Why Nation-State Malwares Target Telco Networks:

Dissecting Technical Capabilities of Regin and Its Counterparts

Author: Ömer Coşkun

***The supreme art of war is to subdue the enemy without fighting**. Sun Tzu*

Outline

1

- Overview
  - Telecom Network Architecture
  - Practical Attack Surfaces
    - GRX Attack Vectors
    - SS7 Attack Vectors
  - Practical Attack Scenarios

- Rootkit Attacks: Regin and it's counterparts
  - Common Rootkit Techniques and Regin
  - Regin vs. Uruborus and Duqu
  - ***Demo: PoC || GTFO***

- Questions ?

$ whoami

Ömer Coşkun (@0xM3R)

- BEng. Computer Science

Research Assistant in Quantum Cryptography & Advanced Topics in AI

- Industry Experience

KPN – CISO , Ethical Hacking

Verizon – Threat & Vulnerability Management

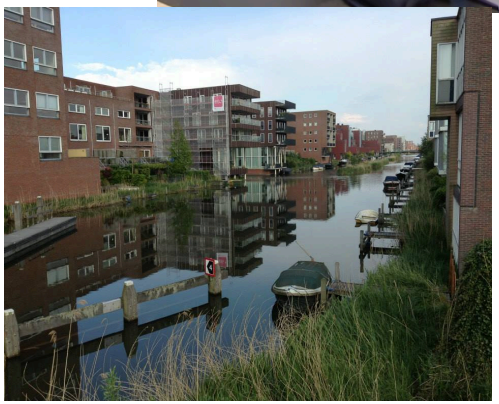
IBM ISS – Threat Intelligence

- Interests

Algorithm Design, Programming, Cryptography, Reverse Engineering, Malware Analysis, OS Internals, Rootkits

$ REDteam

3



kpn

Motivations

4

- Analyze existing vulnerabilities and attack surface of GSM networks
- Governments hack their own citizens
- Surveillance implants shifted focus to telecom networks and network devices
- European Telco companies are really paranoid after Regin attack
- Rootkits are fun : a lot to learn & challenge
- Reproduce the attack scenario and implement it!

GSM Network Architecture

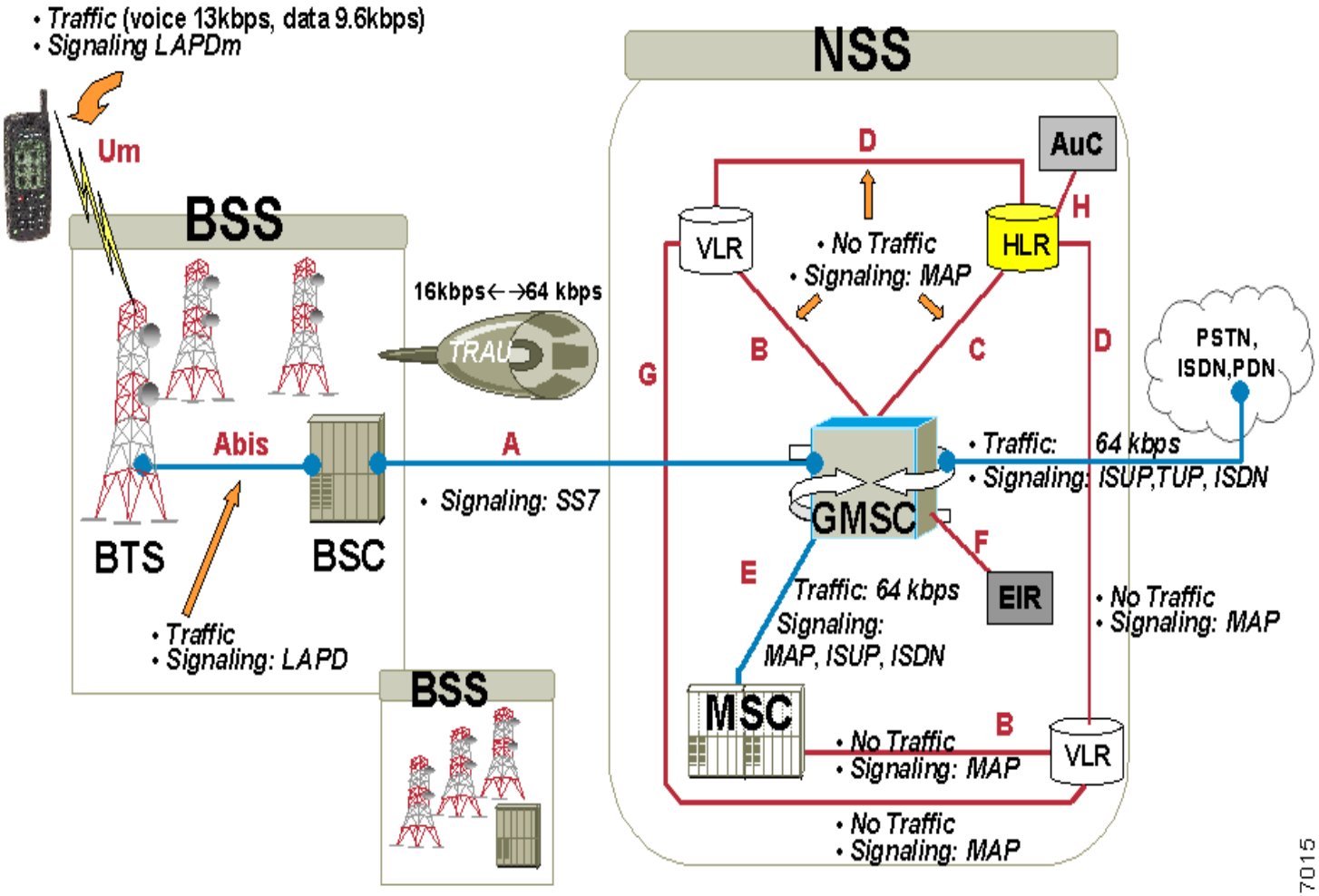
5

UMTS
Node B
RNC
PLMN
GPRS
BG
SGSN
GGSN
Internet
Circuit Switched
Packet Switched
EIR
SMSC
HLR
AUC
BTS
PCU
BSC
GSM
MSC
VLR
OMC
NMC
TMN
ISDN
PSDN

Auteur GIRODON Stéphane

kpn

GSM Network Architecture



77015

Regin targets GSM Networks

7

Regin: nation-state ownage of GSM networks

"Beware of Regin, the master! His heart is poisoned. He would be thy bane..."

