upsell>

up APP

available for:

android iOS

Secure Mobile Voice and Messaging System

Mobile Communication

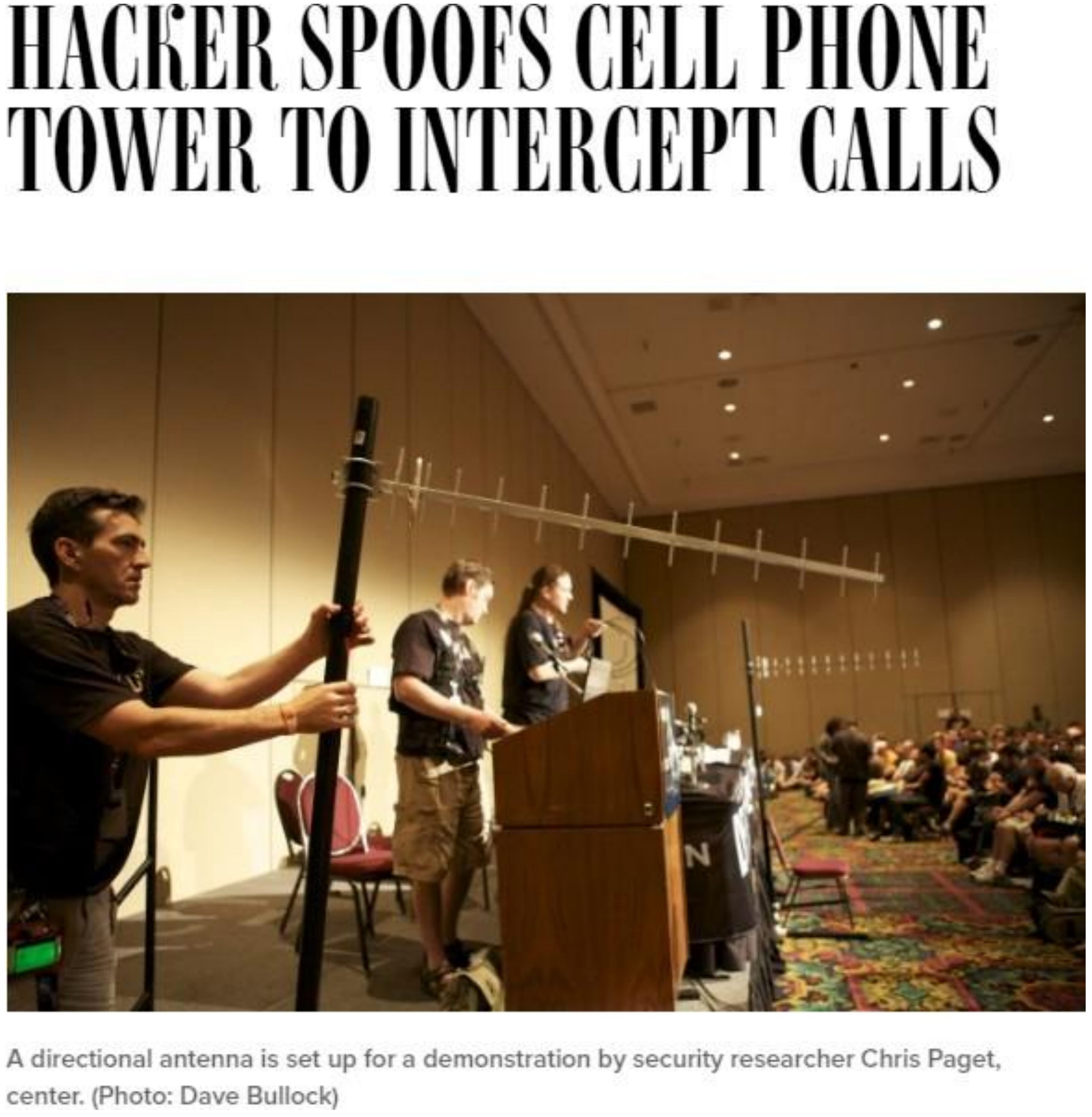
Challenges

MOBILE COMMUNICATION

Vulnerabilities

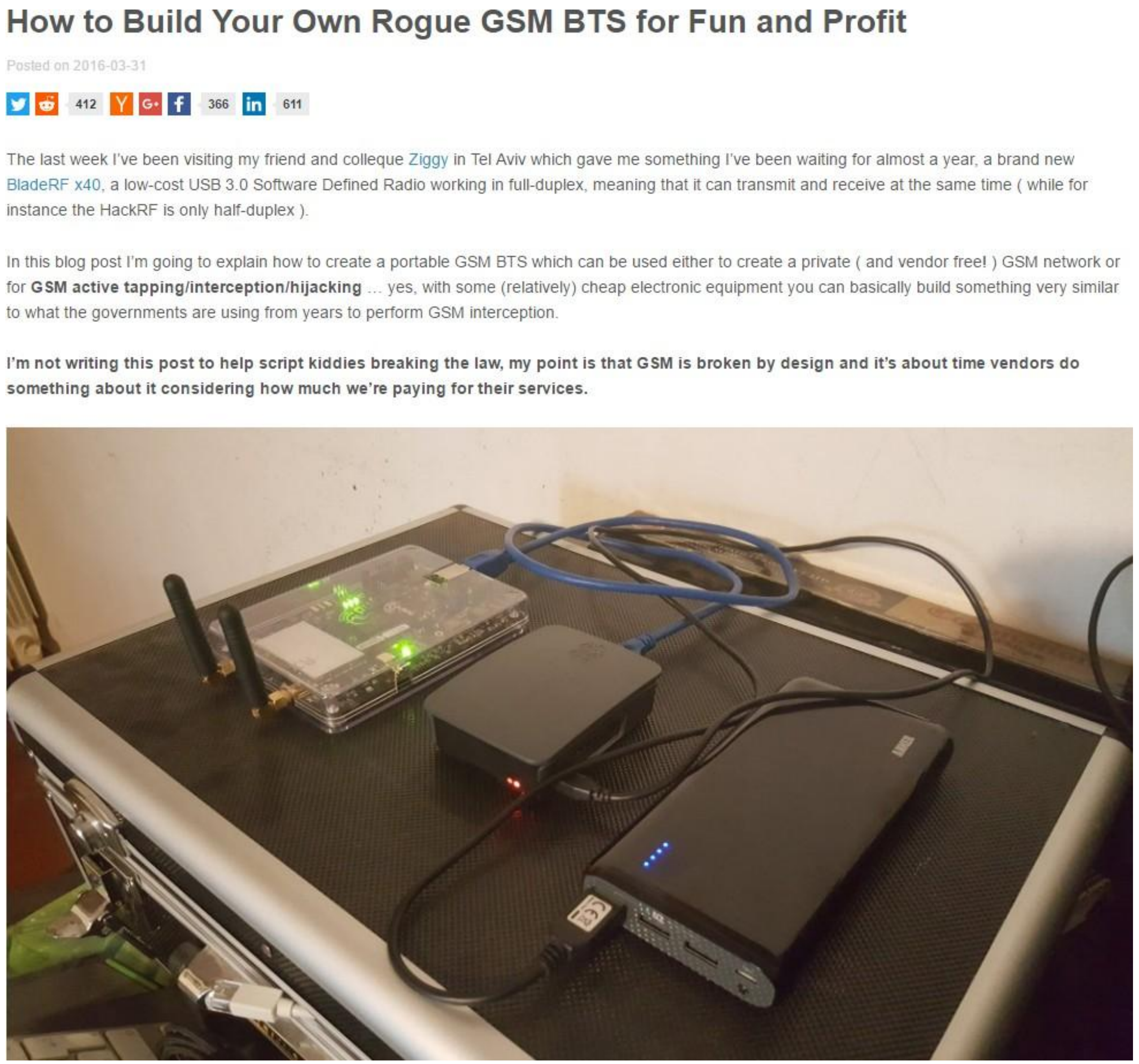
“ … your data isn’t just available to nation states: it’ s also potentially available to that goofball neighbor who bought an IMSI-catcher off the Internet. Or to your business competitor. Or even to that one girl who finally got GnuRadio to compile.”

Matthew Green, On Cellular Encryption, blog.cryptographyengineering.com



HACKER SPOOFS CELL PHONE TOWER TO INTERCEPT CALLS

A directional antenna is set up for a demonstration by security researcher Chris Paget, center. (Photo: Dave Bullock)



How to Build Your Own Rogue GSM BTS for Fun and Profit

Posted on 2016-03-31

The last week I’ve been visiting my friend and colleque Ziggy in Tel Aviv which gave me something I’ve been waiting for almost a year, a brand new BladeRF x40, a low-cost USB 3.0 Software Defined Radio working in full-duplex, meaning that it can transmit and receive at the same time (while for instance the HackRF is only half-duplex).

