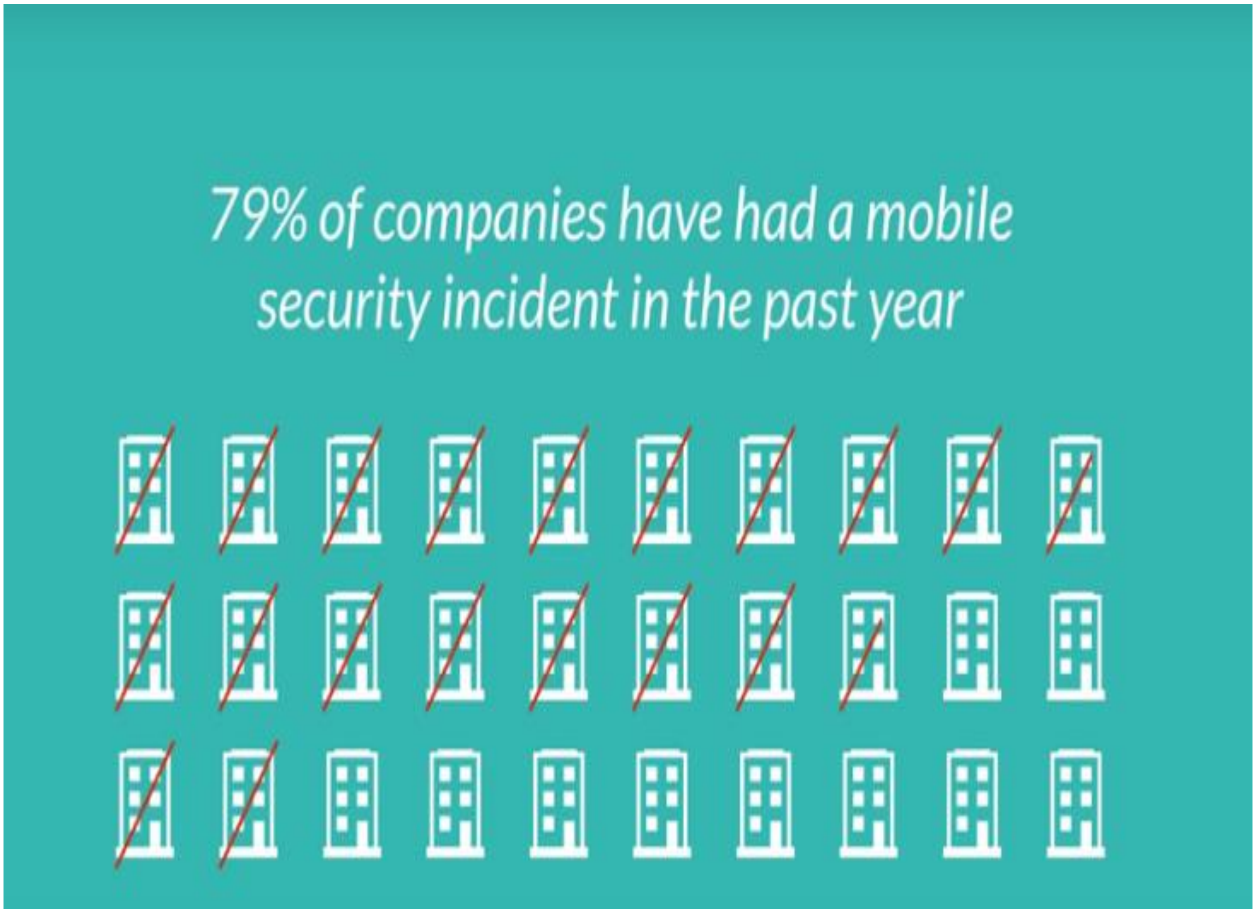
The Basics of Mobile Communications Security GovWare Symposium Singapore,8 October 2015. By Dr. B. Bowitz – Securescrypt Neoi Pte. Ltd. Singapore/Germany

Ladies, Gentlemen.

Building a secure nation. Confidentiality ,Data Connection, Availability, Applications, Data Analytics , Non Repudiation , Integrity and Connectivity. Big words, falling short of the most important part – Mobile Security. To say it loud and clear the Nation has NO mobile security or as it is called Cyber Security. Nobody even thought about Mobile Security, the FRONT end. What is the use of investing millions into a safe back end infrastructure, if the INPUT device, the front end, the Mobile device is an open book?

Alone in 2014 79% of companies had a mobile security incident. Considered we have about 2 billion mobile phones worldwide, 1,58 Billion Mobile Phones have been compromised, hacked, copied or mis-used not only by hackers and criminals, but also by enterprises, commercial organizations and governments.



We are no doubt a Mobile Community. Our Mobile phones carry our utmost secrets, personal, business and Government. Secret Documents, Pictures, Information are stored on Millions of Mobile devices, carried around in the world, without any kind of protection.

While many IT experts explain to users that the transmission of documents are secured with encryption, they do not tell that once the documents are stored on a mobile device they are NOT encrypted, because mobile phones have no such facility, have no user authorization, have no real user identification. Once they come to the screen everybody can read them. You loose the device, it is very easy for a culprit to open any file in the device and copy it. But that is not the worst case, even with a gun to his head, a user will happily let a culprit have access. So called Pin protected devices protect the screen, but not the information.

As I mentioned this is not the worst case scenario, we have another big problem, the problem is called GSM.

My lecture might sound tough and very critical, but we have to be straight forward and open, otherwise we will end up in a data sunami.

