

Identity Management - II

Saurabh Srivastava

Department of Computer Sc. & Engg.

IIT Kanpur

Identity Management - II

Saurabh Srivastava

Department of Computer Sc. & Engg.

IIT, Kanpur

Hi, welcome back. This is the second part of the Identity Management lecture. In the previous lecture we had a look at the personal traits of a human being which can be used by a system. In this part we are going to have a look at something else which we are going to term as system generated identities okay. So we've already seen what personal traits we have like face and iris and all that stuff. We are going to see something else now, some identities which are generated by the system okay.

System-generated identities

- What if the system provides you an identity from its side?
- A Username/Password pair
 - Probably the most common identification mechanism used by computers
 - The system **shares a secret** with you, that it expects, only you know - the Password!
 - Anyone who *knows the secret*, can pose as you - the system can't differentiate you with him/her
- OTPs - One time passwords
 - Variation of Username/Password Scheme
 - Instead of a long term secret, system generates a short password, sent to your phone and/or email - assumes your phone/email is in your possession

so with this become to system generated identities. So suppose any system that wants to identify you provides you an identity from its own site. So a username or password pair is one such identity. So the system will give you a username or password. You can actually choose your username and password and this is a kind of a shared secret. So the system knows this secret and only you know this secret. And if somebody can provide this secret the system simply assumes that it's you and nobody else knows this password.

So anyone who knows this secret can pose as you. This is the aspect that we have to understand. So even though systems are trying to share a secret with you anyone who knows that secret can pose as you. So the system really cannot identify anyone who's different from you if he or she knows the username, password of your, your account.

There is a variation to this called OTPs or One Time Passwords. One Time Passwords are basically system generated identities for short term. So the system generates some kind of a random string. It is sent to your registered phone or email and you are supposed to enter this information say within a few minutes or something like that and well this is how the system identifies you. The assumption that system actually makes is that the phone or email on which the password was sent is in your possession. This is very important. The system assumes that you are having your phone with you and that the email that you provided to the system it is still operated by you only and not by someone else.

System-generated identities (cont.)

- Cookies
 - An extension of Username/Password mechanism
 - Entering password and/or username every time you interact with the system may be irritating
 - How about having a pact with the **browser** you use, to do it for you?
 - **Keep me logged in** - Sounds familiar? Those are cookies at work !
 - The browser stores some information regarding your identity, when you log in to a website
 - It can be *replayed* next time you try to visit the same website
 - The system can log you in automatically using information sent by the browser (stored locally at your computer as a "cookie")
 - Assumes that only you have access to this computer - **don't tick that otherwise**

So with this we come to another interesting concept called cookies. So let us assume that the system was able to generate an identity for you; username and password and you know you now have a shared secret with the system with which you can identify. The problem is that most of the time this username password entering could actually be a kind of you know boring activity that you will have to do. Just imagine if you log into Facebook every day say you know two dozen times and you have to type in your password and type in your username every time. That is going to be boring. That is going to be irritating for the user. So how about having a pact between your browser and system. So in general cookies are a pact between your browser and the system. So you must have seen something like keep me logged in. Many of the sites these days have this kind of a message on their homepage that you are entering username and password and there is an option keep me logged in or keep me signed in something like this. So these are cookies at work. The browser stores some information regarding your identity when you log into a website and then this identity can actually be replayed next time you try to visit the same website. So the system can log you in automatically using the information that was sent by the browser. You do not really need to type in the username password all over again. The system can simply log you in with the help of this cookie.

Again just like the previous cases there are some assumptions. The assumption is you have access to this computer and only you can use that particular browser. If you are using a Facebook or say Gmail or some other website like this on a shared computer then do not tick that.

How secure is our identity?

- Can a computer trust something like a Password?
 - Provided the limitations with other traits, passwords are easy to manage, and provide "acceptable" security
- But passwords are not too secure
 - People tend to keep passwords which could be "easily remembered"
 - Someone could "guess" your password, if you are too predictable with them
 - There are tools, which can do this "guess work", if provided with enough opportunities and resources
 - sometimes, just trying combinations of some publicly available information of a person, like name and birthday can hit the Jackpot
 - Also, passwords could be "sniffed" over a network, if sent without any encryption (ever wondered why some web addresses start with "https" and not "http"?)

