ACTIVE AND PASSIVE EAVESDROPPER THREATS WITHIN PUBLIC AND PRIVATE CIVILIAN WIRELESS NETWORKS - EXISTING AND POTENTIAL FUTURE COUNTERMEASURES – AN OVERVIEW.

François Delaveau
(Thales Communications & Security; Gennevilliers, France; francois.delaveau@thalesgroup.com);
Antti Evesti ; Jani Suomalainen; Reijo Savola
(VTT Technical Research Centre; Oulu, Finland; Antti.Evesti@vtt.fi; Jani Suomalainen@vtt.fi; Reijo.Savola@vtt.fi);
Nir Shapira
(Celeno Comnunications Ltd; Ra'anana, Israël; Nir.Shapira@celeno.com).

ABSTRACT

This paper aims at providing an overview of threats that may deteriorate security level and trust in public wireless networks, because of eavesdropper and hacking technologies that operate at the radio interface, and aims at providing an introduction to relevant counter-measures that deal with "physical based" security in a large sense (Physec). We highlight selected promising Physec technologies that are expected in the future years by mixing classical protections and advanced issues of information-theoretic security, secrecy coding and cooperative jamming. These particular items are studied and developed in the PHYLAWS project (EU FP7-ICT 317562, www.phylaws-ict.org), starting Nov. 2012, which supports this work.

1. INTRODUCTION

Given the growing prevalence of wireless radio-communication technologies, the sufficient confidentiality, integrity, availability and reliability a person or an organization can have of the exchanged information is a major societal challenge for both personal and professional sphere. Moreover, the growing importance of sensing procedures and of pilot channels in future radio access technologies (white spectrum, cognitive networks), will result in numerous radio-transmissions of geo-referenced spectrum allocations and of radio engineering data, whose integrity and confidentiality are major industrial challenges for both operators and administrations. Security of radio-interface within wireless networks appears now as crucial for many applications such as broadband internet, e-commerce, radio-terminal payments, bank services, machine to machine, health/hospital distant services. Most of citizens, professionals, stakeholders, services providers and economical actors are thus concerned by confidentiality lacks and by privacy improvements of the physical layer of wireless networks

This paper first introduces the current radio access technologies and describes briefly the main security protocols that are used at the physical layer of wireless public networks, such as subscriber authentication, control of message integrity, and cyphering procedures of messages' content.

From several known examples inside radio-cells (GSM, UMTS, LTE), Wireless Local Area Networks (WiFi), Short Range Communications (Bluetooth, ZigBee), etc., we will focus on the main failures that may occur in existing security procedures and discuss their multiple causes. By considering these weaknesses, we will then describe possible threats during the initial access attempts, during negotiation protocols and during established calls. We will take into account both passive (radio-eavesdropper) and active (radio-hacker) attacks. Nevertheless, in order to avoid any paranoiac or angelic caricature, we will also consider the (severe) practical radio attack limitations that are caused by complex radio environments in many real field situations.

Then, existing countermeasures for improving security, thrust and privacy within wireless networks will be introduced, by distinguishing radio-signals (transmission security), signaling message content (network security), and content of users' messages (communication security). Advantages and drawbacks of these procedures regarding public worldwide use will be discussed. Additional elements about secure architectures for radio terminals and about risk-driven security metrics will be given too

Finally, we will introduce new protection concepts for radio-communications that exploit the physical properties of radio-environments. Especially when complex dispersive and non-stationary, radio propagation has to be measured by infrastructures and handsets: equalization, RAKE processing, MISO/MIMO coding schemes, sensing procedures of cognitive radios (CRs), etc. The relevant physical information provides significant opportunities in order to enhance security algorithms and protocols during access phases and during established calls.

2. OVERVIEW OF EXISTING PUBLIC RADIO ACCESS TECHNOLOGIES

2.1. Main class of public radio networks and relevant radio characteristics

Figure 1 illustrates the large variety of signals to be taken into account nowadays for privacy considerations in Ultra/Special High Frequency (300 MHz - 3 GHz – 6 GHz)

System	Uplink frequency plan (MHz)	Downlink Frequency plan (MHz)	Channel spacing	Modulation UL - DL	Radio Access Technlogy	Access mode	Range of Terminal Power	Typical propag. Range	ref standard
GSM 900	890 - 915	935 - 960	200 kHz	GMSK + variants	TDMA/FDMA	Aloha	2 W	100 m to 3 km	ETSI
DCS 1800	1710 - 1785	1805 - 1880							
PCS 1900	1850 - 1890	1930 - 1970							
UMTS	890 - 915	935 - 960	5 MHz	(OC) QPSK	DSSS/CDMA FDD and TDD, MISO	Aloha	0,25 W	10 m to 3 km	3GPP
	1920 - 1980	2110 - 2170							
LTE	890 - 915	935 - 960	1,4 - 5 MHz	OFDMA and SC-FDMA	FDD and TDD, MIMO	Aloha	0,25 W	10 m to 3 km	3GPP
	2500 - 2570	2620 - 2690							
IS-95 A/B	824-844 1850 - 1890 other	869-889 1930 - 1970 other	1,25 MHz	OQPSK - QPSK	DSSS/CDMA	Aloha	2 W	100 m to 3 km	3GPP2
CDMA2000 SR1/3GPP2			5 MHz						
CDMA2000 SR3/3GPP2			5 MHz						
WIMAX	2402 - 2480		10 MHz	OFDM and QPSK/CDMA	TDD, SC-OFDMA, MIMO	CSMA/CA	0,25 W	1 to 15 km	IEEE 802.16xxx
	3400 - 3600								
	5150 - 5850								
WIFI L band	2402 - 2480		20 MHz	OFDM and QPSK/MC-CDMA	TDD, MIMO	CSMA/CA	0,1 W	indoor	IEEE 802.11xxx
WIFI C band	5150 - 5850		20 - 80 MHz						
Bluetooth	2402 - 2480		157 kHz	0,5 BT GFSK	TDMA/TDD	CSMA/CA	0,01 W	indoor	IEEE 802.15.1
Zigbee	868 - 868.6		2 et 5 MHz	ASK, BPSK, O-QPSK, MSK	CDMA/TDMA	CSMA/CA	0,01 W	indoor outdoor < 50 m	IEEE 802.15.4
	902 - 928								
	2400-2483.5								
DVB-T		470-862	8 MHz	COFDM	FDD, MISO		20 - 200 kW	>> 10 km	ETSI

Figure 1: Public network to be improved relevant to privacy.

