My Journal on My Research Work

Hasini Gunasinghe (huralali@purdue.edu)

RahasNym

Until 12th Feb, I mostly worked on improving the paper to be submitted to SACMAT.

Biometrics Research Work

Android Development:

Some useful links for study android dev:

1. Starting another activity: http://developer.android.com/training/basics/firstapp/starting-activity.html
2. Intents and intent filters: http://developer.android.com/guide/components/intents-filters.html
3. Interactions between apps: http://developer.android.com/training/basics/intents/index.html
4. Layouts: http://developer.android.com/guide/topics/ui/declaring-layout.html
5. Build System: http://developer.android.com/sdk/installing/studio-build.html, http://developer.android gradle.html
6. Intent Class spec: http://developer.android.com/reference/android/content/Intent.html
7. Android Security Tips: http://developer.android.com/training/articles/security-tips.html

RoadMap:

1. Get two activities in an app communicate. DONE. 1st March.
2. Get two apps communicate and return result. DONE. 14th March.
3. Get an app to communicate with a remote REST service. DONE. 17th March.
4. Integrate ZKP.
5. Run perf test for ZKP with a remote party with static identity.
   Perf test config: Connect laptop to network through wired connection. Run tomcat+services in Windows (so there wont be port forwarding overhead.)
6. Look at the new trend in replacing passwords with FRT and re-write the introduction of the journal. - DONE on 20th March for writing the proposal.
7. Send the update to Prof: Perf. results + introduction re-written. (DEADLINE: 7th April Mid Night.)
8. How to access TrustZone.
9. Look at secure coding of android applications (downloaded).
10. Biometrics work follow.

11. Do an experiment to see if classification gives better results than distance matching, so that we can claim it.

12. I think it is fundementally wrong to say that you generate BID for a user by giving his/her biometrics features into a classification model that did not use his/her biometrics images to train the model. I think I should also test this during the experiments. But training a model is all about using it during prediction. But this will not preserve uniqueness. So I guess that we need to train a model for each enrolling user.

Wed Jan 20

I installed Android studio. I referenced this good tutorial: http://www.androidauthority.com/first-android-app-what-you-need-to-know-619260/
However, in my Ubuntu, I got an error from android studio saying that SDK or libraries could not be installed.
Then this was the solution: http://stackoverflow.com/questions/28804863/android-studio-how-to-install-android-platform-tools-on-ubuntu-14-04-64-bit It was because Android needs 32 bit libs and I have a 64 bit Ubuntu.
Here are some tips I found to make the emulator fast: http://developer.android.com/tools/devices/emulator.ht
linux

Feb 19

Emulator runs Android in a kind of virtual machine, as an Android phone with an Intel processor. This is faster than emulating an ARM processor on your PC.

Feb 22

After lunch, I worked on the mobile app dev. I am still at the very very beginning. Followed first app tutorial till end, and got a problem when running in the emulator. Emulator needs KVM *emulator: ERROR: x86 emulation currently requires hardware acceleration! Please ensure KVM is properly installed and usable. CPU acceleration status: KVM is not installed on this machine (/dev/kvm is missing).*

Then I tried to install KVM based on this tutorial:
https://software.intel.com/blogs/2012/03/12/how-to-start-intel-hardware-assisted-virtualization-hypervisor-on-linux-to-speed-up-intel-android-x86-emul ator
However, there seems to be problems.
1. When I ran the command at the beginning of that tutorial to check if the CPU supports KVM extensions, I get the output as NO. However, since the error from Android studio shows some hope, I tried to install it.

2. Then the install command given in the tutorial doesn't work. Then I tried this: whose command works. https://www.howtoforge.com/tutorial/kvm-on-ubuntu-14.04/
It seems that now I need to relogin to enable KVM for my user accounts.

Feb 24:

Since I had issues in running the hello world app in the emulator due to KVM enabling issue, I thought f checking my bios to see if KVM is enabled.
Before accessing the bios, I needed to backup my important files in bitbucket. Therefore, I spent sometime backing up my files.
Then I spent some fair amount time accessing the bios. First I tried F2 key as mentioned in many online articles which didn't work. Then F12 worked. Intel VT is enabled in the bios.
Then I checked the VMWare settings. So the problem was VT was not enabled in VMWare. When I enabled it, the emulator ran. But it was damn slow.

