



MDRT

The Premier Association of Financial Professionals[®]

2008 Top of the Table Annual Meeting October 22-25, Austin, Texas USA

Title: Hacked!

Speaker(s): Ankit Fadia

Day: Friday, October 24, 2008

The Million Dollar Round Table[®] does not guarantee the accuracy of tax and legal matters and is not liable for errors and omissions. You are urged to check with professionals in your state, province or country. MDRT also suggests that you consult local insurance regulations pertaining to the use of visual material with clients.

© 2008 Million Dollar Round Table[®]

MDRT – Ankit Fadia – “Hacked!”

Moderator:

So how do you like hearing from one of our own? Thank you again, Bruce. How many of you out there have computers? A few of you. How many of you out there have information you might consider sensitive on those computers? How many of you think your computers are secure? A couple.

You're about to hear from an amazing young man I've gotten to know just a little bit over the last few months. He has an interesting experience at starting out at what he terms a job occupation known as a cracker. He converted from a cracker to a hacker.

Now a cracker is someone who might do some activities that, frankly, could be considered criminal. A hacker according to Ankit is now a good guy. He's helped our Federal government solve terrorism problems by cracking codes. He's got the ability to look into just about any of our computers, which is a scary idea, because the most valuable thing I think we all have is our information about ourselves and our clients.

I'd like you to sit back and get ready to be really opened up to new and exciting ways that you could be at risk, but more importantly how you can get an advantage over our competition by being prepared to not be cracked or hacked. Please give a warm welcome to Stanford student, author of best-selling books on the *New York Times* list and an amazing young man who is the age of my youngest daughter, Ankit Fadia.

Ankit Fadia:

Good morning everybody. Computer security is indeed an issue of global concern. It's an issue of concern not only in boardrooms across the globe, but even for the common users who use the Internet just for educational or entertainment purposes. I'm very sure that all of you sitting in this audience will agree with the statement that the Internet has really changed our lives. It's probably one of the best tools and inventions known to mankind.

But the biggest problem with the Internet is that as a user connects to the Internet until the time you disconnect, no matter what you do online, it's always being watched. So with the advent of the Internet in every single home and office, a lot of privacy concerns do come up. And I'd like to start today's event by asking all you certain questions which will make you realize how dangerous or how less private the Internet has made our lives.

How many of you have e-mail accounts, Hotmail, Yahoo, G-mail, or AOL? Stop using them. Hotmail, yahoo, G-mail and AOL put together probably has a few billion users across the globe. But did you know that each and every e-mail being sent or received by all those billions of users is actually being scanned for certain keywords. In other words, if you were to send an e-mail with the keywords “kill George Bush” then you are immediately blacklisted, a background check is done on you and if any links between you and any terrorist organization is found then obviously you are caught, otherwise you are let go free.

How many of you use Google.com, the best search engine on the Internet? Stop using it. Now Google is actually known to keep track of each and every user’s searching habits on the Internet. In other words, each time you connect to Google.com whatever you search for on Google.com gets fed into a database and is stored against your name or stored against your computer’s IP address.

How many of you use instant messenger, chatting programs like Yahoo! Messenger, MSN messenger, Skype, AOL and so on? Stop using them. Because if you remember on most all instant messengers have a small advertisement or banner and that small advertisement or banner is not only a fantastic

marketing tool or revenue stream, at the same time it's a great example of a spyware which keeps track of all your chat conversations and transmits certain keywords to the various chat companies. So that exactly how all the popup advertisements and banners are being displayed on your computer screens.

How many of you use anti-virus software? Like Symantec, Norton, McAfee, F Secure? Stop using them. In the underground community, it's a widely accepted fact that the anti-virus companies are themselves creating viruses, releasing them on the Internet, infecting all the systems and then selling you a counter measure. So purchasing anti-virus software you are indirectly helping an illegal industry to prosper.

How many of you use Microsoft Windows, XP or Vista? Stop using them. Because if you remember each time an error takes place on Microsoft Windows, XP or Vista there's going to be a small popup dialog box that gets displayed on the screen which will ask you whether you wish to report that error message to Microsoft or not. If you choose to not report that error message then things are fine, but for some reason if you choose to report that error message to Microsoft, then along with that error message a complete list of hardware and software installed on your computer gets transmitted to Microsoft.

One last question before I start with the presentation today. How many of you use the Internet? Stop using it. Because this brings me back to what I said earlier, no matter what you do online, no matter what you use the Internet for, every single move of yours is being watched, every single move of yours is being recorded or is being logged on some server or the other.

Now obviously it is not possible for any of us in this room to stop using the Internet. That is where your understanding, your knowledge, your experience regarding the most common tools, techniques and methods which are already known to the computer criminals, really comes into the picture. Because if everybody who uses the Internet understood the risks involved, because if everybody who uses the Internet understood how computer criminals work, then the Internet would be a much safer place to be.

