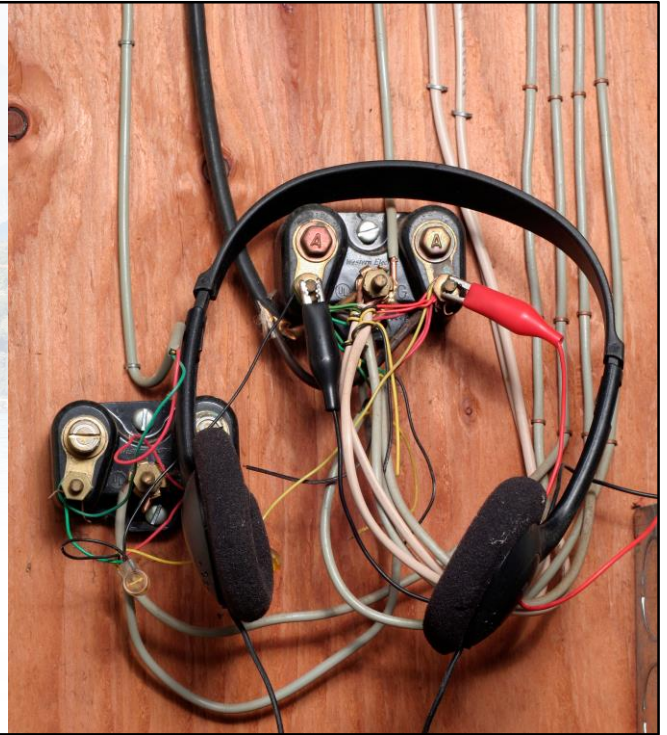


Cybersecurity & Management Challenges Symposium
Lugano - Sept. 21st 2017

ASUT Lunch Forum
Zürich - Sept. 22nd 2017

Mobile Interception

**Risks and Countermeasures
for Corporate and Government**



Tmanco SA – TOOLS TO UNLOCK ENTERPRISE MOBILITY

Strengths
Reaction time
Productivity

Weaknesses
Costs
Workload

Consulting
Costs optimization
Process automation, TEM

Opportunities
Green
Continuity

Threats
Security
Privacy

Partnerships
tangoe KUDELSKI SECURITY

Work is an activity, not a place

KUDELSKI SECURITY Tmanco mobile freedom

Intro Attack Defense White Noise ©2017 KUDELSKI GROUP All rights reserved. 2

Brief presentation of Tmanco – what we do

Tmanco provides tools to **unlock enterprise mobility**

- Mobility has **Strengths**: by enabling people to work anywhere, anytime, it can reduce the reaction time, speed-up processes and increase productivity
- Mobile also offers **Opportunities** for the future: by enabling people to work from home, you can reduce the traffic and this contributes to sustainability (green). But this also contributes to business continuity: imagine a situation of transportation strike, epidemic or terror alert where citizen can't reach the office: if this happens then companies equipped with enterprise mobility will be able to continue doing business and will get a competitive advantage over other companies.
- But mobility also has some **Weaknesses**: companies usually limit the deployment of mobiles because they are worried about increasing costs and more workload.
- And mobility also present serious **Threats** for the security and the privacy of the

communications.

- To address these Weaknesses of Costs & Workload, Tmanco provides consulting for cost optimisations and also has a partnership with Tangoe to offer a TEM solution.
- To address the Threats to Security and Privacy: Tmanco has a partnership with Kudelski Security to offer the product White Noise. This is the topic of this presentation.

Kudelski Group – 3'800 employees



Content Security Solutions	Public Access Security	Cybersecurity Solutions
 <p>More than 500 million users enjoy Kudelski Group solutions every day</p> <p>NAGRA KUDELSKI GROUP</p>	 <p>SKIDATA KUDELSKI GROUP</p>	
World Leader in Integrated Content Security Solutions	World Leader in Public Access Solutions	Switzerland's Largest Cybersecurity Company

<ul style="list-style-type: none"> • Founded in Switzerland in 1951 • HQ in Switzerland. Operating in 33 countries • 1'067M CHF Revenue • 200M CHF R&D budget 	<ul style="list-style-type: none"> • Shares majority by Kudelski family • CEO & Chairman André Kudelski, nominated Head of 'InnoSuisse' • 5'300 patents, 300 new annually
--	---



