Mobile technology

Mobile Station/User Equipment (MS/UE)

CDR (Call Detail Records)

BlueTooth

RFID/NFC

Mobile infrastructure

Mobile security

Obtaining IP/position (1/3)

- Question to carrier/operator how it is done...
- Normally I get a initial mail from some police officer where they ask if they have come to the right place
- I then ask them for a written document which will show if they got the right to view the information, i.e. nothing is reported over the phone etc...
  - You can however begin to extract information but not deliver anything yet...
- The CDRs (Call Detail Records) are stored for a certain time
  - Decided by law since 1 may 2012 – min 6 and max 24 months
  - http://www.idg.se/2.1085/1.441822/har-ar-all-trafikdata-som-ska-lagras
  - http://sv.wikipedia.org/wiki/Datalagringsdirektivet
- In practice the CDRs are stored until the bill is sent to the customer (before datalagringsdirektivet), or 6 months, or
  - If it is needed for technical support or serching for system errors
  - If one depersonalise data from personal information one can save data without restrictions

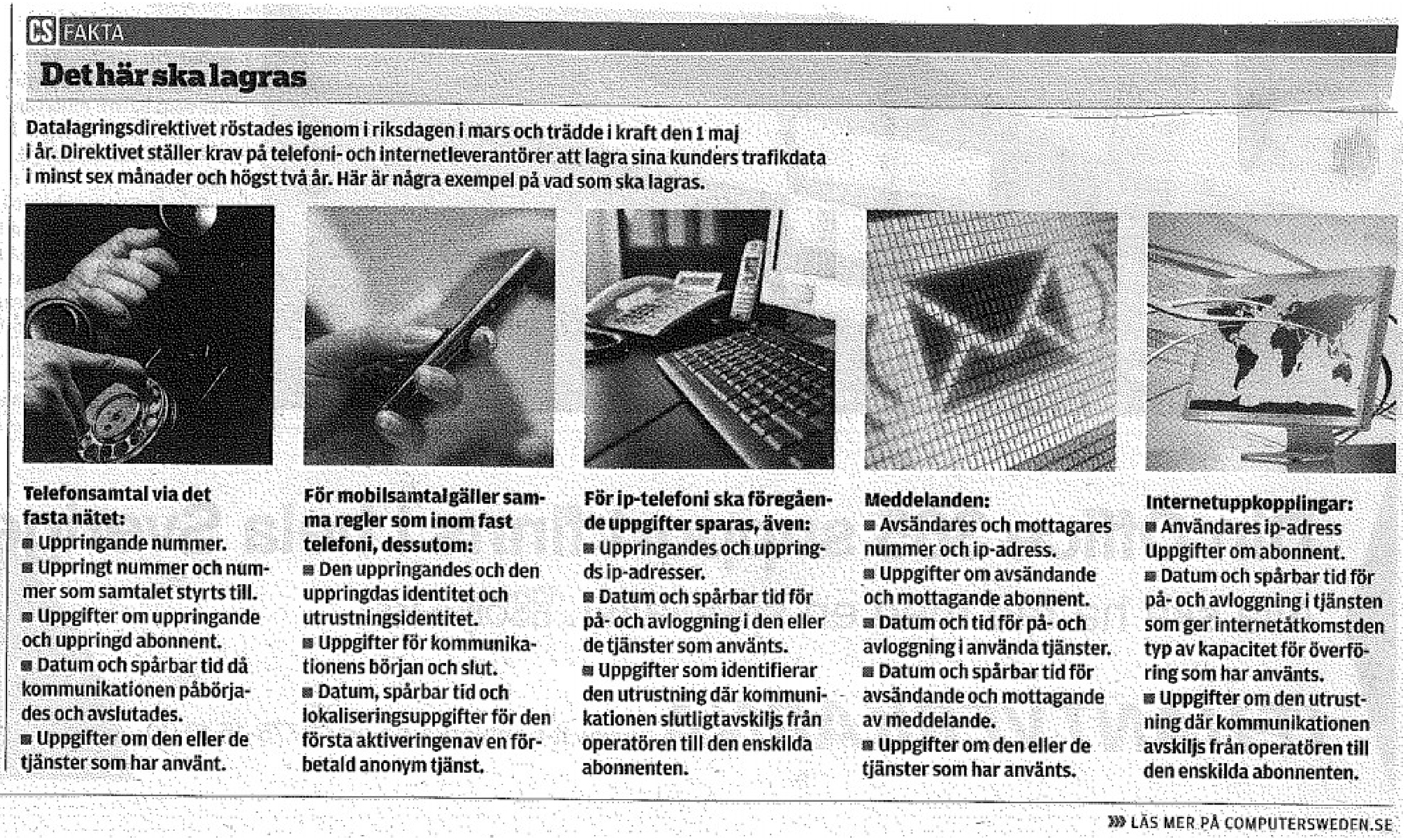
Obtaining IP/position (2/3)

- A CDR contains a lot of information, examples are
  - Calling and receiving number
  - Type
  - Time stamp och lenght (Start/Interim reports/Stop)
  - The customers IP address
  - And about maybe 50 - 60 more parameters...
- What is important for us when we do the trace is that it must be correct
  - I usually ask some control questions to the police/authority about the case
    - IP address
    - Time stamps for events
    - Geographical position
    - And so on... (note that its common with errors in the documents you get from the police...)

Obtaining IP/position (3/3)

- A trace gives a more reliable result if one can track the MS or UE at several separate occasions
  - If it is possible to find several CDRs that points to the same IMSI/IMEI (or ESN) it increase the probability that you found the right customer in the system
- If one get an approximately geographical position one can also check that there is some plausability that a MS/UE is located in for example Göteborg
  - If the customer lives in Kiruna it may be wrong... On the other hand if the customer lives in Göteborg the probability is high...
- ESN (Electronic Serial Number)
  - Corresponds to IMEI in the CDMA standard
  - http://en.wikipedia.org/wiki/Electronic_Serial_Number
- More about CDR
  - http://en.wikipedia.org/wiki/Call_detail_record
  - http://en.wikipedia.org/wiki/Internet_Protocol_Detail_Record

Datalagringsdirektivet - 1 maj 2012



CS FAKTA

Det här ska lagras

Datalagringsdirektivet röstades igenom i riksdagen i mars och trädde i kraft den 1 maj i år. Direktivet ställer krav på telefoni- och internetleverantörer att lagra sina kunders trafikdata i minst sex månader och högst två år. Här är några exempel på vad som ska lagras.

Telefonsamtal via det fasta nätet:

- Uppringande nummer.
- Uppringt nummer och nummer som samtalet styrts till.
- Uppgifter om uppringande och uppringd abonnent.
- Datum och spårbar tid då kommunikationen påbörjades och avslutades.
- Uppgifter om den eller de tjänster som har använt.

För mobilsamtalgäller samma regler som inom fast telefoni, dessutom:

- Den uppringandes och den uppringdas identitet och utrustningsidentitet.
- Uppgifter för kommunikationens början och slut.
- Datum, spårbar tid och lokaliseringsuppgifter för den första aktiveringenav en förbetald anonym tjänst.

För ip-telefoni ska föregående uppgifter sparas, även:

- Uppringandes och uppringds ip-adresser.
- Datum och spårbar tid för på- och avloggning i den eller de tjänster som använts.
- Uppgifter som identifierar den utrustning där kommunikationen slutligtavskiljs från operatören till den enskilda abonnenten.

Meddelanden:

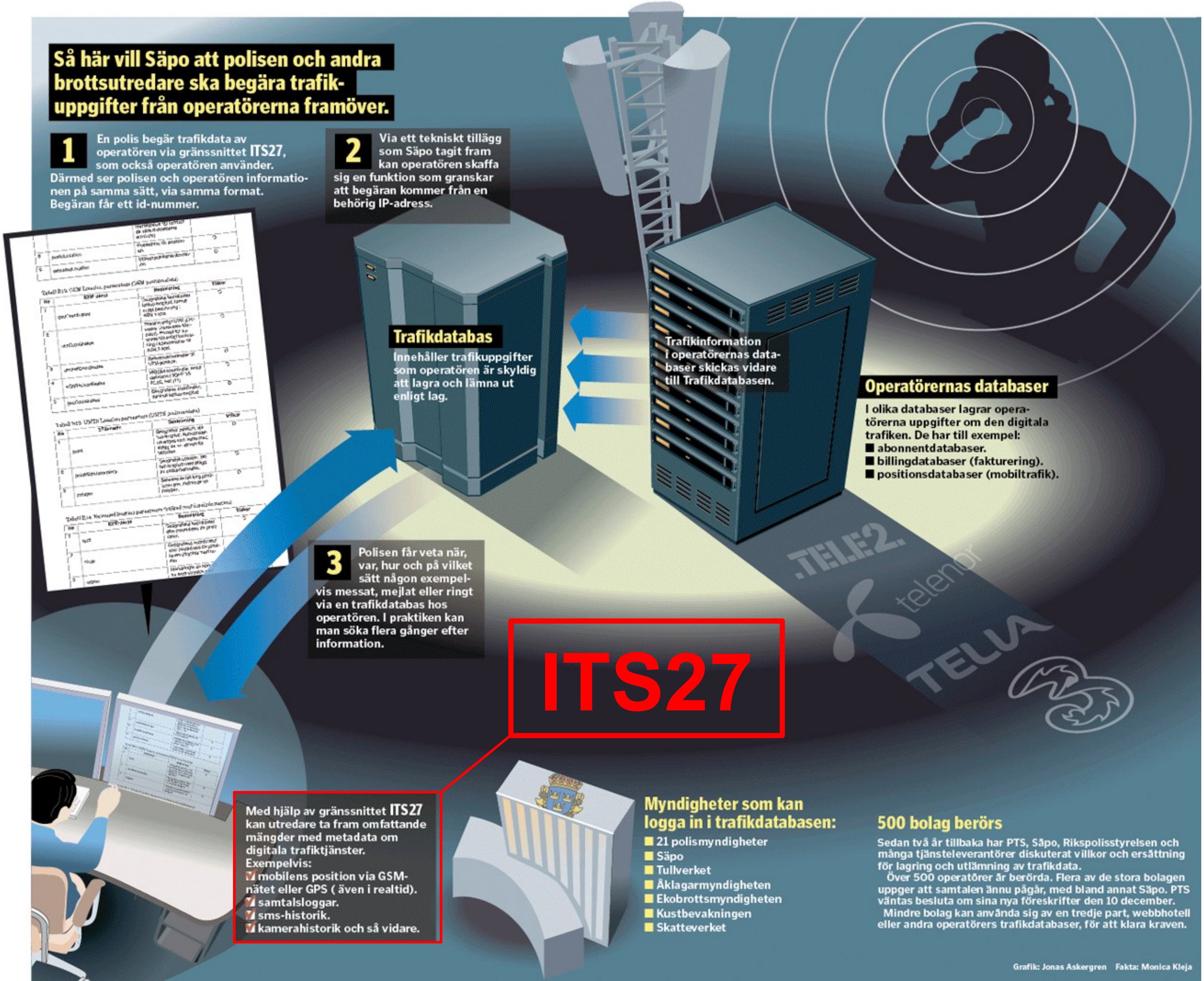
- Avsändares och mottagares nummer och ip-adress.
- Uppgifter om avsändande och mottagande abonnent.
- Datum och tid för på- och avloggning i använda tjänster.
- Datum och spårbar tid för avsändande och mottagande av meddelande.
- Uppgifter om den eller de tjänster som har använts.

Internetuppkopplingar:

- Användares ip-adress Uppgifter om abonnent.
- Datum och spårbar tid för på- och avloggning i tjänsten som ger internetåtkomstden typ av kapacitet för överföring som har använts.
- Uppgifter om den utrustning där kommunikationen avskiljs från operatören till den enskilda abonnenten.

»» LÄS MER PÅ COMPUTERSWEDEN.SE

http://computersweden.idg.se/2.2683/1.441822/har-ar-all-trafikdata-som-ska-lagras



Så här vill Säpo att polisen och andra brottsutredare ska begära trafikuppgifter från operatörerna framöver.

1 En polis begär trafikdata av operatören via gränssnittet **ITS27**, som också operatören använder. Därmed ser polisen och operatören informationen på samma sätt, via samma format. Begäran får ett id-nummer.

2 Via ett tekniskt tillägg som Säpo tagit fram kan operatören skaffa sig en funktion som granskar att begäran kommer från en behörig IP-adress.

Trafikdatabas

Innehåller trafikuppgifter som operatören är skyldig att lagra och lämna ut enligt lag.

Trafikinformation i operatörernas databaser skickas vidare till Trafikdatabasen.

Operatörernas databaser

I olika databaser lagrar operatörerna uppgifter om den digitala trafiken. De har till exempel:

- abonnentdatabaser.
- billingdatabaser (fakturering).
- positionsdatabaser (mobiltrafik).

3 Polisen får veta när, var, hur och på vilket sätt någon exempelvis messat, mejlat eller ringt via en trafikdatabas hos operatören. I praktiken kan man söka flera gånger efter information.

Med hjälp av gränssnittet **ITS27** kan utredare ta fram omfattande mängder med metadata om digitala trafiktjänster.
Exempelvis:
☑ mobilens position via GSM-nätet eller GPS (även i realtid).
☑ samtalsloggar.
☑ sms-historik.
☑ kamerahistorik och så vidare.

Myndigheter som kan logga in i trafikdatabasen:

- 21 polismyndigheter
- Säpo
- Tullverket
- Åklagarmyndigheten
- Ekobrottsmyndigheten
- Kustbevakningen
- Skatteverket

500 bolag berörs

Sedan två år tillbaka har PTS, Säpo, Rikspolisstyrelsen och många tjänsteleverantörer diskuterat villkor och ersättning för lagring och utlämning av trafikdata.

Över 500 operatörer är berörda. Flera av de stora bolagen uppger att samtalen ännu pågår, med bland annat Säpo. PTS väntas besluta om sina nya föreskrifter den 10 december.

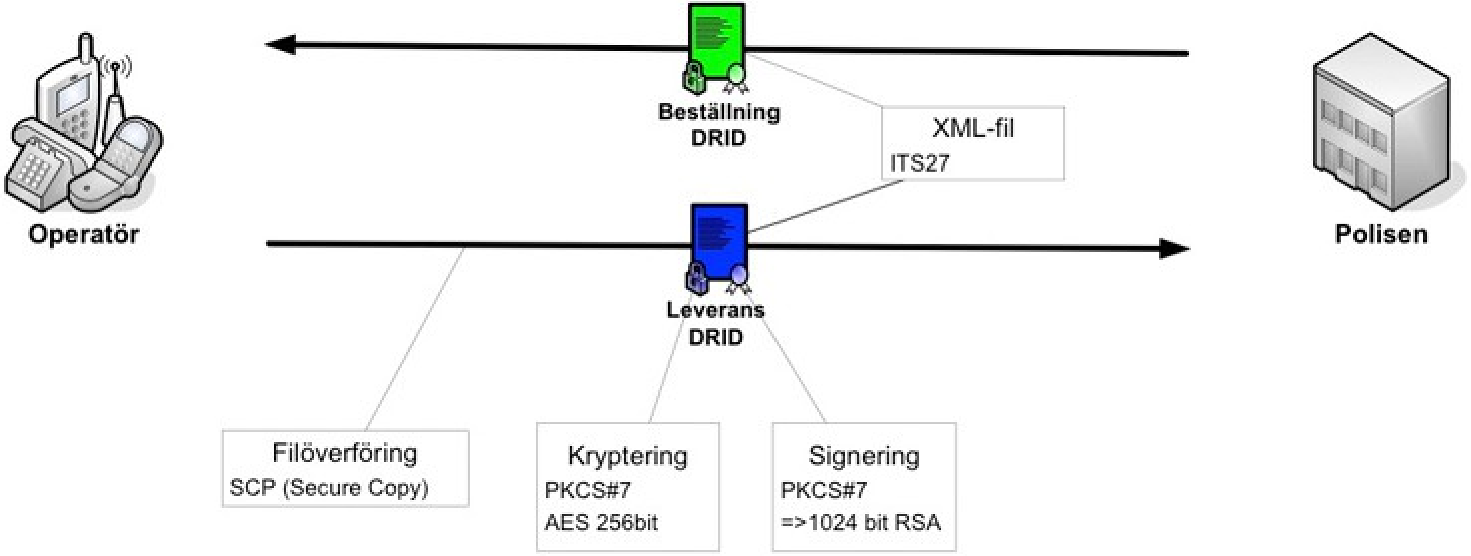
Mindre bolag kan använda sig av en tredje part, webbhotell eller andra operatörers trafikdatabaser, för att klara kraven.

Grafik: Jonas Askergren Fakta: Monica Kleja

ITS27 (förslag dec 2013)

Överföring

2 minuters turnaround time - LEK (Lagen om Elektronisk Kommunikation)



Operatör

Beställning
DRID

XML-fil
ITS27

Polisen

Leverans
DRID

Filöverföring
SCP (Secure Copy)

Kryptering
PKCS#7
AES 256bit

Signering
PKCS#7
=>1024 bit RSA

ITS 27 specifikation

http://sverigesradio.se/diverse/appdata/isidor/files/83/13900.pdf

Artiklar

http://www.nyteknik.se/nyheter/it_telekom/allmant/article3784822.ece

http://www.nyteknik.se/nyheter/it_telekom/allmant/article3788288.ece

Call Detail Records

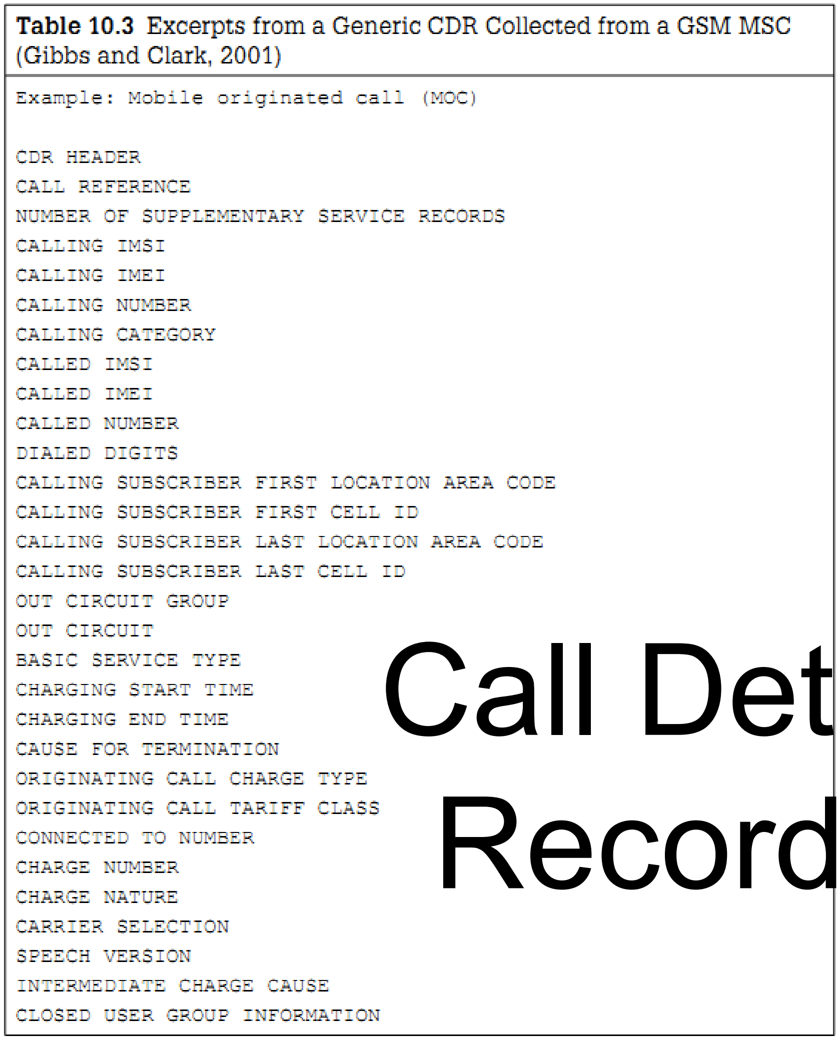


Table 10.3 Excerpts from a Generic CDR Collected from a GSM MSC (Gibbs and Clark, 2001)

```
Example: Mobile originated call (MOC)

CDR HEADER
CALL REFERENCE
NUMBER OF SUPPLEMENTARY SERVICE RECORDS
CALLING IMSI
CALLING IMEI
CALLING NUMBER
CALLING CATEGORY
CALLED IMSI
CALLED IMEI
CALLED NUMBER
DIALED DIGITS
CALLING SUBSCRIBER FIRST LOCATION AREA CODE
CALLING SUBSCRIBER FIRST CELL ID
CALLING SUBSCRIBER LAST LOCATION AREA CODE
CALLING SUBSCRIBER LAST CELL ID
OUT CIRCUIT GROUP
OUT CIRCUIT
BASIC SERVICE TYPE
CHARGING START TIME
CHARGING END TIME
CAUSE FOR TERMINATION
ORIGINATING CALL CHARGE TYPE
ORIGINATING CALL TARIFF CLASS
CONNECTED TO NUMBER
CHARGE NUMBER
CHARGE NATURE
CARRIER SELECTION
SPEECH VERSION
INTERMEDIATE CHARGE CAUSE
CLOSED USER GROUP INFORMATION
```

