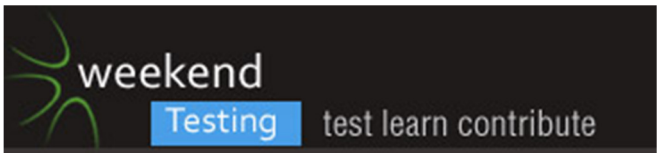


[11:00:32 AM | Edited 11:00:37 AM] Weekend Testers Americas: welcome everyone to Weekend Testing Americas.

[11:00:54 AM] Weekend Testers Americas: This is session #13 (cue ominous music LOL)

[11:01:21 AM] Weekend Testers Americas: It's good to see you all here, and as always, it's a diverse group from all over the world :).

[11:01:28 AM] Shmuel Gershon: Session 13, that can be a reason for people not to come too. Lucky it's not Friday

[11:01:37 AM] Weekend Testers Americas: we have a first timer today, so as always, Introductions first :).

[11:02:11 AM] Scott Seltzer: Hi, all. My name is Scott Seltzer and I live in Israel. I've been in software testing for about 17 years.

[11:02:48 AM | Edited 11:02:59 AM] Michael Larsen: Hello, My name is Michael Larsen, and I'm the facilitator for Weekend Testing Americas, I'm a lone tester in San Francisco, California. I've been doing this for about 8 years (software testing) and actively involved with Weekend Testing for about a year now.

[11:03:49 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.

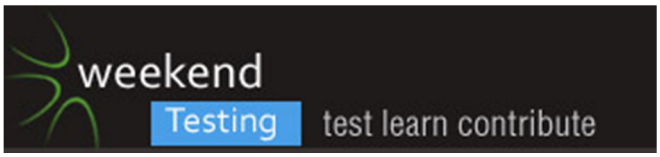
Another thing I am, is lurking. Or I am supposed to lurk now, as I have to finish work before tomorrow.

[11:04:16 AM] Alain Bohon: Hi everyone my name is Alain Bohon and I've been working in the software testing area for 3 years, I'm currently working for IBM. I'm from México

[11:04:42 AM] Ben Simo: Greetings. I'm Ben Simo. I've been making technology (and developers) cry, for profit, for the past 2 decades.

[11:05:05 AM | Edited 11:05:22 AM] Michael Larsen: Oh, additional note. I blog at TESTHEAD (mkl-testhead.blogspot.com) and I'm on Twitter at @mkltesthead.

[11:05:30 AM] eusebiu blindu: Hi, I am Eusebiu Blindu (Sebi) . Doing testing for more than 5 years. Facilitator in European Weekend Testing. I blog at http://www.testalways.com, tweet at @testalways



[11:06:19 AM] Weekend Testers Americas: OK, so some housekeeping details. this is mostly for Alain, since he's a first timer, I know everyone else already knows this ;).

[11:06:24 AM] Ben Simo: Due to a recent engagement as a bicycle crash test dummy, I've only got one usable hand. I may be slow to respond. Expect typos

[11:06:32 AM] Alain Bohon: :)

[11:06:35 AM] Weekend Testers Americas: first, we will announce a mission and a charter.

[11:06:40 AM] Ben Simo: Welcome Alain.

[11:07:11 AM] Weekend Testers Americas: then we encourage discussion for the first hour around that mission and charter. Often we split off and do pair testing, but since we have a small group today, we may all do it here together.

[11:07:17 AM] Weekend Testers Americas: We'll see how things develop :).

[11:07:36 AM] Weekend Testers Americas: after that first hour, we then have a debrief to discuss our findings and our approach and methods.

[11:08:06 AM] Weekend Testers Americas: While most sessions take the two hour block up handily, each session is a little different, so we'll see how things roll today.

[11:08:19 AM] Weekend Testers Americas: With that, here's our mission and charter.

[11:08:42 AM] Weekend Testers Americas: We all are the test team for a medium sized company (say 1,000 people).

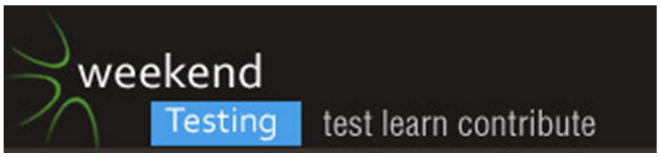
[11:09:23 AM] Weekend Testers Americas: Due to the desire to spread to small regional offices, but keep key documents available we are looking at cloud options to store important documents.

[11:09:53 AM] Weekend Testers Americas: we want to make this as easy for our users as possible, so we are exploring numerous options in the marketplace today.

[11:10:25 AM] Weekend Testers Americas: there are some famous names like Dropbox, Sugar Sync, etc. that we can consider.

[11:10:45 AM] Weekend Testers Americas: But the big concern with corporate is security. How can we make sure that what we put online is safe?

[11:11:23 AM] Weekend Testers Americas: Our mission is to explore testing options, and examine various services (pick additional versions if the two I've mentioned don't float your boat).



