



Universidade Federal do Rio de Janeiro
Instituto de Matemática
Departamento de Ciência da Computação
Grupo de Resposta a Incidentes de Segurança

Rio de Janeiro, RJ - Brasil

Segurança em Códigos QR

GRIS-2012-A-001

Rafael Oliveira dos Santos
rafaelsantos@gris.dcc.ufrj.br

A versão mais recente deste documento pode ser obtida na página oficial do GRIS: <http://www.gris.dcc.ufrj.br>.

GRIS - Grupo de Resposta a Incidentes de Segurança
Av. Brigadeiro Trompowski, s/nº
CCMN – Bloco F1 - Decania
Cidade Universitária - Rio de Janeiro/RJ
CEP: 21949-900
Telefone: +55 (21) 2598-9491

Este documento é Copyright©2012 GRIS. Ele pode ser livremente copiado desde que sejam respeitadas as seguintes condições:

É permitido fazer e distribuir cópias inalteradas deste documento, completo ou em partes, contanto que esta nota de copyright e distribuição seja mantida em todas as cópias, e que a distribuição não tenha fins comerciais. Se este documento for distribuído apenas em parte, instruções de como obtê-lo por completo devem ser incluídas. É vedada a distribuição de versões modificadas deste documento, bem como a comercialização de cópias, sem a permissão expressa do GRIS.

Embora todos os cuidados tenham sido tomados na preparação deste documento, o GRIS não garante a correção absoluta das informações nele contidas, nem se responsabiliza por eventuais consequências que possam advir do seu uso.

Última atualização em: 8 de setembro de 2012

Sumário

1	Introdução	2
2	Desenvolvimento	3
2.1	Códigos QR?	3
2.1.1	Como criar e ler?	3
2.1.2	Código QR vs. Código de Barras	3
2.1.3	Aplicações no dia-a-dia	4
2.2	É seguro escanear Códigos QR?	7
2.2.1	Por que me atacariam?	7
2.2.2	O nosso grande mal	7
2.2.3	Exemplos de possíveis ataques	7
2.2.4	Casos famosos	10
2.2.5	SQRC	10
2.3	Boas práticas	12
2.3.1	Para os que escaneiam	12
2.3.2	Para os que criam os códigos	12
2.4	Curiosidades	12
3	Conclusões	13
3.1	Projetos futuros	13
4	Referências Bibliográficas	14

1 Introdução

Desenvolvido no Japão em 1994 pela DENSO CORPORATION, os Códigos QR (Quick Response) são utilizados para transmitir qualquer tipo de dado através de uma simples captura de imagens em 2D.

Atualmente, os Códigos QR estão ganhando uma popularidade muito grande pela sua praticidade e devido ao mercado de dispositivos móveis, aparelhos capazes de lerem os códigos, estar crescendo muito!

Contudo, até que ponto é seguro escanear esses códigos? Será que existe um Código QR que possa executar códigos maliciosos? Ou mesmo um que ao ser lido roube todas as minhas informações pessoais?

Este artigo visa responder a todas essas perguntas e a entender minuciosamente os cuidados que devem ser tomados ao ler Códigos QR que facilmente podemos encontrar por ai.



2 Desenvolvimento

2.1 Códigos QR?

Em 1994, a DENSO CORPORATION, um fabricante internacional de componentes automotivos, decidiu desenvolver uma espécie de simbologia em duas dimensões e com o objetivo principal de "Ser um código de leitura fácil para o leitor".

A partir daí, muitas versões do Código QR foram desenvolvidas até chegarmos hoje na versão de número 40. Segue abaixo detalhes um pouco mais aprofundados sobre eles:

2.1.1 Como criar e ler?

Podemos definir os Códigos QR como representações em duas dimensões de dados. Para criar os códigos é necessário a utilização de um *QR Code Generator*, ou Gerador de Código QR em português, que é facilmente encontrado na Internet. Um exemplo seria o <http://qrcode.kaywa.com/>.