Intro

Attack

Defense

White Noise

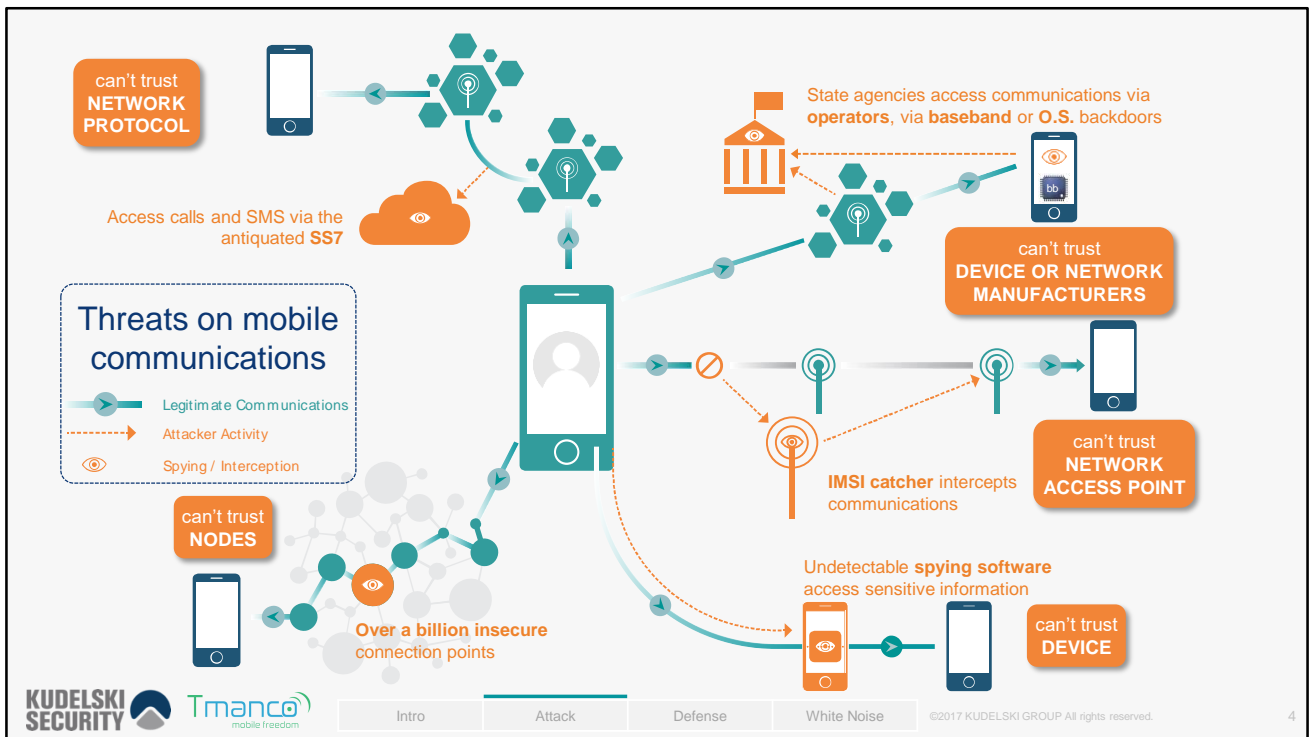
©2017 KUDELSKI GROUP All rights reserved.

3

Kudelski Group: 3'800 employees across 3 businesses

- **Content Security.** This business is focused on helping content providers in securing the delivery of digital media content. At home, many of us have cable TV and associated with that we have a set-top box we received from our cable operator. Within that set-top box is a secure element of hardware and software that prevent people from illegally re-distributing the content to other homes that did not pay the cable operator. We provide all this technology as well as the monitoring services to detect illegal activity. Today, within Kudelski we monitor over 400M devices throughout the world and we have number#1 global market share, our next closest competitor is Cisco.
- **Public Access Security.** Where we protect facilities, parking, ski resorts, and events throughout the world. In this business, think of us as the arm that goes up in the parking lot that controls who gets in or the turn style at the ski resort that let's you on the hills. Again, in this business we hold number#1 global market share
- **Cybersecurity Solutions.** This business was launched in 2012 and until recently was a business focused on the EMEA market place. Today we have operations throughout EMEA, the US, and have begun expansion into Latin America.

Bottom line, Kudeksli Group has over 25 years experience in crypto, and it is this experience that was leveraged to build the product **White Noise** and address the challenges of mobile communication privacy.