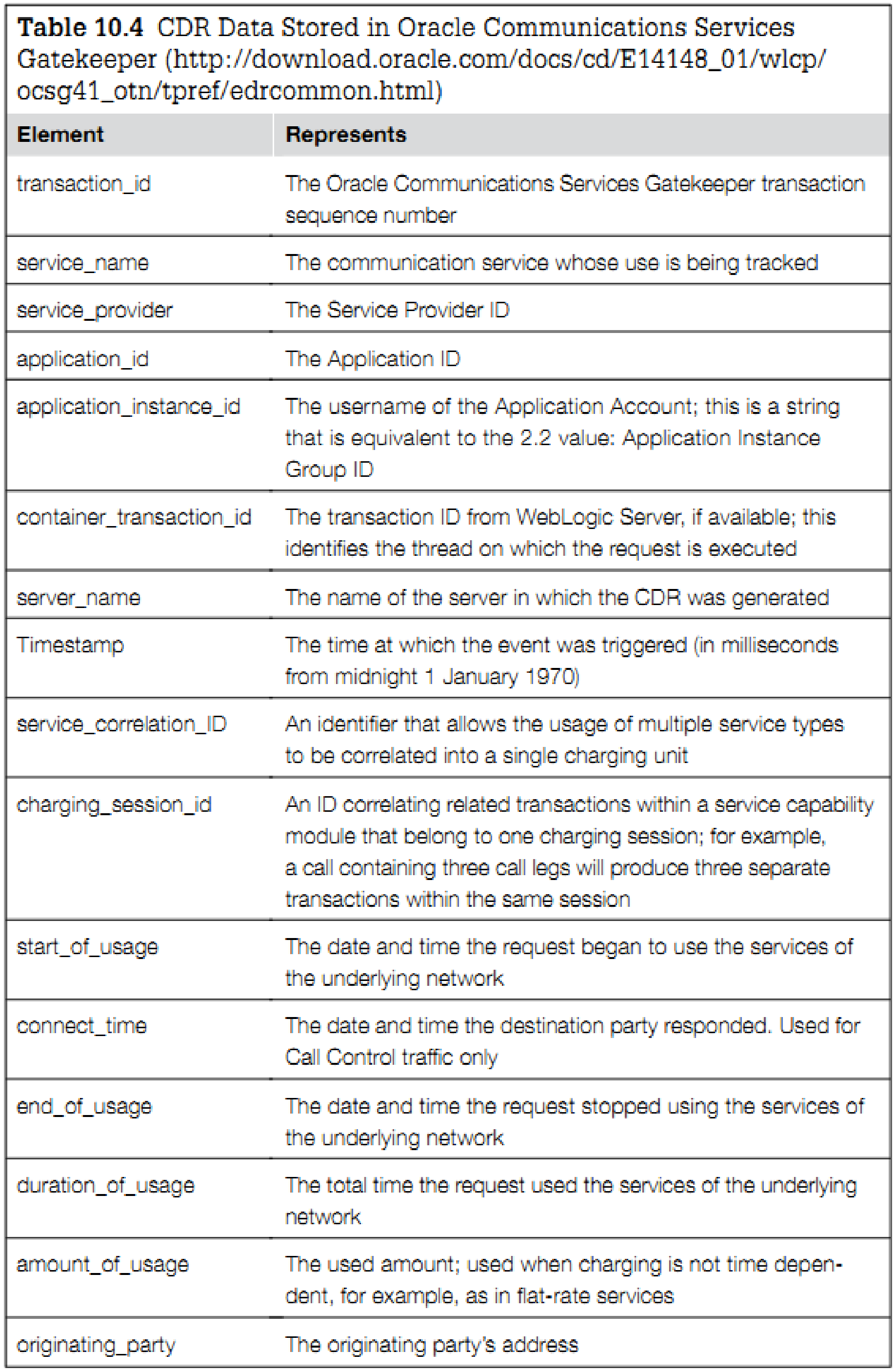
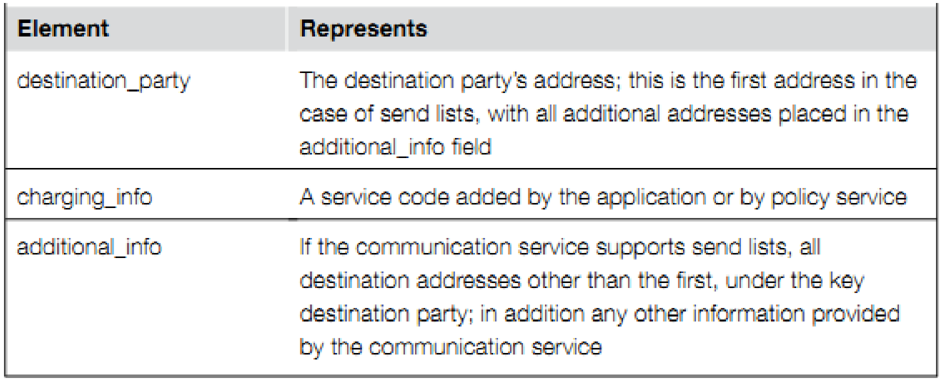


Table 10.4 CDR Data Stored in Oracle Communications Services Gatekeeper (http://download.oracle.com/docs/cd/E14148_01/wlcp/ocsg41_otn/tpref/edrcommon.html)

Element	Represents
transaction_id	The Oracle Communications Services Gatekeeper transaction sequence number
service_name	The communication service whose use is being tracked
service_provider	The Service Provider ID
application_id	The Application ID
application_instance_id	The username of the Application Account; this is a string that is equivalent to the 2.2 value: Application Instance Group ID
container_transaction_id	The transaction ID from WebLogic Server, if available; this identifies the thread on which the request is executed
server_name	The name of the server in which the CDR was generated
Timestamp	The time at which the event was triggered (in milliseconds from midnight 1 January 1970)
service_correlation_ID	An identifier that allows the usage of multiple service types to be correlated into a single charging unit
charging_session_id	An ID correlating related transactions within a service capability module that belong to one charging session; for example, a call containing three call legs will produce three separate transactions within the same session
start_of_usage	The date and time the request began to use the services of the underlying network
connect_time	The date and time the destination party responded. Used for Call Control traffic only
end_of_usage	The date and time the request stopped using the services of the underlying network
duration_of_usage	The total time the request used the services of the underlying network
amount_of_usage	The used amount; used when charging is not time dependent, for example, as in flat-rate services
originating_party	The originating party's address



Element	Represents
destination_party	The destination party's address; this is the first address in the case of send lists, with all additional addresses placed in the additional_info field
charging_info	A service code added by the application or by policy service
additional_info	If the communication service supports send lists, all destination addresses other than the first, under the key destination party; in addition any other information provided by the communication service

Lawful Interception Reports

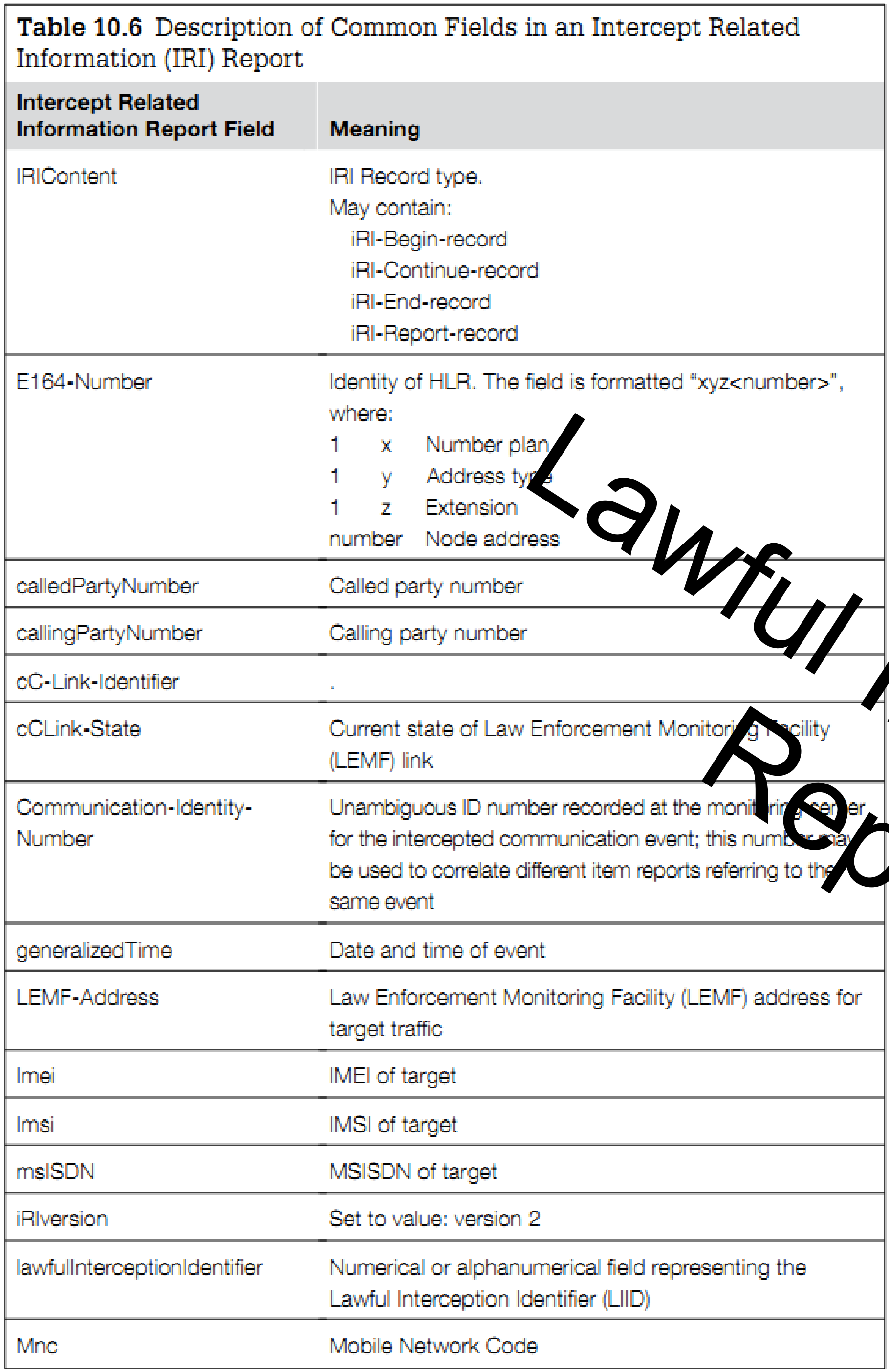


Table 10.6 Description of Common Fields in an Intercept Related Information (IRI) Report

Intercept Related Information Report Field	Meaning
IRIContent	IRI Record type. May contain: iRI-Begin-record iRI-Continue-record iRI-End-record iRI-Report-record
E164-Number	Identity of HLR. The field is formatted "xyz<number>", where: 1 x Number plan 1 y Address type 1 z Extension number Node address
calledPartyNumber	Called party number
callingPartyNumber	Calling party number
cC-Link-Identifier	.
cCLink-State	Current state of Law Enforcement Monitoring Facility (LEMF) link
Communication-Identity-Number	Unambiguous ID number recorded at the monitoring center for the intercepted communication event; this number may be used to correlate different item reports referring to the same event
generalizedTime	Date and time of event
LEMF-Address	Law Enforcement Monitoring Facility (LEMF) address for target traffic
Imei	IMEI of target
Imsi	IMSI of target
msISDN	MSISDN of target
iRIversion	Set to value: version 2
lawfulInterceptionIdentifier	Numerical or alphanumerical field representing the Lawful Interception Identifier (LIID)
Mnc	Mobile Network Code

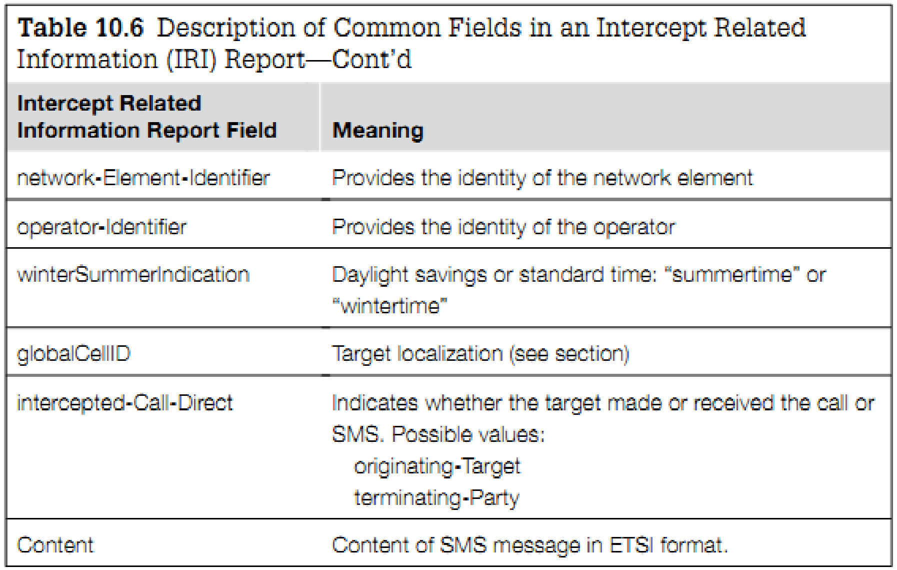


Table 10.6 Description of Common Fields in an Intercept Related Information (IRI) Report—Cont'd

Intercept Related Information Report Field	Meaning
network-Element-Identifier	Provides the identity of the network element
operator-Identifier	Provides the identity of the operator
winterSummerIndication	Daylight savings or standard time: "summertime" or "wintertime"
globalCellID	Target localization (see section)
intercepted-Call-Direct	Indicates whether the target made or received the call or SMS. Possible values: originating-Target terminating-Party
Content	Content of SMS message in ETSI format.

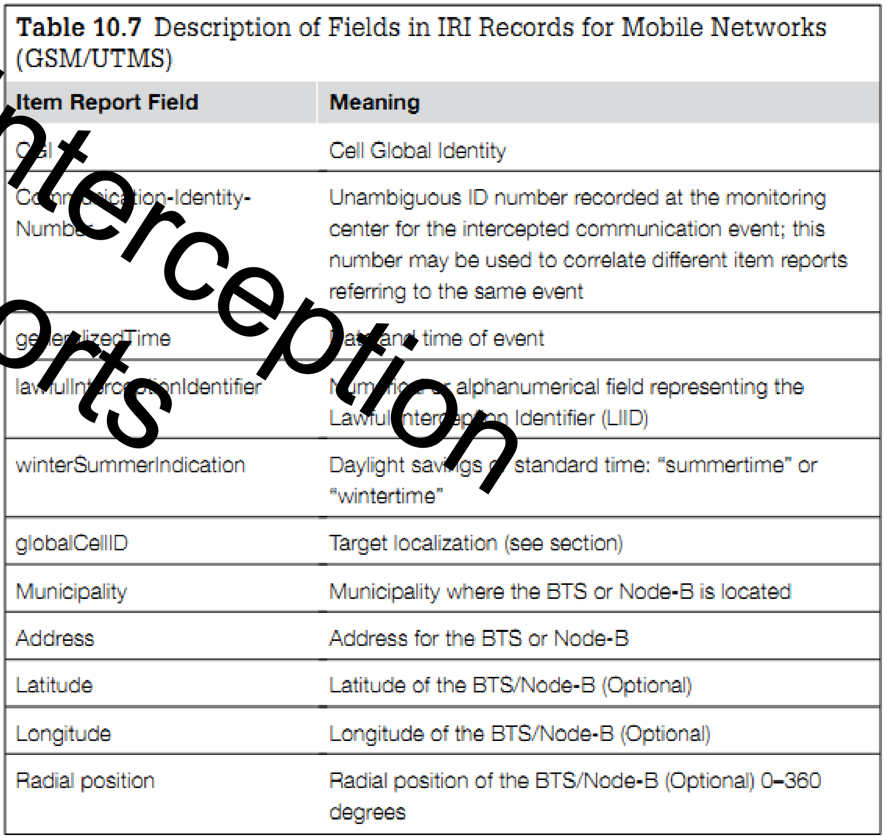


Table 10.7 Description of Fields in IRI Records for Mobile Networks (GSM/UTMS)

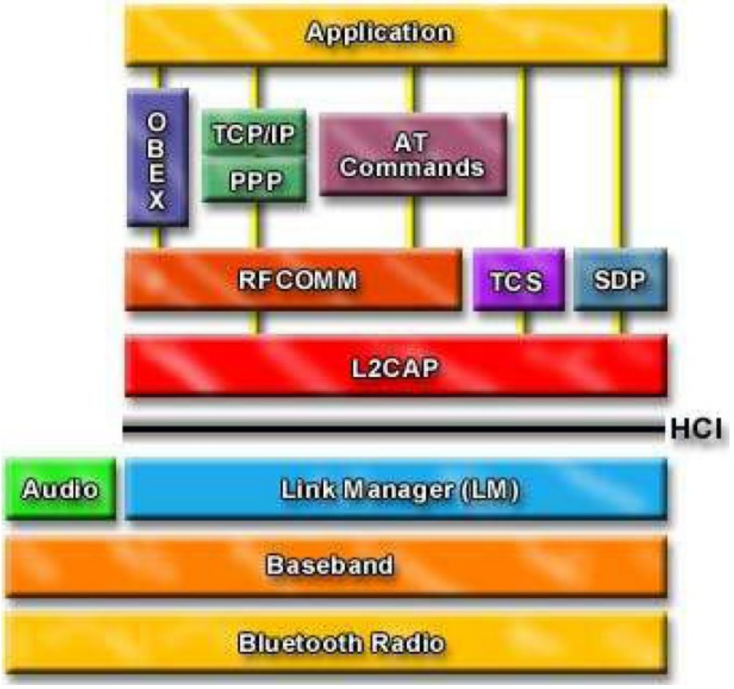
Item Report Field	Meaning
CGI	Cell Global Identity
Communication-Identity-Number	Unambiguous ID number recorded at the monitoring center for the intercepted communication event; this number may be used to correlate different item reports referring to the same event
generalizedTime	Date and time of event
lawfulInterceptionIdentifier	Numerical or alphanumerical field representing the Lawful Interception Identifier (LIID)
winterSummerIndication	Daylight savings or standard time: "summertime" or "wintertime"
globalCellID	Target localization (see section)
Municipality	Municipality where the BTS or Node-B is located
Address	Address for the BTS or Node-B
Latitude	Latitude of the BTS/Node-B (Optional)
Longitude	Longitude of the BTS/Node-B (Optional)
Radial position	Radial position of the BTS/Node-B (Optional) 0–360 degrees

Bluetooth stack

- Purpose - Get rid of the cable
- BT networks may be formed ad hoc and dynamically when near each other (if paired)
- Short range radio 2.45-gigahertz ISM (Industrial, Scientific, and Medical) frequency band, allowing for unlicensed operation worldwide
- PAN (Personal Area Network)
  - Discovery
  - Client activities
  - Server activities
  - Peer activities (both above)
- HCI = Host Controller Interface
- TCS, usually referred to as TCP (Telephony Control Protocol)

Host stack (SW)

Controller stack (HW)



