

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

Lecture – 10

Sometimes people do not even bother changing default device passwords.

(Refer Slide Time: 00:09)

Sometimes People Don't Even Bother Changing Default Device Passwords

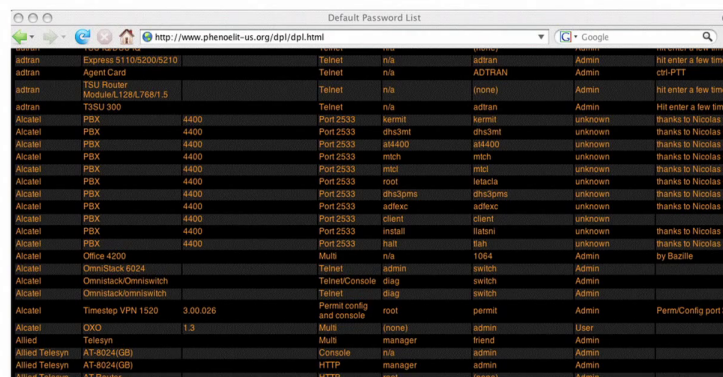
- Not changing default/well known passwords is an extreme example of “picking bad passwords”, but it is still all too common.
- You may or may not be aware that lists of default/well known passwords for particular devices are in widespread circulation -- if you didn't know this, you do now.
- It is absolutely critical that any or all default accounts/passwords get changed (or disabled) when devices are put on the wire.

86

When you buy a device there will be some default passwords that are set in and you do not even change it. It is absolutely critical that all default accounts, passwords, get changed or disabled when devices are put on the field.

(Refer Slide Time: 00:36)

One Example of A Default Password List

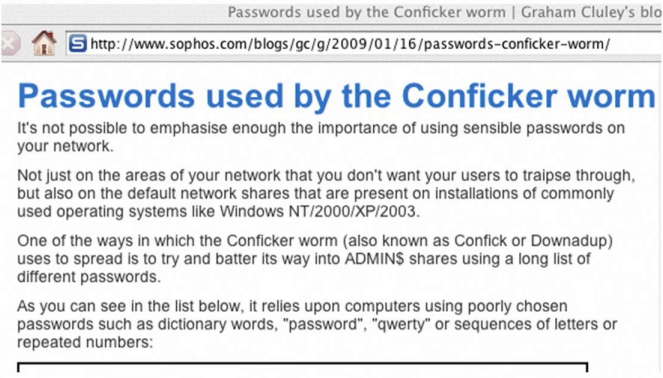


Device	Model	Port	Username	Password	Notes		
adtran	Express 5110/S0005210	Telnet	rla	adtran	Admin		
adtran	Agent Card	Telnet	rla	ADTRAN	Admin		
adtran	TSU Router	Telnet	rla	(none)	Admin		
adtran	Model:1284.7681.5	Telnet	rla	adtran	Admin		
adtran	TSSU 300	Port 2533	kermit	kermit	unknown		
Alcatel	PBX	4400	Port 2533	dhs3mt	dhs3mt	unknown	thanks to Nicolas G
Alcatel	PBX	4400	Port 2533	rla490	rla490	unknown	thanks to Nicolas G
Alcatel	PBX	4400	Port 2533	mitch	mitch	unknown	thanks to Nicolas G
Alcatel	PBX	4400	Port 2533	mici	mici	unknown	thanks to Nicolas G
Alcatel	PBX	4400	Port 2533	root	letacta	unknown	thanks to Nicolas G
Alcatel	PBX	4400	Port 2533	dhs3pm	dhs3pm	unknown	thanks to Nicolas G
Alcatel	PBX	4400	Port 2533	adfwc	adfwc	unknown	thanks to Nicolas G
Alcatel	PBX	4400	Port 2533	client	client	unknown	thanks to Nicolas G
Alcatel	PBX	4400	Port 2533	install	flatrni	unknown	thanks to Nicolas G
Alcatel	PBX	4400	Port 2533	rla	rla	unknown	thanks to Nicolas G
Alcatel	Office 4200	Multi	rla	1064	Admin	by Bazille	
Alcatel	OmniStack 6024	Telnet	admin	switch	Admin		
Alcatel	OmniStack/Omniswitch	Telnet/Console	diag	switch	Admin		
Alcatel	OmniStack/Omniswitch	Telnet	diag	switch	Admin		
Alcatel	OmniStack/Omniswitch	Permit config and console	root	permt	Admin	PermtConfig port 38	
Alcatel	OXO	1.3	Multi	(none)	admin	User	
Allied	Telesyn	Multi	manager	friend	Admin		
Allied Telesyn	AT-8024(OB)	Console	rla	admin	Admin		
Allied Telesyn	AT-8024(OB)	HTTP	manager	admin	Admin		
Allied Telesyn	AT Double	HTTP	root	(none)	Admin		