2.2. Main class of RATs – Early signaling exchanges

Roughly mains RATs can be shared in four classes (fig. 2):

FDMA: (Frequency Division Multiple Access)

- Signal repartition over frequency
- Exemples are 1G standards: NMT, AMPS, etc.
- Propagation equalization is required in receivers
- Hopped/opportunistic frequency variants: Military, ALE (HF)

TDMA: (Time Division Multiple Access)

- Signal repartition over time slot
- TFDMA/FDMA variant with hopped frequency
- Propagation equalization is required in receivers
- Examples are 2G public standards (GSM, D-AMPS), WLAN 802.11b, short range (Bluetooth, DECT), and most of tactical VHF Military ad-hoc networks

CDMA: (Code Division Multiple Access)

- Signal Repartition over spreading codes
- Receiver Rake processing
- CDMA/FDMA/TDMA variants with hopped frequency / slots
- Examples are 3G public standards ([1], [2]), and several UHF and SHF Military ad hoc networks (ex: MIDS).

OFDM: (Orthogonal frequency Division Multiplex)

- signal multiplexing over frequency
- simplified equalization within receivers
- numerous examples: DVBT/H, DRM, LTE, Wifi, Wimax
- advanced planning capabilities: Single Frequency Network;, MISO and MIMO
- derived RATs: COFDM, O-FDMA, SC-FDMA, SC-FDE

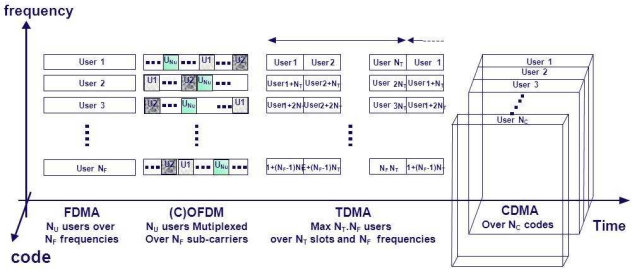

Figure 2: main radio access schemes

Note that in any case, establishing radio links involves early signaling exchanges among infrastructures, nodes and terminals, which are summarized on fig. 3 hereafter.

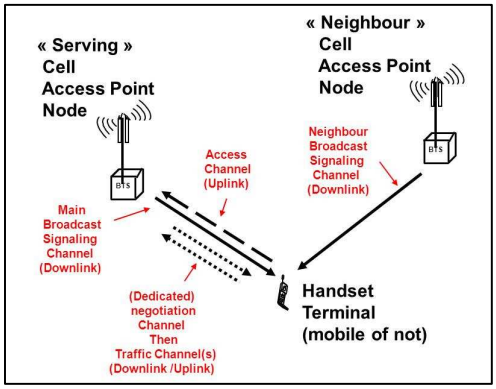

Figure 3: signaling exchanges before and during radio-access

3. SECURITY LACKS OF PUBLIC NETWORKS

3.1. Native privacy weaknesses of worldwide standards

The worldwide nature of modern digital standards induces intrinsic privacy lacks of the early negotiation protocol. Because it must remain simple and generic everywhere and for any subscriber, it is often achieved with unprotected broadcast signaling and access channels (through beacon frequencies, pilots codes, etc.) that provide local system time, easy decoded network parameters, frequency planning. Exchanges of subscribers' identifiers are required for registration, and they are recurrent for roaming and handoff of mobile (radio-cells, PMR, DVB-H, etc.). The frequent use of temporary identifier (such as TMSI in GSM) appears as a poor privacy improvement in many practical cases, even when ciphered (see below).

FDMA, TDMA and ODFM based RAT signals, especially when including synchronization midamble or words, are easy to detect and to demodulate in both DL and UL sense. Within CDMA, synchronization codes or pilots symbols, especially when clocked by GPS system time, allow easy detection and de-spreading of DL signaling and of UL access channels. Pilots symbols included in traffic facilitate both DL and UL synchronization recovery and de-spreading.

All these facilities fasten terminals computations, but they make passive and active attacks easier for recovering of synchronization, for decoding of broadcast and negotiation channels and for demodulation of traffic signals ([10],[14]).
In the following, we will consider the notations and geometry of fig. 4: legitimate link is Alice to Bob, Eve being the eavesdropper or the radio-hacking system.

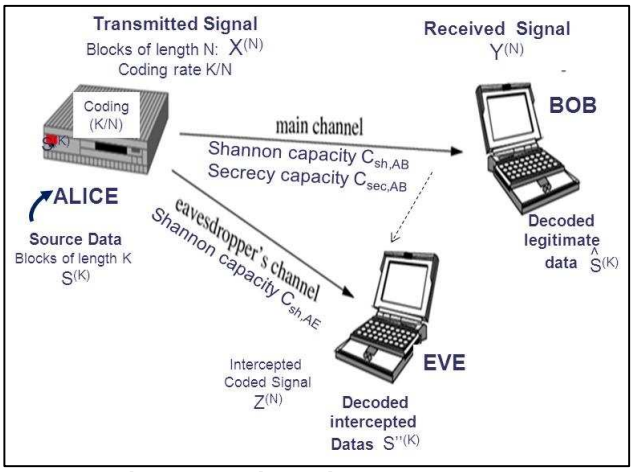

Figure 4: legitimate and eavesdropper geometry - Notations

3.2. (Non-exhaustive) examples of privacy weaknesses in modern public standards

Radio-cells authentication and location attack: When authentication is single sense only or weak, mobiles may be spoofed by using a virtual base station through forced roaming or paging procedures (that succeed when transmitted power is enough to overhead the propagation losses and the cell re-allocation criteria, when carrier and content of broadcast messages is convenient, etc.). These basic active attacks apply to 2G networks such as GSM [12], to many practical cases of 3GPP3/GPP2 and of 4G networks when operators apply weak Auth procedures. As a result ([22]), paging messages from RHS towards idle mobile stations can initiate connections and track location of mobile stations. These messages are selectively sent to the tracking area that the terminal is known to locate in unprotected format: paging messages identify the target terminal by using permanent Ids (IMSI) or temporary IDs (TMSI) which change only when user changes of location update area. A variant consist to initiate call requests (with MSIDSN) to victim terminals and then passively monitor paging messages whether the user locates in the monitored area. Disconnecting paging and call request is even possible before victim's terminal alerts, thus keeping attacks stealthy.