Algumas funcionalidades desses dados representados podem ser divididos em **URLs**, que leva à endereços da Internet, **Textos**, que mostram algum tipo de informação em texto puro, **Número de telefones**, que armazena algum número de telefone, ou mesmo **SMS**, que automaticamente envia uma mensagem de texto para um celular específico.

Com um código já criado, para que a leitura seja feita você precisa de um dispositivo onde seja possível a instalação de um **Leitor de Código QR**. É importante estar sempre atento aos leitores para mantê-los sempre atualizados! Um exemplo de leitor grátiás pode ser encontrado em <http://barcode-scanner.softonic.com.br/android>.

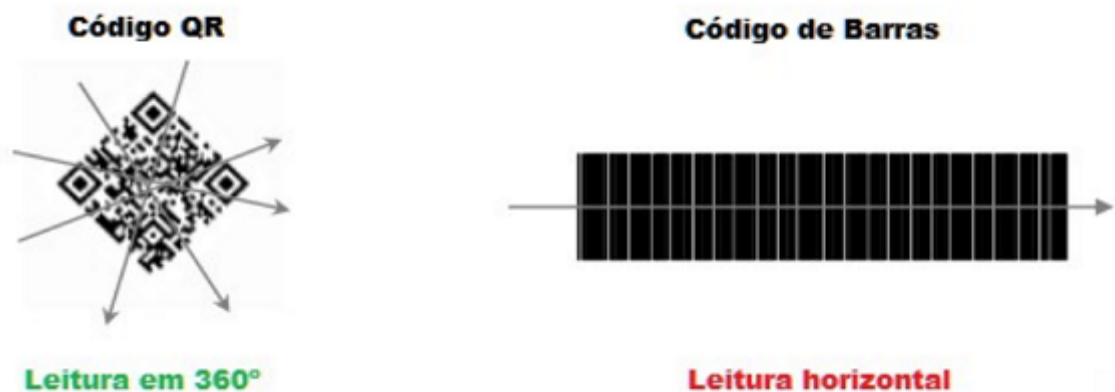
2.1.2 Código QR vs. Código de Barras

Ao conhecer um pouco o Código QR você deve se perguntar: "E os Códigos de Barras já não fazem isso?". Os Códigos de Barras são de grande utilidade para a humanidade atualmente, porém, com a criação dos Códigos QR, muitas outras funcionalidades foram inseridas:

a) Posição onde são armazenados os dados



b) Leitura em alta velocidade



c) Durabilidade contra manchas e danos



d) Representação Kanji



2.1.3 Aplicações no dia-a-dia

Apesar de ser uma tecnologia não muito nova, atualmente, principalmente pelo fato do "boom" dos dispositivos móveis, no Japão e na Coréia do Sul é realidade a utilização de Códigos QR no dia-a-dia. Lá já é até possível fazer compras de supermercado na estação de metrô! Nos EUA, as coisas estão avançando de uma forma estrondosa. É muito comum andar pela *5th Avenue* em Nova York e se deparar com um anúncio gigantesco com um Código QR, por exemplo. Aqui no Brasil não estamos tão distante disso. Muitas ações de marketing ou próprios bancos já estão utilizando os códigos também.

Abaixo seguem apenas algumas figuras para ilustrar as aplicações no dia-a-dia:

