Secure Mobile SM60

INTRODUCTION

In today's world, Mobile phone is the most popular communication device in the world. With productivity enhanced by mobile communication specifically with rise of BYOD and lack of control over the infrastructure, there are risks to cooperate assets, privacy, confidentiality and regularity compliance; and phone conversations are strongly vulnerable to various threats. In fact, voice interception regardless of network standard (PSTN, GSM, 3G, LTE etc.), is unfortunately the proven fact and not a myth.
This solution consists of a system installed on android mobile phones, and the sub system of this solution contains a secure call center. The voice calls can be secured, archived and traced. Secure mobile is capable of providing secure channels with using strong cryptographic mechanism for confidential and authenticated speech. This product acts as a real time and full duplex system and transfers encrypted voice signals via internet network by a private secure server.

SPECIFICATIONS

- Secure voice conversation and Man-In-The-Middle attack protection
- High degree of security, control of calls, user management and real time speech with high voice quality and very low latency
- End to end encryption with strong and native cipher algorithm
- Executable on android 4.1 OS or later and any type of data network (GSM, 3G, 4G, LTE etc.)
- Simplicity and compatibility
- Private secure server for customers

Computer Emergency Response Team CERT

INTRODUCTION

Computer Emergency Response Teams (CERT) are expert groups that handle computer security incidents. Alternative names for such groups include "Computer Emergency Readiness Team" and "Computer Security Incident Response Team" (CSIRT).
The role of CERTs seem inevitable because of Threats and Security Flaws that threaten organizations nowadays, and such groups are pointing out the task of handling computer security incidents instead of other tech support work. The history of CERTs is linked to the very existence of malware, especially computer worms and viruses. Whenever a new technology arrives, its misuse is not long in following. With the massive growth in the use of information and communications technologies over the subsequent years the now-generic term "CERT" / "CSIRT" refers to an essential part of most large organizations structures.
So CERTs are groups formed to study internet security vulnerabilities, and provide assistance to online sites that become victims of cracker or hacker attacks. They ensure the provision of essential services by identification, limiting and preventing the possible damages.

FEATURES

CERT Units

- Informatics Unit
- Training Unit
- Website Unit
- Alarming and Warning Unit
- Call Center
- Security Operations Center
- Triage Unit
- Response Unit
- Data Destruction Unit