By GReAT on November 24, 2014. 2:00 pm

The Register
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE BUSINESS HARDWARE SCIENCE BOOTNOTES

'Regin': The 'New Stuxnet' spook-grade SOFTWARE WEAPON described

'A degree of technical competence rarely seen'

Anti-surveillance rally. Berlin, Ju

Regin Is 'Groundbreaking' Malware Used by UK Spooks

November 24, 2014 // 01:16 PM EST

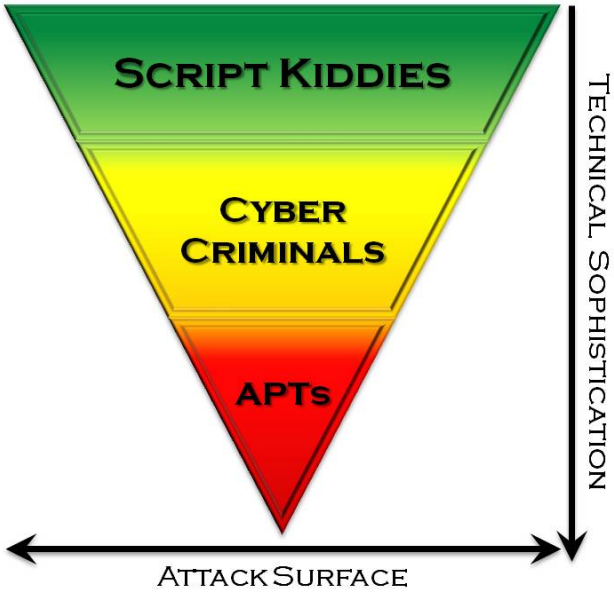
MOTHERBOARD

Written by
JOSEPH COX
CONTRIBUTOR

kpn

Determining Attack Surface

8



kpn

Determining Attack Surface

kpn

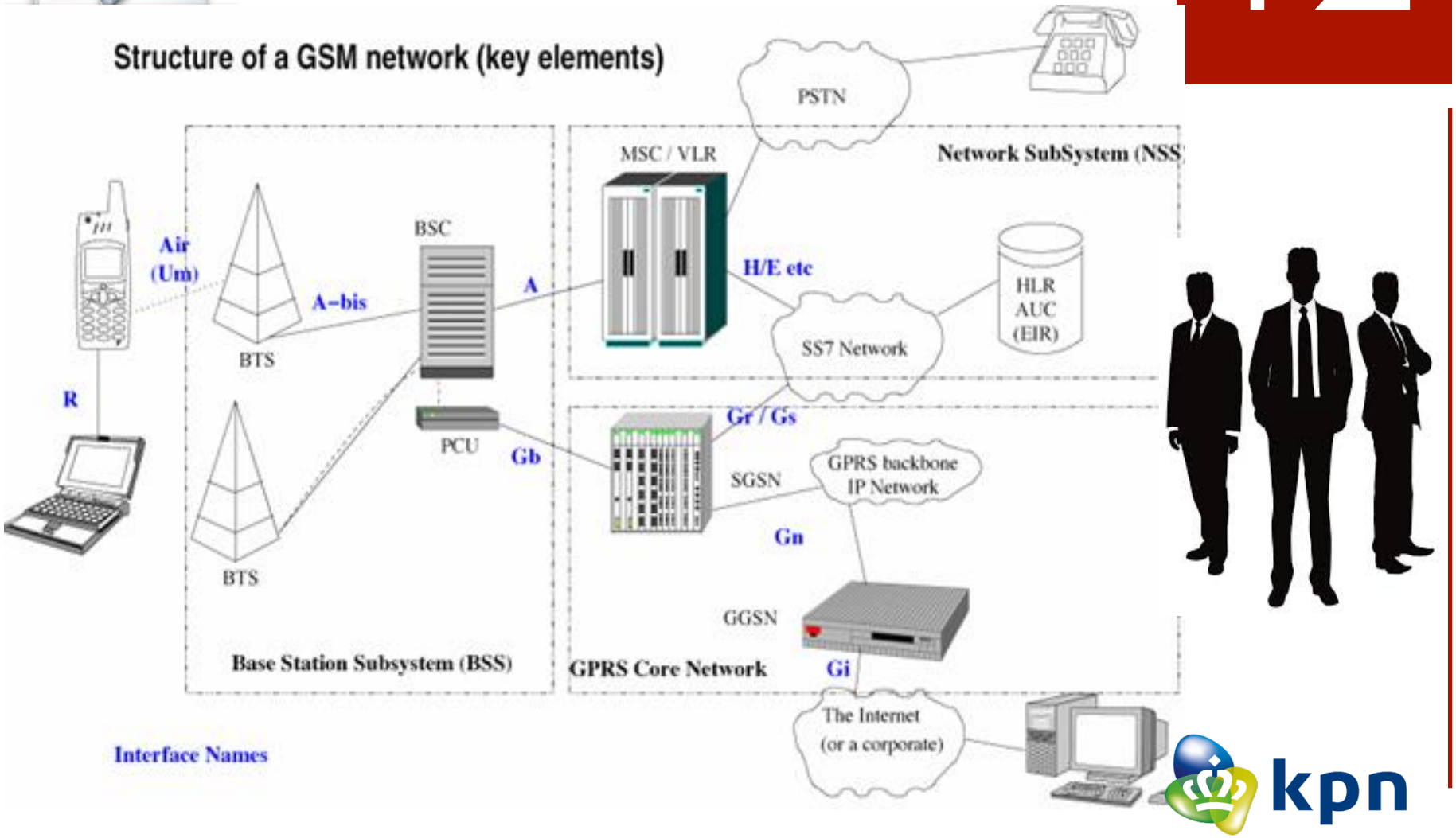
Determining Attack Surface

10

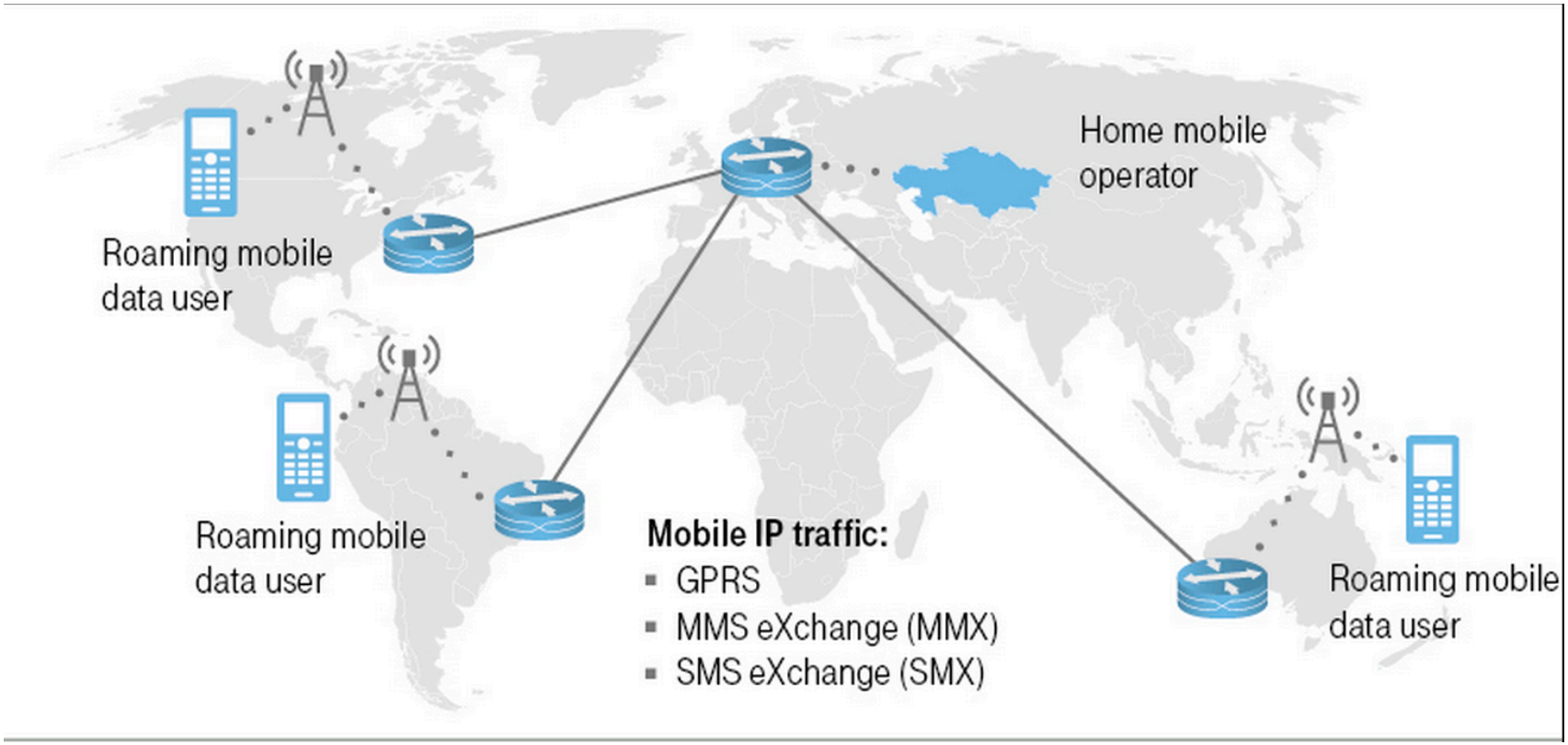
Potential Attack Surfaces

- Absence of physical intrusion detection devices
- Vulnerable services running accessible from BTS
- Absence of tamper resistance and unauthorized access protection
- Improper network segmentation; inner non-routable segments of the Telco company could accessible.
- Core GPRS Network and Network Subsystem (NSS) could be exploitable!

Potential Attack Surfaces



GRX Networks



GRX Networks

- GPRS roaming exchange, interconnecting networks.
- Your local GSM provider abroad
- Trust-based, highly interconnected network, made for internet sharing
- A failure or malicious activity would affect multiple connected machines
- Multiple attacks vectors, not limited to a particular segment where you are originating from.

