باسمه‌تعالی

کارگاه نسل نوین مدیریت امنیت سازمانی
دانشگاه بیرجند، مرکز آپا

فراآش

امنیت مدیریت ، مدیریت امنیت

شرکت فراکنش (۱۳۸۲)

موضوع ارائه:

امنیت در نسل دوم تا نسل پنجم شبکه‌های تلفن همراه

دکتر شهریار بیژنی
عضو هیات علمی دانشگاه شاهد
مدیرعامل شرکت فراکنش

اولین شرکت فعال
در حوزه امنیت
شبکه تلفن همراه
(از ۱۳۸۴)

❖ خدمات

- ❖ مشاوره امنیتی در حوزه شبکه‌های تلفن همراه نسل ۲، ۲.۵، ۳ و ۴
- ❖ تحلیل، ارزیابی امنیتی و تست نفوذ در شبکه‌های کامپیوتری و مخابراتی
- ❖ ارائه راهبردها و راهکارهای امنیتی در رایانش ابری
- ❖ تشخیص و مقابله با کلاهبرداری (Fraud) در شبکه‌ها
- ❖ راه‌اندازی و مدیریت گروه‌های پاسخگو به حوادث امنیتی (MERT و CERT)
- ❖ تحلیل، طراحی و تولید نرم‌افزارهای سازمانی امن
- ❖ تحلیل و ارزیابی امنیتی خدمات ارزش افزوده
- ❖ ارائه کارگاه‌ها و دوره‌های آموزشی تخصصی امنیت برنامه‌نویسی، امنیت نرم‌افزار و امنیت موبایل

- Why Security is Important?
- Security Mechanisms of 2G to 4G
- Attacks on 2G to 4G
- 5G Security Issues

Outline

Statistics

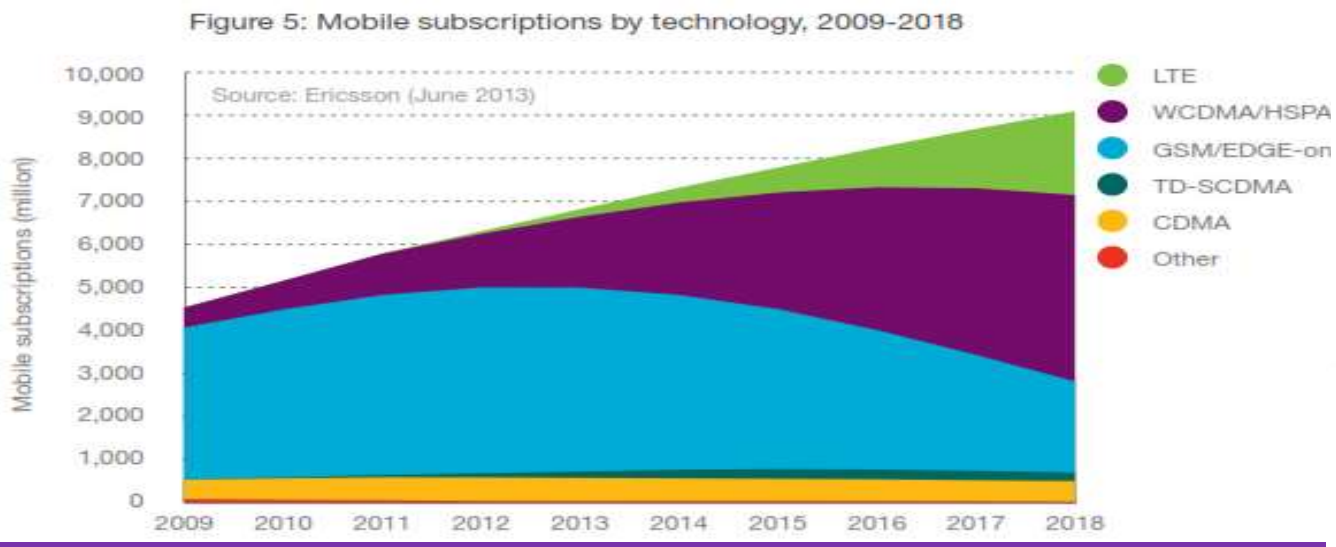


Figure 5: Mobile subscriptions by technology, 2009-2018
Source: Ericsson (June 2013)
Mobile subscriptions (million)
10,000
9,000
8,000
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
LTE
WCDMA/HSPA
GSM/EDGE-on
TD-SCDMA
CDMA
Other

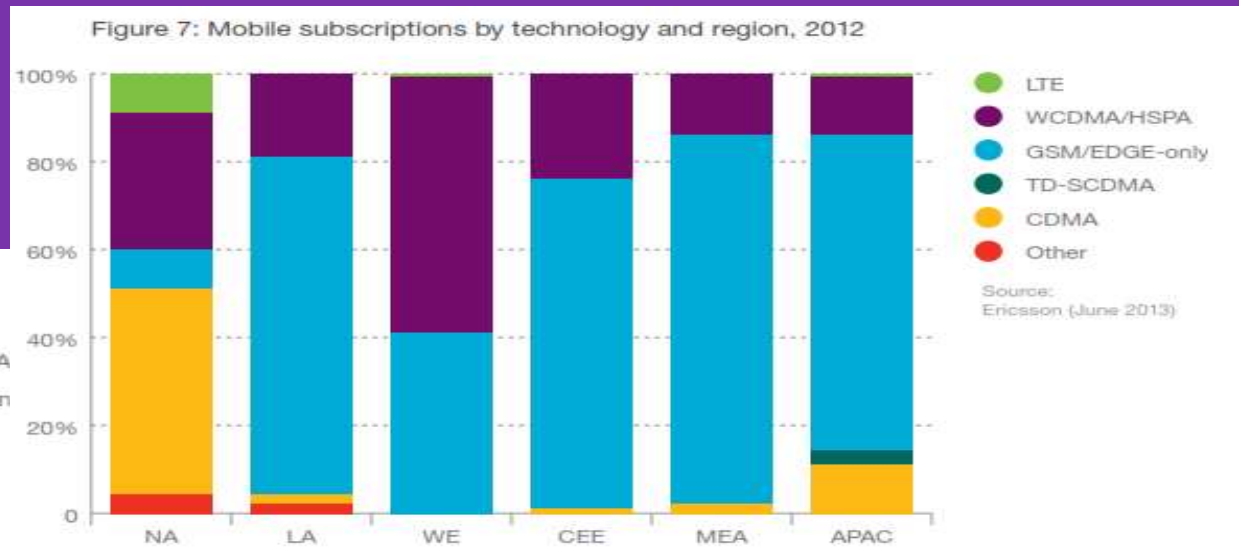


Figure 7: Mobile subscriptions by technology and region, 2012
100%
80%
60%
40%
20%
0
NA
LA
WE
CEE
MEA
APAC
LTE
WCDMA/HSPA
GSM/EDGE-only
TD-SCDMA
CDMA
Other
Source:
Ericsson (June 2013)