We all need SECURE Communications

Enterprises

Military - Police

Financial - Banking

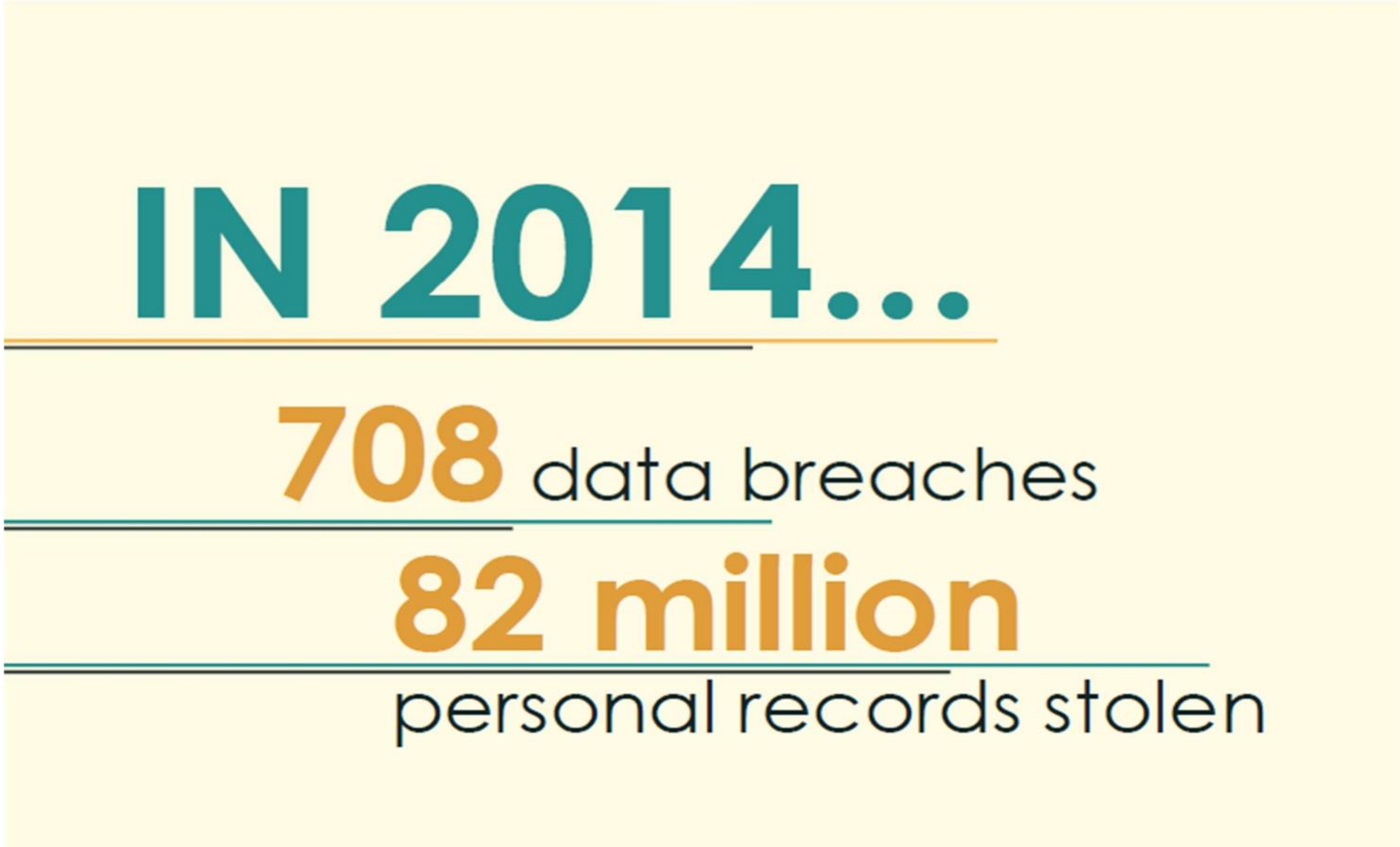
Personal - Consumer

There are a large number of private Security Companies that have profitable contracts with enterprises and governments. These companies are not exactly interested to quickly act on Cyber Security breaches, as this would cut into their profits.

In a fast changing IT environment however, fast and professional reaction to Cyber Security breaches is mandatory to protect us all.

Again the real risk that has never been taken serious is the wireless access to a mobile device thru the GSM part. Network operators have no interest in exploiting that risks, they would have to invest billions of dollars to change the old Network Infrastructure dating back to the let 1970's.

Efforts by a very few smaller companies have been started to secure the mobile devices. I mean secure the 1 Billion + mobiles that are out there and retrofit them with latest state of the art security. It can be done independent of network operators and large interest groups.



IN 2014...

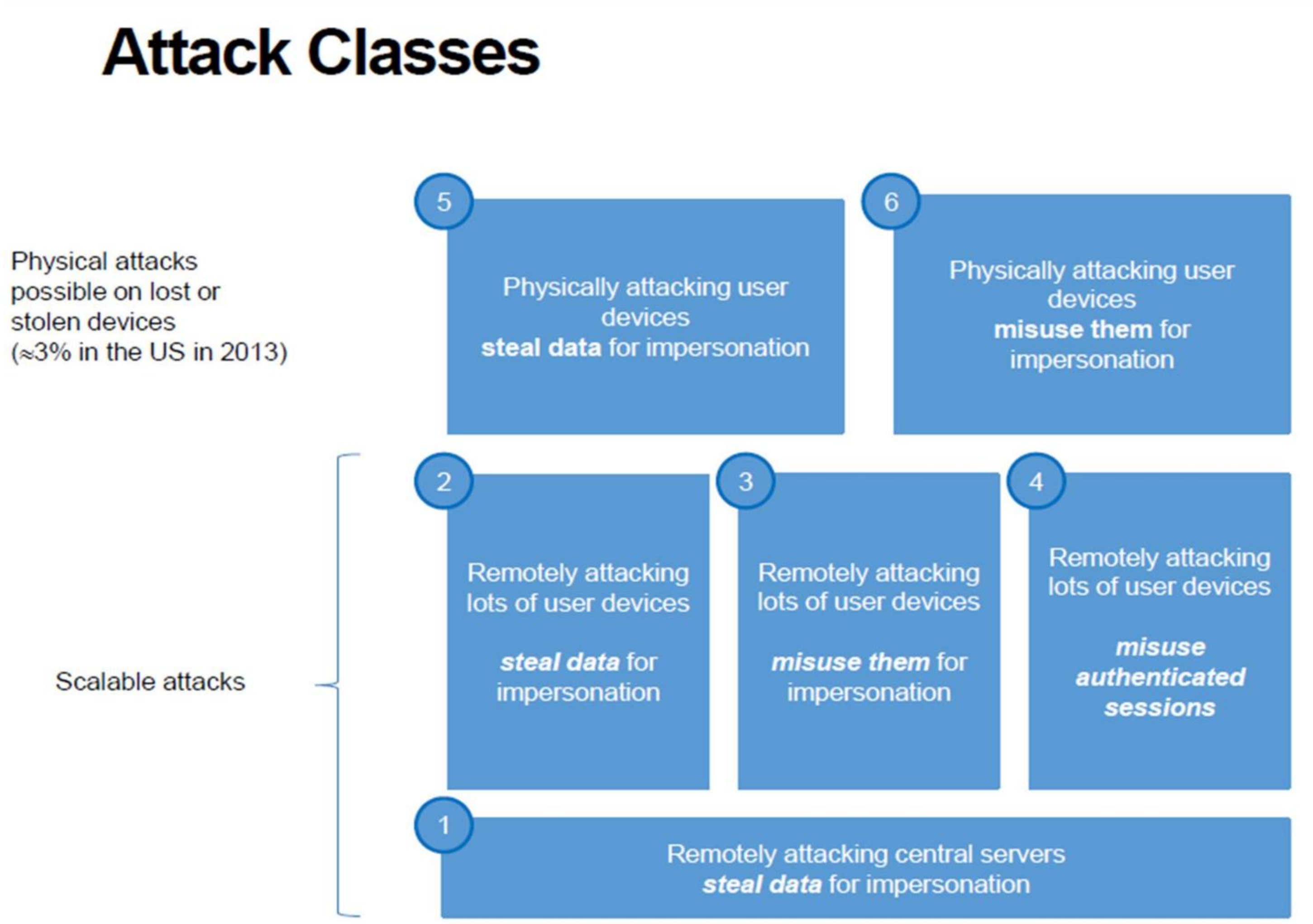
708 data breaches

82 million

personal records stolen

We are, don’t forget, an almost 100% mobile society. Be it at enterprise level, social, government, just any situation, we give away every second valuable information (like passwords, usernames, locations, personal data) to millions of **“watchers”** out there, who scan the internet for such information to be used for illicit purposes.

