

Authentication

Choosing a method that fits

IBWAS'09

Escuela Universitaria de Ingeniería Técnica de Telecomunicación
Universidad Politécnica de Madrid

December 2009

Miguel Almeida

Agenda

- ❑ Who's the guy with the tie?
- ❑ What's this talk all about?
- ❑ Authentication? Why? What for?
- ❑ Threats, you say?...
- ❑ Ok, I'm IN: show me some gadgets!
- ❑ But there's a lot of them... How do I choose?
- ❑ Uh? Risk management?...
- ❑ Got it! But I still have a couple of questions...
- ❑ I'm done. Handover the mike. Off you go...

Miguel Almeida

- ✦ Portuguese. ~~20~~... 38 tours around the Sun;
- ✦ Studied Computer Engineering @ *Instituto Superior Técnico* - Lisbon;
- ✦ From 2000 to 2007 I've worked for KPMG and Deloitte - Risk Management Services - managing their security services;
- ✦ Since January 2008 I became an Independent Consultant, providing Information Security Services - Security tests, reviews and advisory;
- ✦ My work has been focused on security for Financial institutions;

So what's this talk all about, anyway?

- ❑ Authentication - Why did you bring this up?, I mean, this isn't new...
 - ❑ Because this is still a difficult subject that needs to be addressed; and
 - ❑ I'm here to give you some hints directly from the war zone.
- ❑ I'll talk about
 - ❑ The concepts - just a few ideas to synchronize the audience;
 - ❑ The most Frequently used methods for authentication;
 - ❑ The current threats to web applications; and
 - ❑ A set of alternative advanced controls.
- ❑ Also, regarding evaluation of these new controls
 - ❑ I'll throw in some ideas about things to keep in mind when evaluating these solutions.
- ❑ Finally, I'll tell you about the bad news...
 - ❑ None of these is a silver bullet - none will give you perfect security; and
 - ❑ We must accept and deal with this imperfection - manage the risk.

Authentication? Why? What for?

au•then•ti•cate | ô'θenti,kāt | (*)

verb [trans.]

prove or show (something, esp. a claim or an artistic work) to be true or genuine : *they were invited to authenticate artifacts from the Italian Renaissance.*

- *validate: the nationalist statements authenticated their leadership among the local community.*
- [intrans.] Computing (of a user or process) have one's identity verified.

* Shamelessly stolen from Mac OS X's Dictionary.app

Why not just say “I’m Alice. Let me in”?

Because

anyone can say that...

So...

you must *show me some proof!*

“You already know I’m Bob. Just do *this!*”

Sorry...

I’m not sure if it’s *still you*
at the keyboard

So...

please *confirm u want that.*

But are the applications *that* valuable?

It's not about the application. It's about:

- ❑ Information, which is a valuable asset; and
- ❑ Transactions, which manipulate information.

Information, in this context, may relate to

- ❑ Money;
- ❑ Health;
- ❑ Business;
- ❑ Personal data
- ❑ ...

Confirm *all* transactions?! I mean...

Well... Probably not *all*.

That's when risk management comes into play: *some* will need to be confirmed; others, well, will not - we accept the risk.

That's going to be a business decision.

Zen #1

Authentication is
necessary...

- ❖ For letting *you* in; But also
- ❖ To *confirm* (some) transactions.

The dragon is here to cheer up a bit :)
They told me it was cool...



Frequently used methods

The 5 most frequently used controls are:

- ❖ Static Passwords ~64%
- ❖ S-t-a-t-i-c P-a-s-s-w-o-r-d-s ~19%
- ❖ citatS sdrowssaP ~12%
- ❖ 57@71c P@55w0rd5 ~4%
- ❖

| | | | | | | | | | | | |
|---|---|---|--|---|---|---|---|---|---|-----|--|
| s | a | i | | p | s | w | | r | s | (*) | |
| t | t | c | | a | s | | o | d | | | |

 ~1%

(*) This last one is still evolving, really bleeding-hedge, but soon to become state-of-the-art technology (!)

But aren't these enough? Why not?

Well...

- ❖ These are *extremely* weak controls;
- ❖ Unsuitable to defend against the current threats, as we've seen by the latest attacks

"*Weak?* And what do you mean by *threats?*" ...

next slide :)

Threats, you say?...

- ❖ Targeting the credentials or the session:
 - ❖ Pure guessing (many passwords are weak);
 - ❖ Informed guessing (same password all around);
 - ❖ Keyloggers (or, more generally, *loggers);
 - ❖ Man-in-the-middle;
 - ❖ Browser-in-the-middle;
 - ❖ Phishing (the regular kind or by phone);
 - ❖ Opportunistic (local) attacks.