When we establish a communication between 2 mobile devices, the chain is constituted by many components and each one has vulnerabilities.

- **Can't trust NODES**: the worldwide mobile infrastructure consists of over a billion **connection points** (Wifi, GSM, 3G, 4G). We such a high number of nodes under the control of many players, we can't assume that none has been compromised.
- **Can't trust NETWORK PROTOCOL**: the **SS7** signaling protocol used in the network has known vulnerabilities which haven't been patched yet. These vulnerabilities can be used to intercept calls and sms or to perform spoofing. You can even find that as-a-service on the internet.
- **Can't trust DEVICE OR NETWORK MANUFACTURERS**: some state agencies record every single call (e.g. Echelon), they can even wake-up or shut-down phones by acting on the baseband or OS layer, and record everything.
- **Can't trust NETWORK ACCESS POINT**: an **IMSI catcher** is a fake antenna, you phone connects to it thinking it is the legitimate antenna, then all communication transit

through it and enable you to listen to phone calls, read sms, send fake sms, etc.

- **Can't trust DEVICE:** malwares can be present on the device, recording the microphone signal, reading sms or stealing other information. Malwares can be very smart and difficult to detect, installation can be as easy as opening a compromised PDF document.

NOT JUST THEORY: TOOLS ARE HERE, EASIER, CHEAPER ...

The collage consists of six screenshots arranged in a 2x3 grid. Each screenshot has a URL from 'tman.co' overlaid in the top right corner. The top row shows: 1) A 'public intelligence' website with a PDF presentation from Gamma Group. 2) The 'SMS GANG' website featuring a 'Spoof SMS Service' form. 3) The 'FLEXISPY' website advertising monitoring software. The bottom row shows: 4) A video player for 'ability' with a video titled 'While Others Talk, We Listen.' 5) A news article on 'SC' (The Cybersecurity Source) about SS7 vulnerabilities. 6) An Alibaba.com product page for an 'IMSI catcher' device.

And all this is not just theory or fiction.

By doing some research on the internet, here are some examples of services or tools you can find.

- The presentation from **Gamma Group** shows services and devices presented to a state police organisation. If you follow the link, you can access the full presentation in PDF. The picture shows a portable IMSI catcher, meaning somebody can be near you and act as a fake antenna, your phone connects to it and all your communications are intercepted.
- The website **SMS-Gang** is a free on-line Spoof SMS service. With few clicks you can send an SMS to somebody and indicate the “From” number that will appear as the person who sent the SMS.
- **FlexiSpy** is a small spying client you install on somebody’s phone in a couple of minutes. Once done, you can do things like listen into a conversation, activate the microphone, read sms, access pictures, contacts, and much more.
- **Ability**: spying as a service, just watch this short 1’30” video

- **SC Media:** the SS7 vulnerability is still active, the threat is so serious that it is getting attention at the political level
- **IMSI catcher:** buy cheap, 1'800\$ directly from Alibaba.com

AND MORE PEOPLE ARE TEMPTED TO USE THEM

Our Phones Are Being Monitored': How a Hacking Story Unfurled
By AZAM AHMED and NICOLE PERLBOTH JUNE 18, 2017

AUGUST GSM INTERCEPTOR MAP
ENO

Cyber Threats to Mobile Phones
Paul Ruggiero and Jon Foote

NSA tapped German Chancellery for decades, WikiLeaks claims

The Critical Hole at t

More tools available (easier, cheaper) + more information carried over mobile network
= more people are tempted to use those tools.

Here are few examples of situations

- **The New York Times:** a state intercepting the communication of a lawyer who represents the families of the students who disappeared in 2014 in Mexico
- **Popular Science:** a map showing the GSM interceptors identified. This was in 2014, we can reasonably guess that it would look much worse today.
- **The Guardian:** and this well known case of Angela Merkel being intercepted by the NSA.
- **US-CERT:** already in 2011 a report warned about the increasing risk for mobile and the attractiveness for hackers. Recent reports confirm these risks, the situation doesn't seem to be much better today.

- **WIRED:** quite embarrassing when a reserved conversation is intercepted and put on youtube. For a business, it means the risk is not only to be intercepted by a competitor who is interested in the strategy / future products / trade secrets, but the risk can also be to have a critical position exposed to the public and affecting the image of the company (with the subsequent impact on the stock value).