As I speak now, maybe half of the audience already transmits my speech over the internet without even knowing it. Just the fact, that you have a mobile Phone (not even necessarily a smart phone) in your pockets, powered up and connected to the PHONE network of a service provider, makes you already an innocent violator of data security breaches.



Attack Classes

Physical attacks possible on lost or stolen devices (≈3% in the US in 2013)

5 Physically attacking user devices **steal data** for impersonation

6 Physically attacking user devices **misuse them** for impersonation

Scalable attacks

2 Remotely attacking lots of user devices ***steal data*** for impersonation

3 Remotely attacking lots of user devices ***misuse them*** for impersonation

4 Remotely attacking lots of user devices ***misuse authenticated sessions***

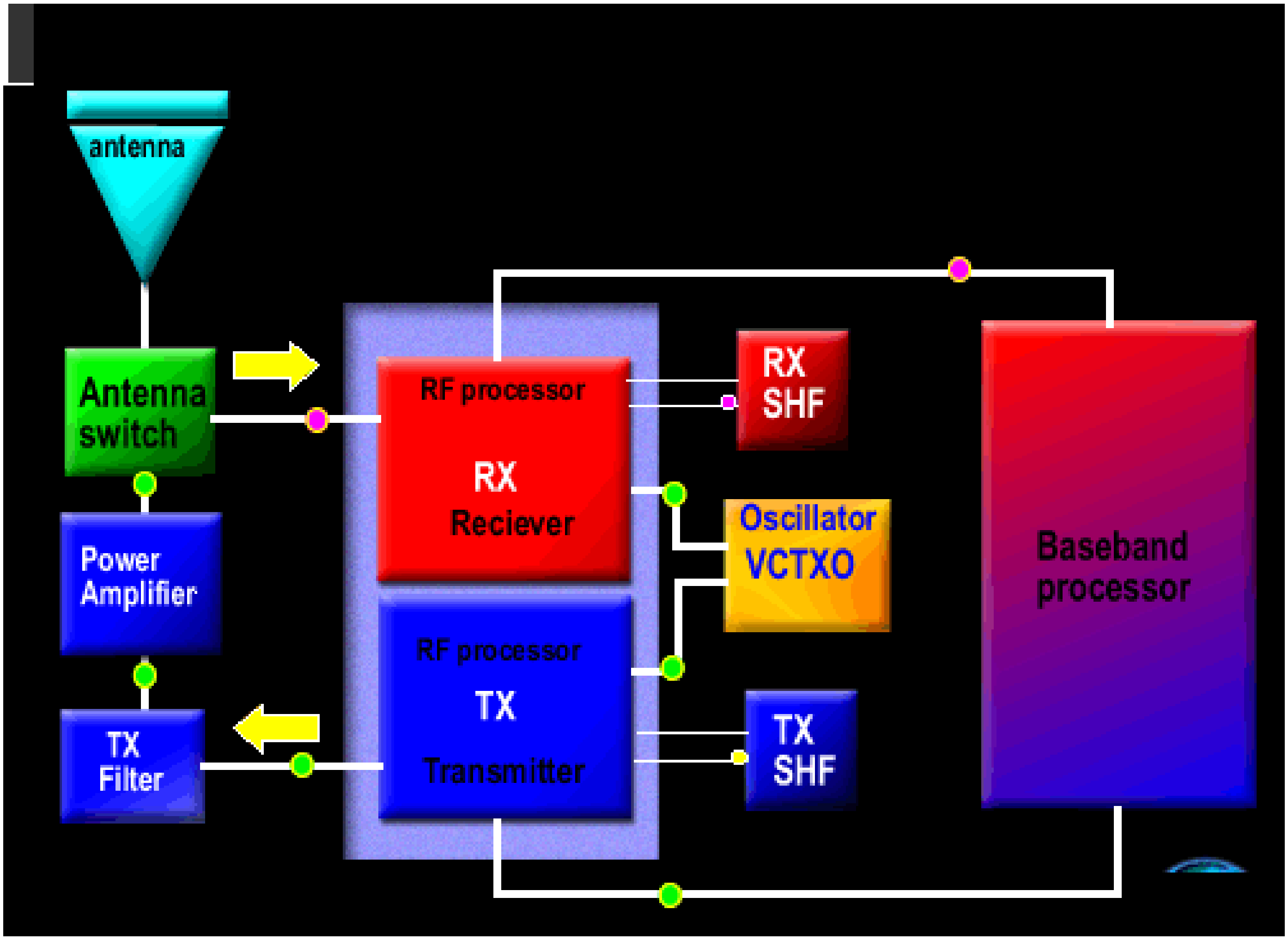
1 Remotely attacking central servers ***steal data*** for impersonation

Large Enterprises do already practice a simple security measurement, switch off the Phones, take out the Battery in important meetings.

For those phones (I believe everybody knows) which have a glued in battery, I can assure you, those phones are manufactured with a second agenda!

While this is a good measurement, it protects only a special situation, it does not protect our Mobile phones from being entered thru backdoors (the GSM section) and steal even encrypted documents, giving the culprits all the time in this world to decrypt the documents.

Let's look at a mobile phone's technical structure and why it is so vulnerable, without getting to technical.



Typical suggestions for mobile security are:

Use advanced encryption and key management techniques..
minimize WLAN-related security vulnerabilities...
use features such as Internet Protocol Security (IPSec) and 802.11
security standards such as EAP and WEP.

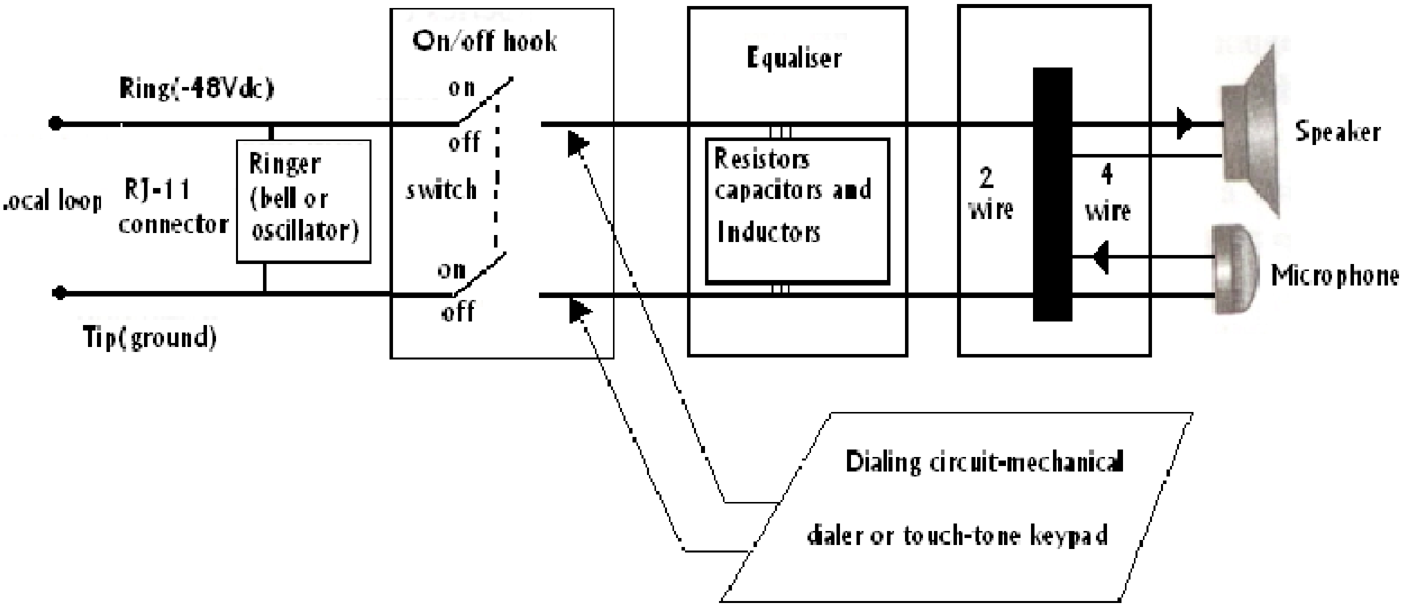
Put strict access privileges on mobile users to protect sensitive information.

