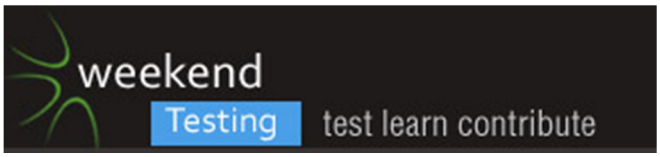


[11:00:21 AM] Weekend Testers Americas: welcome to Weekend testers Americas.

[11:00:22 AM] Albert Gareev: So start stretching your minds :)

[11:00:27 AM] Weekend Testers Americas: This is Session #9.

[11:00:41 AM] Weekend Testers Americas: and we are happy to see you all here today.

[11:00:45 AM] Weekend Testers Americas: First things first.

[11:00:59 AM] Weekend Testers Americas: We have a number of new participants, so please everyone, introduce yourselves.

[11:01:10 AM] Weekend Testers Americas: [shifting over to other computer for his]

[11:01:18 AM] phil kirkham: Phil Kirkham, test consultant, England

Blog: http://expectedresults.blogspot.com

Twitter: @pkirkham

Moderator of Software Testing Club

[11:01:30 AM] Shmuel Gershon: Copy Paste! -->

I'm Shmuel Gershon, write at http://testing.gershon.info and tweet at @sgershon.

I am the author of Rapid Reporter and a technical lead at a testing department in the Jerusalem campus of Intel Corp.

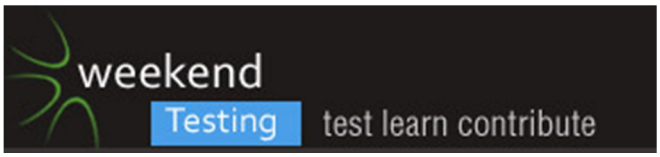
I am convinced that the most significant factor in our quest for quality is people, not features or technology.

[11:01:35 AM] Justin Byers: Justin Byers, Test Team Lead, Victoria, BC Canada

Twitter: @justincbyers

[11:01:44 AM] Scott Seltzer: I'm Scott from Israel. I've worked in QA for various startups over the past 16 years.

[11:01:58 AM] Linda Rehme: Linda Rehme Technical Support Engineer beginning groomed for QA lead



[11:02:05 AM] Aleksander Lipski: Hi, I am Aleksander Lipski (Alek) I live and work in Poland. In testing field for 4 years (or more depending on how you count). Currently work as Test Specialist at Roche

[11:02:08 AM] Deb Amigun: Deborah Amigun, Junior Software Tester

[11:02:10 AM] Linda Rehme: I'm very much new to this.

[11:02:31 AM] Albert Gareev: Albert Gareev. 2nd facilitator at WTAmericas. Toronto, Canada. Visit my blog http://automation-beyond.com/ and find out more about me. Follow me

on Twitter: @AGareev

[11:03:05 AM] Michael Larsen: Copy,Paste:

My name is Michael Larsen. I'm a software tester in San Francisco, California, USA. I am a strong proponent for the continuing education and skills development for software testers. To this end I am actively involved as an assistant instructor with the Association for Software Testing, podcast producer for Software Test Professionals' "This Week in Software Testing" podcast, and a brown belt in the Miagi-do School of Software Testing. I also blogs at mkl-testhead.blogspot.com and can be reached on twitter at @mkltesthead.

[11:03:27 AM] Lanessa Hunter: Lanessa Hunter, Tester for 9 years, Florida. Working on growing my skills and to help others do the same. on Twitter@lanessahunter

[11:03:37 AM | Edited 11:03:48 AM] Michael Larsen: I'm also a co-founder of Weekend Testing Americas and today's primary faciliator.

[11:04:07 AM] Scott Seltzer: Nice to meet you all!

[11:04:14 AM] *** Weekend Testers Americas added Timothy Western ***

[11:04:34 AM] Weekend Testers Americas: Sorry Tiim, I thought I added you earlier (blush!)

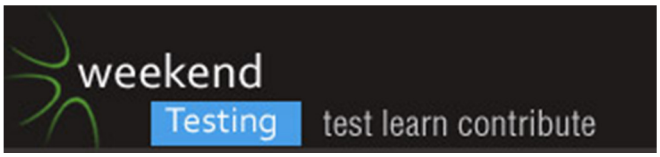
[11:04:53 AM] *** Weekend Testers Americas added rvenkat23 ***

[11:04:53 AM] Timothy Western: No worries, Greetings everyone.

[11:05:23 AM] Deb Amigun: Deborah Amigun, Junior Software Tester, London. Twitter: @debfergie

[11:05:53 AM] Weekend Testers Americas: Tim and Venkat we are doing introductions right now, so you haven't missed anything :).

[11:07:10 AM] *** Weekend Testers Americas removed Lynn McKee from this conversation. ***



[11:07:34 AM] Weekend Testers Americas: Lynn is playing soccer, she'll clearly not be able to participate today :).

[11:07:52 AM] Weekend Testers Americas: OK, so I think we have everyone squared away for today's session.

[11:08:22 AM] Weekend Testers Americas: We will now announde the charter and mission (stick around for this one, as there's some pre-planning involved ;)).

[11:08:30 AM] Weekend Testers Americas: In today's session we will observe behavior of the product, and review problem reports.

Our mission is to explore the context, share and discuss the findings, build and report the models. Each participant needs to provide report in a text file.

We do not provide a template :) ..but we provide sample context-revealing questions.

Questions

What is the product?

Who is the customer?

How the product is used?

What product's features in use we observed?

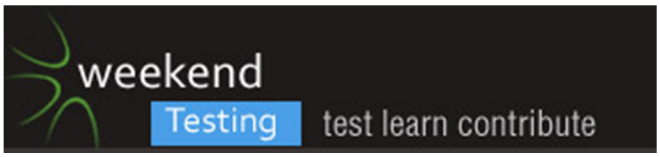
What problems were reported?

How did you recognize a problem?

How you can classify the each problem (threat, risk)?

Can you identify what was a root cause of a problem?

Can you guess what was a root cause of a problem?



Do you suspect there might be more problems, and what problems?

What kinds of tests you would perform to explore the product further?

Please watch the video: http://www.youtube.com/watch?v=__zZxDV91Ao

[11:09:13 AM] Weekend Testers Americas: [11:08 AM] Weekend Testers Americas:

<<< In today's session we will observe behavior of the product, and review problem reports.

Our mission is to explore the context, share and discuss the findings, build and report the models. Each participant needs to provide report in a text file.

We do not provide a template :) ..but we provide sample context-revealing questions.

Questions

What is the product?

Who is the customer?

How the product is used?

What product's features in use we observed?

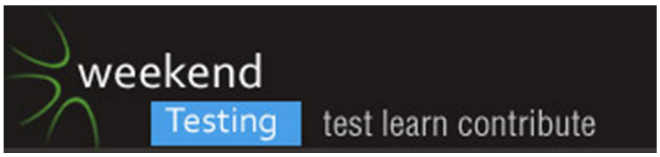
What problems were reported?

How did you recognize a problem?

How you can classify the each problem (threat, risk)?

Can you identify what was a root cause of a problem?

Can you guess what was a root cause of a problem?



Do you suspect there might be more problems, and what problems?

What kinds of tests you would perform to explore the product further?

Please watch the video: http://www.youtube.com/watch?v=__zZxDV91Ao

[11:09:45 AM] Weekend Testers Americas: First thing we recommend is... everyone watch the youtube videl listed (it's only a couple of minutes long).

[11:10:39 AM | Edited 11:11:18 AM] Albert Gareev: No pairing and private chats today, please. Report any bugs found into the common chat with a hashtag #bug. Report any issues into the common chat with a hashtag #issue.

[11:11:50 AM] Weekend Testers Americas: [11:08 AM] Weekend Testers Americas:

<<< Please watch the video: http://www.youtube.com/watch?v=__zZxDV91Ao

[11:14:45 AM | Edited 11:15:21 AM] Michael Larsen: but my passport is RFID.

[11:15:08 AM] Shmuel Gershon: That's scary, uh?

[11:15:21 AM] Albert Gareev: [11:14 AM] Michael Larsen:

<<< Just checked... I don't have an RFID credit card (LOL!).What about your passport??

[11:15:28 AM] Timothy Western: I've never been happy to not have a Major Credit card before.

[11:15:29 AM] Michael Larsen: Yes, it is.

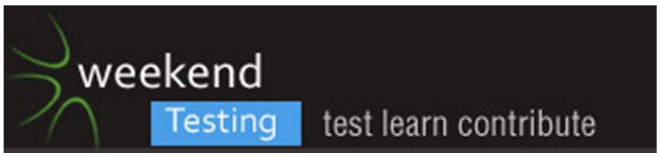
[11:15:33 AM] Timothy Western: until watching that LOL

[11:15:33 AM] Albert Gareev: .

[11:15:50 AM] phil kirkham: Snopes article gives some insight - http://www.snopes.com/fraud/identity/pickpocket.asp

[11:15:56 AM] Albert Gareev: OK, so we got you scared :)

[11:16:12 AM] Justin Byers: So what's the product we're reviewing here... the RFID stealing device or the plastic sleeve that protects?



[11:16:13 AM] Aleksander Lipski: Being scared - is it a finding ?

[11:16:15 AM] Albert Gareev: That wasn't the mission, though :)

[11:16:17 AM] Shmuel Gershon:

What product are we talking about here? There were many on the video.

The credit cards? The protective cases? THe RFID scanner?

[11:16:19 AM] phil kirkham: @Albert whenever I get scared on the internet I head ti Snopes...

[11:16:55 AM] Deb Amigun: It is indeed scary

[11:16:55 AM] Michael Larsen: The first question we as testers should be asking is "OK, we have a potential threat.

[11:17:03 AM] Michael Larsen: but what is the reality o that threat?

[11:17:09 AM] Michael Larsen: Is it something we can protect from?

[11:17:11 AM] Albert Gareev: Product - financial service.

[11:17:13 AM] Michael Larsen: What is its scope?