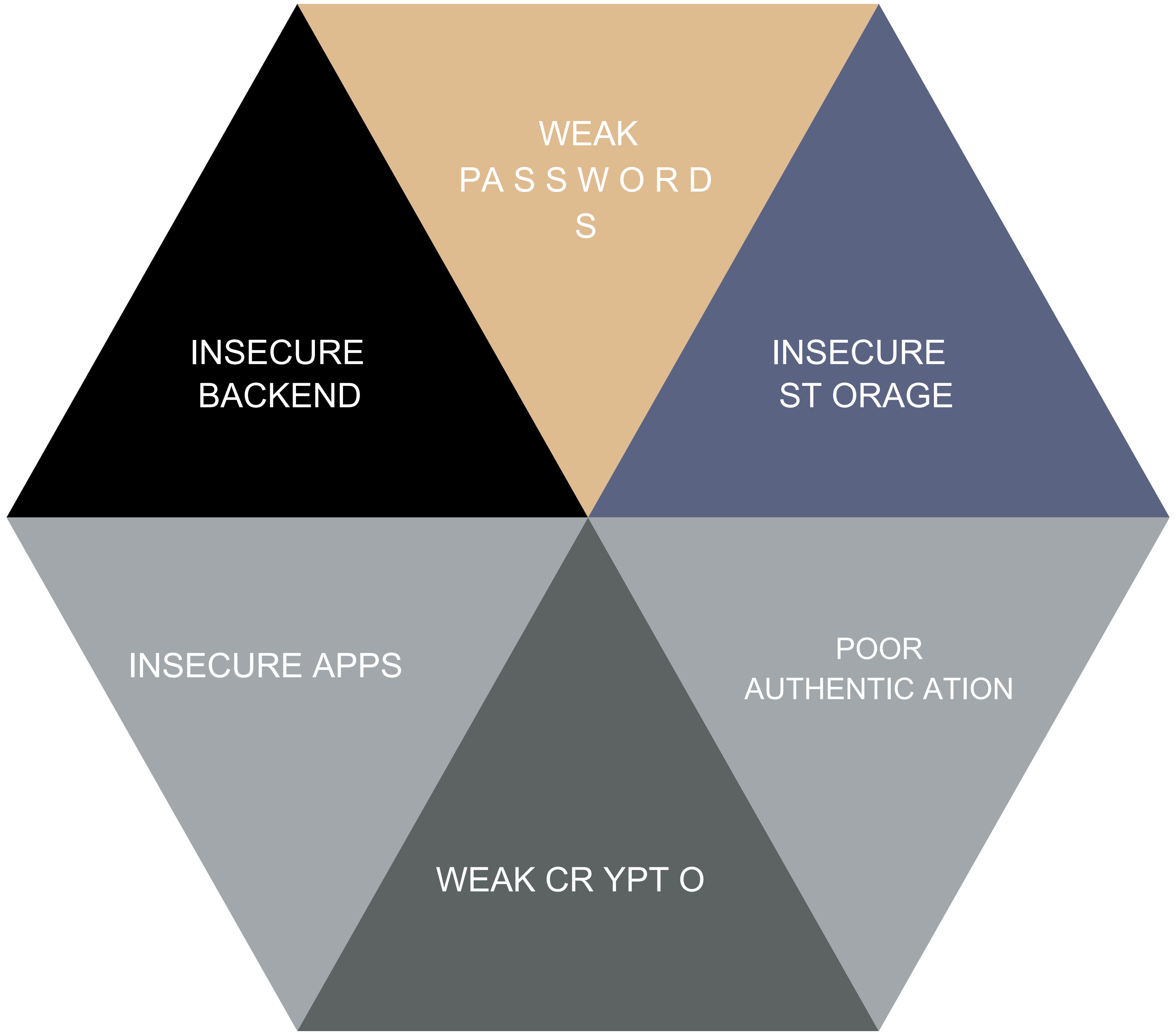
In this blog post I’m going to explain how to create a portable GSM BTS which can be used either to create a private (and vendor free!) GSM network or for **GSM active tapping/interception/hijacking** … yes, with some (relatively) cheap electronic equipment you can basically build something very similar to what the governments are using from years to perform GSM interception.

I’m not writing this post to help script kiddies breaking the law, my point is that GSM is broken by design and it’s about time vendors do something about it considering how much we’re paying for their services.

MOBILE COMMUNICATION

More Vulnerabilities

It is not only about the communication security …



WEAK PASSWORDS

Standard third party apps do not employ additional password protection and let user access to sensitive data via potentially weak passwords.

INSECURE ST ORAGE

Securing data at rest on the mobile application is seldom utilized and hence allows attackers to have access to data easily once the mobile device is compromised

POOR AUTHENTIC ATION

Usually in mobile communications mutual authentication is missing and opens up doors for serious vulnerabilities.

WEAK CR YPT O

Intentional or unintentional use of weak cryptographic primitives stays at the heart of the well-known attack methods in mobile communications.

INSECURE APPS

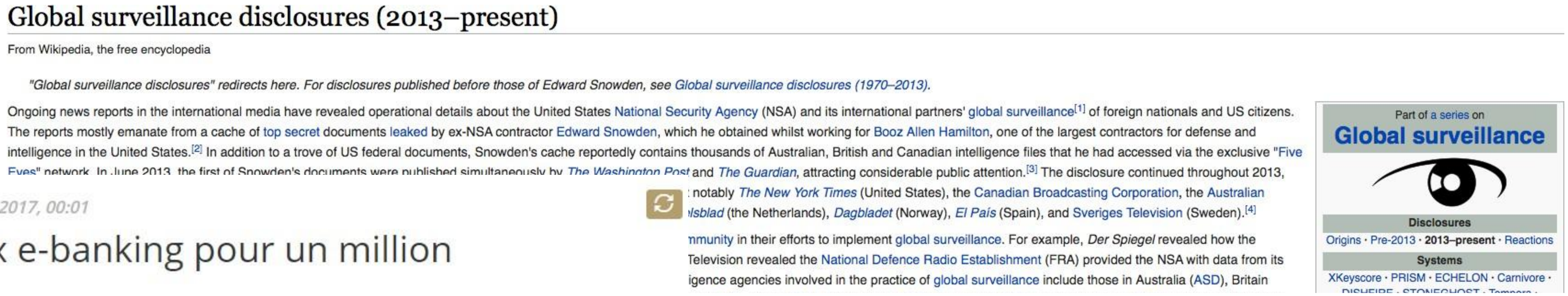
Insecurely developed apps cause major threats against information leakage and data compromise.