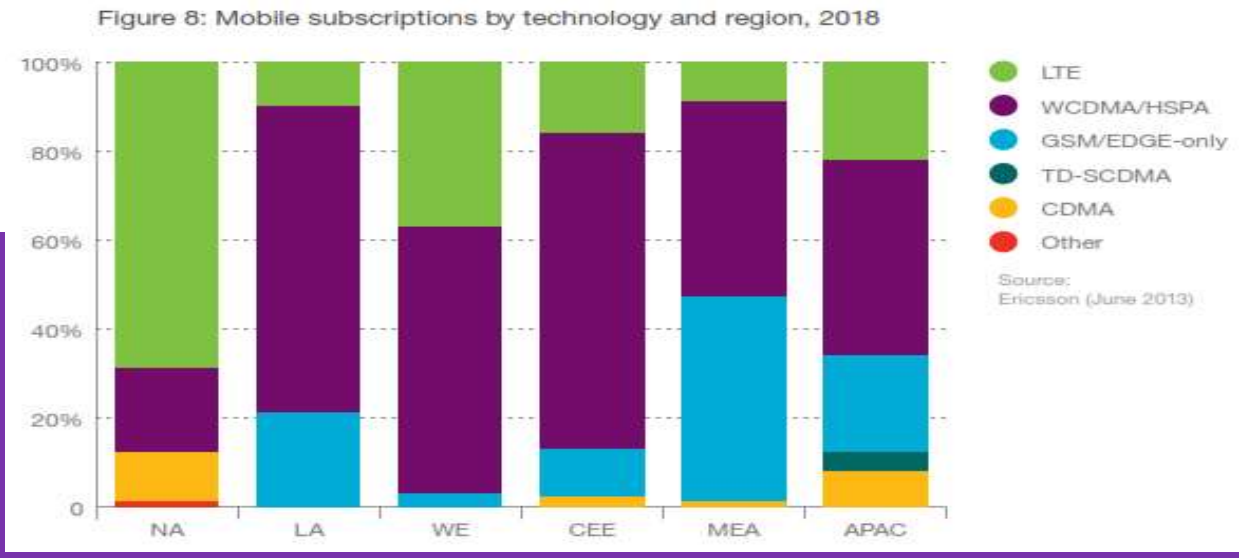
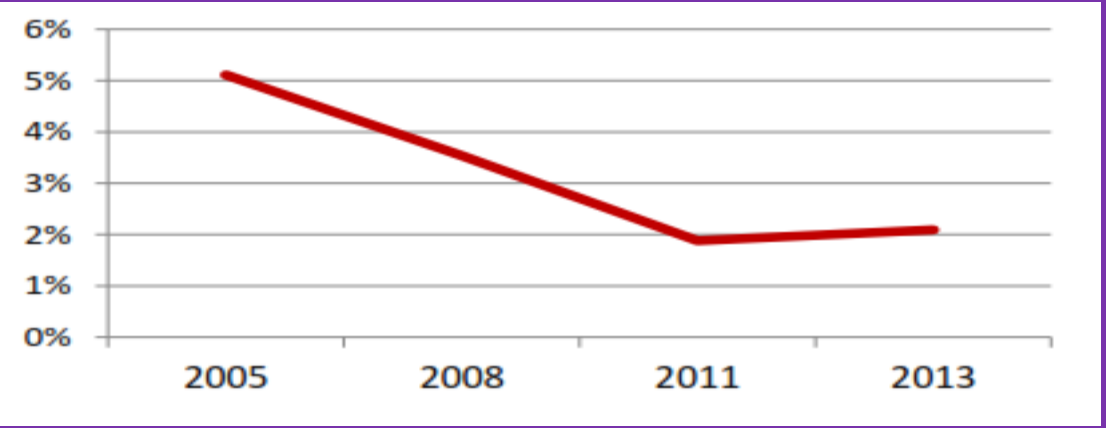


Figure 8: Mobile subscriptions by technology and region, 2018
100%
80%
60%
40%
20%
0
NA
LA
WE
CEE
MEA
APAC
LTE
WCDMA/HSPA
GSM/EDGE-only
TD-SCDMA
CDMA
Other
Source:
Ericsson (June 2013)

Statistics

- Sources of the Stats
  - Governments, Mobile Operators ,International Organisations (e.g. CTIA, CFCA, ACEF, i3Forum …)
- Estimated Communication Fraud Costs
  - 2000: $13 Billion (%5 of the revenue)
  - 2005: $61.3 Billion (%5.11 of the revenue)
  - 2008: $60.1 Billion (%3.54 of the revenue)
  - 2011: $40.1 Billion (%1.88 of the revenue)
  - 2013: $46.3 Billion (%2.09 of the revenue)

Est. Global Telecom Fraud Loss: (CFCA, 2013)



Security Mechanisms in 2G to 4G

www.faraconesh.com

Security Mechanisms in Mobile Networks

Common Security Mechanisms (GSM, GPRS,3G,4G):

- **Anonymity**
- **Authentication**
- **Confidentiality**

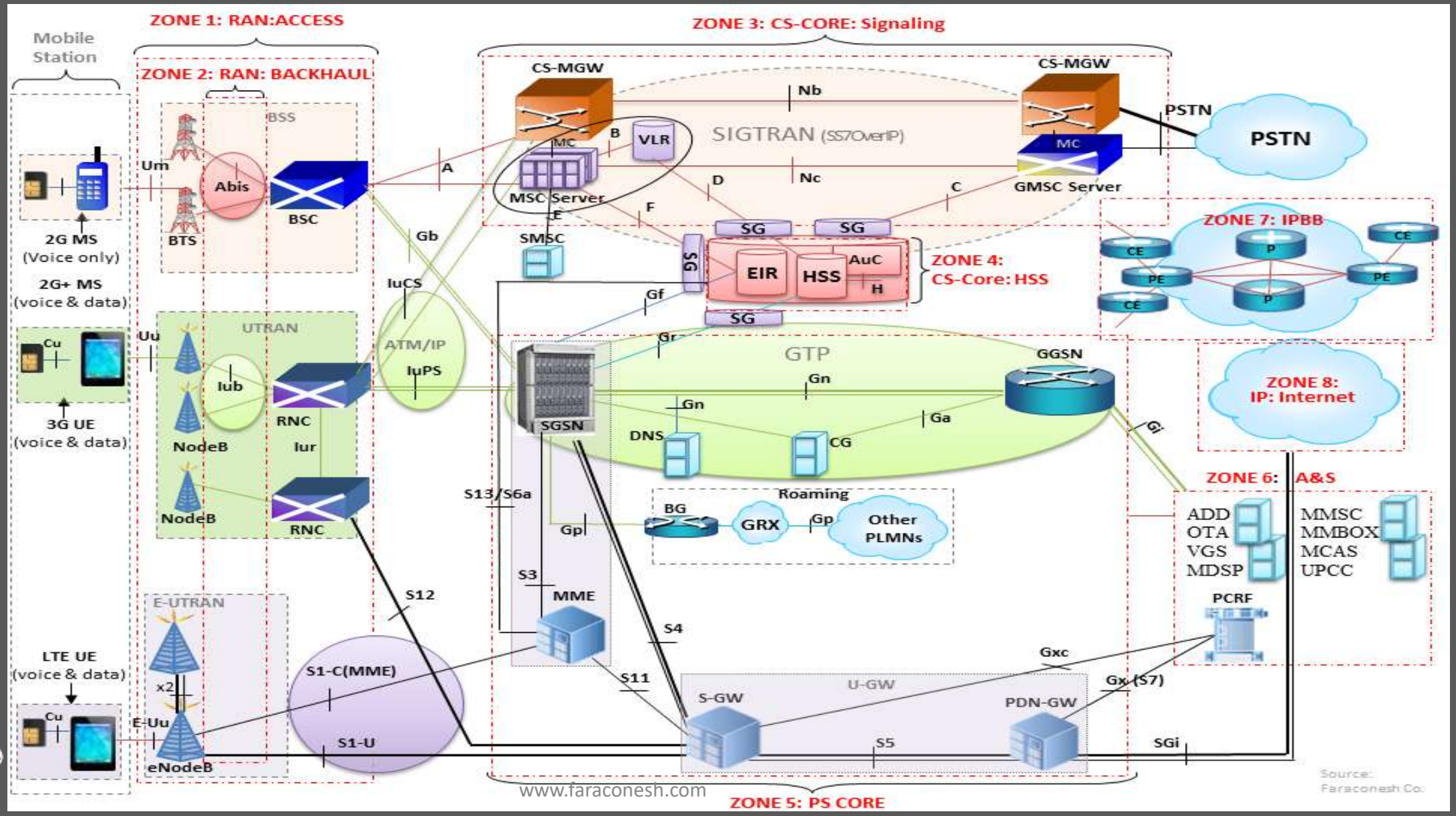
3G+

- **Mutual Authentication**
- **Integrity**
- **Enhancement of the Above Features**