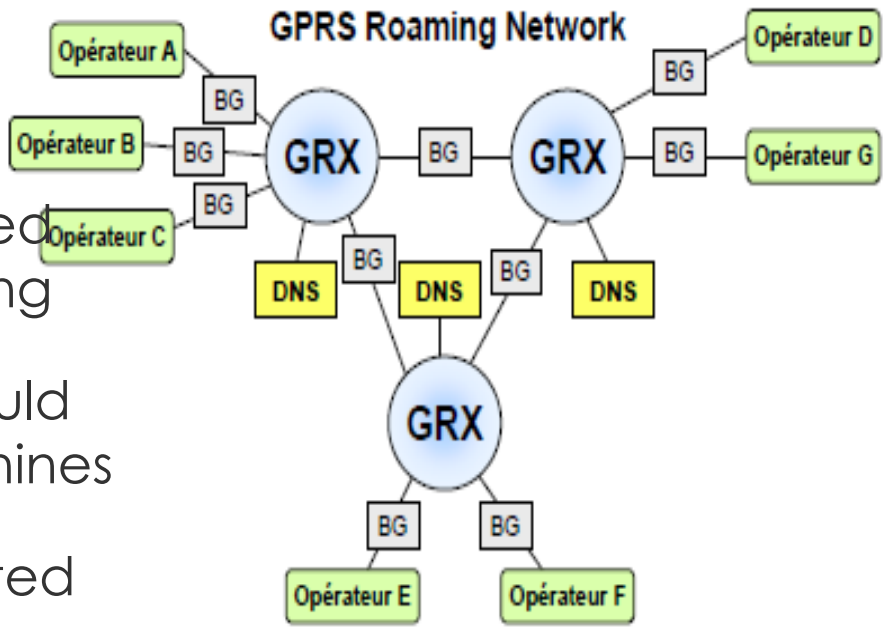
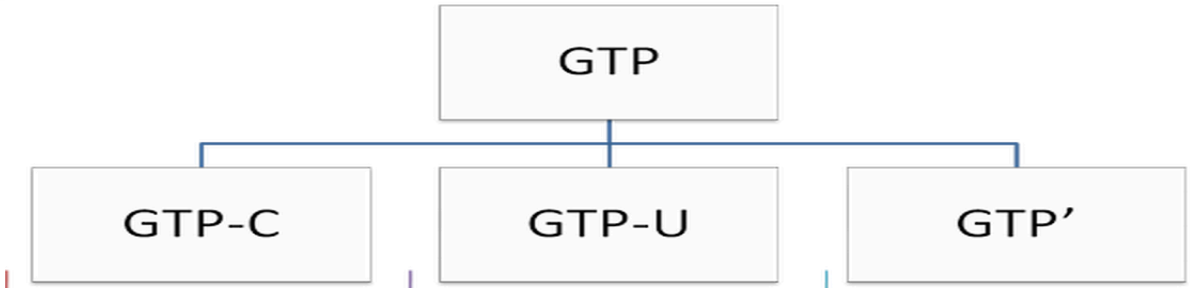
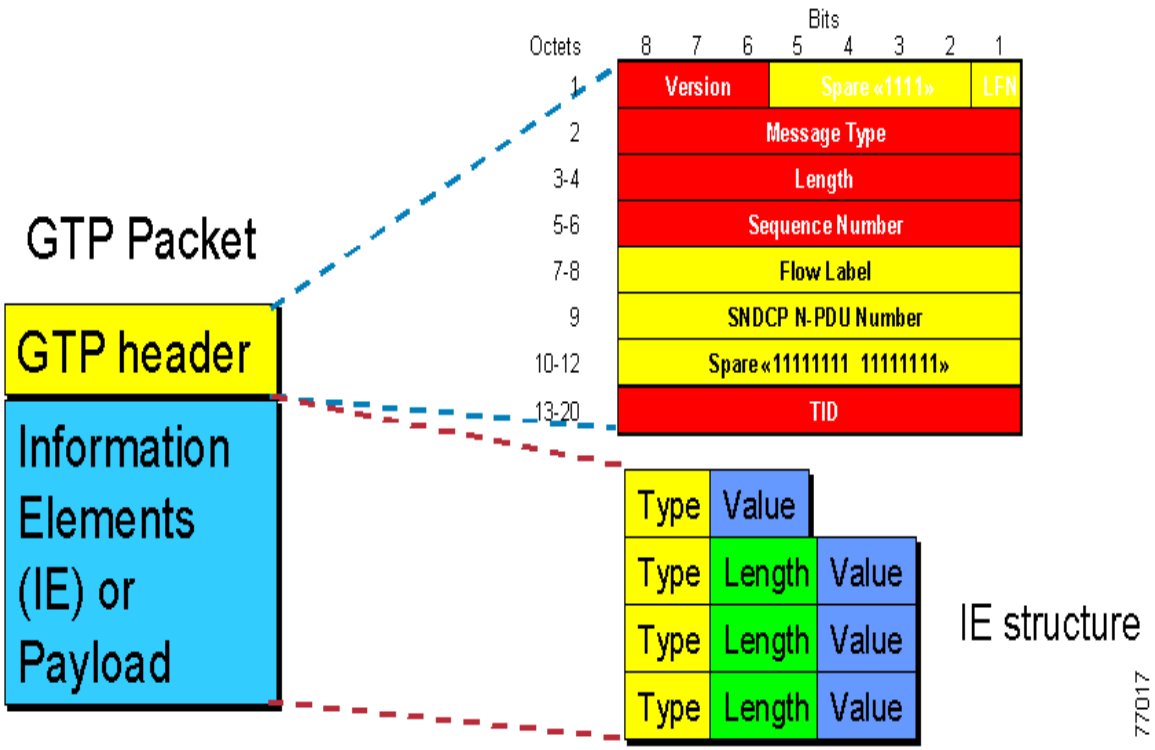