[11:11:55 AM] Weekend Testers Americas: And report back on what we can do to test and confirm this approach (or not confirm it).

[11:12:03 AM] Weekend Testers Americas: ... and there it is.

[11:12:29 AM] Michael Larsen: So here are some of my first thoughts.

[11:12:54 AM] Mohinder Khosla: Hi everyone

[11:13:02 AM] Michael Larsen: For obvious reasons, we are not going to be doing things like denial of service on a live site, but those are options we would have to consider for a legitimate test.

[11:13:16 AM] Shmuel Gershon: What is 'safe'?

[11:13:29 AM] Michael Larsen: Beautiful seque, Shmuel :).

[11:14:10 AM] Shmuel Gershon: Also, is 'safe' also 'private'?

[11:14:15 AM] Michael Larsen: Safe is an arbitrary term, and in different contexts means different things.

[11:14:46 AM] Michael Larsen: @Shmuel, I think that for most people, safe and private are synonymous.

[11:15:00 AM] Michael Larsen: but there are varying levels.

[11:15:36 AM] Ben Simo: I see two equally importand aspects: data is available to those who should have access when needed, and data is not available to anyone else

[11:15:42 AM] Michael Larsen: Let's take facebook as an example. there's a lot of information i share up there that is definitely not private, and that's the whole point. I don't mind sharing those aspects.

[11:16:09 AM] Michael Larsen: My home address, my credit card numbers, my home phone number, those I dont want to share.

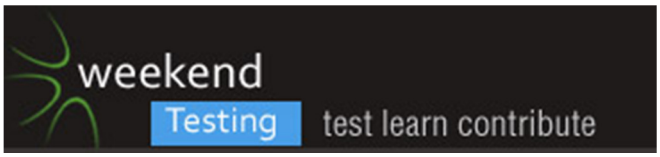
[11:16:25 AM] Michael Larsen: and those I would absolutely want to have kept private (and by extension, safe from others).

[11:17:04 AM] Michael Larsen: So any testing goals would have to be based around determining what data is shared and what is not, and with whom.

[11:17:27 AM] Shmuel Gershon: So, according to Michael and Ben, safe includes private

[11:17:47 AM] Ben Simo: how safe is our data if we keep it in-house? is that where the security bar for putting data in the cloud should be? or do we need better security?

[11:18:01 AM] Michael Larsen: For the purposes of this mission, yes.



[11:18:19 AM] Michael Larsen: So with that in mind, let's brain storm a bit.

[11:18:25 AM] Ben Simo: [11:16 AM] Michael Larsen:

<<< My home address, my credit card numbers, my home phone number, those I dont want to share.all things i've given to facebook to buy ads :P

[11:18:47 AM] Michael Larsen: Aha, good point Ben :). Context is everything.

[11:19:09 AM] Michael Larsen: We do, of course share those details at key times every time we make an online purchase.

[11:19:21 AM] Timothy Western: Sorry to drop in, - Tim Western, Tester, Hinton, WV..... My question for any cloud service, is what safeguards dothey provide for access, what kind of credentialing system, is it Username/Password, do I need to get Smart/CAC Cards to decrypt data on the network, or fingerprint scanners or something like that?

[11:19:43 AM] Scott Seltzer: The service should use SSL.

[11:19:51 AM] Shmuel Gershon: [11:18 AM] Ben Simo:

<<< My home address, my credit card numbers, my home phone number, those I dont want to share.Things we (I) easily share with a waiter in a restaurant

[11:19:53 AM | Edited 11:20:13 AM] Michael Larsen: Timothy, no need to be sorry, those are all good questions and considerations :).

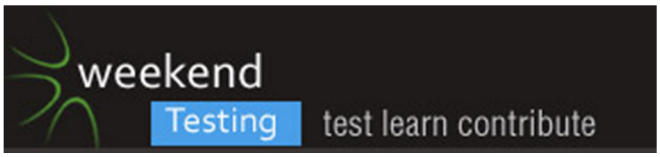
[11:20:03 AM] Timothy Western: And to throw a rinkle, are there any additional security measures we can take as a company to protect the data, (encrypting them before storage, Steganos, etc?)

[11:20:40 AM] Ben Simo: Front end security tells us nothing of back-end security.

[11:20:46 AM] eusebiu blindu: i know little about dropbox but not very confortable. anyway a lot of internal discussions in a company, including private data is done on Skype. So it might be "secure" from most, but not secure from the host

[11:20:49 AM] Michael Larsen: Ok, so we see some criteria emerging.

[11:21:09 AM] Ben Simo: physical security also matters



[11:21:28 AM] Scott Seltzer: Passwords might have requirements such as length, required to contain certain of: caps, lowercase, numbers, letters, punctuation.

[11:21:40 AM] Michael Larsen: Shmuel, you raise a good point. When we give our credit card to wait staff, how confident are we that they are not just recording the numbers to use fraudulently later?

[11:21:44 AM] Scott Seltzer: There may be requirement to change passwords with some regularity.

[11:22:20 AM] Michael Larsen: So let's take some time and set up some ground rules for our testing charter.