[11:17:21 AM] Michael Larsen: How realistic is it to create a device like this?

[11:17:25 AM] Justin Byers: @Michael I don't know who I'm working for yet, so I don't know if there is a threat or not.

[11:17:52 AM] Michael Larsen: Albert, help us out here ;).

[11:18:03 AM | Edited 11:18:23 AM] Aleksander Lipski: Scope - 140.000.000 people ?

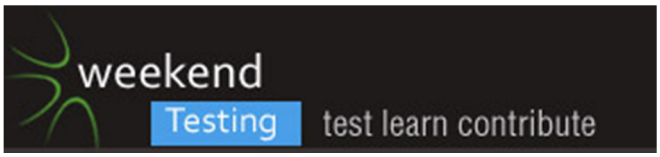
[11:18:06 AM] Scott Seltzer: I like the way you think, Justin.

[11:18:07 AM] Albert Gareev: [11:17 AM] Albert Gareev:

<<< Product - financial service.Credit card? -

[11:19:08 AM] Justin Byers: Thanks Scott :)

[11:19:20 AM] Shmuel Gershon: Michael -- what is the product we are analyzing in the session?



The credit cards? the RFID scanners? the protective cases?

[11:19:26 AM] Shmuel Gershon: Reporter's microphone?

[11:19:29 AM] Timothy Western: I agree with Justin, are we testing for a retailer, CC company,?

[11:19:30 AM] Justin Byers: @Michael How realistic is it to create a device like this... which device?

[11:19:52 AM] Michael Larsen: We need to consider what it takes to make one of these.

[11:19:57 AM] Michael Larsen: What parts would we need?

[11:20:02 AM] Justin Byers: Are we working as a tester for a crime syndicate?

[11:20:16 AM] Michael Larsen: If I were working for a credit card company, I would need to verify that this could actualy be made.

[11:20:19 AM] Deb Amigun: @Justin, it is a threat for the card holder and even the RFID scanner company in the sense that the scanner might leave a trace

[11:20:19 AM] Justin Byers: @Michael define "these"

[11:20:24 AM] Michael Larsen: from the video, we can se, clerly, that i can be.

[11:20:25 AM] Shmuel Gershon: @Michael, "one of these" which?

[11:20:25 AM] Timothy Western: Looks like he needed a CC RFID Ready device

[11:20:32 AM] Albert Gareev: [11:09 AM] Weekend Testers Americas:

<<< What is the product?

Who is the customer?

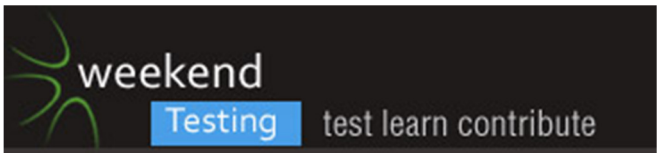
How the product is used?

What product's features in use we observed?

What problems were reported?

How did you recognize a problem?

How you can classify the each problem (threat, risk)?



Can you identify what was a root cause of a problem?

Can you guess what was a root cause of a problem?

Do you suspect there might be more problems, and what problems?

What kinds of tests you would perform to explore the product further?

[11:20:39 AM] Timothy Western: and some computing device that could be connected to it via some cabling means.

[11:20:49 AM] Michael Larsen: So let's start answering these as a group.

[11:20:56 AM] Michael Larsen: First, who is the customer.

[11:21:09 AM] Shmuel Gershon: Michael, the customer of what?

[11:21:22 AM] Shmuel Gershon: You haven't defined the product yet, and I saw at least three inthe video.

[11:21:23 AM] Deb Amigun: The credit card will have a log of where and when it was swiped or in this case scanned?

[11:21:23 AM] Albert Gareev: I helped with the first question: the product is a financial service offered by a bank. Credit card is one of the major features.

[11:21:24 AM | Edited 11:21:46 AM] Michael Larsen: Shmuel, give me a minute, I can't type that fast (LOL!).

[11:21:25 AM] Aleksander Lipski: Cusotome can be both: CC Company

[11:21:52 AM] Deb Amigun: The statment might reveal it as a transaction

[11:22:10 AM] Michael Larsen: The customer of our testing services

[11:22:22 AM] Michael Larsen: and the reason why we are being aske to investigate this problem.

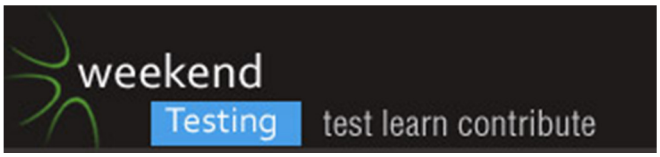
[11:22:33 AM] Timothy Western: So the Customer is a financial institution which uses RFID cards for dispensing of 'beneifts'

[11:22:39 AM] Michael Larsen: Albert has already said it is a financial services firm.

[11:22:48 AM] Michael Larsen: In other words, a maker of RFID credit cards.

[11:23:03 AM] Michael Larsen: Timothy, Yes.

[11:23:16 AM] Deb Amigun: ok



[11:23:23 AM] Shmuel Gershon:

Ok, so we can ignore the protective case presented, we are not 'testing' that one.

[11:23:24 AM] Justin Byers: For customer, I would say: the financial company, the credit card user, the police, possibly other financial companies that we are partnered with

[11:23:28 AM] Timothy Western: come to think of it, they started using cards like this for things like food stamps, andt hose expense plans where you swipe a card and itemize what you spent it on etc.

[11:23:34 AM] Albert Gareev: RFID - feature of the product.

[11:23:40 AM] Albert Gareev: Or is it a bug?

[11:23:42 AM] Justin Byers: I would also say, if this affects passports as well, homeland security may be interested in our findings

[11:23:45 AM] Timothy Western: No its a feature

[11:23:53 AM] Albert Gareev: Or a feature that has bugs?

[11:23:56 AM] Timothy Western: the fact there is a side effect that could be problematic doesn't change that.

[11:24:18 AM] Michael Larsen: Good point, Timothy. Context matters :).

[11:24:31 AM] Shmuel Gershon:

Now, having your credit card number and expiration read by RFID is not more dangerous than handing your credit card to a waiter.

[11:24:35 AM] Lanessa Hunter: @Timothy. Yes, our customer is any consumer of RFId

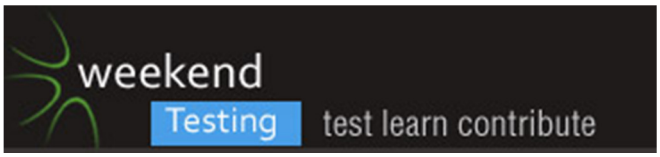
[11:24:48 AM] Albert Gareev: Customers: RFID card owners, passport owners

[11:25:17 AM] Timothy Western: Financial institutions would have incentive to find ways to minimize this risk, so their bottom line isn't threatened by fraudulent transactions.

[11:25:31 AM] Justin Byers: Good point Timothy

[11:25:37 AM] Michael Larsen: So effectively anyone who has an RFID card (both makers and consumers) is our customer here. thanks for the clarification, Albert :).

[11:25:38 AM] Scott Seltzer: And so the customers/potential customers will continue using their service.



[11:26:03 AM] Timothy Western: Could this be similar to other financial transactions, for example, online transactions?

[11:26:27 AM] Linda Rehme: Aren't buisness who accept the RFID cards our "customer" as well?

[11:26:41 AM] Michael Larsen: Linda, yes.

[11:26:53 AM | Edited 11:27:02 AM] Aleksander Lipski: @Linda are they anyhow affected by this device ?

[11:27:33 AM] Linda Rehme: It is a service they supply to their customers.

[11:27:40 AM] Albert Gareev: @Shmuel why do you hand your credit card to a waiter?

[11:27:41 AM] Timothy Western: I'd say depending upon the merchants agreement with the CC company, they could be at risk of loss of money, and no return of product which was fraudulently purchased. (But again that could be contextual)

[11:27:43 AM] Lanessa Hunter: their customers are at risk, therefore their reputation and credibility could be at risk

[11:27:49 AM] Michael Larsen: I think they could be, if the people who use these cards are dissuaded from using them.

[11:27:56 AM] Justin Byers: Yes, businesses for sure. Good one Linda. If we overprotect the RFID to the point where it doesn't work very well at a business, that would be a problem.

[11:28:09 AM] Timothy Western: @Albert some restaurants don't have a check out spot where you hand it pay, and immediately get it back.

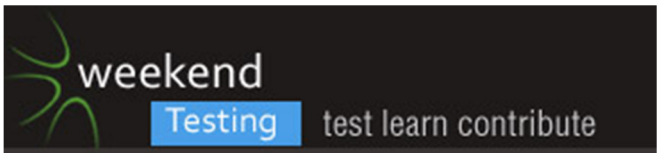
[11:29:01 AM] Albert Gareev: @Timothy, so the purpose is to pay? Your card is an access to your money, right?

[11:29:24 AM] Aleksander Lipski: So for now we 3 groups of customer: CC companys, users(potential users) and business which accept RFID cards

[11:29:29 AM] Shmuel Gershon:

@Albert, it is commong to hand the credit card to service providers. Not only waiters, but other service providers too.

Number, expiration date, name -- these are thigns easy to get.



Or people who buy by phone, for example.

No one that buys over telephone and gives CC data should be that concerned about RFID. :)

[11:29:35 AM] Timothy Western: @Albert it's an access to credit, which potentially could be a cash account, or a credit/pay later account.

[11:30:05 AM] Timothy Western: I'll rephrase my earlier question.

[11:30:15 AM] Timothy Western: We've identified some users of RFID that could be at risk.

[11:30:58 AM] Albert Gareev: [11:29 AM] Shmuel Gershon:

<<< @Albert, it is commong to hand the credit card to service providers. Not only waiters, but other service providers too.Do you *assume* anyone you give your card has a right to use that info any way they want?

[11:30:58 AM] Shmuel Gershon: And different customers -- CC holders, banks, retail business

[11:30:59 AM] Timothy Western: The question I have is, are there similar risks in the financial services industry (Ex online) that could provide ideas for further securing RFID to make even 'E-pickpocketting' more dificult.

