



Autenticação

Escolher um método adequado

Confraria *Security & IT*

Janeiro 2010

Miguel Almeida

Agenda

- ❑ Quem é o gajo ~~da gravata~~ do *Spitfire*?
- ❑ Qual é o objectivo desta conversa?
- ❑ Autenticação? Porquê? Para quê?
- ❑ Ameaças, dizes tu?...
- ❑ Ok, *I'm IN*: mostra lá uns zingarelhos!
- ❑ Mas há montes deles... Como é que escolho?
- ❑ Hã? Gestão do risco?...
- ❑ Percebi! Mas ainda tenho algumas perguntas...
- ❑ 'Tá feito. Passa lá o micro, vá...

Miguel Almeida

- ❑ Um bacano lá do Sado, já com ~~20~~... 38 voltas ao Sol;
- ❑ Estudei Engenharia Informática @ Instituto Superior Técnico, em Lisboa;
- ❑ Entre 2000 e 2007 trabalhei na KPMG e na Deloitte - *Risk Management Services* - e fui responsável pelos serviços de segurança nestas empresas;
- ❑ Desde Janeiro de 2008 tornei-me Consultor Independente, na área dos Serviços de Segurança da Informação - Testes, revisões e aconselhamento sobre segurança;
- ❑ O meu trabalho tem sido focado na segurança para Instituições Financeiras.

Esta conversa é sobre... o quê?

Autenticação - Levantar o tema porquê? Não é uma coisa nova...

- ❑ Porque ainda é um tema difícil que tem que ser endereçado; e
- ❑ Lembrei-me de trazer algumas ideias directamente da zona de guerra.

Vou falar sobre

- ❑ Os conceitos - apenas algumas ideias para sincronizar a audiência;
- ❑ Os métodos usados com maior frequência na autenticação;
- ❑ As ameaças correntes às aplicações *web*; e
- ❑ Um conjunto de controlos alternativos, mais avançados.

Adicionalmente, no que toca a avaliação destes novos controlos

- ❑ Vou juntar umas ideias sobre o que devemos pensar na avaliação destas soluções.

Autenticação? Porquê? Para quê?

au•ten•ti•car (*)

verbo transitivo

1. Tornar autêntico;
2. Reconhecer como verdadeiro;
3. (DIREITO) acreditar (certo acto ou documento) por forma que, no futuro, faça fé em juízo;
4. Certificar; ou
5. Legalizar.

(De *autêntico* + *-ar*)

(*) Gamado directamente, sem vergonha, da Infopédia da Porto Editora...

“Sou o Zé. Deixa-me entrar”...

... não chega porque

qualquer um pode dizer isso...

Portanto...

tens que mo *provar!*

“Já sabes que é a Ana. Faz lá *isto!*”

Desculpa lá...

...mas não estou certo que
ainda sejas tu ao teclado

Portanto...

confirma lá isso, sff...

As aplicações são *tão* valiosas?

O valor não está nas aplicações; está...

- ❑ Na Informação, que é um activo essencial; e
- ❑ Nas Transacções, que manipulam a informação.

Informação, neste contexto, pode representar...

- ❑ Dinheiro;
- ❑ Saúde;
- ❑ Negócio;
- ❑ Dados pessoais;
- ❑ ...

Confirmar *todas* as transacções?!

Bem... Provavelmente, *nem todas*.

É aqui que a gestão do risco entra no jogo:
algumas serão sempre confirmadas;
outras, bem, não serão - aceitamos o risco.

Essa é uma decisão de negócio.

Zen #1

A autenticação é necessária...

- ❑ Para *tu* entrares em sessão;
mas também
- ❑ Para *confirmares* (algumas)
transacções

E o dragão, como alguns já sabem,
está aqui só para dar um certo estilo ;)



Os métodos mais usados

Os 5 controlos mais frequentes são:

- ❑ Passwords Estáticas ~64%
- ❑ P-a-s-s-w-o-r-d-s E-s-t-á-t-i-c-a-s ~19%
- ❑ sacitátsE sdrowssaP ~12%
- ❑ P@55w0rd5 357@71c@5 ~4%
- ❑ $\begin{matrix} p & s & w & r & s & e & t & . & t & c & s & (*) \\ a & s & o & d & & s & á & i & a & & & \end{matrix}$ ~1%

(*) Este ainda está em evolução, mesmo-mesmo novidade, mas promete (!)

Mas estes não chegam? Porquê?

Bem...

- ❑ Estes controlos são *extremamente* fracos;
- ❑ Inadequados para garantir a defesa contra as ameaças correntes, pelo que pudemos ver nos últimos ataques.

