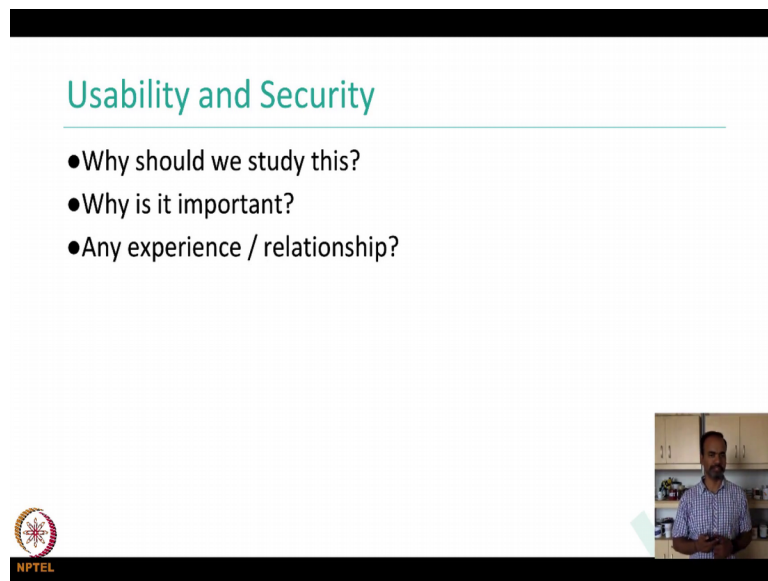


Introduction to Human Computer Interaction
Prof. Ponnuram Kumaraguru (“PK”)
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 18
Week - 07
Usable Security



Welcome back to the course on Introduction to Human Computer Interaction. This is week number-7. I am going to be covering this week on a special topic called usable security and I hope you are enjoying the course. Until now, I hope you are actually trying the things that we are talking about in the class looking at the videos, talking about I see some questions on the discussion forum, but I would expect or I would be happy to see more questions being asked which are not just administrative questions as part of the mailing list also. So, let us look at what is usable security.

(Refer Slide Time: 00:45)



Usability and Security

- Why should we study this?
- Why is it important?
- Any experience / relationship?



I am sure all of you have used systems where you created security policies or you would updated privacy settings, you would have used privacy settings of late stage networks like Facebook or you would have had in your operating system you would be giving file sharing permissions and Google drive, you are actually setting up preference of some who can edit, who is the manager, who can just comment on the document and things like that.

So, one of the ways to think about it is that usable security is like an oxymoron, right, where the words to the words that are put together actually are completely opposite. So, if you really look at usability and security they are actually sometimes if you were to increase the security the usability is going to reduce and if you are increasing the usability security is going to be reduce.

Here are some examples that you can think about where these kind of so to say imbalance is going on between security and usability right for example, your banking website you go to ICICI bank website and you want to actually do a transaction and you wanted to move let us stay transfer money from one account to another account and when you go to the website you are going to give your username and password then they are also started using passcode which is like so to say an image that they will show you and you have to figure out some features in the image or some objects in the image.

Then there was this virtual keyboard right where they said that oh you can type any more the key passwords from the key because key loggers can be there. So, we will actually shift the keyboard to the virtual keyboard where they will press on the keyboard on their screen and you have to pick the keys what they do is the keys that the press on there are actually not the key to be actually a keyboard, but they present it the way they wanted with the jumbled up and everything. So, in that you have to find your characters in typing.

And, then they also start sending you now OTPs is where you have you want to transfer money there is an OTP that is sent to your phone you have to key in that OTP because this is the out of band kind of verification. So, they can actually check whether it is you who is doing the transaction by getting this OTP and then they let you do the transaction. So, what they have done they basically increased the security, of course, they are giving you some level of the good security by all those measures but in the process they have actually drastically reduced the usability of the system because somebody has to go through all this off in making a simple transactions.

So, on the other side meaning if you got a keep think of the door in the office you can actually keep the increase the usability by not having a lock in your office or by having simple doors which can be probably open very easily or something therefore, the usability is very very high, but you are actually dropping off in the security, right. So,

that is the topic that we will cover more and see how. So, usability can also be referred with about called utility. So, it is security versus usability or utility of the system. As the security increases the utility of the usability of the system is going to go down. I am sure many of you are also seen this address bar change in colour in to green when the security when the certificates of the websites are verified and if it is not if it is not an https website the symbol of the address bar changes, right. So, these are all different aspects of so to say usability that is crossing over the security aspect, right.