ACL and L2CAP

http://en.wikipedia.org/wiki/Bluetooth_protocols

CS

- ACL (Asynchronous Connection-Less) communications link
  - The normal type of radio link used for framed data packets using a polling TDMA scheme at the Link Manager (LM) level
    - It can carry several different packet types uni- and bidirectional and is fault tolerant
- SCO (Synchronous Connection Orientated) stream format for voice

HS

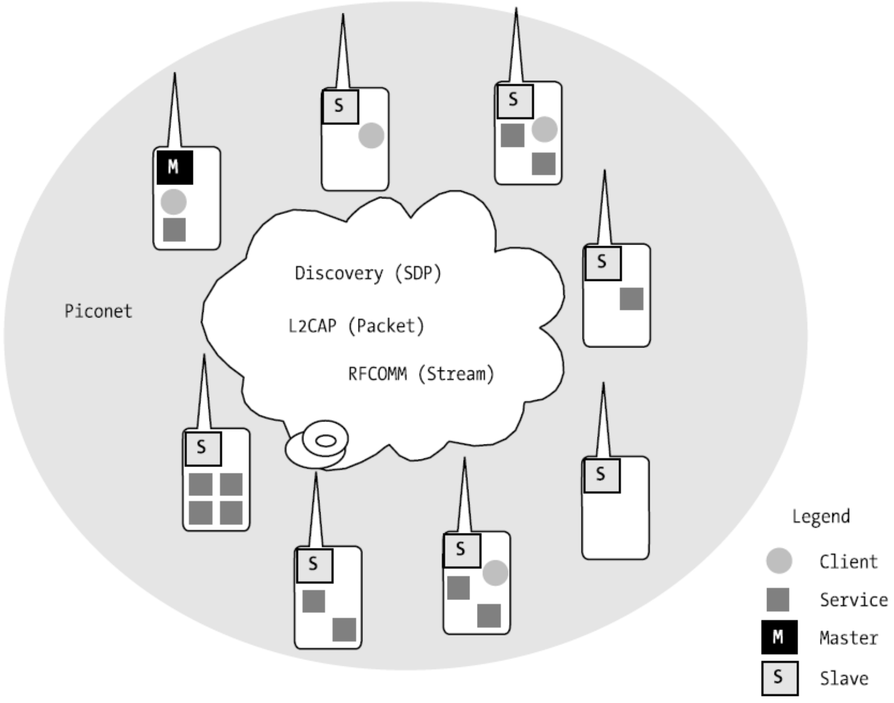
- L2CAP (Logical Link Control and Adaptation Protocol)
  - L2CAP is used within the host stack (OS built in or installable package). It passes packets to either the Host Controller Interface (HCI) or on a hostless system, directly to the Link Manager (LM)
  - L2CAP's functions include
    - Multiplexing data between different higher layer protocols
    - Segmentation and reassembly of packets
    - Providing one-way transmission management of multicast data to a group of other bluetooth devices
    - Quality of service (QoS) management for higher layer protocols
  - L2CAP is used to communicate packets **over the host ACL link**

L2CAP bound protocols

http://en.wikipedia.org/wiki/Bluetooth_protocols

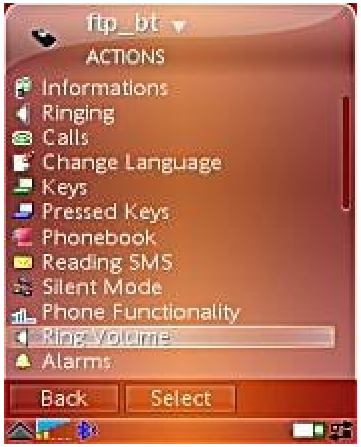
HS

- SDP (Service Discovery Protocol)
  - Determine which Bluetooth profiles that are supported
  - Each service/profile is identified with an UUID 16 number
    - For example: Serial Port (SPP)
- RFCOMM (Radio Frequency Communication)
  - Provides serial port emulation
  - OBEX (OBject EXchange)
    - As HTTP with support for sessions and binary transmissions
- Bluetooth Piconet
  - 1 master and up to 7 slaves (more if bridged)
  - One device can (at the same time)
    - Offer multiple services
    - Be master and slave
  - Devices are UUID 128 identified

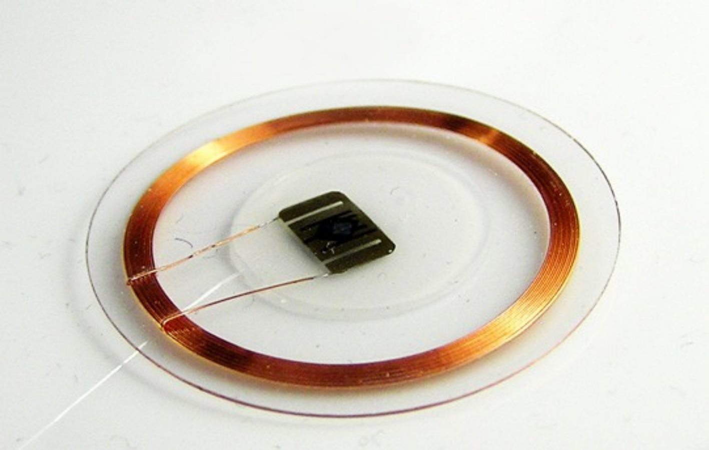


Bluetooth attacks

- The BlueSnarf attack
  - It is possible on some handset makers to connect and get IMEI and PIM data without the users knowledge
- The Backdoor attack
  - Full memory backup from previously paired device
- The BlueBug attack
  - Gaining access to the AT command set via a serial port profile for further attacks
- Bluejacking
  - Send unsolicited messages with OBEX using the name field
  - Fool users to connect using long ”name”, up to 248 chars
- Bluejacking Tools
  - http://www.bluejackingtools.com/downloads/
  - BT INFO 1.08

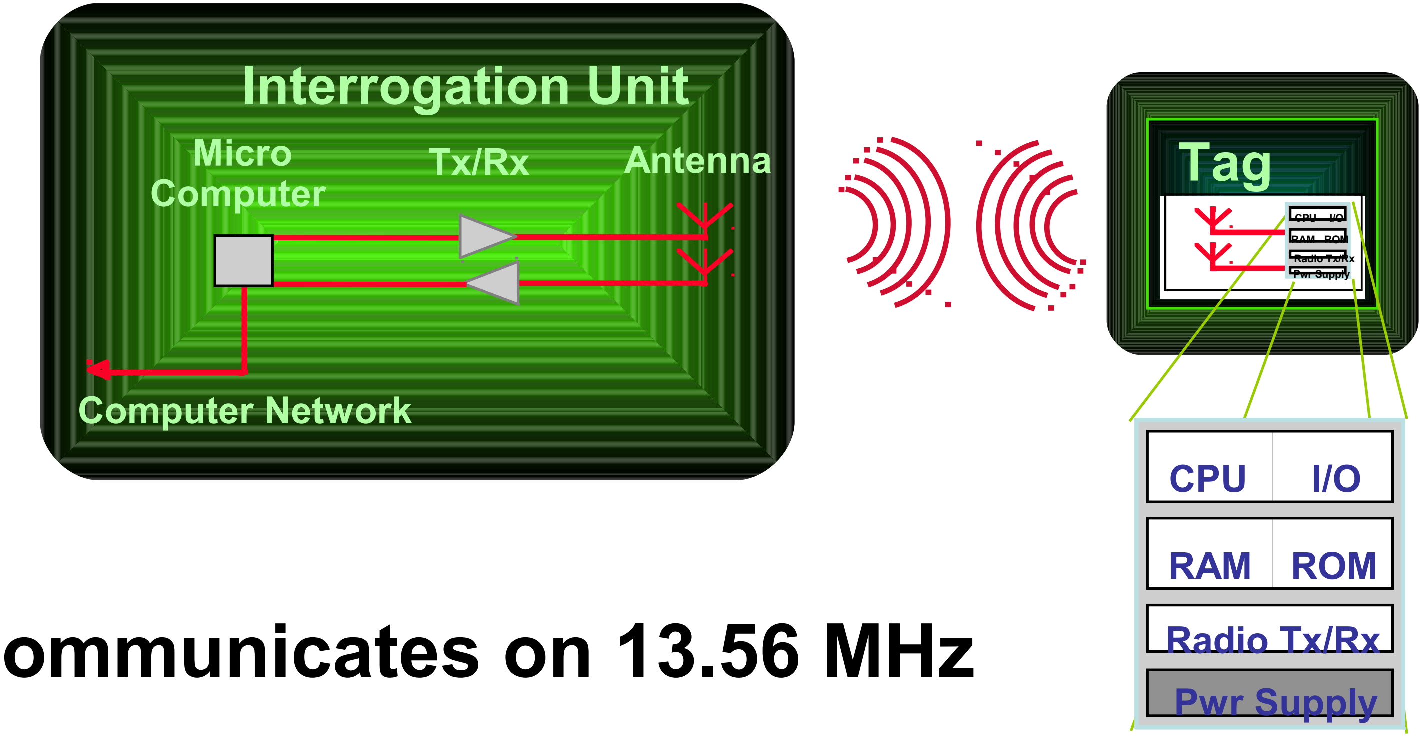


RFID (Radio Frequency IDentification)



- Passive RFID
  - Energy via induction from the reader
  - Range up to 10 meters
- Active RFID
  - Battery powered
  - Range up to around 100 meters
- Semi-passive RFID
  - Mix of passive and active
  - Battery for the circuit but not for antenna (good for sensors and logging)
- Usage of RFID can be a big threat against the personal integrity
  - On top of that alot of security issues...
- RFID Guardian
  - Protect against unwanted reading
  - http://www.rfidguardian.org/

A RFID tag is a portable database



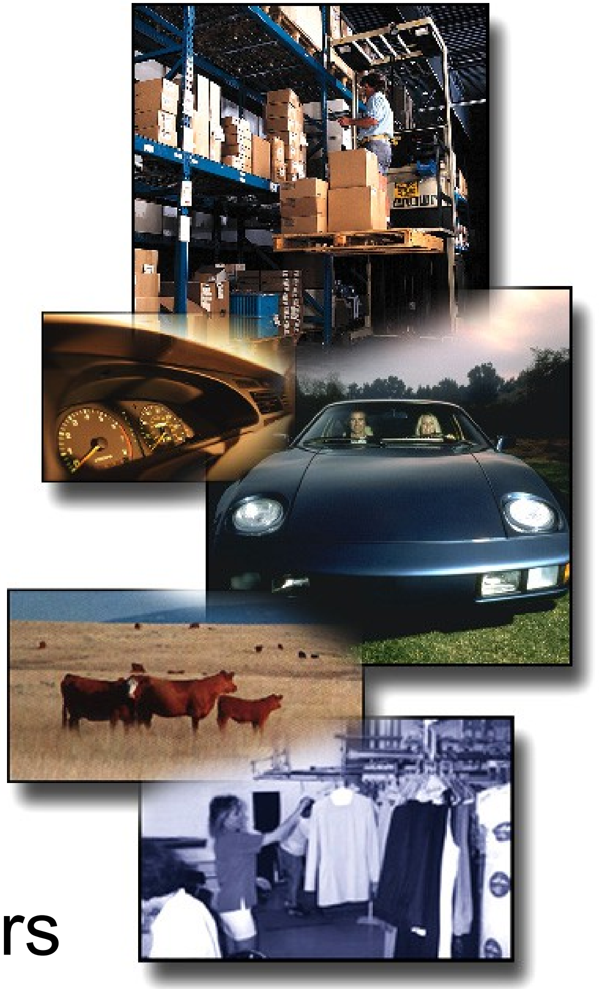
Communicates on 13.56 MHz

…A sophisticated computing and communications device

…A wireless extension of Information Systems

What is RFID? -- The Tags

- Tags can be attached to almost anything
  - Pallets or cases of product
  - Vehicles
  - Company assets or personnel
  - Items such as clothes, luggage, laundry
  - People, livestock, or pets
  - High value electronics such as computers, TVs, camcorders

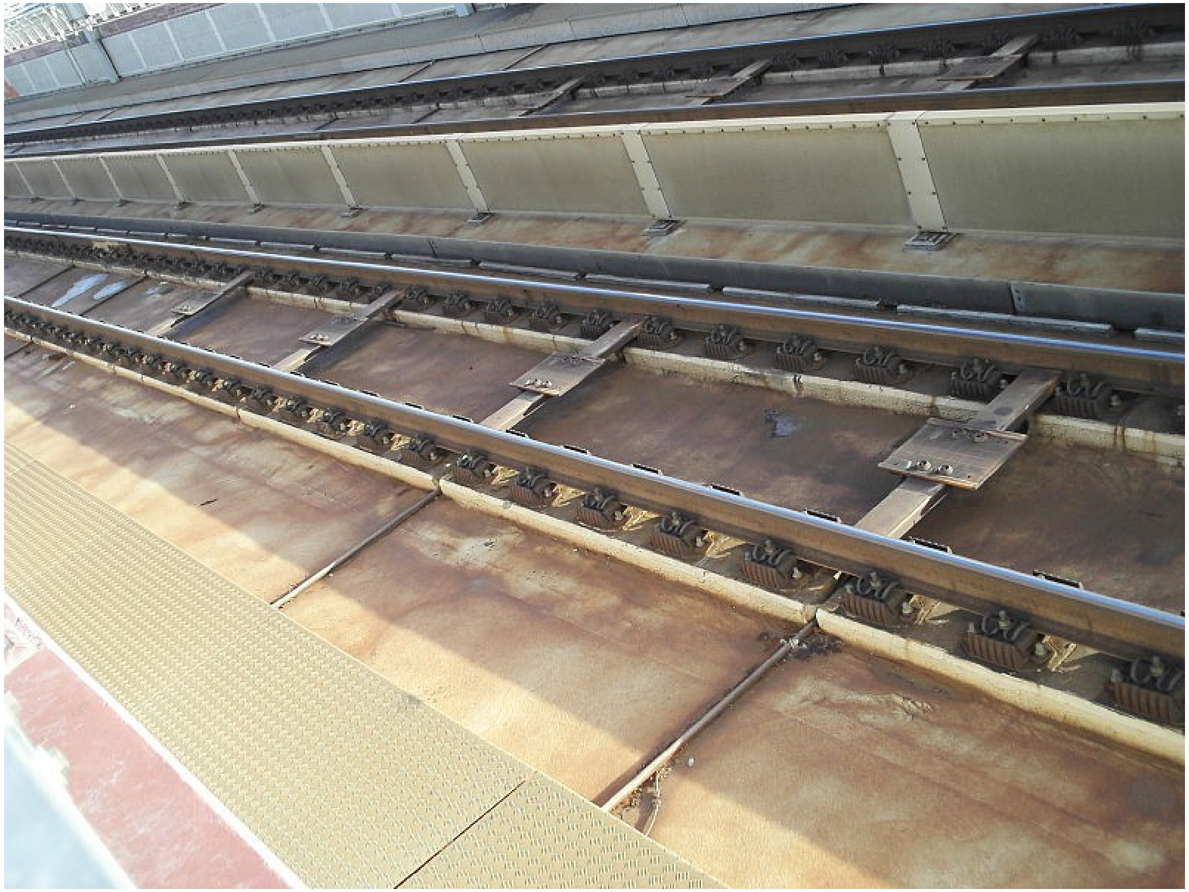


What is RFID? -- The Readers

- Readers (interrogators) can be at a fixed point such as
  - Entrance/exit
  - Point of sale
  - Warehouse
- Readers can also be mobile
  - Fastened (tethered)
  - Hand-held
  - Wireless
  - Etc.

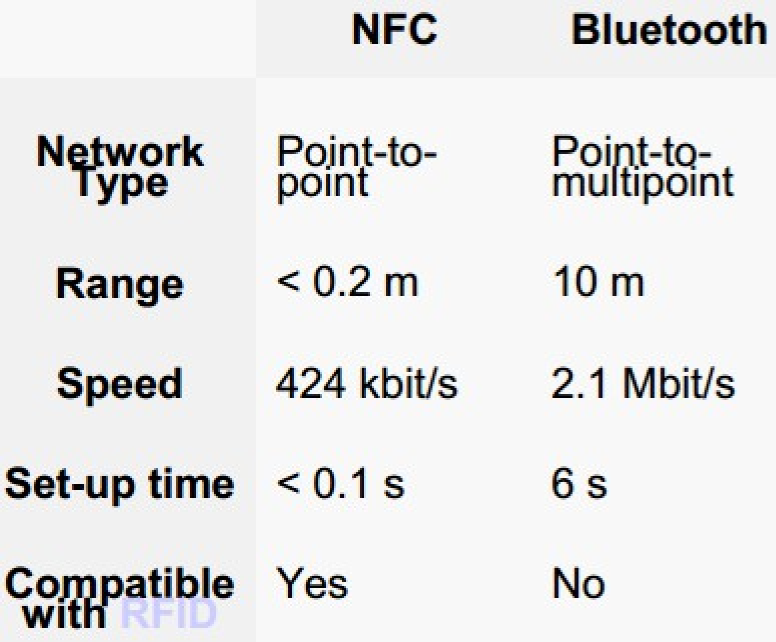
ATC (Automatic Traction Control)

- 2 - 4 “baliser” is placed between the rails
- Give train info as: max speed, rail signals etc.
- Can emergency brake or brake the train normally



Near Field Communication

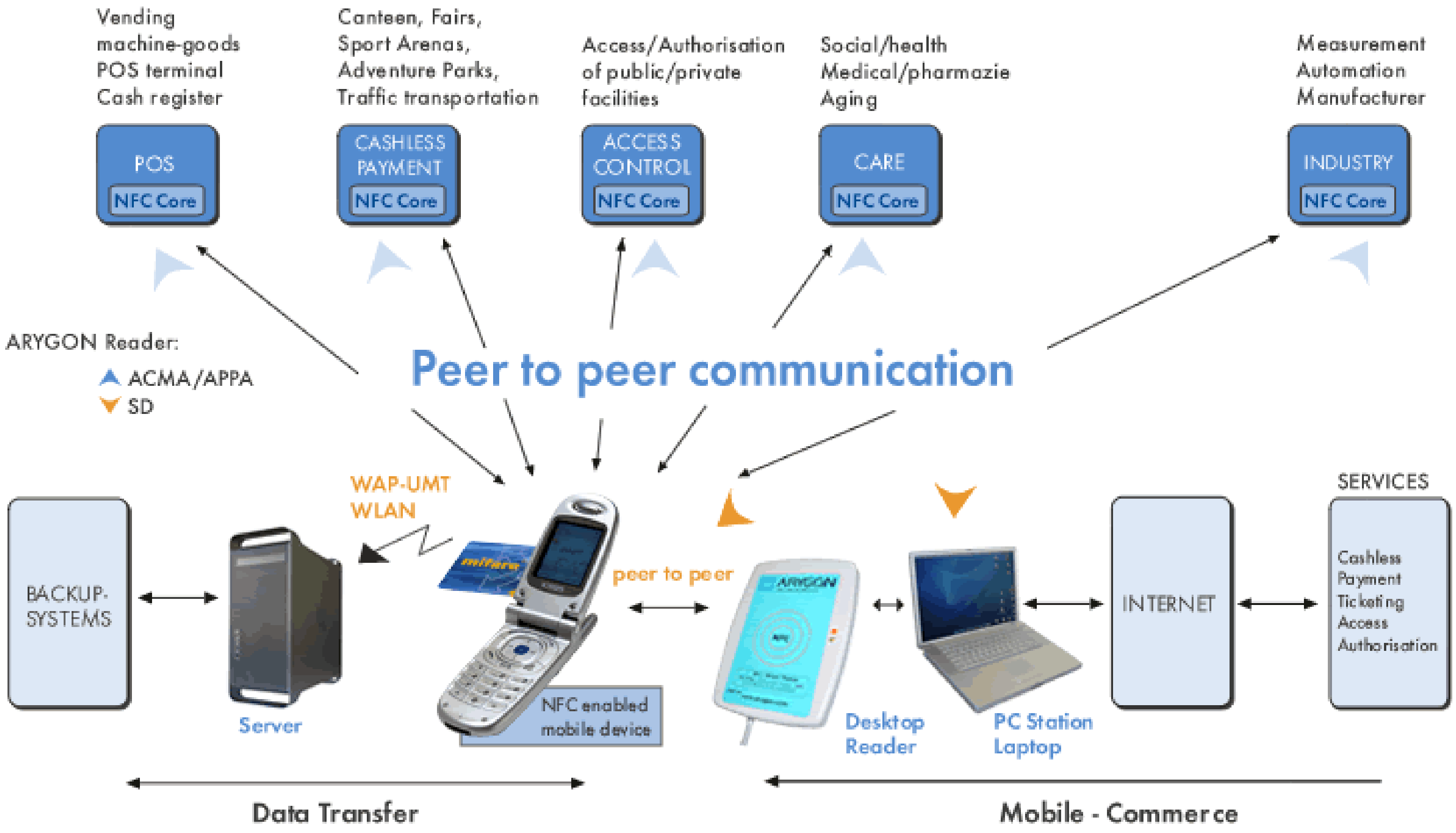
- Combines the interface of a smartcard and a RFID reader into a single device
- There are three main use cases for NFC
  - **Card emulation:** the NFC device behaves like an existing contactless smartcard making mobile payment a reality
  - **Reader mode:** the NFC device is active and read a passive RFID tag, for example for interactive advertising
  - **P2P mode:** two NFC devices are communicating together and exchanging information
- Global open united standard
  - http://www.nfc-forum.org
- Cheap
  - 1$ for the circuit
- GSMA
  - Mobile NFC initiative
- Android >= 2.3 have NFC API