[11:22:31 AM] Shmuel Gershon: Also, to expand on Scott's point... If we are a medium sized company, we may want the service to converge to our current names/password and authentication system.

[11:22:35 AM] Michael Larsen: How many people here are familiar with typewith.me

[11:22:42 AM] Scott Seltzer: Not me.

[11:22:51 AM] Scott Seltzer: Checking...

[11:23:01 AM] Ben Simo: [11:21 AM] Michael Larsen:

<<< Shmuel, you raise a good point. When we give our credit card to wait staff, how confident are we that they are not just recording the numbers to use fraudulently later?guy at burger king drive thru once stole my credit card info

[11:23:13 AM] Michael Larsen: http://typewith.me/EoVTXnFTIs

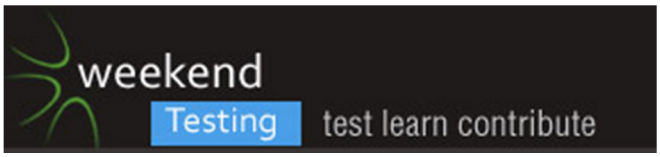
[11:23:28 AM] Michael Larsen: Everyone who wants to contribute notes to our charter, please do so there :).

[11:23:54 AM] Michael Larsen: we're doing good so far, but we can all edit it in real time there (and with this size of group, that shouldn't be a problem).

[11:25:21 AM] eusebiu blindu: yeah but credit cards only give the credit - actual payment is done in couple of days

[11:25:44 AM] Shmuel Gershon: So, do we want authentication with our own intranet system, or we can want a specific system authentication?

[11:22 AM] Shmuel Gershon:



<<< Also, to expand on Scott's point... If we are a medium sized company, we may want the service to converge to our current names/password and authentication system.

[11:25:54 AM] eusebiu blindu: the payment is like all money - just another level of credit

[11:26:54 AM] eusebiu blindu: so sharing data should have a prompt for config with proper warnings

[11:27:38 AM] Timothy Western: Is it reasonable to suggest that if a corporation was buying a 'cloud service' for file storage/backup, etc. that they may make more contact with a provider than a lone home user? You figure some measure of funds would be exchanged, so the Provider and the Client in this case would probably want some kind of 'contract' about the services being offered/paid for etc. Some of these issues might come up during a negotiations stage.

[11:28:14 AM] Timothy Western: Drop Box was very quick to connect to as a lone user, I wonder if for businesses a provider might handle things slightly differently. (maybe this is out scope.)

[11:28:54 AM] Michael Larsen: tim, that's a good question. could latency and delays in service pose a security risk?

[11:29:20 AM] Ben Simo: cloud service authentication is not necessarily the same as what we present to our users. cloud storage svcs are available w no ui. we could create our own ui on top of cloud backend

[11:29:22 AM] Timothy Western: Well I was thinking Volume of Data that might be moved by corporate entity vs individuals, but yeah that's good too.

[11:29:34 AM] eusebiu blindu: Not sure how DropBox works, but in case of a company I would use a system to encrypt my data before sharing it

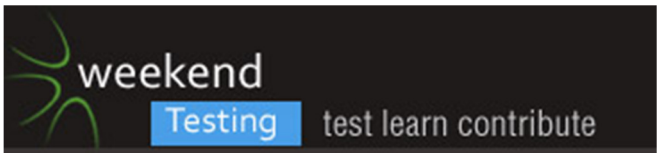
[11:30:22 AM] Timothy Western: Which brings to another issue, what kinds of protections do we currently have internally, that we might expect, but not have? Permissions by Role, Group, User, Folder location, etc?

[11:30:25 AM] Ben Simo: if cloud data service charges for bandwidth & storage volume, cost control may be an important part of security

[11:30:41 AM] Michael Larsen: Note, let's not emphasize any one service per se unless there's a key element that makes for a compelling use case.

[11:30:42 AM] Scott Seltzer: Sebi, why an external system instead of them having encryption built in? You don't trust them? It would certainly be much easier and less time consuming if they do it in the process...

[11:31:26 AM] Ben Simo: any server-side encryption has server side decryption



[11:31:50 AM] Timothy Western: Could it be external to the main offices, but still be within the company? (Off Site Cloud Data Center, vs on site server locations)

[11:31:52 AM] Scott Seltzer: Was that an answer to me, Ben?

[11:32:02 AM] Ben Simo: if u want data secure from svc provider too, encrypt client side

[11:32:23 AM] eusebiu blindu: Well DropBox is just an organisation. Let's say they really intend to be safe and trustworthy. But they have employees that can have easy access to data shared

[11:32:42 AM] Scott Seltzer: The service could have encryption built in to its clients.

[11:33:06 AM] Timothy Western: Your describing what would be a 3rd Party Internal Security threat?

[11:33:19 AM] Timothy Western: A threat taht could be within the provider itself.

[11:33:22 AM] Michael Larsen: Sebi, that's true of any organization. In many of our transactions, we have to accept that there are areas that cannot be totally 1oo% "trusted".

