verification code for this sign-in.



Enter the verification code generated by your mobile application.

Verify

Don't ask for codes again on this computer

Problems with your code? >

# OTP

## 2-Step Verification

Verification codes

App-specific  
passwords

**Registered  
computers**

Security Keys

**2-Step Verification is: ON**

Protecting your account since Jul

THIS COMPUTER



This computer is not registered

When you sign in to your Google Account on this computer, you need to provide a verification code in addition to your password. You can change this during sign-in where you can tell us not to ask for a code again on this computer. We'll still ask for codes on other computers.

[Register this computer](#)

[Turn off](#)

# Internet + Celular

Man in the middle attack



On-line ou Robô



Janela de ataque ~1 dia



Acesso com as credenciais  
do usuário

# Internet + Celular

## Ataque 3



**Usuário acessa site falso e informa suas credencias**



**Em seguida o site falso informa que ele deve “sincronizar” o celular e instala malware**



**Atacante agora controla PC e celular**

# Internet + Ligação p/ usuário

## Microfone



Transação financeira

Ligaçao para o cliente

# Ligação Reversa

- Gravador (captura de credenciais)
- Redirecionamento de chamada

# Man in the Browser

Credenciais

Transação A

Transação B



Credenciais

Transação A

Método de  
autenticação

Transação B



# Redirecionamento de chamada

PROBLEMAS COM O TERMINAL  
LIGUE SOMENTE PARA  
O SAC

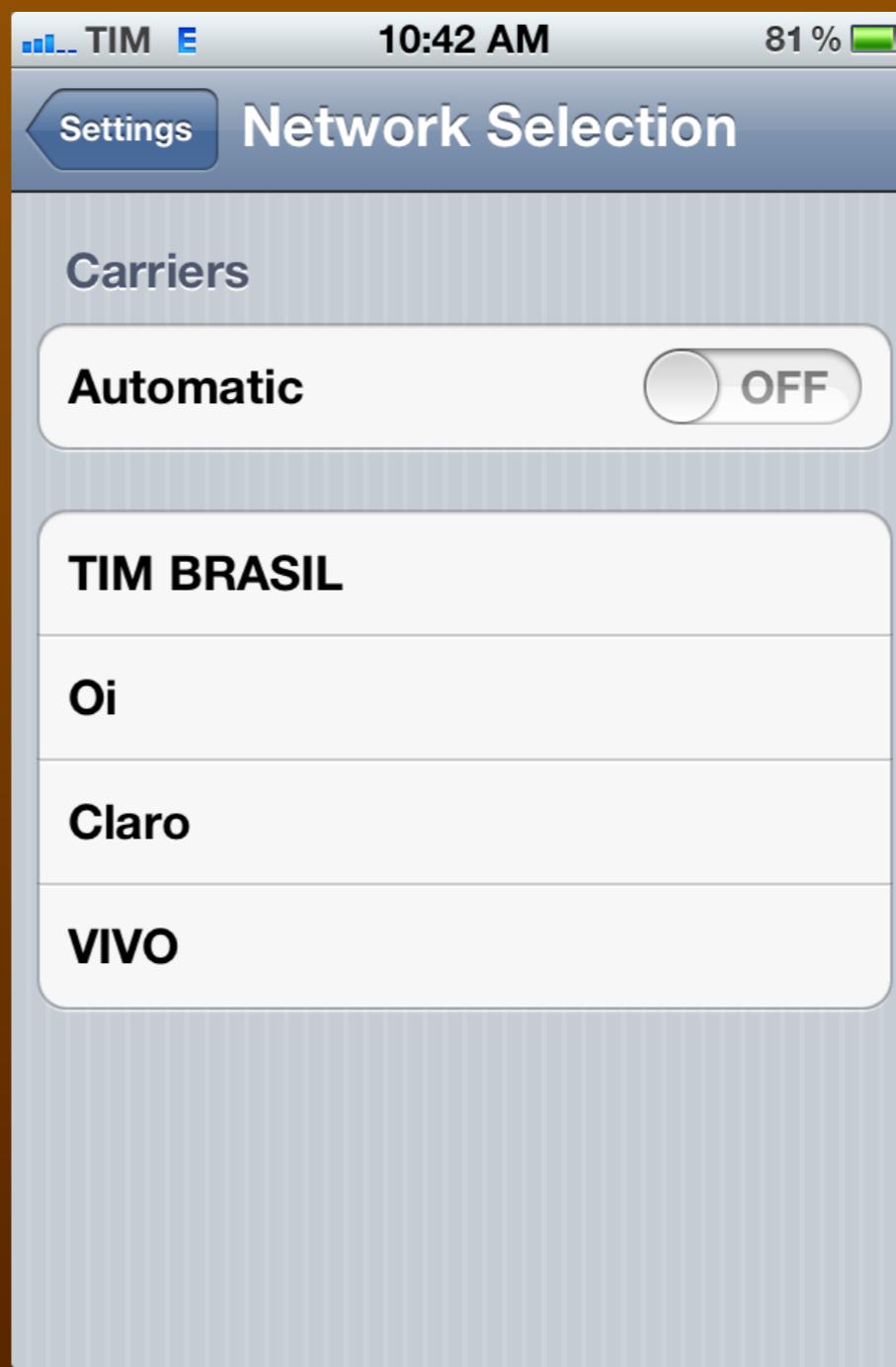
**SAC**

**0800 8922 100**

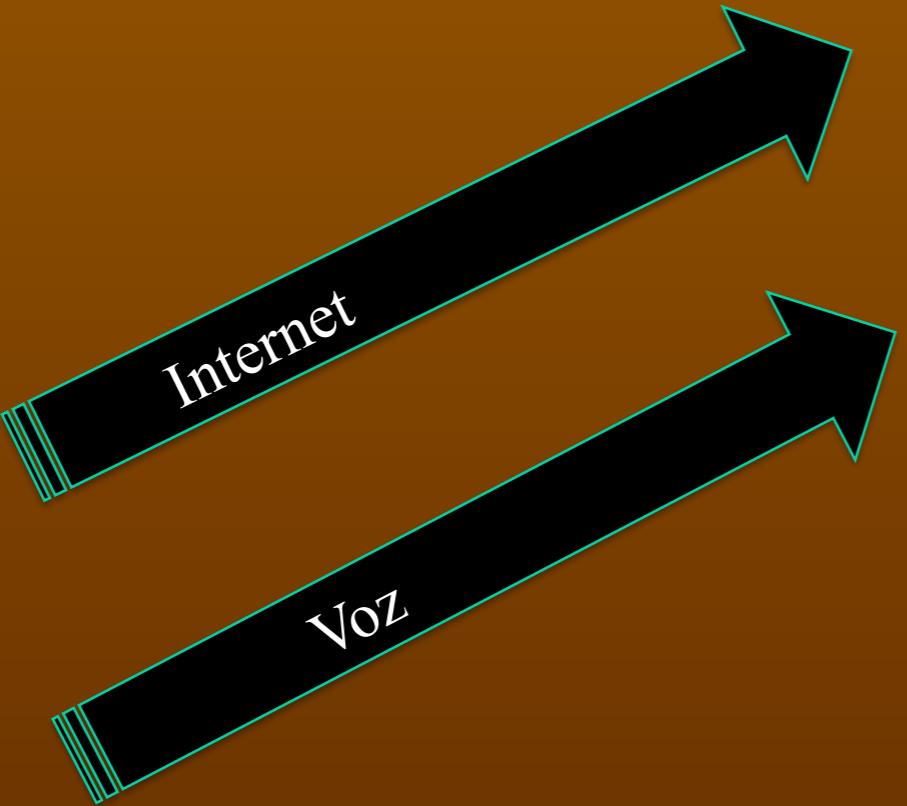
OU

**4003 5619**

# Redirecionamento de chamada



# Redirecionamento de chamada



# Redirecionamento de chamada

**Range Networks**

Welcome to OpenBTS

This Trac is the home of the OpenBTS project. To edit this wiki, you can login as user `rangepublic` with a personal account from Kurtis (log in to the Trac as `rangepublic`). This Trac is licensed under the terms of the [BY-SA 3.0](#).

Quick Links:

- [OpenBTS developer community](#)

What is OpenBTS?

OpenBTS is a Unix application that uses a software radio interface to connect to a cellular network. It might even say that OpenBTS is a simplified form of [IMS](#) (IP Multimedia Subsystem). VoIP backhaul forms the basis of a new type of cellular network that can be used for things like including rural cellular deployments and private cellular networks in remote areas.