Of course we know all this is happening, but are we really aware how easy it can be and therefore how more probable it can be ? Especially if our business can be of interest for some state agency, competitor or criminal organization !

BUT MOST BUSINESS ARE TOTALLY UNPREPARED ...



Security professionals identified the risk of mobile devices, but focus and resources assignment **seem to be waiting for actual catastrophes** to validate the need to properly prepare their defenses

20% experienced mobile breach

24% don't know or can't tell

94% expect frequency to grow

64% doubt can prevent breach

Research report from Dimensional Research
sponsored by Check Point

tman.co/mi-ckp1704

FOR THESE MOBILE ATTACKS

- Communications

- Listen to all Voice calls made or received
- Read all SMS made or received
- Spoof identity to falsely send SMS or Voice calls
- Divert Calls/SMS so they are not received
- Edit all SMS before they are received

- Device

- Access all infos in device (geo-location, mail, contacts, phone-log, pictures, etc.)
- Intercept microphone signal and listen to phone-call despite using encrypted app

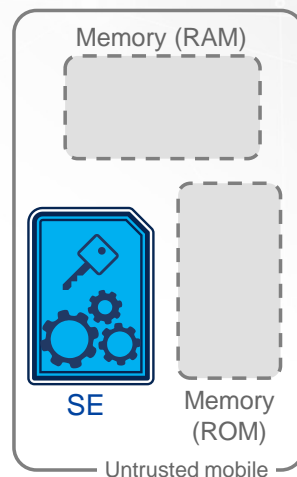
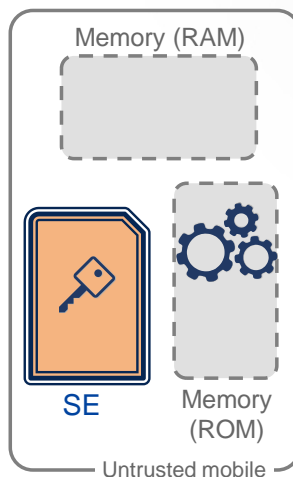
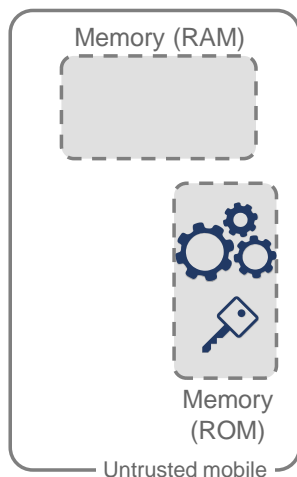
Despite all that, a survey from Dimensional Research reveals that most businesses are totally unprepared. It seems like companies are waiting for the catastrophes to happen.

ENCRYPTION IS THE SOLUTION, BUT WHICH ONE ?