So today's event is one such attempt to introduce all of you to the magical world of computer hacking or computer hackers. So the next time all of you use the Internet you'll be in a better position to protect yourselves and to fight the cyber criminals on the Internet.

On that note, I'd like to start with the event today. The format of today's event is, of course, going to be Power Point slides. However, the majority portion of

today's event is actually going to be live hacking demonstrations. For some of these live hacking demonstrations I'm going to require some brave volunteers from the audience as well. On that note, let me quickly start with the first Power Point slide of the day, which kind of tries to clear a small misconception that a lot of people have.

And the misconception is that whenever you talk about hacking or hackers immediately the image of a dark room and a teenage criminal sitting in one corner of the dark room comes to your mind. But in reality that is not at all true. In reality computer security has two types of people, one are the hackers, the other the crackers. Hackers are actually the good guys who work with the law enforcement agencies and try to protect the Internet. While on the other hand are the crackers who are equally knowledgeable but they misuse their knowledge to break into Web sites, crack into credit card numbers, release viruses, deface Web sites and create havoc on the Internet.

So hackers are good guys, while crackers are the bad guys on the Internet. So now that you know the distinction between hacking and cracking, let me start with the main part of the presentation today.

And just to warn all of you, today's presentation is divided into two different parts. In the first part I'm going to do a little bit of role play where I'm going to talk like a criminal, I'm going to act like a criminal and some of the things that I will be showing to all of you are going to be highly illegal. But do not get alarmed, I'm not trying to promote cyber crime. The whole idea is to take all of you into the minds of a criminal and show you how a criminal thinks because in the second part of the presentation, I'll switch roles and give you solutions that all of you can implement at home to improve your security and to protect yourselves.

But if you look at the screen you'll see a recent FBI intelligence report. And by simply looking at this chart, you can clearly figure out that the number of cyber crimes taking place worldwide has almost doubled in the last couple of years. So clearly cyber crime is a big concern for absolutely everybody who uses the Internet. What I've done now is I've actually listed out the top six most dangerous, most commonly found cyber security threats that all of us face on a very regular basis on the Internet. Today I will try to cover, if not all but at least, most of these threats or attacks.

The first kind of attack I want to discuss today is actually something known as "privacy attacks." Because all of us use the Internet on a daily basis without realizing the extent of damage or the extent of risk, the Internet introduces on a

daily basis into the privacy of our lives and into the privacy of our data. What exactly are privacy attacks? I'm going to start by sharing with you a couple of real life examples or case studies.

The first real life example is actually from Mumbai in India and this happened around three or four years back. There is a lady in Mumbai who lived in a typical Mumbai apartment which is a one room apartment. That lady was really obsessed with the latest technological gadgets. She used to buy herself a scanner, a Web camera, a surround system, the latest processor, a broadband Internet connection and so on. Now this lady also had this habit of chatting on the Internet for several hours together every single evening. One evening when the lady was chatting on the Internet, the person with whom she was chatting managed to hack into the lady's computer and after hacking into the lady's computer, the criminal managed to install a spying software called a "trojan" on the lady's computer.

After installing the trojan on the lady's computer, the attacker probably sitting in some other part of the world, remotely, secretly managed to use the trojan to switch the lady's Web camera on. So from that moment whatever happened in the lady's apartment, which I like to remind you is a one room apartment in Mumbai, was actually being broadcasted live on the Internet 24 hours a day. The lady had absolutely no knowledge that something so terrible was

happening to her. Life continued normally for a few months after which the lady went for a job interview. At that job interview the person who was interviewing the lady, he immediately remarked that “Oh, I will obviously give you the job, I see you every day on the pornographic Web site, why would I refuse?”

That’s the time the lady realized that, wait a minute, something seems to be wrong. She rushed back home, disconnected the computer from the broadband, always on high speed Internet connection, complained to the police, investigations were carried out, but quite predictably the attacker was never caught. And in the meantime the lady probably never wanted to use the Internet again.

And if that case study does not scare all of you enough, there is another case study which I’d like to share with all of you, which is from the government sector.

A few years back, NASA successfully completed a spaceship launch. And a few weeks after the successful completion of the spaceship launch, what NASA officials realized was that a criminal who was later found out to be an 11-year-old boy from Russia. I repeat, the criminal was an 11-year-old boy from Russia.

He had managed to break into the NASA systems and sitting in his bedroom or living room in Russia, he took complete control over the NASA systems and then used them to change the direction of the spaceship in space.

By the time the NASA officials realized what was going on, they had already lost thousands of dollars as far as space food was concerned. So clearly cyber crime is a problem that affects not only individuals like the Mumbai lady, but also affects big organizations like NASA.

I'm very sure that at this point in time most of you in this room are probably asking yourselves two main questions. Number one, is it really possible to use the Internet to switch somebody else's Web camera on? And I'm sure many of you would love to be able to do that. And secondly, is it really possible to use the Internet to change the direction of a spaceship in space?