Subscriber's or terminal's dependent resource allocation: In some CDMA standards, close relationships occur between the allocated code for traffic and identifiers of the subscriber or the terminal. Moreover strong dependence of DL and UL links may exit, such as in 3GPP2 public mode (see [2] [14]): long scrambling codes masks (LCM) manage both UL spreading and DL scrambling among users, with and injective dependence on the Electronic Serial Number of terminals; this determinism may highly facilitate users' selective interceptions by both passive and active threats.

Pilot symbols within traffic CDMA channel: many CDMA signals, such as UMTS traffic channels [1], include low combinatory pilots symbols that highly facilitate exhaustive tests for slot and frame synchronization, for recovery of scrambling codes, in both DL and UL senses [10].

Sub-optimal module order in the transmission chain: In the transmission chain of several standards ([1][2]), coding occur before ciphering and modulation redundancies occur before scrambling. This usually facilitates key attacks.

Unexpected publications of cipher algorithm – GSM example: in this case successful cypher attacks may be facilitated. This occurred in the late 90s' for GSM A5/1-2 cipher algorithm (max key length is 64 bits), and for A3/A8 algorithm that compute authentication results (RES), temporary identifier (TMSI), and cipher keys (Kc) from internal Keys (Ki coded inside SIM card) and from random parameters (NRAND) that are transmitted over the air [16] [17]. In practice, as a result of economic competition and of hacker activities, full secrecy of wireless standards cipher algorithm can never be warranted over numerous years.

4G Networks: A number of potential attack vectors have been identified in [18]: Firstly, efficient jamming attacks can target OFDM pilot tones [19] [20], which are used to correct channel effects and to equalize transmission. Secondly, uplink channel quality information, which is adaptively used in base station to select modulation and coding for the downlink, may be targeted in Denial of Service (DoS) attacks. Thirdly, large amount of 'virtual terminals' (i.e. 'Sybil' identities) can be used to affect base stations resource usage and, in coordinated attacks, to achieve more resources for attacker's terminal. Primary user emulation attacks [21] can also be used in spectral herding to guide a victim into the wanted channel, which is chosen in order to facilitate man-in-the-middle (mitm) attacks. LTE Evolved Packet System–Authentication and Key Agreement solution (EPS-AKA) has been considered to be vulnerable for mitm attacks as it discloses the permanent identifier (IMSI) by sending it in clear text during the first connection [25].
Location privacy attacks such as identified in GSM in [22] are also applicable in LTE [23]. As cell size can in LTE be small the users' locations can thus be resolved in high detail.
The authentication and confidentiality of LTE is based on permanent security associations i.e. long term symmetric keys shared by terminal and network. Consequently, as noted in [24] the key derivation procedure in EPS-AKA

does not provide perfect forward secrecy. If a symmetric key is revealed, all derived session keys and content protected with these keys can be compromised. Moreover, EPS-AKA is backwards compatible with older authentication mechanisms and, therefore, an attacker may gain an access to the LTE network by utilizing security weaknesses found from the GSM or UMTS security algorithms [26].

Bluetooth and ZigBee Short range communications:
Bluetooth is intended to establish wireless ad-hoc networks by means of short range radios. Bluetooth is widely used to connect peripherals to computers and mobile devices. The complexity of the Bluetooth specification causes challenges for security [28]. Moreover, National Security Agency (NSA) lists following threats related to Bluetooth: identity detection, location tracking, DoS, unintended control and access of communication channel and unauthorized device control and data access. Furthermore, National Institute of Standards and Technology (NIST) lists the following Bluetooth specific attacks in its Bluetooth security guide [29]: Bluesnarfing makes it possible to gain access to data stored in a device, Bluejacking makes it possible to send messages for a Bluetooth device, Bleubugging offers access to data and device commands, Car Whisperer makes it possible to send audio to car's audio system and eavesdrop via car's microphone, Fuzzing attacks to send malformed data to device and observe device's behavior in order to reveal possible vulnerabilities in the Bluetooth stack, Pairing Eavesdropping to determine secret keys for data decryption, and Secure Simple Pairing Attacks to cause mitm attacks.
In [28], NSA states that Bluetooth should offer adequate security for situations where unclassified data is handled. In other words, Bluetooth is not applicable for classified information. Default or inappropriate passkeys are one important issue that has enabled attacks towards Bluetooth devices. However, from the physical point of view these relate to upper layers. Nevertheless, Bluetooth is intended for short range communication but the directed high gain antenna may offer signal reception over kilometers [30]. Thus, appropriate encryption is needed in order to avoid eavesdropping and also means to mitigate threats related to traffic analysis. Bluetooth utilizes a Frequency Hopping transmission mode, which actually does not offer much security in the physical layer: Frequency Hopping Sequence is delivered in a clear form during the link establishment, and thus, near devices are able to capture this information [30]. Lastly, it is known that random number generation in the Bluetooth is weak [30]. From the physic viewpoint, this issue can be improved by utilizing any random features of the communication channel.

ZigBee is intended to establish ad-hoc networks, where a low data rate and long battery life are perquisites. In ZigBee, security of the whole network depends on a master key. Thus, achieving the master key threatens the whole network. ZigBee security is investigated from the protocol and implementation viewpoints alike – where the protocol refers to security capabilities of the IEEE 802.15.4 and implementation for manufacturers' implementations. Most of the security risks are due to the implementation made by equipment manufacturers. Three main categories of attacks against ZigBee are physical attacks, key attacks, and replay and injection attacks [31]. From these categories, physical attacks are not performed via network, i.e. attack requires physical access to the programming interfaces of a device.
In addition, the minimal session checking of ZigBee makes it possible to mimic legitimate nodes.
Key attack is another well-known failure in ZigBee [31] [32]. It uses commercial traffic capturing device in order to collect wireless transmissions and analyses the collected data by means of KillerBee [33]. Based on the traffic analysis, such an attack is able to get network key.
Lastly, even if ZigBee is intended to support a long battery lifetime, jamming attacks are able to drain batteries faster than initially assumed. For instance, [32] presents an attack to abuse poll requests in a ZigBee system that prevents the utilization of the sleep mode, which in turn may cause power failures in ZigBee nodes/actuators.