Software only

Hardware + Software

Full hardware



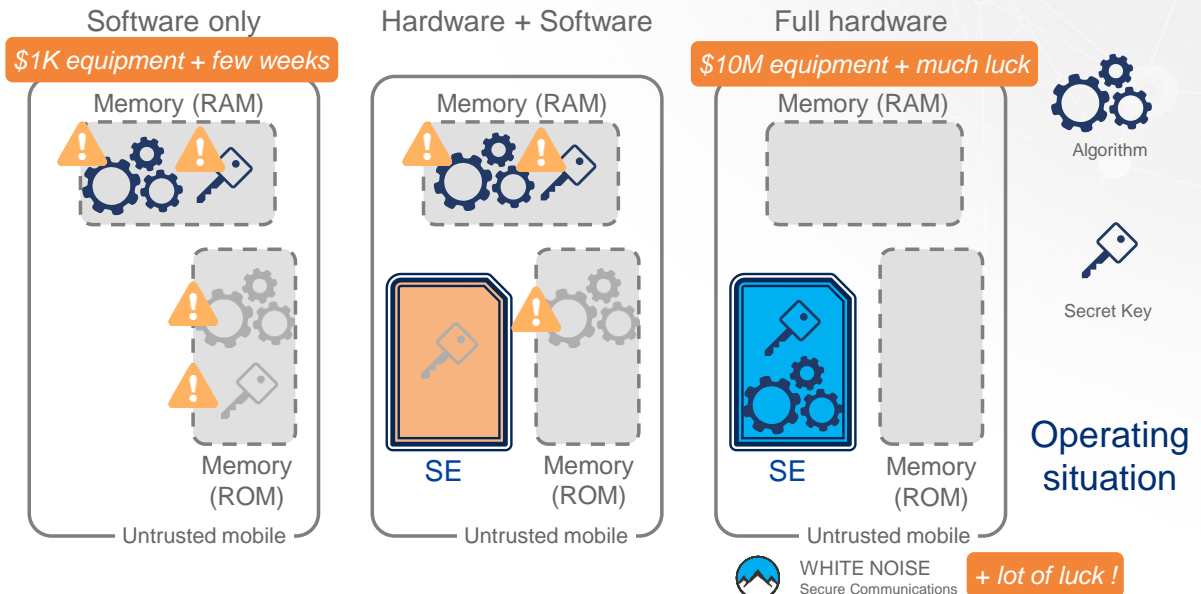
Stand-by situation

How can we protect against all these vulnerabilities ? Encryption is the way to go but which kind of encryption ?

Let's look at the difference between Software & Hardware encryption.

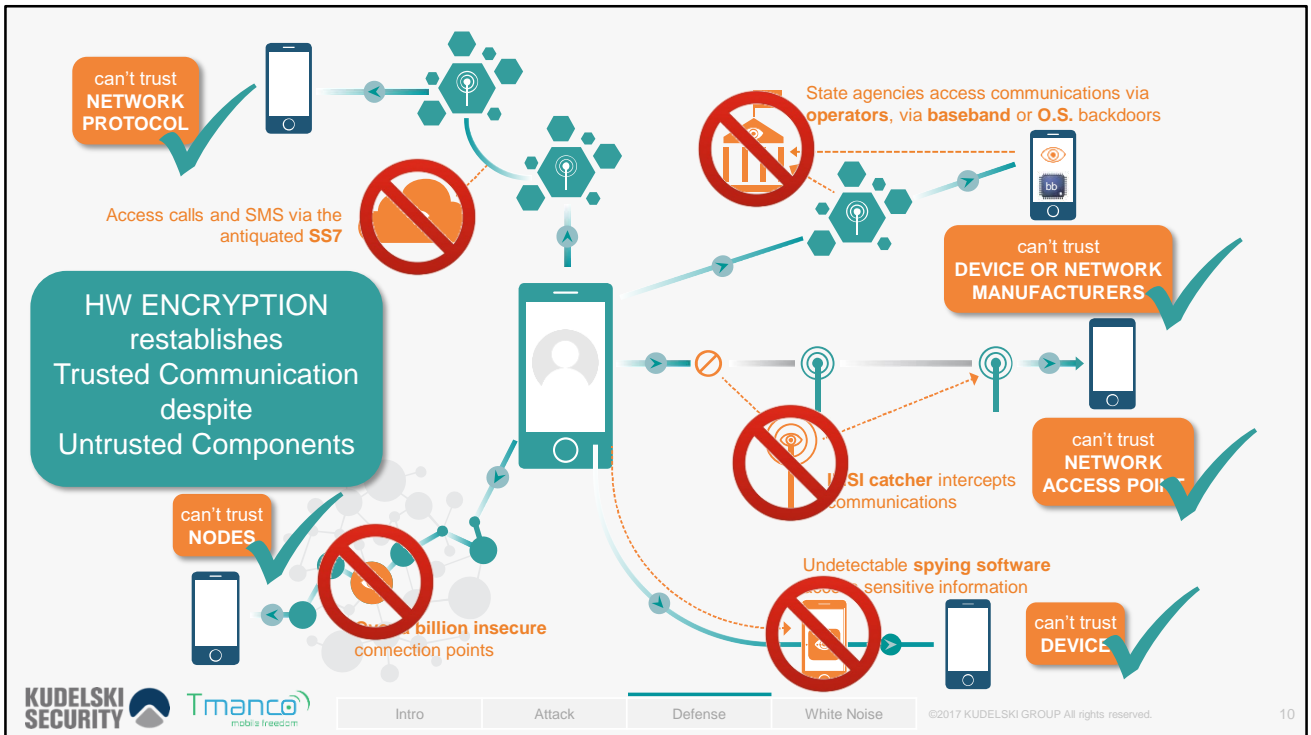
- In a **Software only** solutions: security keys and crypto algorithms are stored in ROM and then loaded into RAM at run time. But because RAM is shared area, accessible by other applications, therefore the key and the algorithm are exposed to malware.
- In a mixed **Hardware + Software** solution, the key is stored in a Hardware secure element and the algorithm is stored in ROM. This is safer than the Software only solution, however the problem occurs at run time because both the key and the algorithm are then loaded into RAM and become exposed to malware.
- In a **Full Hardware** solution, both the key and the algorithm are stored in a Hardware secure element and are never loaded into RAM. The encryption happens in the hardware where no other application or malware is allowed to run. This is the safest mechanism.