[11:31:05 AM] Michael Larsen: So let me ask this question: what do we feel is the risk or potential threat to our customers?

[11:31:39 AM] Timothy Western: The risk is their RFID identity related to the account could be used to post fraudulent charges to their account.

[11:31:47 AM] Justin Byers: personal information being stolen

[11:31:51 AM | Edited 11:32:05 AM] Aleksander Lipski: Risk of accessing to private account or use for online shopping

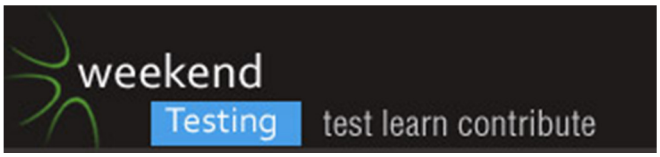
[11:32:25 AM] Justin Byers: loss of money for the financial institutes

[11:32:33 AM] Justin Byers: major inconvenience for users who had their money stolen

[11:32:36 AM] Lanessa Hunter: For financial services company: risk of $ lost in fraudulent charges

[11:32:38 AM] Timothy Western: loss of credit rating to businesses or consumers.

[11:32:52 AM] Scott Seltzer: Risk of jeopardizing our customers' trust and therefore they will stop being our customers.



[11:32:52 AM] Justin Byers: emotional trauma of being robbed

[11:33:00 AM] Michael Larsen: So we see that the potential risk is high, agreed?

[11:33:10 AM] Lanessa Hunter: Agree

[11:33:11 AM] Timothy Western: POtentially, risk of other information being available. Unique identifiers, such as SSN, Passport info, other vital sensitive data.

[11:33:17 AM] Aleksander Lipski: stolen expiration date which can be usefull in taking over new CC

[11:33:27 AM] Timothy Western: Yeah I'd say its a high risk...

[11:33:39 AM] Michael Larsen: Next question (nods to Phil)... what is the likely or actual risk of something like this happening, all things considered?

[11:33:55 AM] Michael Larsen: And do you understand the diference?

[11:33:57 AM] Lanessa Hunter: we have to test that risk

[11:33:59 AM] Albert Gareev: [11:31 AM] Justin Byers:

<<< personal information being stolen ((y)) Living address and date of birth is often good enough to: get access to existing account, open new account, library card, make international phone calls.. shall I continue?

[11:34:00 AM] Timothy Western: The report said they had no instances of such having happened.

[11:34:06 AM] Timothy Western: this guy showed it was possible

[11:34:08 AM] Linda Rehme: We're looking at CC use of RFID but the is a possible future use of the technology for things like medical information or other personal information.

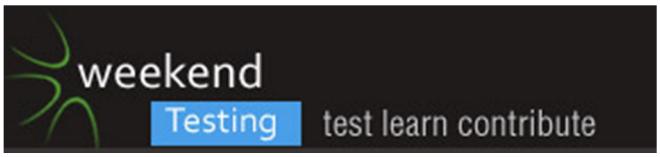
[11:34:16 AM] Timothy Western: but for it to happen you need proximity to someone with that kind of RFID card right?

[11:34:31 AM] Michael Larsen: Timothy, yes.

[11:34:32 AM] Shmuel Gershon:

From Snopes: "The data streams emitted by contactless cards don't include info such as PINs and CVV codes"

[11:34:38 AM] Aleksander Lipski: Being in crowd increase the risk



[11:34:46 AM] Timothy Western: So the risk might be localized to areas with high person density

[11:35:00 AM] Justin Byers: only 20% of credit card holders had the RFID chip

[11:35:17 AM] Timothy Western: As much as I like, Snopes can't guarantee that all Financial institutions, have sufficient safe guards.

[11:35:19 AM] Justin Byers: so it has potential to become a bigger problem in the future as more people move over to this technology

[11:35:24 AM] Shmuel Gershon: (Without the CVV data one cannot use the card to buy without being present, in newer cards.)

[11:35:30 AM] Albert Gareev: [11:34 AM] Timothy Western:

<<< or it to happen you need proximity to someone with that kind of RFID card right?With a strong antenna your proximity is meters!

[11:36:13 AM] Timothy Western: Is this more of a future risk? Or is it a current risk?

[11:36:16 AM] Shmuel Gershon: @Albert, no, I don't think a strong antena can transform than in meters. But not sure.

[11:36:44 AM] Timothy Western: Unless we are going to live in proxmity jamming bubbles around us all the time

[11:36:58 AM] Timothy Western: we eventually will come into contact with people, who could potentially be e-Pickpockets.

[11:37:07 AM] Albert Gareev: [11:36 AM] Shmuel Gershon:

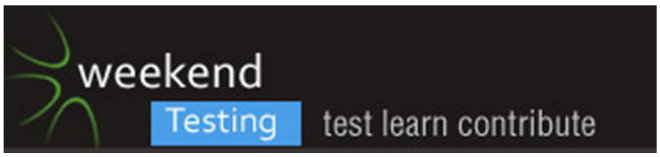
<<< @Albert, no, I don't think a strong antena can transform than in meters. But not sure.You didn't have enough time to explore :) I did. There are even other videos.

[11:37:34 AM] Lanessa Hunter: @ Michael. Likely risk vs. actual risk...

[11:37:40 AM] Shmuel Gershon: @Albert, Ok...

[11:37:46 AM] Shmuel Gershon: @albert it's like tryign to force bluetooth work over dozens of meters.

The card Near Field are close-distance communications.



[11:38:01 AM] Shmuel Gershon: But I don't know enough about the info

[11:38:10 AM] Michael Larsen: @Lanessa, exactly. they are not the same thing.

[11:38:15 AM] Justin Byers: I think if pickpockers are capable of stealing your wallet, they should be more than capable of getting that device right next to your wallet.

[11:38:21 AM] Lanessa Hunter: you are asking us to differentiate between what we saw in the video (likely risk)

[11:38:36 AM] Michael Larsen: Too often, we as testers or when we are answering to stakeholders treat them as though they are.

[11:38:37 AM] Lanessa Hunter: and actual risk - being what we find out based on our "tests"?

[11:38:43 AM] Michael Larsen: We need to be able to make that next step as well.

[11:38:50 AM] Albert Gareev: Some more info on RFID: it's not only *access*. It's a touchless payment. For example, on my card, transactions <$20 do not require PIN or signature to confirm

[11:39:08 AM] Michael Larsen: Sometime we have to calm down our stakeholders who might be freaking out over this news.

[11:39:34 AM | Edited 11:39:41 AM] Aleksander Lipski: @Albert Is the border defined by company or customer (<$20) ?

[11:39:43 AM] Michael Larsen: and reactively planning to spend lots of money to combat a threat that may not warrant such an expense.

[11:39:53 AM] Albert Gareev: That is, by walking in the crowd, you have ability not only stealing for the future, but charging right away.

[11:40:08 AM] Michael Larsen: What can we as testers do to help guide that conversation?

[11:40:09 AM] Lanessa Hunter: @ Michael. I see.

[11:40:10 AM] Albert Gareev: [11:39 AM] Aleksander Lipski:

<<< @Albert Is the border defined by company or customer (<$20) ?Both ways

[11:40:15 AM] Timothy Western: So the question I would ask to that @Michael is what steps, features can be added to the utiliziation of RFID transactions to reduce the usefulness of jacking RFID broadcast

info. The report indicated some ids may not be broadcast, there could be pins for example or verification numbers.

[11:40:58 AM] Michael Larsen: @Timothy, would you ask me, or would you ask the stakeholders ;)?

[11:41:19 AM] Timothy Western: I think that question would be directed at the produces of RFID chips and RFID Readers

[11:41:32 AM] Albert Gareev: #Question. Let's put in a system. If you scanned BOTH passport and card what do you have? What can you do with it?

[11:41:36 AM] Linda Rehme: Most pins are 4 or 6 digits it wouldn't take a computer long to try all the combinations. Are there safegaurds against that?

[11:41:38 AM] Shmuel Gershon:

@Albert, can the communication be closed for authorized reading?

I mean: Do the /cards/ know who is reading them?

[11:41:41 AM] Timothy Western: Very likely the Financial institution in question has a contract with someone to produce these things.

[11:41:51 AM] Linda Rehme: And civ are only 3 digits.

[11:41:52 AM] Michael Larsen: My answer would be that there is a lot of information that can be gleaned from this setup, and that the potential for tampering in sindeed real, but what should the proper response be?

[11:41:59 AM] Timothy Western: THat's a form of 2 factor identification I'd say Albert.

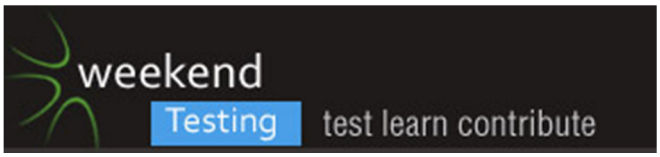
[11:42:05 AM] Timothy Western: You run into the same issue with CAC cards

[11:42:44 AM] Aleksander Lipski: @Shmuel Cards don not know but proxy company do know

[11:42:49 AM] Albert Gareev: @Shmuel, no they (cards) don't

[11:42:53 AM] Michael Larsen: Should it be a better method of masking the data unless proximity is direct? Should there be an encryption algorithm that only asoociated businesses or agencies would have access to? If we did that, how long would that encryption actualy be safe?

[11:43:09 AM] Michael Larsen: I realie that's a bunch of questions as an answer, but you get what I mean (LOL!).



[11:43:22 AM] Timothy Western: what if the there could be a tiny button on the RFID card, that activates its transmission capability? Maybe its heat sensitive or something?

[11:43:44 AM] Timothy Western: Is it necessary for RFID cards to always be broadcasting?

[11:43:47 AM] Timothy Western: is what I'm saying.

[11:44:02 AM] Albert Gareev: Is RFID a pleasant feature? Would you ask for it?

