

“Tech Talk” TV Show

Techno Identification Episode

A young man opens a lap top. The image on the screen is a blue faced head who says, “Hey! Who are you? What are you doing with my keys? You know, I don’t just do what anybody wants! I need to have some kind of an identification. I don’t know who you are. You could be anybody. But I need to know you. Got a name? You got a number? You got an I.D.? I am not doing anything ‘til you tell me who you are.”

Tech Talk intro plays

Hello and welcome to Tech Talk from the University of Minnesota; your source of information about the technology that surrounds us every day. I am your host, Susan McKinnell. You know that computer at the beginning of this show had a point, but thankfully we’ve never been verbally accosted by our electronic assistant as was that poor person. But how does a computer know who you are and why is that important? That’s what today’s program is all about, techno identification. Some of the terms you’ll hear include *biometrics*, *CAPTCHA*, *SSL*, and *Virtual Private Network*. Chris Bongaarts is a systems programmer for the Office of Information Technology at the University of Minnesota. He is also part of the Internet Services group that is responsible for, among other things, authentication services. Thank you for being here today, Chris.

Chris: I’m glad to be here.

Susan: I know the way my computer identifies me is by a password. Can you tell me a little about passwords?

Chris: It is probably the most prevalent form of authentication technology that is out there right now and it has been in use for a very long time. It has very well understood properties so we know how well they work, we know what there problems are (and there are some problems.)But they are generally easy to deploy and easy to deal with in general.

Susan: Okay. I know that a lot of people aren’t that concerned with keeping, say, their email password, or for that matter, their computer password secure. “My computer is in my basement at home. Who is going to bother trying to...unless someone is breaking into my house or something? Are they going to sit there and play with my computer?” Why do people need to keep their passwords secure?

Chris: Well, there are a number of reasons why you would want to do that. One frequent one is that there are so many different systems that use passwords. One frequent technique people use is they’ll use the same password across many systems.

Susan: Much easier to remember.

Chris: Now. It's a lot easier to remember. But you should try to keep that to a minimum. Some systems that people will use is they will have a few different passwords, like you have three different passwords, you have one that you will use for your high security stuff like your home internet banking.

Susan: Mm. Hmm.

Chris: You have one for sort of medium scale stuff like you might use for email and stuff and then a low security one that you would use for like your login...

Susan: For the New York Times website.

Chris: Yeah, exactly.

Susan: They all ask for passwords these days.

Chris: But in general you want to try to keep as many different passwords out there as you can remember efficiently.

Susan: Okay and what the point of that? If I've got a high security password can I use it only for my high security things like my bank or my credit card online? Why would I need to use different ones for those?

Chris: If you...what happens is that if somebody gets a hold of one of passwords then they only have access to the other applications that you use that same passwords with.

Susan: Okay.

Chris: And that is actually something that hackers will look for is if they can get a hold of one of your passwords they are going to try it on every different site that they know of that you frequent.

Susan: Because so many people do that. So many people use the same password.

Chris: Right. Once you've got one password, they'll try it everywhere.

Susan: And I can assume, too, that someone who is hacking in and getting one of my passwords probably has that information about other sites that I might frequent or can get it pretty easily.

Chris: That's right. That's right.

Susan: What about my email password? Do I need to keep that really secure? I mean, I don't care if people read my email.

Chris: Well, you probably should because, for one thing, there are a lot of sites out there that use email to distribute passwords if you forget them, so if you go to that site and say, "send me my password" If someone has access to your email now they can send that email, pick up your email, read that and then get that password and then delete that so that you never knew that it actually happened.

Susan: That's true. And then they have access to all that stuff.

Chris: Yep. Yep.

Susan: So that's one reason to keep your email secure.

Chris: Yep.

Susan: Okay. So how...you said hackers might get a hold of a password. How is that happening?

Chris: There are a number of different ways that you can do that. Probably the most common way right now is just viruses, Nowware, Spyware... all those different evil programs that can run on computers that you may not know that you even have.

