

A REVISTA Nº 1
DA TECNOLOGIA

INVESTIGAÇÃO
REPORTAGEM
TUTORIAIS
TESTES

JÁ USAMOS OS GOOGLE GLASS!



Testámos os
três serviços
durante um mês

COMPARATIVO
ZON, MEO, VODAFONE
QUAL O MELHOR NOS 25 EUROS?

EXAME INFORMÁTICA

90

APLICAÇÕES PARA
iOS, Android,
Windows Phone

Novembro 2013 N.º 221 • Mensal • An
€3 Portugal Continental • €5,04 Revista + DVD

www.exameinformatica.sapo.pt

APRILS

QUE VÃO MUDAR A SUA VIDA

POUPE DINHEIRO / ALIMENTE-SE MELHOR
SEJA MAIS SAUDÁVEL / TREINE O CÉREBRO
SALVE VIDAS... TUDO ISTO A PARTIR
DO SMARTPHONE E DO TABLET



TESTADOS
NEXUS 7 / XPERIA Z1
SÃO ESTES OS MELHORES
ANDROID DO MOMENTO?



VALE A PENA?
A CYBER-SHOT
QX10 PODE
USAR-SE COM
QUALQUER
ANDROID E ATÉ
COM O IPHONE



LUMIA 1020
O SMARTPHONE
COM A MELHOR
CÂMARA... DE
SEMPRE!



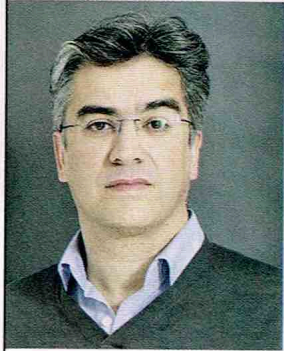
MULTIFUNÇÕES
COMPARATIVO A
8 MÁQUINAS QUE
QUEREM GANHAR
LUGAR NO SEU
ESCRITÓRIO

**Para Marte,
em força!**

Os portugueses
que querem conquistar
o planeta
vermelho



00221
5 603846 017284



Rui Miguel Silva
DIRETOR DO
LABORATÓRIO
UBINET E DA
EMPRESA UBIXPLOIT



ATÉ QUE PONTO A CIFRA RESISTE AO NSA

256 bits. Considerando que os algoritmos assimétricos exigem, no mínimo, o dobro da dimensão da chave para o mesmo nível de segurança dos simétricos, pode dizer-se que existem atualmente algoritmos capazes de resistir a programas de ciberespionagem como o Prism.

No entanto, a segurança das comunicações cifradas não depende apenas da sua robustez criptográfica, que é cientificamente sustentada. Existem condicionantes que podem contornar a fundamentação científica. As implementações de software e hardware dos algoritmos criptográficos podem introduzir vulnerabilidades suficientes para corromper a segurança. Um exemplo: o WEP que utiliza um algoritmo criptográfico simétrico ainda hoje seguro (RC4), mas que devido à sua implementação permitiu a quebra da segurança do sistema. Por outro lado, as más configurações dos sistemas de suporte às comunicações, quer sejam os próprios sistemas operativos quer sejam as aplicações utilizadas podem permitir capturar as comunicações antes de serem cifradas, devido a vulnerabilidades que nada têm a ver com a criptografia.

Se quisermos considerar teorias da conspiração, podemos admitir que a NSA possui um conhecimento superior ao conhecimento público da comunidade científica, ou que possui equipamento com maior capacidade do que é atualmente conhecido. É um domínio propício à divagação, mas considerando a organização do ciberespaço é razoável admitir que NSA e organizações similares de outras nações, com motivações de defesa nacional ou combate ao terrorismo por exemplo, tentem aferir informação no ciberespaço. Podem protocolar formal ou informalmente com companhias operadoras de telecomunicações ou detentoras de sistemas determinantes como a Google ou o Facebook, como veio a público recentemente, mecanismos

que permitam atingir os seus objetivos. A questão fundamental é determinar e proteger o limite dos Direitos, Liberdades e Garantias das Pessoas.

As contra-medidas de ciberespionagem podem fazer-se a três níveis: pela obscuridade; pela utilização de múltiplas cifras; ou pelo aumento da dimensão das chaves utilizadas.

A obscuridade consiste em não divulgar as cifras ou parte dos sistemas de cifra. É uma opção questionável do ponto de vista científico, pois viola o Princípio de Kerckhoff que diz que "Um sistema criptográfico deve ser seguro mesmo que tudo seja conhecido, com exceção da sua chave". Este princípio foi também enunciado por Claude Shannon como "O inimigo conhece o sistema". O uso de múltiplas cifras em sequência é uma alternativa à obscuridade que aumenta a robustez da segurança do sistema. Nesta situação, a quebra do sistema consiste na quebra de mais do que um algoritmo de cifra. Contudo, diminui a eficiência do sistema aumentando os tempos de cifra e de decifra.

A solução híbrida de utilizar uma ou mais cifras conhecidas, como o AES, envolta por uma arquitetura secreta (na obscuridade), aumenta a entropia e a complexidade do sistema e dá margem de segurança se a cifra for quebrada. O aumento da dimensão das chaves é a melhor solução, admitindo que os algoritmos ainda não foram quebrados por agências de ciberespionagem e que estas não possuem tecnologia com capacidades desconhecidas do público. ●

SE OS ATAQUES DE FORÇA BRUTA SEGUIREM A LEI DE MOORE, E DUPLICAREM DE CAPACIDADE A CADA ANO E MEIO, TALVEZ EM 2274 SERIA POSSÍVEL QUEBRAR UMA CIFRA DE 256 BITS