Create security policies specific to mobile device usage.
Minimize the impact of a lost device: Password-protect all devices,
Regularly back up PDA data to a PC (I think that is the worst suggestion, have a back up on another insecure device)
Provide specialized training to mobile device users and administrators…….and so on...
Very nice suggestions, the problem is, they have nothing to do with Mobile / Cyber Security.

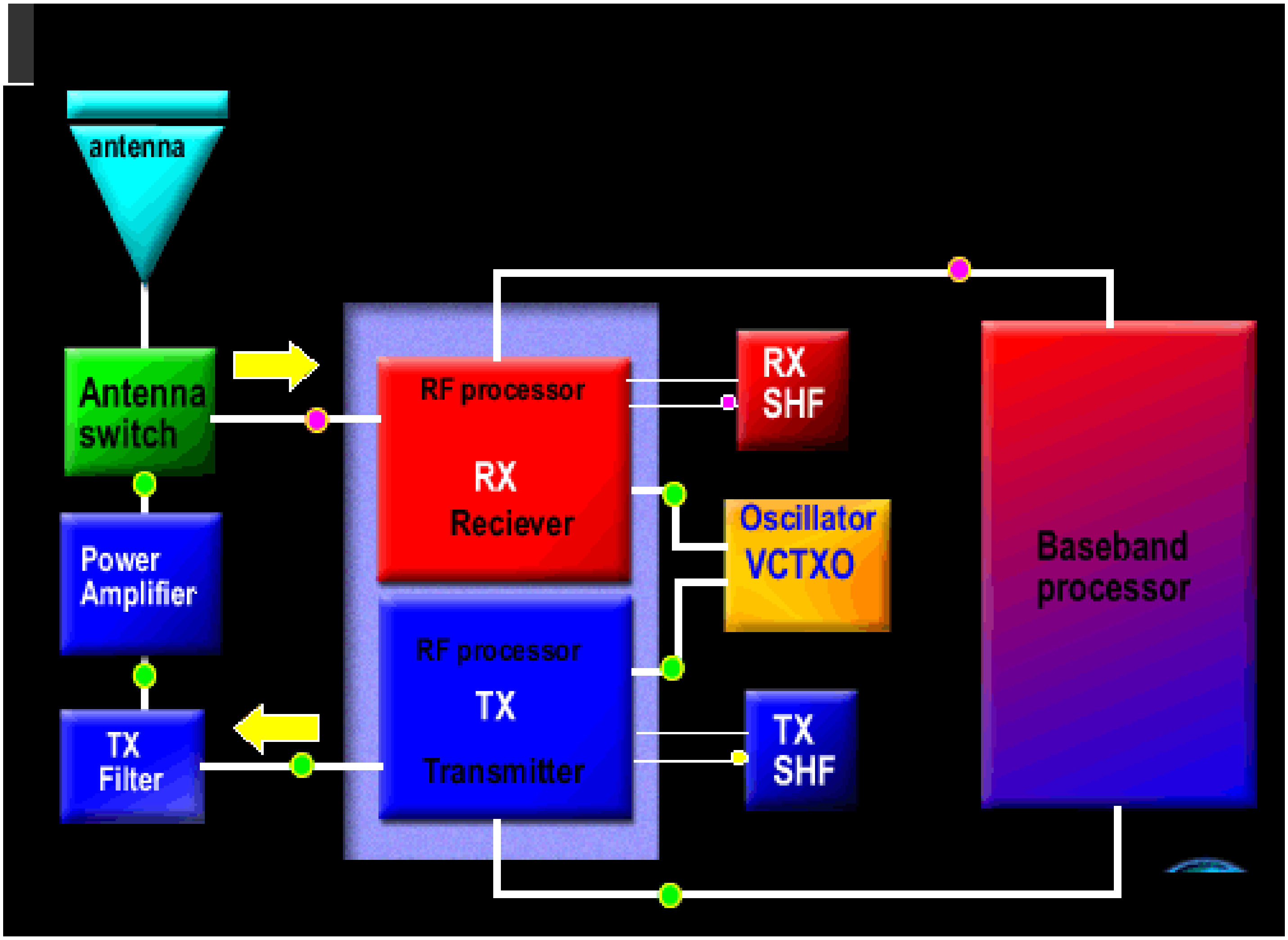
There is not even a hint about one very important hardware vulnerability, the GSM function.

Software developers that come from the Hardware business, have a deciding advantage, they can develop and offer security solutions that can be deployed cross platform on any mobile hardware. In Europe and USA there are a handful of such older generation developers, in Asia they are very hard to find.

A mobile phone is still based on the old telephone theory of Alexander Graham Bell, 2 wires are enough to connect 2 parties. You use an earpiece and a microphone, this way you avoid acoustical feedback and 2 parties can talk over a line that is connected to a DC current source. Of course here it was easy to bug the line, just use 2 crocodile clips anywhere clipped to the two wires connect an earphone, you can listen without any of the 2 other parties knowing it. In today's terms we could call this connection kind of digital, because it uses very low frequencies going along the wires.


On/off hook
Ring(-48Vdc)
on
off
switch
on
off
.ocal loop
RJ-11 connector
Ringer (bell or oscillator)
Tip(ground)
Equaliser
Resistors capacitors and Inductors
2 wire
4 wire
Speaker
Microphone
Dialing circuit-mechanical dialer or touch-tone keypad

The same principal still applies to our so HITECH modern Mobile Phones and not so Smart Smart Phones we are still using GSM even in so called encrypted Phones. THE GSM by nature is full of backdoors, that can be exploited by hackers and professionals to break into the phones memory, SD cards, bug the analog audio or SMS circuits, all in clear language.