HARWARE IS THE WAY TO GO !



The level of security can be measured by the amount of resources it would require to decipher the mechanism.

- To decipher a **Software only** solution, some basic equipment and few weeks could be enough.
- To decipher a **Full Hardware** solution requires a large amount of resources with complex and expensive equipment. Even so, it is not sure you can manage to decipher the mechanism and you may need some luck.
- **White Noise** uses a sophisticated Full Hardware encryption (4 layers, 768 bits) providing a high level of security. Even with sophisticated expensive equipment and with lot of time, it is highly improbable you could manage to decipher the mechanism, unless you have lot of luck as well.






By using **White Noise with Hardware Encryption**, the many vulnerabilities of the network don't matter anymore because even if the communication was intercepted, it would be meaningless to a third party.

We have now restored privacy, with a trusted communication channel despite the fact that we are using a network and a device that can't be trusted.



WHITE NOISE IN A NUTSHELL

100% SWISS  SOLUTION

Base components

- App 
- Security chip 
- Android: chip in MicroSD slot 
- iPhone: chip in special cover
- Desktop: chip in USB

Accessories

- Bluetooth headset with built-in security chip 
- Silent box to isolate microphone 
Protects against spyware

Rich feature set

- Voice
- IM (one2one, group-chat, pictures)
- Closed user group, cross-organisation

Highly secure

- HW in-chip encryption, 4 layers, 768 bits
- Security level up to classified
- Customer sovereignty, no backdoor
- 25 years crypto expertise

For off-the-shelf devices

- Supports iOS, Android, PC

At reasonable cost

- Security for all (not just VIP)

KUDELSKI
SECURITY



Tmanco
mobile freedom

Intro

Attack

Defense

White Noise

©2017 KUDELSKI GROUP All rights reserved.

11

White Noise is a multi-platform solution for unified communication (voice + messaging).

The **base components** consist of:

- An **app**, available for Android, iOS, Windows desktop
- A **security chip** that can be either inserted in the MicroSD slot, or in a special cover (for iPhone) or in a USB slot for desktop.

Some **accessories** provide extra features

- In partnership with Sennheiser, we provide a **Bluetooth headset** which has the security chip built-in. Therefore it can be used in combination with any mobile (Android, iPhone) or desktop without needing extra hardware or special cover.
- To make 100% sure the communication can't be intercepted, even in the case the phone would have a spyware intercepting the microphone signal, we also have a **silent box**. The phone is locked in the box with high acoustic isolation, it receives only the encrypted signal from the Bluetooth headset.

The **rich feature set** provides

- Encrypted **voice** calls

- Encrypted **instant messaging** with one-to-one or group chat and the possibility to exchange documents or pictures
- The ability to define **closed user groups** where people can only see and communicate within the group.

This solution is **highly secure**

- The **very strong encryption** is suitable for classified communications
- The key generation is performed by the customer, Kudelski does not possess the key. If a judge would request the keys in order to intercept a communication, it is only the **customer is sovereign** and is the only one who could provide them. There is no backdoor that could be used either by Kudelski or by a state agency.

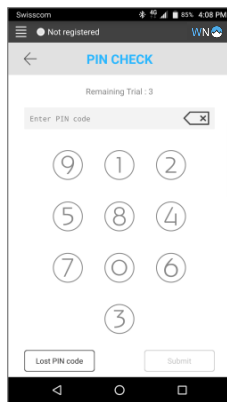
Designed for **off-the-shelf devices**

- Since White Noise works with standard devices (Android, iPhone) it has a better acceptance from the users who can use their preferred phone and don't need to carry a second bulky secure phone.