a) Fazer compras

<http://www.youtube.com/watch?v=3Mqcb7RoN4Y>



b) Publicidade

<http://www.youtube.com/watch?v=SVjWBfVSbY4>



c) Armazenando dados de pacientes

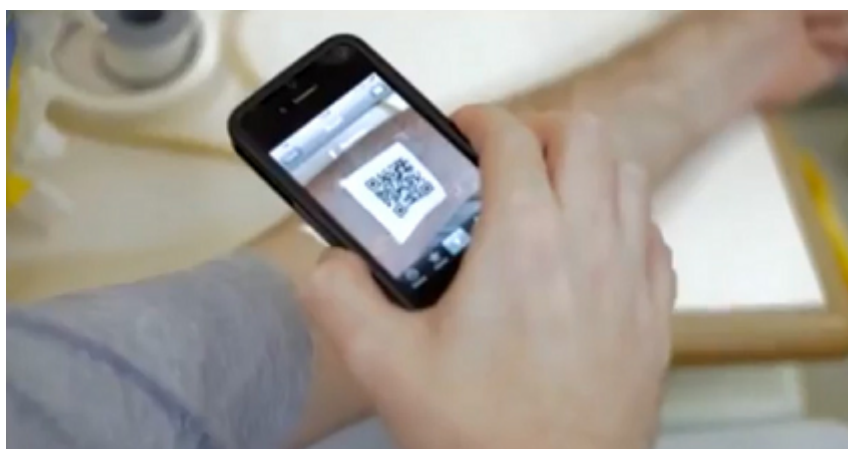


d) Pagamento de contas



e) Durante a doação de sangue

http://www.youtube.com/watch?v=rr8R-vr-Yqg&feature=player_embedded



f) Utilizando softwares de relacionamento

http://www.youtube.com/watch?v=8Y0St_Igp6M



2.2 É seguro escanear Códigos QR?

Depois de todas as novidades e coisas interessantes que podemos utilizar com os Códigos QR fica uma pergunta no ar: É seguro escanear esses Códigos? Será que alguém pode criar um código malicioso que consiga roubar meus dados? Será que algum deles pode instalar um aplicativo sem minha autorização em meu dispositivo?

2.2.1 Por que me atacariam?

O grande incentivo para *crackers* praticarem suas atividades maliciosas utilizando os Códigos QR é que os dispositivos móveis armazenam grande quantidade de informações pessoais. É uma verdadeira mina de ouro! Números telefônicos, conversas via aplicativos de comunicação, transações bancárias, e muito mais!

2.2.2 O nosso grande mal

Infelizmente o que alavanca a possibilidade de ataques bem sucedidos é o grande mal do ser humano: a curiosidade! As pessoas simplesmente não conseguem resistir a curiosidade de descobrir para onde um Código QR vai. Elas simplesmente escaneiam e a sorte está lançada!

É essencial que você se controle e evite esse tipo de falha. Caso suspeite de um código onde a oferta é boa demais, por exemplo, não se arrisque! Mais a frente será mostrado algumas dicas importantes sobre Boas Práticas ao escanear Códigos QR.

2.2.3 Exemplos de possíveis ataques

Seguem alguns exemplos de ataques utilizando Códigos QR:

a) *QRJacking*

Esse ataque funciona trocando um Código QR legítimo por um *sticker* com um outro malicioso. Um ataque muito simples mas que pode trazer consequências catastróficas.

Um exemplo ilustrado a seguir é de um ataque *QRJacking* em uma revista. O atacante cria um Código QR malicioso e imprime vários tamanhos até encontrar o exato ao do legítimo. Logo em seguida ele cola por cima do original e o deixa para que pessoas escaneiem em uma clínica de dentista por exemplo.



Podemos encontrar outros exemplos de *QRJacking*, sofisticados ou não, abaixo também:



b) *ScanJacking*

c) *Phishing*

É possível realizar também ataques de Engenharia Social, como o *Phishing* utilizando Códigos QR. Juntamente com um ataque de *ScanJacking*, um atacante pode criar um código malicioso que leve a vítima à um *site* muito parecido com o legítimo.



Fique atento à site falsos! Esta imagem mostra um exemplo de Phishing do Paypal.