Susan: Okay.

Chris: Because they don't announce their presence for the most part.

Susan: Yeah. I know that I have anti-virus software on my computer and I am concerned about viruses. I know that, you know, viruses in the past have done things like destroy files on my computer. But you are saying that some viruses actually are there to steal passwords?

Chris: They certainly do that. Usually what they'll do is they'll try to figure out your password to get into your computer and then use it as a launching point to go to other computers and do bad things to them. So...

Susan: Try to figure out my password to get onto my computer, your talking about the password I use to login to my computer.

Chris: Um. That's one password that's of concern, but, also if you reuse the same password for multiple things, then if it gets one, then you've got all of them and you can use the same text.

Susan: Exactly, but I just want to point out, I said the password that I use to login to my computer, I know a lot of home users don't use a password to login to their computers. Is this something that people should be concerned about?

Chris: It depends on the operating system. On some of them it's a good idea to...

Susan: Most people use Windows.

Chris: to do that. From a security point of view, the best thing to do is, you know, you have the kind of have complete privileges, like administrative privileges, on your computer. You can sometimes make another account for yourself and it's usually a good idea to do that.

Susan: I understand that all current operating systems that you have out there, Macintosh OSX, Windows XP, they all have the availability for different accounts. You can have an administrator account that lets you install software and then you can have other basic user accounts that just let you use the software and I know I've got that set up at home so that my six year old doesn't install software.

Chris: That's the best application for that.

Susan: Yeah. So you're saying that you might want to do that even for yourself. You might want to set up the one that you use on a daily basis so that if someone does hack into that...

Chris: Think about how often you actually install software. It's not all that frequently.

Susan: Yeah.

Chris: So, if you've got that separation you've just made yourself a lot safer computing environment at home.

Susan: And even with that you might just want to have one administrator account, not all the parents in the household.

Chris: Yes.

Susan: Okay. That's a good point to keep in mind. What are some other ways that we can keep passwords...what are some ways that we can keep passwords safe other than using different ones?

Chris: One thing to do is be careful where you use them.

Susan: Mm. Hmm.

Chris: One of the most frequent ways that people can get their passwords compromised is if you are using, say if you use wireless access, either at home or on the road and you are not using secure means to protect that password when it goes over the network. Because in a wireless environment anyone within range of your computer's antenna can see what you're doing unless you take steps to protect that using, say *VPN, Virtual Private Network* technology.

Susan: Okay, so that would be an additional piece of software that you would use.

Chris: That's usually something that you would find in a corporate environment or...

Susan: Here at the University.

Chris: At the University you can use it to get into the network if you have an account with the University.

Susan: Mm. Hmm.

Chris: You can use *SSL* to protect your email connections.

Susan: Now SSL is Secure Sockets Layer.

Chris: Secure Sockets Layer. And basically all it is it's adding another layer of encryption on top of your session whereas normally your password and everything is going over the network so that anyone can see it this is encrypting that.

Susan: It's sending that actual text, "This is my user name. This is my password."

Chris: Exactly.

Susan: Instead it's going to be in a code.

Chris: Right. It's just going to look like a bunch of random letters, numbers, animal symbols, whatever.

Susan: And then your email program you would have a spot to... probably a check box, to say you want to use SSL.

Chris: It will say turn on SSL for this connection or use a secure connection. It's a good idea to check that especially if you are going over a wireless environment. But, in general it's usually a good idea if your internet service provider supports it.

Susan: Okay and you might see that in two places, too, in receiving your mail and also sending your mail.

Chris: Both inbound and outbound; yes.

Susan: Okay, and now what are some...it's really hard for people remember their passwords and that is why they use the same ones frequently and also they tend to use things they can remember like their children's names or their anniversary.

Chris: Birthdays! Anniversaries. Those are the first things they try.

Susan: And so we obviously shouldn't use those.

Chris: It's not a good idea to use those.

Susan: What is a good password to use? What kind of things do you want to keep in mind when picking a password?