	NFC	Bluetooth
Network Type	Point-to-point	Point-to-multipoint
Range	< 0.2 m	10 m
Speed	424 kbit/s	2.1 Mbit/s
Set-up time	< 0.1 s	6 s
Compatible with RFID	Yes	No

Near Field Communication

- RFID applications using Near Field Communication

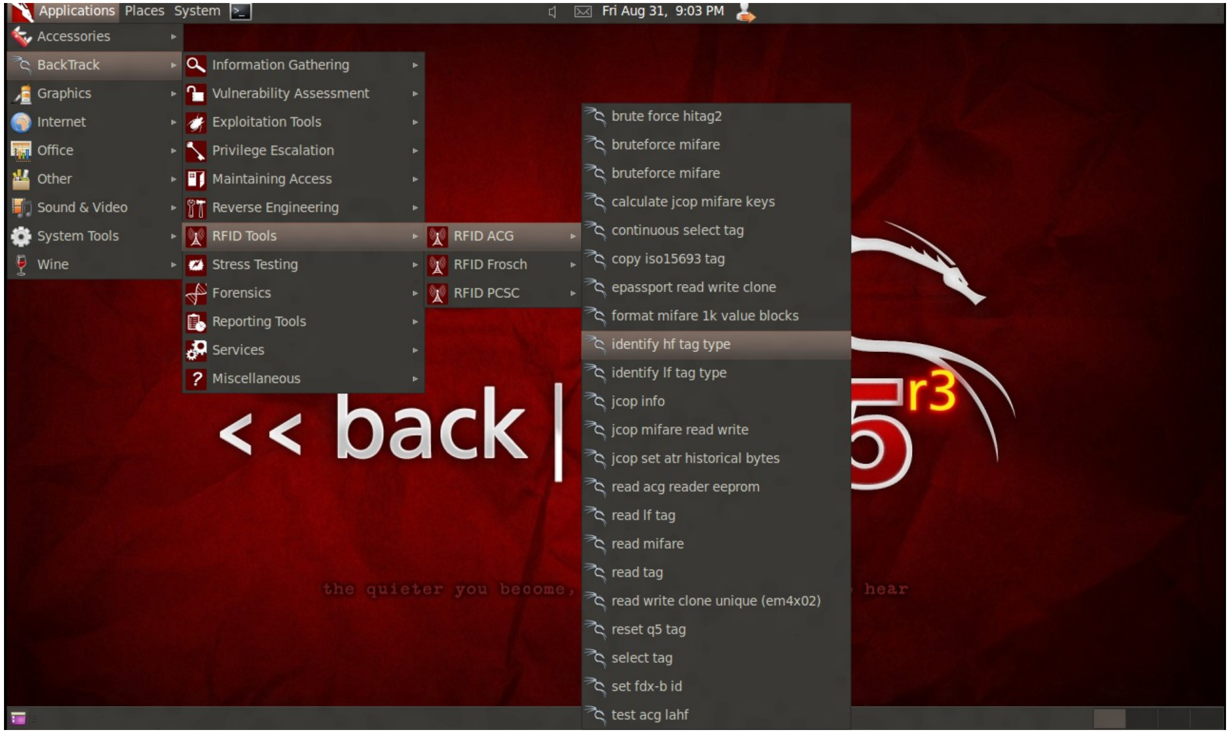


Near Field Communication

- Security aspects
  - Eavesdropping
    - Harder with passive devices
  - Data modification
    - RFID jammer
  - Relay attack
    - MITM replay attack in real-time

Backtrack RF modules

- BlueTooth
  - BluePrint
  - BlueSmash
  - Btscanner
  - HCIDump
  - Minicom
  - ObexFTP
  - Ussp-Push
- RFID Tools
  - RFIDI > ACG
  - RFIDI > Frosch
  - RFIDI > PCSC
    - Bruteforce/Read MIFARE
    - Calculate JCOP MIFARE Keys
    - Chip & Pin info
    - Continuous Select TAG
    - ePassport READ/WRITE/CLONE
    - ...
    - JCOP info etc.
    - Read/Select Tag

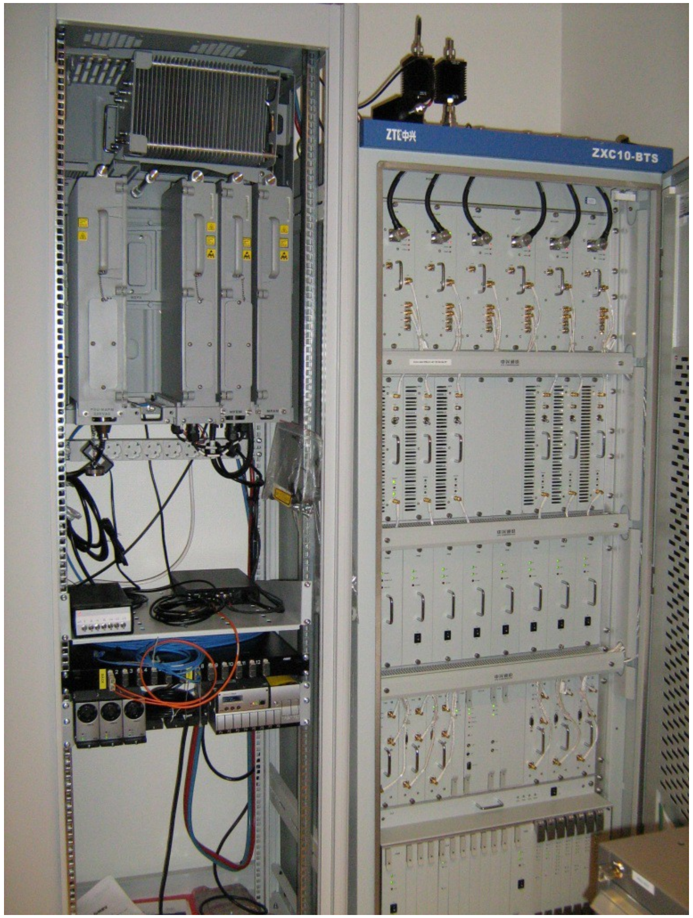


BTS (Base Tranceiver Station)

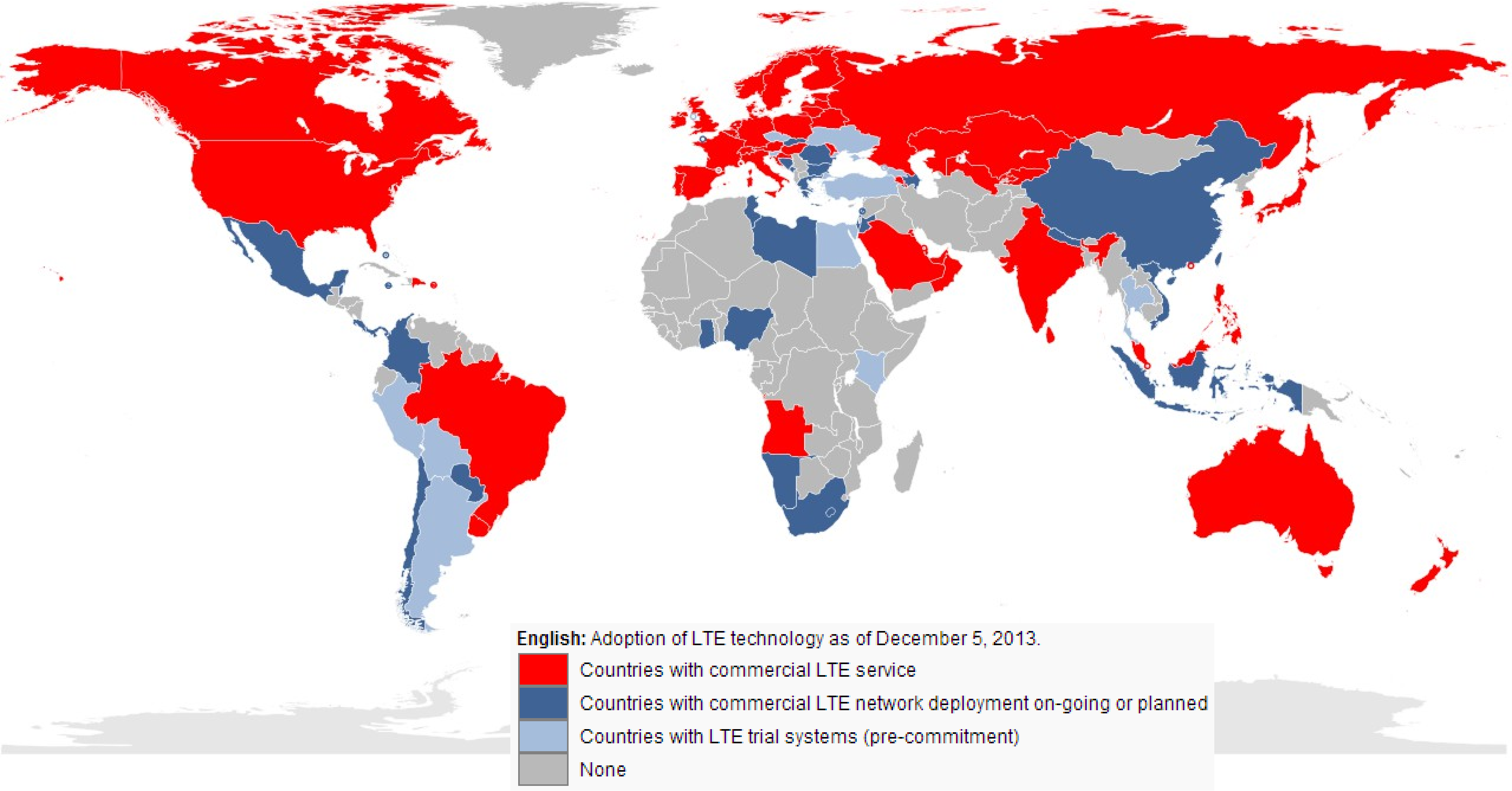
- The mast
  - Sectors
  - Up/down link
- The box
  - Radio transmitter
  - Radio receiver
  - GPS for exact time
  - Connected to the
  - BSC (Base Station Controller)

Faraday cage and Base Station Controller

- EMC (ElectroMagnetic Compability) testing environment
- UE as: modems, fixed wireless phones and mobiles



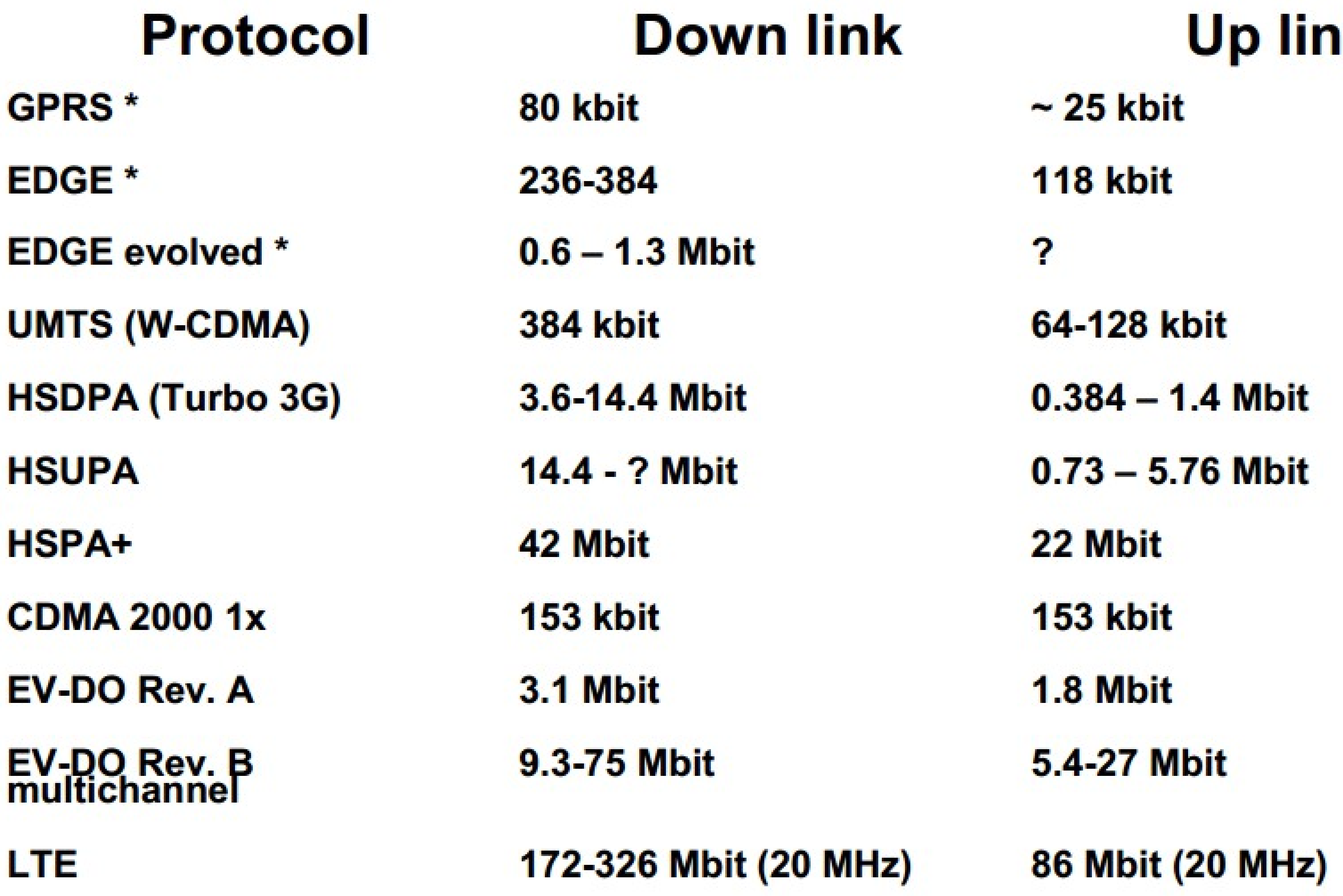
The worlds communications standards 2006 75015366.pdf


English: Adoption of LTE technology as of December 5, 2013.
🟥 Countries with commercial LTE service
🟦 Countries with commercial LTE network deployment on-going or planned
🟦 Countries with LTE trial systems (pre-commitment)
⬜ None

http://en.wikipedia.org/wiki/List_of_mobile_phone_standards → Long Term Evolution (Rel. 8)

Theoretical speed for wireless

*** = time slot dependent**



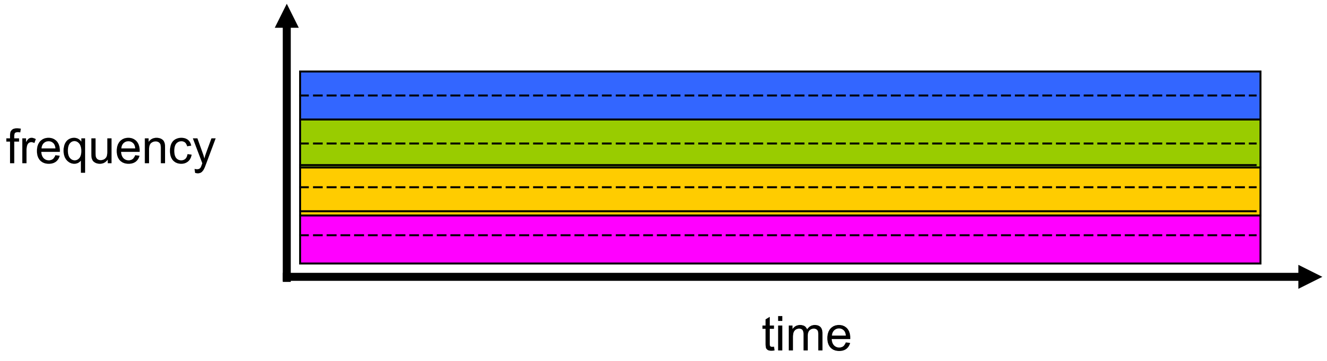
Protocol	Down link	Up link
GPRS *	80 kbit	~ 25 kbit
EDGE *	236-384	118 kbit
EDGE evolved *	0.6 – 1.3 Mbit	?
UMTS (W-CDMA)	384 kbit	64-128 kbit
HSDPA (Turbo 3G)	3.6-14.4 Mbit	0.384 – 1.4 Mbit
HSUPA	14.4 - ? Mbit	0.73 – 5.76 Mbit
HSPA+	42 Mbit	22 Mbit
CDMA 2000 1x	153 kbit	153 kbit
EV-DO Rev. A	3.1 Mbit	1.8 Mbit
EV-DO Rev. B multichannel	9.3-75 Mbit	5.4-27 Mbit
LTE	172-326 Mbit (20 MHz)	86 Mbit (20 MHz)

FDM and TDM

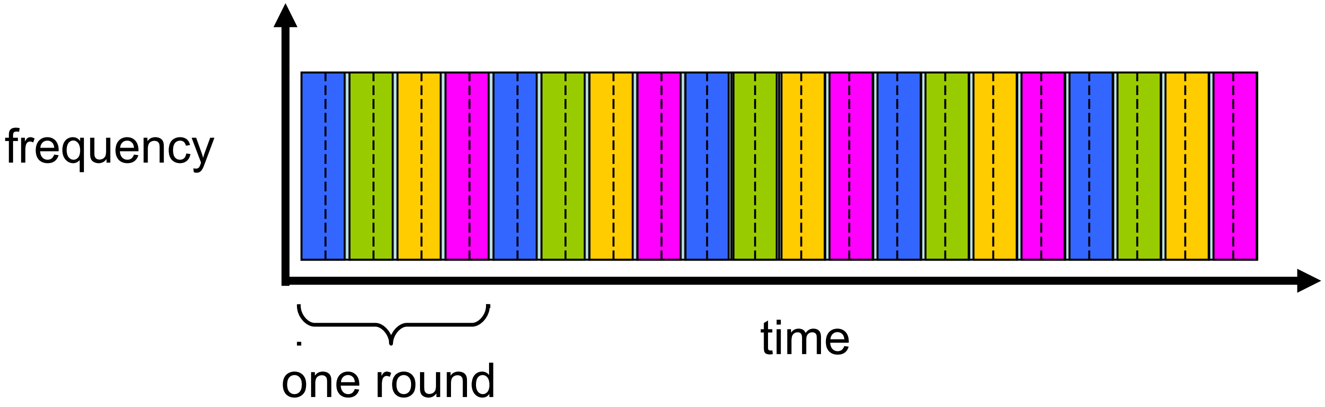
Example:

4 users 🟦 🟩 🟨 🟪

FDM = Frequency Division Multiplexing

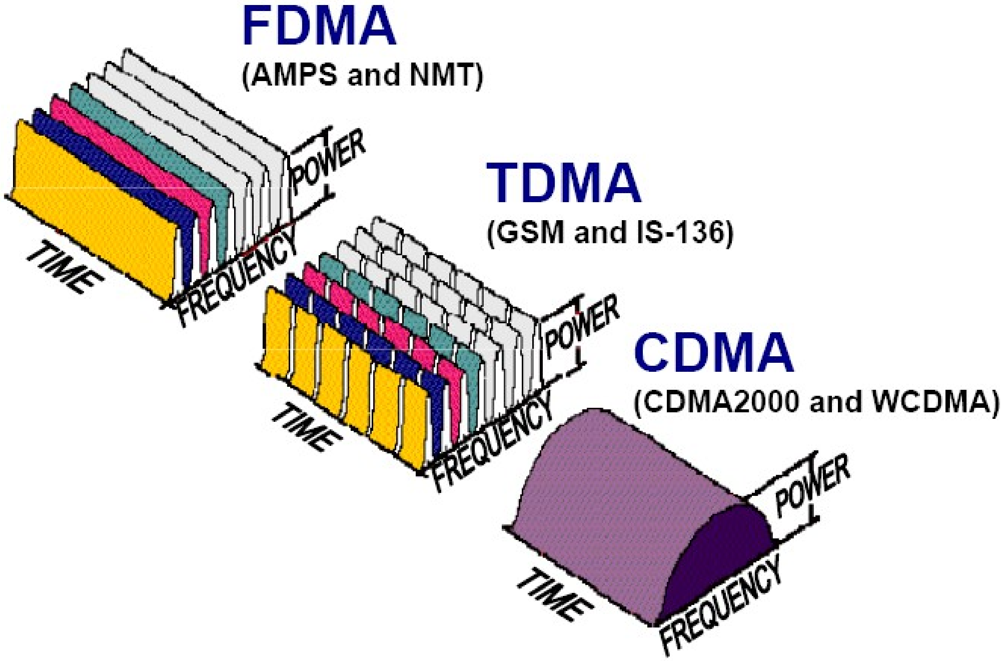


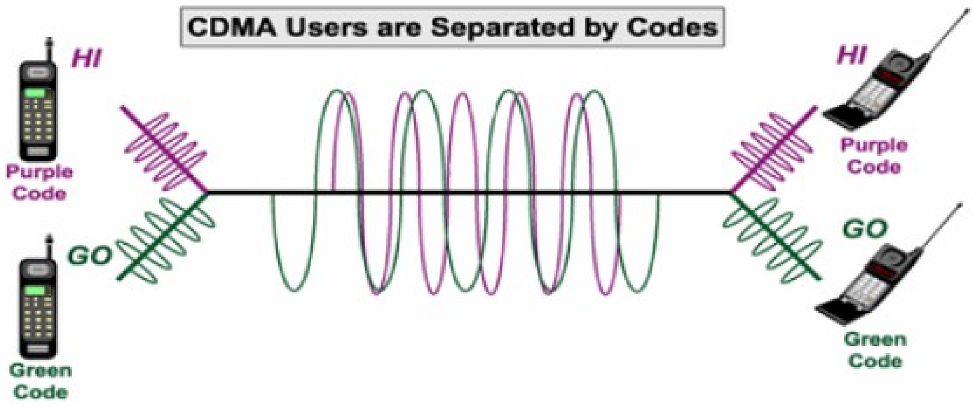
TDM = Time Division Multiplexing



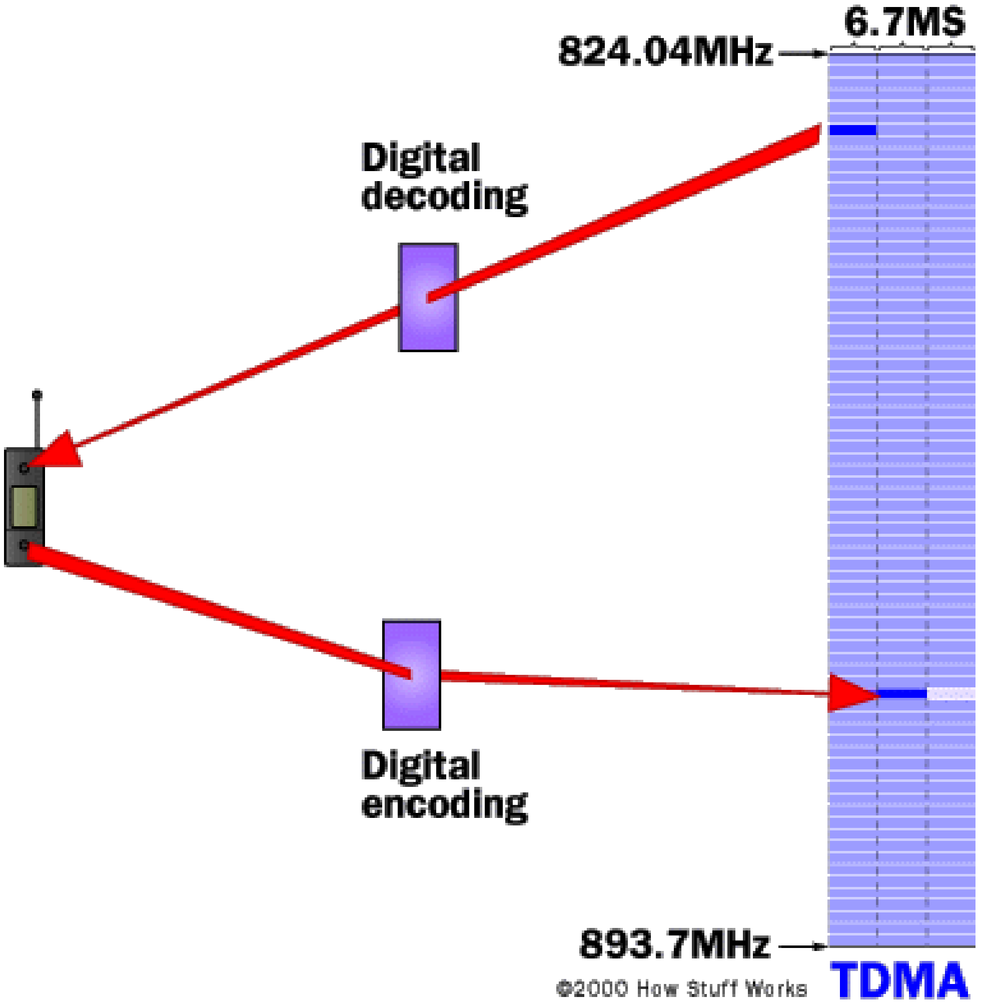
Mobile communication protocols

- FDMA
  (frequency divison)
  - NMT (analogous)
- TDMA (time slots)
  - GSM, GPRS
- CDMA (code divison)
  - CDMA One (IS-95)
  - CDMA 2000 (IS-2000)
  - W-CDMA (UMTS)





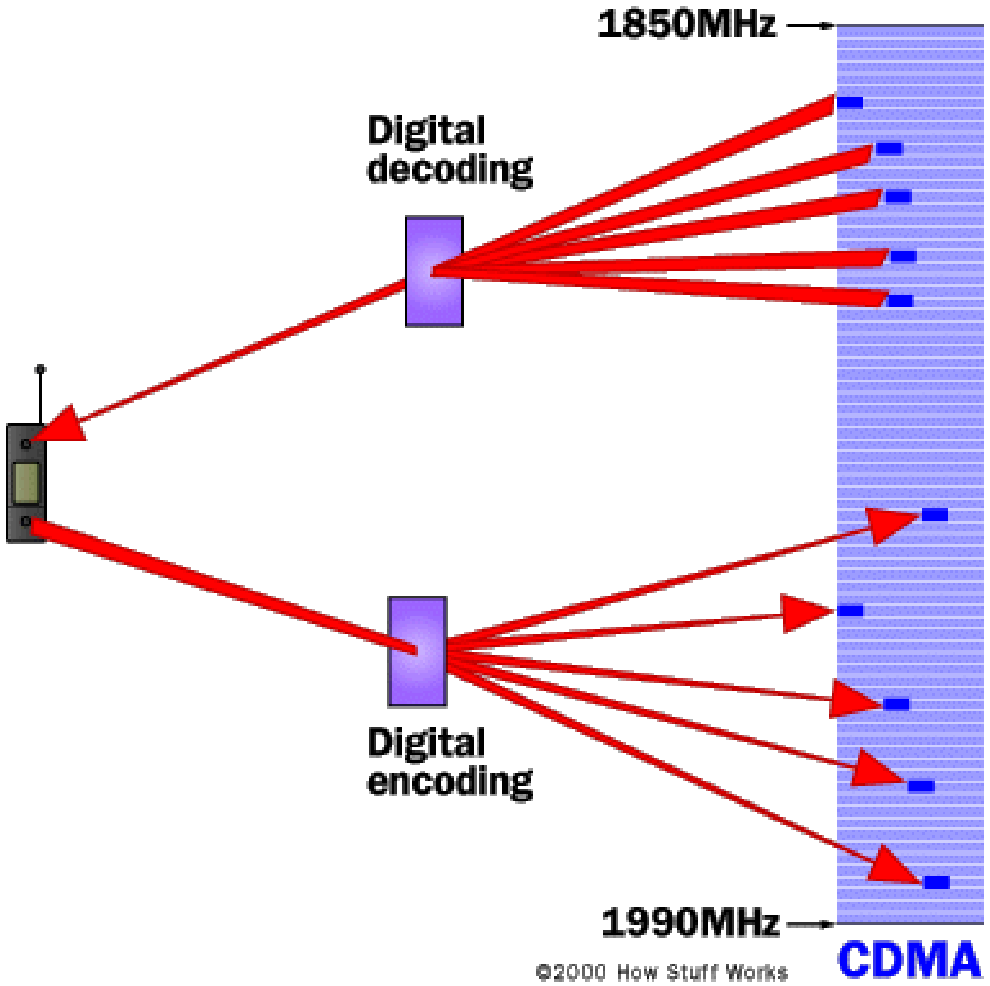
TDMA – Time Division Multiple Access



TDMA assigns each call a certain portion of time on a designated frequency

A narrow band (channel) 6.7 milliseconds long is split time-wise into 3 time slots

CDMA – Code Division Multiple Access

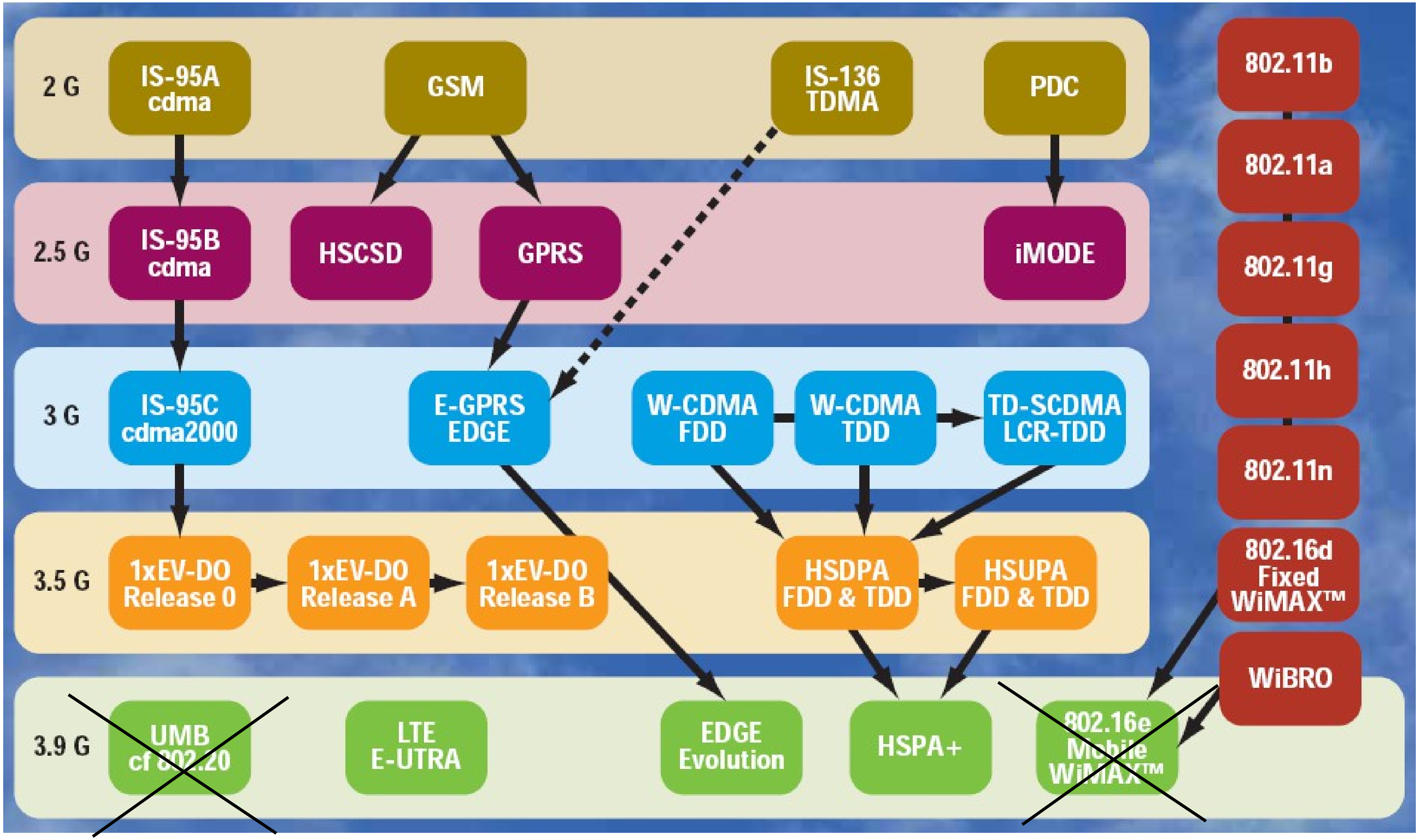


CDMA digitizes data and then spreads it out over the entire available bandwidth.

Multiple calls are overlaid on each other on the channel with each call given a unique code

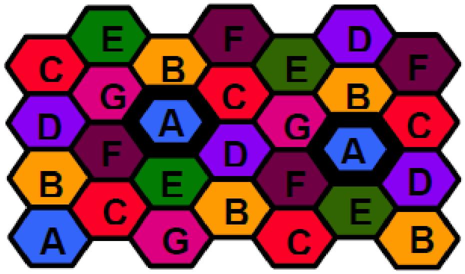
CDMA is more efficient than TDMA for data transmission

Evolution of wireless protocols

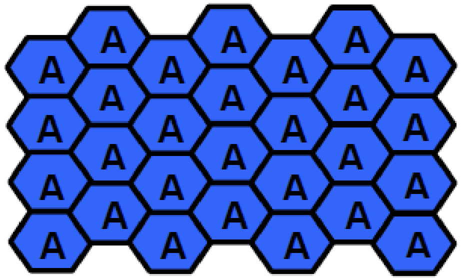


Advantages with (W)CDMA

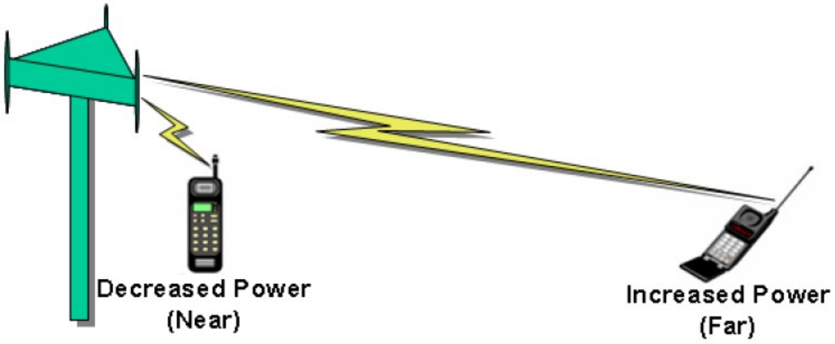
- Multiple Access, can manage most users per MHz
  - Have no specific limit for the number of concurrent users
- Consumes less energy – handles larger cells
- Digital modulation - Spread spectrum
  - Frequency jumping
  - The signal is transmitted on a channel with high bandwith
  - Resistant against ”jamming”
  - Eavesdropping safe
  - Resistent against fading (signal have multiple paths) phenomen
- Soft handoff
  - Soft handover vs. hard handover
  - UE is connected to two or more sectors simultaneously
- Low interference with other electronics
- Disadvantages?



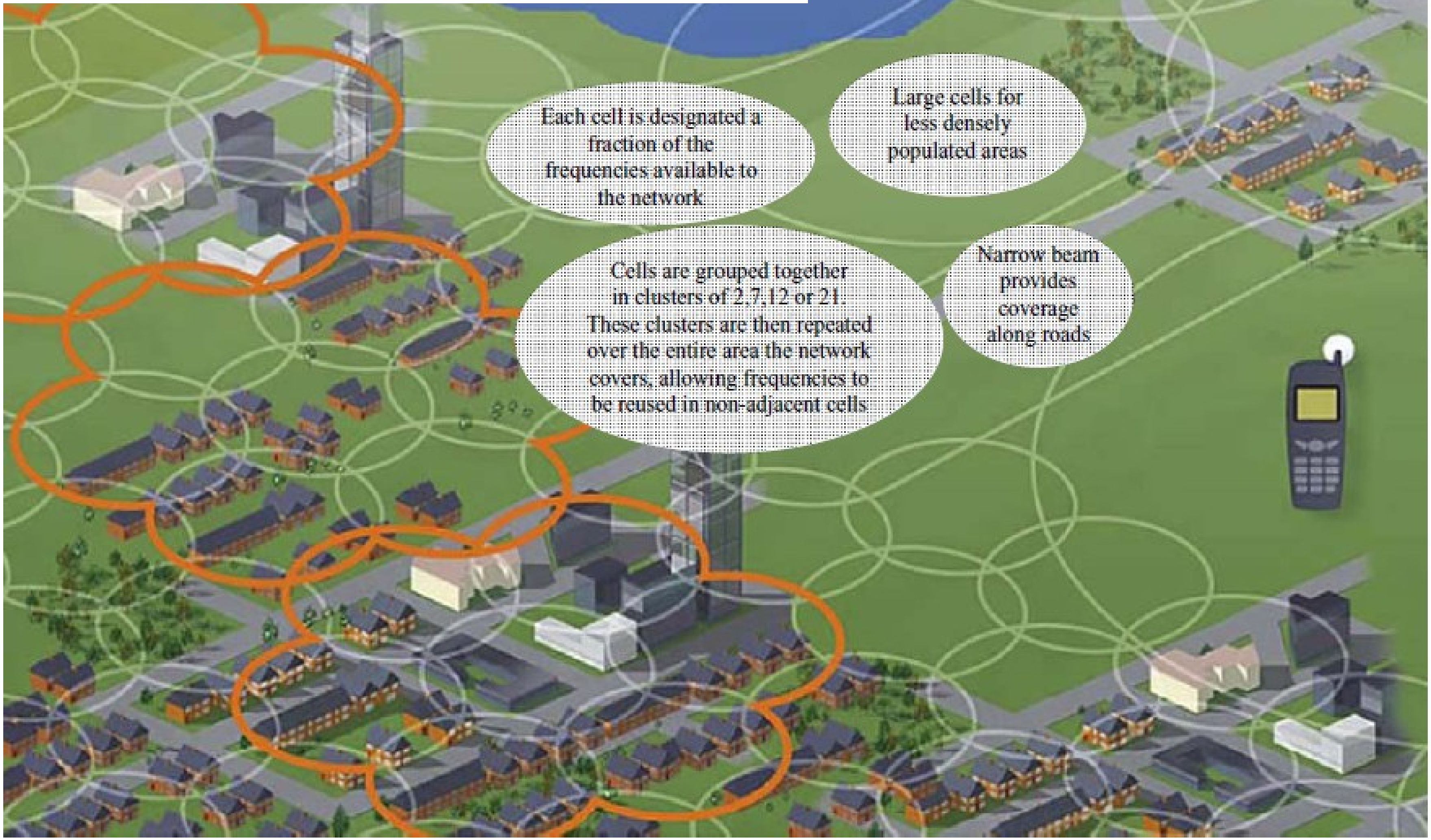
N = 7



N = 1

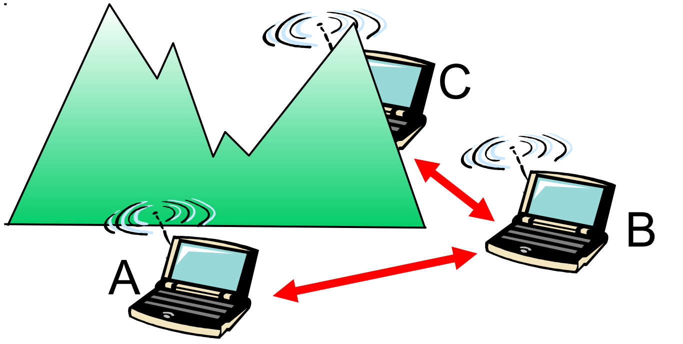


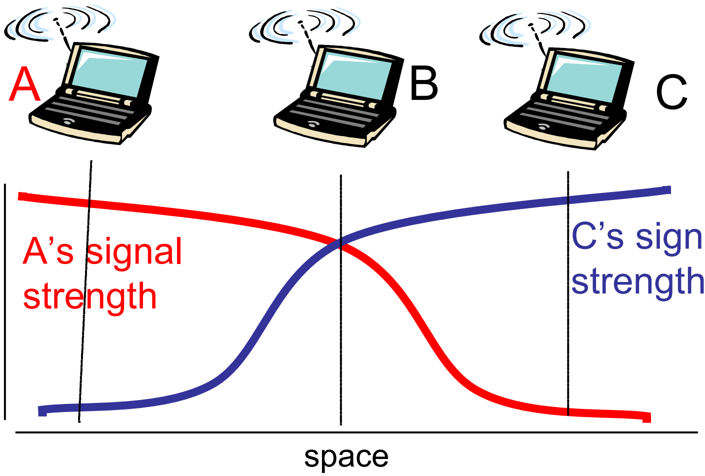
Each color represents a different frequency


