Cybersecurity Communications & IOT Industry: path to the future

Fabio Fischer

January, 2020

SIKUR

find out more at **sikur.com**

Freemium communication Apps and a plethora of mobile operating apps are surfing the wave of smartphone growth and popularity worldwide. When it comes to numbers, about 90% of mobile device users have one of these Apps installed for daily use. However, although this number has a direct relation with consumer user space, many private and public organizations use these Apps as their organizational channels to exchange private information, which is a strategic mistake.

Companies must double-check Apps that have a **history of information leakage** unclear, or even adverse user privacy policies. By considering this fact, it is not hard to find references on the Internet about **Apps with this kind of issue**.

Another recurring problem is about sovereignty, as the cloud is present and moving into a growing number of organizations, data is spread out the globe through mobile devices, for the sake of availability, some might say. But, with the serious risk of outages due to cyber wars, distributed data can be an issue. This **white paper** shows how **vulnerable government** agencies are due to the usage of freemium tools. Technology is crucial these days, but the misuse of its tools and resources might be even more harmful than not having them.

Private organizations now demand local Datacenters to guarantee data sovereignty, and market messaging platforms can't deliver this level of flexibility. That´s why we thus believe in the global trend based on Private Cloud business model, together with encrypted and white label apps to provide secure communication while keeping the data near, which can scale as the user base grows. Unprotected endpoints using weak authentication and poor management are easy targets for cybercriminals. On this road another major challenger arises on automatic global connection front: IOT

As IoT proliferation sweeps across the planet, businesses and consumers are benefiting greatly from the increased connectivity. However, this connectivity is also introducing greater security risks than ever before. These risks must be properly handled by manufacturers to prevent consumers from losing confidence in these devices.

Manufacturers are about **to change their practices and design and build cybersecurity protections** into their products based on negative exposure or regulation. Recently, we've seen emerging security standards for IoT and data privacy. California's new IoT Cybersecurity Law will require manufacturers of connected devices to produce them with "reasonable" security features.

On both fronts: secure corporate communications and IOT applications, several market verticals are facing regulatory problems (data protection laws), leakage of strategic information, fines and negative exposure of the organization, among others. Just to get an idea of the urgency of the topic, as we write this article, the World Economic Forum Centre for Cybersecurity has **published a report**, endorsed by several global telecommunications companies, with direct access to more than 1 billion consumers in 180 countries, formalizing Principles for Cybercrime Prevention for Internet Service Providers.

Very important points are raised there, but with complex implementation, such as: a) Protect consumers by default from widespread cyberattacks and act collectively with peers to identify and respond to known threats; b) Take action to raise awareness and understanding of threats and support consumers in protecting themselves and their networks; c) Work more closely with manufacturers and vendors of hardware, software and infrastructure to increase minimum levels of security.

"Cybersecurity is becoming a public safety issue," said Amy Jordan, "As more and more devices are connected and physical infrastructure becomes increasingly connected, no one company can do it alone. The community needs to come together, and these principles can accelerate and scale impact."

In Sikur´s experience solving companies and governments communications challenges, through one of its product, a communication **encrypted platform**, non-repudiation, data integrity, confidentiality and authentication will play an essential role in all of this, as the number of the device increases exponentially. Sikur's expertise can provide the missing piece for IoT security, where it is essential to make sure that only authorized tools have device access, protecting them from cyber-attacks. The same technology ensures that information exchange between people (H2H) will also be used to ensure security between humans and machines (H2M) and between machines (M2M). In **this report** our CSO explain Vulnerabilities and security issues of IoT devices.

One of the Sikur´s new product, to be launched in February at Mobile World Congress 2020 in Barcelona, for example creates a lightweight, secure and manageable channel for IoT devices, facilitating their deployment and control.

The challenges of the scenario brought by world economic forum report are not restricted only to telecom companies, they also falls on Operational System, Hardware, App, **authentication technology** manufactures and Cloud providers. This reality reaches many market verticals such as **healthcare**, **finance**, defense, **government**, data regulations, autonomous vehicles, **individual privacy** etc.

Even media companies and journalists have been targeted by hackers. In **this article** we can understand as New York Times Journalist has faced this own path on this front. when the New Your times published the article "**one nation tracked**", it has exposed another aspect of the world of device monitoring and georeferencing, played not by hackers but exposing a new use of personal data.

When we start reading things as: " **Apple To Restrict Facebook, WhatsApp Voice Calling Feature To Prevent Background Data Collection**" and " **QualPwn vulnerabilities in Qualcomm chips let hackers compromise Android devices**" , it is a clear sign that the rules of the game are strongly change also in the world of **hardware**, applications and operating systems.

In order to address these challengers Sikur is not just providing an encrypted military-grade App, but going one step further, integrating the concept of private cloud and security all the way down to the endpoint. This is guaranteed by the exclusive model for Apps and device authentication, its operational system (Sikur OS), and software suite with specific guidelines to provide security and privacy at all levels.

As mobility grows and Digital Transformation takes place, a set of new technologies also appears, and one of them is the IoT (Internet of Things). Sikur has a deep experience in cybersecurity, where IoT is currently struggling to take off once and for all. Our thoughts are not only on Secure Communication solutions but also in a foundation that makes possible shielding communication in different situations.

Before having a fully integrated secure communication system, with an Android, iOS, Windows, and a Secure Smartphone, we did foresee (and keep doing it) many other possibilities in the security realm. Trending technologies, like AI (Artificial Intelligence) and ML (Machine Learning), are the most demanding ones lately, but security is often forgotten when implementing them. In the past few years, data exchange occurs not only between humans, but between machines, and Sikur is working on it.

As the world grapples with growing consumer privacy concerns and related regulations, combined with daily, costly data breaches, cybersecurity skills are in more demand than ever. And not just at the IT level. Privacy and security are now a significant factor in the profitability and financial wellbeing of a company, as well as the larger economy. It remains clear when we see European Union **imposing fines of € 114m (£ 97.45m)** under the GDPR regulation. In the United States, the cost of a breach, on average, is the staggering US $3.86 million, up 6.4 percent from the prior year's analysis. These statistics should be of real concern. And this is just the tangible costs of a breach. This amount does not account for the costs of regulatory fines.

Other high **profile insider threats** were reported where core company intellectual property was lost from employee malfeasance. Company boards clearly should be very concerned that cyber-attacks could see the company's core assets lost with a few keystrokes. It is imperative that these boards have the depth of knowledge to ensure their companies are operating to protect their IT infrastructure with state of the art measures.

This is an unsustainable trend that must be addressed at the highest levels of business and government. Echoing this sentiment, Rep. Jim Himes of Connecticut said: "Publicly traded companies should have an obligation to let their shareholders know how they are addressing these serious threats or explain why they are not taking measures to counter attacks.

Mass surveillance by governments and corporations will become normal and expected this decade, and people will increasingly turn to new products and services to protect themselves from surveillance. The biggest consumer technology successes of this decade will be in the area of privacy.