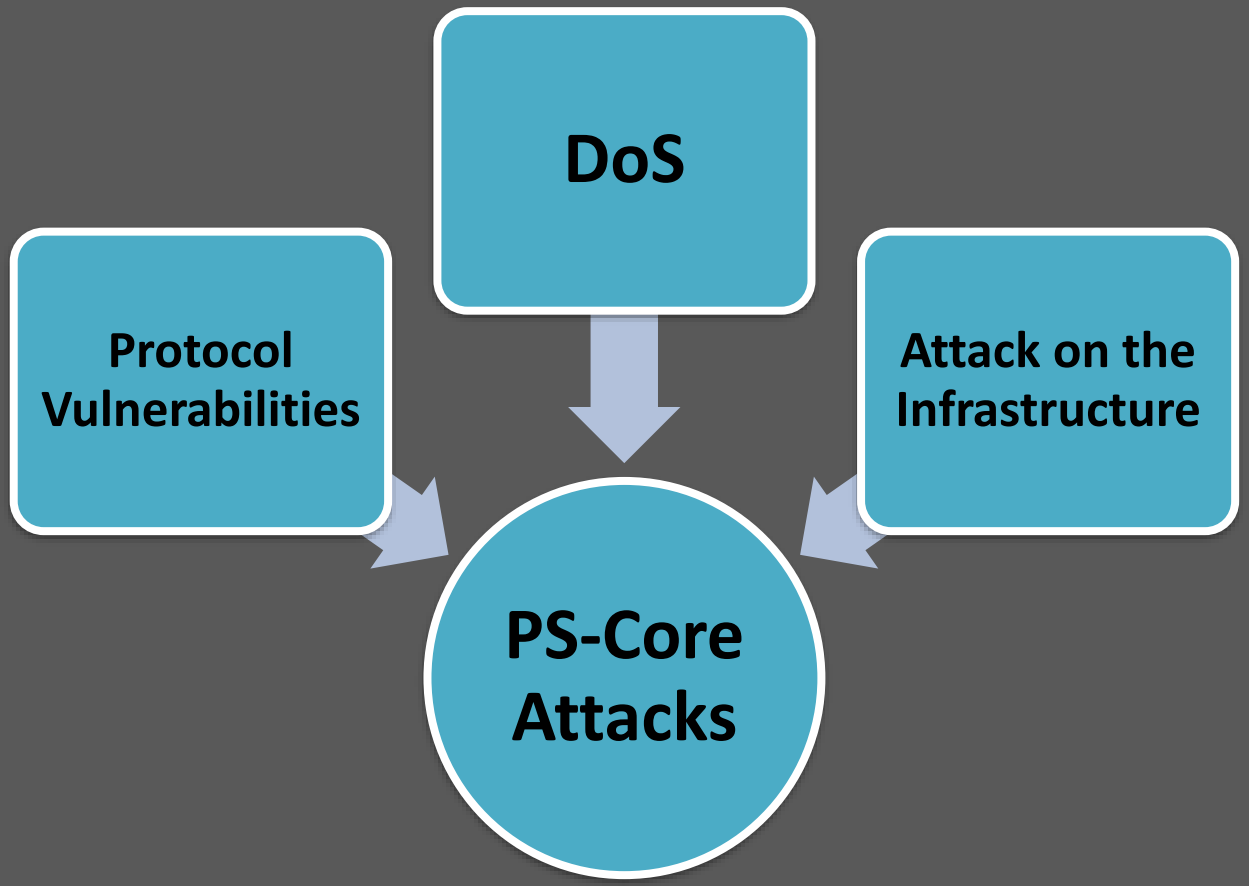
Security Attacks on 2G to 4G

www.faraconesh.com

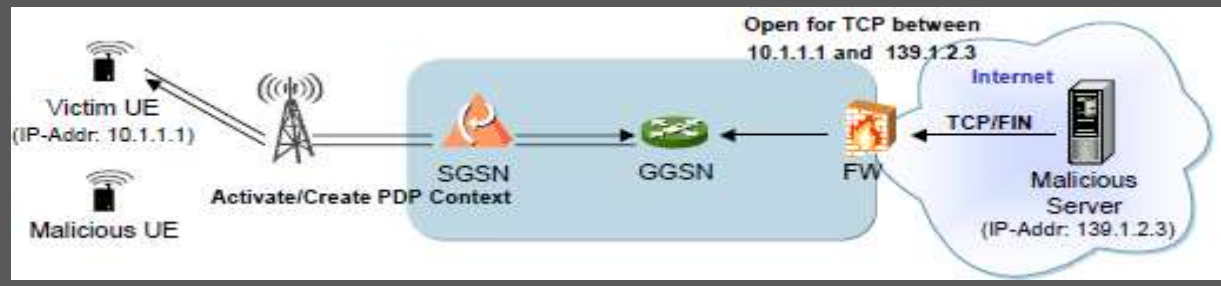
Mobile Network Zones: 2G to 4G

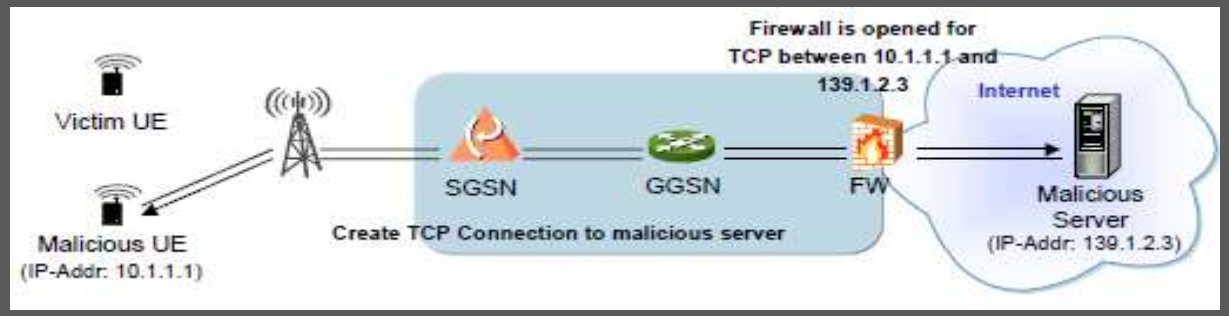


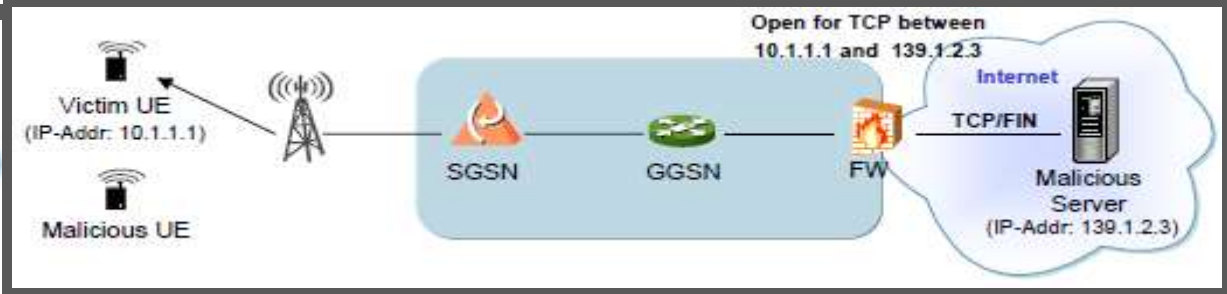
Attacks on PS-Core

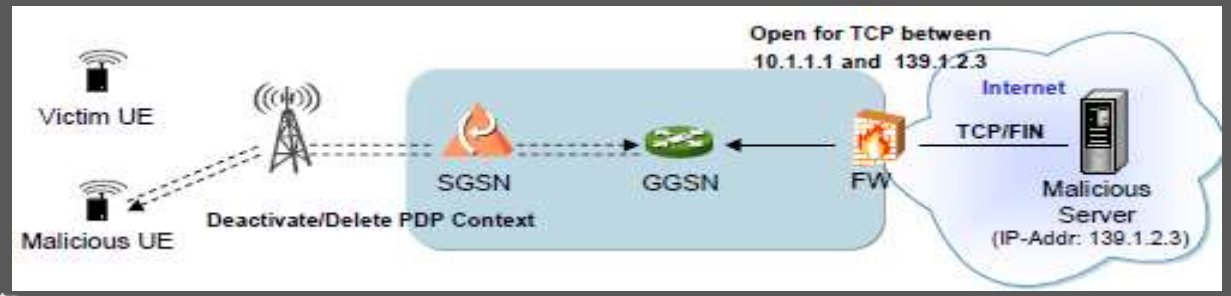


An Example of Overbilling Attack









Attack on Access Networks

DoS attack on Network Cells

Signaling Attacks (SMS, USSD):

- SMS and USSD both use the **SDCCH or FACCH** channels
- These channel are used for call-setup, so
- ***many open USSD sessions may limit new call-setups in the networks.***

Fake BTS/ Fake Node B

Tools

GSS-ProA

- Fully passive (non-detectable) off air interception of GSM communications
- Interception of A5.1, A5.2, A5.3 Encrypted Voice Channels
- Ki-Grab: Extraction oh Ki off air from a distance of 6.5 Km
- Totally covert operation to both target phone as well as network provider
- Automatically intercepts calls to/from target from flagged database
- Will intercept calls made in another countries.
- Standard version has 4 channels in full duplex
- Unit will intercept SMS, Fax and also E-mail.
- Built-in tracking system of targets location, with near GPS accuracy even when target is inside buildings.
- Built-in Voice Recognition System (Military RF Triangulation Technology)
- Automatic or manual scanning of frequency channels search for emission of system cells
- Definition of work regimes and emission parameters, Auto or manual adjustment of reception track on receipt of signal from base station
- Saving of adjustment current configuration as a file on disk, Auto loading of any previously saved configurations
- Recording facility of conversations onto PC hard disk, or to exterior recording system
- Auto monitoring of subscribers from database., Ability to listen & tape conversations in real time.
- Ability to hold and display the protocol of transactions in receiving base stations and protocol of monitored subscribers
- Display of current conditions of receiving channels (presence of synchronization, level and strength signal, and activity in temporary slots)
- Monitoring radius typically 1-5 km with high gain antennas.
- Once any of the number has been stored (as the TMSI, IMSA, or the IMEI) the unit will automatically log into the target's cell phone if it is in operation in the network