Imagine a seguinte situação: Uma empresa X decide criar um anúncio publicitário em uma revista de grande circulação na cidade. Porém, uma pessoa com intenções maliciosas cria um falso Código QR que leva à um *site* também falso muito parecido com o da empresa X. Lá, a vítima fornece todas as suas informações pessoais, senhas, etc. achando que está realizando um compra online, por exemplo, mas na verdade está sofrendo um ataque de *Phishing* muito poderoso!

d) Fraude de SMS

Você já deve ter ouvido em propagandas por aí algo do tipo: "Quer receber notícias sobre seu time preferido? Mande um SMS para o número Y com a palavra TIME.". A empresa fornece as notícias esportivas para quem interessar assinar seu feedback e o usuário paga por isso, diariamente, semanalmente, etc. Esse tipo de serviço pode ser muito interessante para algumas pessoas, porém, o que aconteceria se o usuário pagasse por um serviço e não o recebesse? Ou pior, se pagasse por um serviço que ele nem sabe que está pagando?


É assim que o ataque da Fraude de SMS funciona. Utilizando uma funcionabilidade dos Códigos QR, que é a de enviar SMS para números telefônicos, atacantes podem criar códigos maliciosos que fazem pessoas assinarem ou pagarem por algo que não receberão. Alguns leitores de Códigos QR avisam e mostram a mensagem de texto e o telefone a ser enviada a mensagem, contudo outros fazem esse processo automaticamente.

NOTÍCIAS SBT
 Não fique sem saber o que ocorre no Brasil e no mundo! Envie um SMS com a palavra "NOTICIA" para "44644" Assinatura: R\$0,31 + imp/sms Operadoras participantes: Vivo, CTBC, Oi, TIM, Claro



QR-Code da promoção

Promoção - Quem Sabe Ganha Mais
 Conheça o novo concurso de Perguntas e respostas! A cada resposta certa você ganha 2X chances de levar 10 mil reais! Envie MAIS para 44944 e Participe!



QR-Code da promoção

AVISO: NAO ENVIAMOS MENSAGENS SMS PARA INFORMAR GANHADORES
 Para cancelar o serviço envie a palavra SAIR para 44944
 Custo: R\$1,99 operadora Oi, R\$1,99 + impostos/mag demais operadoras

Portal de Voz do Ratinho
 Participe do Programa do Ratinho, ligue para 015 11 97424-0004 e dê sua opinião. "Custo de uma ligação para celular de São Paulo".

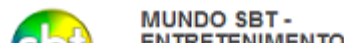
Serviço disponível para todas as operadoras de telefonia móvel e fixa.

Promoção – Tenha Estilo
 Envie MODA para 57550 e Participe!

AVISO: NAO ENVIAMOS MENSAGENS SMS PARA INFORMAR GANHADORES
 Para cancelar o serviço envie a palavra SAIR para 57550
 Custo: R\$1,99+imp por semana para operadoras Claro, Vivo e Tim e R\$1,99 por semana para operadora Oi
 Quiz: R\$0,31+imp/mensagem para operadoras Claro Vivo, Tim e Oi.



QR-Code da promoção



Exemplo de usos de SMS com QR Codes.

Imagine uma situação onde alguém cria uma Código QR fraudulento e divulga no corredor do escritório onde trabalha. Além disso, coloca um anúncio ao lado do código dizendo: "Escaneie e concorra a um Iphone!". Se a cada mensagem recebida o sistema do atacante consegue ganhar R\$1,00 e 20 pessoas escaneiam por dia, o salário extra está garantido!

e) Conectando-se em redes inseguras

2.2.4 Casos famosos

Recentemente ocorreram 2 ataques que ficaram famosos por utilizar um Código QR como ferramenta de ataque. Abaixo segue uma análise feita de cada um.