[11:44:04 AM] Aleksander Lipski: @Timothy maybe a finger must be on card to permit any actions

[11:44:20 AM] Scott Seltzer: @Timothy I think that the point of RFID is so people don't have to take it out of their wallet.

[11:44:32 AM] Timothy Western: @Aleksander exactly... of course what if thief steals wallet and takes your finger?

[11:44:41 AM] Justin Byers: There's always that guy's plastic case as well which blocks the transmission

[11:44:43 AM] Linda Rehme: What about a finger print recognition on the card so that the owner had to be holding the card for the reader... aww you type faster than I Aleksander

[11:44:49 AM] Michael Larsen: I remember having this debate about 8 years ago when I worked at a compan ythat was developing fingerprint sensors. Their response was that RFID and other wireles/touch methods had the issues described here, and that the fingerprint aproach would be moch more dificult to crack.

[11:45:12 AM] Timothy Western: @Scott is that how RFID works? Or does it have to be waved over a scanner, just not run through, or a pin or sig?

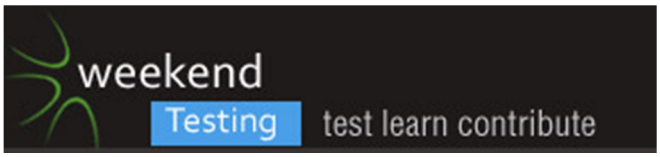
[11:45:14 AM | Edited 11:45:22 AM] Michael Larsen: Stealing finger... wow, now *that's* getting a litle crazy (I hope you mean fingerprint, not actual finger ;)).

[11:45:22 AM] Albert Gareev: [11:44 AM] Justin Byers:

<<< There's always that guy's plastic case as well which blocks the transmissionIt's no plastic. It's metal which blocks magnetic field.

[11:45:34 AM] Scott Seltzer: @Timothy that's what I understood from the video.

[11:45:40 AM] Timothy Western: Which brings me to another question, how do you deal with interference? What if you have more than one RFID card in your wallet?



[11:45:41 AM | Edited 11:45:55 AM] Aleksander Lipski: @michael imagine that your fingerprint was stolen once, you can't have 2nd one

[11:46:26 AM] Shmuel Gershon: @Michael, @Aleksander, also, according to movies, stealing fingerprints is bloody and painful...

[11:46:29 AM] Justin Byers: Should we be trying to solve the problem?

[11:46:36 AM] Timothy Western: @michael Stealing a finger might be an extreme case, but not all countries where RFID is may be considered 'civilized' either.

[11:46:51 AM] Michael Larsen: @Alexander, that's a good point... well, you can if you used only one finger, you have ten you could work with, theoretically, but sorry, this is becoming a tangent :).

[11:46:59 AM] Shmuel Gershon: @Justin, we don't even havea problem defined yet :) -- but talkign about solutions can help us define it

[11:47:03 AM] Linda Rehme: @Timothy maybe you carry a RFID card whose purpose is to block any reading

[11:48:04 AM] Timothy Western: I don't have an RFID card, so I'm not 100% sure how they work, I've not seen any RFID readers around here either, so I'm asking based on what I've read, which admittedly isn't detailed research.

[11:48:40 AM] Shmuel Gershon: @TImothy, if you have a badge for entering your work, or a parking lot that you just tap at the entrance, then you have an RFID card

[11:48:47 AM] Michael Larsen: This also looks to be a cottage indutry developing. Think of it: special sleeves for your credit cards, special shielded wallets, bags lined with a special mesh to block the ability to be read. Clothing with shielding built in... why the possibilities are endless ((smirk)).

[11:49:04 AM] Timothy Western: @Shmuel ooo good point Schmuel, I hadn't thought of that, excellent!

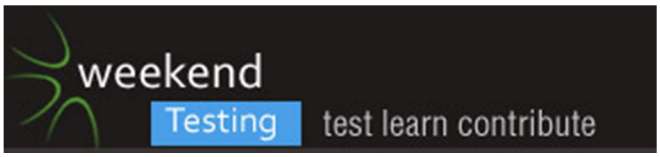
[11:49:23 AM] Michael Larsen: And that brings me to another question we should consider... who else could be a stakeholder in this debate?

[11:49:35 AM] Justin Byers: the police

[11:49:55 AM] Timothy Western: Wallet and purse manufacturers?

[11:49:57 AM] Lanessa Hunter: The technology companies

[11:50:04 AM] Michael Larsen: In other words, who also could profit or be affected by this, outside of the obvious candidates?



[11:50:06 AM] Shmuel Gershon: Who we got?

Credit card companies, banks, users, retail business, policy, wallet manuf...

[11:50:25 AM] Aleksander Lipski: potential thiefs

[11:50:28 AM] Timothy Western: Well if I understand Shmuel, high security facilities, Hospitals, government, education, etc.

[11:50:42 AM] Timothy Western: Depending on how they consume RFID of course.

[11:50:45 AM] Timothy Western: it may not be a risk at all

[11:51:28 AM] Aleksander Lipski: Should we stick to financial use of RFID devices ?

[11:52:31 AM] Michael Larsen: Right, the potential stakeholders for this could be very broad or very narrow. Scope creep could doom any testing approach we decide upon.

[11:52:46 AM] Linda Rehme: That depends on which end of the problem you try to protect. Do you protect the reading of the card or at the end where the fraudulent transaction is made?

[11:53:12 AM] Linda Rehme: If you protect the reading of the card it covers multiple industries.

[11:53:33 AM] Timothy Western: @LInda What if a reader is compromised?

[11:53:37 AM] Justin Byers: I would say your personal information getting stolen is much more likely to happen at a reader that has been hacked in a store rather than by some dude on the street

[11:53:41 AM] Shmuel Gershon: Snopes mentioned data encryption on the card -- how does encryption affects our conversation?

[11:53:52 AM] Lanessa Hunter: @Linda. I would think for the benefit of all stakeholders, you'd want to protect both. especially considering non-financial aspect. building security, for example

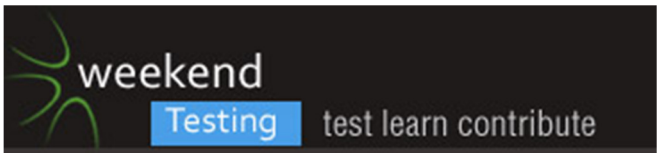
[11:54:22 AM] Timothy Western: @Shmuel encryption implies some kind of cryptography applied to scramble the data, so that only authorized devices can unlock it. What kinds of devices are authorized though?

[11:54:44 AM] Michael Larsen: OK, so I think we have deterined the risk factors and the potential danger, as well as the likelihood of actual dangers.

[11:54:58 AM] Michael Larsen: Let's defocus a bit and ask some different questions now...

[11:55:08 AM] Michael Larsen: So where's the bug?

[11:55:21 AM] Michael Larsen: Or bugs?



[11:55:22 AM] Lanessa Hunter: in the design -

[11:55:26 AM] Aleksander Lipski: Is there a bug ?

[11:55:40 AM] Michael Larsen: There is indeed :).

[11:55:47 AM] Scott Seltzer: Security wasn't considered properly in the design.

[11:55:59 AM] Michael Larsen: think back to the video.

[11:56:10 AM | Edited 11:56:21 AM] Michael Larsen: what was the "thief" able to construct?

[11:56:37 AM] Timothy Western: The bug is feature might be poorly implemented.

[11:56:38 AM] Justin Byers: We don't know if security was considered or not, but we do know it wasn't fixed

[11:56:44 AM | Edited 11:56:54 AM] Aleksander Lipski: If we let any devices read secure informaiton without opening the pocket than we should asssume that anyone can do this on the street with proper device

[11:56:50 AM] Michael Larsen: think about the construction of the device in the feature.

[11:57:10 AM] Michael Larsen: @Aleksander, you are part o the way there, yes.

[11:57:14 AM] Justin Byers: @Michael The thief just had a reader that you'd find in the store in a bag

[11:57:26 AM] Justin Byers: Based on my observations, he didn't have to construct much himself

[11:57:35 AM] Michael Larsen: think about it, the security is so light that a card reader and a netbook is all that's needed to compromise the security iof the cards.

[11:57:35 AM] Justin Byers: And he said himself, he bought it online for $100

[11:57:52 AM] Michael Larsen: @Justin, you got it :).

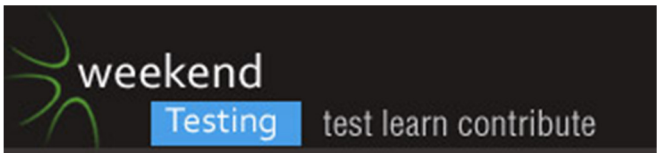
[11:58:23 AM] Michael Larsen: So let's continue down this line, if I may be so bold :).

[11:58:29 AM] Shmuel Gershon:

@Michael what bug is there in being able to buy for $100?

[11:58:31 AM] Justin Byers: So, how do you protect against something that is an intended use?

[11:58:41 AM] Michael Larsen: Is the issue with the technology, or with the implementation?



[11:58:44 AM] Lanessa Hunter: there are no checks in place b/n the communication from the RFID to the reader - nothing in place to prevent the communication

[11:59:36 AM] Lanessa Hunter: @Michael, perhaps both

[11:59:40 AM | Edited 11:59:53 AM] Aleksander Lipski: technolgy allows you to do anything , the implemation is desigend because both parts agreed that want such fragile thing

[11:59:49 AM] Scott Seltzer: I say the technology works as it should. The implementation is bad because it can work without the card holder's intent.

[12:00:10 PM] Shmuel Gershon:

@Michael / @Justin , why being easy to build makes it a bug?

If it was something he had to construct at home, then it would not be a bug?

Hackers are quite resourceful, you know.

I'm more afraid of devices that are unknown than of things that are easily built and perhaps more known to relevant people.