Figure 3 : Réseau GRX

GRX Networks – Attack Vectors

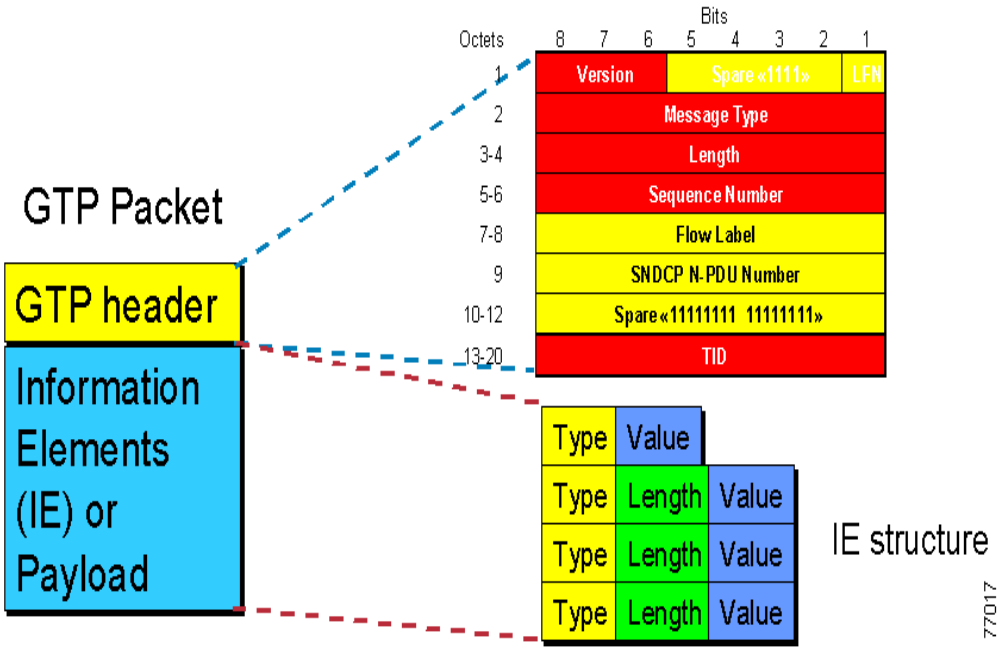




77017

GRX Networks – Attack Vectors

- GPRS roaming exchange, interconnecting networks.
- Your local GSM provider abroad
- Trust-based, highly interconnected network, made for internet sharing
- Multiple attacks vectors, not limited to a particular segment where you are originating from.



GRX Networks – Network Flow

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

```
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▼ Ethernet II, Src: Cisco_d5:cc:70 (00:0a:8b:d5:cc:70), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: Cisco_d5:cc:70 (00:0a:8b:d5:cc:70)
    Type: IP (0x0800)
▼ Internet Protocol Version 4, Src: 10.10.97.3 (10.10.97.3), Dst: 10.10.97.5 (10.10.97.5)
    Version: 4
    Header Length: 20 bytes
  ▶ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 241
    Identification: 0x1018 (4120)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
  ▶ Header checksum: 0xd4c7 [validation disabled]
    Source: 10.10.97.3 (10.10.97.3)
    Destination: 10.10.97.5 (10.10.97.5)
```

```
0010  00 f1 10 18 00 00 ff 11  d4 c7 0a 0a 61 03 0a 0a   ........ ....a...
0020  61 05 08 4b 08 4b 00 dd  6b 0b 48 20 00 d1 00 00   a..K.K.. k.H ....
0030  00 00 0b 83 f8 00 01 00  08 00 33 33 33 33 33 33   ........ ..333333
0040  33 f3 4c 00 08 00 13 21  08 00 01 10 50 f3 56 00   3.L....! ....P.V.
0050  0d 00 18 00 00 00 00 01  00 00 00 00 00 d4 d4 53   ........ .......S
0060  00 03 00 00 00 00 52 00  01 00 06 4d 00 02 00 00   ......R. ...M....
0070  00 57 00 09 00 8a 00 00  00 69 0a 0a 61 03 57 00   .W...... .i..a.W.
0080  09 01 87 00 00 00 00 0a  0a 61 06 47 00 1e 00 06   ........ .a.G....
0090  61 61 61 63 6f 6d 03 63  6f 6d 06 6d 6e 63 30 30   aaacom.c om.mnc00
00a0  30 06 6d 63 63 30 30 30  04 67 70 72 73 80 00 01   0.mcc000 .gprs...
00b0  00 00 63 00 01 00 01 4f  00 05 00 01 00 00 00 00   ..c....O ........
00c0  7f 00 01 00 00 48 00 08  00 00 00 51 ec 00 00 a3   .....H.. ...Q....
00d0  d8 5d 00 25 00 49 00 01  00 05 50 00 16 00 48 05   .].%.I.. ..P...H.
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 5f 00 02 00  01 00 03 00 01 00 98      ...._... .......
```

Text item (text), 34 bytes | Packets: 10 · Displayed: 10 (100.0%) · Load time: 0:00.000 | Profile: Default

GRX Networks – Network Flow

Filter: Expression... Clear Apply Save

```
GPRS Tunneling Protocol V2
Create Session Request
    Flags: 0x48
    Message Type: Create Session Request (32)
    Message Length: 209
    Tunnel Endpoint Identifier: 0
    Sequence Number: 754680
    Spare: 0
    International Mobile Subscriber Identity (IMSI) : 333333333333333
        IE Type: International Mobile Subscriber Identity (IMSI) (1)
        IE Length: 8
        0000 .... = CR flag: 0
        .... 0000 = Instance: 0
        IMSI(International Mobile Subscriber Identity number): 333333333333333
    MSISDN : 311280001001053
        IE Type: MSISDN (76)
        IE Length: 8
        0000 .... = CR flag: 0
        .... 0000 = Instance: 0
        Country Code: 31 Netherlands (Kingdom of the) (length 2)
        Address digits: 311280001001053
    User Location Info (ULI) : TAI ECGI
        IE Type: User Location Info (ULI) (86)
        IE Length: 13
```

```
0010  00 f1 10 18 00 00 ff 11  d4 c7 0a 0a 61 03 0a 0a   ........ ....a...
0020  61 05 08 4b 08 4b 00 dd  6b 0b 48 20 00 d1 00 00   a..K.K.. k.H ....
0030  00 00 0b 83 f8 00 01 00  08 00 33 33 33 33 33 33   ........ ..333333
0040  33 f3 4c 00 08 00 13 21  08 00 01 10 50 f3 56 00   3.L....! ....P.V.
0050  0d 00 18 00 00 00 00 01  00 00 00 00 00 d4 d4 53   ........ .......S
0060  00 03 00 00 00 00 52 00  01 00 06 4d 00 02 00 00   ......R. ...M....
0070  00 57 00 09 00 8a 00 00  00 69 0a 0a 61 03 57 00   .W...... .i..a.W.
0080  09 01 87 00 00 00 00 0a  0a 61 06 47 00 1e 00 06   ........ .a.G....
0090  61 61 61 63 6f 6d 03 63  6f 6d 06 6d 6e 63 30 30   aaacom.c om.mnc00
00a0  30 06 6d 63 63 30 30 30  04 67 70 72 73 80 00 01   0.mcc000 .gprs...
00b0  00 00 63 00 01 00 01 4f  00 05 00 01 00 00 00 00   ..c....O ........
00c0  7f 00 01 00 00 48 00 08  00 00 00 51 ec 00 00 a3   .....H.. ...Q....
00d0  d8 5d 00 25 00 49 00 01  00 05 50 00 16 00 48 05   .].%.I.. ..P...H.
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Juicy information is here.

GRX Networks – Network Flow