WLAN: the direct use of subscriber identifiers or MAC address in WiFi registration procedure occur intrinsic vulnerability regarding user's privacy. WiFi encryption is applied on frame's payload only and not on MAC header which is present in all frames, thus user's privacy and identity is inherently compromised. This is particularly useful for Eve to classify traffic according to source-destination pairs. Until very recently, WiFi protocol management frames were not encrypted at all, thus exposing the network to various sorts of active attacks and DoS. In 2009 IEEE has standardized 802.11w, which defines encryption of management frames. Still, some management frames are excluded from 802.11w, amongst them all CSI feedback related frames, making them an easy target for interception and for both passive and active attacks. Moreover, strong failures of the initial Wifi WEP keys were highlighted in the early 2000s, and weaknesses are pointed out relevant to new WAP and WAP2 ciphering keys [15]).
Another physical layer vulnerability resulting from network security lapse is the unnecessary exposure of both the AP's and the terminal's capabilities. The capability exchange, which transpires during the association procedure before authentication and establishment of a secure link, includes many of the physical layer's attributes (supported modulations and error correction codes, beam-forming capabilities, etc.) that can be utilized in smart passive or attacks. Here, physical security could be greatly enhanced by simple protocol upgrades, i.e. exchanges of capabilities after authentication procedure, over a secure link.

Channel negotiation in MIMO RATs: advanced close loop MIMO RATs include early propagation channel estimation procedures. In particular the 802.11n/ac based WLAN protocol defines a closed loop sounding procedure wherein the terminal returns Channel State Information (CSI) to the Access Point (AP) for performing single or multi user beam-forming transmissions. The channel state UL feedback message (included in a Management frame and being not encrypted) is easy to intercept, thus it compromise security and facilitate passive and active attacks. The closed loop sounding procedure can also be easily attacked either on the DL (sounding frame) or the UL (feedback CSI frame), by a protocol aware jammer ([19] [20]).

Geo-location services: When un-protected (through most of SMS transmissions for example), geo-location services that use GPS location propagation delay measurements or decoding of signaling, induce serious privacy lacks. Protection of geo location messages becomes now crucial for subscribers, operators and administrations when considering the massive signaling procedures that are studied for future 4G and cognitive networks ([3] [4] [5]), such as:

- Downloading of network data in order to improve RAT through geo-referenced allocations of radio-resource.
- Geo-referenced uploading of sensing report by mobiles.

Multi-RATs handset: Multi-RAT handsets are now very usual. Unfortunately, the vulnerabilities of each RAT may be cumulated, especially when facing active threats: brief jamming procedures of the most protected mode is often enough to force commutation on the worst one.

Personal L–Band satellite communications (L-PCS): Most of L-PCS phones include dual ground-satellite modes and many of the usual satellite RATs are very weak regarding privacy (ex: public services of Iridium, Thuraya, etc.): terminal have high output power and low antenna directivity, waveform are easy to demodulate, un-ciphered transmissions of subscriber's location and ID are usual at early stages of access attempts (this facilitates roaming and billing), etc.

Sub-optimal radio-engineering practices regarding privacy. Examples are fixed frequency planning in GSM networks, low-random code allocation in CDMA, poor time recurrence for changing Temporary IDs and ciphering keys, single authentication sense (instead of dual sense), low power threshold values for cell re-allocation criteria, un-ciphered transmissions of IDs at borders zones, etc.

Users' misunderstood of security aspects (parameterization of secret key, regular change of personal passwords, etc.), and policies restrictions that may occur too, such as ciphering forbidden, Temporary identifier forbidden, etc.

3.3. About passive eavesdropper

3.3.1. Principle of passive attack in public networks:

Passive eavesdropper usually follows the usual RAT:

- Decoding of the broadcast signaling at first,
- Search and decoding of access and paging messages,
- Following of the complete access protocol such as the terminal and nodes do, demodulation of negotiation messages (including subscribers and/or terminals IDs, GPS locations, radio measurements, etc.).
- Recovering and demodulation of traffic channels
- Attempts to decipher negotiation and traffic messages

Several variants are described in [9]. In some cases (i.e. when the key is not found in real time), passive eavesdroppers conduct off line from massive signal records.

Passive attacks take advantage of geometric propagation (close range), of high output powers, of easily detected and demodulated signals (FDMA, TDMA, OFDM). They may be disturbed by fast power control, by weak and complex signals (CDMA), by dense spectrum occupancy, by interferences and signal mixtures (MIMO, full duplex [6]).

Relevant to access protocol, passive eavesdroppers directly take advantage of any privacy default: especially a priori knowledge or un-protected information relevant to subscribers or terminals IDs or relevant to network engineering allow strong reduction processing complexity.

3.3.2. Passive processing techniques:

Data-aided Processing (DAP) is very usual and efficient for signal processing when facing digital civilian radio-communication standards mentioned fig 1. Usually more sensitive and more accurate than all other techniques, DAP can process medium to strong interference when merged into smart antennas (see [35]). When based on matched filter (inter-correlation of synchronization words, of midambles, of pilot codes, etc.) DAP can achieve early recognition of signals, efficient synchronization and equalization (fig 5) and decoding of messages (fig 6 and 7).

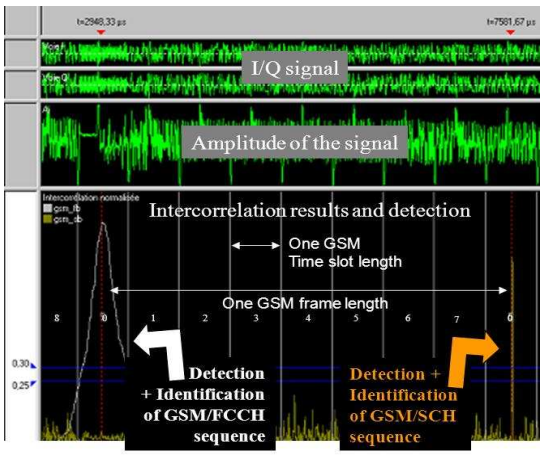

Figure 5: processing into passive eavesdroppers. Example of GSM slot+ frame synchronization (data-aided SISO)

Usually, data-aided techniques apply to any digital standard except CDMA UL traffic signals. In this later case and without extra knowledge, combinatory is prohibitive, and passive attacks take better advantages of symbol modulation characteristics and of pilot symbols into the frame for achieving synchronization and de-spreading ([10]).