Now, this is an interesting site which gives you for each when vendor, each model, each version, each access type, the user name and password with all the privileges and with some notes. So, this is a very interesting sites the phenoelit-us dot org, you can go and find out for every device that you many of the devices you purchase, it is goes on the network, you can find the default user name and password. So, many times these many installations do not change these passwords, which leads to a very, very big security vulnerability.

(Refer Slide Time: 01:24)

Some Malware Includes Password Attack Code Targeting Poor Password Choices



Passwords used by the Conficker worm | Graham Cluley's blo

<http://www.sophos.com/blogs/gc/g/2009/01/16/passwords-conficker-worm/>

Passwords used by the Conficker worm

It's not possible to emphasise enough the importance of using sensible passwords on your network.

Not just on the areas of your network that you don't want your users to traipse through, but also on the default network shares that are present on installations of commonly used operating systems like Windows NT/2000/XP/2003.

One of the ways in which the Conficker worm (also known as Confick or Downadup) uses to spread is to try and batter its way into ADMIN\$ shares using a long list of different passwords.

As you can see in the list below, it relies upon computers using poorly chosen passwords such as dictionary words, "password", "qwerty" or sequences of letters or repeated numbers:

So, in some malware whose objective is not basically to crack password, but its objective is to go and do something more in the system. But, the way they get installed in the system is by targeting poor password choices. So, it will go and target different admin passwords, if an admin has a very weak password, then the malware gets installed in that system very easily using this weakness.

Once it gets installed into one system inside the network, then it can do many things within the network. So, malware whose primary goal is not to crack password, actually it goes and does a password attack to get administration privileges with which it can do much more damage to the system.

(Refer Slide Time: 02:30)

2. People Will Disclose Their Passwords

- Users will disclose their passwords in many different ways.
- For example, phishing exists because people can be “socially engineered,” into revealing their passwords.
- If you have users whom you’ve trained to be cynical, skeptical and defiant, they may (properly) refuse to reveal their passwords when receiving phishing attacks. Unfortunately, some groups (including higher education, unfortunately) have cultures which reward trust and unquestioning compliance when confronted with authoritatively presented demands:
Phisher: “Tell me your password immediately!”
User: “Okay, okay! It’s LetMeIn123, don’t ‘disable’ me!”

The next important problem or next very commonly noticed problem is the people voluntarily disclose their passwords. Sometimes, just an authoritative command I am going to disable your account, there is some problem with your account, there is some transaction which is missing, so some sort of intimidative, but authoritative statement by a phisher will make people bit worried and they immediately go and say OK this is my password, do not disable get this. So, this type of some authoritative statements and some intimidation, people do really gets scared and leak the password.

(Refer Slide Time: 03:24)

Source: <http://news.bbc.co.uk/2/hi/technology/3639679.stm>

Passwords revealed by sweet deal

More than 70% of people would reveal their computer password in exchange for a bar of chocolate, a survey has found.
It also showed that 34% of respondents volunteered their password when asked without even needing to be bribed.
A second survey found that 79% of people unwittingly gave away information that could be used to steal their identity when questioned.
Security firms predict that the lax security practices will fuel a British boom in online identity theft.