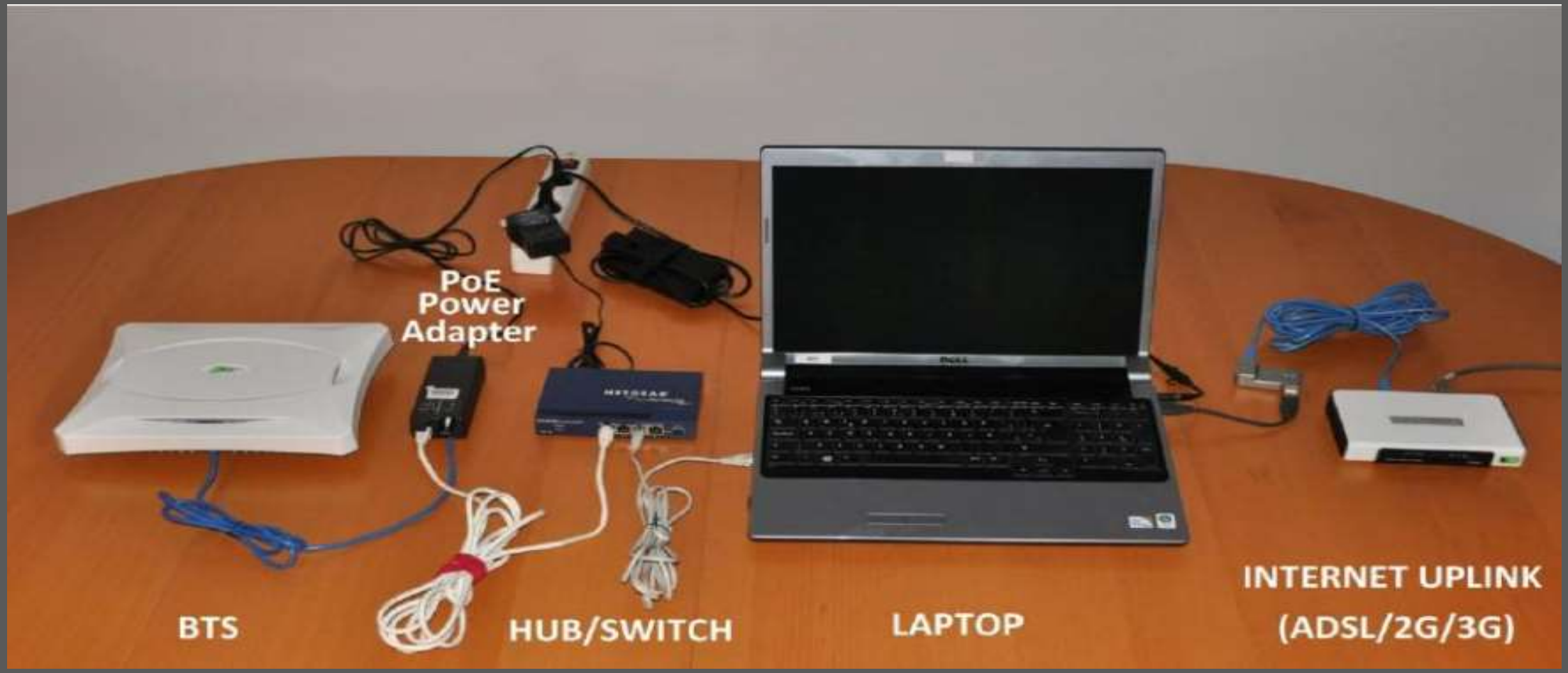
www.faraconesh.com

Tools

GSM Interceptor Pro

- 8 channels 900/1800 MHz,
- (System with 1900 MHz is also available).
- The system can target specific numbers or randomly screen GSM mobile Communication.
- Conversations are monitored and logged simultaneously to voice and data logger for storage and retrieval
- Housed in industrial PC 19” rack mounted portable cabinet with attached keyboard and LCD monitor. Weight:12 Kg
- Decodes voice codes LPT, RPE and EFR.
- Works with identificators IMSI, TMSI, IMEI,and MSISDN.
- Can receive BCCH, CCCH, SACCH, SDCCH, FACCH, and TCH.
- Find incoming call number when call ID is available.
- Intercept 1 voice duplex Channel.
- Possibility to receive SMS Messages.
- Working range: Forward Channel 25 KM, Reverse Channel depends on conditions - varies from 300 to 800 meters

Attack Tools!



Nano BTS (NodeB)

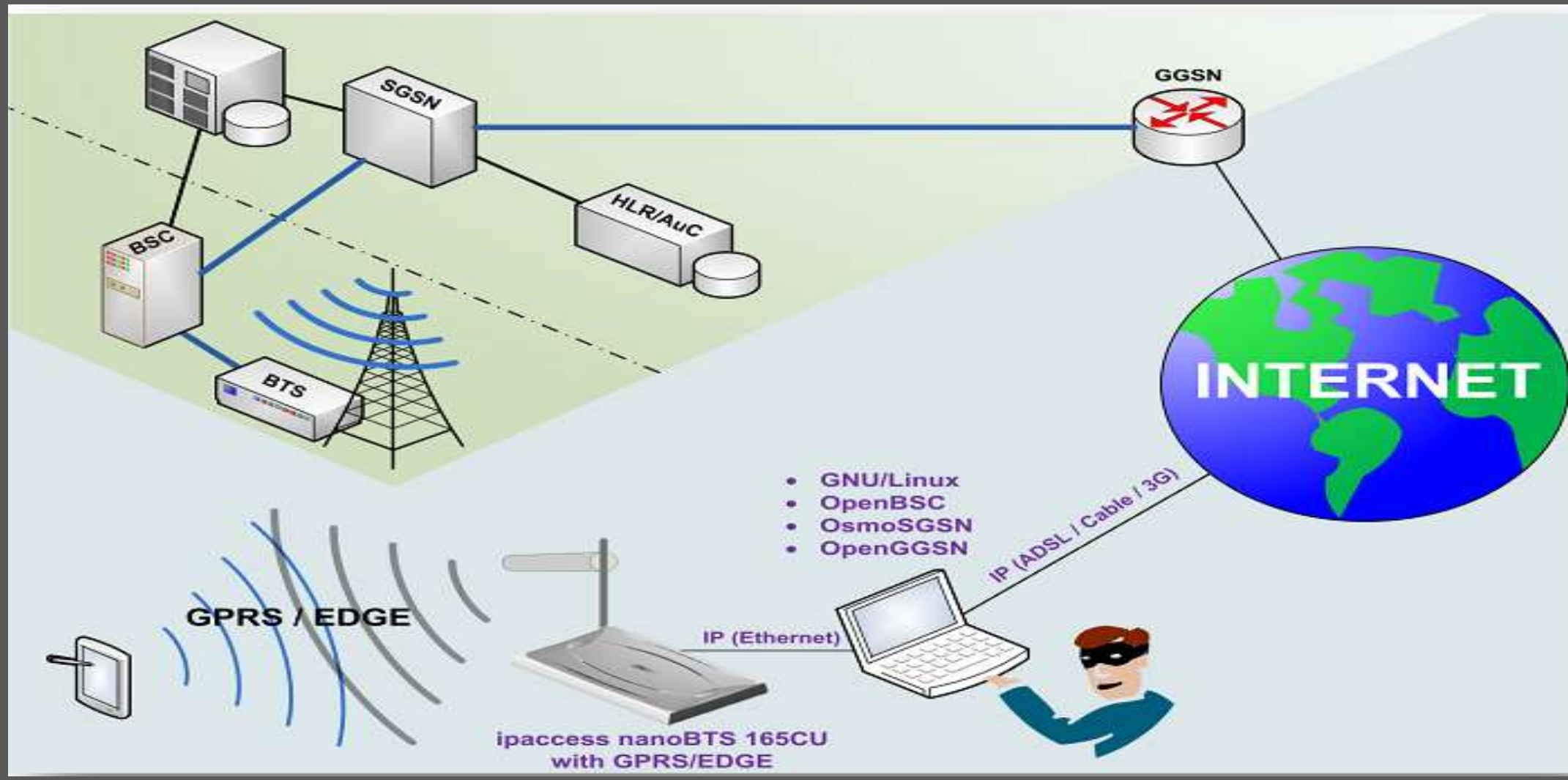
ip.access nanoBTS - Model 165CU - EGSM900