The basics of even a smart phone are still the same

GSM (**Global System for Mobile Communications**, originally **Groupe Spécial Mobile**), is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second-generation (2G) digital cellular networks used by mobile phones, first deployed in Finland in July 1991 by Nokia. 2G standard or maybe better 2 wire standard, where the 2 wires were simply replaced by a radio communications module. A radio communications module used also in two way radios, PTT devices etc.

I don’t know if some of You still remember the first Radio Telephone called “Mobile Telephone”

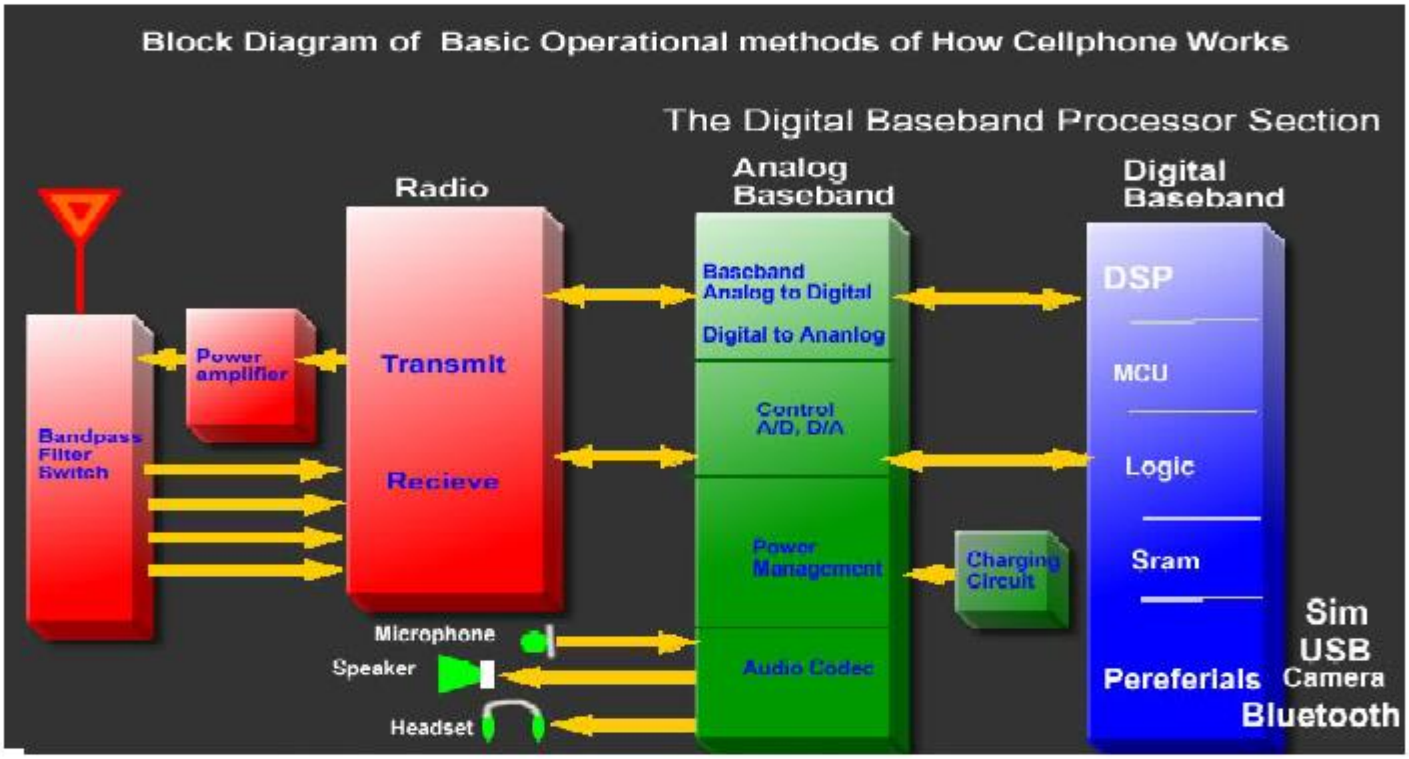
AMPS (**Advanced Mobile Phone System** (**AMPS**) is an analog mobile cell phone system standard developed by Bell Labs,) 450 and 850 Mhz Radio Telephone, operating on existing Government owned two way radio or UHF Networks since 1980..

The standard GSM was created in 1991 as a so called digital continuation of the earlier AMPS standard. AMPS and D-AMPS have only been phased out in 2008 in favor of either CDMA2000 or GSM, which allow for higher capacity data transfers for services such as WAP, Multimedia Messaging System (MMS), and wireless Internet access. However it is not a totally changed system, it still today contains some of the old features, like backdoors to the phone processor.

Our Smart Phones today are only much smaller and higher integrated.

What happens in this Module? Again there are 2 analog devices connected (earphone speaker, and microphone) to a chipset. This chipset (by some called a digital chipset) made everybody believing the connection is digital and so it is better than the 2 wires from old time. Wrong**…. Digital does not mean secure nor does it mean encryption it just means higher capacity data transfers for services such as WAP, Multimedia Messaging System .**

The 2 wires are replaced by a pair of radio frequencies, that by nature are exactly the same working like 2 wires (Transmit/Receive) , making connections between 2 devices. The digital part are the radio frequencies not the actual voice or message origination.