Radio parameters | Network parameters

	FU	Level(dBm)	C/I(dB)	CI	LAC	MNC	BSIC	FN
BTS1	70	-99.2	-13.1	39911	33391	1	50	69932
BTS2	70	-94.4	-7.9	35562	240	20	40	1251388
BTS3	70	-89.0	-0.6	2581	21235	1	2	1119767

	List of Cell Allocated frequencies	List of Border Cell beacon frequencies
BTS1	70	98 99 100 102 103 104 107 108 111
BTS2	70 101	90 94 100 104 110 116 118 124 675 681 689 697 705
BTS3	70 113 114 115 116 117 118 119 120	101 103 110

Figure 6: GSM beacon decoding (data-aided SIMO)

Layer 3 messages

Sense		Message	Frame ID	length	Frame Number		
DL	OM	Sync Channel Info	0x013819	4	31	28	25
DL	RR	System Info Type 6	0x013824	9	42	28	10
DL	OM	Sync Channel Info	0x013823	4	41	28	09
UL	MM	Authentication Response	0x013822	4	40	28	08

Message content

Offs.	Bytes (hex)	Mask	Fields
-2	05	00001111	Protocol Discriminator = Mobile Management
-2	05	11110000	Skip Indicator = 0
-1	54	00111111	Message Type = Authentication Response
			Message Content:
			Authentication Parameter
0	4E 5A B3 58		SRES = 4E 5A B3 58

Figure 7: GSM SDCCH decoding (data-aided SISO)

3.3.3. Practical limitations of passive attacks in real field.

Communities of crypto-analysis and of physical layer security usually consider "maximal" attack risk and ideal attack situation: complete a-priori knowledge of the legitimate link, negligible demodulation errors and infinite message lengths. Nevertheless, when facing realistic radio networks and real field propagation, passive attacks are fully dependent of radio conditions (over the complete access protocol and during the data transmission) as they cannot influence communication protocol at nodes neither at terminals. In addition, they are limited by signal structures.

. The power control being relevant to the legitimate link only, it often induced high non-stationaries and low signal to noise ratios (SNRs) at Eve's part (often less that Bob's SNRs). Similarly, interference situations are often stronger for Eve than for Bob. Here, different radio-environments and geometries such as close range indoor, dense outdoor, pedestrian, vehicular, etc. may induce significant differences regarding operational efficiency of passive attacks, whatever are Eve's radio-performances.

. Time, space and Doppler coherence of the propagation channel is finite (and often limited in complex environment); length and redundancy of reference signals and of messages are usually limited by slots duration and by frame structure. All these constraints decrease Eve's integration capabilities

. Eves processing may be (unintentionally) hardened by the standardized procedures themselves (for example fast power control in DS/CDMA systems, soft handover procedures, MIMO/MISO and full duplex RATs [6] increase and the apparent randomness).

In practice numerous passive eavesdropper are thus highly disturbed when unexpected randomness occur into legitimate links and when radio-environment is complex.

3.4. About active radio-hacking systems (RHS)

3.4.1. Principle of active attacks

Radio hacking systems usually exploit weaknesses relevant to authentication or to integrity control in order to fool the victim terminal node or infrastructure, and to influence radio-access procedure in the weakest privacy modes.

3.4.2. Active processing techniques:

Active catching: One basic principle to control a victim terminal is to substitute the local communication node with a virtual node in order to force registration or roaming procedure of terminals (fig. 8). This simplest catching mode requires no synchronization with the real network but only achievement of a (cell re-selection) power criteria and a suitable cloning of beacon channels (see fig. 9). Then RHS controls the caught victim terminal and it can force its registration roaming and identification procedures, it can page it on IMSI IMEI or TMSI, it can intercept calls initiated by the victim terminal, call the victim terminal and force max power, etc. These procedures can be achieved with a protocol tester and a test mobile that access to the network and relay the message of the victim mobiles ([12]).

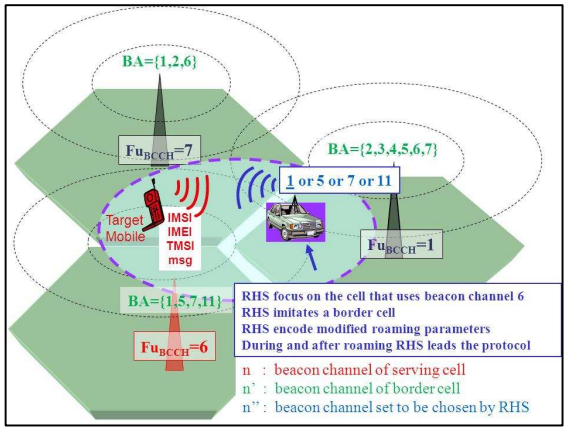

Figure 8: example of active catching and control of radio-cells.

More advanced RHS concepts ([13]) achieve prior synchronization with the real network, follow complete paging and access procedures and perform full duplex synchronized relay of the messages exchanged between the caught terminal and the real network.

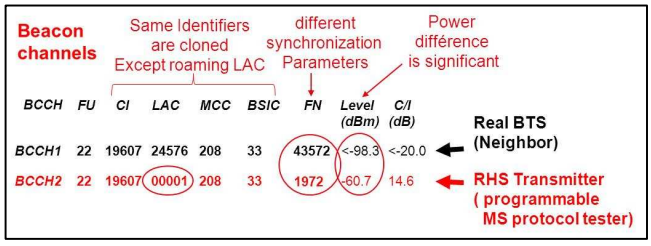

Figure 9: real field example of cloning a GSM beacon channel.

Active catchers practical efficiency fully depend on the network radio-engineering characteristics at the earliest access phases, and thus of relevant propagation conditions. Then, having the full control of the caught terminal, they are less disturbed by radio conditions.