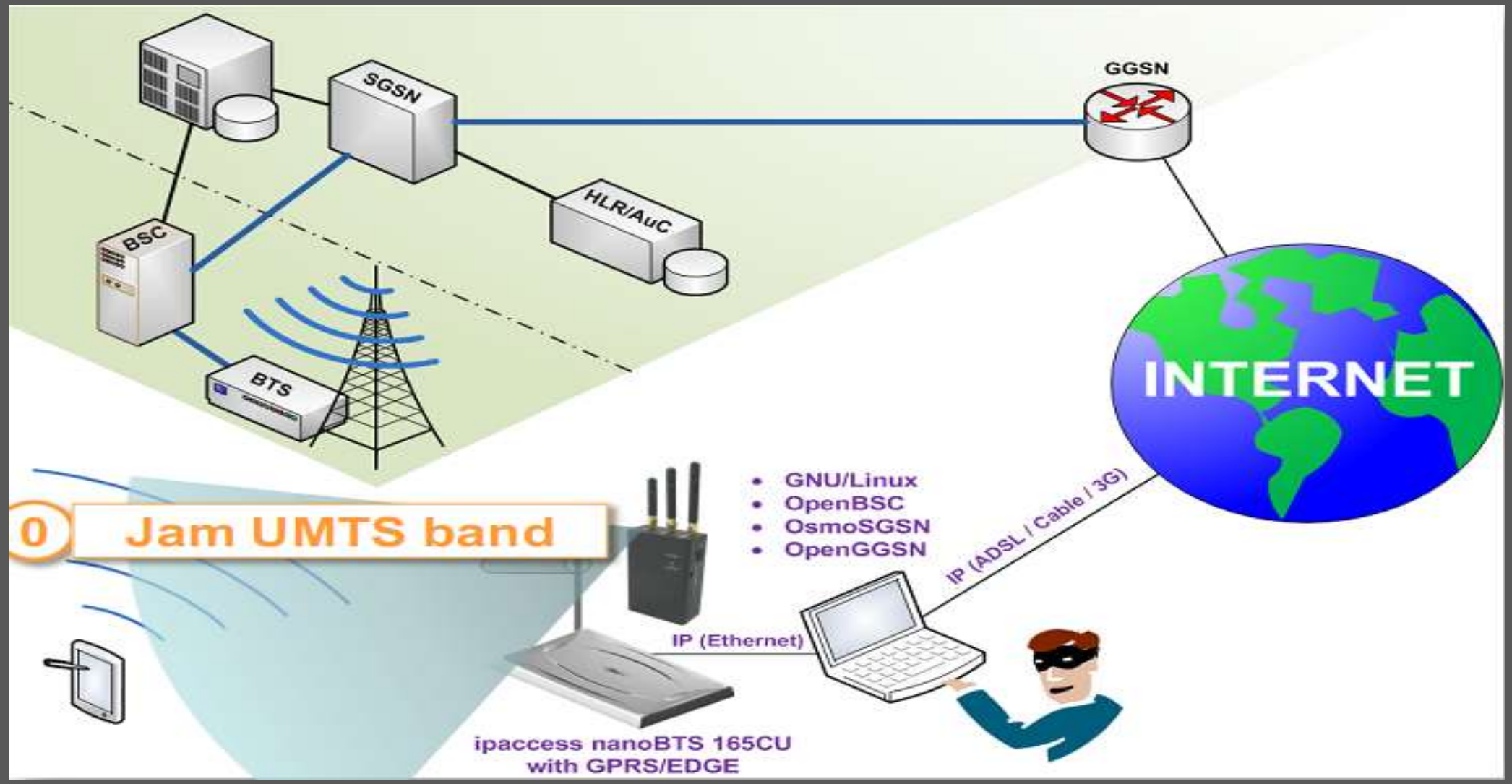
Attack Software:

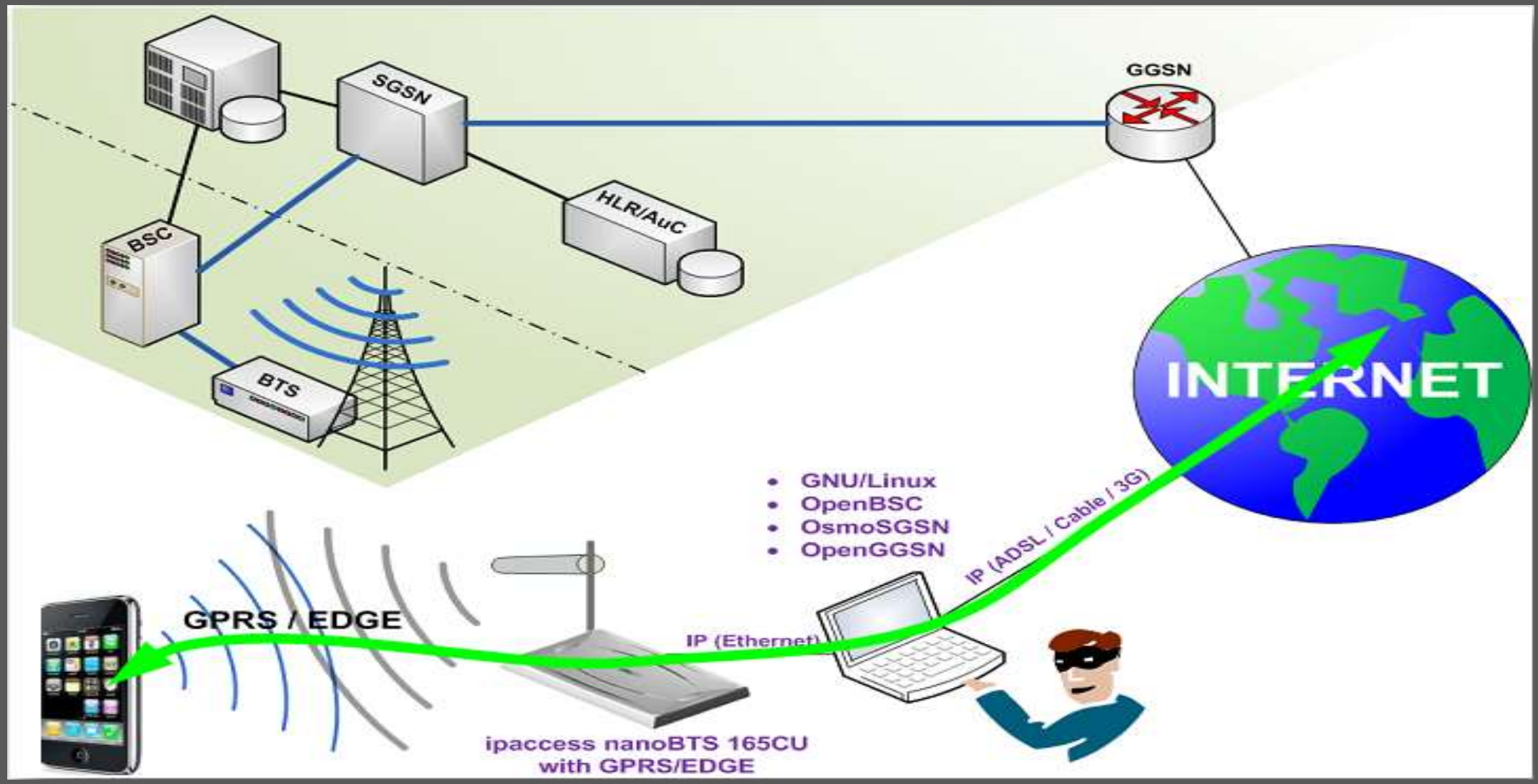
- Linux OS
- OpenBSC
- OsmoSGSN
- OpenGGSN

