

Introduction to Information Security
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 12
Two Factor Authentication

Now, we will discuss about two factor authentication because single factor authentication namely password – we have enough feel that it is not fully secure.

(Refer Slide Time: 00:29)

**The Most Common Alternatives
To Just Traditional Passwords**

- Two factor authentication combines two or more types of authentication, such as:
 - Hardware cryptographic tokens (crypto key fobs)
 - Biometrics (such as thumbprint scanners)
 - Smart cards or USB thumb drives with certs
- Today, let's just consider hardware crypto tokens.
- Given all the problems that traditional passwords represent, why haven't sites rushed out to deploy hardware crypto tokens?

The most common alternatives to just traditional password is to have this hardware tokens or biometric or smart cards. The hardware tokens are very interesting especially the key. The hardware token generates a random key and thus the key that is shown on the token is synced with the key that is generated on the server. And so, along with your password, you also enter the value of this key and the server also will compare this key with the entered key. And, since these keys are synced up, the login can happen. If the keys are not synced up; that is, if you do not have access to the key and you put a random key, then the key will not match and essentially the system will not allow the user to login. So, this token – the hardware token is a very very interesting stuff as a second factor – two factor authentication. So, why people have not rushed to having this hardware crypto tokens? That we know that conventional passwords are problematic; why this security measure is not even seen in many organizations.

(Refer Slide Time: 02:00)

Cost Is One of The Primary Reasons Why There's Resistance to Replacing Passwords

- As expensive (and insecure) as passwords may potentially be, the cost of alternatives is one of the primary reasons why there's resistance to replacing passwords with something else.
- For example, some hardware cryptographic tokens may run Rs. 1,800 per year per person (e.g., Rs.3,600 for a crypto token with a 2-3 year life from one vendor).
- That's a non-trivial expense, particularly if passwords are "free" (even though we know they're NOT really "free.")

One of the thing is – of course it is very very expensive. Today, we are talking of cryptographic token which will go up to 1,800 per year per person. And, this is a non-trivial expense like look at an organization with 3,000 employees or 5,000 employees. And to spend some 1000 rupees for each would be just for an authentication would be extremely costly affair and this is going to be your recurring expenditure also.

(Refer Slide Time: 02:34)

PayPal SecurityKey: Rs.400

PayPal Security Key



PayPal Security Key
Add another layer of protection to your account

[Get Yours Now](#)

Get an extra layer of protection with the PayPal Security Key - it's easy to use and portable, so you can access your account with confidence from just about anywhere.

What is it?
The PayPal Security Key creates random temporary security codes that help safeguard your PayPal account when you log in. It comes in 2 types, each with different advantages:

1. **Security key:** You carry this small credit-card sized device with you. It creates a unique security code on the go.
2. **Mobile phone security key:** You can sign up to get security codes sent by text message to your mobile phone.

How much does it cost?
The mobile security key has no costs, except your mobile provider's standard text messaging charges. Check with your mobile provider for details.
Each security key is \$5, and there's no monthly service fee or additional cost. Replacement keys are the same price.

Already have a security key?
[Activate Now](#)
It will also work with your eBay account.
[Click Here](#) 

Now, for the some websites, for example, PayPal has a security key, which is costing around 400 rupees. Now, what is that security key? There are two types of security key:

there is a normal security key; again, there is a mobile phone security key. And, if you use the normal security key, it actually gives the same functionality that I described of a hardware crypto key. And, this can be used at 400 rupees and for all transactions with PayPal, so that nobody... So, your login into PayPal is actually authorized much beyond a password with more security than a password.

(Refer Slide Time: 03:26)

Sample Token Vendor Competing On Price...

Entrust IdentityGuard Mini Token

Versatile and convenient, Entrust now offers the security of one-time-password tokens to provide strong authentication for enterprises, governments and consumers.

Small form, big introduction

Who would have thought that the introduction of something as small as the new Entrust IdentityGuard Mini Token could have such a huge impact on the authentication market. The Entrust IdentityGuard Mini Token and **its industry-first \$5 price tag** eliminates past barriers to leveraging hardware tokens as part of a versatile authentication platform.

With its smart, simple, one-button design, the Entrust IdentityGuard Mini Token offers easy-to-use capabilities that can be deployed alone or in combination with other authentication methods as part of the Entrust IdentityGuard platform — a highly respected versatile authentication solution.

Affordable, smart pricing from Entrust

Priced at \$5 per token the Entrust IdentityGuard Mini Token demonstrates that secure, reliable hardware authentication can be had at an attractive price. The real value for organizations is the ability to leverage affordable tokens in parallel with the full spectrum

Entrust IdentityGuard Tokens
QUANTITY ONE: \$5

There are other vendors who compete on price. So, this itself... So, if you look at this statement – I marked it in red; you say this industry is first dollar 5 price tag. So, as you see here, the price tag becomes extremely important; and thus, just because of this price, people did not rush to using hardware crypto tokens in addition to passwords.