So how secure is our identity? Well can I computer trust something like password? Well provided the limitations with other traits passwords are a very good way of identifying people. They are fairly robust and they are easy to manage. They are actually acceptable for a number of reasons because considering the amount of hardware you will actually be required for using something like biometric traits, password is a fairly good what shall I say fairly good trade-off; but passwords are not very secure. People tend to keep passwords which could be easily remembered. This is the whole point of putting up passwords. If we do not remember passwords what are they for so. If the password is easy to remember it would probably be easy to guess as well. So if you are too predictable with what you give as your passwords that can actually be guessed quite easily. In fact there are some tools which can do this guess work for you and then just trying combinations of some publicly available information like your name, your date of birth, the name of your spouse, the name of your parents just trying combinations of that can you know give the password in a number of cases.

Also passwords could be sniffed over a network. So what does sniffing means? So basically just assume that you are connecting to a system by a network and somebody is trying to listen what data packets are going on that network by the virtue of just sniffing what data is going through people can actually figure out what you typed. So they can actually figure out your username. They can actually figure out your password; whatever text messages you write on say Facebook everything can actually be sniffed over network. So this is something that is possible using network sniffing. And there will be a homework on this. We will talk about HTTPS and HTTP. You would have seen certain websites start with HTTPS and certain websites start with HTTP. So there will be a homework on this just to tell you what is the difference between the two; how HTTPS makes your website more secure than HTTP. We'll come back to this.

Prevention and/or Cure?

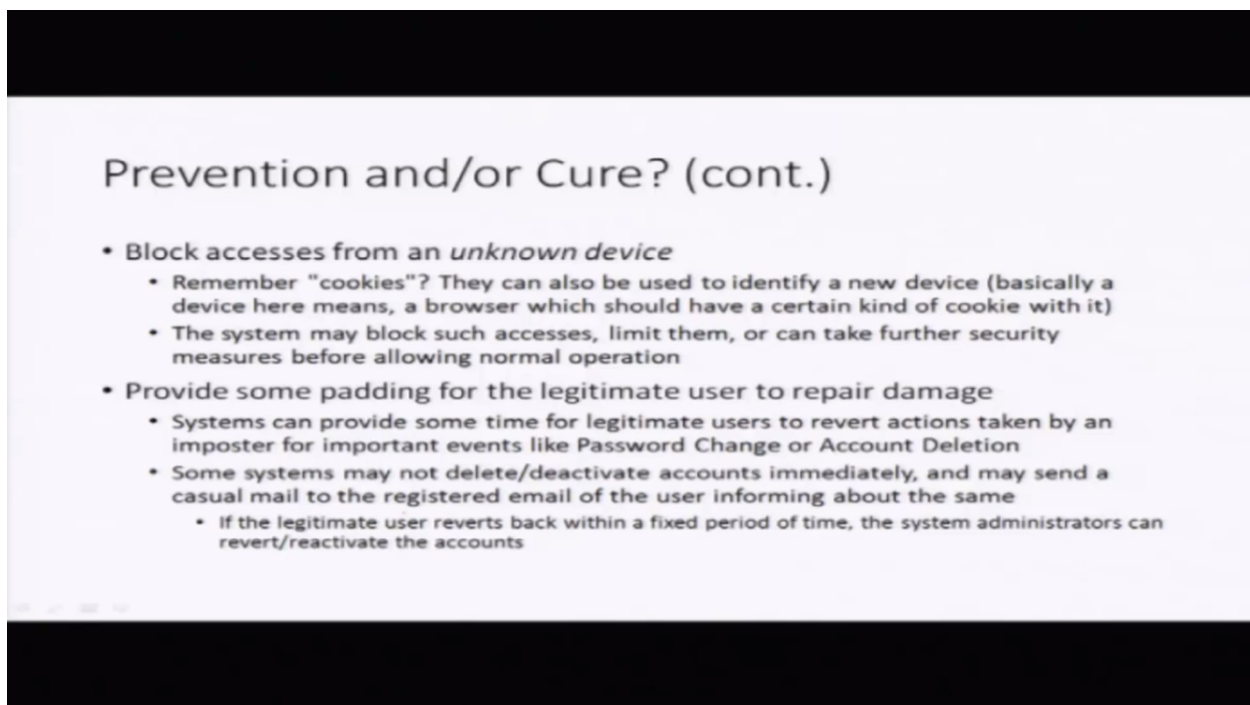
- Force regular password changes
 - Some systems force the users to change their passwords on a regular basis
 - It might be a nuisance to the user though, since finding an *easy to remember, yet difficult to guess password* is often not trivial
- Can the systems detect an imposter posing as you?
 - Some systems deploy *heuristics* to detect probable imposters
 - What if someone who logs in from Kanpur regularly, logs in from Beijing?
 - We'll know more about how systems know your location in the next lecture
 - May or may not be an imposter, but could be a good idea to ask some questions or send an OTP to your mobile, just to be sure it's you !