**OpenBTS Release**

**Asterisk**™

• Power Supply

wush.net/trac/rangepublic

rangepublic

Reader

Search

Home » Product Categories » USRP Network Range Networks

rangepublic

Search

Login Preferences Help/Guide About Trac

Roadmap Browse Source View Tickets Start Page Index History Last Change

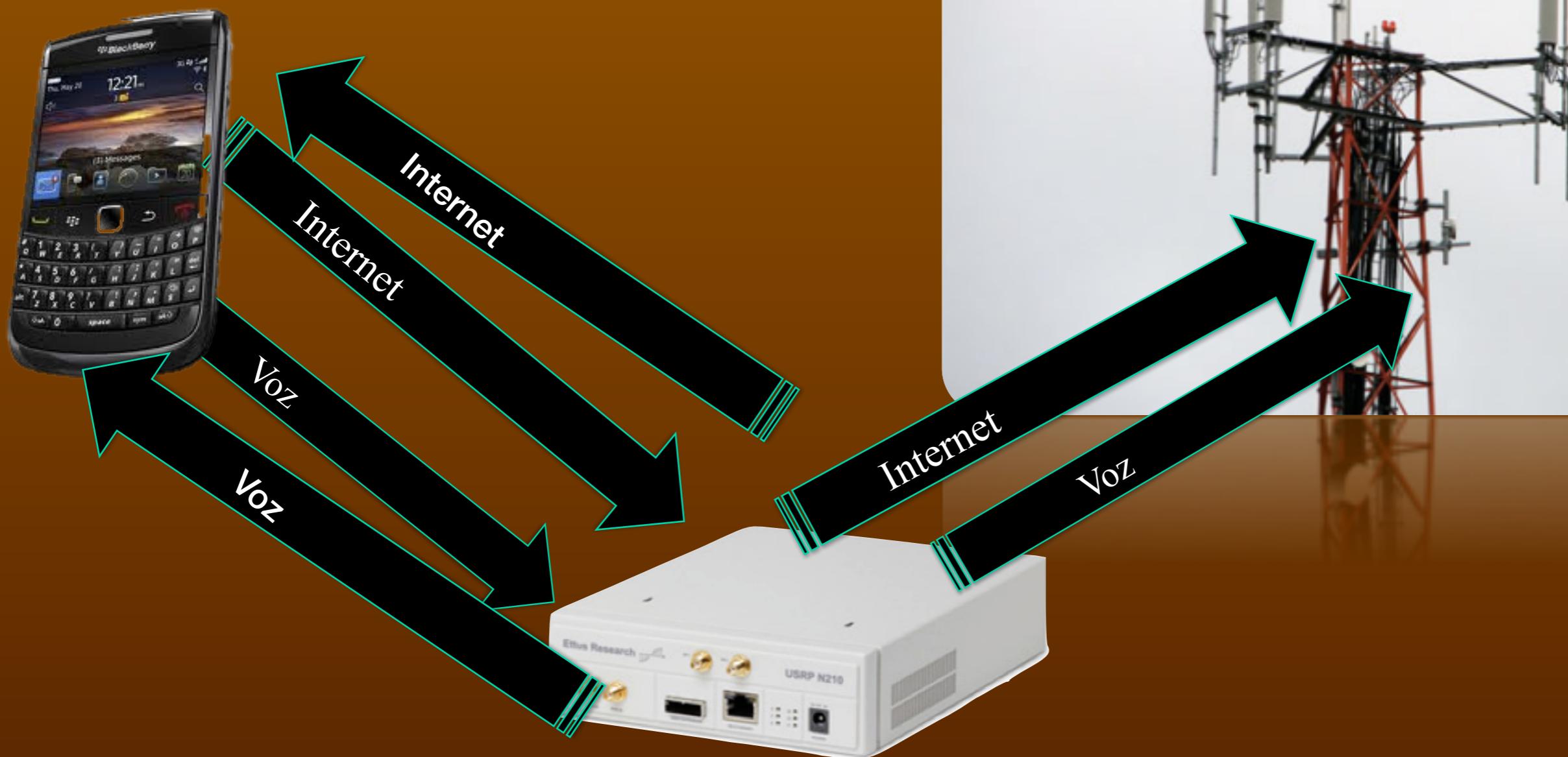
Contents

- [What is OpenBTS?](#)
- [How do I get started?](#)
- [Where can I get the latest code?](#)
- [How do I build and install and run the code?](#)
- [Where documentation?](#)
- [How do I get support?](#)
- [Who else is using OpenBTS?](#)
- [Decoding UMTS](#)
- [SMQ2](#)