- a) th3j35t3r
- b) JimRussia

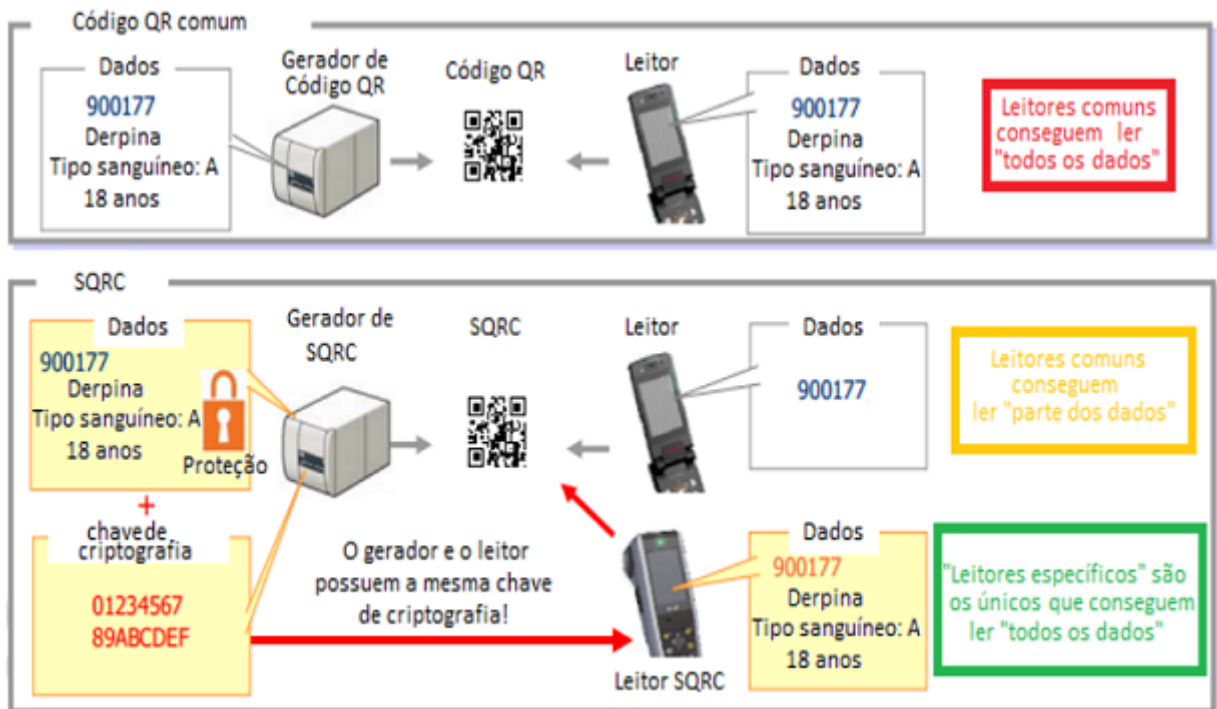
2.2.5 SQRC



Como uma forma de tentar proteger e amenizar o vazamento de informações pessoais através de Códigos QR, foi desenvolvido o SQRC - *Security Quick Response Code*. A sua utilização funciona da seguinte forma: Um gerador do código deve ser um especial, o Gerador de SQRC, onde o código é gerado utilizando uma criptografia que somente um determinado Leitor de SQRC é capaz de

decifrar. Mesmo que uma pessoa consiga escanear o Código QR em um leitor comum de celular, por exemplo, ela só conseguirá pegar parte dos dados por não utilizar o Leitor de SQRC.

Abaixo segue um diagrama para exemplificar melhor sua utilização:



2.3 Boas práticas

Após conhecer algumas ameaças fique sempre atento a partir de agora ao utilizar Códigos QR. Evite também criar uma preocupação extrema com eles pois podemos tirar grandes proveitos ao utilizá-los corretamente. Para tal, segue algumas boas práticas para utilizar no dia-a-dia:

2.3.1 Para os que escaneiam

2.3.2 Para os que criam os códigos

2.4 Curiosidades

3 Conclusões

3.1 Projetos futuros

4 Referências Bibliográficas

Referências bibliográficas utilizadas nas pesquisas.

Referências