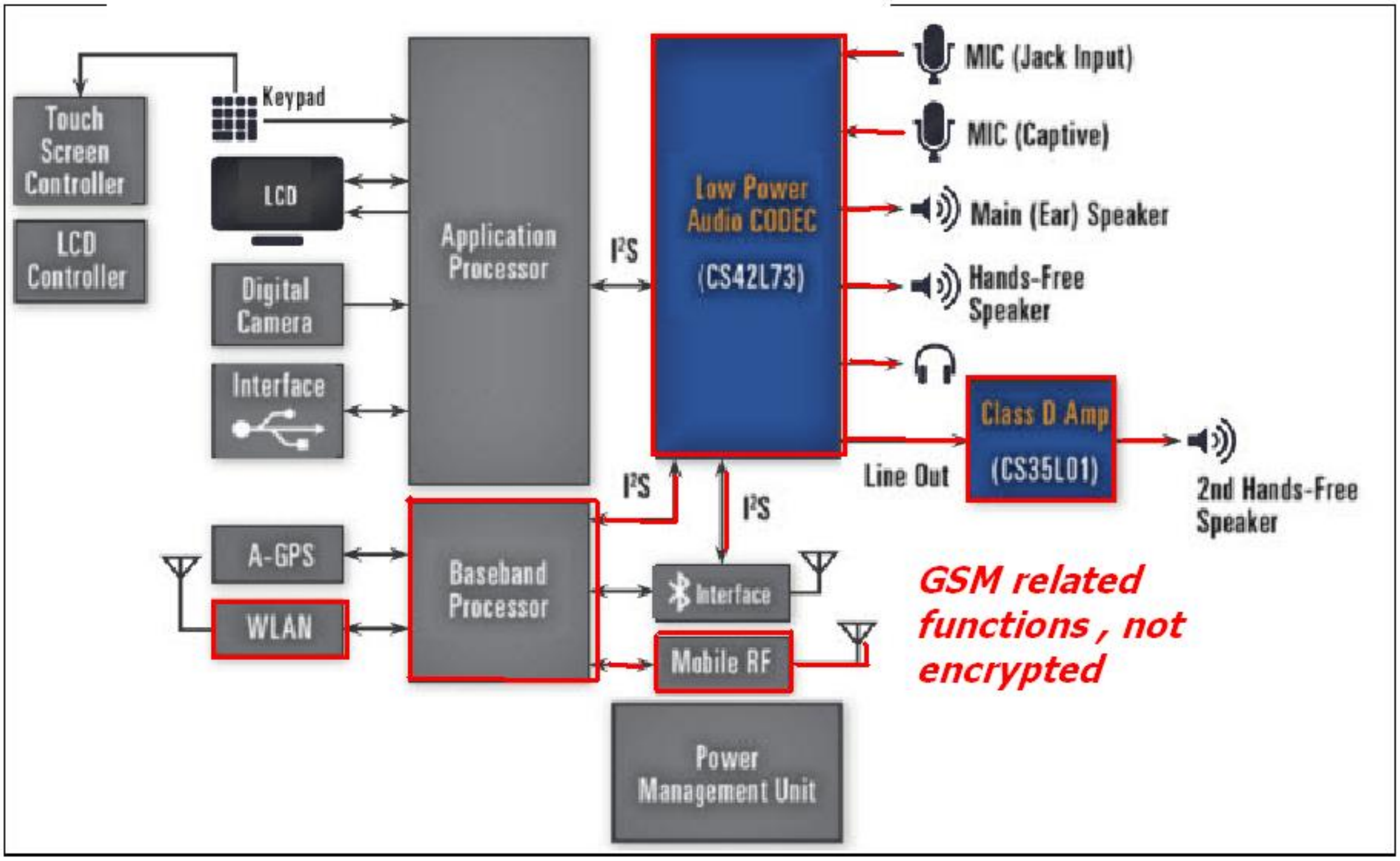


Here we are, Alexander Graham Bell again, a simple analog Telephone, wireless just on a higher frequency. First GSM were on 450 Mhz, then 800,900,1800,1900 etc.. But modulated on that frequencies were still the same analog signals which easily could be listened to with another radio on the same frequency.

The Smart Part was added later, called WCDMA (or today 3G,4G, LTE), but this Smart part has other Functions, higher frequency, more Bandwidth to transmit Data at High speed. It still has very little in common with the GSM part for Voice and Message (SMS) which is open and quasi analog.

If You look at the picture, Speaker and Microphone are analog devices, there is an analog to digital converter, but thru the GSM part, you still can enter the Phone secretly.

However hackers in these days do not need to go that more complicated way of bugging thousands of frequencies, the GSM systems makes it easy.



As long you know either the location or the phone number of a mobile phone, you simply connect to the GSM part of the mobile phone, and go directly to the Microphone or earphone connection on the GSM chipset, and here we are, the Mobile Phone becomes a perfect silent transmission device or listening device, without even known that to the owner. As long the Battery is connected, the GSM transmits the ID, (ID is a complex number consisting of so called IMSI, IMEI, Phone number etc.) to the service provider, to make the phone transparent to incoming calls. The same like the 2 wire phones are always connected to the DC source..

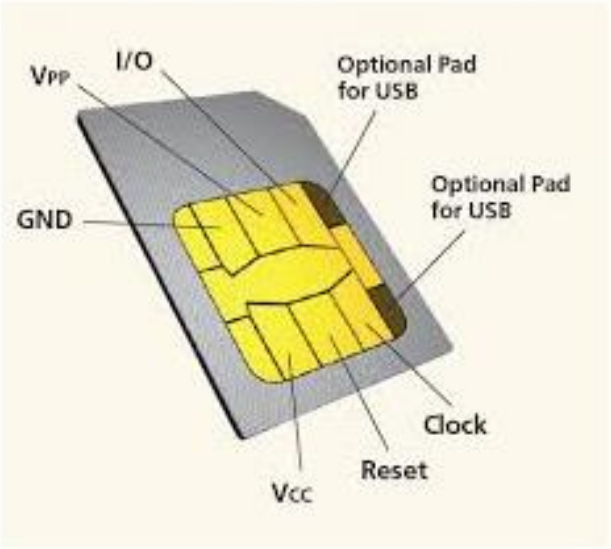
Knowing the location of a GSM phone, now makes it easy to exploit the entire Phone. With simple computer programs an intruder can listen to the voice communication, record passwords and user names, read the entire Directories and files of a mobile phone, copy the entire SD cards, just do anything he wants.

Believing You do a secure Internet Banking transaction, use a credit card that is encrypted , absolutely wrong.

Banks send You a second Pin Number over by SMS, this is “party time” for the intruder, SMS is a part of GSM and open as a book. 3 Minutes time to use this pin number to enter an account and empty it because during connection through the Smartphone, the intruder already recorded the user name, password and maybe second password, all these information is open information, not encrypted. The owner of an account would not even know anything, because the intruder correctly used the username, password and telephone pin, directly from the owner’s device. The Bank does not even know or identify the real user, there is no such process to know who is the man in the middle or the other end.

Sounds bad? It is, because as mentioned in the beginning more than 1,58 billion mobile phones have been compromised, banks do not care, because they are insured. Last Year over 500 million dollars were stolen, only because the culprits used mobile devices to do the transactions, mobile devices with prepaid SIM cards, cards that have no identification of its owner. Here another big Security Risk SIM CARDS.

Easy to be hacked, getting all the necessary data to clone accounts and simulate a mobile phone accessing the network.



So what are the counter measurements?

First of all in important and confidential meetings, switch off the Mobile Phone, take out the battery, that cuts off the GSM part , snaps the 2 wires, Mr. Bell is out of business. For those phones with a glued in battery, just leave them outside the meetings.

To say it in simple words, as long there is GSM used, there is no mobile security

New concepts have to be developed, the entire Telephone part has to be moved away from GSM. Yes there are IP and SIP phone solutions, using only the Data channel, do not need GSM anymore. BUT… though we have these solutions, they are not compatible with the close to 1 Billion GSM Phones in use. Only about 20% of the worlds service providers have already Data networks, the others use GSM or so called 2G.

Now what to do for security on existing mobile devices.

First of all new concepts have to be developed, to minimize the usage of GSM. To extinct the usage completely is impossible, worldwide networks are based on this GSM technology, changing wireless networks completely is out of question. For those who want really peace of mind, they must use the Data channels with encryption.

But even if we use the Data section of a Smart Phone for IP Telephone, we have to make sure all communication is end to end (or P2P), so it leaves no traces on any server in between. Servers shall only carry the minimum of connection information, NOT related to GSM and encrypted with PKI, so intruders cannot identify the phones location and particulars. Such servers shall be located in a secure country where legislation clearly regulates access. Germany would be one of those countries.