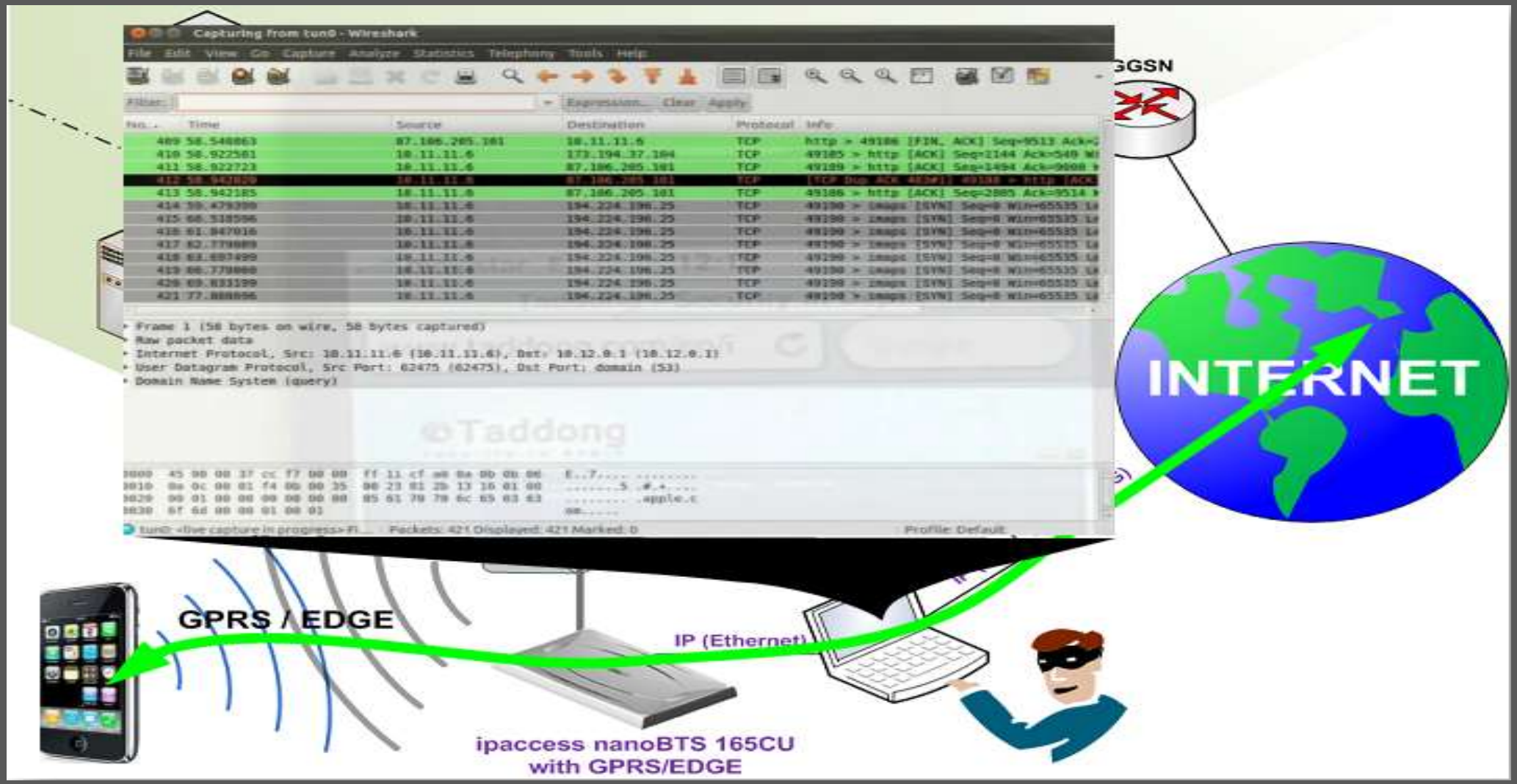
Jammer

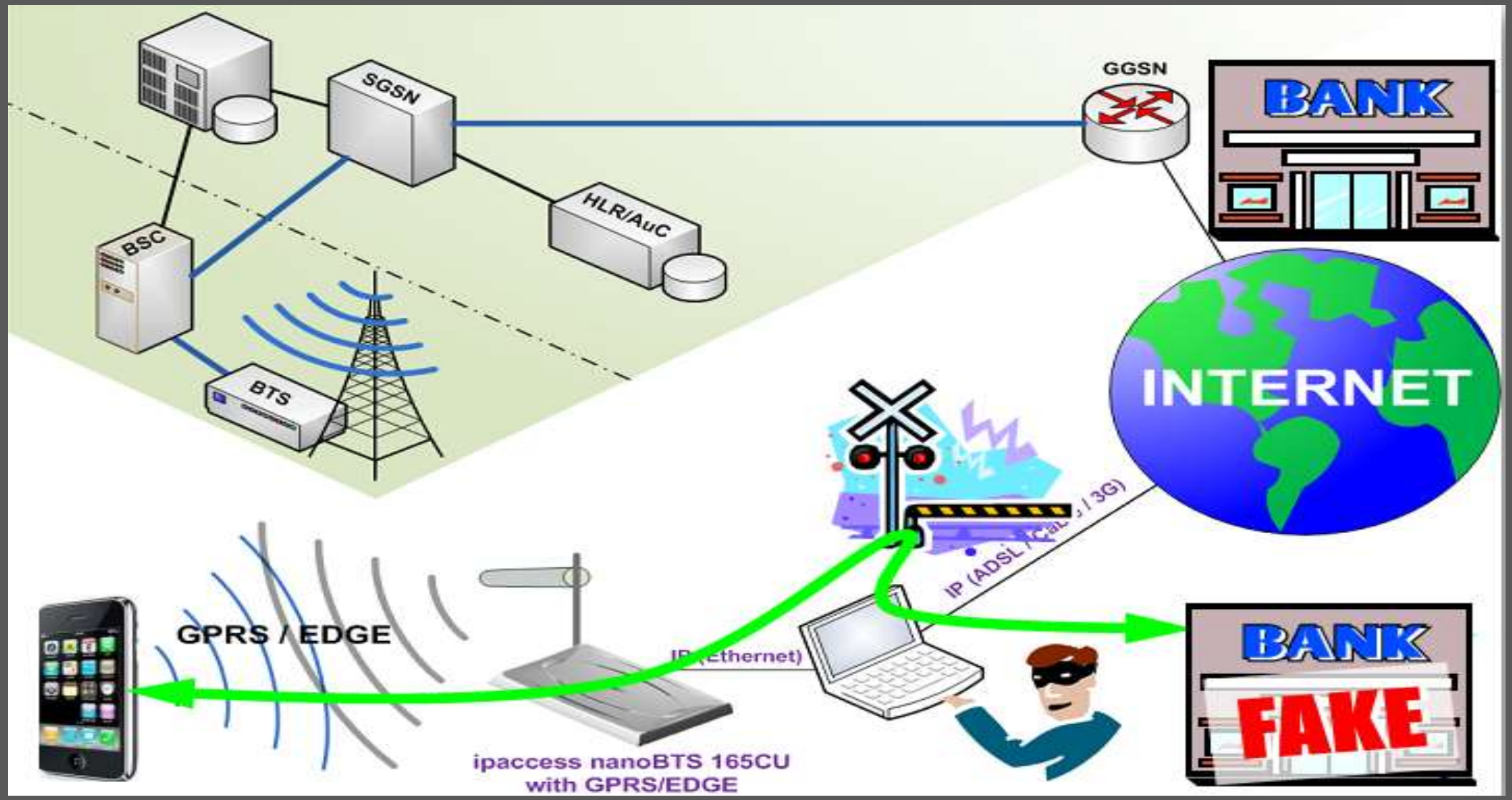
http://www.techwisetech.com/products/PCB1050.htm