"*Fracos?* E o que significa isso das *ameaças?*..."

No próximo *slide* ;)

Ameaças, dizes tu?...

Que têm por alvo as credenciais ou a sessão:

- ❑ Puro palpite (muitas *passwords* são fracas);
- ❑ Palpite informado (as mesmas *passwords* em todo o lado);
- ❑ *Keyloggers* (ou, genericamente, **loggers*);
- ❑ *Man-in-the-middle*;
- ❑ *Browser-in-the-middle*;
- ❑ *Phishing* (por correio electrónico ou por telefone); e
- ❑ Ataques de oportunidade (locais).

Puro palpite

Auto-explicativo. Os standards actuais em *passwords* incluem:

- ❑ 123456 (por vezes são mais fortes: até 8!)
- ❑ password (um *vintage*...)
- ❑ Password (mais *high-tech*: 'P' maiúsculo)
- ❑ Vitória de Setúbal | Benfica | Porto | Sporting ...
- ❑ etcetc
- ❑ ... (agora é que vem mesmo o etc.)

Disseram-me que houve um artista que conseguiu, aqui há algum tempo, mais de 500 *passwords* em menos de 10 minutos, a partir de um conjunto tão pequeno como este, a fazer um ataque remoto na rede.

Palpite informado

- ❖ Se tu - sim, TU - usas a mesma *password* em dois (ou mais) serviços diferentes, levanta o braço e prepara-te para “o castigo” :)
- ❖ Adivinha lá: um desses serviços pode tentar *essa password* em todos os outros serviços...
- ❖ Uma vez ouvi uma conversa em que um gajo qualquer tinha catado mais de 10.000 *passwords* e verificado, sem grande espanto, que muitas também eram válidas no Gmail e no Hotmail...

**loggers*

- ❏ Texto estático que seja introduzido num computador pode ser capturado por algum *malware*, e enviado sub-repticiamente para um sítio manhoso, algures na Internet...
- ❏ ... onde um *hacker* qualquer ficará muito agradecido e, claro, irá usá-lo para movimentar umas *lecas* valentes para a sua própria conta, a partir da qual irá levantar a guita nas ATMs.
- ❏ Vi uma demo, aqui há atrasado, em que uns bacanos mostravam uma máquina comprometida a enviar credenciais para um servidor FTP no... (hmm... qual era o nome?... vocês sabem, aquele sítio de onde veio o Borat...) Cazaquistão! Aí.

Man-in-the-middle

- ❏ Cenário em que alguém observa (e/ou altera) as comunicações entre vosso computador e o servidor da aplicação, estando posicionado entre os dois.
- ❏ O SSL mitiga esta ameaça. Mas... *nem todas* as aplicações utilizam SSL, e *nem todas as pessoas* verificam "o cadeado".
- ❏ Pode ser despoletado por um convite por correio electrónico, sugerindo uma visita a uma aplicação forjada. Também pode ser realizado directamente numa *proxy* (sem SSL, ou mesmo com SSL se o *SysAdm* controlar as CAs reconhecidas pelos computadores).
- ❏ Já preparei umas demos mas nunca vi, nem nunca ouvi falar, de ataques reais por este método.

Browser-in-the-middle

- ❑ É, provavelmente, o ataque mais letal.
- ❑ Um programa dentro do *browser* que observa as credenciais ou altera as transacções, e.g. um *Browser Helper Object* (no contexto do IE).
- ❑ Pode ser programado para modificar a informação que é apresentada no ecrã.
- ❑ O programa pode ser instalado por um vírus, ou pela transferência e execução daquele jogo fabuloso que foi sugerido por um *mail*...
- ❑ Já ouvi falar num ou noutro ataque deste género - existem, de facto.

Phishing

- ❖ O envio de uma mensagem muito educada, alegadamente enviada pelo vosso Banco (ou outra organização em que confiam), convidando-vos a visitar o *site* - forjado, pronto para capturar as credenciais - para realizarem aquela operação muito urgente e importante. E está feito.
- ❖ Também pode ser realizado pelo telefone.
- ❖ Já vi alguns destes. Não funcionam com todas as pessoas. Mas, em abono da verdade, funcionam com algumas.

Ataques de oportunidade (locais)

- ❑ Uma sessão aberta durante a pausa para o café.
- ❑ Um cartão ou uma matriz surrupiados da carteira de alguém lá de casa.
- ❑ Pegar num telemóvel de alguém próximo e apanhar um SMS de confirmação.
- ❑ Não é preciso testemunhar um destes cenários para saber que, de facto, acontecem.