[12:00:38 PM] Justin Byers: @shmuel the problem is, the device is doing what it is supposed to do. it's the same device you find at the store

[12:00:43 PM] Lanessa Hunter: technology should include safeguards in its implementation

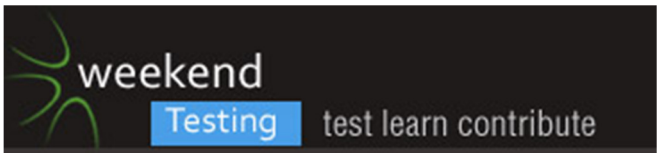
[12:00:52 PM] Scott Seltzer: In terms of the problem being with the technology, I'd say that maybe essential features might be missing...

[12:01:04 PM | Edited 12:01:11 PM] Weekend Testers Americas: OK, everyone, we're at the 12:00 PM mark, but this time, irthink we are doing good with the discussion and would like to hold off on the debrief foa while longer.

[12:01:09 PM] Shmuel Gershon: @Justin, I don't see a problem with that

[12:01:45 PM] Michael Larsen: So here's a thought...

[12:01:49 PM] Justin Byers: @Shmuel How do you combat the misuse of a device if the misuse is the same as regular use?



[12:02:10 PM | Edited 12:02:57 PM] Michael Larsen: Is the speed in which the device is being read, or the power of the sensor perhaps part of the problem?

[12:02:32 PM] Scott Seltzer: Seed?

[12:02:43 PM] Albert Gareev: [12:00 PM] Shmuel Gershon:

<<< If it was something he had to construct at home, then it would not be a bug?You buy a reader; a program; a laptop; you plug a reader via USB port and install the soft. Not so much work.

[12:02:48 PM] Lanessa Hunter: combat through safeguards on interfaces/interfacing transactions

[12:02:57 PM] Albert Gareev: There are online guides how to make such a device

[12:03:03 PM] Michael Larsen: speed, sorry, corrected.

[12:03:10 PM] Scott Seltzer: Thanks.

[12:03:30 PM] Justin Byers: @Michael certainly if there was no sensor, this wouldn't be a problem

[12:03:37 PM] Michael Larsen: Is the encryption algorithm too simple?

[12:03:41 PM] Aleksander Lipski: @Micheal good points, if we decrease speed, would this affect te customer ?

[12:03:45 PM] Justin Byers: no RFID chip I mean

[12:04:03 PM] Shmuel Gershon: @Albert, I am saying that the problem exist in the exact same way

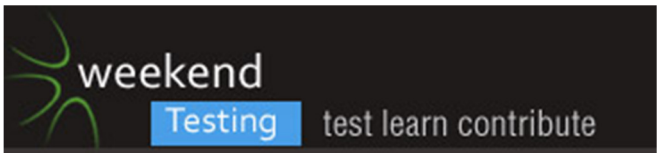
if you can buy a Card-Steal-o-Scanner at HomeDepot

or if you have to build it from resistors and wires.

[12:04:10 PM] Michael Larsen: Is the fact that a sensor and a netbook all that was needed to capture this data at all telling?

[12:04:11 PM] Scott Seltzer: I think that one solution might be better feedback. If the card beeped when a transaction went through, then the user might know. Perhaps it could also be set up to send a message to your bluetooth headset when a transaction happened.

[12:04:41 PM] Justin Byers: @Michael It implies to me that there isn't much in the way of security happening



[12:04:53 PM] Shmuel Gershon: @Michael, I don't think so. Bad guys are not afraid of complexity. If it is easy or if it is hard does not affect how dangerous it is.

[12:05:09 PM] Linda Rehme: This is similar to the problem of secure communications on the web where we have signature agencies to verify the server that you are contacting.

[12:05:12 PM] Michael Larsen: @Scott, OK, interesting, these seem like good engineering approaches to solving the problem, but do we feel that we understand what the bug is?

[12:05:14 PM] Justin Byers: Why does the vendor need such easy access to the credit card number? Isn't it just the financial institute which needs that information?

[12:05:16 PM] Timothy Western: @Scott beep is interesting, but if its in the wallet in a crowded loud area, you may not notice it. Plus, you'd be announcing to everyone you used an RFID chip, perhaps heightening risk.

[12:05:50 PM] Scott Seltzer: Yes, the data collection should be encrypted so it has to be approved by the credit card company without the business intermediary seeing the numbers in any meaningful way.

[12:05:59 PM] Albert Gareev: @Michael, if a netbook can decrypt data in a second of communication then the encryption is too simple

[12:06:12 PM] Michael Larsen: @Albert, right!

[12:06:18 PM] Justin Byers: Still, as Shmuel mentions, bad guys aren't afraid of complexity, so even if it was encrypted, I'm sure they could get around it

[12:06:19 PM] Michael Larsen: Can you elaborate a bit more on that?

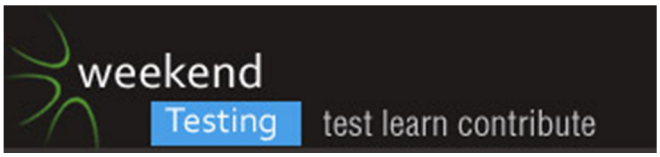
[12:06:42 PM] Michael Larsen: @Justin, you are correct, bad guys can get around things if they really want to.

[12:06:43 PM] Justin Byers: To me, the problem seems to be with the RFID chip, having such valuable information available to pick up through the air

[12:07:09 PM] Aleksander Lipski: @Justin feature which is a bug ?

[12:07:11 PM] Timothy Western: @Justin but the battle between encryption and processing power will always be back and forth won't it be? I don't think encryption alone is sufficient reason to change the encryption. It might be part of a solution, its not enough of ofone IMO.

[12:07:11 PM] Michael Larsen: But we as engineers (and as testers) can raise the issue to make it just that much more dificult for them, too).



[12:07:13 PM] Albert Gareev: The *right* (wanted by a customer) communication should be quick; has to be long/hard/impossible in the ways of unwanted use

[12:07:17 PM] Shmuel Gershon:

@Michael, @Albert, er... how does the speed by which an authorized device decrypts data tells anythign about how well it is encrypted?

[12:08:08 PM] Shmuel Gershon: Unauthorized decryption takes time. Authorized decryption can be quick even for strong algorithms

[12:08:21 PM] Timothy Western: Brute force methods

[12:08:22 PM] Justin Byers: @timothy yes, I agree. encryption can always be broken by those persistent enough

[12:08:35 PM] Michael Larsen: @Shmuel, I'm not entirely sure it does, but if there is a little more time in the process, or requre a litle more horsepower to do, it might make such "portable scanners' much less effective.

[12:08:38 PM] Shmuel Gershon: @Tim, brute force is for unauthorized decryption

[12:08:41 PM] Albert Gareev: @Shmuel: RFID is driven by a chip on the card. It's not like "read me". It's a 2-way communication procedure

[12:08:46 PM | Edited 12:09:17 PM] Aleksander Lipski: looking on the big picture, don't you think that CC company didn't know this potential risk before ?

[12:08:59 PM] Timothy Western: but in this case he used a reader just like you might see at a legitimate biz

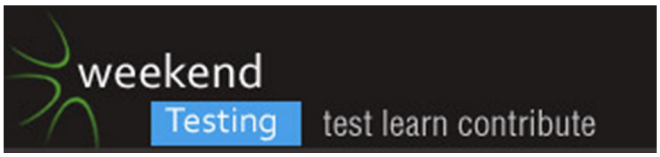
[12:09:21 PM] Michael Larsen: Again, this is my limited understanding of this technology working. I'd likely have a different opinion and approach were Ito discuss this with a security expert.

[12:09:34 PM] Shmuel Gershon: @Aleksander, one of the question is if they care about this potential risk.

And maybe the potential is not so potential and the irsk not so risk?

[12:10:09 PM] Michael Larsen: @Shmuel, abslutely right. that's why I made the distinction between potential risk and actual risk.

[12:10:33 PM] Michael Larsen: not to totally derail this discussion, but sometimes the potential and actual risks never match up.



[12:11:15 PM] Shmuel Gershon:

To analyze that, we can back of and ignore RFID for a second.

Credit Card companies print the CC number on top of the card.

Aren't they aware of the risk on that? Do they care?

[12:11:20 PM] Timothy Western: Could there be a comparison here between how RFID works, and how SSL and TLS work for secure internet transmissions?

[12:11:37 PM] Justin Byers: I think it is interesting that the credit card companies probably had a discussion about how the convenience of this feature for users was worth the minor risk of this type of theft

[12:12:51 PM | Edited 12:13:03 PM] Aleksander Lipski: Convienence for users means bigger profit for companies

[12:13:24 PM] Albert Gareev: If we look at RFID passports, is the risk of identity theft a bee or a hornet? For a person? For a security?

[12:13:50 PM] Linda Rehme: @Timothy I absolutely think there is a comaprison. You need for the sender (CC) and receiver(banking institution) to be able to identify each other.

[12:14:21 PM] Timothy Western: @Linda exactly my thinking, and those are published standards, lots of servers and clients have that capability today.

[12:14:31 PM] Linda Rehme: @timothy to identify each other securely.

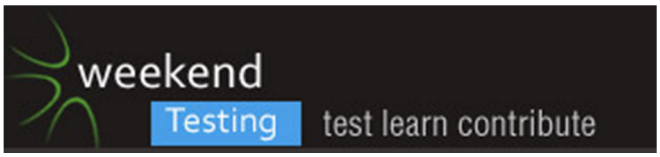
[12:14:54 PM] Timothy Western: Is having an RFID reader sufficient for making use of RFID information for a transaction? Or is there another step in authentication, out in the network/internet layer there?

[12:15:19 PM] Linda Rehme: If they can't identify who they are talking to then no transaction would take place.

[12:15:30 PM] Albert Gareev: [12:15 PM] Timothy Western:

<<< Is having an RFID reader sufficient for making use of RFID information for a transaction?

[12:15:47 PM] Shmuel Gershon: @Tim, @Linda, SSL and TLS require sides to know who they are talking too.



I asked @Albert if the card can't know who is reading it.. he said no.

[12:16:18 PM] Shmuel Gershon: @ALbert, like we wrote above, CVV or PINs are not transmitted in RFID. So depends on which transactions.