I searched about how to make the android studio fast. I got some answers:
1. http://www.viralandroid.com/2015/08/how-to-make-android-studio-fast.html
This suggested either to test in real device or in genymotion emulator: https://www.genymotion.com/download

Option 1: I tried to install genymotion emulator, but it requires VirtualBox to run. Hmmmm. VirtualBox on VMWare!. So I thought of first running in the real device and see because I anyway have to install it in a real device.
Option 2: Option 2 is to install genymotion+virtual box on windows, compile the project in Linux and run it in the genymotion running in Windows. https://dzone.com/articles/genymotion-simply-best-android

I tried to install it in my phone (I upgraded my phone too for this reason. My phone is running Android 4.4.2). But somehow it didn't get installed. I was so tired by then and went to sleep.

TODO: Read how to make android studio faster:
1. https://dzone.com/articles/how-speed-android-studio
2. http://www.codeproject.com/Articles/803935/How-To-Make-Android-Studio-Really-Fast-On-A-Window

Feb 25:

I continued my attempt in installing in the real device. But I still couldn't. I found that there is no apk built when I run the project. So the studio complains that no local path

exists. So I need to understand what the heck is going through the Android build process. See how slow my progress is! :(

Oh... Android studio integrated gradle build is a crap!. It didn't even complain that the build was not successful. That is why there was no apk local path existed.

I ran gradle build from command line according to this tutorial: http://developer.android.com/training/basics/app.html
Steps:
1. invoke the assembleDebug build task using the Gradle wrapper script (gradlew assembleRelease).
chmod +x gradlew
./gradlew assembleDebug

I got an error when running ./gradlew: "libz.so.1: cannot open shared object file", followed by: "Exception in thread "png-cruncher_4" java.lang.RuntimeException: Timed out while waiting for slave aapt process, try setting environment variable SLAVE_AAPT_TIMEOUT to a value bigger than 5 seconds".
It seemed that both errors are due to not installing the library: zlib1g as mentioned in: http://stackoverflow.com/questions/21256866/libz-so-1-cannot-open-shared-object-file
After doing: sudo apt-get install zlib1g:i386, the gradle gave me: BUILD SUCCESSFUL Total time: 1 mins 16.537 secs. :)

2. Then I wanted to deploy the app in my phone also from the command line (mentioned in the same above tutorial).
Added android-sdk/platform-tools to PATH and ran: adb install app/build/outputs/apk/app-debug.apk
Yeyyy... I got my first android app installed on my phone! :) Now the floor is mine to do cool stuff.

Command line worked so smooth compared to crappy android studio.
Commands to build and run in the phone:
./gradlew assembleDebug
adb install -r app/build/outputs/apk/app-debug.apk

I went step further, I editted my app and tried to run again in my app. First I failed because it was already installed. Solution was to install it with the -r option. :)

29th Feb:

I didn't do much. I re-organized my research journal and went to apt with the hope of working more. But I was so tired and went to sleep.

1st March:

Learned many new things. At the end of the day, I have an app running in my phone with two activities linked (http://developer.android.com/training/basics/firstapp/starting-activity.html).

1. How to add a new activity and what are the other parts of an android project related with an activity: AndroidManifest.xml, the activity.xml under the res/layout folder, strings.xml file.

2. How to change the layout of an activity and use layout weight.

3. How layouts are related with parent-layout (as indicated in the activity_layout.xml and AndroidManifest.xml).

4. View and ViewGroups.

5. How to add a method for a view to be responsive. Method should satisfy following: Be public. Have a void return value. Have a View as the only parameter.

6. Intent:
   create Intent : newIntent(),
   add name-value pairs to it: intent.putExtra(name, value),
   start activity passing the intent: startActivity(intent),
   receive data sent thru an intent: getIntent(), getStringExtra(name).

7. Accessing View elements of an activity through:
   findViewById(R.id.¡id_name¿) method.

Next step: getting two apps to communicate. I might want to understand intents and intent filters properly before that.