INSECURE BACKEND

Allowing clear sensitive data, either real or metadata, in the backend components, has been one of the major reasons for data leakage in the recent attacks.

Threats

It is not only the intelligence agencies; anyone who can benefit from the existing vulnerabiliities is a threat.



Global surveillance disclosures (2013–present)

From Wikipedia, the free encyclopedia

"Global surveillance disclosures" redirects here. For disclosures published before those of Edward Snowden, see Global surveillance disclosures (1970–2013).

Ongoing news reports in the international media have revealed operational details about the United States National Security Agency (NSA) and its international partners' global surveillance[1] of foreign nationals and US citizens. The reports mostly emanate from a cache of top secret documents leaked by ex-NSA contractor Edward Snowden, which he obtained whilst working for Booz Allen Hamilton, one of the largest contractors for defense and intelligence in the United States.[2] In addition to a trove of US federal documents, Snowden's cache reportedly contains thousands of Australian, British and Canadian intelligence files that he had accessed via the exclusive "Five Eyes" network. In June 2013, the first of Snowden's documents were published simultaneously by *The Washington Post* and *The Guardian*, attracting considerable public attention.[3] The disclosure continued throughout 2013,

: notably *The New York Times* (United States), the Canadian Broadcasting Corporation, the Australian
lsblad (the Netherlands), *Dagbladet* (Norway), *El País* (Spain), and Sveriges Television (Sweden).[4]

nmunity in their efforts to implement global surveillance. For example, *Der Spiegel* revealed how the
Television revealed the National Defence Radio Establishment (FRA) provided the NSA with data from its
igence agencies involved in the practice of global surveillance include those in Australia (ASD), Britain