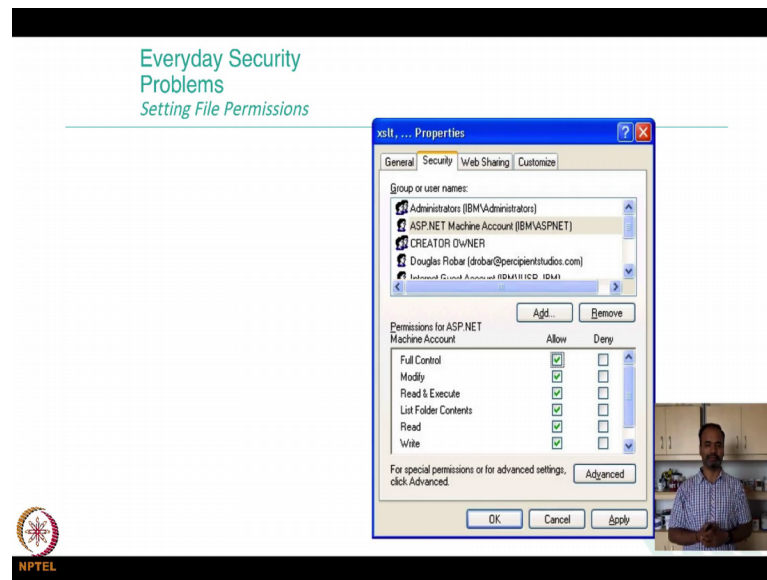
So, it is an important topic it is actually very exciting topic also in the last few years the area is grown pretty big and there are lots and lots of research done in this space. So, we look at some of them today and I will also give you some pointers which can actually give you more insights into this topic if you are interested in this topic.

So, why should we study this right the importance of studying this is for example, again the end users license agreement there is this when you download I am sure many of you downloaded a app in the last month or 6 months or 2 months or so, before actually downloading the app and installing it that this is end users license agreement which the app developer or the organization presents there is a button I agree how many of you actually read the end users license agreement before clicking on the button I agreed by right.

So, that is these are the kinds of security versus usability topics that are interesting to study and why is it important? It is important because there is lots of questions that you can answer for example, what should be the default settings in Facebook, right, when you create an account what should be the default settings when you create a Uber account right what should be the default settings about using your credit card you know connecting to Paytm and just like that. So, studying the settings of what the user should use is actually an important topic also right if there are any experiences and relationship you see between usability and security please drop it in the mailing list will be happy to actually have a discussion around what you think about this topic.

So, that is the relationship between usability and security let us dig more into this topic.

(Refer Slide Time: 06:01)



So, this is the image that you are seeing on the right hand side is the file permission setting on Microsoft windows at some point in a time, right. So, there are there are lots of issues in terms of setting up this file functions instead of issues let us just call it as that is a processor it takes time to actually set up these privacy preferences properly, right settings properly. So, here is what I think one of the PhD thesis Bob Reeder if any of you are interested in looking and this PhD thesis is PhD thesis done by a Bob Reeder where he actually looked at how to reduce this particular problem of setting file permissions into easier ways of doing it, right.

So, the way that he try it was this is in this case I think in a thesis he argues that it takes about 13 steps to figure out correctly the file permission that is if there is a document what document that you have to share with somebody and they are part of the mailing list and they are part of some users group how do you set the file permissions properly, for example, if I went to think of some settings here is one there is also another project around this topic which we can talk about it later where I want to share my current locations to people who are asking, right.

So, for example, students from students who were taking this NPTEL course should probably not have access to where I am in from my location information, but as students have triple IIT Delhi would taking my course all who were generally triple IIT Delhi such should have access to my location when I am in my office probably and the days

when I am teaching probably the students were taking my course should have access to my location and for the TA's teaching assistants for the course they should have access to my locations probably a little more than what the students in the course should have whereas, the faculty would probably have more whereas, my wife should have access to my location always, right. So, that is the kind of setting scenario that you could actually have where this permissions for this information is different for different sets of users.

Now, there are also problems in terms of actually setting up these file permissions properly for example, there is a student who is taking the course taking a course of mine is also a year of a course that I am teaching another course that I am teaching. So, all kind of file permissions how do you manage these file permissions among the users, rights. So, these are all classical problems that people are trying to solve, but I am just trying to highlight that there is a problem in terms of setting these kinds of permissions for in your daily day to day activities also right. Google drive I am sure many of you are using Google drive where you are trying to give sharing permissions with people who can edit, who can actually comment and all that.

Again, the PhD thesis Bob Reeder feel free to take a look at it. The way that he solved it was he created something called is expandable grants when you drive in a said that we can actually reduce such problem into a grid form where you just have this allow and deny for different users for different settings and for different users in different documents the file permissions can be set.

(Refer Slide Time: 09:15)

Secure, but usable?



So, if you look at this picture right, it looks like secure probably it has a very little physical access people unless people can just steal and take away the whole machine. So, if you really look at the kind of attacks that are going on now they do not really attack the physical so to say a right infrastructure they attack more the semantic type of the attack versus the human being type of the errors that we make, right.

So, these kind of things are secured or not but they are not just usable I am just trying to give you a sense of this difference between security and usability and secure and usable of course, unusable security frustrates users.

(Refer Slide Time: 09:56)

Usable Privacy and Security

“Give end-users security controls they can understand and privacy they can control for the dynamic, pervasive computing environments of the future.”

- Grand Challenges in Information Security & Assurance
Computing Research Association (2003)

More research needed on how “cultural and social influences can affect how people use computers and electronic information in ways that increase the risk of cybersecurity breaches.”

- Grand Challenges for Engineering
National Academy of Engineering (2008)



Here are the some kinds of codes that you can actually take a reference at. So, the first code reads as it is from computing research association, the second one is from national academy of engineering the first one reads is given users security controls they can understand and privacy they can control for the dynamic pervasive computing environments of the future.