```
    F-TEID IPv4: 10.10.97.6 (10.10.97.6)
▼ Access Point Name (APN) : aaacom.com.mnc000.mcc000.gprs
    IE Type: Access Point Name (APN) (71)
    IE Length: 30
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    APN (Access Point Name): aaacom.com.mnc000.mcc000.gprs
▼ Selection Mode : MS or network provided APN, subscribed verified
    IE Type: Selection Mode (128)
    IE Length: 1
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    .... ..00 = Selection Mode: MS or network provided APN, subscribed verified (0)
▼ PDN Type : IPv4
    IE Type: PDN Type (99)
    IE Length: 1
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0

0030  00 00 0b 83 f8 00 01 00  08 00 33 33 33 33 33 33  ........ ..333333
0040  33 f3 4c 00 08 00 13 21  08 00 01 10 50 f3 56 00  3.L....! ....P.V.
0050  0d 00 18 00 00 00 00 01  00 00 00 00 d4 d4 53     ........ .......S
0060  00 03 00 00 00 00 52 00  01 00 06 4d 00 02 00 00  ......R. ...M....
0070  00 57 00 09 00 8a 00 00  00 69 0a 0a 61 03 57 00  .W...... .i..a.W.
0080  09 01 87 00 00 00 00 0a  0a 61 06 47 00 1e 00 06  ........ .a.G....
0090  61 61 61 63 6f 6d 03 63  6f 6d 06 6d 6e 63 30 30  aaacom.c om.mnc00
00a0  30 06 6d 63 63 30 30 30  04 67 70 72 73 80 00 01  0.mcc000 .gprs...
00b0  00 00 63 00 01 00 01 4f  00 05 00 01 00 00 00 00  ..c....O ........
00c0  7f 00 01 00 00 48 00 08  00 00 00 51 ec 00 00 a3  .....H.. ...Q....
00d0  d8 5d 00 25 00 49 00 01  00 05 50 00 16 00 48 05  .].%.I.. ..P...H.
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00f0  00 00 00 00 5f 00 02 00  01 00 03 00 01 00 98     ...._... .......
```

And more juicy information is here.

GRX Networks – Attacks & Flaws