Each cell is designated a fraction of the frequencies available to the network
Large cells for less densely populated areas
Cells are grouped together in clusters of 2,7,12 or 21. These clusters are then repeated over the entire area the network covers, allowing frequencies to be reused in non-adjacent cells
Narrow beam provides coverage along roads

Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access)





Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other

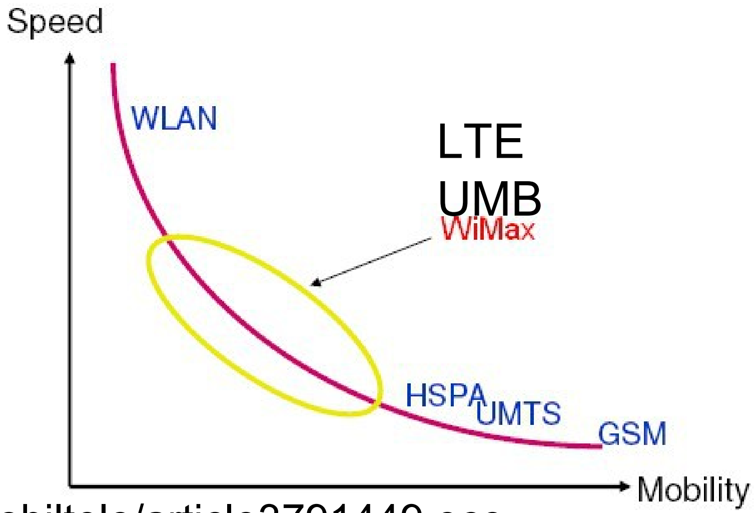
means A, C unaware of their interference at B

Signal fading

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interferring at B

Just now – 4G (not the real 4G)

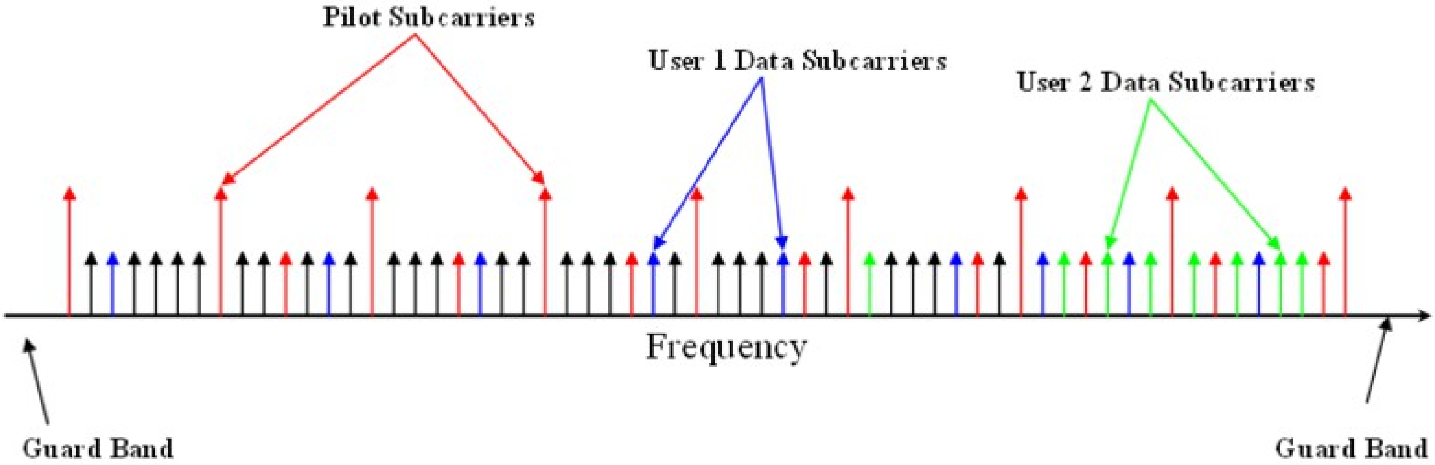
- Orthogonal Frequency Division Multiple Access (OFDMA)
  - LTE (Long Term Evolution)
  - WIMAX – will soon be dead?
  - UMB (Ultra Mobile Broadband) – dead at arrival
- MIMO advanced antenna tech., enable speed up to
  - > 275 Mbit/s down
  - > 75 Mbit/s up
- On the market since 2011
  - Compatible with
    - W-CDMA
    - 1x EV-DO Rev. *
- Massive MIMO 2017
  - http://www.nyteknik.se/nyheter/it_telekom/mobiltele/article3791449.ece



LTE
UMB

Mobile technology

- FLASH (Fast Low-latency Access with Seamless Handoff) OFDM
  - OFDM (Orthogonal Frequency-Division Multiplexing)
    - ADSL, DVB (DVB-T, DVB-T2), DAB etc.
  - WiMax is a variant of SOFDM (Scaleable …)
- OFDMA
  - Gives many advantages…
    - http://en.wikipedia.org/wiki/OFDMA
  - Combines CDMA and TDMA
  - Subcarrier channels are allocated to users

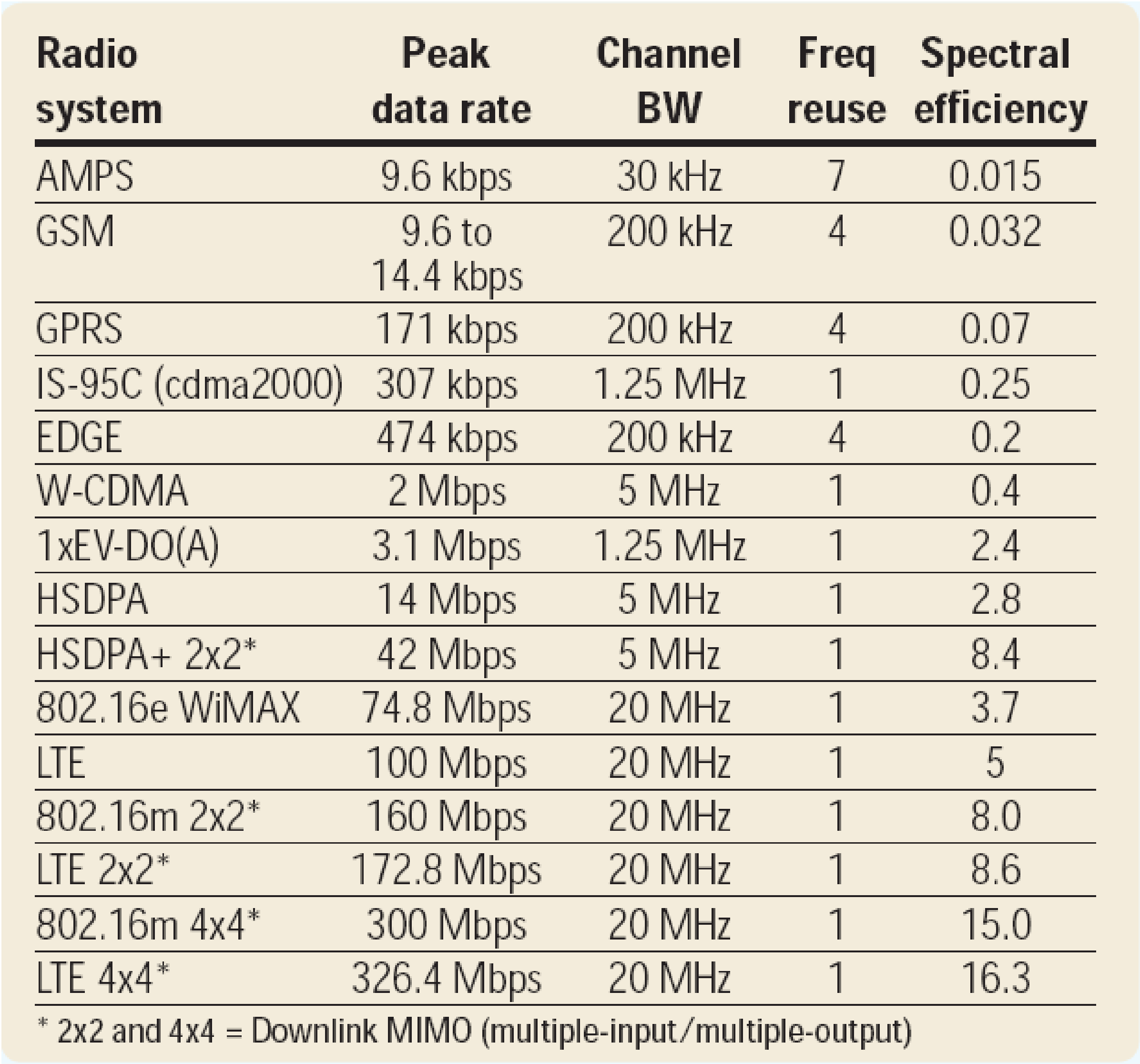


LTE - 4G

- LTE (Long Term Evolution)
  - Gives many advantages…
    - http://en.wikipedia.org/wiki/3GPP_Long_Term_Evolution
  - Combines OFDMA in down link and SC-FDMA (DFTS-FDMA) in up link
  - MIMO
  - Over 200 clients in every cell
  - Sub 5 ms latency
  - Spectrum flexibility
  - Up to 100 km cell size
  - Co exist with older standards
  - MBSFN (Multicast Broadcast Single Frequency Network)
  - Massive MIMO
  - And so on...

Ericsson Berta LTE prototype mobile

Comparision between max data speed in down link och spectral efficiency

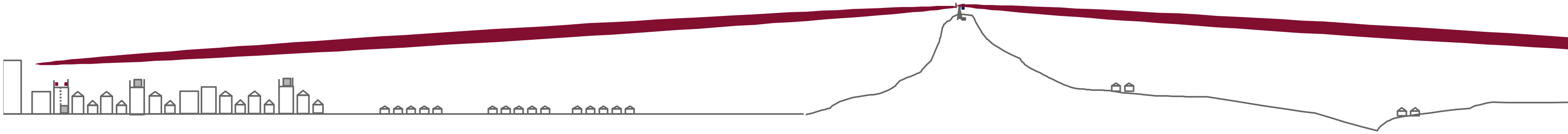


Radio system	Peak data rate	Channel BW	Freq reuse	Spectral efficiency
AMPS	9.6 kbps	30 kHz	7	0.015
GSM	9.6 to 14.4 kbps	200 kHz	4	0.032
GPRS	171 kbps	200 kHz	4	0.07
IS-95C (cdma2000)	307 kbps	1.25 MHz	1	0.25
EDGE	474 kbps	200 kHz	4	0.2
W-CDMA	2 Mbps	5 MHz	1	0.4
1xEV-DO(A)	3.1 Mbps	1.25 MHz	1	2.4
HSDPA	14 Mbps	5 MHz	1	2.8
HSDPA+ 2x2*	42 Mbps	5 MHz	1	8.4
802.16e WiMAX	74.8 Mbps	20 MHz	1	3.7
LTE	100 Mbps	20 MHz	1	5
802.16m 2x2*	160 Mbps	20 MHz	1	8.0
LTE 2x2*	172.8 Mbps	20 MHz	1	8.6
802.16m 4x4*	300 Mbps	20 MHz	1	15.0
LTE 4x4*	326.4 Mbps	20 MHz	1	16.3

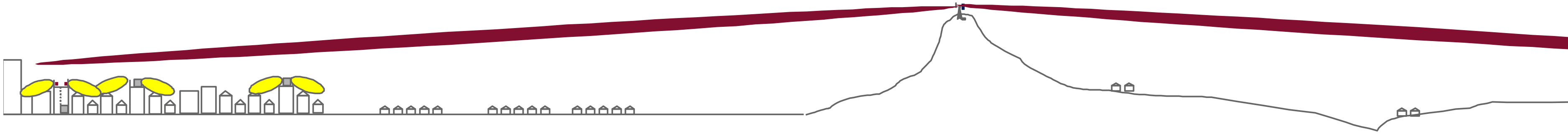
* 2x2 and 4x4 = Downlink MIMO (multiple-input/multiple-output)