3rd March:

I learnt how to invoke an app from one app that accepts an intent and return a result. However, I could not implement. I am writing down notes while I am reading a tutorial which slows me down. IDK
Anyway, below is something I can modify to abstract the high level idea and metion in the implementation details of the journal.

Intents:
- Following is from: http://developer.android.com/guide/topics/manifest/manifest-intro.html#ifs
The core components of an application (its activities, services, and broadcast receivers) are activated by intents. An intent is a bundle of information (an Intent object) describing a desired action including the data to be acted upon, the category of component that should perform the action, and other pertinent instructions.

- Android locates an appropriate component to respond to the intent, launches a new instance of the component if one is needed, and passes it the Intent object.

- Components advertise their capabilities the kinds of intents they can respond to through intent filters. Since the Android system must learn which intents a component can handle before it launches the component, intent filters are specified in the manifest as ¡intent-filter¿ elements. A component may have any number of filters, each one describing a different capability.

- An intent that explicitly names a target component will activate that component; the filter doesn't play a role. But an intent that doesn't specify a target by name (implicit intents) can activate a component only if it can pass through one of the component's filters.

14thMarch:

- I created a new project with two app-modules : authapp and clientapp and started adding the basic logic to it.
Actually, even this simple thing took me several hours to get right. Thing is, when I create a new android project, the app in that project is named just 'app', and doesn't hold the name that I give at the creation time. Although I tried renaming etc, didn't work. So, what I did was: create the android project, leave the default app that gets created, and create two new modules for my use with the names that I want.

- I made the client app to invoke the auth app, passing the SP URL to it.
Auth app printed the passed infor and returned the session id to the client app which the client app printed in a toast.
Troubles:
First the app crashed because the name of the method written for the button didn't match.
Then I learned to debug the app while it is running in the phone.
Then I couldn't invoke the second app because the way I have declared the data field in the intent filter didn't match.
Everything worked after I removed the data field from the intent filter.

15thMarch:

I couldn't do much. But I searched for some good tutorial to learn how to invoke a REST service from mobile app.

Then I found this good and complete tutorial (http://programmerguru.com/android-tutorial/android-restful-webservice-tutorial-how-to-call-restful-webservice-in-android-part-3) which uses async Http client (http://loopj.com/android-async-http/) which is based on the apache Http client.
I also drew the sequence diagrams for enrollment and authentication using ZKP, before starting implementing. Then I realized that we need an additional step to allow users to obtain:

- different IDTs with different To fields, with same commitment. For this, user just have to send the IDT issued by the IDP at the enrollment time with To field having IDP name and carry out ZKP to prove that the token belongs to him/her.
- different IDTs with different To fields and different commitments to achieve unlinkability. For this, user needs to send a biometrics capture, IDP runs it trough BID generator and create a new commitment. **We follow this approach because we do not store BID anywhere.**.

16thMarch:

I started writing a REST service to be invoked by the android app.

I thought of going for Jersey rather than CXF because, jersey is said to be more light weight and meant for REST, compared with CXF which is more focused on SOAP.

I followed these tutorials to learn. It was very easy. You only need web.xml.

- (2015) http://tutorial-academy.com/restful-webservice-jersey-maven/
- (2011) http://www.mkyong.com/webservices/jax-rs/jersey-hello-world-example/
- (Not so good, but it has client code.) http://www.vogella.com/tutorials/REST/article.html#installation
- (Jersey modules and dependencies:) https://jersey.java.net/documentation/latest/modules-and-dependencies.html

Troubles:
I got an issue of not being able to access the REST service. It was due to the fact that in

servlet filter pattern, we need to specify the path ignoring the path until the webapp's name.

Oh god, now I have basic REST service written in jersey to play around with.

I read a bit about android http clients before start writing the client side for the REST service.
This article gives a very good history: https://packetzoom.com/blog/which-android-http-library-to-use.html
But it doesn't mention about async http client. Also, the quora thread doesn't mention about it: https://www.quora.com/What-is-the-best-library-to-make-HTTP-calls-from-Java-Android
From the first article above, it seems that OkHttp is promising, but it seems that it requires some additional things to get REST, json, images etc working such as Retrofit..

