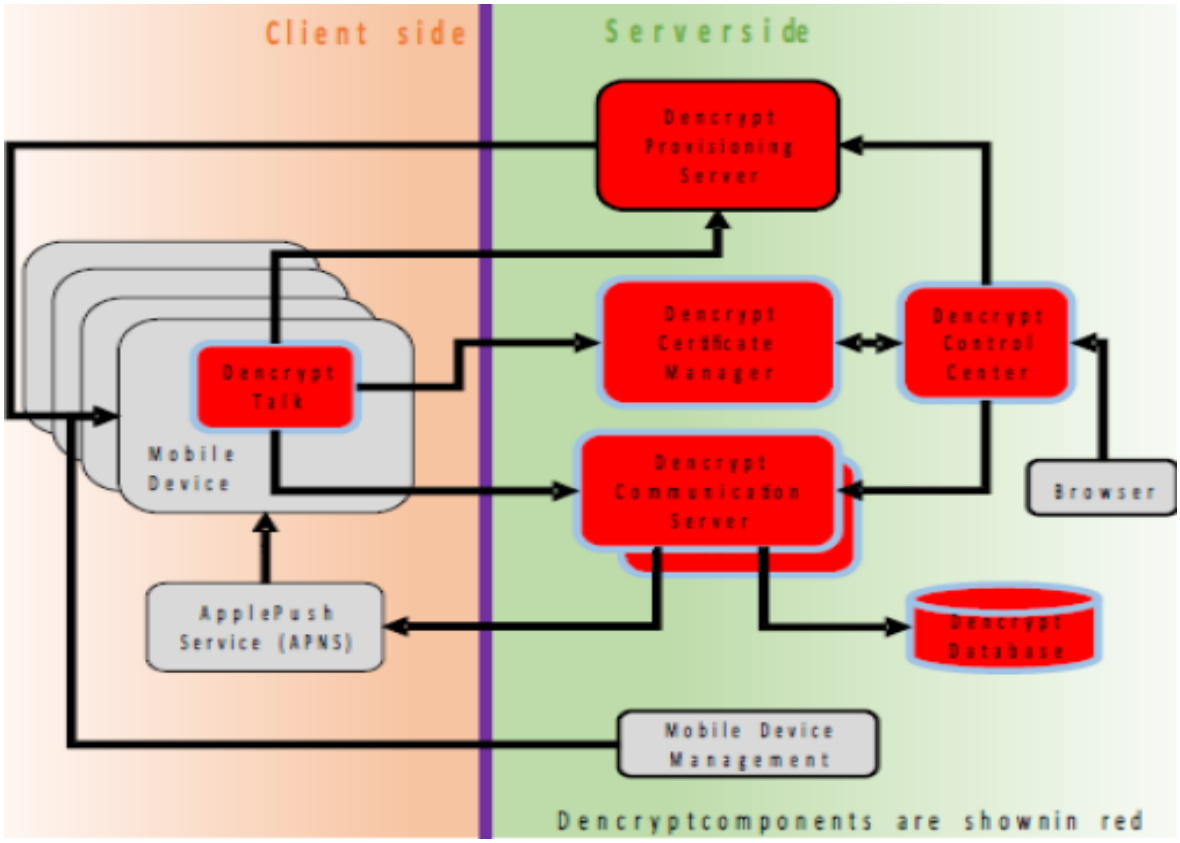
PV204 Phase One report

This report is basically a written-out version of my original full-length presentation. I was analyzing the security certification for **Dencrypt Talk for iPhone version 4.2.794** which is an iOS application intended for chat and VoIP calls within a managed closed group of users.

The important thing to note here is that, as expected, there is a number of components for the service to be functioning properly, for example messaging server, KPI, etc. All of these components, including any third party tools needed to establish the Target of Evaluation (TOE) environment are not a part of the TOR. The TOE here is only the iOS client.

The TOE was granted EAL4 with ALC_FLR.2 flaw reporting enhancement, meaning that besides the EAL level, the Dencrypt team also has in-place an adequate system for reporting and addressing any security or other flaws found in the systems by users after release. The evaluation was done by atsec Information Security ag and the certification is issued by CSEC, the Swedish certification authority.