Chris: The kind of depressing part is that the best password is the one that is kind of hard to remember.

Susan: There's always some bad news.

Chris: But there are ways you can kind of get around that.

Susan: Okay.

Chris: One frequent way is that has been suggested is that if you think of a phrase and take the first letters of first letter in each word of the phrase and that's your password because it will give you a pretty good—better distribution that you're going to get from actual dictionary words.

Susan: So, something like, "I Like To Eat Pizza On Friday Nights" rather than taking "pizza" as a password. Taking the first letter and then mixing it up a little bit too.

Chris: Yep. Mix up. One of the easiest ways that you can get a good password is to vary the case instead of it being all lower case which is usually what people will do. Throw in some upper case. Throw it in the middle of it; kind of mix it up between letters.

Susan: Not upper case at the beginning.

Chris: Throw a couple numbers in there, frequently if you use symbols, too.

Susan: Oh. Okay. One thing that I try to do with numbers is, and you want to be kind of creative with this but try and replace a letter with a number.

Chris: As long as it's meaningful to you.

Susan: Yes.

Chris: So you can remember it.

Susan: But creative so that it's not necessarily obvious to someone else.

Chris: Keep in mind that the hackers do that for fun. So, they know the substitutions; they know that you are going to substitute an "I" with a "1". They know that you are going to

substitute an “O” with a zero. So if you can kind of shake it up a little bit you can really get a good password that way.

Susan: And again, starting not with a Basic English word or a name, but a phrase-type thing.

Chris: That is probably the most important one, because one of the easiest attacks that you can do against a password of someone is trying to get your password...is there are lists on the internet all around that have all the different words that you can imagine and then some and then they have variations of all those different words with variations with ones on the end or twos on the end.

Susan: Because that is common.

Chris: Because that is what people will do.

Susan: So we have to work a little bit against human nature here, don't we?

Chris: Right.

Susan: Thanks, so much for being here today, Chris. But there is something that in high security areas is slowly replacing some of the things we've already talked about, it's called Biometrics. We've been introduced to it recently in a number of spy movies but according to Doug Bieniek at Low Voltage Contractors it's over a century old.

Doug: Biometrics really are nothing new. Biometrics were first introduced by Alfonso Berling back in about 1890. He created a series of measurements and contraptions that would measure a man's shoulder width from the top of his head, the shape of his skull, the measurements between the cheek bones. That really was the birth of biometrics. Since that time biometrics have evolved into, most commonly, the fingerprint. Fingerprints have been used since the 1920's by the FBI. Great Britain was actually the first country to ever use the fingerprint to verify identification.

Susan: Low Voltage Contractors sells the two biometrics systems currently in use in the Twin Cities.

Doug: What we have here is a thumb print recognition system. What we do with the thumb print is we actually use it to verify the identity of a user code. We create a mathematical template based upon the distance between the ridges of your finger, the swirl characteristics, et cetera, et cetera. All those features that make my fingerprint unique from anyone else's. So how we use this is we have a ten-digit key pad on top of this reader; I'll enter my four-digit security code and it asks me to put my fingerprint again, to verify I am who I say I am. The failure rate or what we call false positives or false rejects is about 1 in 1,000 for this reader.

What we have here is another biometric device that we call a Hand Geometry reader. What a Hand Geometry reader does is it actually measures about 96 different points upon your hand. Again, like we had on the thumbprint reader we create a mathematical template based upon the length of my hand, the width of my hand; certain pressure points. So when I approach the reader, I enter a four-digit number that is unique to myself. I place my hand into the reader to verify I am who I say I am. To make Biometric security devices more user-friendly and to alleviate some of the concerns regarding identity theft, HID, Corporation has developed a device called a Smart Card. A Smart Card is an access control card like we're used to using today, only we've taken this card and we've actually embedded a microchip. Your template, remember every electronic device, every Biometric device creates a template to verify you are who you say you are. Instead of storing that template, that verification algorithm on a supercomputer or computers that may be accessed by who knows who, we actually store your template on this Smart Card. So, when I approach the biometric device, whether it be a fingerprint recognition device, Hand Geometry, Iris, what have you, I'll present my card, I'll place my fingerprint and it actually verifies my thumbprint to the template that is stored on the Smart Card. The Smart Card is always in my possession. Never leaves my where-with-all, I am who I say I am because this is my card.