Attractive greenfield opportunity - Scalability

- Start with umbrella cells benefiting from the coverage properties

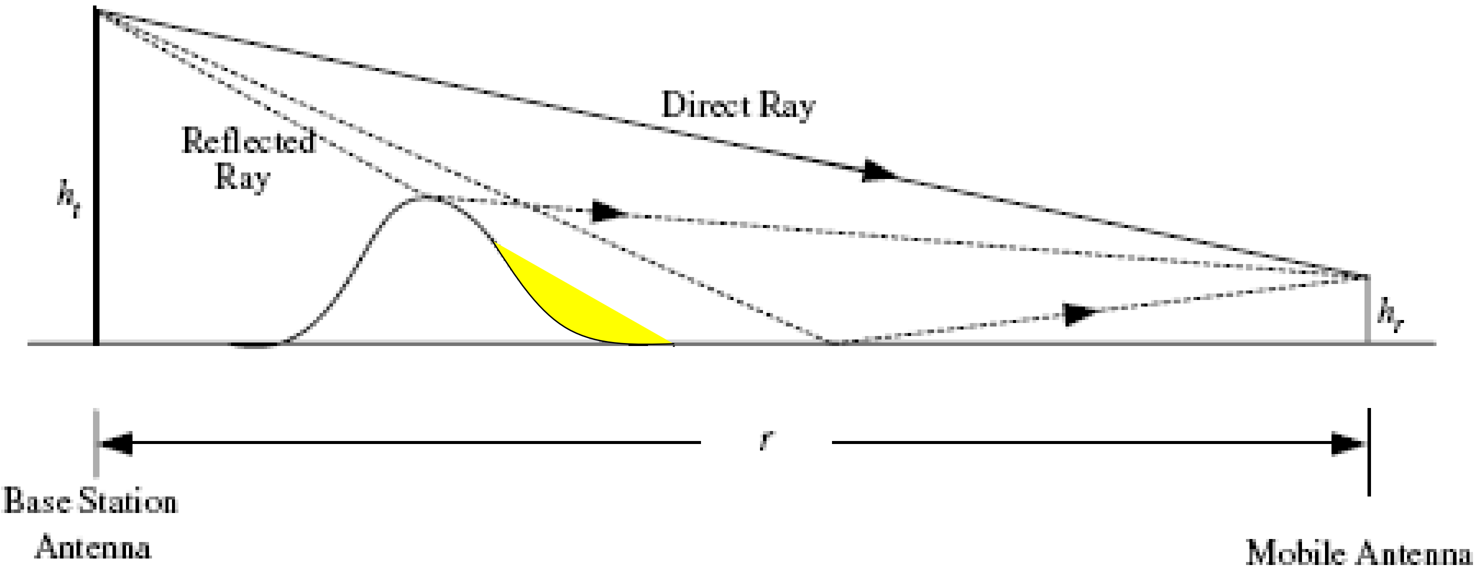


- Add lower base stations as better urban indoor coverage and capacity is needed

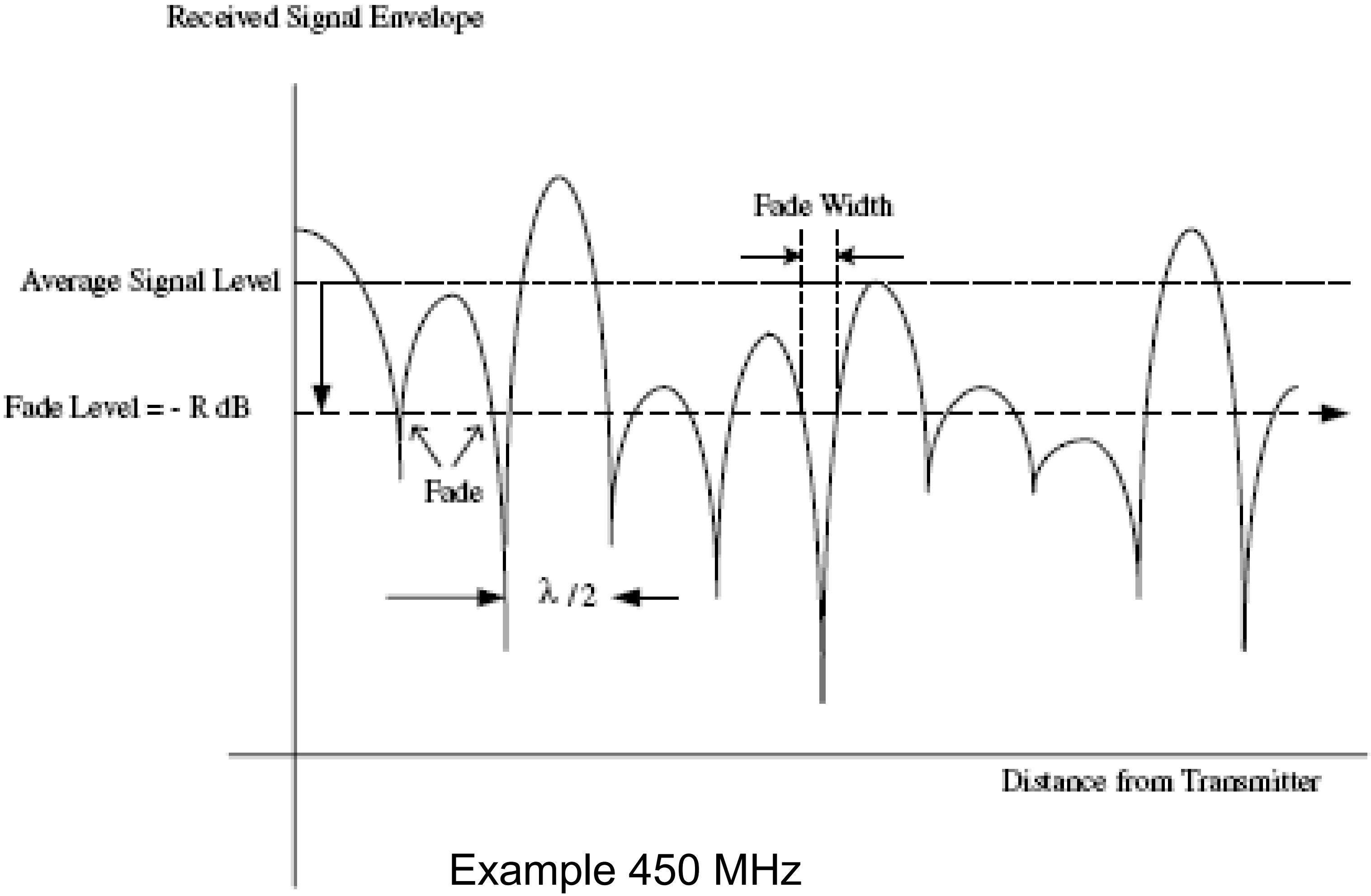


- Result: Best coverage, scalable capacity, redundancy

Range 1


Direct Ray
Reflected Ray
h_t
h_r
r
Base Station Antenna
Mobile Antenna

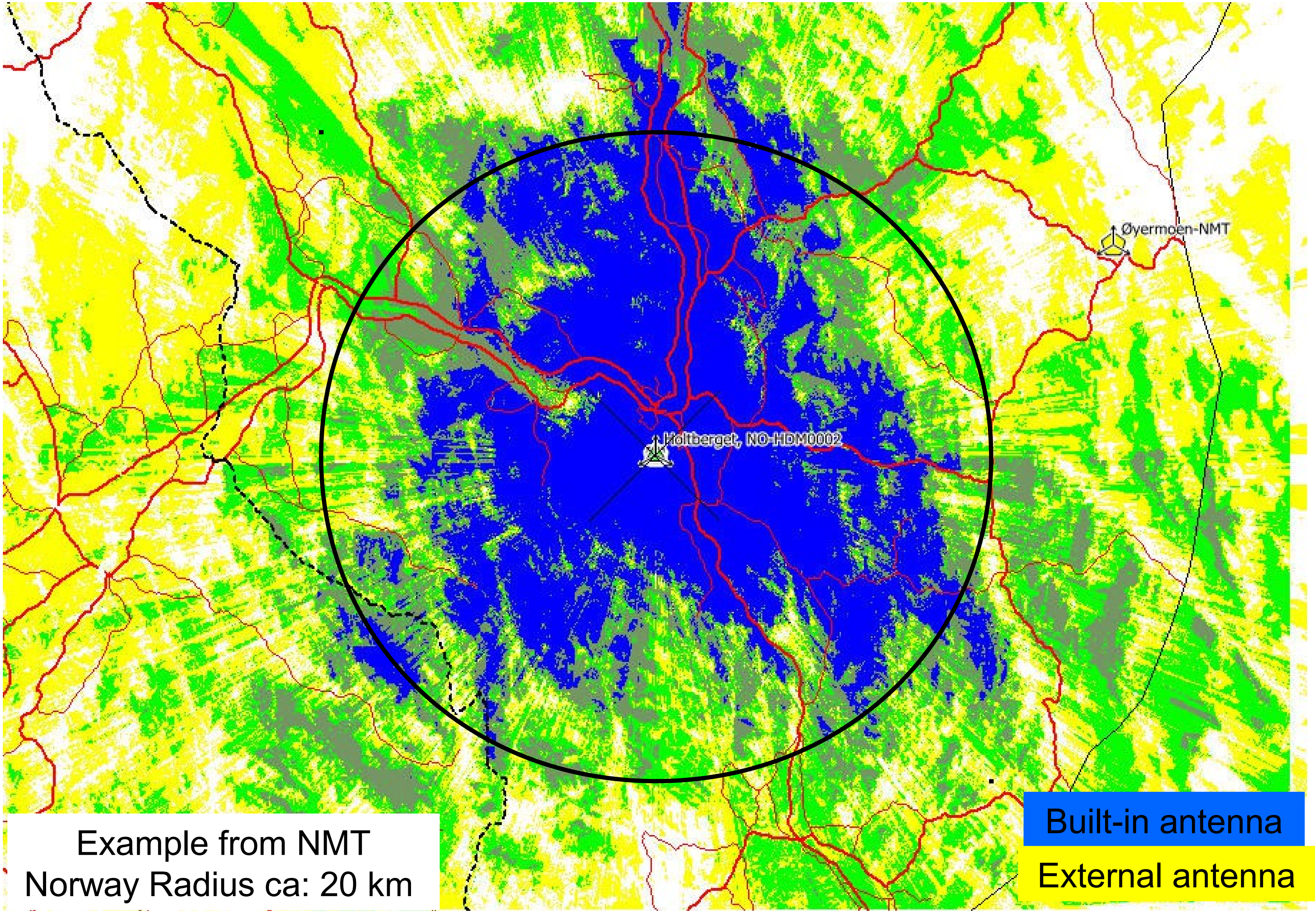
Range 2



Example 450 MHz

300/450/2 = 0,33 meters
antenna length is optimal (lambda/2)

McGraw Hill - W-CDMA and cdma2000 for 3G Mobile Networks

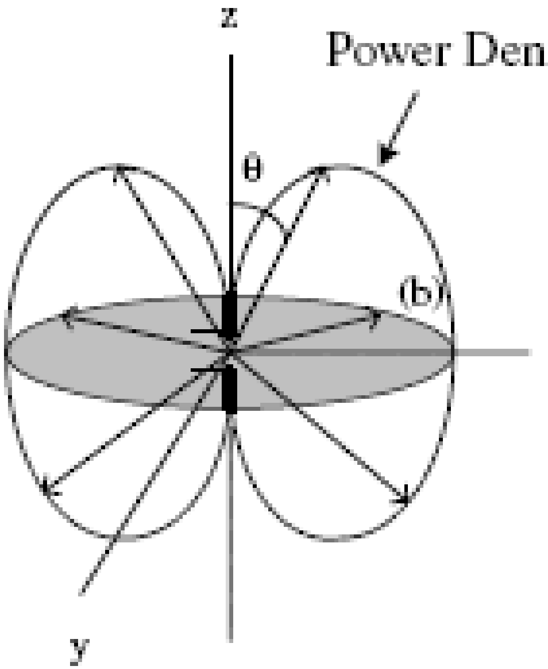


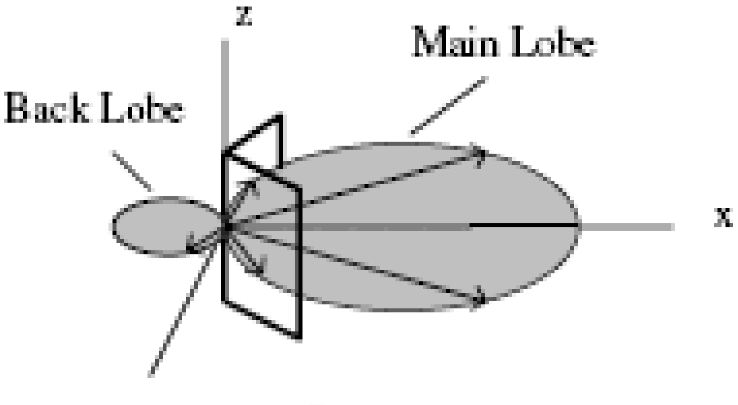
Example from NMT
Norway Radius ca: 20 km

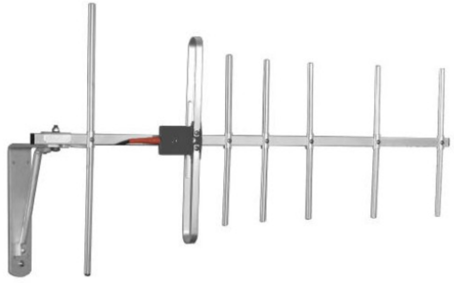
🟦 Built-in antenna

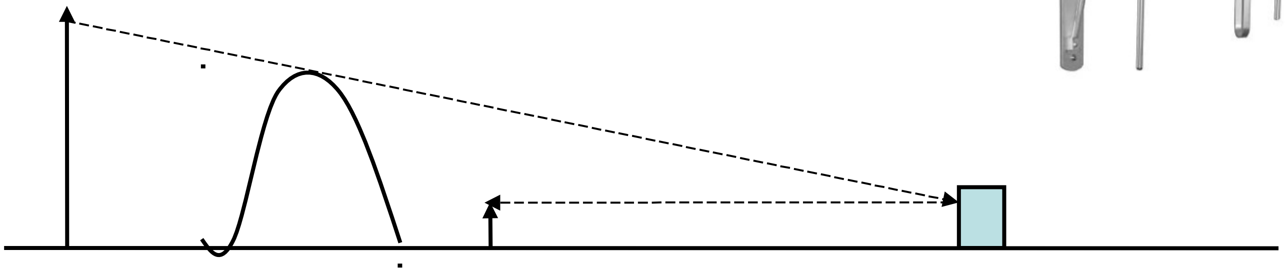
🟨 External antenna

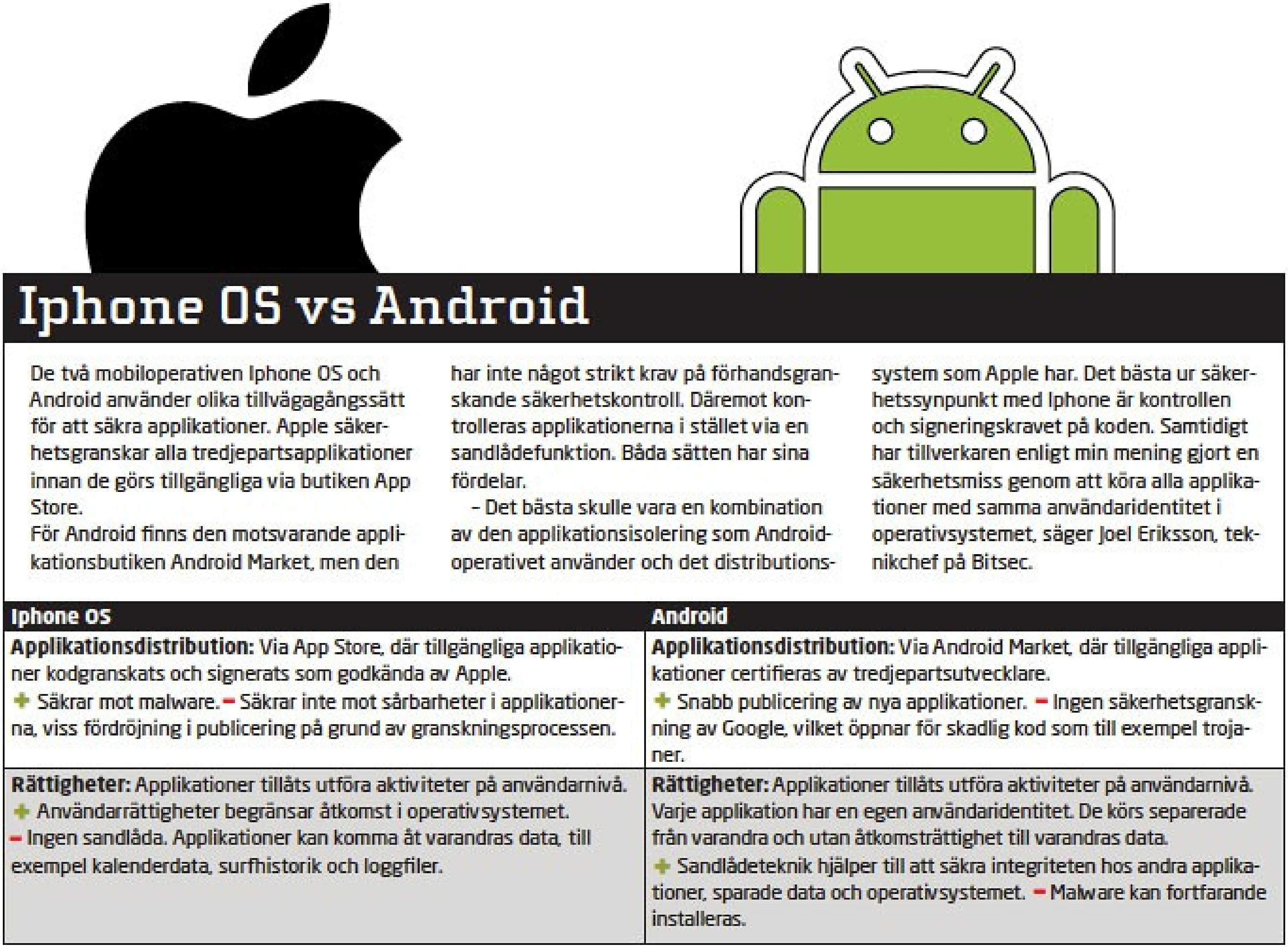
Range 3











Iphone OS vs Android

De två mobiloperativen Iphone OS och Android använder olika tillvägagångssätt för att säkra applikationer. Apple säkerhetsgranskar alla tredjepartsapplikationer innan de görs tillgängliga via butiken App Store.

För Android finns den motsvarande applikationsbutiken Android Market, men den har inte något strikt krav på förhandsgranskande säkerhetskontroll. Däremot kontrolleras applikationerna i stället via en sandlådefunktion. Båda sätten har sina fördelar.

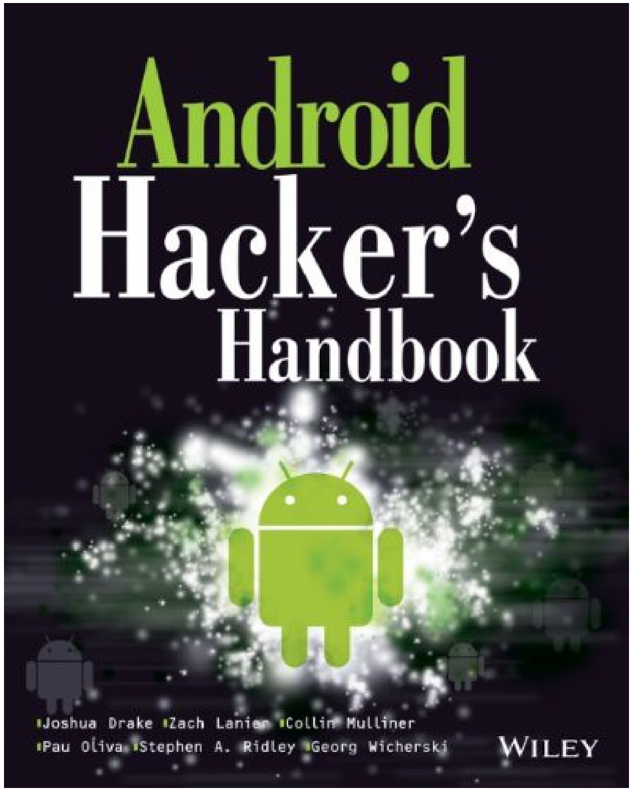
– Det bästa skulle vara en kombination av den applikationsisolering som Android-operativet använder och det distributionssystem som Apple har. Det bästa ur säkerhetssynpunkt med Iphone är kontrollen och signeringskravet på koden. Samtidigt har tillverkaren enligt min mening gjort en säkerhetsmiss genom att köra alla applikationer med samma användaridentitet i operativsystemet, säger Joel Eriksson, teknikchef på Bitsec.

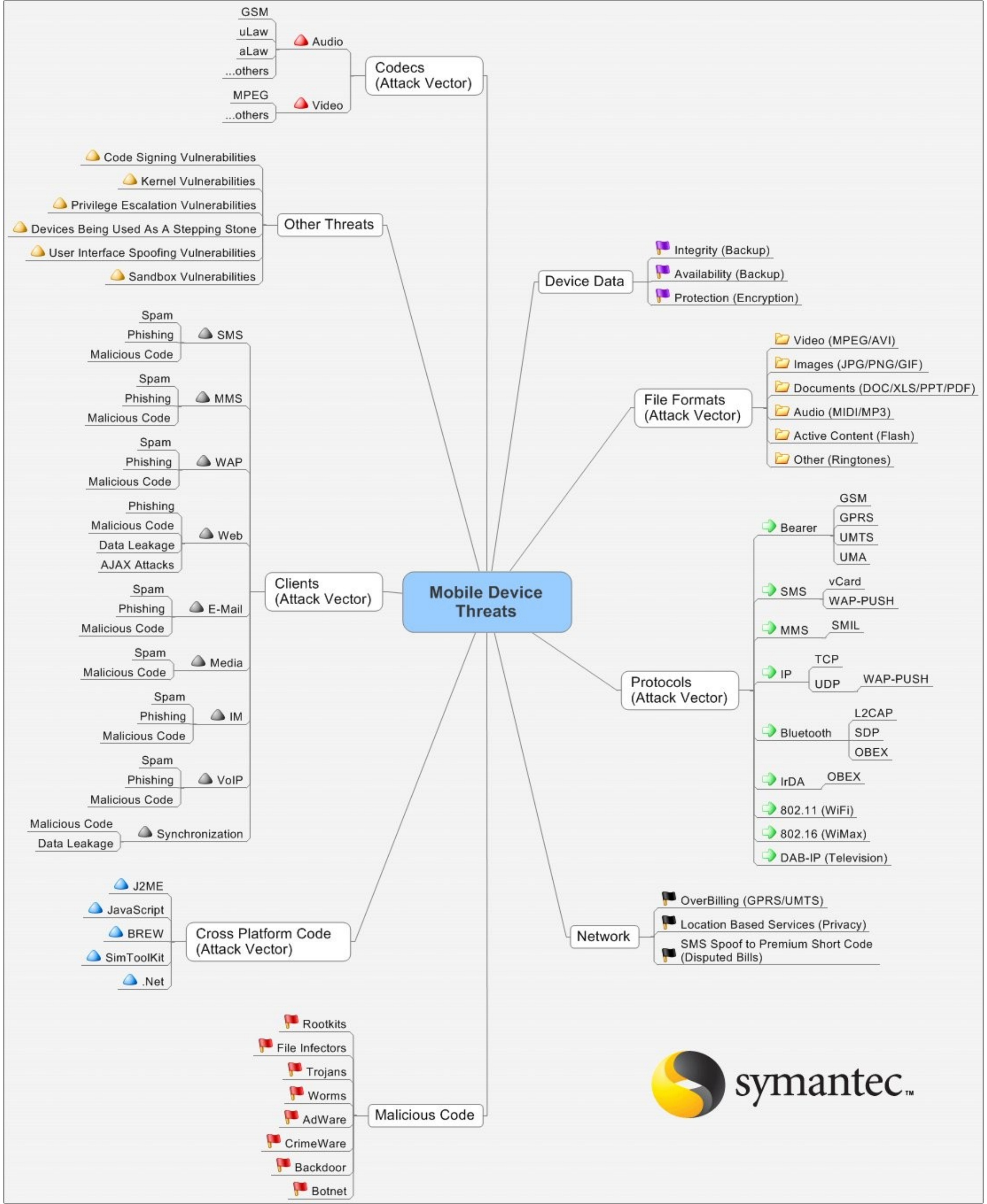
Iphone OS	Android
Applikationsdistribution: Via App Store, där tillgängliga applikationer kodgranskats och signerats som godkända av Apple. + Säkrar mot malware. – Säkrar inte mot sårbarheter i applikationerna, viss fördröjning i publicering på grund av granskningsprocessen.	**Applikationsdistribution:** Via Android Market, där tillgängliga applikationer certifieras av tredjepartsutvecklare. + Snabb publicering av nya applikationer. – Ingen säkerhetsgranskning av Google, vilket öppnar för skadlig kod som till exempel trojaner.
Rättigheter: Applikationer tillåts utföra aktiviteter på användarnivå. + Användarrättigheter begränsar åtkomst i operativsystemet. – Ingen sandlåda. Applikationer kan komma åt varandras data, till exempel kalenderdata, surfhistorik och loggfiler.	**Rättigheter:** Applikationer tillåts utföra aktiviteter på användarnivå. Varje applikation har en egen användaridentitet. De körs separerade från varandra och utan åtkomsträttighet till varandras data. + Sandlådeteknik hjälper till att säkra integriteten hos andra applikationer, sparade data och operativsystemet. – Malware kan fortfarande installeras.

http://www.idg.se/2.1085/1.384830/smart-mobil-kraver-smart-sakerhet/1

Mobile security Android

- Android Hacker's Handbook (2014)
  - http://www.amazon.com/Android-Hackers-Handbook-Joshua-Drake/dp/111860864X
- Presentation from book author (in course docs folder)
  - An Android Hacker's Journey - Challenges in Android Security Research.pptx
- Goes thru
  - Background
  - Ecosystem
  - Patching
  - Disclosure
  - Attack Surface
  - Tools
  - Exploitation
  - Hardening
  - Recommendations
  - Conclusions





Mobile device attack surface

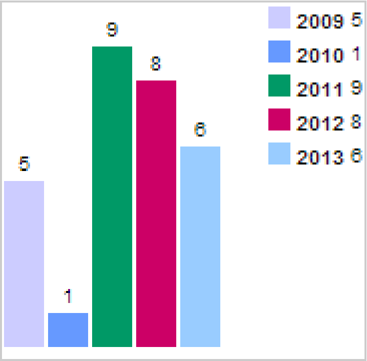
- The attack surface is HUGE and continuously growing!
- Lots of background services are running on-device
- http://recxltd.blogspot.se/2012/02/reflecting-on-mobile-security-today.html