Pure guessing

- ❏ Self explanatory. The current standards in password controls include:
 - ❏ 123456 (sometimes stronger: up to 8!)
 - ❏ password (a vintage...)
 - ❏ Password (High-tech: caps P)
 - ❏ Benfica | Barcelona | RealMadrid | Liverpool ...
 - ❏ etcetc
 - ❏ ... (really etc.)
- ❏ I've been told there was this guy who once got over 500 passwords in less than 10 minutes, with just a small set like this one, doing a remote network attack.

Informed guessing

- ❖ If you - yes, YOU - use the same password for two (or more) different services, please raise your hand and be prepared for punishment :)
- ❖ Guess what: that other service may try that same password on all the other services...
- ❖ I once heard this conversation where some guy had gotten over 10.000 passwords and had found that a lot of them were also usable on Gmail and Hotmail...

*loggers

- ❖ *Static text* that is entered in a computer can be captured by some malware, and surreptitiously sent to some dark place on the Internet ...
- ❖ ... where some hacker will give thanks and use it to move a few thousands to his own account, from where he (or she) will draw the money in ATMs.
- ❖ I've seen a demo where these guys showed a specially compromised machine sending the credentials to some FTP server in... (what's it called?... you know, that place Borat is from...) Kazakhstan! There.

Man-in-the-middle

- ❏ When someone observes and/or changes the communications between your computer and the application server, while being in the middle.
- ❏ SSL mitigates this threat. But then again, *not every app uses SSL and not every person checks "the SSL lock"*.
- ❏ Can be triggered by an email invitation to go to that (fake) application. Also, it can be done at a proxy (without SSL, or even with SSL if the SysAdm controls the CAs your computer trusts).
- ❏ I've setup some demos but haven't seen or heard of a real attack myself.

Browser-in-the-middle

- ❏ Probably the most deadly attack;
- ❏ A program inside the browser watching and changing your transactions or credentials, e.g. a Browser Helper Object (for IE);
- ❏ Can be programmed to change the info you read on the screen;
- ❏ The program can be setup by a virus or an invitation to download and install that great game...
- ❏ I've heard of a couple of these attacks - they do exist.

Phishing

- ❖ Sending a polite email, pretending to be your Bank, inviting you to do this very important thing [at another fake site], and asking for your credentials. Done.
- ❖ I've seen some of these. They don't work for all people but, well, they do for some.

Opportunistic (local) attacks

- ❏ Coffee break while the application is in an open session
- ❏ Going through some family member's wallet do get a matrix or a smartcard
- ❏ Picking up the mobile phone when some confirmation code is arriving by SMS
- ❏ No need to witness the scene to know these actually happen.

Zen #2



Main ideas so far:

- ❖ Information and transactions are valuable
- ❖ Users and transactions must be authenticated
- ❖ Frequently used controls aren't strong
- ❖ There are real threats to current applications

Ok, I'm IN: show me some gadgets!

In a nutshell:

- ❑ Pseudo One-time passwords
 - ❑ Matrices
- ❑ One-time passwords
 - ❑ Hardware tokens
 - ❑ Smartcard-based tokens
 - ❑ SMS
- ❑ Public Key Crypto.
 - ❑ Soft Digital Certificates
 - ❑ Smartcards
- ❑ Call-back verification
- ❑ Biometrics

Note: this is just a class sample set!

Pseudo OTP: Matrices

| | 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 |

Usually used to confirm transactions. The user is given a coordinate (e.g. B2) and must enter that cell's value.

Positive

- ✦ Portable
- ✦ Cheap
- ✦ Easy to use
- ✦ Doesn't require a computer
- ✦ May defeat a *logger (a simple keyboard logger)

Negative

- ✦ Doesn't stand a change against:
- ✦ A proper *logger that includes screenshots
- ✦ A man-or-browser-in-the-middle
- ✦ Phishing (really!!)
- ✦ Opportunistic attacks

OTP: Hardware tokens

Usually used to login and to confirm transactions. Generates random passwords. Can be time-synchronized or simply event-based. Some can "sign" challenges



Positive

- ❑ Sort of portable
- ❑ Easy to use
- ❑ Doesn't require a computer
- ❑ Defeats guessing, *loggers, and phishing

Negative

- ❑ Expensive
- ❑ Doesn't stand a chance against:
- ❑ A man-or-browser-in-the-middle
- ❑ Opportunistic attacks

OTP: Smartcard-based tokens

Usually used to login and to confirm transactions.
Generates random passwords. It's usually event-based and can "sign" challenges - e.g. EMV-CAP



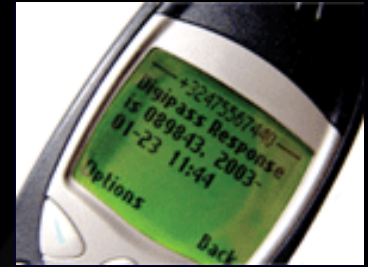
Positive

- ❑ Sort of easy to use
- ❑ Doesn't require a computer
- ❑ Defeats guessing, *loggers, and phishing
- ❑ One reader, many different cards - for several applications and providers