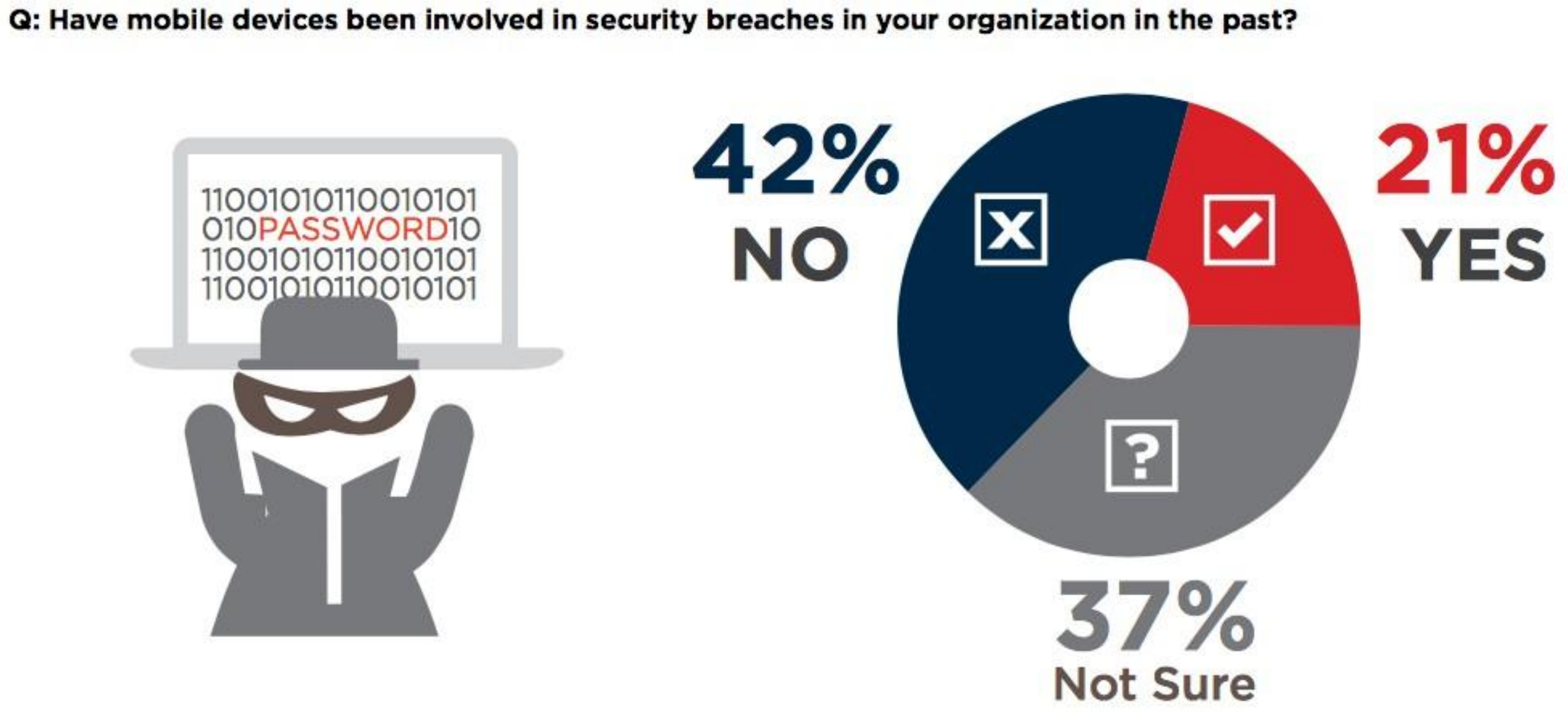
Part of a series on
Global surveillance

Disclosures
Origins · Pre-2013 · **2013–present** · Reactions

Systems
XKeyscore · PRISM · ECHELON · Carnivore ·

11.02.2017, 00:01

Faux e-banking pour un million



Q: Have mobile devices been involved in security breaches in your organization in the past?

Trends

More and more sensitive world related information is exchanged through mobile devices

Q: What are the main drivers and benefits of BYOD for your company?

- 61% Improved employee mobility
- 56% Greater employee satisfaction
- 55% Increased employee productivity
- 47% Reduced cost
- 21% Reduced security risk
- 16% Employee privacy
- 5% Other

Q: What stage of BYOD adoption has been reached by your company?

40%
BYOD is available to all employees

32%
BYOD is available to select employees

13%
We have no plans to support BYOD

9%
We do not support BYOD, but plan to start in the next 12 months

3%
BYOD was tried but abandoned

3%
Other

Responses do not add up to 100% because survey participants selected multiple choices.

Risk Analysis

VULNERABILITIES

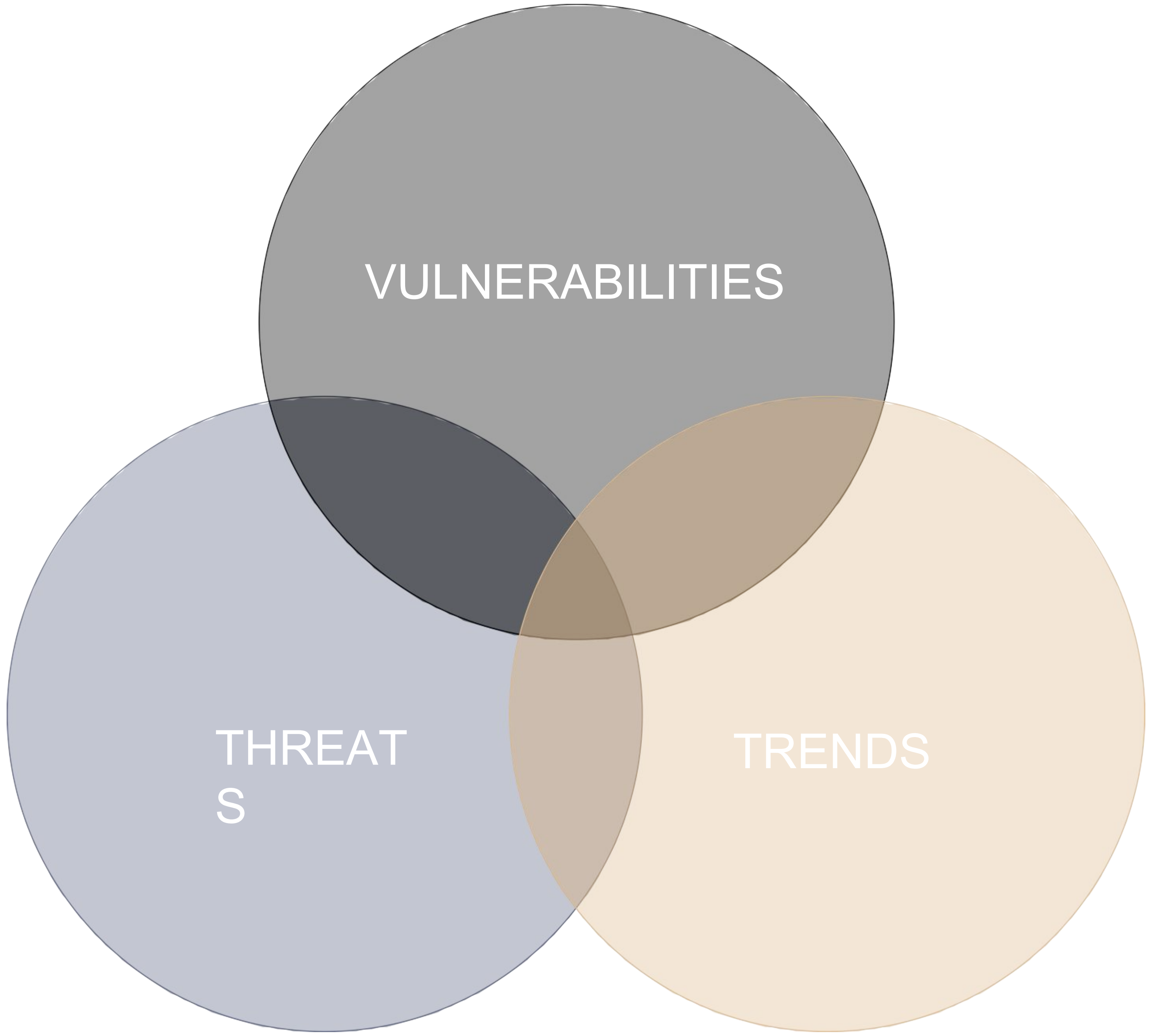
Standard mobile communication systems are inherently insecure and there are very well-known vulnerabilities.