[12:16:29 PM] Albert Gareev: @Shmuel ..but you can question that :)

[12:16:33 PM] Linda Rehme: But couldn't the reader know who it is talking to?

[12:16:33 PM] Shmuel Gershon: Remote transactions less than other RFID transactions

[12:16:45 PM] Timothy Western: my understanding of how CC readers in the past have worked, is that people buy them from some vendor who handles that routing. So those who have it, would have to somehow be legitimate businesses. Plus might the RFID reader have unique information indicating who's it is?

[12:17:41 PM] Timothy Western: So if someone stolle an RFID reader, that would get reported eventually, or if a reader was detected as being used for Fraud could aid adjudication of the fraud.

[12:17:45 PM] Scott Seltzer: @Timothy that can be forged/spoofed/stolen.

[12:17:47 PM] Weekend Testers Americas: @Deb, @Lanessa, what are your thoughts on how to approach this?

[12:17:54 PM] Lanessa Hunter: @Timothy."Plus might the RFID reader have unique information indicating who's it is?"

[12:18:10 PM] Shmuel Gershon: (@Albert, oh, I can question a lot on this WT session :), but am more rolling on.

I have too little domain knowledge to make a useful conversation on this...)

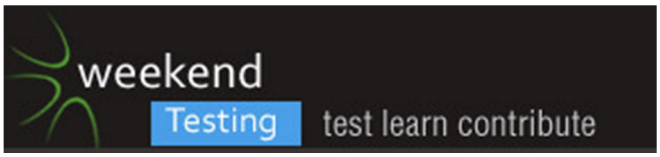
[12:18:13 PM] Timothy Western: @Scott Without knowing more about how any individual RFID reader works, I'd say that's possible, but could such things be built in that are not spoofable?

[12:19:01 PM] Lanessa Hunter: CC companies would have an agreement with the vendor, so I think that safeguard would be in place to prevent a a fraudulent transaction

[12:19:14 PM] Shmuel Gershon: @Timothy, no need for proxy or vendor.

[12:19:26 PM] Weekend Testers Americas: Time check ((o))

[12:19:32 PM] Albert Gareev: @Shmuel you wanted to assume it does. If it does, where it goes? If we take that as a fact, how it aligns with other facts?



[12:19:56 PM] Shmuel Gershon: RFID readers send the data to where you want, connect it over USB and you get the read data

[12:20:31 PM] Weekend Testers Americas: OK everyone, we could carry this on for hours, but we do have a time limit :).

[12:20:39 PM] Aleksander Lipski: What we are now discussing , sorry I am lost :)

[12:20:54 PM] Lanessa Hunter: didn't we say that CVV and PINs are not transmitted

[12:20:58 PM] Weekend Testers Americas: It's time to bring it back together and start the debrief.

[12:21:00 PM] Timothy Western: but is the data read significant for a transaction to be processed? Isn't there a clearing house for CC transactions?

[12:21:13 PM] Weekend Testers Americas: Or in this case, let's see how we did based on the mission and charter.

[12:21:29 PM] Weekend Testers Americas: Let's look at ourt questions and see if we answered them.

[12:21:34 PM] Weekend Testers Americas: [11:08 AM] Weekend Testers Americas:

<<< What is the product?

Who is the customer?

How the product is used?

What product's features in use we observed?

What problems were reported?

How did you recognize a problem?

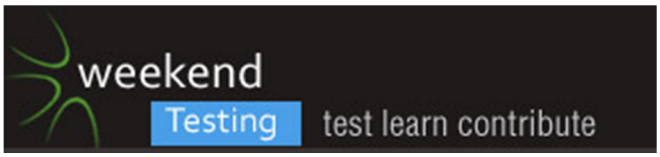
How you can classify the each problem (threat, risk)?

Can you identify what was a root cause of a problem?

Can you guess what was a root cause of a problem?

Do you suspect there might be more problems, and what problems?

What kinds of tests you would perform to explore the product further?



[12:22:18 PM] Michael Larsen: Overall I think we dida good job of identifying the customer, the use of the product and the product features.

[12:22:39 PM] Michael Larsen: We recongnized a number of problems and reported quite a few.

[12:23:15 PM] Michael Larsen: I think we have an idea as to the root cause of the problem if not specifically the root cause. I think the guesse are very sound and well reasoned.

[12:23:53 PM] Michael Larsen: I think the discussion of risk was very good and the strongest of the lot. Maybe we spent too much time on it, actually, but that may be my fault ;).

[12:25:08 PM] Michael Larsen: Now please... do *NOT* let my thoughts be the end of this discussion. I'm the facilitator, but I do not have final say on any of this. If you think I'm wrong about any of these areas, by all means call me on it!

[12:25:41 PM | Edited 12:25:46 PM] Aleksander Lipski: Did we find any further tests ?

[12:26:08 PM] Justin Byers: I think we did a good job exploring other problems that might arise from this kind of technology

[12:26:16 PM] Linda Rehme: We didn't specifically discuss what kinds of test we would perform although we raised plenty of questions that would have required further investigation.

[12:26:20 PM] Justin Byers: which to me would be further tests

[12:27:02 PM] Timothy Western: There are other potential bugs of course, but how many result in harm to the people consuming them? Example if RFID can be read in your wallet, and you have more than one RFID card....The interference combined might not constitute a material loss for using the RFID, that's something I'd assume would have to be considered in the implementation of the solution.

[12:28:39 PM] Shmuel Gershon:

Did we have anyone with Domain Knowledge about this? I would have liked to have one.

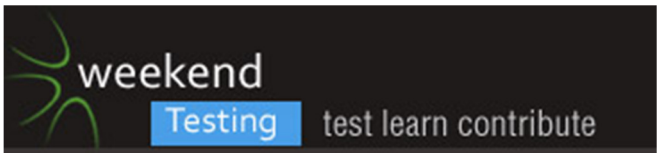
[12:28:46 PM] Aleksander Lipski: @Timothy may be little offtopic but from my experience having 2 parking cards wich interfere eventually leads to damage

[12:29:05 PM] Aleksander Lipski: and need for card replacement

[12:29:08 PM] Justin Byers: @Shmuel Having no domain knowledge, good point... That's an issue

[12:30:19 PM] Justin Byers: Did anyone take good notes on the points we discussed?

[12:30:32 PM] Lanessa Hunter: we spent time discussing root cause(s) of the problem and the risks. do we have a consensue about the actual risk?



[12:31:08 PM] Albert Gareev: What questions you'd ask to a SME, then?

[12:31:16 PM] Timothy Western: I actually have seen a problem with having 2 RFID cards in a slightly different situation. When close together, reader wouldn't read them, but by bringing one closer, and separating, the interference was nullified.

[12:31:21 PM] Lanessa Hunter: I understand that's where our furthers tests would come into play and the SME.

[12:32:13 PM] Timothy Western: really talking about only a centimeter of difference to really get it to read the right one in the case I saw. So could that risk be mitigate dby having them on opposite sides of the Wallet?

[12:32:22 PM] Albert Gareev: If you had a device like that guy had (reader+netbook) what kinds of tests you'd try?

[12:32:52 PM] Timothy Western: Varied Distance from RFID card

[12:33:02 PM] Timothy Western: Varied levels of insulation/cloting/packing/covering between card and reader

[12:33:12 PM | Edited 12:33:33 PM] Aleksander Lipski: More than one RFID card together

[12:33:32 PM] Justin Byers: I'd try a variety of credit cards to see what information I get from each one

[12:33:37 PM] Michael Larsen: I would try to see how many methods I could come up withn to stymie the card reader.

[12:33:49 PM] Linda Rehme: placing car remote near the CC for interference

[12:33:53 PM] Timothy Western: Maybe other types of signals active nearby, cordless phone, AM/FM radio, blue tooth networks, etc.

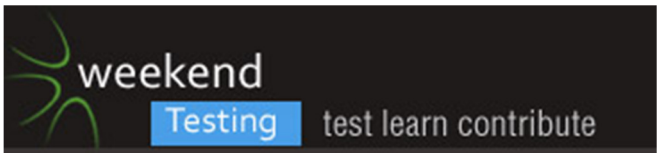
[12:33:55 PM] Michael Larsen: Proximity tests, determine which materials might nullify the ability to read the card.

[12:34:02 PM] Michael Larsen: Orientation of cards.

[12:34:26 PM] Michael Larsen: Radio frequencies (such as having my MP3 player receiving FM signals, etc.

[12:34:32 PM] Albert Gareev: Would you try a performance test? For what purpose?

[12:34:37 PM] Michael Larsen: Shieding of diferent kinds.



[12:34:41 PM] Justin Byers: I'd test the battery life of the device. If I only have enough battery to steal 5 credit cards, it might not be worth it.

[12:34:48 PM | Edited 12:34:55 PM] Aleksander Lipski: I would try to determine time range for device to stole the information

[12:35:15 PM] Justin Byers: @Albert You'd want to make sure it gets the information fast.

[12:35:34 PM] Albert Gareev: [12:34 PM] Aleksander Lipski:

<<< I would try to determine time range for device to stole the informationCan you explore further on that?

[12:35:49 PM] Lanessa Hunter: speed, distance - those things seem to point to performance tests and reliability

[12:35:57 PM] Michael Larsen: Agree with battery life tests, with stacking different cards with RFID chips to see if it could read one or others.

[12:35:59 PM] Albert Gareev: [12:35 PM] Justin Byers:

<<< @Albert You'd want to make sure it gets the information fast./Why/ it needs to be fast?

[12:36:02 PM] Linda Rehme: Time from stealing the information to putting through a fraudulent transaction?

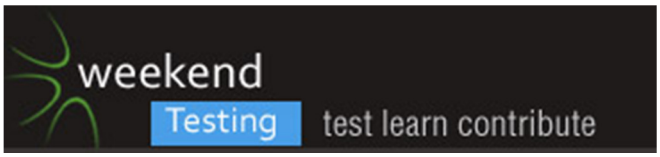
[12:36:23 PM] Scott Seltzer: I would make sure that the device doesn't beep and say in loud voice, "Credit card information retrieved!"