Mobile security

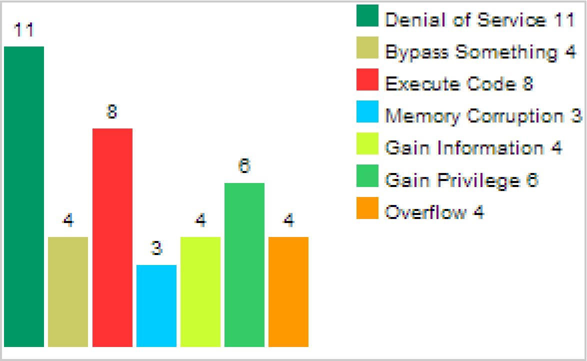
CVE Details
The ultimate security vulnerability datasource

- Android
  - http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224
- iOS
  - http://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49
- Windows Mobile
  - http://www.cvedetails.com/product/23230/Microsoft-Windows-Phone.html?vendor_id=26

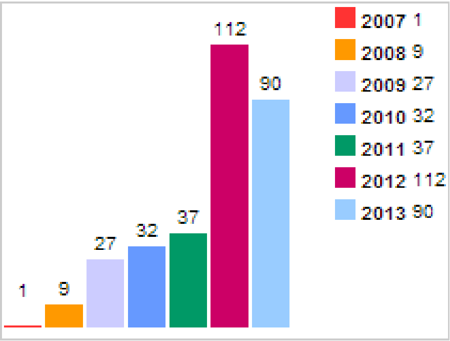
Vulnerabilities By Year



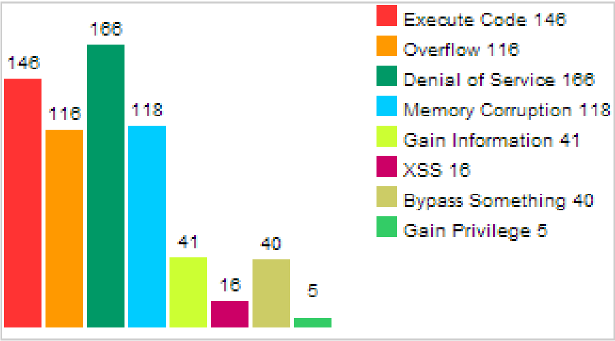
Vulnerabilities By Type



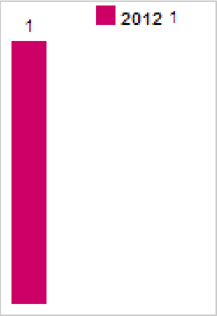
Vulnerabilities By Year



Vulnerabilities By Type

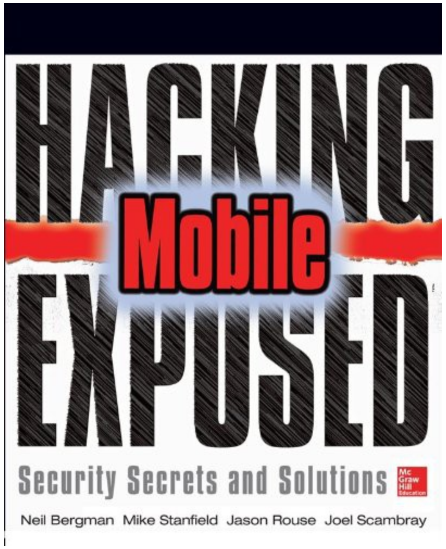


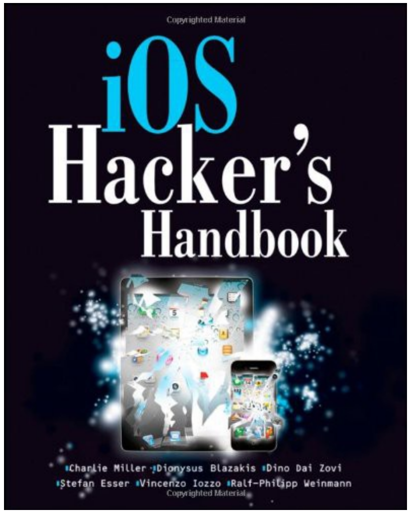
Vulnerabilities By Year

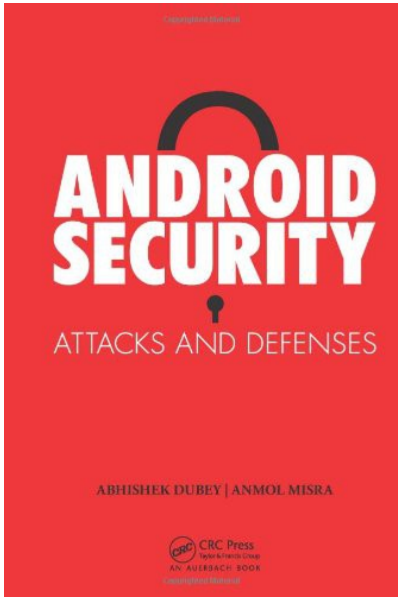


More mobile security

- Historically good technical site about mobile security
  - Not up to date with the latest stuff
  - http://www.mulliner.org/
- Hacking Exposed Mobile Security Secrets & Solutions (2013)
- iOS Hacker's Handbook (2012)
- Android Security: Attacks and Defenses (2013)
- XDA Developers' Android Hacker's Toolkit: The Complete Guide to Rooting, Roms and Theming (2012)

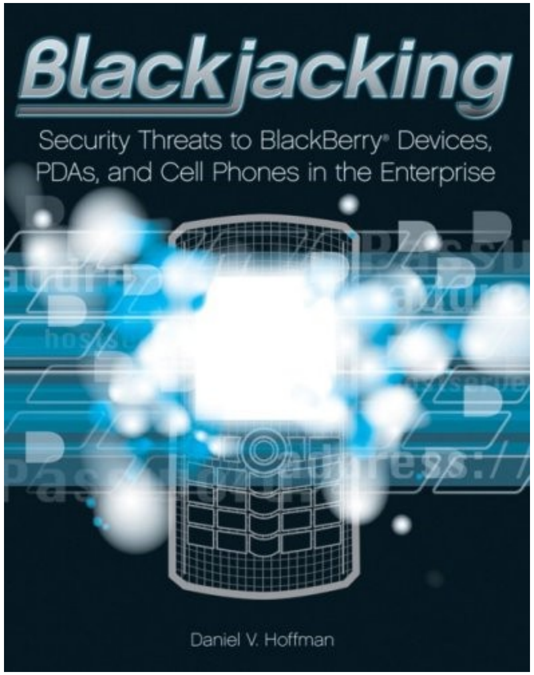

HACKING
Mobile
EXPOSED
Security Secrets and Solutions
Mc Graw Hill Education
Neil Bergman Mike Stanfield Jason Rouse Joel Scambray


Copyrighted Material
iOS
Hacker's
Handbook
Charlie Miller Dionysus Blazakis Dino Dai Zovi
Stefan Esser Vincenzo Iozzo Ralf-Philipp Weinmann
Copyrighted Material



Old mobile security (but still true)

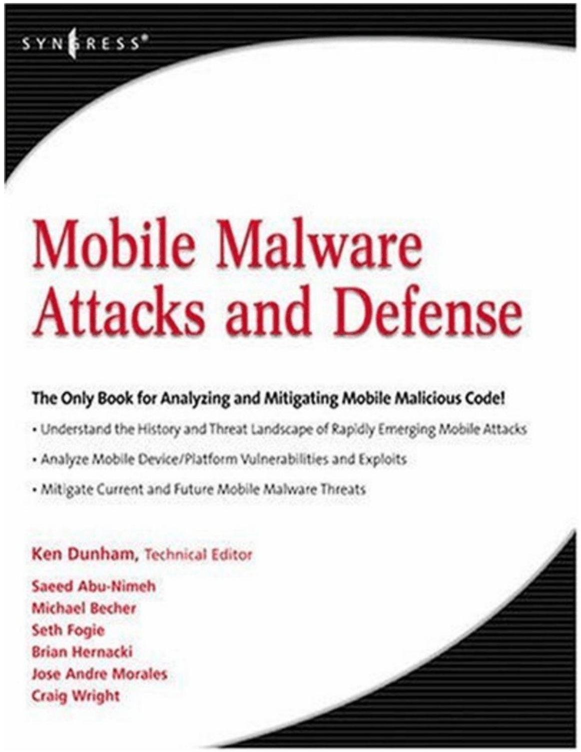
- Blackjacking - Security Threats to Blackberry, PDA's, and Cell Phones in the Enterprise (2007)
  - http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470127546.html
- Conlusion is that mobile phones must be treated exactly as computers regarding malware
  - Be equipped with personal firewalls
  - Have the latest updates
  - Be configured securely
  - Possess non-traditional antivirus programs
- Common attacks
  - Direct attack against OS and apps
  - Data-communication interception
  - Authentication spoofing and sniffing
  - Physical compromise
  - **WiFi connected phones may be an especially easy target in hotspots etc.**
  - **Do you connect to open WiFi networks?**


Blackjacking
Security Threats to BlackBerry® Devices, PDAs, and Cell Phones in the Enterprise
Daniel V. Hoffman

Mobile malware & analysis

Lookout

- Viaforensics and Lockout have many reports
  - https://www.lookout.com/
  - https://viaforensics.com/resources/reports/
- Google for
  - Mobile security reports
- With increasing numbers of smartphones malware have skyrocketed
  - Up 614% 2012 – 2013 (92% on Android)
  - http://www.mobilemarketingwatch.com/juniper-mobile-malware-threats-up-614-in-one-year-33875/
- Mobile malware attacks and defense (2008)
  - http://www.elsevier.com/wps/find/bookdescription.cws_home/715445/description



SYNGRESS®

Mobile Malware Attacks and Defense

The Only Book for Analyzing and Mitigating Mobile Malicious Code!

- Understand the History and Threat Landscape of Rapidly Emerging Mobile Attacks
- Analyze Mobile Device/Platform Vulnerabilities and Exploits
- Mitigate Current and Future Mobile Malware Threats

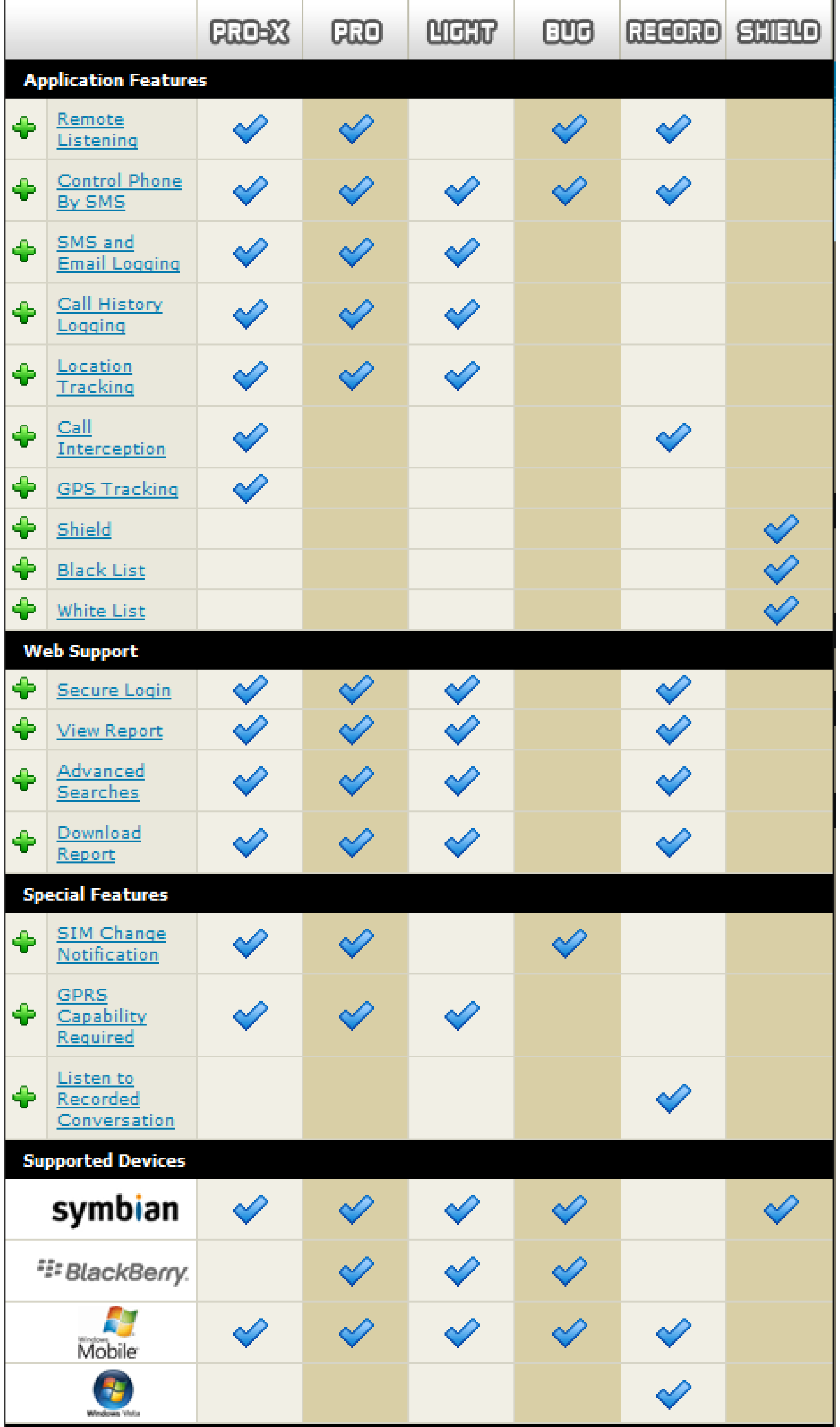
Ken Dunham, Technical Editor

Saeed Abu-Nimeh
Michael Becher
Seth Fogie
Brian Hernacki
Jose Andre Morales
Craig Wright

:)

- Snoopware
  - http://flexispy.com
  - iPhone support
  - http://www.f-secure.com/v-descs/flexispy_a.shtml
- Often (still!) SMS is used
  - Sexy View, 18 feb 2009
  - Trick users to install signed malware
- Nexus SMS bug

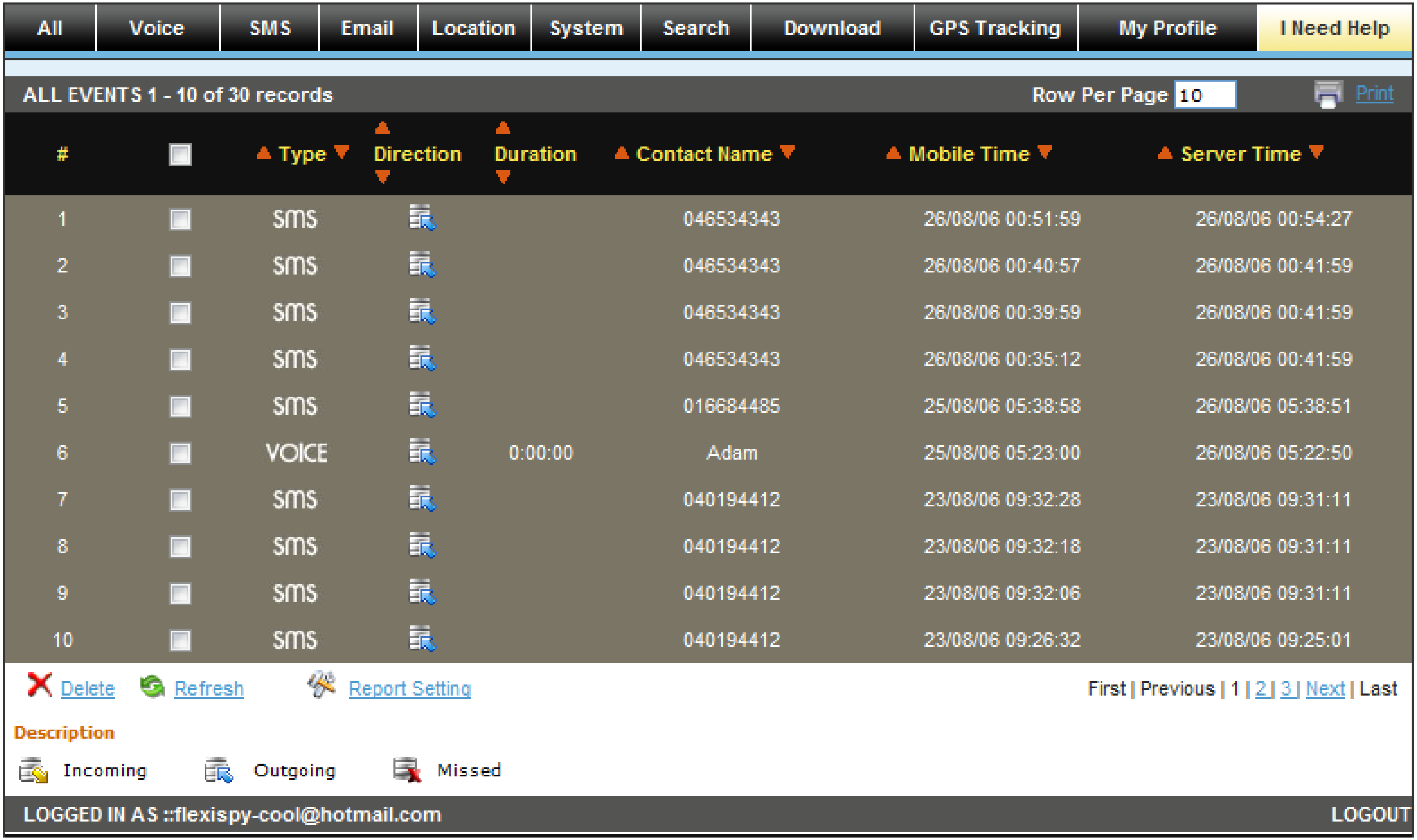
http://www.androidpolice.com/2013/11/29/sms-vulnerability-in-nexus-devices-can-be-exploited-to-force-a-reboot-or-kill-cellular-connectivity/



	PRO-X	PRO	LIGHT	BUG	RECORD	SHIELD
Application Features						
Remote Listening	✓	✓		✓	✓	
Control Phone By SMS	✓	✓	✓	✓	✓	
SMS and Email Logging	✓	✓	✓			
Call History Logging	✓	✓	✓			
Location Tracking	✓	✓	✓			
Call Interception	✓				✓	
GPS Tracking	✓					
Shield						✓
Black List						✓
White List						✓
Web Support						
Secure Login	✓	✓	✓		✓	
View Report	✓	✓	✓		✓	
Advanced Searches	✓	✓	✓		✓	
Download Report	✓	✓	✓		✓	
Special Features						
SIM Change Notification	✓	✓		✓		
GPRS Capability Required	✓	✓	✓			
Listen to Recorded Conversation					✓	
Supported Devices						
symbian	✓	✓	✓	✓		✓
BlackBerry		✓	✓	✓		
Windows Mobile	✓	✓	✓	✓	✓	
Windows Vista					✓	

FLEXISPY

Protect Your Children | Catch Cheating Spouses



ALL EVENTS 1 - 10 of 30 records

Row Per Page 10

#	□	Type	Direction	Duration	Contact Name	Mobile Time	Server Time
1	□	SMS	↗		046534343	26/08/06 00:51:59	26/08/06 00:54:27
2	□	SMS	↗		046534343	26/08/06 00:40:57	26/08/06 00:41:59
3	□	SMS	↗		046534343	26/08/06 00:39:59	26/08/06 00:41:59
4	□	SMS	↗		046534343	26/08/06 00:35:12	26/08/06 00:41:59
5	□	SMS	↗		016684485	25/08/06 05:38:58	26/08/06 05:38:51
6	□	VOICE	↗	0:00:00	Adam	25/08/06 05:23:00	26/08/06 05:22:50
7	□	SMS	↗		040194412	23/08/06 09:32:28	23/08/06 09:31:11
8	□	SMS	↗		040194412	23/08/06 09:32:18	23/08/06 09:31:11
9	□	SMS	↗		040194412	23/08/06 09:32:06	23/08/06 09:31:11
10	□	SMS	↗		040194412	23/08/06 09:26:32	23/08/06 09:25:01

Description

↙ Incoming ↗ Outgoing ✗ Missed

LOGGED IN AS ::flexispy-cool@hotmail.com