Unfortunately or fortunately, the answers to both these questions is a big "yes." That "yes" absolutely anybody with some basic computer hacking knowledge can actually do that and in the next five or seven minutes we'll actually see on the big screen as to how all of you can do it as well.

So let me quickly move on to the next slide which is of a very interesting software hacking tool, which is something known as a trojan. So what exactly is a trojan?3

It's no longer something that you can buy at the gas station. It is also something that can be used to hack into somebody else's computer. So trojan is basically a RAT, or a remote administration tool, that gives an attacker remote control or remote access to the victim's computer. In other words, imagine a scenario where I'm the criminal, you're the victim. If I'm able to install a trojan on your computer, then using that trojan I can practically control all aspects of all hardware and software on your computer.

For example, if you're trying to move your mouse towards the right, I can control your mouse and make it move towards the left. If you're trying to type A, B and C, I can type P, Q and R on your computer. If you're listening to music, I can increase the volume, decrease the volume, change the song that you're listening to, open the CD tray, close the CD tray, download files, upload files, delete files and maybe even format your entire hard disk. Essentially once a trojan gets installed on the victim's computer, the attacker or the criminal can do absolutely anything that he wants to do on the victim's computer.

At this stage I like to give the first live hacking demonstration of the day. I'm going to show you one of the most powerful trojans there are available on the Internet. The name of the trojan which I would like to show to all of you is a trojan known as NetBus. So I'm going to quickly open up the NetBus trojan on my computer. This is what the NetBus trojan looks like. The way it works is, in this space provided, you need to enter the victim's IP address. Obvious discussion over here is how are you going to find out the victim's IP address? Now today since we have limited time, I won't be able to get into how you can find out somebody else's IP address, but if you e-mail me, I'll be happy to send you a 10 page, step-by-step tutorial on how you can find out somebody else's IP address.

So at this stage let's assume that all of you already know the victim's IP address. And of course the victim could be your competitor, it could be a customer, it could be a client, it could be anybody. So once you have the victim's IP address, you need to enter it in the space provided and for the purpose of today's demonstration, I've infected my own laptop with a trojan. I'm going to enter my own laptop's IP address and click on the "connect" button.

As soon as I click on "connect," in the status bar it says connected to the victim's computer. Now that I've connected to the victim's computer, I can start

using all these various buttons and options to remotely do things on the victim's computer.

For example, the first option is a very interesting option known as the open CD-ROM option. I'm going to try and show this to all of you. This is where my CD tray is if you look at my laptop and if you notice all I'm going to do is click on the "open CD-ROM option" and hopefully within a few seconds, the CD door opens. And this can be done across continents, across countries and trust me when the victim notices that his CD tray is opening or closing on its own, he or she is going to get really, really scared.

Not only that, there's another very interesting option known as the "swap mouse button." As soon as the attacker clicks on the swap mouse button what happens is on the victim's computer left click becomes right click and right click becomes left click. There is a message manager available as well. Using the message manager it is possible for you as an attacker to display pop-up text messages on the victim's computer screen. So all you have to do is click on message manager and in the space provided you can type in absolutely any message that you want to display on the victim's computer screen. I'm going to type something like I am watching you. Click on send message and within a few seconds if you look at the screen, the text message that I just typed has now been displayed on the victim's computer screen. And of course the victim

will have no clue as to who is actually sending these messages onto their computer screen.

A very good suggestion, which I like to give, is the first time all of you try out the message manager option, try to do it in such a manner that you have physical eye contact with the victim. Because what happens is when that message pops up on the screen, the kind of facial reaction, expression the victim is going to have are going to be very, very interesting.

Now on a more serious note, next comes one of the most dangerous options. And it's an option known as the "screen dump" option. The way the screen dump option works is, imagine a scenario where your competitor or the victim is in some other part of the world. Now wouldn't it be great if you had a live video feed of your competitor, or of your victim's computer screen. So basically whatever the victim can see on his screen, you can actually see that or spy upon that on your computer screen as well. That's exactly what the screen dump option does.

All you have to do is click on screen dump and the trojan will take a photograph of the victim's computer screen and display it on your computer screen. So all presentations, e-mails, documents, chat conversations, bank

account details, credit card information, anything that gets displayed on the victim's computer screen can be spied upon using the screen dump option.

Next comes one of my all-time favorite options. It's an option known as an exit Windows option which allows you to remotely shut down the victim's computer, power if off, log off the user and even restart the victim's computer all remotely through the Internet.

The next option is another very interesting option. It's an option known as a "syntax button." Imagine the scenario wherein the victim is typing an important e-mail to his client or maybe typing out a contract or a document and what if you as an attacker wanted to add your own sentences or text to that e-mail or document. All you have to do is click on syntax, type in absolutely anything that comes to your mind, click on "OK" and as soon as you click on "OK", all the text that you just typed into this dialog box will become a part of the e-mail or document that the victim was working on at that given point of time. So you've just got to be creative and you can actually cause a lot of damage to the victim using the syntax option.