Prevention or cure so can the system's actually prevent themselves from any kind of attacks or any impostor? Well there are some heuristics that can be used. One is forcing regular password changes. So some systems for example the banking website these days they will force you to change your password fairly regularly. For example they will ask you to change your passwords say every six months or so. So this is one way of trying to minimize the effect of anybody trying to hack your password or anybody trying to guess your password. So basically if you keep on changing them regularly the chances are that they won't be able to guess it but surely it is going to be a nuisance for the user because finding an easy to remember password which is difficult to guess well that is not an easy task. Generally won't be able to come up with so many passwords which are easy to remember but difficult to guess.

Okay can the systems somehow detect an imposter? So let us assume that the imposter did get hold of your username and password and now the imposter wants to login to the system as you. Can this can the system still do something? Well some systems reply heuristics to detect probable imposters. For example if I am logging to their website from Kanpur regularly if suddenly I login from something like say Beijing that is going to be suspicious because regularly I login from Kanpur how the hell can I go to Beijing in say a few hours of time. Some systems use this information to you know detect detect probable attacks. They are not sure whether it was actually an attack or not but the activity is suspicious. It may actually be looked upon in a bit more detail.

Now one more wave y which probably the bank websites try to minimize any kind of attack is by using of OTPs. We talked about OTPs. They are One Time Passwords which are sent to your mobile and/ or your email ID. So if an imposter somehow gets hold of your username and password it may still be difficult for him to be able to enter that OTP that was sent to your mobile because the mobile will still probably be with you and the email will probably still be in your position. So being able to enter that OTP is not that easy. So that is one way let us say it is kind

of an extra layer of security that the banking website or some other website is trying to add. It may or may not be helpful but yeah it may be used to detect or say stop certain importers.



The slide is titled "Prevention and/or Cure? (cont.)" and contains a bulleted list of security measures. The list is as follows:

- Block accesses from an *unknown device*
 - Remember "cookies"? They can also be used to identify a new device (basically a device here means, a browser which should have a certain kind of cookie with it)
 - The system may block such accesses, limit them, or can take further security measures before allowing normal operation
- Provide some padding for the legitimate user to repair damage
 - Systems can provide some time for legitimate users to revert actions taken by an imposter for important events like Password Change or Account Deletion
 - Some systems may not delete/deactivate accounts immediately, and may send a casual mail to the registered email of the user informing about the same
 - If the legitimate user reverts back within a fixed period of time, the system administrators can revert/reactivate the accounts

So what can the systems do other than this? Cookies. We talked about cookies. The cookies can actually be used for something more than that. They can also be used to identify a new device. So basically suppose I bought a new laptop and I logged into Facebook from that new laptop. Facebook might actually block my access to it because that device is not identifiable. Basically by identifiable I mean it they should have a certain kind of cookie within it. So when the browser connects to Facebook it sends some information to it and if the browser is not able to send that information Facebook may feel you know this is something suspicious. This is not the device from which you login regularly. So the system may actually blocks such accesses, actually Facebook does that. It will probably ask you to first identify yourself by entering some one-time password or it might even ask you tag some friends of yours you know before going ahead. So this is actually something that systems do use. They can take further security measures before allowing you or they simply block your access for now.