The reason I didn't go with Volley: https://developer.android.com/training/volley/index.html (although it is from google) is that it has very few number of threads as per the first article above. But the plus point is that it is said to work with all types of devices including low power devices.

I thought of going with async http client as it is based on Apache HTTP client, but the only problem is that it says it is compatible with Android API 23 and higher. Let's see. If problematic, I will switch to OkHttp or Volley.

HTTPS clients with Async Client:
http://stackoverflow.com/questions/21833804/how-to-make-https-calls-using-asynchttpclient

Troubles and Solutions:

1. The first problem I got was: the dependency for the async http client was not resolved by Android studio, although I could build the project using command line gradle. I tried several things: File-¿Invalidate Cache and Restart etc. Only thing which worked was: moving the entry for async http client one entry up in the gradle script. It was this stackoverflow thread which helped me: http://stackoverflow.com/questions/19508649/android-studio-says-cannot-resolve-symbol-but-project-compiles

2. There was another wired issue: I couldn't assign response's values to local variable defined in onAuthButtonClicked method of AuthActivity of AuthApp, because the response received in the onSuccess method of an inner class of async http client. I had to declare the variable as final and had to make it an array too. Related stackoverflow thread: http://stackoverflow.com/questions/27558425/local-variable-access-to-inner-class-needs-to-be-declared-final

3. So, finally, I was able to build the mobile app with async http client. But I wanted to return the response as JSON. Actually, Jersy has very good support for object to json conversion. This tutorial is a good starter: http://www.mkyong.com/webservices/jax-rs/json-example-with-jersey-jackson/.

4. Troubles continues: I couldn't invoke the rest service from the mobile app. I left Hicks undergrad, after my first try.
   Came home, did exercise, cooked, ate, talked with amma, thaththa and Thil and tried again.

   I could access the service through host (windows) browser, but not from android. I debuged, and got the exception as: connection time out. Actually, in order to debug, I had to avoid the normal route of client app invoking the auth app, and implement AuthActivity invocation from the mainactivity of the Auth app itself, Silly me didn't realize that the IP of VM is not visible to outside. I went to sleep thinking it might be the reason that async HTTP client is said to be compatible only higher than API 23 or something

Opportunity: Prof. asked me to write a proposal for PRF. I would like to write it. I need to steal some good time from my busy schedule to write down one of my ideas for the proposal. I am thinking of writing the GC idea for biometrics authentication which could avoid some of the drawbacks in our current method. I need to read the previous (NDSS paper) and get an idea where things stand today. May be I should spend the research three days of next week for writing the proposal (Sunday, Tuesday and Thursday).

17th March

Today morning I got up at 7.15 and thought that I will do only PL, cause I spent whole day yesterday on research proj. But I missed the bus at 8am so I thought I will try to connect mobile app to phone till next bus.

The journey:

1. First I tried to access the tomcat home page from phone and ipad browsers, which failed.

2. From this thread (http://stackoverflow.com/questions/9887621/accessing-localhost-of-pc-from-usb-connected-android-mobile-device), I tried to make a hotspot in phone and tried to connect to it from laptop. But, as soon as the hotspot is made, the normal internet connection in phone goes off. Seems like it should be made using the data connection in the phone. So that option is out.

3. From some other reading, I realized that firewall may be blocking. Then I tried to disable the firewall and tried to access the tomcat home of server in VM Ubuntu, from phone-no hope. Silly me didn't try to first access a server in host OS and see at least if it works.

4. Then I added an inbound rule in firewall to allow connections on port 8080, since I am scared of disabling firewall. It didn't work either.

5. I installed tomcat on windows and tried to access its home page from phone browser. It worked only after disabling the firewall. But still no luck accessing the tomcata in Ubuntu VM.

6. Then my understanding improved and I checked VM settings. The networking is enabled through NAT, which doesn't make VM visible to outside, that is why the phone couldn't access the tomcat running in VM. Hmmmmmmmmmmmmmmmmmmmmmmmmm.