Now before I show you the next option, I'd like to actually take a couple of minutes to invite a brave volunteer from the audience. I'm looking for a

volunteer who either has a Hotmail, Yahoo!, G-mail or an AOL e-mail account. Can I request you to come up here please? What kind of e-mail account do you have? AOL. So our brave volunteer has an AOL e-mail account. What I'm going to do is I'm going to open up my browser and I'm going to connect to the AOL Web login page. Go ahead and log into your e-mail account. I want to make sure he entered the correct username and password so let's wait for his e-mail account to get logged in.

As you can see he entered the correct username and password. Before I continue, just to make things a little bit more exciting, I actually like to invite the chairman of MDRT to the stage for the same demonstration. Mark Dorfman, would you like to volunteer for the same demonstration? Do you have a G-mail, Yahoo!, AOL e-mail account? Since our second volunteer has a G-mail account, let me quickly open the login page for G-mail. I'm going to request a second brave volunteer to go ahead and log into his G-mail account. That's a very long password. Not working, maybe at next year's conference you'll volunteer and make sure you remember the password.

So we have a brave volunteer who is kind enough to volunteer and brave enough to log into his AOL e-mail account. Now what if you wanted to try and find out what his e-mail account password is? This does not work each and every time so I'm going to keep my fingers crossed and let's hope for the best. If

I go back to the trojan, let's see what the trojan did. The trojan has actually recorded absolutely all keys that were pressed on this computer, so our brave volunteer typed in his username and his username got recorded, then he typed in his password and his password also got recorded. Is that the current username and password? All right, thank you. You can change it later. You want to change it now? And what he does not know is that while he's changing the password, he needs to type the new password in so the trojan will record the new password as well.

The whole point to this demonstration was to show you that once a trojan gets installed on the victim's computer, you can use that trojan to record absolutely all keys that are being pressed on the victim's computer. And when I say all keys, I'm of course referring to all usernames and passwords, credit card numbers, bank account details, e-mails, documents, absolutely anything that gets typed.

Next comes another one of my all-time favorite options, it's an option known as the go-to URL option. Imagine a scenario that the victim is in the middle of an important presentation like this one and what if you as an attacker wanted to display an inappropriate Web site of your choice on the victim's computer screen? So all you have to do is click on go-to URL, type in an inappropriate Web site address in the space provided, click on "OK" and as soon as you click

on “OK” that Web site will automatically popup on the victim’s computer screen. I’m obviously not going to show that Web site, sorry to disappoint some of you. But the whole idea is you can actually cause a lot of embarrassment or put the victim in a very sticky situation using the go-to URL option.

There are a bunch of other interesting options as well. There is a file manager using that you can download and upload files from the victim’s computer and there’s a sound system option. If the victim has a Webcam or a microphone installed, the attacker could click on the record button and record all audio and video from the victim’s rooms. So that pretty much takes invasion of privacy up to the next level.

So as you can see, trojans are extremely dangerous tools and I’m pretty sure many of you are now wondering as to where you can get a trojan from. That absolutely best thing about trojans is the fact that most trojans are available as a free download on the Internet. But the problem is if you do a simple Google search, you will probably not be able to get down to the trojan because Google has a bad habit of blocking access to those Web sites that allow trojan downloads. So let me instead give all of you a Web site from which all of you can easily download a trojan. And the Web site address is <http://www.beckettstrongsecurity.org> and at this stage while all of you are writing down the URL, I’d also like to recommend some other powerful trojans

to all of you. One of the most powerful trojans by far is, of course, NetBus. There's another very interesting trojan known as Back Orifice, Sub Seven and Girl Friend. And all of them are available as a free download on this Web site. Just click on "search" and type in the name of the trojan that you wish to download, as simple as that.

So as you can clearly see trojans are extremely dangerous tools and at this point in time I'd like to move on to the second most commonly found, second most dangerous attack on the Internet which is something known as "e-mail spoofing."

E-mail spoofing, like the name suggests, is basically the art of being able to send a fake e-mail from somebody else's e-mail account without knowing the password. In other words, using e-mail spoofing it is possible for any of your competitors to send an e-mail from your e-mail account to all your employees, to all your customers, your clients, your partners, investors and the media worldwide. And the e-mail would look very real, very authentic.

I'd like to give you a demonstration that shows you how easy it is to carry out e-mail spoofing on the Internet. There are thousands of ways in which e-mail spoofing can be carried out on the Internet but the easiest way is to simply start your browser and connect to one of my all-time favorite Web sites on the

Internet. I'm going to quickly bring that Web site on the screen. The Web site address is anonymiser.n/fake-mailer. The way it works is on this part of the Web page there is an online form and e-mail spoofing is as simple as filling out this online form. In this example what I'd like to do is send an e-mail from BillGates @microsoft.com to a friend of mine offering him a job at Microsoft.