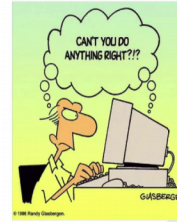
So, these into about three just imagine how futuristic they were in terms of actually developing this idea of giving the end users the control for setting things up. For example, in a Facebook right can people tag you on pictures, if they tag you I should get a review notification and can I make my friends list public, can I make only partial list public and things like that these are all so to say your security controls that you want which can be actually controlled by giving you preferences in which you can control this.

The second mode for national academy of engineering is more research needed on how cultural and social influences can affect how people use computers and electronic information, right. That is clear, that the way that the privacy or the security aspects of things have understood in India versus in the US versus in the Europe are actually very very different right we are still figuring out how to define privacy it is still figuring out what levels of privacy controls to be provided whereas, in the western world they have already privacy laws privacy act GDPR all of that is already very well established.

(Refer Slide Time: 11:31)

Humans are weakest link

- Most security breaches attributed to “human error”
- Social engineering attacks proliferate



And, the interesting thing about this whole area of usable security or even the security itself is that humans are the weakest link right we make the most kinds of errors and if you have read about these kinds of breaches most security breaches happen because of human error right social engineering attacks actually proliferate a lot.

So, I am I do not know how many of you know what social engineering is, if I were to actually collect the information about you I will call a few people ask them to pretend as though I am so and so and I will actually try finding information about your lipstick I pretend as though it is your friend who is calling, whose brother is actually in your class or her sister is connected to you or things like that, right. So, if you are interested in looking at more about social engineering read about Kevin Mitnick he is one of the very popular person who did the social engineering very effectively.

(Refer Slide Time: 12:21)

The slide features a title in teal text: "How can we make secure systems more usable?". Below the title is a horizontal line. A bulleted list follows, with the first item being "Make it 'just work'", which has a sub-bullet "Invisible security". The other main items are "Make security/privacy understandable" (with sub-bullets "Make it visible", "Make it intuitive", and "Use metaphors that users can relate to"), and "Train the user". In the bottom left corner is the NPTEL logo, and in the bottom right corner is a decorative graphic of teal diagonal bars.

- Make it "just work"
 - Invisible security
- Make security/privacy understandable
 - Make it visible
 - Make it intuitive
 - Use metaphors that users can relate to
- Train the user

But since this course is not about security I am going to focus on the usable security part. So, how can you make secure systems more usable, right. So, the question is can you actually build systems which can be secure and which can be usable also? right. So, the broader theme of the course is about building usable systems usable and useful has been our theme and in that one particular area that we are focusing on is can build systems which is secure and unusable. We will also look at later about mobile devices itself particularly h c l or user experience in a mobile devices, but for now we look at the security point.

So, three ways to actually attack and solve this problem which is make it just work make security privacy understandable and friendly user, right. So, let me take you let me walk you to an example how this can be actually in this you will be able to understand this better. So, all of us use e-mails right and when and even when an email comes there is some spam filter sitting somewhere sitting and checking whether this email is legitimate or not and it has a lots of features particularly if you look at Gmail it has a lot of features that it is understood or all the emails that they receiving or all the features that people have even then saying that by reporting an email as spam you are actually giving them some features about those emails. So, through all this process they figure out that what email is which emails are most spammy versus which emails are not.

So, keeping that in mind what they would do is they create a score for every email and depending on what the score for that email they will actually decide whether this email is spammy or not so to say, right. This feature will help you to design the whole feature extraction and figuring out whether this emails is unable help you to decide whether they keep the email in the inbox or should move it to the spam folder, right. So, that is may just work which is that security is not even visible to the end users right because I really do not know what are the events that are going into my spam or in my trash because of the decisions that I have made in the past or the others like me you have made in the past.

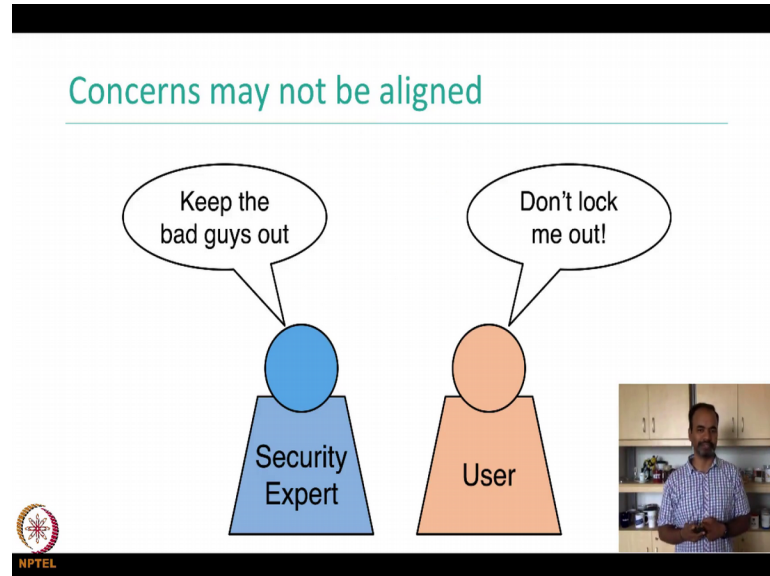
Make security or privacy understandable is that make it visible, make it intuitive, use metaphors, right. So, let me explain some examples here make it visible, right. So, make it possible is if you want to make if you are going to a website called let us take Amazon dot com I want to show that whether it is legitimate or not. So, in the address bar I will give you a green colour and if there are websites that you go to for example, there are multiple a tool box which actually allows tells you whether this domain is actually legitimate or not, right. If you give scores again all this domain was registered on tenth of March of 2000 and this domain was registered on tenth of March of 2018, right. So, which can give you a sense of which site is more legitimate versus not legitimate, right.