Security shock
The survey on passwords was carried out for the Infosecurity Europe trade show due to take place at Olympia in London from 27-29 April.
The survey data was gathered by questioning commuters passing through Liverpool Street station in London and found that many were happy to share login and password information with those carrying out the research.
As well as people simply telling the questioners their passwords or saying they would hand them over in exchange for some confectionery, a further 34% revealed the word or phrase they used when asked if it had anything to do with a pet or child’s name.
Family names, pets and football teams were all used by those questioned to provide inspiration for a password.
The survey found that, on average, people have to remember four passwords, though one unlucky respondent had to remember 40.
Many adopt very unsafe tactics to remember these login names. Some of those questioned simply use the same password for every system they must log on to.
Those that used several passwords often wrote them down and hid them in a desk or in a document on their computer.
Almost all of those questioned, 80%, said they were fed up with passwords and would like a better way to login to work computer systems.

Here very, very interesting news that comes out from the BBC, there are people who are ready to reveal the password in exchange of a chocolate.

(Refer Slide Time: 03:43)

Sharing Passwords

- Sometimes users will “voluntarily” share their password with others (even without chocolate!)... For example:
 - An executive delegates triage of her email to her administrative assistant; sometimes the administrative assistant is out sick or on vacation, so the executive's password is also shared with the backup admin assistant, and of course the password's never changed...
 - Supervisors may demand to know the password of subordinates accounts so that they can “access critical files” the subordinate may be working on, when the subordinate is sick or out on vacation.
 - Spouses often will routinely trust each other with their passwords, even though they shouldn't (sorry dear, we've been married 25 yrs but you simply dont need to know!)

There are many instances even without a chocolate people would voluntarily share the password. For example, an executive delegates gives password to his administrative assistant and someday his administrative assistant is sick, so they give, the administrative assistant gives to her admin assistant and so the password never gets change, because now three to four people know the password. So, this is a voluntary sharing and this is share just for convenience.

Now, a supervisor can actually call an employee and say tell the password, because I need to access critical file which is very important and since you really can't come , tell me the password and normally the subordinate obligesfor this . Spouses often will routinely trust each other with their passwords, even though they should not. For example, very rarely you can hear a statement from a spouse, sorry dear though we've been married for 25 years, but you simply do not need to know my password, very wrong very rarely we use this, get these type of statements.

(Refer Slide Time: 05:02)

Writing Passwords Down

- If password requirements are sufficiently complex, users have little choice but to record them if they're to have a hope of remembering all them.
- The yellow sticky note on the side of the monitor is the stereotypical password repository site (although others may favor the top drawer of their desk).
- This presents obvious risks if you have visitors (and even if you don't think you have visitors, you probably at least have custodial staff occasionally servicing your office)
- Carrying ones passwords in ones wallet is probably at least marginally more secure, although it isnt ideal. (You can read one person's take on the wallet as an option at <http://askthegEEK.kennyhart.com/index.php/2009/02/04/why-your-wallet-is-the-best-password-manager/>)

When your password becomes extremely complex, because your system wants it is rules, you tend to write these passwords, you put it on a yellow sticky note, almost in a notice board and what happens is that people who visits your office can note this, people who, custodial staff who comes in cleans your office can note this and the password can leak. But, there is one very interesting article, you can go to the web page, ask the key web page which talk about carrying ones password in ones wallet is probably or at least marginally more secure, although it is not ideal.

So, the article basically describes that if you keep your password in your wallet, then you do not store it anywhere you do not write it anywhere and once in 15 years or 10 years a careful person actually uses his wallet, give it to someone and that probability of you losing the password is much, much lesser than the probability that somebody hacks into your system where you have stored you password and gets it. So, sometimes writing password people argue that writing password and keeping it in a safe place is much more secure than having it in some electronic form.

So, another thing is that I do not want to remember the password. So, I make my E-mail client or my web browser to remember the password, so that I could automatically login. This has a lot of implications. Implication number 1 is that when you move away from the system, somebody else can come and login and start using your system and they can login as yourself, because you already stored the password and your system automatically logs in.

Why do we store all these passwords, because it is very difficult for us to remember. There are too many passwords around, passwords are ubiquitous. So, some solutions are suggested for this problem like we allow the users to store the password, so that they could automatically login.