7. The solution was to make VM settings such that network mode is: bridge. But so so badly, for some mysterious reason, all the real network adaptors are not made available to VM Ware settings. I do not know if it is done by Windows 8 or if it is due to some other reason.

   I should check : just like enabling virtualization for CPU, whether I need to enable something from bios. But bridging for VMs seems to be something that trivially work for others, but not for me.

   Following are some links that I found useful when searching to get over this issue:
   - Good article: https://pibytes.wordpress.com/2012/11/16/vmware-workstation-networking-basics/
   - Threads: http://askubuntu.com/questions/629457/i-cant-connect-to-virtual-ubuntu-server-from-smartphone, http://askubuntu.com/questions/237461/how-do-i-access-ubuntu-server-running-in-virtualbox-from-outside

   As this thread (http://superuser.com/questions/810097/vmware-player-bridged-networking-no-longer-works-host-win8-1-guest-mint-17-l) says: lot of Virtual Box related adaptors are made available, which I unchecked in Bride settings, but still no luck.

   As this thread (http://stackoverflow.com/questions/4601762/how-to-connect-wireless-network-adapter-to-vmware-workstation) suggests, I also tried making a loop back, as described here: (https://4sysops.com/archives/how-to-install-loopback-adapter-in-windows-8/). Still no luck.

8. My final fall back was to use same old NAT for VM and use port forwarding, as suggested in this thread: http://stackoverflow.com/questions/10355702/connecting-to-apache-web-server-that-is-running-on-a-vmware-from-any-device-in-t
   The tool made available in this site (http://www.quantumg.net/portforward.php): saved me finally. I hope I can trust that is not a malware. Even if it is, I have no other option.

   Well, I have one, which is: run tomcat on Windows-¿copy .wars to it and access from phone. But I feel it will be very time consuming during the dev process. It will be good for perf testing.

To Dos:

1. Study the mobile phone's security architecture and find about the latest work in the secure architecture/trust zone.
2. Discuss the attack surface/vulnerability window and argue that it is very small.
3. Look at Daniel's journal paper to see how to prepare a journal paper.
4. Do an experiment to see if classification gives better results than distance matching.

Literature Survey:

Feb 19

Today, I was just searching zero knowledge biometrics authentication for remote services. I got a bunch of results - papers and a commercial product.
Sedicii
This commercial product : sedicii (https://www.sedicii.com), seem to be doing exactly what I have done: ZKP based identity verification/authorization. They say that they do credit card authorization as well as biometrics authorization in ZKP - exactly my two works. They have not described how they do biometrics authentication in ZKP, however, it should be similar to their website loging scenario: I have written how their credit card authorization is comparable to ours in my RahasNym journal.

Brain Storming:

Feb 2

I went through their attack descriptions. Their attack target is Android fingerprint authentication/authorization framework, in which the features extracted from user's fingerprint is stored in encrypted form, for matching during authentication time.
They show that these can be stolen if TrustZone (a form of TEE) is not used and that they can be permanently lost since they are not revocable.
Since we do not store the biometrics features as it is (and not even the biometric identifier, which is revocable as well), our approach is secure against the rooting attack they mention. However, since we had proposed to use the TEE to securely store other artifacts, I need to look into the attacks against the TEE further, in the third presentation linked above. I will update you on that too.

Feb 3

I read the white paper on Exploiting Trust Zone in Android [1].
Summary is: by exploiting a vulnerability in the kernel of TEE, any user-mode application

could read from/write to any physical memory location. This has made possible for a malicious local application to read the fingerprint image from sensor which is supposed to be read only by the trusted application related to fingerprint scanning.
However, under the responsible disclosure note at the end of the paper, it says "These vulnerabilities were disclosed to Huawei PSIRT in March 2015,a fix was provided by Huawei in May 2015.CVE IDs were assigned as CVE-2015-4421 and CVE-2015-4422."

Feb 19

Lot of biometrics based authentication mechanisms are defined for authenticating to devices. Once authenticated into the device, different services that the user accesses are already logged in with username/password security. In such cases, critical remote services are relying on the device biometric authentication, which is not usually strong.
TODO:
See how device biometrics authentication works in Android and Apple.
Also, if a malware is installed by some mistake by the user, client of the remore service is at risk (password can be stolen, session stolen etv.).
TODO:
See how bank apps work in mobile devices.