[11:33:25 AM] Timothy Western: Yeah, I agree that's always a risk.

[11:33:48 AM] Michael Larsen: However, there are mechanisms that can be put in place to limit those options.

[11:33:54 AM | Edited 11:34:01 AM] Michael Larsen: Salted paswords fields for example.

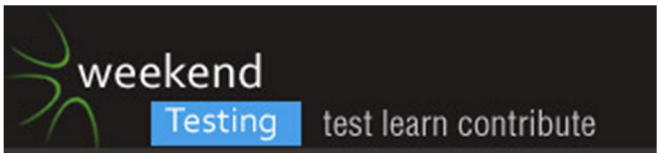
[11:34:14 AM] Timothy Western: Even when you upload pictures to say 'Facebook' or some other storage site like 'Photobucket', there's always the chance someone else can gain access to those photos, use, misuse, or abuse them for other means.

[11:34:41 AM | Edited 11:35:04 AM] Michael Larsen: In a well developed system, even in house developers shouldn't be able to get in and decrypt those fields easily, but I'm sure a determined internal hacker could do it if they really wanted to.

[11:35:15 AM] Timothy Western: The question we need to ask is, what is the host provider doing to help provide reasonable assurance of security, and what can we do on our end to help make sure the work we do on the host is as secure as possible from our end.

[11:35:42 AM] Michael Larsen: OK, the doc is filing up nicely. We're about 35 minutes in, we have 25 minutes more for the active testing and test planning.

[11:35:47 AM] Timothy Western: Those are two differnt avenues of Threat, the Server Side, and the Client Side. both need addressing I think.



[11:35:53 AM] eusebiu blindu: well data loss is a risk for example that can have same effects as security issues

[11:36:13 AM] Michael Larsen: I'd encourage anyone whowants to to take some time with a service that provides file sharing and do some quick tests to help expand our coverage set.

[11:36:22 AM] eusebiu blindu: i think now storage is becoming cheap, so companies would not prefere it

[11:36:45 AM] Michael Larsen: I think there are two levels of danger.

[11:36:46 AM | Edited 11:37:04 AM] eusebiu blindu: if they have a lot of data to store, then sharing externaly becomes slower

[11:37:06 AM] Michael Larsen: IF we have an onsite riule for data, and a catastrophic event takes place, an organization could be sunk.

[11:37:46 AM] Michael Larsen: even with offsite back-ups or redundancy, there could be situations where a huge impack could cmpletely take a player out of the game.

[11:37:46 AM] Ben Simo: i don't see a 1000-person company using something ike dropbox or photobucket for a standard cloud storage platform. i'd expect use of a cloud storage service accessible via api put behind some other (perhaps built inhouse) document management ui

[11:37:47 AM] Timothy Western: So then a Cloud Service File service could serve as a contingency backup, should the main File Service (perhaps in house, but could be external) fail?

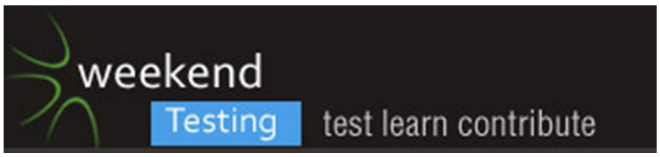
[11:38:05 AM] Michael Larsen: Think of the situation in Japan.

[11:39:16 AM] Timothy Western: I think that's an excellent point Ben. If what is provided is an API, and that API makes it significantly difficult to some how spoof another client who is trying to connect, (depending on the API, you might even have a multi factor identifier on the machines themselves that provide additional security, like with a VPN type client, or something similar)

[11:40:06 AM] Michael Larsen: So backing up a bit here... Services like Dropbox and Sugar Sync (just to name a couple) are really meant for individuals or small groups. I'd consider a 1000 person company to be outside of the target market for a product like DB or SS, but the tools and approach would be desirable.

[11:40:38 AM] Ben Simo: in my experience, companies in the data hosting business take security more seriously than many 1000-person companies - or 25k person companies

[11:40:42 AM] Michael Larsen: but does that very simplicity invite predators?



[11:40:54 AM] Shmuel Gershon: I agree with Ben. A company like that would go for Amazon's service, that is more 'comanyish'

[11:41:39 AM] Timothy Western: From the little test I did on Dropbox earlier, it seemed almost as seamless to connect to it as if it was a server on my network.

[11:41:53 AM] Michael Larsen: So even if we include Amazon's Cloud Service and other large players in this sphere, we'd still need to have a similar gameplan for determining security compromises.

[11:42:08 AM] Timothy Western: I think that's what Michael means, it needs to have corporate level security safeguards, but not so obtrusive to use that it's more of a headache or pain to use then what we currently may use in house.

[11:42:12 AM] Shmuel Gershon: Right

[11:42:25 AM] Michael Larsen: Timothy, exactly.

[11:42:51 AM] Michael Larsen: Alain, what considerations would you want to see addressed?