(Refer Slide Time: 07:51)

Sharing Passwords With Any/All Users of Their Computer

- We all know people who routinely save their passwords in applications such as email clients, so that anyone who physically is at their computer can automatically "login" as them just by sitting down at their computer and starting the application with the saved password.
- Requiring a username and password to login to the computer, and/or consistently employing a locking screen saver, and/or using RF proximity cards (such as the "walk away security" cards from Xyloc), may help control that exposure, but saving passwords in apps is still an evil practice, and one that causes a lot of forgotten password issues ("I can't remember what I set my password to, I just saved whatever it was in my client").

But, then when they are not near the system, then the system automatically locks and then they come near the system, near in the sense say less than a meter away from the system, where they could clearly see the monitor, then only the system unlocks itself and this is achieved using some RFID type of card. So, there is... So, one of the interesting solutions is by Xyloc, you can go and visit the website which is called walk away security.

So, the user actually has a card and it is like a narrow proximity card and the software is installed in the system. So, when the user is near and it is coupled with the user, so when the user comes near the system, the system unlocks, but when the user moves away from the system, the system locks itself. So, though I have made a login and password being stored in the system, so when I login you automatically login to the system, my proximity will dictate whether the system should be lock or it should be unlock. So, this is a very interesting solution.

Another important problem would be that we tend to share password across multiple sides. One interesting thing is that when I want to forward E-mail from one, when I want to use the pop for consolidation of E-mail, I want I have several email accounts, but I

want to see the E-mail in one of such accounts. So, I send email to one server.

(Refer Slide Time: 09:50)

Another Form of Password Sharing: Password Reuse on Multiple Sites

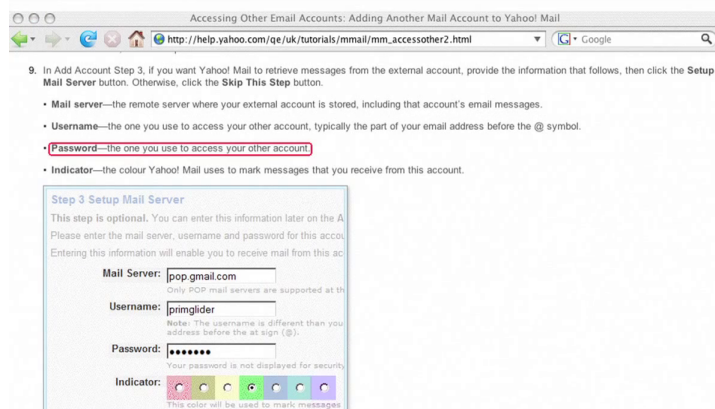
- Other users will share passwords across multiple systems, using the same password for critical, highly sensitive administrative systems, and for their online club account (and for <fill in the blank>). If I can crack their password on any of those systems, I'll be able to get into ALL of their accounts, including the highly sensitive ones.
- Sometimes users will even give login information, including passwords, to other sites to save and routinely re-use.

Classic example of this is email POP consolidation, where a free web email account may offer to use your credentials to periodically fetch other email by logging in to a remote system as you. Obviously, unless it is going to prompt you for your password each time it does this, it needs to know/save your unhashed (raw) password.

So, we use this pop consolidation and when we do this pop consolidation, we actually give to one of the E-mail clients the password in an unhashed raw form.

(Refer Slide Time: 10:03)

Example of POP Email Consolidation: Yahoo



Accessing Other Email Accounts: Adding Another Mail Account to Yahoo! Mail

9. In Add Account Step 3, if you want Yahoo! Mail to retrieve messages from the external account, provide the information that follows, then click the **Setup Mail Server** button. Otherwise, click the **Skip This Step** button.

- **Mail server**—the remote server where your external account is stored, including that account's email messages.
- **Username**—the one you use to access your other account, typically the part of your email address before the @ symbol.
- **Password**—the one you use to access your other account.
- **Indicator**—the colour Yahoo! Mail uses to mark messages that you receive from this account.

Step 3 Setup Mail Server

This step is optional. You can enter this information later on the **A**. Please enter the mail server, username and password for this account. Entering this information will enable you to receive mail from this account.

Mail Server:
Only POP mail servers are supported at this time.

Username:
Note: The username is different than your address before the at sign (@).

Password:
Your password is not displayed for security.

Indicator:
This color will be used to mark messages.

