Skype Censoring with Low-level Hooks of internal APIs

¡ Reverse engineer a highly-protected application and analyze its core logic to produce a hook solution that survived 2 years of regular application updates!

The Client Task

Apriorit team is working with a big security vendor on a proactive enterprise security solution. The next stage required Skype control functionality with a set of monitoring and management features:

- ✓ Skype activity monitoring (calls, messages, file transfers)
- ✓ Skype message censoring
- ✓ Action blocking (block calls, contact addition, files and messages sending/receiving)

The possibilities provided by public Skype APIs (skype4com library) were not enough for the required features, in particular action blocking and full monitoring. A brief research of the existent analogue solutions showed that they were all based on GUI hooks and could not provide advanced functionality like message censoring or action blocking.

The Client team had two alternatives: either simply implement basic Skype monitoring features to keep up with the majority of competitors or insist on deep Skype research and convert these advanced features in market differentiator for the product.

As the result, Client called Apriorit Research and Reverse Engineering group.

Research Task

Apriorit specialists made up a detailed feature list to be implemented and prepared functional specification for it. Using these documents, they composed the list of corresponding internal Skype APIs to be discovered and described.

The next task was to research the core logic of Skype application to detect the points to set up custom hooks for the obtained inner APIs.

And the final task was to implement the required hooks.

Working On

Being a very popular commercial communication solution, Skype is highly protected application. Authors used debug protection techniques, internal code obfuscation, hook prevention technologies, in particular check sums for executable code.

Researchers sequentially went through all code protection levels and started code restoration. Thus they managed to describe all necessary functions.

After that, the code analysis started. As Skype is a frequently updated application (update each 2-3 weeks), it was essential to set up hooks in a core logic part so that the resulting security solution would be able to work with the Skype new versions without significant rework.

Code analysis allowed Apriorit researchers to detect effective points for hooks, where Skype application logic would not change significantly with version updates.

Results

The full-functional Skype security management component was completed in 1.5 man-year of research and development. The provided solution has already survived 2 years of regular Skype updates (from v 5.1 to 6.7 so far) with minimal support around.

As the publisher states, new Skype versions will not have public APIs, that means that the competitive security solutions will have to completely change their functioning strategies. Meanwhile, Apriorit team believes that the created solution, which uses internal APIs, will require minimal additions within regular maintenance work.

What’s next?

Get the **free estimation** of time and effort for your research task! Unlike many R&D service providers, we understand the specifics of research projects and completely rely on the professional skills of our specialists. So it won’t be just one phrase with the total sum and dead line.

Apriorit free research estimation pack includes:

- Basic task dropdown with the research approaches indicated;
- Each task-approach time & effort estimation supported by our broad research project experience;
- Prototype development estimation.

After we’ve received your request for proposal, usually it takes 2-7 business days to prepare the estimation for your task.

¡ So let’s start solution search right now with a zero-risk estimation stage !

All we need to start is a brief research task description sent to the info@apriorit.com with “RFP” mentioned in the subject.