This shows the requirement for remote services to have their own authentication of user to make sure that the genuine user invokes some request, with strong verification, beyond usernam/password, and without relying on device autentication.
ZKP is a good candidate. There are some previous works, suffers from some drawbacks.
Main issue is identity is not static.
The works differ by the approach they address this non-static nature of the biometrics.

This should be a standard mechanism, that any app resides in user's device-communicating with the remote service can integrate easiliy.
TODO:
See this could be developed as a service in Android which could be invoked by other apps.

Contributions of our work:

- Secure protocol for remote authentication using biometrics. Preserves good properties of biometrics (i.e: uniqueness). Avoids non-desirable properties of biomertics (i.e: non-repeatability, non-revocability).
- Prototype implementation that is a proof of concept. That can be integrated to any app.
- Security Analysis and Performance Analysis.

Feb 20

I started documenting what I wrote down on paper during the weekend. I felt I need a brainstorming/mind mapping tool. And I got FreeMind and noted down different aspects.

16th March:

I found these articles which talks about Amazon, Alibaba and Google adopting selfies or FRT to make payments instead of password. But I think it is bad. Coz now, instead of passwords, you store templates to pattern match, which has higher risk than passwords, coz passwords can change and you can use different passwords at different SPs unlike your frt template. You need a secure (in the sense that biometric template is not stored) and privacy preserving (in the sense that user's biometrics are not exposed to third party SPs that the user does not trust.)

17th March:

1. https://thestack.com/security/2016/03/15/amazon-wants-to-replace-passwords-with-selfies-and-videos/
   Motivation: Hard to type passwords in small screens.

2. https://thestack.com/cloud/2016/03/03/google-hands-free-facial-recognition-trial-san-francisco/
   Motivation: To make it super easy: users do not even have to take out wallet or phone. To protect CCN.

   Picture taken from in-store camera is verified against your Hands-free profile picture and the temp pics are deleted.

   Hands Free never shares your full credit card number with the store and all your payment details are stored securely and shared only with the payment processor.

   The cashier can only charge you when Hands Free detects that your phone is near the store. The cashier then verifies your identity to make sure that they are charging the right person. You'll get instant notifications after every purchase, so you can check purchase details right away.

3. https://thestack.com/security/2015/03/16/alibaba-demonstrates-facial-recognition-payment-system-at-cebit/
   Motivation: People forget passwords.

4. https://thestack.com/iot/2016/02/22/mastercard-rolls-out-selfie-verification-for-mobile-payments/
   Motivation: To prevent the cost of false decline of transactions.

   Consumers will be asked to upload their pictures online to be stored on MasterCard servers. These registered images will then be used as a reference every time a user opts for facial verification during a transaction.

5. https://thestack.com/world/2016/02/19/hsbc-voice-biometric-online-banking/
   Motivation: quicker and easier for customers (15 million of its customers by summer 2016).

   Biometric banking has been used by other banks in the past, notably Barclays, which rolled out voice recognition to its top 300,000 wealthiest corporate customers in 2014. In the U.S., Citibank has approximately 250,000 customers who have signed up for voice authentication since the company launched the technology in April 2015.

6. http://www.americanbanker.com/news/bank-technology/banks-embrace-biometrics-but-will-customers-1078867-1.html

   Citi: When customers call in, their voices are matched to the prerecorded data.

7. http://www.americanbanker.com/news/bank-technology/biometric-tipping-point-usaa-deploys-face-voice-recognition-1072509-1.html

   The key thing, and what may turn out to be USAA's secret sauce, is the company uses device identification in the background, so each time a member logs in, an encrypted token is sent from their phone to USAA that is matched against the ID of the device registered at enrollment. So for a fraudster to successfully impersonate a member with a photo or video (or trying to mimic their voice), they would also have to steal the member's mobile device.

   The other safety mechanism is that USAA requires the member to blink, which rules out the use of a static photo or video replay, because video can't blink at the right moment.