THRE ATS

There are various well-established threats who have already made and can still make use of the existing mobile vulnerabilities.

TRENDS

Considering the effectiveness of the use of mobile devices at work, more and more sensitive information will be exchanged through mobile devices.

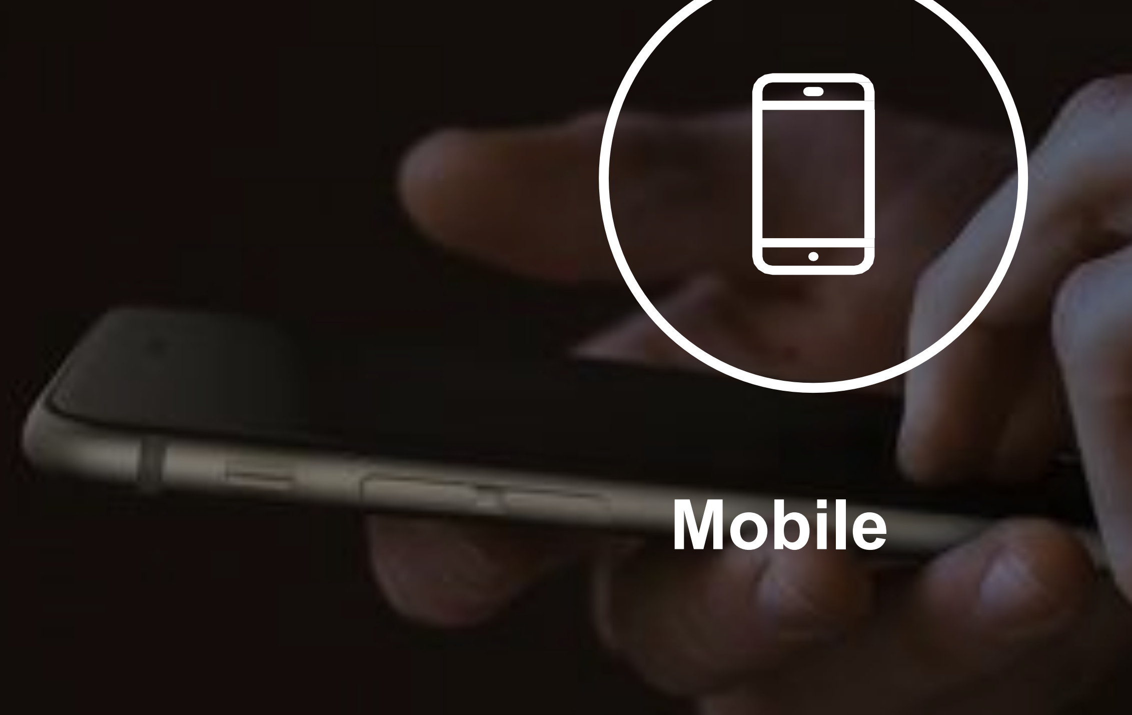


! The risk of exposing sensitive organizational information is high!

Our Product

OUR PRODUCT

Secure mobile communication in closed circles



Secure

Carefully designed to allow for secure communication among closed circles using state-of-the-art cryptographic methods.

Mobile

Aims to provide a secure solution for mobile communications. Available on the most widely used mobile OS: iOS & Android.

Communication

Provides user-friendly solutions for the most widely used mobile communication methods for organizations: voice, messaging and file sharing.

OUR PRODUCT

Major Features

Central Management

Central and web-based user, group and system management.

Secure Contacts

Secure, trusted and closed circle of contacts generated and managed centrally.

Secure Call

Secure one-to-one, conference and external calls (via PBX integration).

Secure Messaging & File Sharing

Secure instant messaging, file sharing and SMS within your contacts.