[11:42:53 AM] Timothy Western: Because, if connecting, setting up, and using is difficult, then you will develop the situation you don't want. Hoarding files on local boxes, that are more at risk for malware, virus infection, or hardware failure do to regular use.

[11:43:37 AM] Michael Larsen: Don't be shy, we want to have everyone offer brainstorming ideas :). Don't let the vets intimidate ya :).

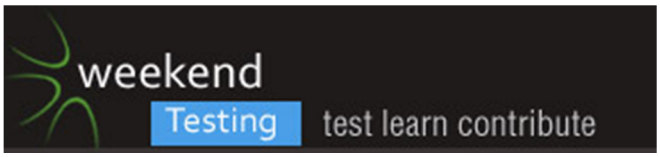
[11:43:38 AM] Timothy Western: You want people to feel like that Cloud Service, is just as if it was OUR actually physical box, we want to be cozy with it, but we also want to make sure we have assurances that it is, as was said earlier 'safe' and 'private'.

[11:44:30 AM] Timothy Western: The questions, to ask then since the charter is primarily dealing with security, what can we do to test and assure that sufficient safe guards are in place.

[11:44:53 AM] Ben Simo: with a cloud storage svc, ease of use would be a client-side issue. and not a security issue... exce4pt to the extent that bad ui encourages ppl to use less secure storage

[11:45:19 AM | Edited 11:47:48 AM] Michael Larsen: Cool, so we have some good expectations and some specific ideas. I've added an area caled Methods of Testing. Let's think of some ways that we culd actually test these services to provide enough information for a go/no go decision.

[11:46:12 AM] Ben Simo: to tim's point, people feel safer when they ctrl a physical box; even if it is less safe than a cloud service offering



[11:48:30 AM] Michael Larsen: Ben, this answers back to the same idea that we feel less anxious about giving our credit card to a cashier than we do to an online service.

[11:48:43 AM] Ben Simo: so addressing perceptions may be something testing can help with. even if tech ppl know a cloud svc is technically better in some way than our own systems, demonstrating it in testing can help

[11:48:47 AM] Michael Larsen: It's the same sense of false security.

[11:48:58 AM] Michael Larsen: We don't believe someone we are in direct contact with will rtip us off.

[11:49:10 AM] Timothy Western: I wonder, when we connect to the Cloud Service... could we be adding risk for potential 'attacks' from the server end?

[11:49:24 AM] Michael Larsen: In many ways, we are much more vulnerable to "insider corruption" than we are to the shapeless cloud (statistically speaking, of course).

[11:50:05 AM] Ben Simo: [11:49 AM] Timothy Western:

<<< potential 'attacks' from the server end?from server end?

explain pleaSE

[11:50:36 AM] Timothy Western: Well, given there is some kind of authentication scheme to connect to the cloud. Once you are connected.

[11:51:29 AM] Timothy Western: My thoughts are could a malicious file, or program snuck onto the host system from somewhere then haev access back. What I'm describing I suppose, is could there be a risk for a Trojan Horse back door to other computers on our network?

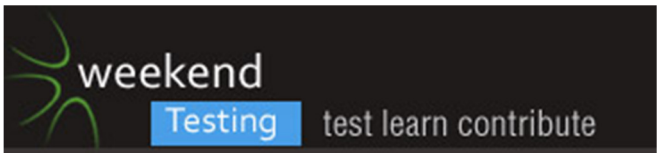
[11:51:44 AM] eusebiu blindu: capturing network traffic and replaying it can show vulnerabilities

[11:51:55 AM] Michael Larsen: Timothy, so do you mean that with a number of active connections, the number of connections could increase the risk of server side compromise?

[11:52:27 AM] Michael Larsen: Sebi, yes, classic bait and switch process for hacking a network service :).

[11:52:31 AM] Ben Simo: i'd hope a data storage svc isnt executing code other than the storage sstem code.

[11:52:35 AM] Timothy Western: If I understand the Cloud Correctly, we might be sharing boxes with other corporations? even if our data i segmented, a connection is a connection.



[11:53:17 AM] Timothy Western: Even on private networks you may have the risks for Trojans or Worms propagating through that, is that still a risk with the Cloud? Is it something we can prevent short of education of users?

[11:53:19 AM] Ben Simo: yeah, there's risk of alternate (not thru public ui/api) access routes in internal and cloud systems

[11:53:45 AM] Ben Simo: which is why i like idea of client-side encryption

[11:54:12 AM] Michael Larsen: Here's a thought, what if we were to use a cloud service to "stress" another cloud service. Amazon allows the ability to spin up multiple machines at various intervals. Imagine spinning up multiple machines to deluge a network with file uploads from multiple sources.

[11:54:33 AM] Ben Simo: also, a cloud storage svc may offer redundancy and retention we wouldn't have in-house

[11:54:43 AM] Michael Larsen: could we compromise the server's ability to respond to those requests and therefore leave files in an "ambiguous state" between public and private?

[11:55:38 AM] Ben Simo: michael, hopefully something tested for...

[11:55:45 AM | Edited 11:56:07 AM] Michael Larsen: Note: that's an honest question, I really don't know the answer to that :).