   GREAT! Swenson said USAA's technology analyzes facial bone structure and dimensions, allowing it to see through such alterations (beard, glasses, aging etc.).

8. Apple Touch ID: Activates the scanner on contact which then takes a high-resolution picture of your fingerprint. That fingerprint is then converted into a mathematical formula, encrypted, and carried over a hardware channel to a secure enclave on the Apple A7 chipset. If the fingerprint is recognized, a "yes" token is released. If it's not, a "no" token is released.

   Secure Enclave: The A7 also includes an area called the "Secure Enclave" that stores and protects the data from the Touch ID fingerprint sensor on the iPhone 5S and iPad mini 3.[10] The security of the data in the Secure Enclave is probably enforced by ARM's TrustZone/SecurCore technology.

9. ARM's TrustZone: Wikipedia: https://en.wikipedia.org/wiki/ARM_architecture#Security_extensions_.2
   It provides a low-cost alternative to adding another dedicated security core to an SoC, by providing two virtual processors backed by hardware based access control. This lets the application core switch between two states, referred to as worlds.
   Open Virtualization[81] and T6[82] are open source implementations of the trusted world architecture for TrustZone.
   In practice, since the specific implementation details of TrustZone are proprietary and have not been publicly disclosed for review, it is unclear what level of assurance is provided for a given threat model.

March 21st and March 22nd til 4pm and March 24th from 4pm to mignight and March 25th from 11.30am-2pm

I wrote PFR proposal. It takes lot of time to write.

Professor liked the proposal very much.

She said that she is very confident that I could do the prelim early this Fall.

New Ideas:

I attended Prof. Dongyan Xu's research award talk. I liked how he presented his research work as branches of a tree.

0.1 Privacy Preserving Personalized Medicine

The research that I wanted to do so eagerly, once upon a time.
After the discussion with Fang-Yu about that, he mentioned about indistinguishability obfuscation, in addition to GC based solution that I had in mind.
Today (18th March), I found this paper on that topic: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnum
Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits (Extended Abstract) by Sanjam Garg IBM Research Craig Gentry IBM Research Shai Halevi IBM Research Mariana Raykova IBM Research Amit Sahai UCLA Brent Waters UT Austin

PrivBioAuh and PrivBioGeneAuth

I can have two projects under the umbrella: PrivBioAuth. Two will be: PrivBioMTAuth and PrivBioGeneAuth.

How to address the security issues in health care data collected from IoT devices using biometrics.

Professor suggests to see how to generate keys from biometrics to protect the medical data.

Fuzzy Zero Knowledge Scheme:

Feb 23:

I worked on the research the whole afternoon after lunch - but on an apparently useless one. I tried to comeup with a fuzzy zero-knowledge protocol based on the ideas from fuzzy identity based encryption. But I had no luck.
I need to look at fuzzy commitment and fuzzy vault before talking about this with anyone else.
Professor mentioned we can talk with Professor Atallah or Italian professors.

Storing the machine learning model by encoding it in a garbled circuit

Feb 19

- I got an idea yesterday that I could use the same method of obtaining a circuit from IDP for authentication verification later.

But the circuits can be used only once, which is a problem.
QUESTION:
- Good question I can ask in the summer school: are garbled circuits re-usable?

- Also, I argue that due to memory forensics techniques etc, secret information unfolded in the memory can be compromised in our previous approach. Wouldn't this solution have any secret information unfolded in memory? Not even keys? I doubt.
REFERENCES:
This is a very nice project website - a resovair of resources. http://www.mightbeevil.org/ and http://www.mightbeevil.org/mobile/

27th March

Completed writing a proposal on this idea to be submitted for PRF funding. Professor Bertino liked it.

Meetings with the advisor:

Feb 25:

- I spent lot of time getting ready for the meeting - how I explain what I did, and my ideas to the Professor. At the beginning, she was not in a very good mood. But the end was very good.
- It is ok to have 35% overlap with the conference paper. If I could get the implementation on the mobile phone and do the Performance evaluation, that would be an excellent extension for the journal paper. Need to get it by the end of this semester. Usually we do not submit new work for journals. Only extensions.
- I need to look at Daniel's journal to see how I can prepare my journal paper.
- I need to study the mobile phone android security architecture and write about it.
- Professor mentioned about the new idea of protecting the medical data.
- Professor was interested in two of my new ideas. Professor mentioned we can ask Prof. Atallah or her Italian collaborators. She said it is a very specialized area.
- Professor gave me the two recommendations for the communication requirement and the travel grant application.