So, if we carefully look in to this, this is the pop E-mail consolidation of Yahoo and please see that password the one, who you used to the access your other account, so you are giving the password to some site in a completely unhashed raw format, the real password goes there.. So, this is one another way by which the password is shared.

(Refer Slide Time: 10:32)

Password “Safes”

- Some users, overwhelmed by password proliferation, don't even attempt to memorize all the passwords they need to juggle, they simply store them in an online encrypted password “safe” or password “wallet.” One example of such a product is KeePass (see <http://keepass.info/>).
- While this is convenient, obviously this is a case of putting all one's eggs in one's basket. Should the password safe or password wallet be compromised, you are likely to experience severe problems.
- I would be particularly wary of password safes which tightly integrate with browsers or other applications; if you use a password safe, I'd suggest using one that merely displays your username and password, at which point you can manually enter those values into applications as you deem appropriate.

So, there are also electronic wallets keepass.info please, you can visit this website. So, you just keep these password in these wallets, one example of such a product is keypass, while this is very convenient as you need not remember the password, but it is something like we are putting all the eggs into one basket. So, if the electronic wallet is compromised, then all your passwords are compromised.

So, this is one very important thing that we need to keep in mind, regarding using of a single point of storage for all your confidential information. Passwords necessarily need not be broken, the password can also be sniffed.

(Refer Slide Time: 11:33)

3. Passwords Will Be Sniffed

- In addition to people picking weak passwords, and sharing those passwords in various ways, passwords will also be captured, or “sniffed.”

Sniffed in the sense that when you are entering the password, somebody can find out what the password is.

(Refer Slide Time: 11:41)

“BUT ,We’ re 100% switched! We’ re Safel”

- From time-to-time I run into people who believe that they don't have any sniffing exposure because their network architecture is 100% switched, and in such an architecture network traffic shouldn't be visible to eavesdroppers (the way it would be on a shared network link).
- I would suggest that between arp spoofing, mac flooding, and mac duplication (among other methods), there's a good chance that a bad guy or bad gal can still arrange to see network traffic even in a fully switched environment.
- For those who insist on details, see for example <http://monkey.org/~dugsong/dsniff/> or <http://www.oxid.it/cain.html>
- **Switched networks do NOT provide sufficient protection against network traffic sniffing**

So, sniffing is not just on the network but let us first talk about network. When you login to the internet, the entire internet is not dedicated to you. The internet is availability you in a swctced form, there will be many users were using the internet. So, for some milli seconds the internet is given to you, then it is switched to somebody else and then it is switched to somebody else and then again in some fashion, it will come back to you.

So, when you are using the internet you are 100 percent switched, now when you are 100 percent switched how can somebody go and sniff some packet that is originating from your, sniff in the sense go and find the packets, analyze the packets later and find out the information, this is the entire procedure for sniffing from a network. But, how can one sniff if you are 100 percent switched network?

Because, you don't know which packet belongs to whom, but that is not actually the case, if you carefully look at arp spoofing, or mac flooding, mac duplication, among other methods. You can actually that there is a good chance that a bad guy or a bad girl can still arrange to see network traffic, even in a fully switched environment..

In the later courses we will deal about that this particular aspect in more detail, but what I suggest now is that you can go and see the websites, the monkey dot org and oxide dot it to get more details about how one can sniff in an 100 percent switched network. So, though your network is switched it does not provide sufficient protection against network

traffic being sniffed.

(Refer Slide Time: 13:53)

“BUT ,We have a VPN!”