[11:55:46 AM] Scott Seltzer: That's what I was thinking - target the DoS attack just on the encryption mechanism, not the entire service.

[11:56:44 AM] Weekend Testers Americas: (o) time check. five more minutes.

[11:56:56 AM] Ben Simo: credibility of provider & likerlyhood they'll be around long term could be important factors. don't want a startup going under and taking our data with it

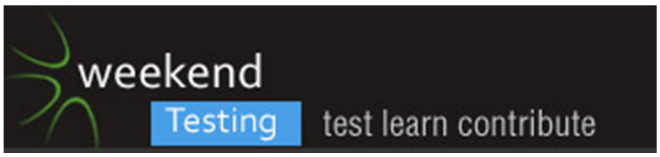
[11:57:10 AM] Mohinder Khosla: I lost Skype connection at 11:15 SF time. It is sorted now

[11:58:44 AM] Ben Simo: ddos attacks are likely standard fare for any big hosting providers

[11:58:48 AM] Timothy Western: One last thing I'd suggest, what can we do to check the security of the service, Deep Packet Inspection maybe? See what data is really being passed back and forth, and could it be vulnerable.

[11:59:10 AM] Michael Larsen: Thanks, Mohinder, was wondering where you went :).

[11:59:14 AM] Timothy Western: and now, I've got to step out... sighs.



[11:59:18 AM] eusebiu blindu: @Mohinder - you gave an idea :) connection to the DropBox - how fast, reliable, resuming it is?

[12:00:06 PM] Michael Larsen: @Sebi, good point. How quickly could we re-establish a cnnection if we were dropped out of an upload/download.

[12:00:25 PM] Weekend Testers Americas: OK gang, time's up!

[12:00:47 PM] Weekend Testers Americas: Let's take a few more minutes to compile additional thoughts into the typewith.me doc.

[12:01:12 PM] Michael Larsen: http://typewith.me/EoVTXnFTIs

[12:01:27 PM] Michael Larsen: from there, we can start the debrief.

[12:03:11 PM] Ben Simo: understanding architecture of considered systems could help in testing. but providers may not share sufficient detail - for security reasons

[12:05:15 PM] Michael Larsen: Ok, so let's go ahead and get started with the folow-on discussion.

[12:05:33 PM] Michael Larsen: Show of hands, how many here would consider themselves well versed in security testing.

[12:05:48 PM] Michael Larsen: [Note michael does not raise his hand here, as it's not a real specialy on my part ;)]

[12:05:49 PM] Scott Seltzer: Not me.

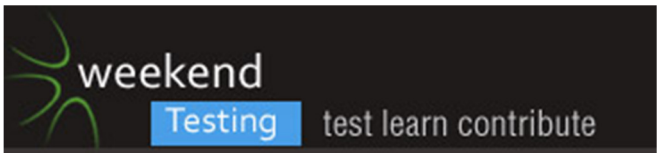
[12:05:55 PM] Ben Simo: (y)

[12:07:22 PM] Michael Larsen: What I found interesting was the fact that, even though some of us wouldn't consider ourselves necessarily strong in the areas of security testing, there was no end of ideas coming out.

[12:07:47 PM] Michael Larsen: Is this just an aspect of rapid braintorming, or is there some level of "personal interaction" that makes security more engaging that other tet areas.

[12:08:05 PM] Alain Bohon: I haven't been very related to security testing or cloud services. Honestly the first thing I did as early as I read the topic that was going to be discussed was run to google and make some research on dropbox security. I found this session very rewarding and It gives me a lot of material to study and research.

[12:08:36 PM] Michael Larsen: I think for me, even though I may not know all the potential permutations, I feel a certain visceral response to it.



[12:09:21 PM] Michael Larsen: Add to that, even if we aren't diretly testing security, we play with it every day.

[12:09:29 PM] Ben Simo: yes. keep ideas flowing. those trying to gain unauthorized access keep ideas flowing. they don't create a fixed set of attacks and then stop learning.

[12:10:16 PM] Michael Larsen: We're always logging into services, we're accessing important and sensitive areas, and many of those areas could make or break a person if they got out.

[12:10:47 PM] Michael Larsen: I found the idea behind client side or server side encryption interesting.

[12:11:06 PM] Michael Larsen: and the fact that there was a good debate about the merits and desrability of both.

[12:11:32 PM] Michael Larsen: For me personally, I think I'd want to have control over the data encryptions and have the ability to set or not set it as I saw fit.

[12:12:34 PM] Mohinder Khosla: I had couple of sessions on security testing of public sites and find how easy it is for an expert to steal information.If you are going to giv access to common files held on tan external server then it is going to be risky if not managed properly. Microsoft can provide private cloud if you have a big customer base or shared cloud for a small customer base. To me that is better optin than Dropbox

[12:12:34 PM] Michael Larsen: Of course, I do not put files up that I would feel are that mission critical or sensitive. For example, I store articles I'm in the process of writing, or paper proposals. While I supose someone could go in and steal those, I don't give a lot of thought to that being acessed.