These measurements are a good step forward, but not enough. Mobile devices have to be secured with new Identification and authentication procedures, to 100% identify the real user on both ends.

Today’s state of the art would be biometrics. But not such Biometrics offered by some suppliers, like this “ rubbing fingerprint sensor, on screen fingerprint sensors, or other consumer level solutions, all these can be easily fooled.

There are a very few high end mil-grade solutions available recently. The first patented optical fingerprint scanner as retrofit to any Phone, to any platform. The solution stores no image (which could again be copied) it stores a PKI, Public Key. All verifications are done locally, no passwords are necessary or stored in Data banks, identification and authentication is password less.

Several more solutions have to be combined, to make the Mobile devices almost 100% secure.

So far "Encryption" these days a so much discussed and offered solution is NOT the answer, it is only a part of the answer, because encryption encrypts only the wireless connection between 2 wireless points, but does not encrypt anything inside the phone..

Many applications are innocently been used everyday (for example Google's free location service) to locate an unprotected mobile device's cell location.

Modern encryption technology is so advanced, that a short data burst or voice communication does not give enough time to de-crypt the wireless connection, not to consider, mobile phones are just that, mobile, they change locations, cells, frequencies and so on, giving even the most sophisticated super computers not enough time to log in and listen or decrypt. But there is still the GSM part working, which is vulnerable.

We cannot change the networks, so we have to develop methods to encrypt, secure our phone's inner technology.

What is also not possible, that everybody buys a new Phone, with such technology, phones that cost 3,500.00 dollars and more, but even then you cannot be sure, because such phones might be subsidized by interested parties just to do the opposite, give certain party's free and easy access for listening, planting new bugs.

We want to protect the 2 billion plus users out there, without have them buying new phones, and such protection must be cross platform compatible, android, Iphone, blackberry, windows and so on.

Independent Software developers that have the knowledge of ALL Technologies, Mobile Phone Hardware, Radio Frequency Technology, Analog Communications, Digital Communications, Software and much more are needed, developers that date back to the beginning of Mobile Telephone Services.

What is the lack of our young and super intelligent software developers? They can provide solutions like Facebook or what's up, Google search and location, but they do not have the experience in real designing mobile hardware. They depend on the manufacturers information, which is not enough. That is the reason, why so suddenly after more than 35 years of Mobile Phone usage, the industry talks about Cyber Security, Mobile Encryption and so on. Hackers demonstrated to the Software world the fundamental errors in the development of mobile applications.

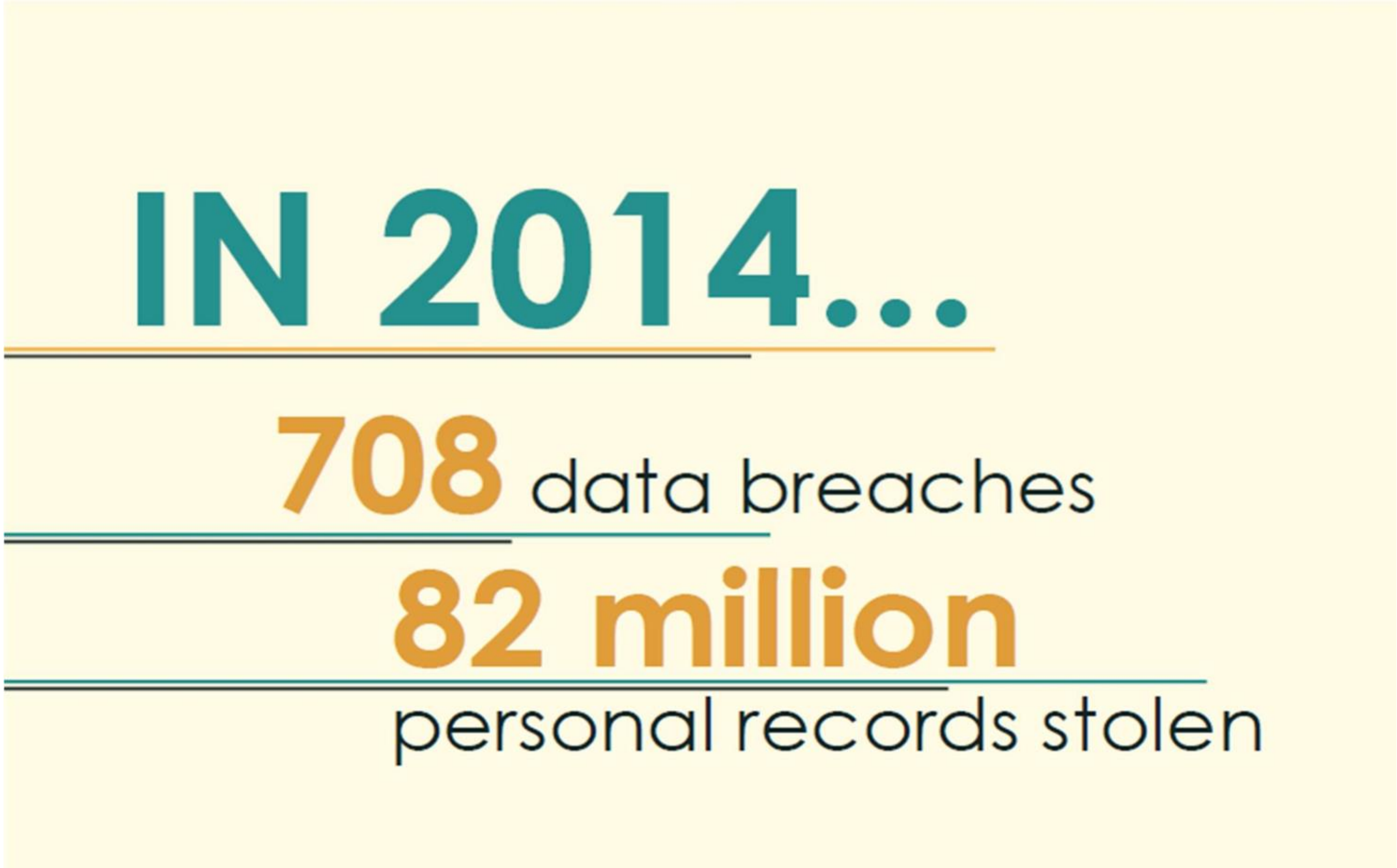
It is important to note that the key issue to mobile security is, that no single security solution will work, given the nature of the mobile environment. And just extending the existing security infrastructure for mobile devices simply isn't practical. Enterprises must treat mobile security as an independent task and mobile-usage-specific security policies must be created and implemented. A comprehensive risk analysis of the potential security hazards associated with the use of mobile devices should be the first step along the path of mobile device security policy creation.

PASSWORD the biggest security risk.

Here is one more security aspect, Mobile devices communicate with fix networks of course, company networks, open networks , cloud servers and so on, so the security of all parties has to be considered.

THE DEATH OF PASSWORDS

First of all Passwords have to be a matter of the PAST.



IN 2014...