So in the first field which is the sender field, I need to type in the e-mail address from which I'd like to send this e-mail. So I'm going to type billgates@microsoft.com, in the second field I need to type the recipient's e-mail address. And just to make things a little bit interesting, I'm going to send this e-mail to myself so I can actually open the e-mail from Bill Gates and show it to all of you on the big screen. So I'll send it to my G-mail account and I do remember the password of my G-mail account. The subject is job proposal and finally in this field I can type the body of that e-mail as well. I'm going to type something like, "Dear Ankit, heard a lot about you from my representatives in Austin. Would you like to work as part of my personal technical advisory team here in Redmond? Of course a seven figure U.S. dollar salary will be offered to you. Please call me at your convenience on my cell phone. Thanks a ton. Warm regards. Bill."

And when you're ready to send this e-mail all you have to do is click on send and hopefully a few minutes later when I check my e-mail account I will

probably will have received an e-mail from billgates@microsoft.com offering me a job at Microsoft. So let's quickly log into my G-mail account and let's see whether I actually do have an e-mail from Bill Gates or not. And if you look at the screen, the first e-mail is indeed an e-mail from Bill Gates. It looks very real, very authentic. It says sent from Bill Gates, less than a minute back, from is billgates@microsoft.com, sent to me, subject is job proposal and that body is exactly what I just typed.

Imagine a disgruntled employee or a competitor or anybody in the industry who wants to bring you down or bring your company down, they just have to go to this Web site and send a spoof e-mail from your e-mail account to maybe spoil relationships or maybe just cancel an order or just cause miscommunication.

So e-mail spoofing is extremely dangerous. Unfortunately, there is no countermeasure available. There's nothing that we as Internet users can do to protect ourselves from e-mail spoofing.

At this stage I would like to quickly move on to the third demonstration of the day. The next demonstration is actually a real life example. A real life cyber crime investigation case that I've personally been involved in.

After the September 11 attacks, the U.S. Government intercepted a few encrypted e-mails sent by the Al Qaeda terrorist network. So you can imagine how important those e-mails were. First of all they were intercepted immediately after September 11. Secondly, they were sent by the Al Qaeda. But the problem was when the government opened those e-mails the only thing they found was photographs of popular actresses, actors, celebrities, political figures, sports personnel and so on but the actual e-mail was completely blank. So the government had a bunch of e-mails that had photographs attached to them but the actual e-mails did not have any text. So the government had no idea as to what was going on.

So they contacted a bunch of different consultants to try and solve this case. Even I was contacted, and to be very honest, for the first two or three weeks I had no idea as to what was going on. But sometime in the middle of the fourth week what I soon realized was that this is a classic example of a very interesting technique known as stagenography. Now stagenography is basically the art of taking a text message (it could be absolutely any message) and hiding that text message inside a photograph, audio file or a video file. In other words, when all of you look at this photograph it looks quite innocent but in reality this photograph contains some sort of hidden message or some sort of hidden data.

I'd like to show you a demonstration which shows you how easy it is for all of you to go back home today and start hiding data inside photographs, audio files or video files.

The name of the software you need is known as S-Tools. S-Tools is available as a free download over the Internet. Once you download S-Tools, the way it works is, let's imagine for a moment that I am a terrorist and I'm planning a major terrorist attack. And in relation to that attack I want to send an important e-mail communication to my terrorist Kaleg. And the message that I want to send is, "Bomb the Parliament Building today on 24 October at 9 p.m."

If I was to send this e-mail as a regular e-mail, then anybody who intercepts the e-mail will obviously know what the message means. So instead, what I'd like to do is I'd like to actually take this message and hide it in absolutely any photograph of my choice and I'm going to use George Bush's smiling photograph for this particular demonstration. In order to actually do that, first of all I need to start the S-Tools software and this is what the S-Tools software looks like. Once I've started the S-Tools software, step number one would be to drag the photograph inside which I want to hide the data. So I just drag this photograph onto the software.

Step number two would be to drag the file that I want to hide inside that photograph and as soon as I do that, the software will ask me to choose a password. I can choose any password of my choice. Reenter the password, click on “OK” and within a few seconds if all of you look at the screen the software creates an identical copy of the photograph. Can anyone in the audience point any differences between the two photographs? The human eye cannot differentiate between the two photographs.

The only difference is that this photograph on the left does not contain any hidden data, so I'll go and close that. While this photograph on the right contains the hidden data. So now I can right click on it, save it with any filename of my choice, attach it to an e-mail, send that e-mail to my terrorist Kaleg. Anybody who intercepts the e-mail will only see the smiling photograph of George Bush, but when my terrorist Kaleg receives this e-mail all that he or she needs to do is drag this photograph back onto the software, right click on the photograph, click on the, enter the same password that was used at the sender's end, click on “OK.” And hopefully, if I remembered the password, the secret file as all of you can clearly see on the screen is now ready to be revealed. I'm going to save it on the desktop and open it for you. It “Bomb the Parliament Building today on 24 October at 9 p.m.” As simple as that.