(Refer Slide Time: 03:53)

Incremental Deployment Is Also A Possibility

- If you can't afford to deploy hardware crypto tokens everywhere due to cost, potentially consider an incremental deployment strategy.
- For example, perhaps you may want to consider initially deploying hardware crypto tokens just for administrative system users, or privileged users, or even just for all faculty/staff.
- By limiting the number of tokens you initially deploy, you can:
 - focus on the most security-sensitive areas first
 - keep the total cost for the project low
 - gain experience deploying and administering tokens
 - help users become familiar with tokens and how they work (many users may never have heard of them)

So, one of the suggested way is to have an incremental deployment of this hardware security tokens. First, give it to security-sensitive people; then, totally... then, moved on to administration people and slowly percolate to other employees. So, by limiting the number of tokens you initially want, you can go and slowly keep incrementally deploying these hardware tokens and incrementally giving the tokens to the employees, so that you do not have a single one-time cost; but, you have a cost which is incremental. So, this is one suggested mechanism.

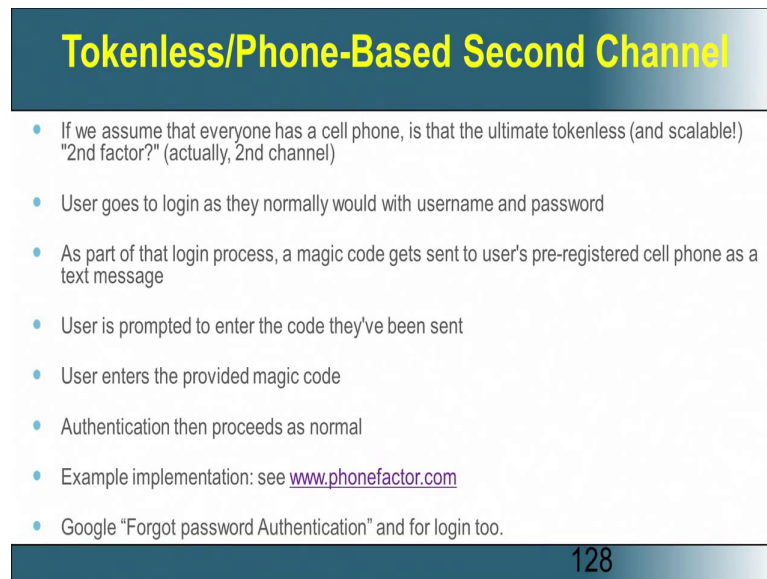
(Refer Slide Time: 04:37)

Example #3



This was another example at Purdue...

(Refer Slide Time: 05:05)



Tokenless/Phone-Based Second Channel

- If we assume that everyone has a cell phone, is that the ultimate tokenless (and scalable!) "2nd factor?" (actually, 2nd channel)
- User goes to login as they normally would with username and password
- As part of that login process, a magic code gets sent to user's pre-registered cell phone as a text message
- User is prompted to enter the code they've been sent
- User enters the provided magic code
- Authentication then proceeds as normal
- Example implementation: see www.phonefactor.com
- Google "Forgot password Authentication" and for login too.

128

This is the boiler key, which is similar to the hardware token key. But, this was used for anyone to get access into the Purdue network. The alternate channel could also be a phone-based... It is a tokenless phone-based stuff, which could be used as a second factor. So... But, this essentially assumes that everyone has a mobile phone and a magic number is sent. Whenever you want to login, a magic number is sent or a passcode is sent to your... or a one-time passcode is sent your mobile number; and then, that passcode need to be entered. So, if you lose your cell phone, then the person who gets a cell phone can basically get the password – can basically get access, because he can try to login, but he should know your password. And, if he knows your password, then this second factor authentication is of no use, because he has access to your cell phone. So... But, this certainly... If everyone has a mobile phone – a personal mobile phone; then, it is the company need not invest on this hardware token, so that it becomes a very very cost effective scheme.

(Refer Slide Time: 06:16)

Conclusion/Summary

- Traditional passwords have many security issues, but they are still all-too-widely used
- The time has come for you and your site to replace them with something stronger, such as hardware crypto tokens
- You may NEED to do so for compliance reasons (PCI-DSS)
- Leading online sites (such as eBay, gaming sites, and brokerages) are already deploying hardware tokens, and so are leading educational institutions (at least for selected groups)
- Cost remains a potential issue, but can be potentially finessed
- Scalability is the other issue we need to keep in mind; second channel authentication (e.g., magic codes sent to user cell phones via text messages) may be one answer.

So, to conclude, what we have done so far in module 1; we started looking at again C-I-A – the confidentiality, integrity and availability. And, we now started looking at controls, which will ensure confidentiality, integrity and availability. We saw administrative controls; we saw logical controls or technical controls. And, inside technical control, we have currently seen access control; the access control again was of two types: a physical access control, which was more of administrative and the technical. Then, we started looking at access control for identification and authentication. And, there we looked at passwords; we found that passwords are not very much secure. And, we looked at two-level authentication. And, we also looked at some of the recommendations of standards.

What we will do next is on application level security. Applications are those that are part of your process in terms of interpreting and manipulating data. And now, how do we get control over the application? So, we now talked about how do we get control over the people. Now, we will now talk about how do we get control over the process. And finally, we will also see how do we get control over the technology.

Thank you.