Zen #2



Ideias principais até aqui:

- ❑ A informação e as transacções têm valor
- ❑ As pessoas e as transacções têm que ser autenticadas
- ❑ Os controlos mais frequentes não são fortes; e
- ❑ Existem ameaças reais contra as aplicações

← Olha! Afinal bicho 'tá vivo...

Ok... então e os tais zingarelhos?

❏ Pseudo *One-Time Passwords*

- ❏ Matrizes

❏ *One-Time Passwords*

- ❏ *Hardware tokens*
- ❏ *Smartcard-based tokens*
- ❏ SMS

❏ Cripto. chaves públicas (PKI)

- ❏ Certificados digitais
- ❏ *Smartcards*

❏ Confirmação por *call-back*

❏ Biométricos

Nota: são apenas alguns exemplos, por classe!

Pseudo OTP: Matrizes

	1	2	3	4	5	6
A	12	33	88	98	32	27
B	99	09	83	37	36	88
C	00	98	32	22	12	66

Geralmente usadas para confirmar transacções. É pedido o valor de uma célula (e.g. B2) e o utilizador tem que introduzir o seu valor num formulário.

Pontos Positivos

- ❑ Portável
- ❑ Barato
- ❑ Fácil de usar
- ❑ Independente do computador
- ❑ Pode derrotar um **logger* (um *keylogger* simples)

Pontos Negativos

- ❑ Não resiste a:
 - ❑ **loggers* que incluam os ecrãs
 - ❑ *Man-or-browser-in-the-middle*
 - ❑ *Phishing* (a sério!)
 - ❑ Ataques de oportunidade

OTP: *Hardware tokens*

Usados no *login* e para confirmar transacções. Geram *passwords* aleatórias. Podem ser sincronizados por tempo ou por eventos. Alguns podem "assinar" desafios (vulgo, *challenges*).



Pontos Positivos

- ❑ Mais ou menos portátil
- ❑ Fácil de usar
- ❑ Independente do computador
- ❑ Derrota os palpites, **loggers* e *phishing*

Pontos Negativos

- ❑ Dispendioso
- ❑ Não resiste a:
 - ❑ *Man-or-browser-in-the-middle*
 - ❑ Ataques de oportunidade

OTP: *Smartcard-based*



Usados no *login* e para confirmar transacções. Geram *passwords* aleatórias. São geralmente sincronizados por eventos e podem “assinar” desafios. Exemplo: EMV-CAP nos cartões Multibanco.

Pontos Positivos

- ❑ Mais ou menos fácil de usar
- ❑ Independente do computador
- ❑ Derrota os palpites, **loggers* e *phishing*
- ❑ Um leitor, diversos cartões para várias aplicações e organizações

Pontos Negativos

- ❑ Não é muito portátil
- ❑ Dispendioso
- ❑ Não resiste a:
 - ❑ *Man-or-browser-in-the-middle*
 - ❑ Ataques de oportunidade (contra o cartão)

OTP: SMS



Poderiam ser usados no *login* mas são geralmente usados para confirmar transacções, apenas. Transportam uma OTP e, muito importante, incluem informação específica sobre a transacção solicitada na aplicação.

Pontos Positivos

- ❑ Portável
- ❑ Fácil de usar
- ❑ Independente do computador
- ❑ Derrota praticamente tudo *desde que* os utilizadores leiam a informação sobre a transacção

Pontos Negativos

- ❑ Moderadamente dispendioso
- ❑ Não resiste a:
 - ❑ Ataques de oportunidade (assumindo, claro, que alguém já tem acesso às credenciais ou a uma sessão aberta)

PKI: Certificados Digitais (*soft*)

Tipicamente usados no *login*. Poderiam ser usados para assinar digitalmente transacções se fosse instalado um componente específico nos *browsers* (e.g. um ActiveX ou equivalente). Funcionam através da autenticação em SSL, ao nível do cliente.

Pontos Positivos

- ❑ Portável
- ❑ Barato
- ❑ Fácil de usar (mas a instalação pode não ser fácil)
- ❑ Derrota os palpites, **loggers* e *phishing*

Pontos Negativos

- ❑ Depende de um computador
- ❑ Pode ser roubado do computador
- ❑ Não resiste a:
 - ❑ *Man-or-browser-in-the-middle*
 - ❑ Ataques de oportunidade

PKI: Cert. Digitais (*smartcards*)

Funcionalmente equivalentes aos certificados por *software* com as seguintes diferenças:

- ❑ Não podem ser roubados de dentro de um computador

Mas...