Next Meeting:

I should mention about the issue of recovering from memory images. May be we can ignore it for the moment.
Can we mention about the counter measures that we took in order to avoid the threats arise due to specifics of our architectural decisions and the specifics of the framework?
May be we can mention them as the security best practices for client implementations.

March 22nd:

I met with Professor to talk about the proposal. I worked hard and sent an initial draft of the proposal to her just about 1 hour before the meeting. She said it looks reasonable. Then I mentioned breifly

Real world stories:

Biometrics:

1. From: https://thestack.com/security/2015/03/16/alibaba-demonstrates-facial-recognition-payment-system-at-cebit/

New York City Universitys Center for Catastrophe Preparedness and Response (CCPR) published an interesting report [PDF] in 2009 detailing some of the more pervasive problems of FRT systems:
As the size of the identification database increases, the probability that two distinct images will translate into a very similar biometric template increases. This is referred to as the biometric double or twin. Obviously, biometric doubles lead to a deterioration of the identification system performance as they could result in false positives or false negatives.

Ninety per cent of the factors individuating one face from another occur in just 10% of the facial area, and as the enrolled database of volunteered face images grows, the differences can become trivial enough to obtain either a false ID (the wrong person succeeds in identifying as someone else) or a double-match (the probe picture matches more than one face in the database).

Australias SmartGate FRT technology (pictured right), designed to speed passengers more quickly through airport security, was duped by two similar-looking journalists (Ibid) when first launched at Melbourne Airport in 2002. The two similarly-featured journalists had previously succeeded in duping other facial recognition systems, and successfully got through the SmartGate system after swapping passports.

According to the report, FRT accuracy is very sensitive to the aging effect, stating: For 18 to 22 year-olds, the average identification rate for the top systems was 62%, and for 38 to 42 year-olds, 74%. For every ten-year increase in age, performance increases on average 5% through age 63,

Getting my theory right:

I really need to learn the primitives I have used in my projects right, so that I can teach them to someone else correctly.

Zero Knowledge Proof of Knowledge:

1. Pedersen Commitment
2. Zero Knowledge Proof of Identity paper
3. Formal Language for ZKP by Camenish and Stadler (get the reference from DAA paper.)
4. DAA - the first real world implementation of ZKP? Sure? What about Idemix?

5. Implementations:

   (a) Bringing Zero-Knowledge Proofs of Knowledge to Practice. Endre Bangerter Stefania Barzan Stephan Krenn Ahmad-Reza Sadeghi Thomas Schneider and Joe-Kai Tsay (https://eprint.iacr.org/2009/211.pdf)

   (b) On the Design and Implementation of Efficient Zero-Knowledge Proofs of Knowledge (same authors) (http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BKSST-speedcc09.pdf)

   (c) An implementation of zero knowledge authentication (NARWHAL): https://courses.csail.mit.edu/6.
   cheu-jaffe-lin-yang-zkp-authentication.pdf

   (d) Implementation and Evaluation of Zero-Knowledge Proofs of Knowledge (https://securewww.esat.ku
   206.pdf)

Garbled Circuits:

1. First one by Yao
2. Security By Lindel
3. Formalization by Rogway

Biometrics Features:

1. Refer that paper I reviewed.
2. FisherFaces nice tutorial: http://www.bytefish.de/blog/fisherfaces/
3. MultiModal/Fusion:

   (a) Robust Multi-Modal Biometric Fusion via Multiple SVMs : Sabra Dinerstein, Jonathan Dinerstein, and Dan Ventura (http://axon.cs.byu.edu/papers/dinerstein.smc07.pdf)

   (b) An Ensemble Approach to Robust Biometrics Fusion : http://ieeexplore.ieee.org/stamp/stamp.jsp?t