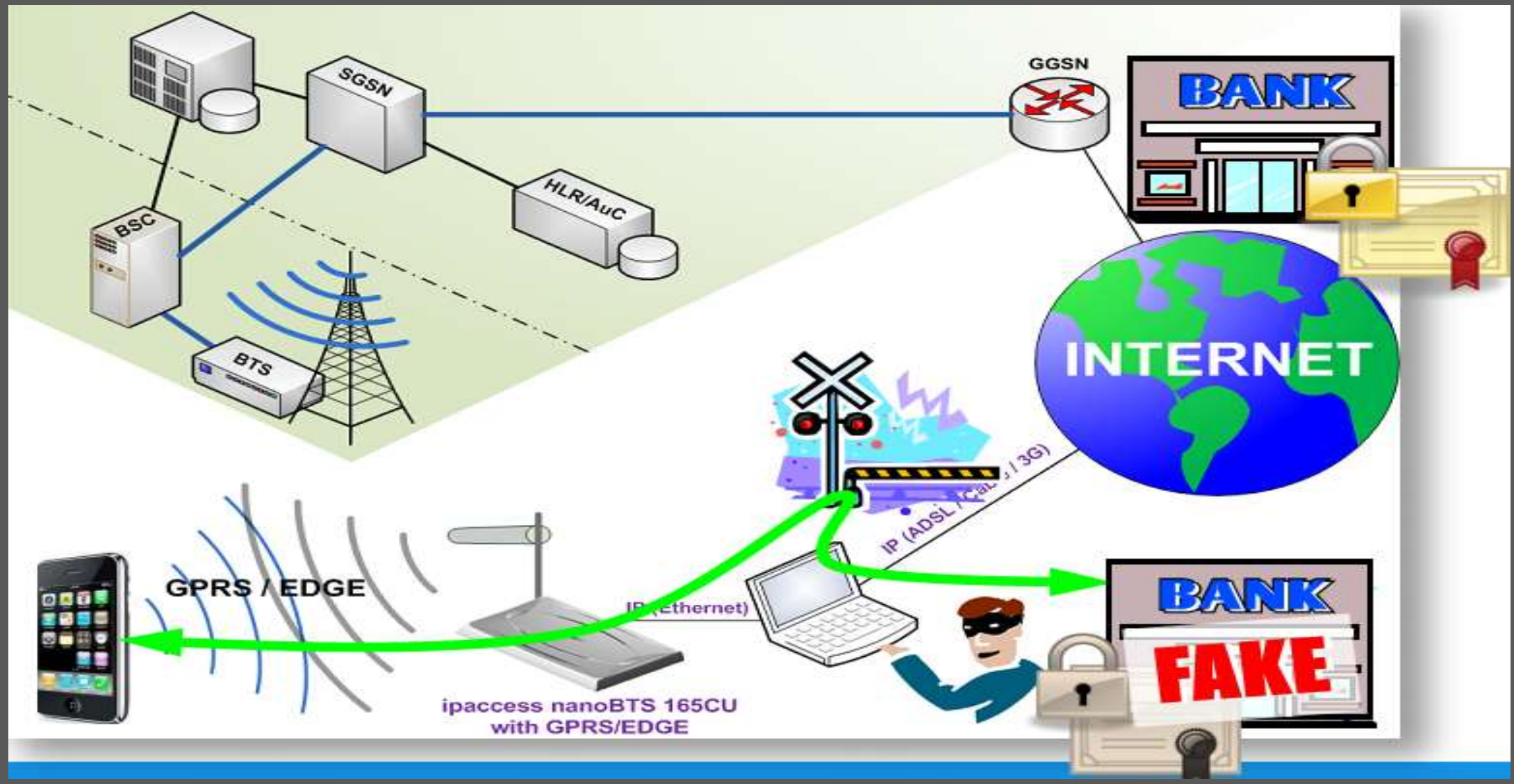

SGSN
GGSN
HLR/AuC
BSC
BTS
INTERNET
GNU/Linux
OpenBSC
OsmoSGSN
OpenGGSN
IP (ADSL / Cable / 3G)
GPRS / EDGE
IP (Ethernet)
ipaccess nanoBTS 165CU
with GPRS/EDGE

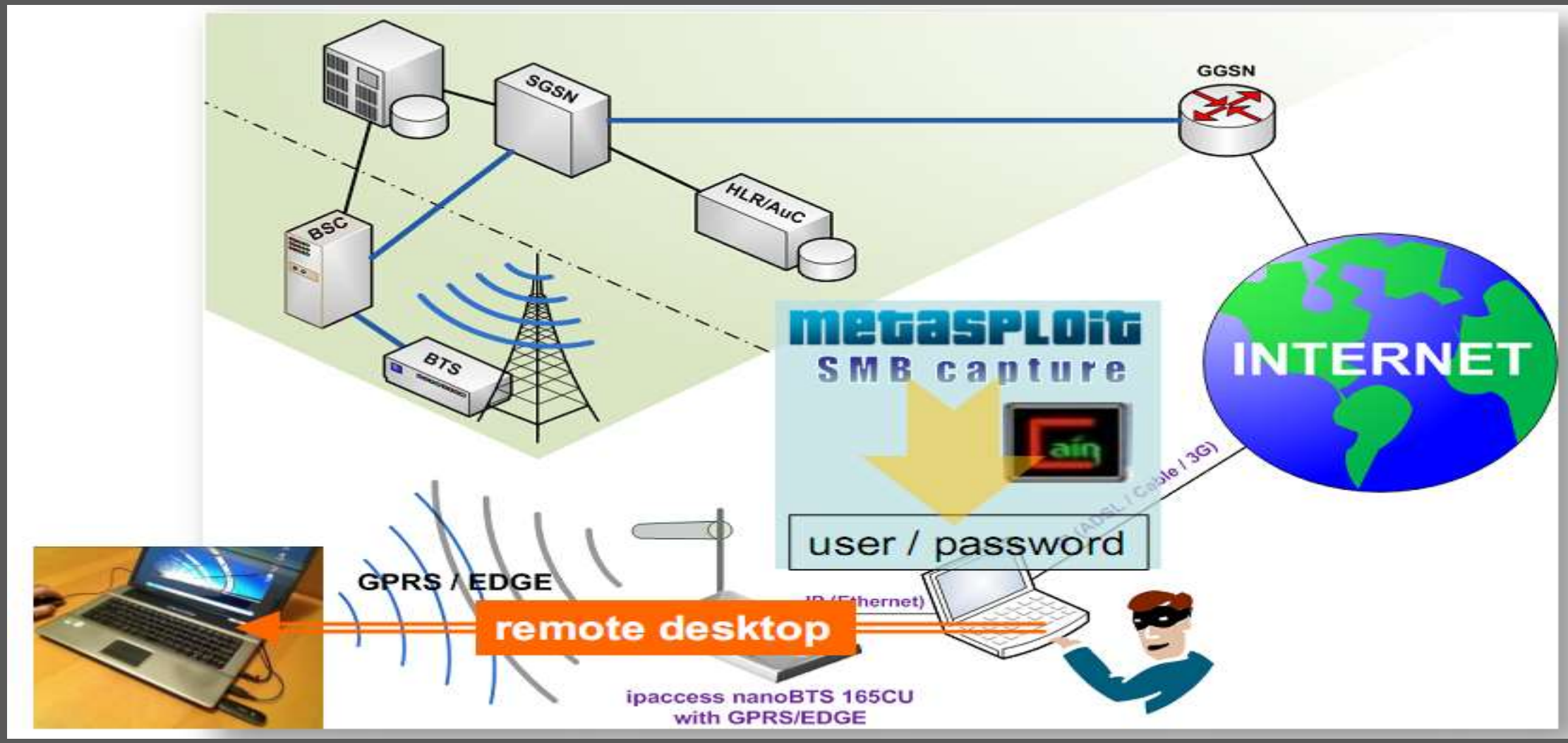

SGSN
GGSN
HLR/AuC
BSC
BTS
INTERNET
0
Jam UMTS band
GNU/Linux
OpenBSC
OsmoSGSN
OpenGGSN
IP (ADSL / Cable / 3G)
IP (Ethernet)
ipaccess nanoBTS 165CU
with GPRS/EDGE