Mobile App

Extensive Feature Set

VOICE

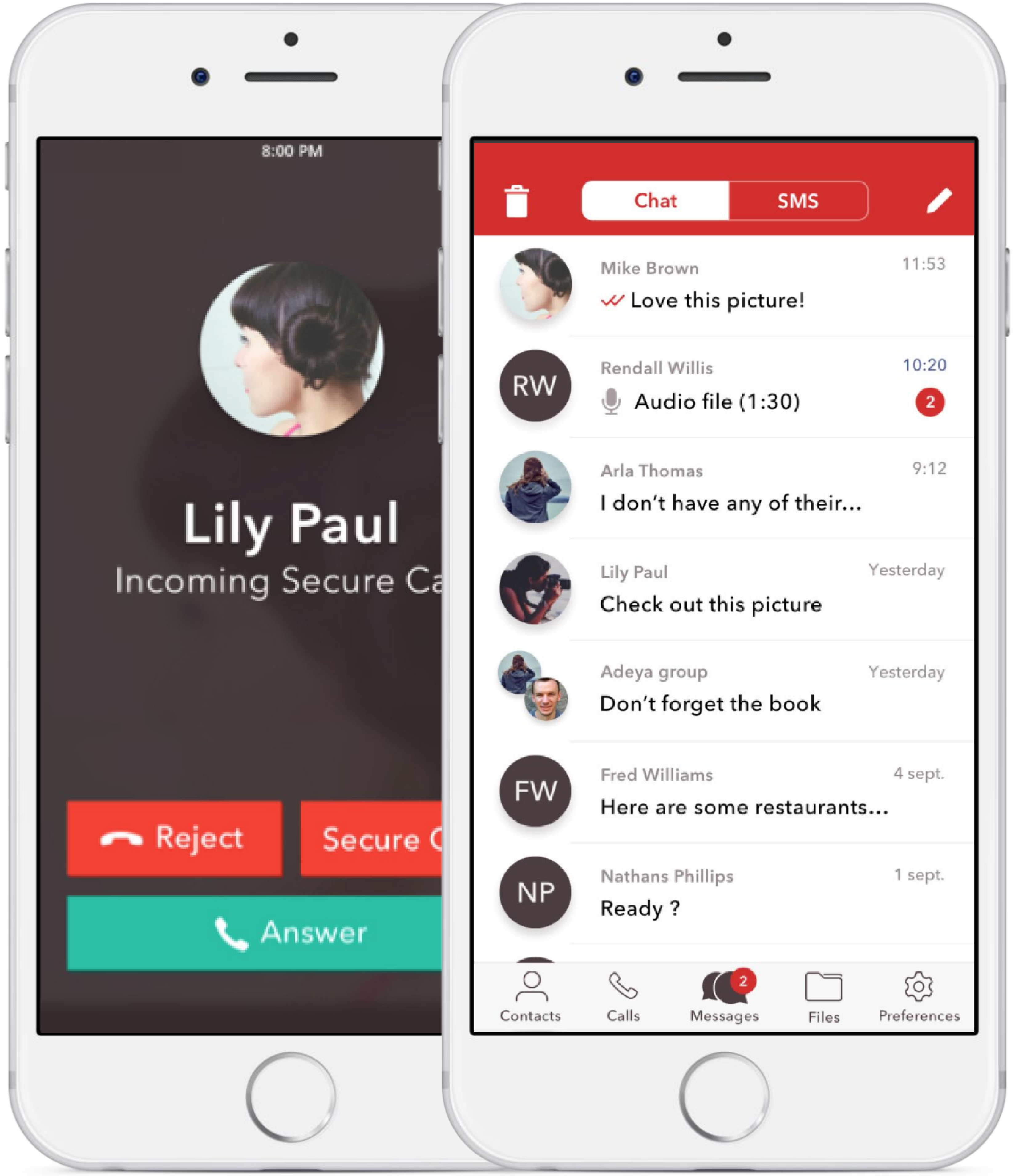
One-to-one call
Conference call
External call
Voice mail

SYSTEM

Password protection
Secure storage
Presence
History Screen lock

MESSAGING

Text Messaging Image sharing Video file sharing
PDF document sharing MS File Sharing* Audio file sharing
Geo-location sharing
Message broadcast
Message forward Group chat
Message auto-destruction
Message take-back
Secure SMS SMS
Notification
Message delivery/read status



Mike Brown 11:53
Love this picture!

RW Rendall Willis 10:20
Audio file (1:30) 2

Arla Thomas 9:12
I don't have any of their...

Lily Paul Yesterday
Check out this picture

Adeya group Yesterday
Don't forget the book

FW Fred Williams 4 sept.
Here are some restaurants...

NP Nathans Phillips 1 sept.
Ready ?