Susan: Across town at Twin Cities International Airport, another identification system is in operation. Northwest Airline pressed the Transportation Security Administration, the TSA, to implement it here in the Twin Cities. It doesn't scan your palm, it might scan your finger, but mostly it scans the iris of your eye. Andrea Stegeman of the TSA shows us how it works.

Andrea: What I'll do is I'll approach the machine and I'll stand in front of the machine, there is a certain distance that is actually marked on the floor, you put your toes on the line and you'll adjust the mirror to fit your eyes. Right now we're connecting irises. And when you can see that there's a small, yellow halo and you can see that halo with both eyes, you touch the touch screen to proceed. At that point the machine takes an image of your eye to compare it to the database. If it can't get a good image it will ask you to turn left, go a little bit right, step forward, step back until it can get the perfect image that it needs to get. If it doesn't get a good image on the first try, it'll attempt to do it a second time and on the second time it will say yes, it's been a success, you can proceed or it'll say please see the attendant if for some reason it wasn't able to detect you in the system.

Susan: Twenty-five hundred Northwest flyers are taking part in this experimental program. It's designed to get passengers through airport security quicker. Because those 2,500 have undergone through various background checks and security clearances. Fingerprints, palms, irises, and there are even more ways of identifying you. Professor Yongdae Kim knows many of them. He teaches in the department of computer science in the University and his interests lie in network and computer security. Thank you for being here with us today, Yongdae.

Yongdae: Thank you for your invitation.

Susan: A lot of these fancy technologies, fingerprints, iris scans are very expensive I presume. Why would you use these?

Yongdae: Because it provides much better security and also those technologies are not used alone because usually, for example, there are other tests you can do, for example, if you do like a fingerprint, thumbprint, then you can cut the thumb.

Susan: You don't see that kind of thing in spy movies.

Yongdae: Also there are more fancier tests, for example if you take the fingerprint from the card, then they can build a rubber finger and they can pass the test.

Susan: So just make a copy of my fingerprint, yeah.

Yongdae: So usually what we have to do is we have to mix different technologies.

Susan: Okay.

Yongdae: For example you want to mix a password with a fingerprint.

Susan: We saw in the video previously that he used a four-digit code in addition to the fingerprint.

Yongdae: Yes. Also there are like a SecureID.

Susan: I know that we've got the things that identify you as a person the fingerprints, the iris scans, but there are other ways to have more than one type of security at once in addition to the password. So like the password is...I know AOL is coming out with a program where they give you a special little card that has a number that changes.

Yongdae: Yes. That's called SecureID and there are other companies that are making it. I think that RSA.

Susan: RSA is one of those big companies.

Yongdae: is providing such a service. There is a small device where it changes the number every time you log in so that anybody who could not steal that device cannot log in for you.

Susan: They need to have the device with the number.

Yongdae: Right.

Susan: Because it changes every minute or every thirty seconds?

Yongdae: Yeah. So, basically they have to steal both your password...

Susan: Which, hopefully you have in your brain.

Yongdae: And also the SecureID also.

Susan: They have to have both things.

Yongdae: Yes.

Susan: (inaudible) And so that's the same idea as using part of your body as an identification.

Yongdae: Right.

Susan: But you pointed out that parts might be stolen. Also, are there some issues with the reliability of...how reliable is a fingerprint scan? How often does that work?

Yongdae: So, basically the fingerprint is analogue information.

Susan: Analogue information. Mm. Hmm.

Yongdae: But, what you determine is digital information.

Susan: Mm. Hmm.

