[u] Space

END TO END ENCRYPTED PLATFORM

How Uspace Developed its first end to end encrypted messaging platform

INTRODUCTION

USpace was introduced when WhatsApp, Slack didn't had the end to end encryption and were targeting the organizations to use the platform. Uspace followed a policy and was tested on different levels to achieve a stage where it passed the CIA Triad and related laws on user security.

USpace had a key system where each message was encrypted by unique key chains and can only be decoded by the parties to the chat. The most important aspect was not only the encryption of the messages but also every media and related details of a particular user. User were given access on the ground level to select the privacy.

> USpace Delivers Discreet And Private Communications Network Available To The Public

RESULTS & DISCUSSION

We needed to go over the whole architecture 4 times and made sure that USpace was delivering what is was supposed as the stakes were high and the market was expecting the platform.

Queues and vulneratbilities made sure we are standing every aspect of user security to pass the CIA triad. Uspace became the frst end to end encryption platform.

KEY LEARNINGS

- *Vulnerability*
- *Infra logging*
- *Queue system*
- *Polling*
- *Encryptions*

VULNERABILITY & PENETRATION

Even after integrating all the security protocols. Tests such as nmaps, intrusion, failover, and acl's revealed so much about the final platforms which helped us make it more secure. There is always a scope for security in any platform. Some are more secure some don't have any security. The platform had 100 open ports.

QUEUES & LOGGING

The queue was added to the platform which made sure of the right polling to the users as well as we had every task in the queue system associated with the platform. The logging was not only done at the system level but even at the infrastructure level which allowed us to shut down any infrastructure changed without the platform's permission.