Here is an image of the overall architecture of the TOE environment to demonstrate the complexity and to help better illustrate the later points:



Next, let me briefly summarize the Security Assurance requirements (SARs) that were needed and met during the assessment. In the development cathegory, the lab has assessed if principles of mudilar design were followed, if the functional specification and security architecture is sufficient and so on. What was interesting to me was the fact that these criteria are quite similar to the principles taught in software engineering and software quality courses.

In the Documentation area of SARs, the deployment and user guides were evaluated, these are also used later to establish the requirements and it is assumed that the administrator and users are adhearing to doccumentation perfectly.

For Security Target area the evaluation criteria seem to be more formal, checking if components and requirements were defined and so on. For tests both automated and manual tests were executed, including trying to modify values of tests and checking output. The developers have also supplied a specific version that is able to extract keys to evaluate the randomness of key values. Subset of manual tests was executed.

Lastly, in terms of penetration testing the application was tested against known CVEs as well as manipulated components of the TOE enviroment. As for sidechannel testing from what I have noticed, there was traffic analysis done, but nothing trully sidechannel such as timing attack.

The software provides 4 security functions: secure initialization (enrollment inside an MDM enviroment using link which needs to be fresh), secure management (calls and chat can be done between phonebook entriues only, phonebook is managed remotely, can not be modofied on deide). Secure messeaging and secure channel towards the other components.

If we add organizational security policies, the software also has to provide key generation, closed comms and forward secrecy

In terms of cope of the attacker model that ithe software os evaluated against, there are three main vulnerabilities: data breach (attacker gets access to credentials, phonebook, settings), impersonation (another user in the closed groups tries to assume identity of someone else) and sniffing (traffic on the network is captured by a third party).

Before I get to product evaluation and what is out of scope, let me briefly mention the security concepts used here and mainly the differences I found between this and for example the Signal protocol mentioned in the latest lecture. Firstly, the application seems to be for real-time communication only, or rather for end to end ecommunication only. A server is used for the initial signaling to start establishing a session (to fullfill the need for an updated off-device phonebook), but after that, the SIP call session that is essentuially running in the background is between two devices only without any storage capabilities on the sever.

As for the encryption, there are a few interesting features for me, one is that the application is running an encrypted version of SIP and basically runs Diffie-Hellman together with the process of derivating keys, applying multiple keys and all that we discussed in class, but they are also randomly selecting the encryption algorythm for each messeage, which seemed really unique to eme and from what they say is a part of their patern.

Another, quite interesting thing, is that for both call and chat sessions they use the same process, so a chat session has a VOIP call running in the backround, but without any voice content. This kind of seems like a good anti side channel meassure, although they don’t mention it in detail, as I suspect it may be used to make it harder to sitinguish between chat and call data.

Now, moving on to what is note in scope of the certification/TOE. Essentially everything. As you can see from the image on the first page, the Dencrypt system needs a lot of other components that are out of scope. This includes a corporate Mobile Device Management solution that you need to even deploy the application. In the report you can also see that nothing beyond what I listed is considered, no physical threads, no inside threads, it is

presumed iOS if flawless, everyone behaves exactly as expected, the system provided RNG is truly random and so on.

On top of this, the Dencrypt Communication Server is certified at EAL2, and as it is required to run Dencrypt Talk, I am not sure why EAL5 here would matter. Also, as noted by the certification authority, the versions of iOS change, headset models change, applications models change, so the validity of this particular certification is quite short.

So, to my personal remarks, would I buy this solution? Depends. If, for some regulatory reason, I really needed it, then I would. I appreciate the unique security implementation, but given all of the other components it seems overly complex with a large attack surface. For corporate applications I'd likely use a third party or something like Signal, for government use, this is likely not suitable for highly classified material.

Lastly, a note, during my research I found that this application is approved for NATO RESTICTED confidentiality level. This is not particularly high, as it seems to be similar to the NBU's restricted classification, the lowest level in Czechia. That would be in line with my personal assessment of Dencrypt Talk.