Semi-active spoofing: Semi active variants consist to exploit large acknowledgement latencies and poor integrity control in order to repeat and change the content of dedicated UL or DL messages inside the real negotiation phase, before the acknowledgement of several protocol steps. For example,

- Suitable repetition of "subscriber identity" messages by including modified indications can force transmission of IMSI (or even IMEI) instead of TMSI,
- Suitable repetition and modification of "terminal cipher capability" messages can force clear text transmission.

Semi active variants thus require at least frame synchronization with the exchanged messages and repetition + propagation delay times that lower than protocol tempos.

Selective jamming attacks: Both Active catching and semi active spoofing may be sustained by selective jamming in order to influence the cell selection processing and to forbid more protected access protocols that may be used by multi-RATs terminals, etc. Several classical active attacks variant are described in [9]. Some authors have shown that "aware jamming attacks" of propagation negotiation protocol may be significant threats for MIMO RATs [19][20].

3.4.3. Practical limitations of (semi) active RHS in outdoor.

The main drawbacks of active attacks rely in the power constraints and in the real time mode of use. The received power at the victim terminal or node that has to be sufficient

. to forbid at first any unexpected handoff initiative of the terminal. In dense radio-environments, this may require additional selective jamming (and it thus it induces energy dispersion, it requires more accurate network recovery for suitable parameterization of jamming + beacon signals, etc.)

. to better influence the cell re-selection criteria.

Thus, when facing dense urban networks with BS at building roofs, outdoor pedestrian and vehicle embedded RHS usually have poor effective range (typically less than a few hundred meters, often a few ten meters only).

In addition, the intrinsic real time use mode of RHS reduces processing capabilities and practical efficiency when facing adverse radio conditions, dense environments, etc.

Moreover, as active non synchronized attacks are very intrusive within the real network (fig 9), they often disturb many mobiles in the neighborhood. This leads to saturation risk of the RHS which has to manage multiple roaming/detach procedures of non-targeted terminals.

Semi active variants are more discrete and they usually require less transmitted energy at the RHS part. Nevertheless, semi active RHS highly depend on the network engineering over the full protocol duration (and not only of early negotiation phases): frequency planning, multiplexing schemes, time reference of victim node/terminal, latencies of the negotiation protocol. They thus require an accurate recovery of frame/slot/symbol synchronization (more difficult when facing wideband CDMA), they need fast real time reactions and they have to take into account propagation delays. All these constraints dramatically limit their practical range of use: typically a few hundred meters, often to a few ten meters only.

3.5. Special threats relevant to SDR and CR.

Within CR networks (see [3-5]), access attempts should be sustained with numerous procedures such as the following:

. Geo-referenced database downloading will inform terminals about the available radio-networks and the relevant radio-access parameters.

. Terminal will perform sensing and report to nodes and cognitive managers about the local radio spectrum.

. Terminals should perform geo-referenced access attempts that would involve systematic transmission of subscribers' locations in the early stages of the negotiation protocols

. Dedicated "beacon" signals such as DL/UL-CPC (Down Link and Up Link Cognitive Pilot Channel) should be broadcasted in order to support both downloading and sensing + channel sounding procedures within terminal and nodes. Network downloading and terminal embedded sensing should be based on a DL-CPC. Sensing information reporting and BS/node sensing should be based on the use of a UL-CPC signal. For simplification, both DL-CPC and UL-CPC should be designed for fast recognition, accurate measurements and easy decoding. Thus, they should be very weak regarding both passive and active threats.

4. EXISTING COUNTERMEASURES PRINCIPLES

4.1. Transec countermeasures.

Transmission Security (transec) is relevant to the protection of the wave form face to interception/direction finding of the transmitted radio signal, face to jamming of the user receiver, and face to intrusion attempts into the radio access protocol. Some transec technics are described hereafter:

Randomization of transmitted signals: this can be achieved
. with frequency hopping and time hopping of burst signals (RATs involving TDMA and TDD mechanism),
. with pseudo noise spreading (such as CDMA RATs),
. with random jitter and scrambling of midamble, of synchronization words and or pilots symbols (any RAT),
. by using long term pseudo-random schemes for modulation, coding, scrambling and interleaving of signaling and access messages, for allocation of traffic radio resource.

Use of furtive signals for supporting access protocol and traffic: for improving privacy of access of negotiation phase and of traffic allocation, transec often uses short duration messages that are randomly jittered within long protocol frames, progressive protected and acknowledged DL and UL exchanges for early device's identification, such as applied in the domain of Identification Friend and Foe (IFF).
Transec applies mainly at the radio interface and usually re-enforce advantages of propagation diversity. Moreover, with convenient adaptations, several characteristics of public RATs could provide some transec capabilities:
. TDMA standards could provide some transec if frequency hopped modes (FHM) were used over numerous channels. Unfortunately, FHM in public TDMA RATs are usually dedicated to frequency diversity and not to privacy.

. CDMA standards provide native protection in the UL sense when using a-synchronous long pseudo noise codes. Unfortunately, it dramatically decreases when low combinatory pilots symbols are present (3GPP), when system time reference is GPS (3GPP2) and when code allocation is terminal dependent (3GPP2 public mode).

. Complex data multiplex schemes within OFDM signals and associated RATs would provide transec protections if scattered pilots and signaling were more difficult to synchronize and to decode (DVB-T/H, LTE).

. Any adaptive MISO and MIMO RAT full duplex access schemes induce native space time diversity and randomness that could re-enforce propagation non-stationary effects and generate signal mixtures that provide intrinsic interferences at eavesdropper part.

4.2. Netsec countermeasures.
Network Transmission Security (netsec) is relevant to the protection of the signaling of the network (including the subcriber's part). Netsec applies either at the radio interface and at the medium access protocol layer, with request to upper protocol layers. Netsec techniques involve mainly transmitter authentication protocols, integrity control and ciphering of signaling and of negotiation messages. Severe netsec weaknesses exist in most of public wireless networks:
. Only few public wireless networks are able to protect and to control the integrity of the signaling messages that are broadcasted by BSs or nodes, same lacks apply to first paging messages sent by node and to first access messages sent by terminals.
. Many networks apply no authentication or single sense authentication only, because of standards lacks or because of sub-optimal operators' engineering.
.Ciphering procedures are usually initiated in the later part of the RAT procedure, thus after authentication and identification steps, whose data remain un-ciphered.
. Netsec failures are often re-enforced into multi-RATs terminals, especially when involving L-PCS RATs.