So, in the interface is the information is presented it is actually the end user is making the decisions. For example, when an email comes that email is marked as some value and it still goes through the filter saying that it looks like it is legitimate. So, then it is present it to you, but there is some highlights in the email saying this email looks actually spammy so to say right. So, now, the email came through the filter pass through the end user we see and still they make mistakes, right, still many of us click on links, still many of us open attachments which are not legitimate.

So, for to avoid the second level of problem if that goes to the user also the tools and everything then third option or the last final option is actually trying the user. So, the logic is that there is these three solutions these three source and methodologies have to work together in terms of finding a solution, right. So, nothing not a single one will actually solve the entire problem and I am going to take a more deeper look into the aspect of training the user because that is where this whole idea of usability and security

is actually playing a more role and that is where I actually know more things to talk about also.

(Refer Slide Time: 16:27)



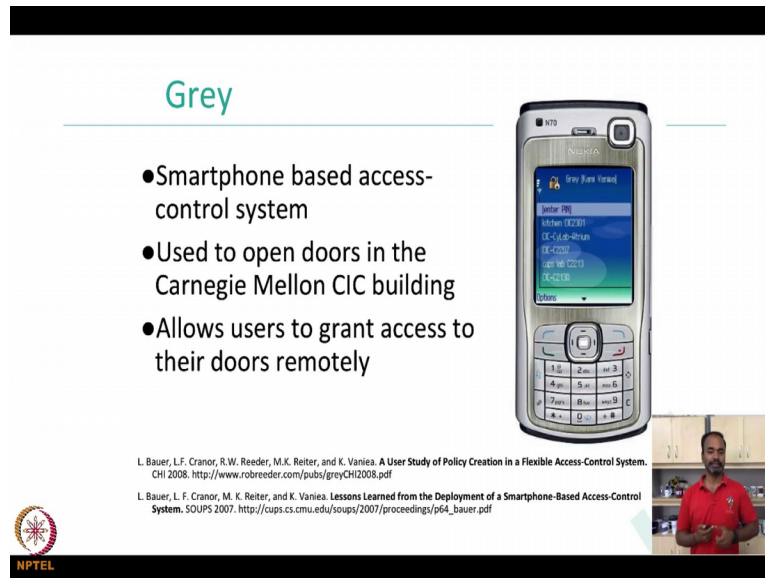
If you really look at the concerns right concerns of a security expert versus the user then not (Refer Time: 16:35) concerns for a security expert is that to make sure that things are hard for the end user to do as the example I said, banking website in terms of giving you a virtual keyboard making the password very hard, right passwords many passwords by itself is actually hard to figure out mean if you are interested take a look at some literature around this password, but there is a tech talk by (Refer Time: 16:59) which actually talks about passwords itself right passwords what kind of passwords are more popular what kind of passwords do people keep right.

So, again password is also some kind of a usability versus security agents right because companies organizations let us you create passwords for this a lot of a rules around it which is that oh it has to have one capital letter one smaller the same letters cannot come again and again and it cannot be from dictionary it cannot be from you have to use so to say the alphanumeric characters all of that right.

So, security experts the align the concerns of security experts is created this as hard as possible so the bad guys cannot get in. The problem of the users is that users think that was I do not want to be locked out, I do not want to forget my password every time I log

into the system right. So, that is the problem with the keep the bad guys out and do not lock me right. So, that is the misalignment of the security expert and the user.

(Refer Slide Time: 17:59)



Grey

- Smartphone based access-control system
- Used to open doors in the Carnegie Mellon CIC building
- Allows users to grant access to their doors remotely

L. Bauer, L.F. Cranor, R.W. Reeder, M.K. Reiter, and K. Vaniea. A User Study of Policy Creation in a Flexible Access-Control System. CHI 2008. <http://www.robreeder.com/pubs/greyCHI2008.pdf>

L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea. Lessons Learned from the Deployment of a Smartphone-Based Access-Control System. SOUPS 2007. http://cups.cs.cmu.edu/soups/2007/proceedings/p64_bauer.pdf

NPTEL

Now, let me walk you through one of the super exciting projects on unusable security which was done some years back. This project is called Grey and the main aim of this project was to actually give access to end users through their phone to open up their office doors, to open up the floor doors and this project interested me what they did in this project was they actually had a microprocessor chip microprocessor placed in every door of the building so they would actually talk to the microprocessor to interact with the processor for giving it instructions for doing some tests.

So, here this is Smartphone based access control system where the scenario is that I am I want to get into my office from morning and coming out of my parking lot I open up my phone, I say that I am near the office, I click a button and my office door open when I am walk near the door. So, that is the whole idea of this project called grey. Used to open doors in one of the buildings in campus CIC building allows users to grant access to their doors remotely.

For example, the scenario here is that I am travelling and I want my and I am teaching of course, this semester I have kept the copies of the examination quiz question papers in my office and I want my teaching assistant to get access to my door and take these copies of the quiz. So, what do I give I press a button my TA also has this their system she gets

access to the office and I give her she is able to get access to my office to get this first questions and she takes away the quizzes.