What is really scary about this demonstration is the fact that this was the level of sophistication of communication channels for the terrorists way back in 2001. And you can imagine how advanced or complex the communication channels of today have become when we are in 2008. So unfortunately, the bad guys or the terrorists are always one or two steps ahead of the good guys in the war of cyber terrorism.

If you notice most of the demonstrations that I've given until now have all been simulated demonstrations on my laptop. So for the first time today what I'd like to do is be a little more adventurous and a little bit more brave, venture out in the wild and maybe hack into some real live Web sites that actually exist on the Internet. But before I continue, a quick warning for all of you, do not repeat what I am going to show you next on your own because believe it or not in the next demonstration, I will be breaking the cyber laws. I will be breaking into a real life Web site that actually exists on the Internet.

When you do this you could be traced back, you could get caught as well. The reason why I'm not afraid of getting caught. There are two big reasons, first of all the Internet connection right now has been arranged by MDRT so legally MDRT is responsible for everything that happens. And secondly and more importantly, I'm flying back to San Francisco on the 3 p.m. flight. So when the

law enforcement agencies get to this hotel venue, I will probably already be on my way back to San Francisco.

But if any of you do this you have to be extremely careful, you could get into a lot of trouble.

What I'm going to do in the next demonstration is I'm going to break into two different Web sites from two different parts of the world and each of those two Web sites are from two different industries. The first Web site is going to be a telecommunications provider and the second Web site is going to be an online jewelry Web site. Both of these Web sites are from two completely different parts of the world. The first Web site, I can see a lot of Indian people in the audience and the first Web site is a Web site that everybody from India can easily relate to, it's the Web site of India's largest telecommunications provider, which is BSNL. They are close to 20 to 25 million customers nationwide. Think of BSNL as India's version of Cingular.

They have a Web site wherein you can pay your bills online and things like that. Now the problem is for the last two or three years I've been suffering from a major disease and the disease is the fact that I do not like to pay for things. If you also suffer from the same disease, I think the next two demonstrations are

going to be very, very interesting for you. So the first is BSNL and the second is a Web site from the U.S., it's an online jewelry Web site so basically if you have a credit card you can purchase a diamond bracelet, diamond necklace, diamond pendant and so on. But of course I'm going to show you how you can purchase all the same stuff without using your credit card as well.

For the first example, which is Bharat Sanchar Nigam Ltd. (BSNL). I'm actually not going to use any software. The only thing that I will be using will be my Internet browser. So I'll open up my browser and open the BSNL login page on the screen. Give me a minute while the Web page gets displayed on the screen. If you look at the URL, it does say BSNL.com., in so I'm not trying to fool anybody here. This is the real Web site of BSNL. However, there is a slight problem. The problem is asking me to enter the administrator username and password. Obviously, I do not know the administrator username and password of BSNL. So we have a problem over here. However, let's try and solve this problem. Since I do not know the administrator username, a very good guess would be admin because, believe it or not, system administrators worldwide are not very creative and cannot come up with better usernames. So they continue to use the default username which is admin.

Next comes the password problem. Since I do not even know the password of the administrator of BSNL, what I'm going to do instead is I'm going to open my

hacking toolkit and from a hacking toolkit I'm going to copy and paste this magic code into the password field. This is not the correct password, it is not the real password, I just copied that and I'll paste it into the password field and I'm going to click on the submit button, keep my fingers crossed and within a few seconds hopefully the complete customer database nationwide will get displayed on the screen.

And now that I've managed to do this, there are a couple of things that I can do with this Web site. At the end of this month when I receive my telephone bill, I'll obviously not pay that bill. Next month I'll receive another reminder, I'll not pay my bill even then. Finally after the third month, they will go ahead and send me a final notice even then I'll not pay my bill. So BSNL will have no choice but to disconnect my telephone or my cell phone connection and when they do that always remember they're not actually taking the handset away from you. They're not actually removing the cell phone towers or the wiring from your house or from the place that you're at. The only thing they're going to do is at the backend, they're going to put your name into a database which saves a list of rejected users.

So, since my name is now in the list of rejected users, all I need to do is hack into this Web site, find my name in this database and then simply click on the approve button and my telephone or cell phone connection will start working

all over again. As simple as that. And if I continue to do this every three months, I would have guaranteed myself a lifetime of free cell phone and telephone access on my connections.

Now that was an Indian Web site. I'm sure that many of you are probably arguing that this does not really help all of you.

So let's quickly move on to the online jewelry Web site. The Web site address is www.sendjewelry.com and I'm going to quickly open it up on my browser and usually, of course, you need to enter your credit card information. You need to chose the piece of jewelry that you want to purchase and you need to enter a delivery address. And within maybe a week or so the piece of jewelry would get delivered to your address.

However, what if you wanted to hack into this Web site? All you've got to do is: in the URL, I'm going to type sendjewelry.com/admin and press enter. It will again ask me for the administrator username and password. And obviously the username is going to be admin and the password is going to be the magic code. Once I click on submit, I'm going to be able to hack into this Web site and all the orders that have already been placed by existing customers will be displayed on the screen.