4.3. Comsec countermeasures.
Communication Security (comsec) is relevant to the protection of the content of the user messages (voice, data). Comsec applies at the radio interface and at upper layers. Comsec techniques involve ciphering and integrity control of users messages at several protocol layers and even at several interfaces when transmission relay occur (examples are point to point ciphering of each user data flux before multiplexing, ciphering of IP packets, of artery, etc.).
Native comsec capabilities of public wireless standards are controlled by legal authorities (key lengths are limited).
Native comsec failures exist in many standards and un-expected failures were pointed out exist in several cases. Examples above pointed out lacks of integrity control in many standards, security conception errors (Wifi, Bluetooth), un-expected publication of (initially secret) cipher algorithm (GSM), etc.

4.4. Elements about secure terminal architectures.
Information security modules (infosec) are dedicated to the generation of random data.
In most of wireless public standards, infosec modules exploit shared keys (that are present into SIM cards, into terminal -electronic serial numbers-, and/or into operators' databases), and they generate random parameters that are transmitted over the radio interface. These parameters initiate or acknowledge computations of keys at both node and terminal part. Usually these procedures start during the later stages of the negotiation protocol and the earlier data exchanges remain thus un-protected.
There exist too "source ciphered" handsets [7] [8] that improve comsec. Nevertheless, such handsets induce heavy constraints for operational use (limited set of subscribers) and they usually remain non-operant for transec and netsec.
In more secure terminal and node architectures, infosec is based on an initial shared secret and avoids dedicated exchanges. It provides several independent pseudo-random sequences to be followed by RATs, to be xorred with the data stream, to be added inside messages for integrity control, etc. Therefore, infosec apply very early in the negotiation protocol and it is placed at the core of the terminal architecture so that it is called for any security procedure and it cannot be shortcut.

4.5. Elements about secure military radios - relevant opportunities for privacy of public standards.

Military communications usually use advanced transec netsec and comsec protections that are managed with transverse infosec modules, secret system time reference and a priori secret information that are shared over terminals and nodes. For example data bases are pre-computed and implanted into terminals and nodes that are relevant to frequency plans, to pseudo random sequences, to transec netsec and comsec keys, etc. Nevertheless, massive sharing of a priori secret information remains a major difficulty: even with medium number of terminal and nodes, this induces strong system constraints, mission preparation, etc.

Thus, in order to transpose some of privacy concepts from military communication skills to public worldwide mass market standards, there are strong needs for shared and private random sources. Physec solutions introduced in § 5 are expected to provide suitable alternatives for that.

4.6. Risk analysis and risk-driven security metrics

Systematic methods such as security metrics development and management are needed to be able to develop sufficient security and privacy countermeasures for physic (see §5). A high-quality risk analysis is the starting point of all security work and its results set the reference level for security metrics. The reference requirements used in security and privacy are either based on (i) security risk, or (ii) best practices and regulations. The former category assumes direct availability of risk analysis results, while the latter does not. To some extent, security can be managed with the help of best practices, but the lack of risk knowledge could result in costly and incorrect security countermeasures.

Security metrics can be used to reason about the effectiveness of countermeasures, to support configuration management and to show compliance to security and privacy regulations and legislation. Security metrics should be based on the prioritized collection of security risks, making them risk-driven. A security metrics development approach based on hierarchical decomposition of security objectives was introduced in [27].

5. PERSPECTIVES OFFERED BY PHYSICAL LAYER SECURITY (PHYSEC)

Physec concepts take advantage of the physical characteristics radio-environments, especially when complex, dispersive and non-stationary, and try to take the benefit of radio propagation parameters that have to be measured by infrastructures and handsets for the purpose of their proper communication services [34][36]. Nowadays, the relevant information is used for equalization in FDMA and TDMA RATs, for RAKE processing in CDMA RATs, for adaptive modulation/coding schemes in MIMO RATs, for interference mitigation in full duplex RATs [6]. Sensing procedures and opportunistic spectrum access within cognitive radios are other opportunities for privacy improvements. Finally, any intrinsic physical randomness, especially when measured by legitimate links during access attempts and established calls, should contribute to security the air interface, with low impact at upper layer and no constraints at other network interfaces (Abis, A).

. Dedicated coding schemes (secrecy codes) were proven to provide intrinsic secrecy of legitimate radio link facing passive eavesdropper (fig 4), when better radio quality is achieved for the legitimate [34]. Roughly, secrecy codes mitigate the information about the legitimate link at any radio-eavesdropper location, up to a given "secrecy capacity" ($C_{sec,AB}$). In general, secrecy capacity is (of course) less than the legitimate Shannon capacity and greater than the Shannon capacity difference of the legitimate and of the eavesdropper link: $0 \leq C_{sh,AB} - C_{sh,AE} \leq C_{sec,AB} \leq C_{sh,AB}$.

. Secrecy codes could be merged with advanced RATs that generate signal mixtures in order to disturb Eve: MISO and MIMO, artificial jamming [34], full duplex techniques [6].

. Diverse non-stationary artificial random source facilitate transec (versatile allocation of traffic resource, adaptive changes of modulation and coding etc.), thus making interception, eavesdropping and spoofing more complex.

. Propagation-dependent random sources are added value for generation of secret keys, of control pattern, etc. especially when combined with existing comsec schemes.

. In order to enhance security of access phases, early identification procedures should be designed by using weak/furtive low data rates signal that would be mixed with strong signals that are already broadcasted [11], before terminal's dedicated (and protected) signaling is made intelligible for further access attempts.

6. CONCLUSION

In this paper, we illustrated several security lacks of civilian wireless networks and relevant passive and active attacks at the radio interface that may dramatically deteriorate both subscribers' privacy and security and operators' confidence, especially when focusing on signaling, on first radio access attempts and on negotiation phases.

By considering realistic radio environments, existing counter-measures and secure terminal architectures, we pointed out that large perspectives exist for significant privacy upgrades by merging traditional privacy techniques, secrecy coding and other physec concepts.