So, that is Grey project. Let me walk you through more details about this Grey project giving you actually how a usable security is actually playing an interesting role and an important role in actually solving these kinds of problems.

(Refer Slide Time: 19:50)

Data collection

- Year long interview study
- Recorded 30 hours of interviews with Grey users
- System was actively used: 29 users x 12 access per week


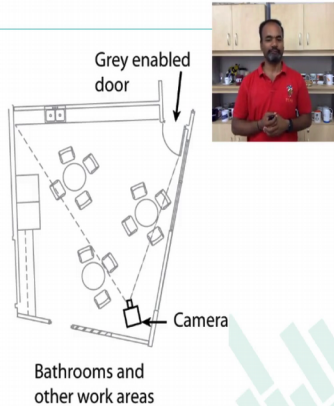
The slide features a detailed floor plan of a building with numerous small circles placed at various door locations. A small video inset in the bottom right corner shows a man in a red shirt speaking. The NPTEL logo is visible in the bottom left corner of the slide.

So, what do you see the image that you see on the right hand side is a floor plan of one of the floors of the CIC building? The circles present if there are the doors that are that has a processor. It was not yearlong study; it was just that the student was collecting data from these doors for one year. 30 hours of interviews with the people who were using this Grey system. The way it was working was if I am the resident of this building I would get a Nokia phone which has this Grey application, I would use the application for opening my doors, for opening my floor and everything the researchers working on the project, to collect data about how many people are using it, when are they using and all that kind of information, and then we use it to make judgment on how with the application is.

(Refer Slide Time: 20:46)

Users complained about speed

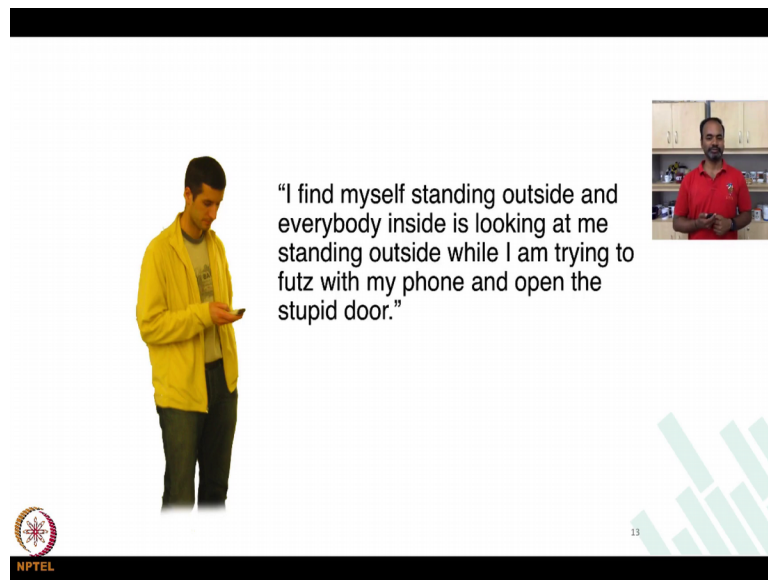
- Users said Grey was slow
- But Grey was as fast as keys
- Videotaped a door to better understand how doors are opened differently with Grey and keys



So, here this one usability study that was done I was actually looking through the I was also there physically when this study was done. So, it is an interesting way to look at how our study design could be done like this which is the. So, just look at the image on the right hand side now which is there is a camera at the end of the room, the camera is looking at the people coming into the door and the student who is doing this project is actually sitting on one of the tables on the left hand bottom side and seeing how people are actually using the keys versus using the Grey versus other ways of actually opening the doors, right.

So, the feedback that was received from the participants were Grey was slow, but Grey was fast as keys because they were actually able to open the doors with the application Grey on the phone and videotaped the door to better understand how doors are opened differently that is what I was saying trying to say which is in the right hand top corner there is a door, the student is actually sitting and seeing it through the door how users are actually opening the door through their phone versus keys.

(Refer Slide Time: 22:03)



Also, this is one of the code from the researcher who is studying this project which is, I find myself standing outside and everybody inside is looking at me standing outside while I am trying to futz with my phone and open this stupid door, right. So, that is the kind of reaction that users is giving while they were using the application there, so what they ended up actually finding was that they ended up finding that Grey after some level of vibrations Grey was actually the way that people were using Grey and the time that it took for users to open the door was actually slightly faster, they could actually get to the they do not have to, for example, if I have to show you how my keys are so, my keys are presented this way.

So, these are my, so, let us do it right. So, these are my keys and if you look at my keys that are there are two keys which are very similar and I want to actually try and change the I want to try and use this keys and I make mistakes which key to the which doors. So, what I have done is I have just added one level of identification for myself saying that there is this black colour thing attached to it which would allow me to say that this is one of the door versus the other door and people end up coming with these kind of so to say rudimentary or these kind of hack to get around the problem.

(Refer Slide Time: 23:31)

Train the user



Now, let me walk you through this one of the aspect of this usable security problem which is training the user training the user is important this because when you when you look at make it just work provide the information to the user, train the user comes bottom of the pipeline, but none of these solutions independently can solve all the problems. So, therefore, putting them all together and making it work is actually the key for making usable solutions.

(Refer Slide Time: 23:59)

Why do humans fall for phish?