All I now need to do is click on “modify” or “edit” and change the delivery address of any piece of jewelry that I really like so that it gets delivered to the address of my choice. So now what happens is somebody else’s credit card gets billed for it but the piece of jewelry gets delivered to the address of my choice. And when you do this, obviously you should never get it delivered to your real address, that’s exactly how you’re going to get caught. Get it delivered to your neighbor’s address and pick up the package when the package arrives at your neighbor’s place.

I’m very sure that many of you also are curious to know as to what really happened over here, what is that magic code and what does it actually really do. Now the magic code is not the real password, it’s an example of something known as “SQL injection” and the magic code is now being displayed on the screen. What it basically does is, there is a security vulnerability on a SQL database that is used by thousands of Web sites worldwide where in the password field if I enter this magic code, I will be logged in as the administrator even though I do not know the correct password.

What it does is it bypasses or skips the authentication step so I don’t need to enter the correct username and password and I’m logged in automatically.

There are thousands of such similar Web sites which can be hacked within a matter of a few seconds.

I think we have time for one more demonstration. After which, I will switch roles and give you solutions that you can implement. For the next demonstration, I'd like to once again invite a brave volunteer from the audience. I'm looking for a volunteer this time who is carrying a credit card with them. Please come up. While he's coming up, a quick question for all of you. How many of you use the cut and paste or the copy and paste option? I think everybody uses that, right? So after the next demonstration you'll probably never want to use cut and copy again. And what I'm going to do is request our brave volunteer to go ahead and type in your 16 digit credit card number. I'm not going to look at the screens but later I will tell you what those 16 digits were and feel free to copy his credit card number down if you want.

Now, can I request you to highlight those 16 digits? Just press control and A, that's select all. Press them together. All right, now press control and X, that's cut. Thank you. So what I'm trying to simulate over here is a classic example where an average user cuts or copies important data. Once you cut and copy important data you will paste it somewhere and after you've pasted that data, most people tend to forget about it. And once you have forgotten about it, you'll continue with your Internet activity. And if that happens, the next time you

visit a Web site, it could be absolutely any Web site on the Internet, simply look at what happens.

I'm going to quickly open a Web page on the screen and just look at the text in yellow. That's his credit card number. So the point I'm trying to make over here is once you cut or copy data it gets stored in the temporary memory on your computer which is the clipboard. And the next time you access any Web site on the Internet that remote Web site which could be in some other part of the world, has the capability of reading data from your clipboard.

Now think about all the sensitive data that all of you cut or copy on a daily basis which all of your employees cut or copy on a daily basis without even thinking twice about it. So all that data is at risk. Thank you.

I think I've shown you a bunch of different demonstrations and the whole idea was to show you how a criminal works and how easy it is to break into Web sites, servers and e-mail accounts. Now, let me switch roles and I'd like to actually give to all of you the best security practices which all can be implemented at home and at your workplace that will increase the amount of security awareness and give you up to 95 percent security. There is nothing

that's 100 percent security but I think the whole idea is to increase the amount of security that exists in your network, in your organization.

I like to call it the six best security practices. First, I will give you countermeasures or solutions for the home environment and then I'll modify them and tell you what you need to do in the corporate environment as well.

First of all, you need to install a firewall on your computer. Most people think that firewalls are extremely expensive and extremely technical. But in reality that is not at all true. There is a very good firewall which I would like to recommend to you, it's called Zone Alarm. It's available as a free download on the Internet. You just do a Google search and it allows you to download Zone Alarm onto your computer. Basically a firewall will monitor all activity that happens on your computer and when it notices that some sort of malicious activity is going on, it will block that and notify you that something malicious is going on. That's the first countermeasure.

The second countermeasure is that you need to install an anti-virus software on your computer. I think most of you already have an anti-virus software on your computer, but what is more important is you must update it on a weekly basis. You have to understand security is a very dynamic industry where

everything changes every single day. There are new viruses, loopholes being discovered on the Internet on a constant basis so you need to update your anti-virus software at least once a week.

You need to also install an anti-spyware software on your computer. Most people only have an anti-virus, but you need to also have an anti-spyware software on your and a very good anti-spyware software which I like to recommend is a software known as Spy Sweeper or Prevx. Unfortunately Spy Sweeper or Prevx is not free. You've got to pay \$30 annual license fee for either of the two, however, if you don't want to pay that annual license fee we need to talk offline and I can tell you how you can actually use it for free as well.

Actually, let me just go ahead and tell all of you, if you want to crack any software, for example, if you download a software from the Internet and realize that it is a trial edition software that expires in 15 days or 30 days, afterwards you have to pay for it. If you want to convert the trial edition software into a full edition software then all you have to do is start your browser and connect to any of the following Web sites: cracks.am, cracks.ru, astalavista.box.sk. These are basically software cracking Web sites. They behave like search engines, so you have to type the name and the exact version of the software that you wish to crack, click on search and in the results you'll get sort of registration keys that you can use to convert your trial edition software into full edition and

you'll never have to pay for it again. So that's the third countermeasure. Always you need to update your anti-spyware on a weekly basis as well.