* Road map

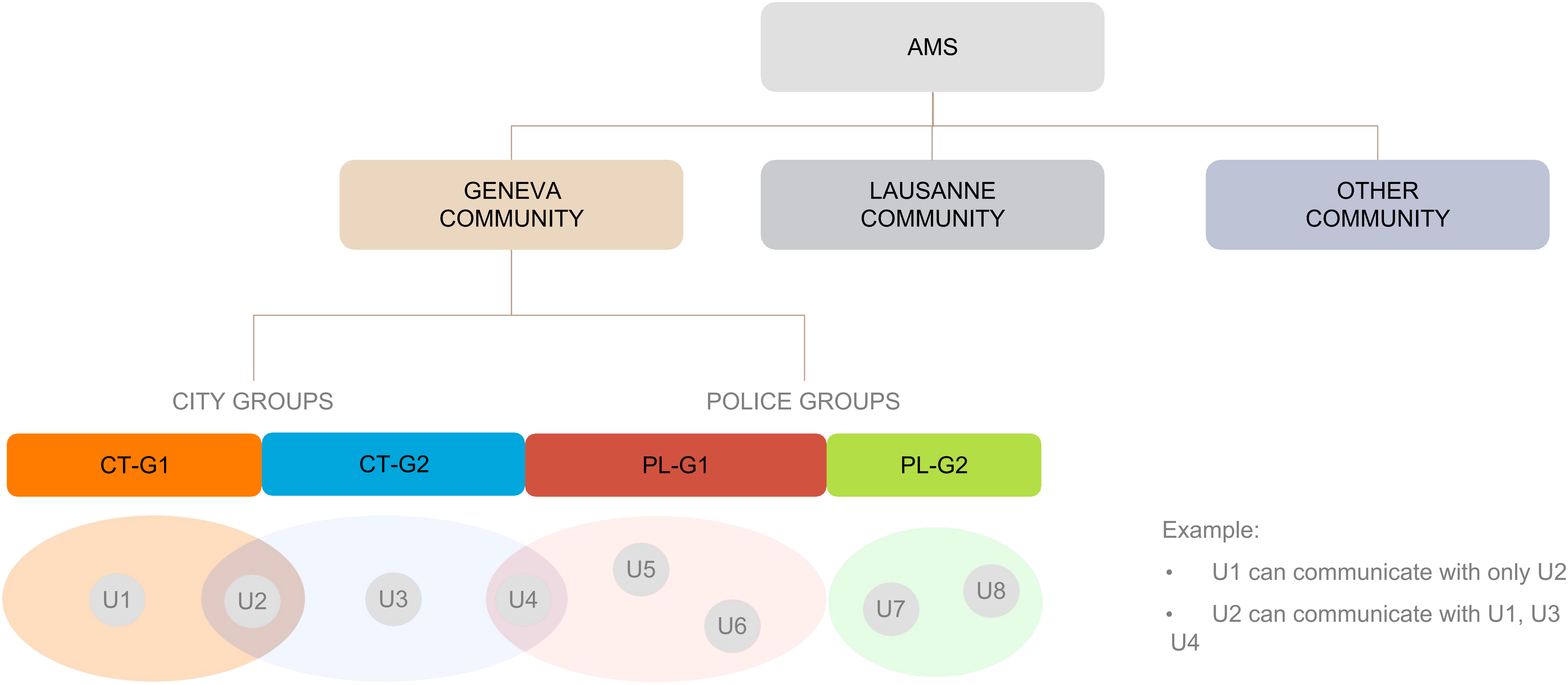
MANAGEMENT SYSTEM

CLOSED COMMUNITY CONCEPT

A closed community is a set of predefined users distributed over a set of communication groups.

Each community has a dedicated manager. A community can be deployed on a single gate or a cluster of distributed gates.

Each community has it own settings: store, App branding, set of communication features, etc.



Example:

- U1 can communicate with only U2
- U2 can communicate with U1, U3 and U4

ADVANCED TECHNOLOGY FOR SECURITY AND PRIVACY

Deployment Types

Our product is flexible enough to be deployed in two ways: either in a private cloud to allow for more restricted on premise installations or in a public cloud in a simpler and more cost effective way

On-Premise

Allows for dedicated on-premise deployments.

Target Market

Government & Defense, ICT Service Providers

Public Cloud

Allows for efficient deployment on a highly-secure Swiss based datacenter.

Target Market

Enterprises, SMBs

Key Product Features

USPs

SECURE

E2E encryption in closed circles with maximum control, while providing the highest degree of usability.

SWISS

High privacy standards and high quality software; Swiss-based public cloud version ensured by strict Swiss laws for data protection.

FLEXIBLE

Numerous installation and customization options allowing organizations to easily comply with specific requirements.

Market Segments

Target Market Segments

GOVERNMENT

- Parliament Presidency
- Ministry of Interior
- Ministry of Foreign Affairs
- Civil Police
- State & Cantonal Departments

DEFENSE

- Ministry of Defense
- Army
- National Guards
- Intelligence Services
- Military Police

FINANCIAL SERVICES

- Banking
- Insurance
- Tax & Audit

HEALTHCARE

- Ministry of Health
- Hospitals
- Clinics
- Pharmacies

OTHER

- Oil & Gas
- R&D
- Start-ups
- Law Firms
- Family Offices

upsell®

Poststrasse 24, 6300 ZUG, CH

☎

+43 676 88 72 76 66

@

office@upsell.ch