Yongdae: Right. So, you need some kind of conversion and if you make the determination too harsh then nobody can pass the test. So you will have a lot of false positives.

Susan: So a lot of false positives.

Yongdae: But if you make the threshold too low, most of the time you can log in, there is not problem, but there are false negatives.

Susan: Somebody else can log in as well.

Yongdae: Right.

Susan: You don't want that to happen.

Yongdae: So setting up the threshold is not that easy. Because, I mean, you need to think about usability or security.

Susan: I would suppose that when I put in my password its obviously very clear to the computer that I'm a "one," and "A" that can't be misinterpreted as anything else. But

with my thumbprint I might put it down a little differently the next time and that is what you mean by analog, right.

Yongdae: Right. Right. Right. So the placement of the finger is also important but as we've seen in the video before, I think nowadays mostly the success rate is pretty high but that means that there can be some false negatives and that is why we have these rubber finger attacks.

Susan: Someone might have the technology to steal your fingerprint. And of course, once they steal your fingerprint it's not like you're going to get yourself a new one.

Yongdae: Right. You cannot buy a new one.

Susan: That's a little bit of a problem there. And so that's why you might have that...these technologies that are using parts of your body to identify, I assume we're not using them for too many every day things because they are more expensive.

Yongdae: Yeah. It's much more expensive. You cannot use it for, I think, at home. Unless you're really...

Susan: That's a really high-secure home. Yeah. Something that's really, really...

Yongdae: So, usually at home we're usually using computers and just using internet and login to AOL, that's kind of everyday life. But there are other technologies to prevent attacks on your password. Even though it is just a single password the text they are launching have an automatic, some computer generated program that guesses your password.

Susan: Mm. Hmm. Chris was saying that they've got dictionaries and so that might try and go through all the different words and try them one after the other

Yongdae: So, it's dictionary attacks using some kind of computer programs, now, how can you prevent that? There is a fancy technology that can prevent that...so, the idea in aCAPTCHA project is how to tell apart a computer program and a human.

Susan: CAPTCHA is the name of the program.

Yongdae: Yes. So, in the CAPTCHA program they want to compare if the one who is failing the password login is a human or not.

Susan: Because if it's a computer you go...Oh..they don't want to let a computer do that. They want to make sure it's a human who may just be forgetting their password and not doing it right.

Yongdae: Right.

Susan: So, how does this work? How does CAPTCHA work?

Yongdae: Oh. Let's take a look at your screen.

Susan: Okay. And so what we have here is ah...

Yongdae: This is kind of blurred text.

Susan: I can tell that there are some words here, I can see "button," I can see "angry."

Yongdae: So, humans can read this easily. However, there is no computer program that can distinguish this.

Susan: Because this is actually an image of a word it's not actually the letters, the text itself..

Yongdae: It's kind of blurred image so its and there is another interesting CAPTCHA.

Susan: Okay. So this looks like a different way of approaching this problem.

Yongdae: So, most people think the same thing when we see the pictures. So for example, here, what is this?

Susan: We're looking at pictures of brains, here. It's pretty obvious to me.

Yongdae: Right, so everybody can distinguish what it is, however, the computer program by looking at these four pictures doesn't know.

Susan: Because the computer is storing picture information digitally as well. So it's all just a bunch of zeros and ones to computer.

Yongdae: Right. So, that's the idea of the CAPTCHA project. So, for example when you fail the log in three times, then they will show this to you.

Susan: And they say, prove that you're a human.

Yongdae: Yeah. But you can slow down the dictionary attacks and you can check whether the other person is a human or not.

Susan: Absolutely and I see that then you just choose a word from this list and I see that there's a bunch of words in here so you'd have to be able to figure out...the computer wouldn't be...

Yongdae: You'd have to be human.

Susan: Exactly. Um. Now I know that one of the big problems with passwords is that people have a hard time remembering them, I know that you...

Yongdae: So there are two things, it's again the trade-off. If it is easy to remember, it is easy to break.

Susan: Exactly.