- Not motivated to pay attention to training
 - "Security is not my problem"
- Mental models inconsistent with reality
 - "If site looks professional it must be legitimate"
- Need actionable advice they can understand
 - Difficult to be alert if you don't know what you're looking for



So, let me walk you through some background on why people fall for phishing with something intuitive and this is not a security class. So, I will keep it actually very preliminary which is people are motivated people are not motivated to pay attention to training right if you keep telling people put a flyer, put a poster the officers schools saying please do not share passwords do not open the of the attachments all of that, but not many people are going to actually look at it in adhere to the solutions that you are giving, right. Security not is my main problem, right the when I am when my relatives when my family goes to transfer money from one account to another account in a bank website they are not looking at security as the main thing, they are not looking at oh I need to actually look at how this bank is implementing the security policy, right.

So, mental models are inconsistent with reality, right. If psych looks professional with mass appeal estimates I will give you actually some pointers for example, Phd thesis (Refer Time: 25:00) Taneja from a UC Berkeley looked at this problem of showing a bank website and asking people how they think it is legitimate and what are the features that they are looking at to make the decision whether it is legitimate and people actually think that some of the fake websites that they showed is actually legitimate because they think that it looks very professionally done and therefore, it must be actually legitimate.

And, also users need actionable advice they can understand. You cannot provide them information that they cannot do that they cannot try themselves, difficult to be alert if you do not know what you are looking for, right. So, because if you are not telling me what should I look for it is actually going to be hard, for example, you I am sure you are reading it in newspapers and in other places scams like 419 where they send you an email they call you and tell you that, we want to actually you transfer some large amount of money to one account to another account or to India or that we need a small token money from you if you do it well give you actually two percent of the entire money that we are going to transfer. People give away money for such things, right.

There are so many scams like this where people are actually trying to get the citizens and people fall for in giving money away and the point is that you have to be alert, you have to be told what you should be looking for, right. Do not call these numbers, right. In general, if you just tell I think it is not going to do not call this numbers in particular scenario particular situation. That is probably a better way of actually promoting or giving the suggestion that you want to give or take material that you want to clear.

(Refer Slide Time: 26:40)

How do we get people trained?

Learning science principles
+
Teachable moments
+
Fun

P. Kumaraguru, S. Sheng, A. Acquisti, L. Cranor, and J. Hong. Teaching Johnny Not to Fall for Phish. *ACM Trans. Internet Technol.* 10, 2 (May 2010), 1-31.

NPTEL

So, when we were looking at how do we actually start solving the problem of train the user, we stumbled on this whole area I actually spent some time and studying some of these more formally also which is learning science principles to some courses on this topic, understood how people actually learn understood people are learn through online medium right and you teach a class what are the ways by which you can actually get students attention, how do they learn what kind of techniques will actually help learn better.

Teachable moments; teachable moments is another one which is actually very critical because when you are young you would remember that and when you made a mistake people told me something you would actually learn it that you will remember it better and of course, some level of fun knows to be very useful.

So, these are the three important ways that we took away from understanding this domain of, ok, I want to solve this problem security, I want to train people on security aspects. So, I want to actually find out what are the ways to do with learning science, teachable moments and fun. These are the ways that we thought that we could fix the problem and so that is these are not the only ways to fix the problem.

(Refer Slide Time: 27:56)

PhishGuru embedded training

- Send email that look like phish
- If recipient falls for it, train in succinct and engaging format
- Study demonstrated effectiveness of PhishGuru and found that same training was not effective sent as regular email

Learning science principles
+
Teachable moments
+
Fun

NPTTEL

The slide features a title 'PhishGuru embedded training' in teal. Below it are three bullet points. To the right is a small photo of a man in a blue shirt. Below the bullet points is a graphic with a black box containing the text 'Learning science principles + Teachable moments + Fun' and a cartoon orange fish wearing glasses. The NPTEL logo is in the bottom left corner.

So, the way that we attack this problem is that we created a system called PhishGuru and the next thirty, forty minutes of the lecture is actually going to be looking at PhishGuru in more detail, how the design decisions were made what are the design so to say iterations that where went on and how the evaluation was done and what kind of evaluations was done around this topic.

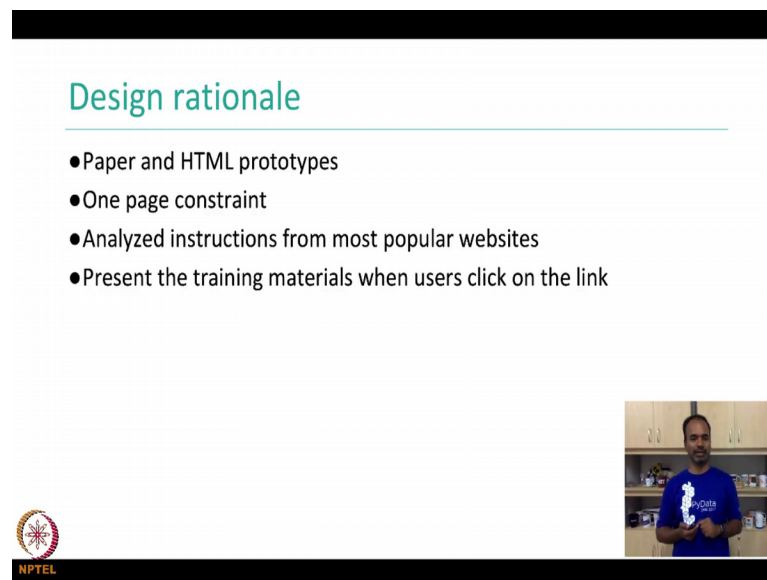
The way PhishGuru works is any email sent, for example, if I were to actually understand how my students behave with a phishing emails I would come to PhishGuru and I would tell PhishGuru saying that please tell me please let us find ways by which I could actually learn how my students are falling for this phishing attack. What would PhishGuru do? PhishGuru would send emails to my students the technique master was actually really nice right send emails that look like phish where they are phishing emails that you are sending them if recipient was for it you actually train them, stop them while they are actually going to give away the password you use a name and tell them that oh what you just do not give you is actually not less demand you should not have done this, alright.