[12:36:33 PM] Justin Byers: LOL @ Scott

[12:36:37 PM] Aleksander Lipski: @Albert what is the shortest time to steal the inforamtion, in othr words how long it takes to steal the information

[12:36:44 PM] Michael Larsen: from the persective of a potential thief, time is of the essence. If I were to see someone standing next to me for an extened period with a device at my trousers, I might get suspicious.

[12:36:46 PM] Lanessa Hunter: i'm kinda stuck on the actual info that can be obtained by the reader and what the "bad guy" can do with it beyond that in terms of financial transcations



[12:37:18 PM] Michael Larsen: @Lanessa, there's two issues at play here. the actual santioned transactions, and the potential for misuse.

[12:37:21 PM | Edited 12:37:34 PM] Albert Gareev: [12:36 PM] Michael Larsen:

<<< from the persective of a potential thief, time is of the essence. If I were to see someone standing next to me for an extened period with a device at my trousers, I might get suspicious.But as a customer would you want to stand long time at the counter?

[12:37:30 PM] Scott Seltzer: How frequent can you read cards. Do you have to wait in between each reading until an answer is returned or can you already start scanning the next?

[12:37:47 PM] Lanessa Hunter: @michael. thanks for separating those for me. that helps me think a bit more clearly about it

[12:38:04 PM | Edited 12:38:21 PM] Michael Larsen: Is there a balance beteeen the two? Can we make a system that is sufficiently quick to be effective in a business setting, yet slowed down by other factors to make misuse in the manner described less appealing?

[12:38:54 PM] Michael Larsen: In truth, I don't have the answer for that, but I could create a matrix that shows how certain approaches affect the signal and time to process.

[12:39:03 PM] Linda Rehme: Try to tamper with a reader to hijack the financial information

[12:39:08 PM] Justin Byers: Thieves can usually find a way around those safeguards

[12:39:19 PM] Michael Larsen: from there, the stakeholders can determine if that mitigates the risk or if additional measures would be required.

[12:39:37 PM] Michael Larsen: @Justin, absolutely. Very little will stop a determined thief.

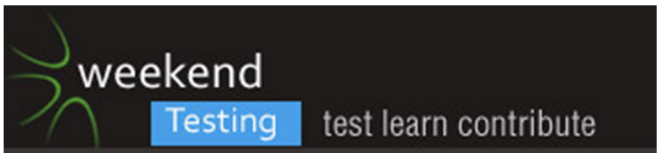
[12:39:38 PM] Linda Rehme: Can I retrieve the information from the reader for later use?

[12:39:39 PM | Edited 12:40:03 PM] Albert Gareev: Where are we going: to prevent from stealing data or to prevent from using the stolen data?

[12:39:40 PM] Justin Byers: Plus it introduces the risk that it could go slow in a legitimate case

[12:39:59 PM] Lanessa Hunter: I like matrices:)

[12:39:59 PM] Michael Larsen: So again, we have deermine additional test cases now.



[12:40:14 PM] Scott Seltzer: I would check that unexpected data doesn't cause problems. For example if it is expecting a date but gets a string, then the software shouldn't have problems continuing.

[12:40:16 PM] Michael Larsen: How have we donw with the questions?

[12:40:23 PM] Aleksander Lipski: Yes additional tst cases were highlighted now:)

[12:40:36 PM] Weekend Testers Americas: [12:21 PM] Weekend Testers Americas:

<<< What is the product?

Who is the customer?

How the product is used?

What product's features in use we observed?

What problems were reported?

How did you recognize a problem?

How you can classify the each problem (threat, risk)?

Can you identify what was a root cause of a problem?

Can you guess what was a root cause of a problem?

Do you suspect there might be more problems, and what problems?

What kinds of tests you would perform to explore the product further?

[12:40:54 PM] Lanessa Hunter: i believe we've done pretty well with the questions

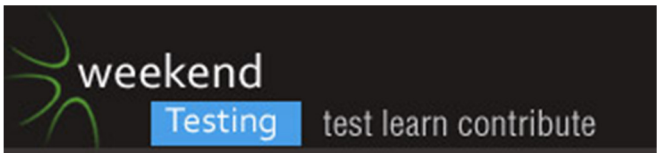
[12:40:58 PM] Shmuel Gershon: @Scott, yes, it would be funny.

I'll start carrying fake RFID card sending malformed data, to hack the thieves' reader!

[12:41:00 PM] Albert Gareev: What is the actual problem with RFID?

[12:41:18 PM] Lanessa Hunter: kaching!

[12:41:28 PM] Shmuel Gershon: @Albert, there is no problem with RFID.



[12:41:37 PM] Albert Gareev: *Reverse*: what problem you DON'T have with a card that doesn't have RFID feature?

[12:41:50 PM] Aleksander Lipski: That the ease of use is same for customer and potential thief

[12:42:08 PM] Justin Byers: @Albert It makes your personal information more accessible

[12:42:16 PM] Justin Byers: It's both a problem and a benefit

[12:43:00 PM] Timothy Western: is the ease of access really a problem?

[12:43:13 PM | Edited 12:43:28 PM] Michael Larsen: The issues with RFID in my opinion that are not present when you have to scan the actual stripe, or get a reading off the cards is time. the technology makes a tradeoff between convenience and security.

[12:43:15 PM] Timothy Western: or is it the consumption of what can be retrieved via some RFID Reading device that's the problem?

[12:43:45 PM] Justin Byers: @Michael very nicely put

[12:43:46 PM] Timothy Western: I can get your License plate number from your car, but there's very little I can do with it beyond maybe find your address or court records I believe.

[12:44:35 PM] Timothy Western: 70.07.

[12:44:49 PM | Edited 12:45:04 PM] Aleksander Lipski: @Timothy, you are right I have assumed that CCards always need to have secure information

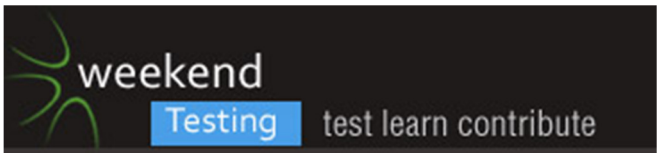
[12:45:02 PM] Michael Larsen: While it's true that it's possible to have our card information compromised by the person we hand the card to, there's a number of steps that have to be done, an those take time to perform.

[12:45:07 PM] Timothy Western: I know each of your names from this Skype chat for example, doesn't mean that's necessarily something I can do something with by itself.

[12:45:09 PM] Albert Gareev: How the process of purhasing with RFID card is different from the one with a swipe card?

[12:45:39 PM] Michael Larsen: Databases can be hacked, systems can be stolen, but those require a focused and deliberate attempt at theft with potential barriers (not impossible to overcome, but they are there).

[12:45:40 PM] Aleksander Lipski: @Timothy but this can be 1st step



[12:45:42 PM] Justin Byers: @Albert The card has to be removed from your pants, so you're more aware that it might be vulnerable

[12:46:01 PM] Lanessa Hunter: process/physical process might be different, but the data interchange and checks might also be different

[12:46:19 PM] Michael Larsen: With the RFID system, we have shown that the potential to steal that information is real, albeit not rampant, but it can be done much more easily that traditional methods.

[12:47:25 PM] Timothy Western: @Michael @Aleks right, my point though, is without knowing what information beyond Expiration, etc is available from a reader, makes it difficultto say that its information that is compromisable. If an RFID Chip makes a unique ID for each transaction for example, you might steal one transaction, and then its no good, you'd almost need real time access to taht RFID card in close proximity to continue to charge it, and that might show up as fishy on a security scan of transactions.

[12:47:30 PM] Michael Larsen: So yes, in a way, the conveniuence factor is the bug. It all depends on how you want to look at it.

[12:47:51 PM] Michael Larsen: Would I advocating scraping all RFID devices because there is the potential for havking in this way? No.

[12:48:17 PM] Timothy Western: I would definitily push back at the SME on the product with a question of what information is emitted, and how its expected to be consumed.

[12:48:41 PM] Lanessa Hunter: @timothy, yes

[12:48:45 PM] Michael Larsen: Do I think it makes sesnse to be aware of the risk and perhaps know how to mitigate those risks, yes.

[12:49:01 PM | Edited 12:49:12 PM] Michael Larsen: Am I out of my league when talking about a lot of this stuff. Right now, definitely (LOL!).

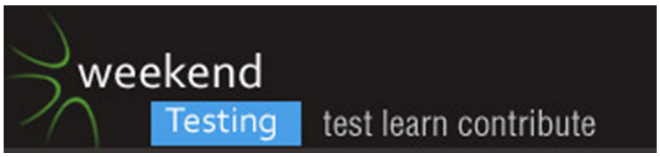
[12:49:09 PM] Justin Byers: Haha

[12:49:30 PM] Albert Gareev: [12:45 PM] Justin Byers:

<<< @Albert The card has to be removed from your pants, so you're more aware that it might be vulnerableYou still have to take RFID card and bring it close to a conventional reader at the store. You don't say: "tap my pocket" :)

[12:49:32 PM] Lanessa Hunter: @michael. i think we're in the same boat as you:)

[12:50:06 PM] Justin Byers: @Albert Haha good point.. although maybe next time I *will* say that ;)



[12:50:33 PM] Lanessa Hunter: i keep thinking about my RFID badge for work and wondering if a reader could be used to create a replicated card

[12:50:36 PM] Timothy Western: Without having the specs on a particular RFID Card/Reader solution, its difficult to understand how that information is consumed by the reader, and then used to complete a transaction hand shake between the reader and vendor of the reader data for clearing to the financial account being used to remit payment..

[12:51:05 PM] Timothy Western: wow that was a mouthful

[12:51:49 PM | Edited 12:51:58 PM] Albert Gareev: Some further reading (easy to find on google) : http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid5.htm

[12:51:58 PM] Lanessa Hunter: I'm sure my work card is not as secure as a Dept of Defense CAC card

[12:52:30 PM] Albert Gareev: Two possible forms of identity theft that could occur with e-passports are:

•Skimming happens when someone uses an RFID reader to scan data from an RFID chip without the e-passport holder's knowledge.