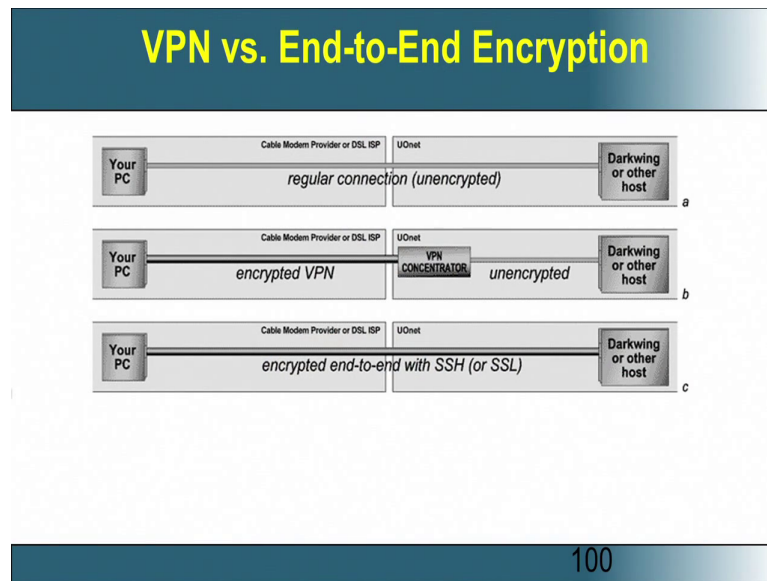
- Another technology that's often trotted out as a solution to the problem of sniffing is the use of VPNs.
- Virtual private networks provide an encrypted tunnel between the end user's workstation and the VPN concentrator. As far as they go, they're fine, *they just don't far enough*: VPN's are NOT “end-to-end secure,” they're only “one-end-to-VPN-concentrator secure”, and a bad guy can still attempt to sniff the VPN's traffic after it exits the VPN in clear text.
- Don't get me wrong, VPNs can help reduce the traffic exposure problem, and if you've got one, I'd certainly encourage you to still use it, you just need to recognize that you still have traffic that's exposed.
- VPNs are not (complete) protection against sniffing.

99

The next question comes we have this virtual private network, though I am switched I have the virtual private network and essentially I am sending data in an encrypted form through this virtual private network. This virtual private network, please understand does not give you an end to end security, if I am a client I am accessing a server, the encryption does not happens from the outlet of the client till the inlet of the server.

Actually the encryption happens from the outlet of the client to the inlet of a VPN concentrator which will be in the local LAN. After that point from the VPN concentrator to the server machine, the data goes in an unencrypted form and that is certainly a vulnerability.

(Refer Slide Time: 14:48)



As you see in this the three types of connection, the first connection is a regular connection which is completely unencrypted and people can sniff. The second one is a encrypted VPN connection, Virtual Private Network, but then the encryption goes only till the VPN concentrator, after the VPN concentrator they it is inside the LAN from that point to the server, it is still unencrypted. So, one can sniff the data internally. The next solution for it is that we start using SSH or SSL which gives you an end to end encryption.

(Refer Slide Time: 15:37)

“BUT We *DO* Encrypt End-To-End!”

- Excellent! I’ m delighted to hear that you’ re using ssh and SSL/TLS to minimize your exposure to sniffing on the wire! It is an important step!
- Unfortunately, you’re still not safe from eavesdroppers snarfing your passwords...

Let me give you just a few examples...

It is excellent if you use SSL, TSL, because this certainly minimizes your exposure to sniffing. But, this does not solve the problem in total, though on the network I can stop

sniffing by having this SSH and SSL type of protocols, still sniffing can happen locally and we will give some very interesting examples.

(Refer Slide Time: 16:06)

The image shows a screenshot of the KeyGhost website. At the top, there is a blue banner with the text "Hardware Keystroke Grabbers" in yellow. Below this, the website content is visible. The main heading is "KeyGhost USB Keylogger". The text describes it as a simple plug-and-play device for Mac and PC USB keyboards that records all keystrokes. It mentions a "NEW! TimeDate USB/HUB KeyGhost device released" and "NEW! High-capacity and compact Plug-style USB KeyGhost devices released." The website also features a navigation menu on the left with links for Home, Products, Reviews, Demonstration, Testimonials, Photos, Specifications, FAQ, Press releases, Download, Legal Disclaimer, Affiliates, and Distributors. There are logos for VISA, MasterCard, and QIDO. A central image shows two black USB keyloggers. The bottom of the page contains a disclaimer and a list of features: "KeyGhost USB Keyloggers work by recording USB traffic in hardware. There is no software to install to record or retrieve keystrokes on PC or Mac." and "Easy to use. Just plug KeyGhost to your keyboard and record all USB keystrokes typed on that keyboard. Can be connected regardless whether PC is turned on or off."