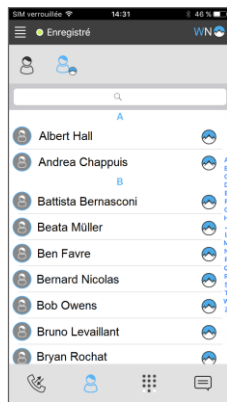
At **reasonable cost**

- This means security for the mass and not just for the VIP. Because, as we know, a hacker would probably not target the highly secured top manager but may manage to obtain the desired information by targeting people like the assistant, the developer, the marketing, etc.

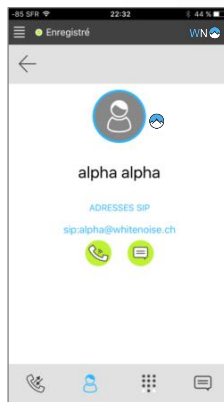
MOBILE APP – USER INTERFACE



PIN code screen
Keypad is **scrambled**
for security



WHITE NOISE
dedicated contact list



WHITE NOISE secure calls
management



These screenshots show how the application looks like on a mobile phone.

- Launching the application requires a pin code.
- Once launched, the application shows the directory of all people reachable (can be limited with the closed user group feature).
- A presence status shows if the person is available for call and/or chat
- When two devices establish a call, they negotiate a one-time security key

USE CASES – SECURED UNIFIED COMMUNICATION

CALL
using iPhone
with Secure-chip in cover



INSTANT MESSAGING
using Android phone
with Secure-chip in MicroSD slot



PRIVACY IN BOARDROOM
all phones in a silent-box



CLASSIFIED CALL
using Smartphone in silent-box
with Secure Headset



CALL
using Smartphone
with Secure Headset



CALL
using Desktop
with Secure-chip in USB slot



Intro

Attack

Defense

White Noise

©2017 KUDELSKI GROUP All rights reserved.

13

White Noise has been designed for unified communication with the capacity to handle a variety of situations.

- CALL
- INSTAND MESSAGING
- PRIVACY IN BOARDROOM
- CLASSIFIED CALL
- CALL WITH HEADSET
- CALL WITH DESKTOP

WHITE NOISE: FINALIST FOR SWISS ICT AWARD 2017



SWISS ICT AWARD
14. NOVEMBER 2017
KULTUR- UND KONGRESSZENTRUM LUZERN

www.swissict-award.ch



Kudelski Group mit White Noise



Darum sollten Sie uns wählen:

In einer Zeit, in der Hacking-Angriffe noch nie gesehene Ausmasse erreichen, brauchen Regierungen und Unternehmen neue Wege, um sicherzustellen, dass ihre Kommunikation nicht abgefangen wird. White Noise ist eine einfach zu bedienende, sichere Kommunikationslösung, die einen bahnbrechenden Sicherheitsgrad bietet.

Jean-Michel Puigati, Senior Vice President, Kudelski Group - IOT Security

Das Unternehmen aus der Kudelski-Gruppe hat mit «White Noise» eine sichere Kommunikationslösung auf den Markt gebracht, welche massgeschneiderte Hardwareverschlüsselung für Anrufe und Textnachrichten verspricht. Die Lösung funktioniert dabei plattformübergreifend und soll Kunden die vollständige Kontrolle über die Sicherheit ihrer Geräte auf iPhone, Android oder PC garantieren. Entwickelt und gehostet in der Schweiz, sollen damit alle Sicherheits Herausforderungen gemeistert werden.



Nominierungen

- Artanim
- Eyeware Tech
- Imito
- Kudelski Group**
- Nomos System

Nominierungen Newcomer

- Advertima
- Bexio
- Crowdhouse
- Recapp
- Swisscognitive

SWISS ICT PUBLIC AWARD: START OF THE VOTING

Who wins the Swiss ICT Public Award 2017? Now it's your turn. Give your vote at the Swiss IT Magazine readers voting.

tman.co/ictaward-vote



Intro Attack Defense **White Noise** ©2017 KUDELSKI GROUP All rights reserved. 14

White Noise is a very innovative product and has been selected as finalist for the Swiss ICT Award 2017.

Thank You

Toni LAZAZZERA

Partner, Tmanco SA
toni.lazazzera@tmanco.ch

Bernard BENOIT

White Noise General Manager, Kudelski Security
bernard.benoit@nagra.com

Alain HENRIETTE

Product Line Manager, Kudelski Security
alain.henriette@nagra.com