So, these are the, that is how you know that is the teachable moment that we are trying to implement which is when I get an email, there is a link in the email, it is a phishing email, I click on the link, I go to this website, the website is not a list different websites why could actually stop the user saying please read these instructions and hoping that

people would actually read and remember these instructions and the other another stage of doing it is phishing email link, click on the link go to the website give the username password and then stop you saying oh you should not have just given the username and password because it was a fake phishing email that PhishGuru who sent it to all of us.



And, it was also we also found that PhishGuru effectiveness of PhishGuru and found that the same training was not effective sent us the regular email, right; so because if you send the same training material as an email itself security notices another one, right. So, you will get security notices saying, oh, please beware of for example, these days we can SMS's do not share your OTP to people because we do not we do not call companies or banks do not call you to ask you for OTP. Do not share this OTP with anybody else, right. These kinds of SMS's, that you will be getting. How many of us actually adhere to it, how many of us read it, how many of us understand. Probably we understand, but when it comes to saying that as a transaction going somebody is calling you and saying we just saw you doing some transaction there is OTP that we sent you, give it to us, people end up actually giving it.

(Refer Slide Time: 30:44)



Design rationale

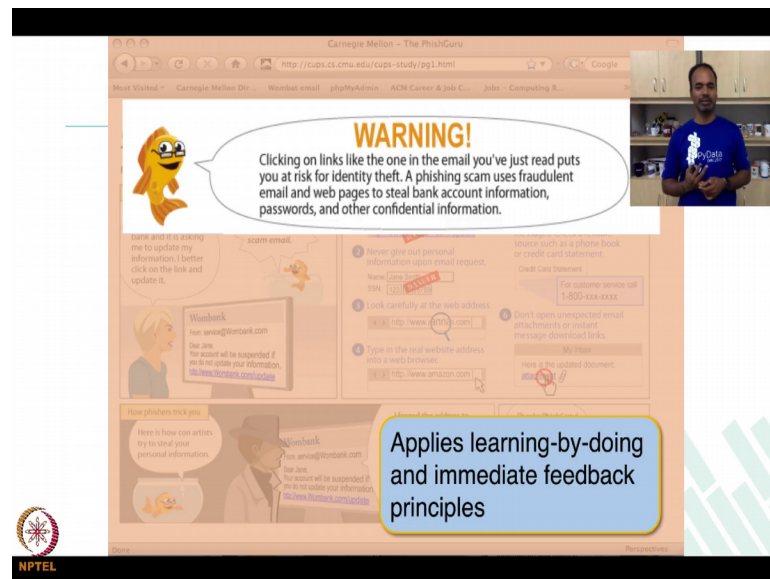
- Paper and HTML prototypes
- One page constraint
- Analyzed instructions from most popular websites
- Present the training materials when users click on the link



Let me walk you through the design rationals that we made in the designing PhishGuru. One of the primary thing that we saw in the design patterns also is to present all the information in above to fold was a design pattern that we saw, right. So, keeping that in mind we want to actually have all the important information that we are presenting to the

user in just one screen that was one of the design pattern and one page constraint is that design rationale that we had to take unless instructions from most popular website because there is hundreds and thousands of websites actually which is giving you all the kind of instructions that you would need. We were trying to distil off and then create something that is not unique, create something that is actionable that was the goal that we were trying to actually achieve. Present the training materials when users click on the link that I said before.

(Refer Slide Time: 31:27)



Next five, six slides is going to walk you through the design. Do not worry about actually the background image what the instructions are on things like that, but I am going to I am going ask you to focus on the bottom right content which is the text on top which tweets in warning clicking on link clicking on links like the one in the email you just read puts you at risk for identity theft. A phishing scam uses formal email and web pages to steal bank account information, passwords and other confidential information, right.

So, that is the warning that PhishGuru is presenting and it is actually applying something the whole concept of PhishGuru is applying learning by doing because they are actually doing falling for link falling for the emails by clicking on the links and immediate feedback when you click on the link make a mistake PhishGuru is stopping you and telling you some feedback.