The core idea is to combine high combinatory channel codes, advanced modulation schemes and traditional countermeasures in order:

- To trend toward secrecy capacity
- To take the maximal benefit of adverse radio environments that are often encountered by eavesdropper and by RHS.

These concepts largely exploit new randomness sources and propagation advantages that are measured and/or generated locally by legitimate communications nodes and terminals for their proper communication services. Complements about principles, theoretic advantages and practical expectations for wireless networks privacy can be found in [35] and deeper explanations are given in [34] .

We conjecture that introducing physec-privacy concepts into wireless public standards should be particularly efficient:

. For access attempts and negotiation phases in general

. For downloading/uploading procedures within CRs

. During established call: upgrade of current cipher schemes.

We are confident that current national and European research programs will establish convincing feasibility proofs in the future years, thus preparing standardization and industrial development of trustworthy and full-secure RATs.

7. REFERENCES

[1] www.3GPP.org

[2] www.3GPP2.org

[3] http://standards.ieee.org/findstds/standard/1900.6-2011.html

[4] https://standards.ieee.org/findstds/standard/1900.4a-2011.html

[5] J. Mittola: Conference "Secure Geospatial Dynamic Spectrum Access". GDR ISiS Telecom Paris tech 9 Mai 2011.

[6] "Full Duplex Radios for Local Access" EU EU FP7-ICT 316369. URL: http://www.fp7-duplo.eu

[7] URL: http://www.cryptophone.de/en/products/mobile/cp400/

[8] URL: http://www.defense.gouv.fr/dga/actualite/la-dga-livre-les-premiers-telephones-teorem

[9] Y. S Shiu and al. Physical Layer Security: a tutorial in IEEE Wireless Communications • April 2011

[10] Procédé « protocole orienté » de traitement des signaux stationnaires, partiellement stationnaires, ou cyclo-stationnaires, patent Thales FR 10.05017, PCT/EP2011/073420 WO2012.084956

[11] Procédé de taggage radio-électrique des signaux de brouilleurs et d'autres émetteurs. Patent Thales FR 12.03071

[12] Patent Rohde and Schwarz EP 1051 053 B1

[13] Method of controlling and analysing communications in a telephone network. Patents Thales FR 04.04043, PCT WO 2005/112497 A1

[14] R. Gautier, G. Burel, J. Letessier and O. Berder « Blind estimation of Scrambler offset using encoder redundancy », in IEEE 2002

[15] URL: http://fr.wikipedia.org/wiki/Wi-Fi_Protected_Access

[16] http://web.archive.org/web/20090318143444/http://www.scard.org/gsm/a3a8.txt http://cryptome.org/gsm-a512.htm (Originally on www.scard.org),.

[17] E. Biham, O. Dunkelman, Cryptanalysis of the A5/1 GSM Stream Cipher, Progress in Cryptology, proceedings of Indocrypt'00, Lecture Notes in Computer Science 1977, Springer-Verlag, pp. 43-51, 2000

[18] Shahriar, C., Sodagari, S. & Clancy, T.C. Physical-layer security challenges of DSA-enabled TD-LTE. Proceedings of the 4th Int. Conf. on CRadio and Advanced SM. Barcelona, Spain, New York, NY, USA: ACM, 2011. CogART '11. pp. 40:1.

[19] R. Miller, W. Trappe ; "On the Vulnerabilities of CSI in MIMO Wireless Communication Systems » IEEE Tran. on Mobile Computing, Vol. 11, N°. 8, August 2012

[20] Sodagari, S. & Clancy, T.C. Efficient jamming attacks on MIMO channels. IEEE (ICC) 2012. p. 852.

[21] Ruiliang Chen, Jung-Min Park & Reed, J.H. Defense against Primary User Emulation Attacks in Cognitive Radio Networks. Selected Areas in Com., IEEE Journal 2008, Vol. 26-1, pp. 25-37.

[22] Kune, D.F., Koelndorfer, J., Hopper, N. & Kim, Y. Location leaks on the GSM air interface. Network & Distributed System Security Symposium (NDSS). 2012.

[23] Ta, T. & Baras, J.S. Enhancing Privacy in LTE Paging System Using Physical Layer Identification. Teoksessa: Pietro, R., Herranz, J., Damiani, E. & State, R. (eds.).September 13-14, 2012. Vol. 7731. Springer Berlin Heidelberg, 2013. Lecture Notes in Computer Science. p. 15.

[24] Vintila, C., Patriciu, V. & Bica, I. Security Analysis of LTE Access Network. 10th Int. Conf. on Networks (ICN 2011). 2011. p. 29.

[25] Hyeran Mun, Kyusuk Han & Kwangjo Kim 3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA. WTS 2009. p. 1.

[26] Bikos, A.N. & Sklavos, N. LTE/SAE Security Issues on 4G Wireless Networks. Security & Privacy, IEEE 2013, Vol. 11, No. 2, pp. 55-62.

[27] Savola, R. and Abie, H., Development of measurable security for a distributed messaging system, *Int. Journal on Advances in Security*, Vol. 2, No. 4, 2009, pp. 358–380.

[28] NSA National Security Agency, Bluetooth Security, URL: http://www.nsa.gov/ia/_files/factsheets/I732-016R-07.pdf

[29] Padgette J., Scarfone K., Guide to Bluetooth Sec., NIST, 2011.

[30] Bluetooth Vulnerability Assessment Technical Publication ITSPSR-17A, Communications Security Establishment Canada, 06/2008.

[31] Bowers B., ZigBee Wireless Sec. 2012: A New Age Penetration Tester's Toolkit. URL: http://www.ciscopress.com/articles/article.asp?p=1823368,.

[32] Vidgre and al. Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lesson Learned.: 46th IEEE Hawaii Int. Conf. on System Sciences, 2012, pp. 5130-5136.

[33] KillerBee, URL: http://code.google.com/p/killerbee/

[34] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge University Press, 2011

[35] Procédé d'optimisation de la planification dans un système de communications de type CDMA Patent Thales FR 04.01475.

[36] J.C. Belfiore, A. Sibille, C. Ling, F. Delaveau, E Garrido ; "Physec Concepts for Wireless Public Networks, introduction, state of the art, perspectives" Winncomm 2013, Munich.