•Eavesdropping happens when someone reads the frequencies emitted from the RFID chip as it is scanned by an official reader.

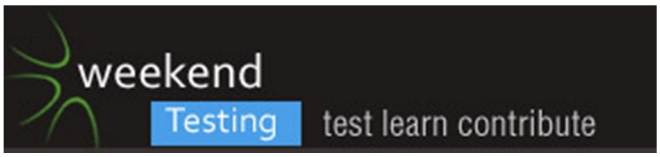
[12:52:33 PM] Timothy Western: I think this has been an excellent session., which reminds me of another potential user, stores putting RFID on certain products for loss prevention

[12:52:51 PM] Albert Gareev: However, the DHS insists that the e-passport is perfectly safe to use and that proper precautions have been taken to ensure user confidentiality.

•For protection against skimming, the e-passport contains a metallic anti-skimming device. This device is a radio shield inserted between the passport's cover and first page. When the e-passport is closed, it can't be scanned at all; when it's open, it can only be read by a scanner that is less than 10 centimeters away [source: Department of State].

•To guard against eavesdropping, DHS has mandated that all areas where the e-passport is scanned be thoroughly covered and enclosed so that signals cannot be picked up beyond the authorized RFID reader.

[12:54:02 PM] Timothy Western: Good article Albert.



[12:54:11 PM] Justin Byers: @albert I wonder if those safeguards are either not practical for credit card companies (they don't have a cover) or are too expensive

[12:54:36 PM] Michael Larsen: I'm endlessly surprised at the way that many of these sessions turn out. I suppose I shouldn't be (LOL!). It's always fun to see the different perspectives that are brought out, and answers to questions I would not have considered to ask, which leads to additional questions and ideas.

[12:55:31 PM] Lanessa Hunter: Thanks for organizing the session, Michael, and thanks to all for the great questions and discussions

[12:55:51 PM] Timothy Western: yes great session, Michael. I"m glad I attended :D

[12:55:58 PM | Edited 12:56:51 PM] Michael Larsen: I think the key for us as testers is that we owe i to ourselves and our stakeholders to keep considering things that are maybe beyond our understanding. I know if I was tasked with this issue today as a lone tester, I'd be scrambling, but with everyone's feedback, I think we came up with a good approach.

[12:56:13 PM] Justin Byers: Yah that was an interesting discussion and another indication that testing starts as soon as you start thinking

[12:57:07 PM] Shmuel Gershon: It was also an indicatio that you need people with Domain Knowledge on the team, else you mostly speculate.

[12:57:09 PM] Michael Larsen: So a quick question for our first timers.

[12:57:09 PM] Lanessa Hunter: Good lesson in that, Michael. - those things we did not consider, that other teammates would

[12:57:12 PM | Edited 12:57:21 PM] Aleksander Lipski: and the limited knowledge and understanding decrease with number of participants

[12:57:28 PM] Michael Larsen: Did this experience meet your expectations?

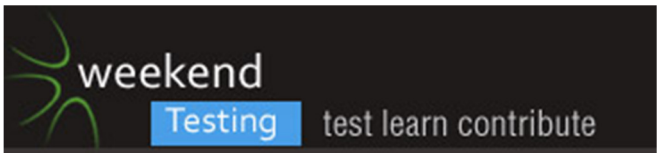
[12:57:47 PM] Scott Seltzer: No, I was expecting something with more practical hands-on testing.

[12:58:08 PM] Scott Seltzer: This was more like a brainstorming session.

[12:58:12 PM] Timothy Western: I had no expectations. This was my 2nd WTA attendance I believe.

[12:58:34 PM] Timothy Western: Then again, I didn't think to come till pinged that it was today either, :D

[12:58:57 PM] Linda Rehme: I agree with Scott, but I enjoyed it immensly. It was a "get my brain thinking in a different way" good.



[12:59:12 PM] Michael Larsen: @Scott, OK, thanks for letting us know. We try to vary the approaches, but we can make sure the next session involves a hands on product to play with (I have one in mind for the next session already :)).

[12:59:13 PM] Scott Seltzer: I liked some of the discussion on possible test cases but that came in very late and wasn't enough of the session.

[12:59:13 PM] Timothy Western: I love discussions like this.

[12:59:15 PM] Lanessa Hunter: Yes, it met my expectations in that the group was given a mission and came up with testing-related questions to figure out a plan of attack so-to-speak, but like Scott, I was also expecting hands-on. There was alot of value in the session for me.

[12:59:24 PM | Edited 12:59:48 PM] Aleksander Lipski: It was my 3rd WTA session, having the previuos experience I haven't epxected much as it always turn to the other direction

[1:00:10 PM] Lanessa Hunter: Ditto @ Scott. I dug the test case ideas.

[1:00:39 PM] Justin Byers: I think it shows you can do a lot of testing without getting hands-on

[1:01:01 PM] Lanessa Hunter: Exactly.

[1:01:06 PM] Scott Seltzer: I found the initial mission a bit confusing. It took a while to get what the goals were. It wasn't even clear at the start which product you were referring to.

[1:01:19 PM] Michael Larsen: OK, so our next session will then be focused on a specific application to test. I have some in mind, but I encourage enyone to also share things they would like to play with by sending us an email at WTAmericas@gmail.com.

[1:01:43 PM] Timothy Western: I think to really test this effectively, another session might be necessary to further drill down to the context we are dealing with for the client.

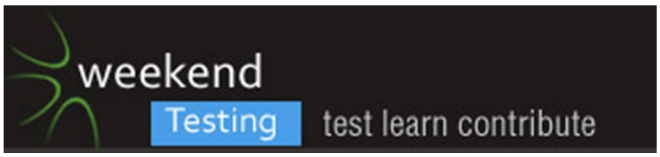
[1:01:55 PM] Shmuel Gershon: @Scott, "what is the mission" is the most popular discussion in the sessions

[1:02:11 PM] Aleksander Lipski: Thanks Micheal for this session, and thanks all you for your valuable input

[1:02:18 PM] Scott Seltzer: Funny, Shmuel.

[1:02:27 PM] Michael Larsen: @Timothy, this is something we have been discussiong, i.e. having sessions that would bridge.

[1:02:56 PM] Lanessa Hunter: bridge across more than one session? that sounds really cool.



[1:03:03 PM] Justin Byers: Thanks Michael, another great session.

[1:03:17 PM] Timothy Western: @Michael I'm just suggesting if we continued with the project from here, where would need to go to really geto to the hands on type of testing. Not saying we

[1:03:23 PM] Michael Larsen: It requires people commiting to attend multiple sessions, but it can be done if there's enough interest.

[1:03:26 PM] Scott Seltzer: Maybe in the session announcement you can explain if it's more of a hands-on session or discussion/conceptual?

[1:03:27 PM] Timothy Western: need to do it in WTA, but if this was a team being brought in.

[1:04:01 PM] Michael Larsen: @Timothy, I think that's fair, w could pre-announce that in the lead up to the sessions.

[1:04:04 PM] Scott Seltzer: I'll definitely try out the next one, though.

[1:04:41 PM] Lanessa Hunter: Thanks everyone, see you at another WTA session soon!

[1:04:49 PM] Weekend Testers Americas: OK everyone, time check again ((o)). We have reached the end of our session.

[1:04:57 PM] Scott Seltzer: Thanks, all!

[1:05:04 PM] Weekend Testers Americas: actually, we're a little over (LOL!).

[1:05:10 PM] Justin Byers: Thanks everyone!

[1:05:19 PM] Timothy Western: @Michael right its not a criticism, this is still part of testing, but in every project I've been in with discussions like that, if there's further that needs done later, but no time in that session, you note it, and bring it up in a later meeting/session. I'm trying to think what next steps might be LOL.

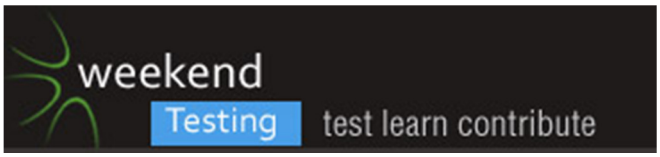
[1:05:41 PM] Aleksander Lipski: Good bye and see you next time

[1:05:50 PM] Linda Rehme: Thank you all.

[1:05:53 PM] Timothy Western: This was fun, thanks alL!

[1:05:57 PM] Weekend Testers Americas: My thanks to Albert for developing the charter and Mission today, and myu thanks to everyone who attended as well. We will put the chat transcript and the Experience report up on the weekendtesters site and post to twitter when it is ready.

[1:06:16 PM] Lanessa Hunter: Awesome. Thanks, Albert!



[1:06:53 PM] Weekend Testers Americas: Our next session will probably be in two or three weeks. check Twitter and the Weekendtesting site and the Software Testing Club for announcements.

[1:06:59 PM] Timothy Western: (applause)

[1:07:05 PM | Edited 1:07:35 PM] Albert Gareev: I put experience reports on past sessions here: http://automation-beyond.com/category/testing/wtamericas/ Feel free to use as testing challenges for your teams (some people do/did)

[1:08:34 PM | Edited 1:10:26 PM] Weekend Testers Americas: Also, again, if you have ideas for Weekend Testing Sessions, have a product you would like to consider testing, or would like to lead a session by proposing a mission and charter, please email us a WTAmericas@gmail.com. We are happy to work with other testers and develop ideas and approaches to keep this experience fun and interesting for everyone.

[1:08:57 PM] Albert Gareev: Once we decide on the session's date, we put announcement at STC: http://www.softwaretestingclub.com/events/event/listUpcoming

[1:09:46 PM] Albert Gareev: You can RSVP there, and we can discuss some details of the upcoming session.

[1:10:03 PM] Justin Byers: Sounds good

[1:10:53 PM] Weekend Testers Americas: Thanks for coming everyone, see you next time :).

[1:11:18 PM] Albert Gareev: Tell your colleagues :)

[1:11:34 PM] Lanessa Hunter: will do!:)