(Refer Slide Time: 32:16)

The slide displays a browser window with a URL <http://cps.cs.cmu.edu/cps-study/pg1.html>. The main content is a phishing email from 'Wombank' with the subject 'Dear Jane, Your account will be suspended if you do not update your information.' and a link to <http://www.Wombank.com/update>. A character is shown reading this email. A speech bubble from the character says: 'This email is from my bank and it is asking me to update my information. I better click on the link and update it.' A large red 'STOP!' sign with the text 'Don't fall for this scam email.' is overlaid on the email. To the right, a 'WARNING!' box contains text: 'A link like the one in the email you've just read puts a lot of pressure on you to identify theft. A phishing scam uses fraudulent e-mail pages to steal bank account information, credit cards, and other confidential information.' Below the warning, there are several numbered tips: 1. Don't click on links in an email. 2. Don't call company phone numbers in emails or instant messages. 3. Don't open unexpected email attachments or instant message download links. 4. Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement. 5. For customer service call 1-800-434-4344. The slide also includes a small inset video of a man in a blue shirt. At the bottom right, a yellow box contains the text 'Applies story-based agent principle'. The NPTEL logo is in the bottom left corner.

So, this one reads this is a top left corner content reads that how we were attract, this email is from my bank and it is asking this is the character which is reading it this is the email from my bank and it is asking me to update my information I better click on the link and update it, that is what mostly the users would do. PhishGuru is saying that, stop do not fall for this scam email and this is actually a blind story based agent principle which is where there is a story, there is a character, there is a character which is actually suggesting you what should you do and what you should not do. And there are characters which are actually walking you through the content of the characters that are providing you information which you should be reading about.

So, in this case this ladies picture here is she is a character I will show you some more characters that people as part of this design itself.

(Refer Slide Time: 33:05)

The screenshot shows the 'The PhishGuru' website with a 'How to help protect yourself' section. It lists six numbered tips: 1. Don't trust links in an email (with a red 'DANGER' stamp over a link); 2. Never give out personal information upon email request (with a red 'DANGER' stamp over a form); 3. Look carefully at the web address (with a magnifying glass over a URL); 4. Type in the real website address into a web browser (with a magnifying glass over a URL); 5. Don't call company phone numbers in emails or instant messages; 6. Don't open unexpected email attachments or instant message download links. A video inset shows a presenter in a blue shirt. A yellow callout box at the bottom right contains the text: 'Applies contiguity principle' and 'Presents procedural knowledge'.

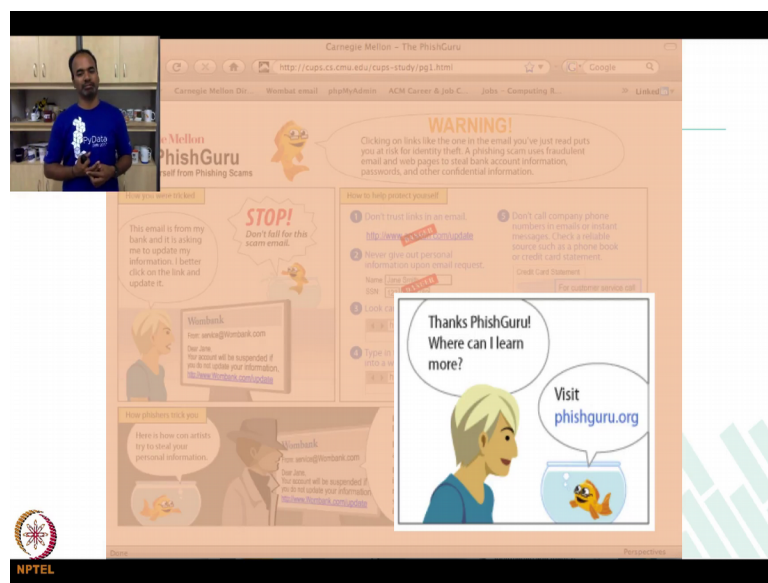
How to help protect yourself? These are direct instructions: do not trust links in the email, never give out personal information, look careful on the web address, type in the real website address in to web browser, right. All of this is clearly actionable information that is presented to the user when they actually fall for it applies contiguity principle, presents procedural knowledge. Contiguity principle and procedure knowledge going hand in hand, it actually presents information which you can take and we apply and use it.

(Refer Slide Time: 33:41)

The screenshot shows the 'The PhishGuru' website with a 'WARNING!' section. It features a cartoon character in a hat and a speech bubble that says: 'Here is how con artists try to steal your personal information.' Below this is an email from 'Wombank' with a link to 'http://www.Wombank.com/update'. A speech bubble from the character says: 'I forged the address to look genuine. I threatened the user with an urgent message. I added a link that looks like it goes to Wombank - but it really sends people to my site so I can steal their information and money!'. A video inset shows a presenter in a blue shirt. A yellow callout box at the bottom right contains the text: 'Applies personalization principle' and 'Presents conceptual knowledge'.

Here is another character which is actually so to say the bad guy how phishers trick you. Here is how con artist tried to steal your personal information; I forged the address to look genuine. I threatened the user with an urgent message. I added a link that looks like it goes to warm Wombank, but it really sends people to my site so I can steal their information and money. Applies personalization principle, presents conceptual knowledge, right. Personalization because it is actually talking about I, I am doing it, you are falling for it, how phishers trick you. Presents conceptual knowledge also because it is telling you ok, I sent you this link, link in the email I made it urgent and all that.

(Refer Slide Time: 34:24)



Finally, this bottom right says that, thanks PhishGuru. Where can I learn more? It says a PhishGuru dot org; that is the URL you should go to check for this content if you want to read more about it. It is called PhishGuru who is telling character.