The fourth countermeasure is you must update your operating system which is Windows, Mac, Linux, doesn't really matter which one you're using, you need to update it every 15 days. When I say you need to update your operating system every 15 days, what I'm referring to is you've got to click on start, all programs and then click on "Windows Update." Make sure you're connected to the Internet. What this will then do is connect to the Microsoft Web site and download security patches that will give you a higher level of security on your operating system. And just to let all of you know, the updating on the anti-virus, anti-spyware and your operating system can be an automated procedure as well. You can automate it in such a way that any given point of time, any time of the day or week, it will automatically connect to the Internet and download the latest updates.

Next, you need to also install a key scrambler on your computer. There are thousands of key scramblers available on the Internet. What a key scrambler does is it will remember, in the trojan example where we had a volunteer log into his AOL account and the trojan recorded all the keys that were typed. If I had a key scrambler on my laptop, the key scrambler would have scrambled the keys in such a way that the trojan would not be able to record the correct

password. Just do a Google search and there are thousands of key scramblers that you can download off the Internet.

Now these are the six basic security practices that all of you need to implement. I would like to add a few optional security practices. Nowadays, a lot of people have wireless networks at home. Basically, your house is wireless, you can sit in any part of the house and access the Internet. If you have such a wi-fi or wireless network at home, it is a big security risk. Because if I'm a criminal I could actually be parked across the street from your house, I could hack into your wireless network, install a data sniffer and record all communication that comes in and out of your network. So if you want to prevent that what you need to do is you need to make sure that WEP, which is wireless encryption protocol, or WPA keys are enabled on your wireless network. What this basically means is when you connect to your wireless network, if you're asked to enter a password then you don't need to worry. But if you're not asked to enter a password, then it probably means it is not a secured wireless network and it can easily get hacked.

Another optional countermeasure is anonymous surfing. In other words, if you want to protect your identity on the Internet, if you want to protect your IP address and if you want to be anonymous on the Internet then instead of directly visiting Web sites on the Internet, for example, if you want to connect

to Google, normally you start your browser and type Google.com. But the problem in this case is Google knows who I am. On the right inside top corner, Google also displays my e-mail address and Google also knows that somebody from Austin in Texas in the United States just accessed the Web site. And now whatever I search for on Google.com will get recorded in a database against my name, my age, my exact street address and so on.

If I wanted to connect to Google.com anonymously then all I need to do is instead of directly connecting to Google, I need to first connect to a Web site known as Cooltunnel.com. Cooltunnel.com is basically like a proxy server that protects your identity and protects your IP address on the Internet. Once you connect to Cooltunnel.com you have to scroll down and in the space provided you can type in absolutely any Web site address that you want to visit anonymously, safely and securely. I just typed in Google.com and I want to click on browse and within a few seconds Cooltunnel.com will connect to Google.com and display it on your computer screen. And as you can clearly see, now my e-mail address is no longer displayed on the screen. So it's completely anonymous, it's completely secure.

If you have some criminals in the audience and if you want to commit a crime and never get traced back for it, I don't recommend that you use Cooltunnel.com. Instead, I like to recommend a Russian Web site which is

Anonymizer.ru and the way it works is, on the right inside top corner in the space provided, you've got to type in the URL of the Web site that you want to hack into or access anonymously. I just typed in Google.com and then you need to click on whatever looks like to go button. You don't need to know Russian for this. And within a few seconds Anonymizer.ru will connect to Google.com, fresh the Web page and display it on your computer screen. Google thinks that somebody from Russia is trying to access the Web site, but in reality I'm accessing Google from Texas in the United States. And if you look at the screen, Google is displayed in the Russian language, so that actually proves to you that this thing actually works.

So these are the sort of eight countermeasures which I like to recommend for the home environment. For the corporate environment, there are a few modifications. Instead of Zone Alarm I would recommend a firewall called Checkpoint or a Cisco based firewall. Anti-virus, anti spyware, updating your OS, key scrambler, wi-fi connection, anonymous surfing, all of that is the same. I'd just like to add one more countermeasure. It's not an option, it's a compulsory countermeasure. You need to install an IDS or an IPS system. IDS is basically intrusion detection and IPS is intrusion prevention system. What this will do is it will monitor all traffic and block all attacks into your network and finally you've got to have strong security policies which means you need to restrict user and file access in your network.

For example, somebody in your marketing department does not need to access the technical information in your organization. None of your employees actually need to be allowed to use instant messengers like MSN, Yahoo! or AIM because it causes inefficiency, it's also a big security loophole.

I think we're pretty much out of time. I hope all of you enjoyed today's presentation and thanks a lot for giving me this wonderful opportunity. Thank you.