# Redirecionamento de chamada



# Redirecionamento de chamada



# Redirecionamento de chamada

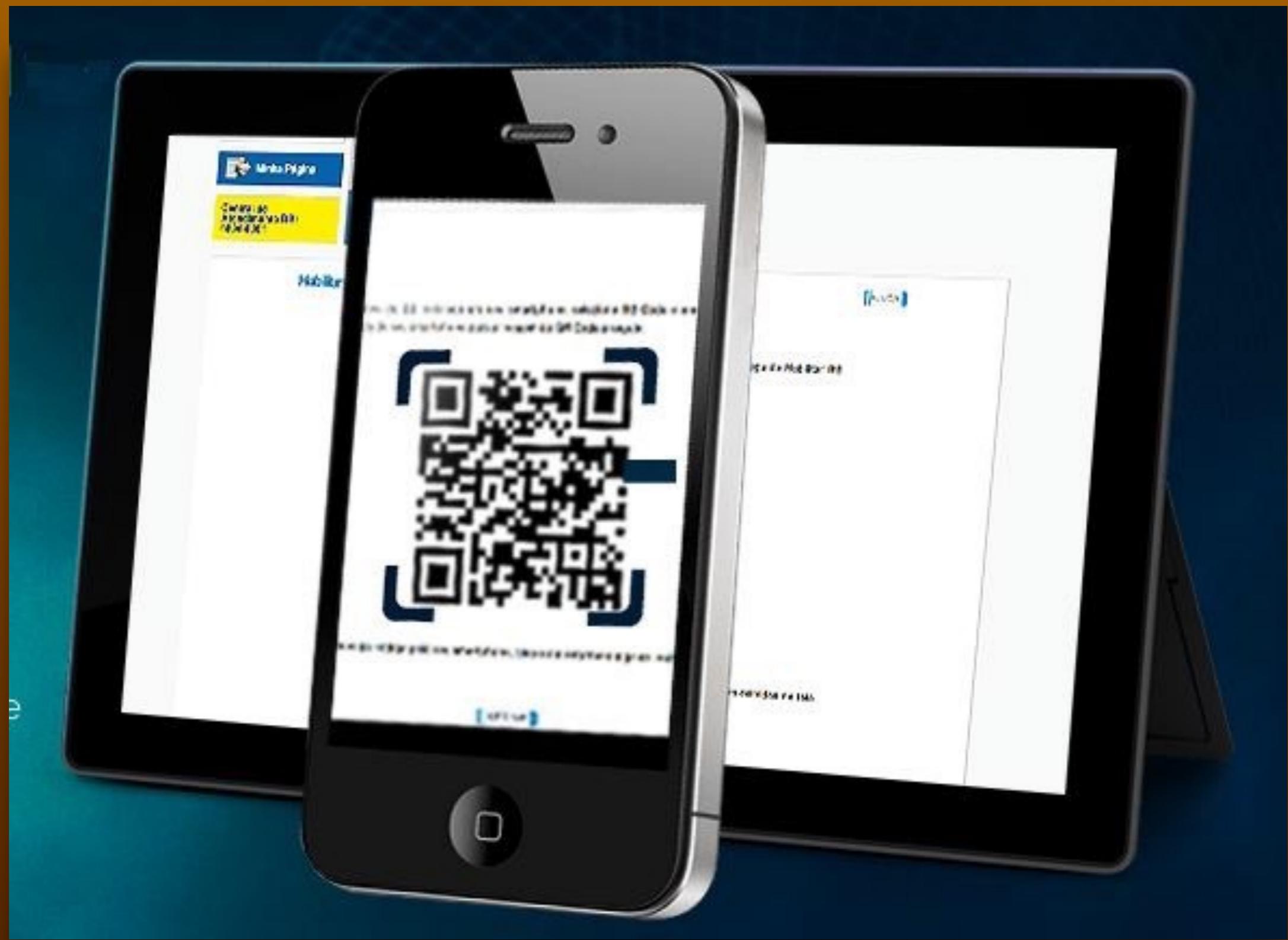


# Redirecionamento de chamada



# Redirecionamento de chamada







Operadora

Posicione o  
em destaque  
da câm Autorizar Recadastrar Voltar

Voltar

TRANSFERENCIA  
CORRENTE P/ CDATA DA TRANS  
HORA DA TRANS

VALOR TOTAL: 1

\*\*\*\*\* TRANSFER

CLIENTE: PEDRO

AGENCIA: 7988-&gt;

170.159-2

 Cancelar

Código Autorizador

008062

 Confirmar Confirmar

# Autenticação baseada em 2 fatores

Nelson Murilo