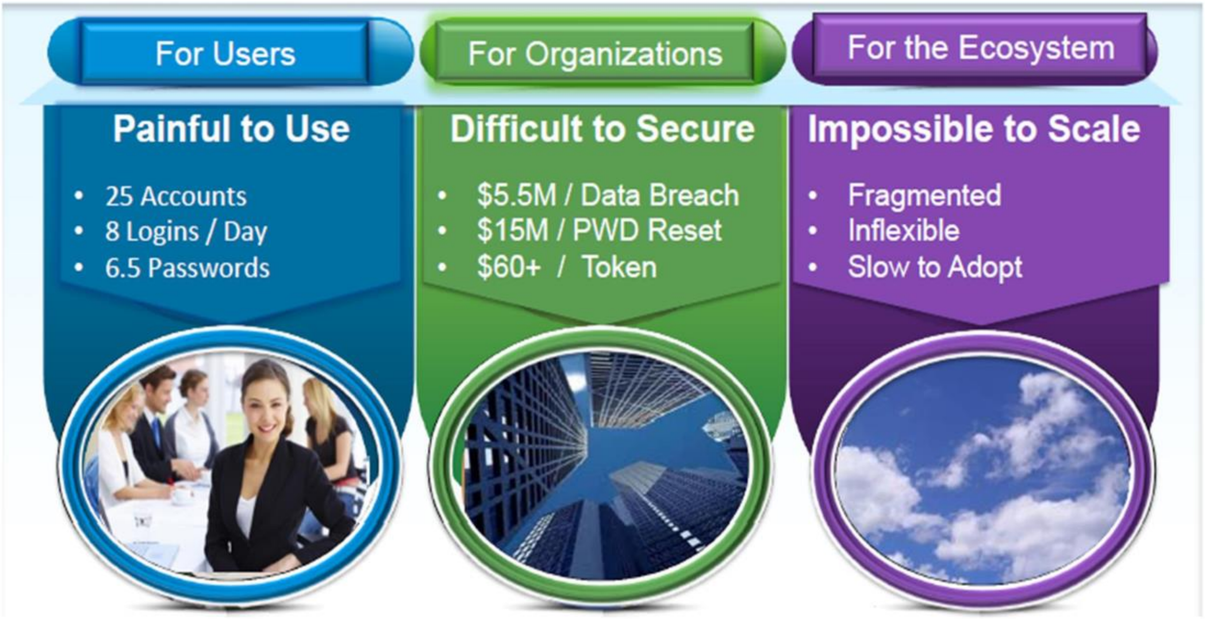
708 data breaches

82 million personal records stolen

Opportunity for Better Authentication is Upon Us

Passwords in Mobile Networks Just Do Not Work!

Mobile devices MUST use password less access and authentication. Changes in networks are NOT costly, especially for financial transactions, the PASSWORD LESS system MUST become a MUST, if accessed from a wireless device.



For Users

Painful to Use

- 25 Accounts
- 8 Logins / Day
- 6.5 Passwords

For Organizations

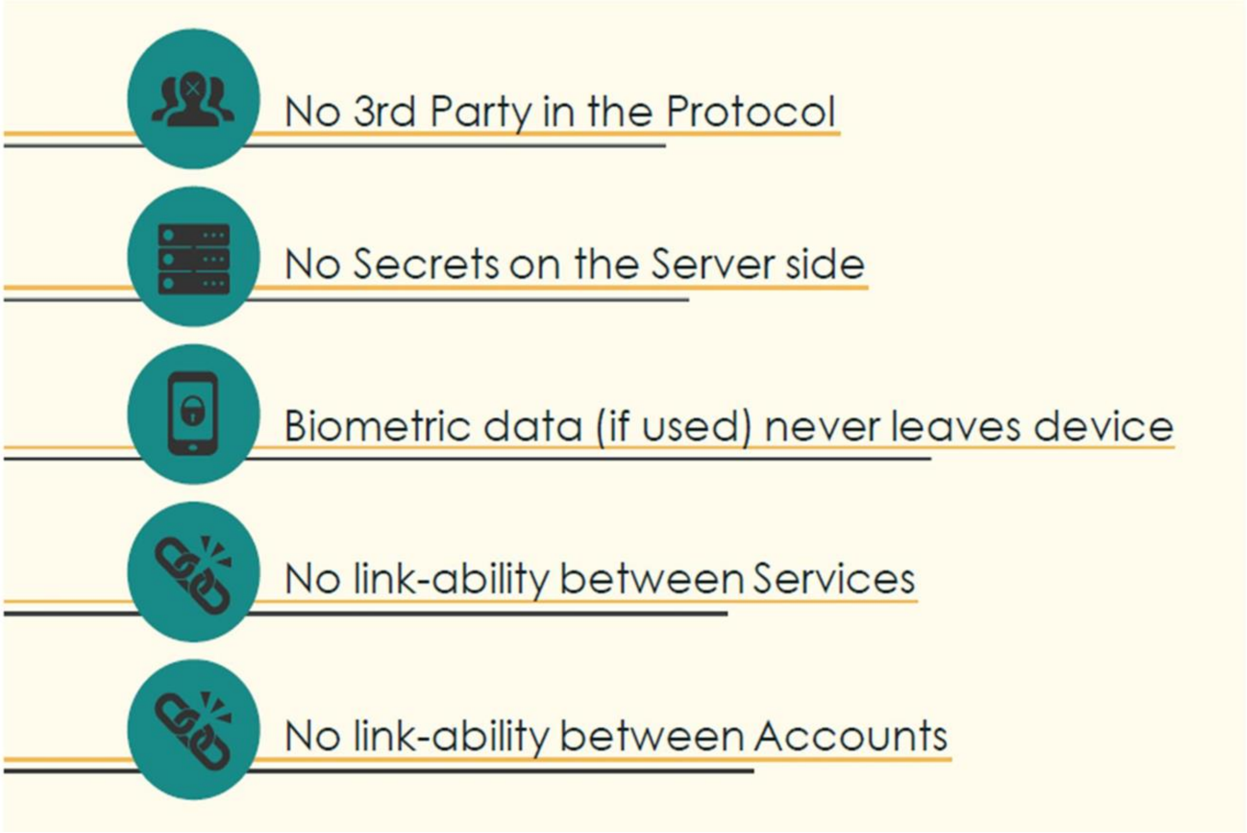
Difficult to Secure

- $5.5M / Data Breach
- $15M / PWD Reset
- $60+ / Token

For the Ecosystem

Impossible to Scale

- Fragmented
- Inflexible
- Slow to Adopt



No 3rd Party in the Protocol

No Secrets on the Server side

Biometric data (if used) never leaves device

No link-ability between Services

No link-ability between Accounts

No storage of any user sensitive information on cloud severs. The less information is transmitted or stored outside the device, the less the chances of being compromised.

Only then we can use encryption inside the Mobile sets and over the air.

So now let’s make this nation the first with real cyber security, the nation first that offers what Mobile users deserve, peace of mind. Let’s all work together. Thank You very much.

This lecture is available on the internet under :
http://securescrypt.com/lectures/govware2015.pdf