- ❑ Não são tão portáteis
- ❑ Não são tão baratos
- ❑ São igualmente fáceis de usar, mas a instalação do leitor pode não ser fácil

Confirmação por *call-back*

Geralmente usada para confirmar transacções, tal como é realizado, actualmente, para confirmar algumas transacções realizadas com cartões de crédito.

Pontos Positivos

- ❑ Portável (assumindo que transportamos um telemóvel)
- ❑ Fácil de usar
- ❑ Derrota quase tudo (mas pode sucumbir a um atacante oportunista *informado*)

Pontos Negativos

- ❑ Pode ser um mecanismo caro se não for usada uma análise de risco de transacções em tempo real

Biométricos

Leitores de impressões digitais; Íris *scanners*.

Tipicamente usados no *login*. Pessoalmente, não conheço aplicações *web* que utilizem estes mecanismos - só os vi em sistemas de controlo de acesso físico, e.g. em portas.

Pontos Positivos

- ❑ Fácil de usar
- ❑ Derrota os palpites, **loggers* e *phishing*

Pontos Negativos

- ❑ Caro e não é muito portátil
- ❑ Depende de um computador
- ❑ Não resiste a:
 - ❑ *Man-or-browser-in-the-middle*
 - ❑ Ataques de oportunidade (uma sessão aberta)

Tantos... Como é que escolhemos?

A considerar numa avaliação:

- ❑ As transacções são mesmo importantes na aplicação?
- ❑ É fácil compreender e usar o controlo? Quem são os clientes?
- ❑ É portátil? E isso é relevante?
- ❑ É fisicamente resistente?
- ❑ Pode ser usado em aplicações telefónicas? Novamente, isso é relevante?
- ❑ É baseado em standards? Ou é uma solução proprietária?
- ❑ Como pode ser distribuído e suportado?
- ❑ Como substituí-lo se for perdido ou roubado?
- ❑ Quanto custa? Quem paga?
- ❑ Contas feitas, quão adequado é para mitigar os riscos da aplicação?

E compreender que nenhum destes controlos é uma panaceia!

As perguntas conduzem-nos a...

... mais perguntas :)

Dada *esta* aplicação e *este* controlo:

- ❑ Qual será a probabilidade de alguém querer contorná-lo?
- ❑ Quão fácil será parti-lo considerando os controlos A, B, ...?
- ❑ Então e se for quebrado: qual será o impacto?
- ❑ Como é que recuperamos dessa situação?

O método de autenticação que escolherem será uma tentativa de responder às duas primeiras perguntas, apenas.

Será sempre gestão do risco

- ❑ Nenhum destes métodos é perfeito
- ❑ Não podemos confiar nos computadores pessoais
- ❑ As pessoas não são perfeitas - vão falhar

- ❑ Os controlos das vossas próprias aplicações também vão falhar...

Para além da autenticação...

Considerar...

- ❑ Baixar os valores máximos permitidos nas transacções
- ❑ Introduzir análises heurísticas das transacções
- ❑ Monitorização activa
- ❑ Transferência da responsabilidade (para os clientes?)
- ❑ Seguros
- ❑ ...

Master Zen

- ❖ A autenticação é importante no *login*, mas também nas transacções
- ❖ Existem ameaças reais contra as aplicações *web*
- ❖ Existem diversos controlos disponíveis para enfrentar os ataques
- ❖ Nenhum deles é uma panaceia
- ❖ A vossa escolha depende de vários factores - não apenas da segurança "perfeita"
- ❖ No final do dia, tudo se resume a gestão do risco



Boa. Mas ainda tenho dúvidas...

Q&A

Obrigado (!)



Miguel Almeida

Consultor Independente

Serviços de Segurança da Informação

- ✉ +351 962 608 928
- ✉ miguelalmeida@miguelalmeida.pt
- ✉ www.miguelalmeida.pt

- ✉ www.linkedin.com/in/mjnalmeida
- ✉ www.facebook.com/mjnalmeida
- ✉ www.twitter.com/mjnalmeida



FIHANKRA. "casa/edifício" - símbolo de segurança. Os símbolos Adinkra foram criados originalmente pela tribo Akan do Gana e pela tribo Gyaman da Costa do Marfim, na África Ocidental. Os símbolos representam conceitos ou aforismos. São utilizados em tecidos, murais, cerâmica, marcenaria, e logos. São muitas vezes utilizados para transmitir mensagens que evocam facetas da vida das pessoas.