Yongdae: Right and if it is long enough and it is random enough if you are doing symbols and characters then yeah, it may be more secure but it is hard to remember.

Susan: Could you show me pretty quick because we're running out of time, but can you show me I know that there is a new picture-based password technology.

Yongdae: Mm. Hmm. So, there are a lot of pictorial passwords. They are having a lot of research on pictorial-based passwords and this is one of the technologies called random art.

Susan: Mm. Hmm.

Yongdae: And basically their idea is that an image is much easier to remember...

Susan: For most people it's much easier to remember a picture.

Yongdae: So, for example, if you type a very long secure string and that will generate this kind of beautiful randomized and what you need to do is you need to just choose the picture that you want to remember and then next time when you login you will see tens or twenties of these pictures and you need to choose which one...

Susan: Which one is the right one.

Yongdae: Is your password.

Susan: And most people have an easier time remembering this, don't they?

Yongdae: Yes. They have a user study and they show that people can remember this much much better than long string passwords.

Susan: Maybe it'll be easier in the future. Thank you so much for being with us today, Yongdae.

Yongdae: Thank you, Susan.

Well, that's our show on techno-identification. Some important points we think you should remember include these, for you files.

Susan: Systems programmer Chris Bongaarts suggested that you should have different passwords for different uses.

Chris Bongaarts:

You have one that you use for your high security stuff like your home Internet banking. You have one for your medium scale stuff like you might for your email and stuff. And then a low security one that you might use as your log into the web forums ... (Susan: New York Times)

Chris: ... yeah exactly.

Susan: Hackers get your passwords using viruses or spyware. But they have other ways.

Chris: One of the most frequent ways that people can get their passwords compromised is if you're using say, if you use wireless access – either at home or on the road ... because in a wireless environment anyone within range of your computer's antenna can see what you're doing unless you take steps to protect that using say VPN, virtual private network technology.

Susan: To prevent that, Chris suggests using SSL, Secure Sockets Layer.

Chris: Basically all it is, is adding a layer of encryption on top of your session. Whereas normally your password is going over the network so that anyone can see it. This is encrypting that.

Susan: Computer science professor Yongdae Kim said some hackers use computer programs to guess your password.

Yongdae: —the attacks they are launching have an automated ... some computer generated program that guesses your password. Now how can you prevent that? In the CAPTCHA program you want to compare ... if the one who is failing the password login is human or not. So humans can read this easily. However, there is no computer program that can distinguish. When you fail the login three times. Then they will show this to you.

Susan: and they'll say, prove that you're a human.

Yongdae: Yeah, by that way you can slow down the dictionary attacks.

Next week, now that we've figured out who you are, we'll tell you how to protect your identity, something that is being threatened by a new and increasing crime. Next week we are talking identity theft. Thanks for watching. Until then, I'm Susan McKinnell.

Tech Talk is produced by Academic & Distributed Computing Services and the Digital Media Center, Office of Information Technology in cooperation with University Relations, University of Minnesota

Executive Producer

Robert H. Bruininks

Special Thanks to:

Steve Cawley

Shih-Pau Yen

Host

Susan McKinnell

Producer / Director

Susan J. Tade

Associate Producer

J.B. Eckert

Field Shooting

Jonathan Kranzler

Assistant Director

Rich Reardon

Technical Director

Steve Barbo

Audio

Gary Bleskachek

Floor Director

J.B. Eckert

Cameras

Laura Cervin

Jonathan Kranzler

David Lindeman

Lighting

Laura Cervin

Set Design

Richard Stachow

Graphic Design
Nicky Torkzadeh

Effects Design
Paul Pecilunas

Make-Up / Prompter
Sharon Davis

Web Development Team
Christina Goodland
Lance Cunningham

Thanks to:

Low Voltage Contractors

Transportation Safety Administration

CLA Studio B

Radio K

Bakken Library & Museum

KSTP Meteorology Department

Pavek Museum of Broadcasting

Antique Telephone Collectors Association

© 2005 University of Minnesota