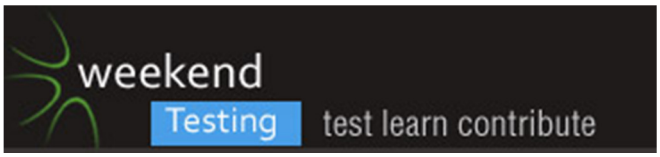
[12:13:14 PM] Michael Larsen: By contrast, I definitely feel leery about how easily my entire medical history can be accessed online, and wish there were a few more safeguards on that data an what is displayed and how.

[12:13:37 PM] eusebiu blindu: But there is a very good option for particular data anyway to have such a hosting service.

[12:14:56 PM] Mohinder Khosla: If you are going down this road storing company information on a public cloud then make sure your files are encrypted.

[12:15:19 PM] Ben Simo: also, i didn't mentioned: look at security beyond the front door. does authorized access as one user unintentionally give access to other info. e.g.: recent url hacking of bank website that gave hackers logged in as one user access to others' data

[12:15:24 PM] Michael Larsen: Actually, I'm not really all that weided out about the details of the medical information being online or available. I think financial documents and accounts are the most worrisome, yet they are the ones that are really ubiquitous when we discuss online availability.



[12:15:42 PM | Edited 12:17:26 PM] Michael Larsen: And we haven't even gotten started with the desktop vs wireless, vs mobile debate.

[12:16:17 PM] Mohinder Khosla: Your company data would be gold dust to a competitor

[12:17:33 PM] Ben Simo: yet many companies outsource work, and access to data, to companies also working for competitors and customers :(

[12:17:40 PM] Michael Larsen: Mohinder, yep.

[12:18:11 PM] Ben Simo: weakest link in security is usually people. social engineering

[12:18:52 PM] Michael Larsen: Ben, I find it interesting how many companies use services like GitHub for doing their source code versioning. Don't get me wrong, I think the servcie is geat and I love using it, but every once in awhile, I marvel at how trusting many companys are with their crown jewels of their organiztions.

[12:19:16 PM] Mohinder Khosla: @Ben Network is the weakest link in my opinion if data is not encrypted before pushed across the network

[12:20:56 PM] Michael Larsen: So next question... what are some areas that we culd look into and help us become more savvy when it comes to testing web and online security?

[12:21:06 PM] Ben Simo: if i can call a help desk (or another employee) and get them to give me access, network encryption is useless.

[12:21:25 PM] Michael Larsen: And I'll pipe down for awhile because I feel like I'm monopolizing the conversation ;).

[12:22:09 PM] Ben Simo: owasp.org

[12:22:50 PM] Ben Simo: gary mcgraw's podcast: http://www.cigital.com/silverbullet/

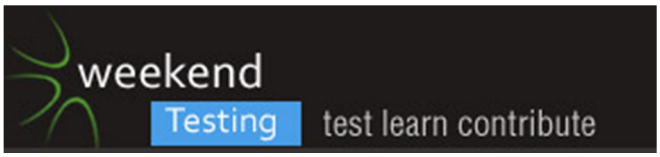
[12:23:05 PM] Scott Seltzer: Great links, Ben. Thanks!

[12:23:23 PM] Michael Larsen: Nice, good stuff :).

[12:24:24 PM] Mohinder Khosla: I am a member of OWASP and hear lots of cases where people burn their fingers badly because they do not do their homework without considering the options properly

[12:24:37 PM] Ben Simo: frank abagnale (con artist turned consultant) is big on social side.

[12:25:13 PM] Michael Larsen: what I found interesting over the years wa that when we were firt emerging into online communication, there was a huge emphasis on privacy and the ability to encrypt everything. I remember the Cypherpunks alias back in the early 90s, and participated in it for awhile.



[12:25:27 PM] Michael Larsen: those types of groups seem to be much less vocal today.

[12:25:51 PM] Ben Simo: read about the security failures of others.

[12:26:02 PM] Mohinder Khosla: Paco Hope from cigital has a written a book on web security testing but seems to be for developers

[12:26:11 PM] Michael Larsen: It it becaus they were co-opted, or was it because we just decided it was much ado about nothing (generally speaking).

[12:27:17 PM] Ben Simo: security innovations has a good online security course for testers. not free, but i think a great deal to bring into a company

[12:28:22 PM] Scott Seltzer: URL, Ben? I see lots of sites with that name.

[12:28:37 PM] Ben Simo: watch documentary hacking democracy if you need more reason to distrust software security

[12:29:52 PM] Michael Larsen: Cool, Ben, I think I'm adding this one to my Netflic queue :).

[12:29:52 PM | Edited 12:30:17 PM] eusebiu blindu: i would think for example antivirus companies invent viruses, having the solution for it

[12:30:22 PM] Michael Larsen: there's a certain circular logic to that, isn't there, Sebi).