Negative

- ❑ Not so portable
- ❑ Expensive
- ❑ Doesn't stand a chance against:
 - ❑ A man-or-browser-in-the-middle
 - ❑ Opportunistic attacks (against the card)

OTP: SMS



Could be used to login but it's usually used to confirm transactions only. Generates an OTP code *and* carries information about the transaction

Positive

- ❑ Portable
- ❑ Easy to use
- ❑ Doesn't require a computer
- ❑ Defeats almost everything AS LONG as the user reads the transaction information

Negative

- ❑ Moderately expensive
- ❑ Doesn't stand a chance against:
- ❑ Opportunistic attacks

Public Key Cryptography: Soft Certs

Usually used to login. *Could be used* to digitally sign transactions *if* a special component was installed in the browser. Works via SSL client-side authentication

Positive

- ✧ Portable
- ✧ Cheap
- ✧ Easy to use (but not so easy to install)
- ✧ Defeats guessing, *loggers, and phishing

Negative

- ✧ Requires a computer
- ✧ Can be stolen from the computer
- ✧ Doesn't stand a chance against:
- ✧ A man-or-browser-in-the-middle
- ✧ Opportunistic attacks

Public Key Cryptography: Smartcards

Basically the same as the soft certificate with the following differences:

- ❑ Cannot be easily stolen from inside the computer

But

- ❑ Not so portable
- ❑ Not so cheap - more like expensive
- ❑ As easy to use but may be harder to install the reader

Call-back verification

Usually used to confirm transactions, as it's already being done with credit card operations.

Positive

- ✦ Portable (as long as you have a mobile phone...)
- ✦ Easy to use
- ✦ Defeats almost everything - but an *informed* opportunistic attacker may defeat it

Negative

- ✦ May be expensive, unless real-time transaction risk-analysis is in place

Biometrics

Fingerprint readers, iris scanners.

Usually fitted to login; I haven't seen it being used for web applications - only physical security related controls, e.g. for doors

Positive

- ✧ Easy to use
- ✧ Defeats guessing, *loggers, and phishing

Negative

- ✧ Expensive
- ✧ Not so portable
- ✧ Requires a computer
- ✧ Doesn't stand a chance against:
 - ✧ A man-or-browser-in-the-middle nor a coffee break and an open session

There's a lot of them. How do I choose?

- ❑ Things to evaluate:
 - ❑ Do you really care about transactions in your app?
 - ❑ Is it easy to understand and use? Who are your clients?
 - ❑ Is it really portable? Does it matter?
 - ❑ Is it physically resistant?
 - ❑ Is it usable for phone-apps? Again, does it matter?
 - ❑ Is it standards-based? Or a one-company solution?
 - ❑ How can it be deployed and supported?
 - ❑ How do we replace it if it's lost or stolen?
 - ❑ How much does it cost? Who pays for it?
 - ❑ All in all, how well does it mitigate your application's risks?
- ❑ Also keep in mind that *none of them is a silver bullet!*

Those questions also lead us to...

- ❖ Given *this* application and *that* new control
 - ❖ What's the probability of someone wanting to break it?
 - ❖ How easy will it break considering controls A, B, ...?
 - ❖ What if it breaks: what will be the impact?
 - ❖ How will we recover?
- ❖ The authentication method you choose will be your attempt to minimize the response for the 1st two questions.

Will always be about risk management

- ❖ No single method is perfect;
- ❖ Personal computers aren't to be trusted;
- ❖ Users aren't foolproof - they fail;
- ❖ Your own application controls will fail...

Besides authentication, consider...

- ✧ Lowering maximum transaction values
- ✧ Heuristics-based transaction analysis
- ✧ Active monitoring
- ✧ Responsibility transfer [to the clients?]
- ✧ Insurance
- ✧ ...

Master Zen

Wrapping it up

- ❖ Authentication is about logins but also about transactions
- ❖ There are real threats out there to web applications
- ❖ Several kinds of controls are available to face the attacks
- ❖ None of them is a silver bullet
- ❖ Your choice depends on several factors - not just "perfect" security
- ❖ At the end of the day, it will always be about risk management



Got it! But I still have some questions...

Q&A

Thank you (!)



Miguel Almeida

Independent Consultant

Information Security Services

- ✘ +351 962 608 928
- ✘ miguelalmeida@miguelalmeida.net
- ✘ www.miguelalmeida.net

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



FIHANKRA. "house/compound" - symbol of security and safety. Adinkra symbols were originally created by the Akan tribe of Ghana and the Gyaman tribe of Cote d'Ivoire in West Africa. The symbols represent concepts or aphorisms. They are used on fabric, walls, in pottery, woodcarvings and logos. They are often used to communicate evocative messages that represent parts of people's life.