Then suppose the impostor actually logged in as you and he was able to go through all the security checks the system had. Now what? So let us say an impostor may actually go and delete your account or may deactivate your account. Can the system provides some padding to the legitimate user? Can the user can get back to the system and save the situation? Well some systems can provide some time for legitimate users to revert actions. So for example if you actually if the impostor did some kind of events like changing the password or deleting your account well the legitimate user can be sent an email and he can be informed about what just happened. If the actual legitimate user was someone who didn't do that he can actually get back

to the system by say within certain amount of time within 24 hours or 48 hours and the system administrators can actually revert the account back.

Now some systems may actually do not delete all your stuff as soon as you actually do that. They actually keep that stuff within their database or their storage and they wait till say 48 hours or say one week or something like this and you can actually get back to them if you think somebody else actually hacked your account and they did some stuff. So some systems keep backup of your data as well and they can actually restore the state of your account to an older state.



Okay. So a quick recap of till of what we've learned till now.

Conclusion

- Systems need to identify people, before communicating with them, just like we do
- The usual traits employed by us (face or voice) are generally not usable by systems
- The most common way to do so is via **shared secrets**, e.g. Passwords
- Cookies can be used to reduce the actual number of times the user needs to enter the secret in a form
- Modern Systems use multiple heuristics to detect, avoid and repair possible attempts to a breach of Identity

So systems need to identify people before communicating with them just like we do. We communicate with someone only after we recognize them. The usual traits employed by us are say face or voice and these states are generally not usable by systems. The most common way by which systems identify us are by shared secrets. These are passwords. We just talked about passwords and usernames. Cookies is actually a mechanism by which we can reduce the actual number of times the user will be required to type in the username or password. We we talked about how boring it can be to type username and password each and every time you log into some system. Now modern systems also apply some kind of heuristics to detect, avoid, and repair possible attempts of a breach of security. So basically it is possible that the system may actually take care of recording your locations every time you log in and with the help of your location the system is able to figure out if somebody is trying to hack into your account. So the systems use some kind of heuristics these days and with the help of those heuristics they can figure out certain security breaches.

Homework

- Figure out the difference between "http" and "https". How does it affect Identity Management?
- Why clicking on "**Keep me logged in**" is a horrible idea, if you are accessing Facebook from a Cyber Café? What could go wrong here, with respect to your identity?
- There's an exercise on Slide 10. That's more fun actually. Try logging in to the IRCTC website, with the same account, from two different browsers, one after the other (don't log out from the first session, before logging into the second). Now try to see your booked ticket history from the first session.
Can you relate this somehow to Identity Management?

Homework. So we talked about HTTP and HTTPS. We were talking about them in the context of key logging; how somebody can actually put some kind of a keylogger and record all the keys that you press on a keyboard and with the help of that they can probably figure out your username and password. Well there are some ways to avoid this. Some websites use something called HTTPS. This is HTTP Secured. So your homework is go and try to find out what is the difference between these two; HTTP and HTTPS. Can this kind of key logging be saved? How can some systems try and protect your passwords when they are in transit. The other thing is that you could probably do is check out this Keep me logged in feature. You just just read a little bit more about what this keep me logged in feature does and you just have to figure out why it is a horrible idea if you are using some site like Facebook from a cyber cafe to put tick on this keep me logged in. what what can go wrong here? You have to think and figure out what would be a problem by ticking keep me logged in. It can actually cause some serious problems for you.

So you have to figure out what could go wrong here with respect to identity management. And this is a fun exercise the last one. So basically we are talking about the IRCTC website we talked about how the IRCTC website uses your username and password as your identity. Do this go to the IRCTC website and try to login to the IRCTC website from the same account but with two different browsers. So you can use say Firefox and Chrome. So log into Firefox first and use your username and password. Log in there. Open another instance say Chrome log in there with the same username password as you did in Firefox and then from the first session the one in Firefox try to access some information, something like your booked history or or cancellation history and see what happens. There will be something that that will be surprising for. Let's just leave it here and find it out what you see in that.

So you can probably somehow relate it to identity management. This is what your task is, relating it to identity management.

Thank you.