[12:30:33 PM] eusebiu blindu: corrected that :)

[12:30:51 PM] Ben Simo: http://www.securityinnovation.com/products/elearning/courses.shtml <- testing courses at bottom of page. i think TEST 311 is the one i'm thinking of

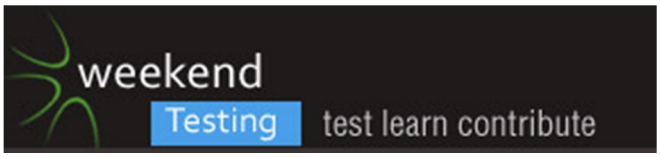
[12:31:03 PM] Scott Seltzer: Thanks.

[12:31:27 PM] Michael Larsen: but I get what you mean. does it seem at times that we are puting out trust in those that have the most to gain by gaming the system?

[12:32:38 PM] Ben Simo: Hugh Thompson (one of the experts i n Hacking Democracy) is great. he's got some interviews on youtube

[12:33:00 PM] Michael Larsen: I guess if you want to have the portability of documents, then the coud option makes a lot of sense, but it requires a certain sense of caveat emptor. to me, I don't hink there is a really and truly safe and secure method out on the clour, or in the datacenter on site, for that matter.

[12:33:47 PM] Michael Larsen: I don't remember who said it, I read it years ago, but one of the great quotes was that "to be 100% free, we must be willing to be 100% open about eerything".



[12:33:51 PM] Scott Seltzer: Ben, I'm reading all your links and learning a lot. Thanks so much!

[12:34:03 PM | Edited 12:34:13 PM] Michael Larsen: Ditto, Scot :).

[12:34:15 PM] Mohinder Khosla: You can try wordpress scanner http://code.google.com/p/wpscan/

[12:36:32 PM] Ben Simo: [12:33 PM] Michael Larsen:

<<< I don't hink there is a really and truly safe and secure method out on the clour, or in the datacenter on site, for that matter.right. you just want to be far from the easiest target. and realize, for those who try to protect data with tech, people are still the weakest link. last study i read still reported most leaks come from within

[12:37:01 PM] Ben Simo: welcome

[12:37:04 PM] Michael Larsen: Heh, was just about to throw out another question, but I think that makes the point nicely :).

[12:37:40 PM] Michael Larsen: So gang, I'm going to make a heretical proposition...

[12:38:18 PM] Michael Larsen: Unless we have other ideas or suggestions, it's a nice summer day, I'm willing to wrap it up here if everyone else is, too :).

[12:38:40 PM] Michael Larsen: Smaller groups allow for that ;).

[12:39:03 PM] Michael Larsen: OK, for those of you in Israel, it's night time, of course :).

[12:39:05 PM] Scott Seltzer: 10:38pm where I am so that's fine by me. I'll read more of the info on those links tomorrow.

[12:39:12 PM] Mohinder Khosla: Time for icecream then

[12:39:29 PM] Scott Seltzer: Thinks Michael and everyone!

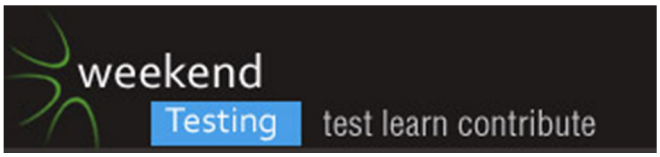
[12:39:53 PM] Alain Bohon: thanks everyone

[12:40:05 PM] Weekend Testers Americas: thanks everyone for participating today.

[12:40:20 PM] Mohinder Khosla: Nice chatting with you everyone

[12:40:26 PM] eusebiu blindu: thanks

[12:40:35 PM] Weekend Testers Americas: WTA will be offline for the next two Saturdays due to Michael Larsen being up at Scout camp :).



[12:40:38 PM] Mohinder Khosla: Sorry to miss half an hour of fun

[12:40:49 PM] Weekend Testers Americas: Tentative next session will thus be July 16th 2011

[12:41:12 PM] Ben Simo: thanks all. chow.

[12:41:22 PM] eusebiu blindu: chow?

[12:41:23 PM] Scott Seltzer: Marked my calendar.

[12:41:33 PM] Alain Bohon: adiós amigos

[12:41:36 PM] Mohinder Khosla: Bye for now

[12:41:47 PM] Weekend Testers Americas: Also, form those interested, I will be running a special Weekend testing session at CAST 2011, which will include conference attendees and those elsewhere, so more on that as we get closer to the date.

[12:41:48 PM] Shmuel Gershon: Er... Bye!

[12:41:50 PM] eusebiu blindu: seems like there is a similar in many languages

[12:41:50 PM] Scott Seltzer: Shalom.

[12:41:59 PM] Weekend Testers Americas: Ciao ;).

[12:42:16 PM] Shmuel Gershon: שלום

[12:42:31 PM] Weekend Testers Americas: Have a great day everyone, see you next time!

[12:42:40 PM] Mohinder Khosla: (bow)

[12:42:52 PM] Ben Simo: ciao spelled wrong

[12:43:22 PM] eusebiu blindu: (music)

[12:43:34 PM] Ben Simo: tschüß