Somebody inserts a pen drive to copy some data from your system and at that point of time, you login to your internet to get the data and copy into this pen drive. This pen drive this USB drive need not just be a simple USB drive, it can be one of those keystroke grabbers which looks like an USB drives in which you can store files. But, at the same time it can grab all that you type on a USB keyboard.

So, simple way of getting a password is to come and ask something from the internet and so you please copy it on this pen drive and you insert the pen drive and you go to the internet, when you are going into the internet, the proxy may ask you for a password. Probably at the time you will also login to your Gmail or you login to your facebook and all these key strokes that happen from the point of insertion till the point of removal of that USB drive would be captured in the keystroke grabber.

(Refer Slide Time: 17:24)

Trojan' d ssh/sshd

- If I can get root on a box you login to, a cracker can install a trojan' d sshd, and having done that, he can then collect username/password pairs at his leisure, even if you consistently use end-to-end encryption.
- Think this doesn' t happen?

“The Stakkato Intrusions,”
www.nsc.liu.se/~nixon/stakkato.pdf

Another way by which SSH can file is that one can have a Trojaned SSH or SSHD the SSH Daemon and this can also leak the password, though I am doing end to end encryption, before the encryption happens I can leak the password. For some details on this, the Stakkato intrusions are very, very nice examples for this. So, in these two slides what I try to convey is though I have end to end encryption by the SSH and SCL protocol, it does not necessarily mean that my password is protected and it is not sniffed.

(Refer Slide Time: 18:19)

Shoulder Surfing and/or Video Cameras Watching Keyboards

- This can be a very low tech attack (as simple as your seat mate watching your fingers while you login to your laptop on an airplane or at a conference), or a very sophisticated high tech attack (perhaps using clandestinely-installed ceiling-mounted miniature wireless cameras focused on office workstation keyboards).

Either way, the bad guys can still “get” your password.

The other thing which is a very low tech attack is to just two shoulder surfing. So, when you start entering the data, when a person is logging in, you just go and sniff through his shoulder and you have some a little more hi-tech could be to have some video cameras,

which will be watching the keyboards and very miniaturized video wireless cameras are there, it could be take inside an office, work station keyboards and one can basically find out what password is being typed by looking at the image. And there are many, many malware which are targeting passwords including online banking credentials.

(Refer Slide Time: 19:09)

Don't Forget About Malware Targeting Passwords

- Passwords (including online banking credentials!) are a prime target for major malware infestations these days, including:
 - Clampi/Ligats/Ilomo/Rscan
 - Zeus/Zbot/WSNPOEM/NTOS/PRG
 - Koobface
 - Taterf
- Speaking of mitigation, why isn't everyone doing the right thing, and encrypting all their traffic?

So, some of them we are listed like Clampi, Zeus, Koobface, etcetera. So, speaking toward we are talking of speaking of mitigation of password threat, mitigation of sniffing of password, why isn't every one doing the right thing and encrypting all the traffic. We could have some access controls by which we may not sniff inside, but at the same time why cannot we just go and encrypt that traffic. But, the company says I would like to encrypt, but we just cannot, because then I cannot monitor what the user is doing.

So, now there is a very, very important question that we would like to ask before you end discussion. What is the bigger risk, if I have a bad guy who is sniffing your password, is it a bigger risk or go and encrypt all the data and but then having an employee who is playing around, checking out his favorite team on ESPN.

(Refer Slide Time: 20:25)

“We’ d LOVE to Encrypt, But We Just CAN’ T!”

- One such argument normally goes something like this...
 - A. We’ d love to use end-to-end encryption, but after thinking about it, we just “can’ t”
 - B. Why not?
 - A. If everyone were to use strong encryption we ourselves couldn’ t monitor what people do on the network -- all that traffic would be opaque to our monitoring systems!
 - B. But what’ s the bigger risk: having a bad guy sniffing your passwords, or having an employee who’ s playing around checking out his favorite team on ESPN, eh?

If you go and encrypt, certainly the bad guy cannot sniff your password. But, then employee can still go and visit ESPN without your knowledge, because you do not know what he is doing, because we have encrypted. On the other hand, if you do not encrypt the bad guy can sniff your password, but then you can find whether an employee is going to the ESPN site or not which one is a bigger risk, it is just for you to decide.

Thank you.