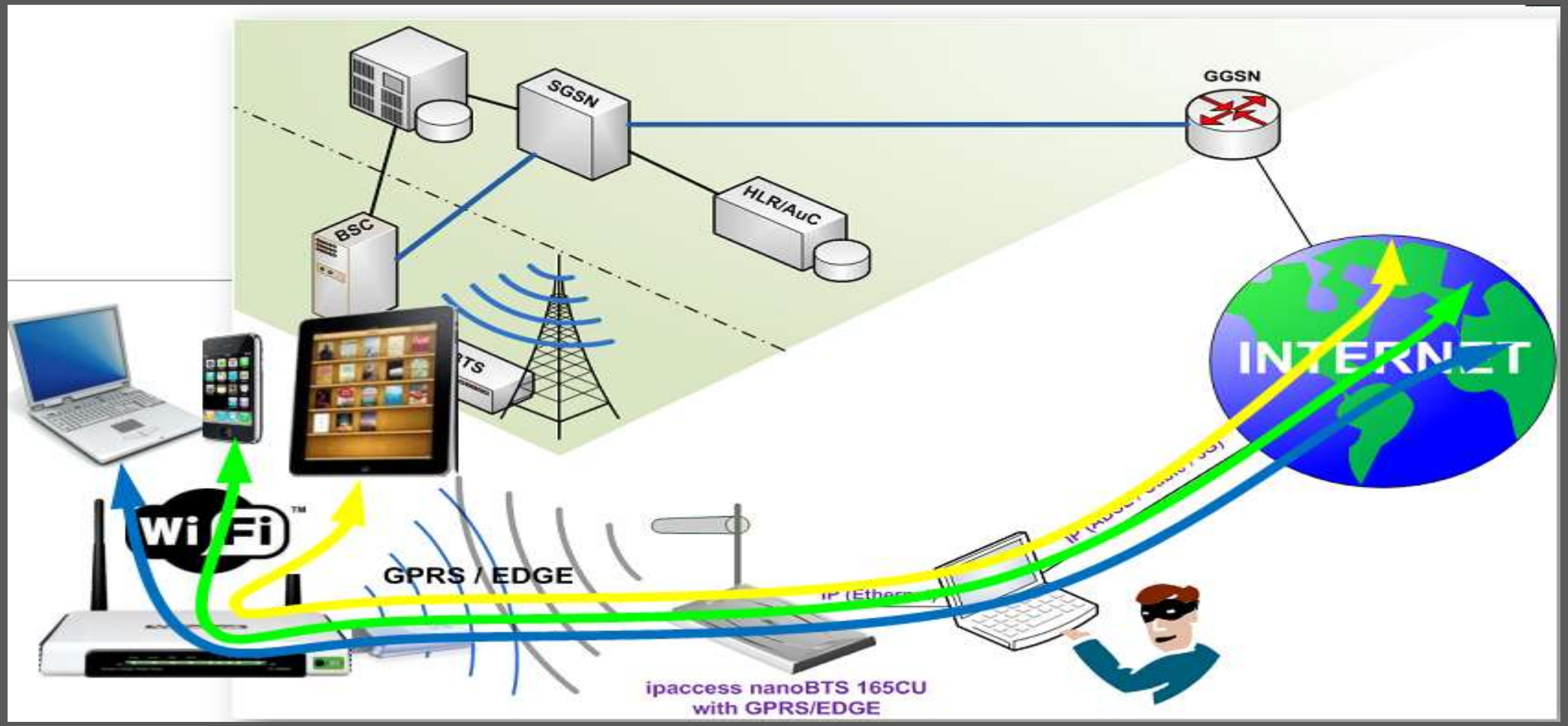

SGSN
GGSN
HLR/AuC
BSC
BTS
INTERNET
GNU/Linux
OpenBSC
OsmoSGSN
OpenGGSN
IP (ADSL / Cable / 3G)
GPRS / EDGE
IP (Ethernet)
ipaccess nanoBTS 165CU
with GPRS/EDGE


Capturing from tun0 - Wireshark
GGSN
INTERNET
GPRS / EDGE
IP (Ethernet)
ipaccess nanoBTS 165CU
with GPRS/EDGE


SGSN
GGSN
BANK
HLR/AuC
BSC
BTS
INTERNET
GPRS / EDGE
IP (Ethernet)
ipaccess nanoBTS 165CU
with GPRS/EDGE
BANK
FAKE


SGSN
GGSN
BANK
HLR/AuC
BSC
BTS
INTERNET
GPRS / EDGE
IP (Ethernet)
ipaccess nanoBTS 165CU
with GPRS/EDGE
BANK
FAKE


SGSN
GGSN
HLR/AuC
BSC
BTS
metasploit
SMB capture
INTERNET
user / password
GPRS / EDGE
remote desktop
ipaccess nanoBTS 165CU
with GPRS/EDGE


SGSN
GGSN
HLR/AuC
BSC
INTERNET
GPRS / EDGE
ipaccess nanoBTS 165CU
with GPRS/EDGE

5G Security

www.faraconesh.com

More Security Issues on 5G!

Why?

- the IP-based **open architecture** of the 5G system
- the diversity of the **access network** technologies
- Huge # of mobile & dynamic **communicating devices**
- the **heterogeneity of device** types in terms of their computational, battery power and memory storage capabilities
- the **open operating systems** of devices
- **non-professional users** in security issues

5G Security Threats

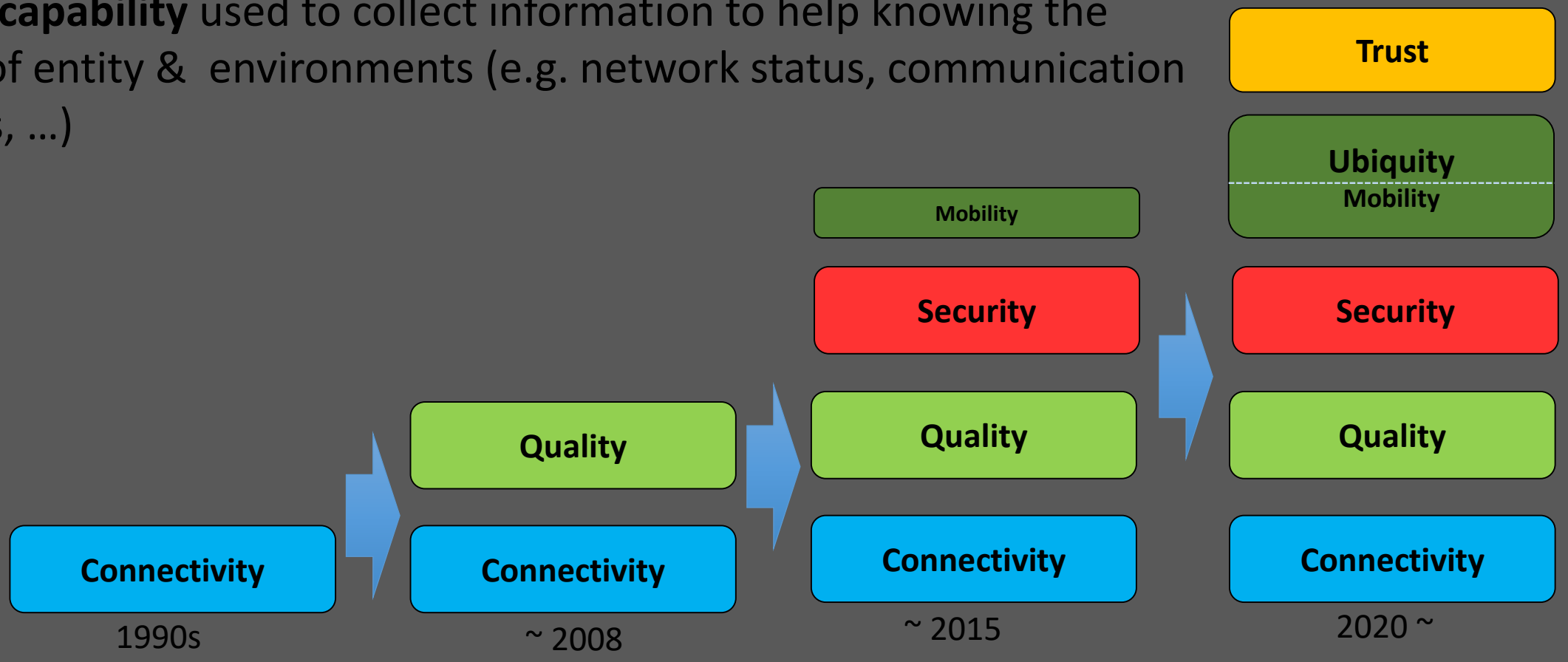
- **All the security threats of the Internet** !:Since 5G is a secure IP based solution.
- **Compromise of a single operator may lead to the collapse of the entire network infrastructure:** Since all the network operators and service providers would share a common core network infrastructure.
- **The theft of service and billing frauds**: third-parties can masquerade as legitimate users.
- **Spam over VoIP** may become serious: the Spam over Internet telephony (SPIT).
- **Interception** of private communications.
- **Phishing attacks:** Smishing (via SMS) and Vishing (voice-mail messages)
- **Stealing** bank account details and other secured information, are more likely

Security Attacks on 5G

- *User Equipment*
  - Mobile Malware, BotNet, ….
- Access Networks
  - Attacks on 4G Access Network
    - UE Location Tracking
      - UE Location Tracking Based on C-RNTI
        - Based on Cell Radio Network Temporary Identifier (C-RNTI)
        - Based on the packet sequence numbers
    - Attacks Based on False Buffer Status Reports
    - Message Insertion Attack
  - HeNB Femtocell Attacks
- Attacks on Core Network
- Attacks from external IP networks

Evolution in Mobile Generations

- **Smart Capabilities for Trustworthy:**
  - **trustworthiness relationships:** each parties should knew others
  - The **level of trust**: dependent on the level of knowing each other
  - **Smart capability** used to collect information to help knowing the details of entity & environments (e.g. network status, communication sessions, …)



آدرس: خ سهروردی جنوبی، ساختمان بانک تجارت ، پلاک ۲۷۱ ، طبقه ۲ ، واحد ۳

پست الکترونیک:info@faraconesh.com

فراکنش

تلفن:۸۸۳۷۰۳۸۳

www.faraconesh.com

امن سازی شبکه های ارتباطات سیار - تولید نرم افزار های امنیتی

ارائه خدمات مدیریت امنیت - امنیت شبکه های کامپیوتری و مخابراتی

فراکنش

امنیت مدیریت ، مدیریت امنیت

www.faraconesh.com

WWW.FARACONESH.COM