Are you telling me all your communication intercepted and logged including your physical location?.

NSA: We'll move your metadata into /dev/null

stop suing us

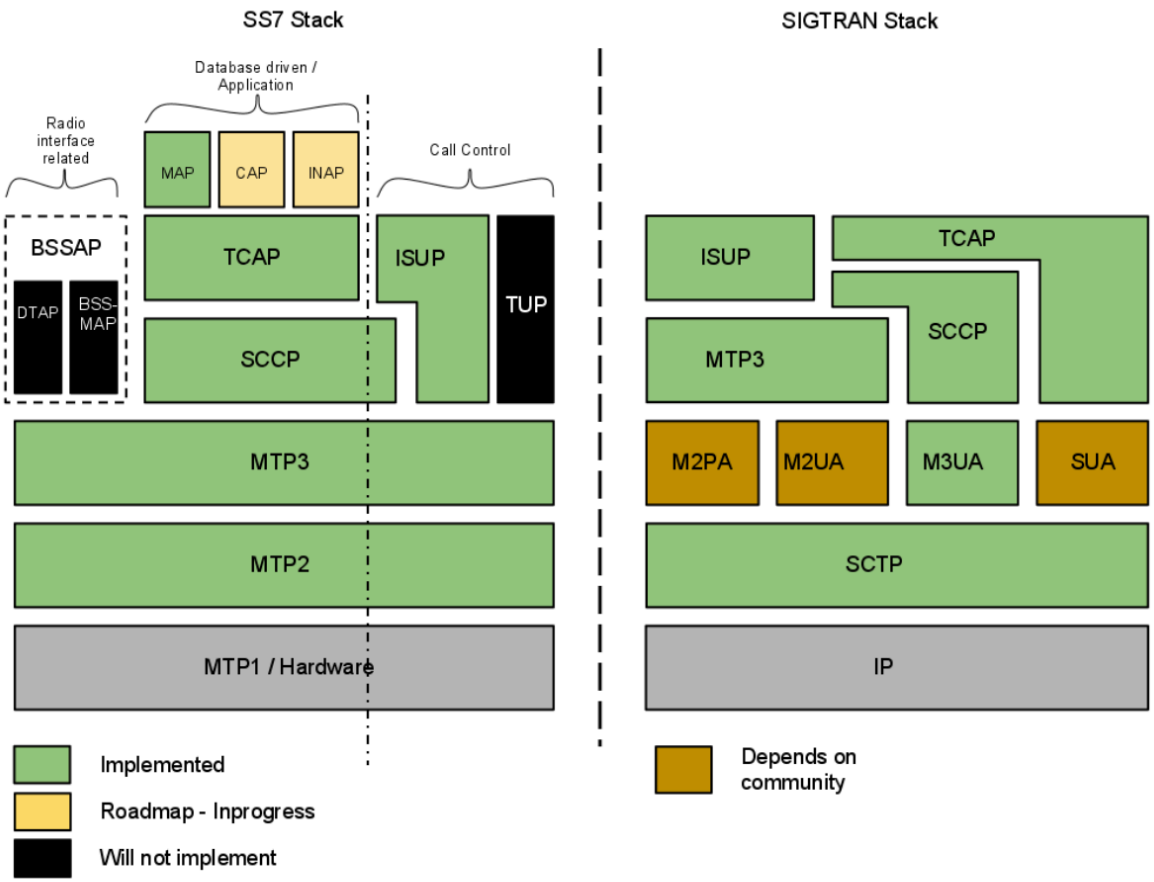
collection

The NSA promises to delete its phone metadata early next year

Digital Trends - 2 days ago

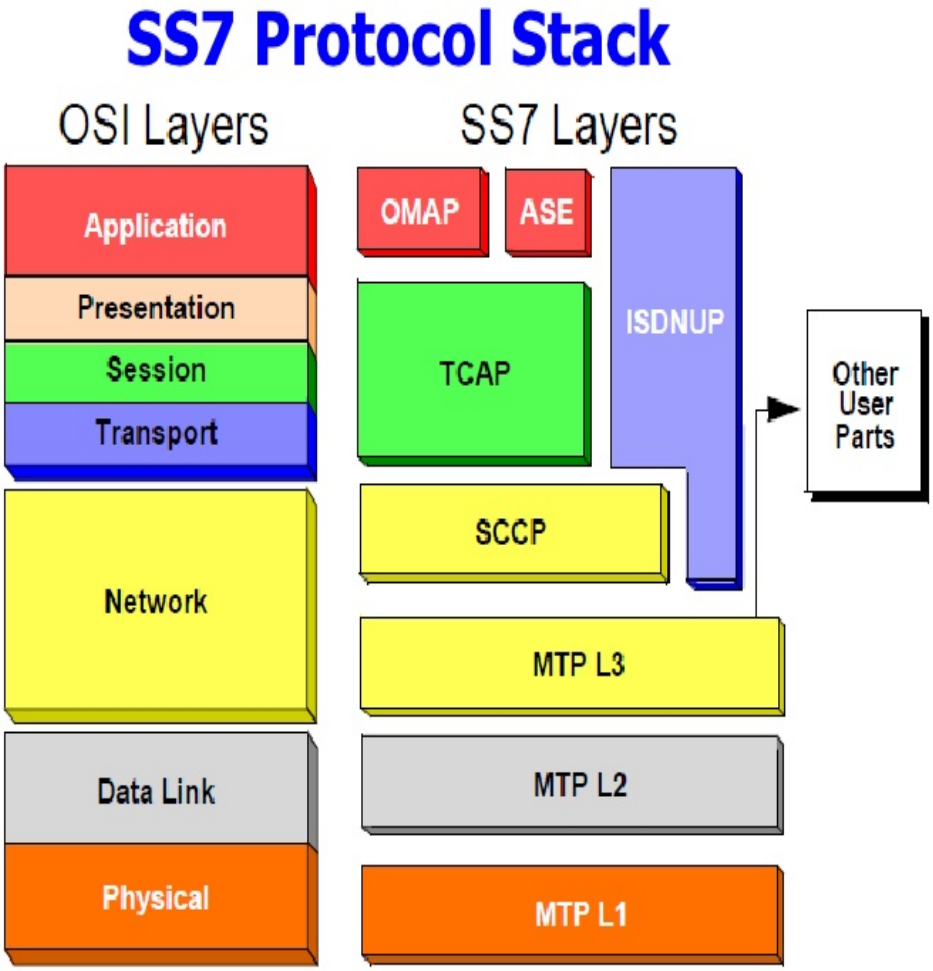
The **National Security Agency will** lose the power to keep and

SS7 & SIGTRAN



http://www.telestax.com/

SS7 & SIGTRAN



SS7 Introduces procedures for

- User identification.

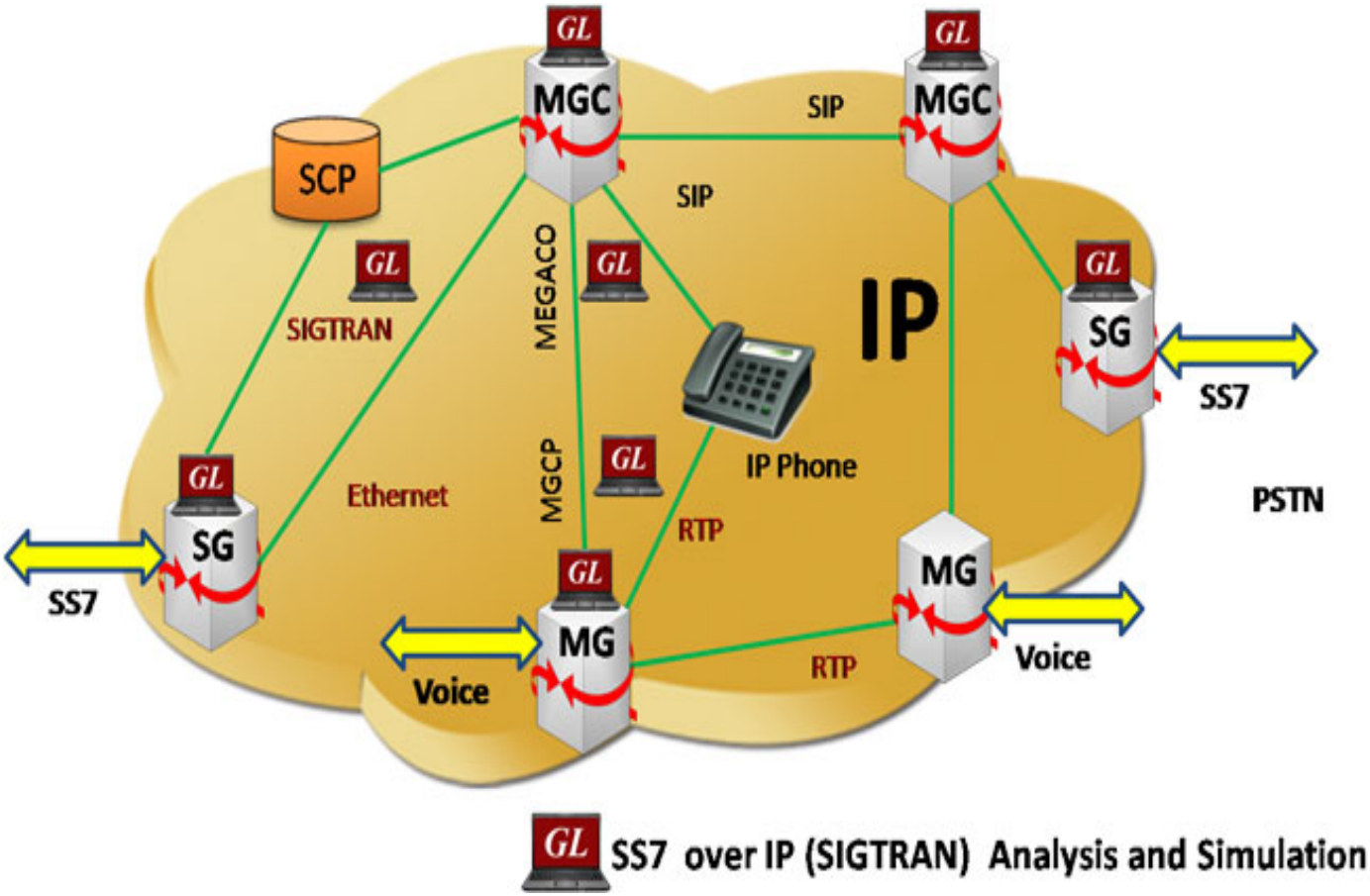
Routing

- Billing
- Call management

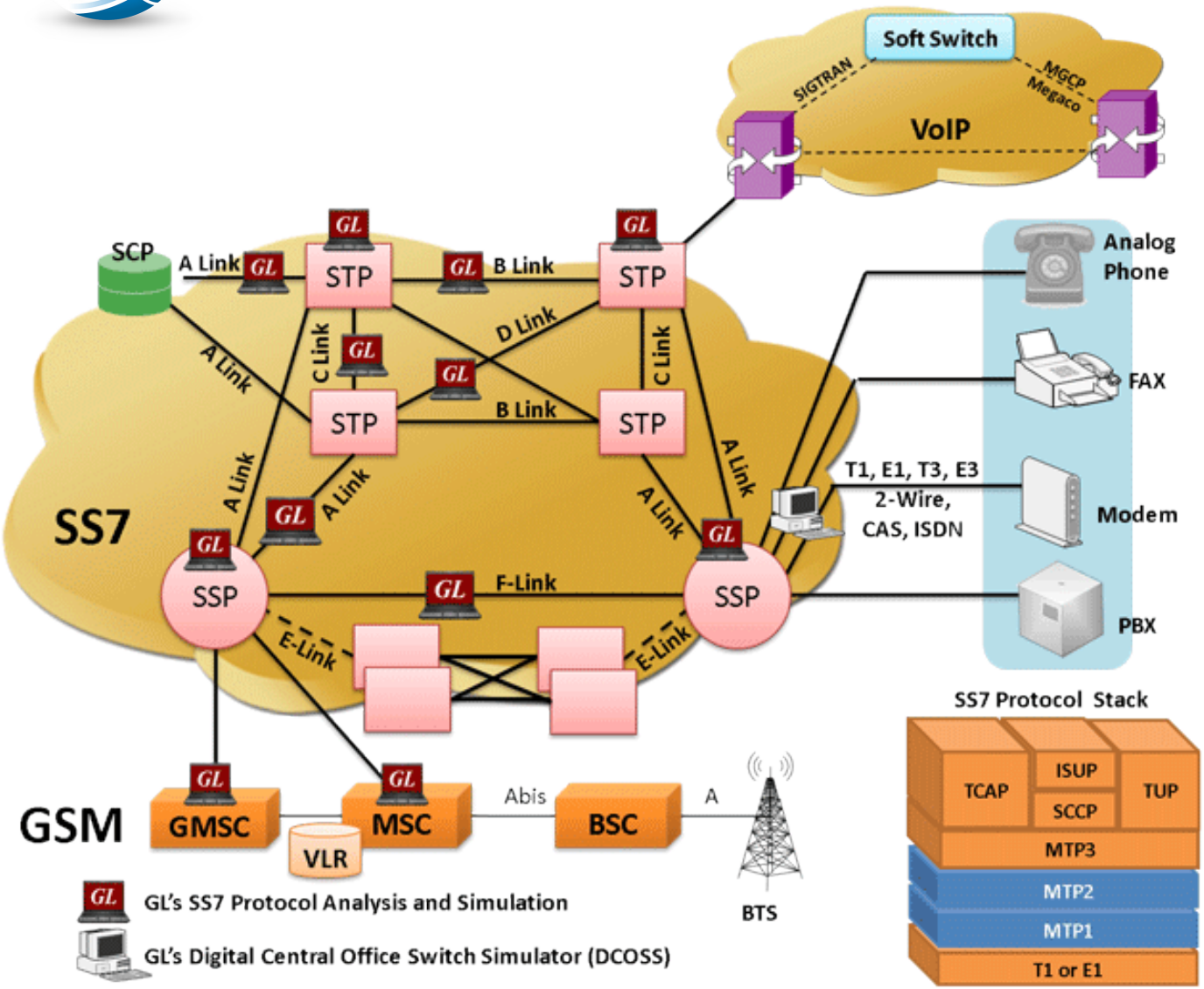
SS7 & SIGTRAN

- SS7 Features:
  - Flow control of transmitted information
  - Traffic congestion controls
  - Peer entity status detection (GT + PC or SPC)
  - Traffic Monitoring and monitoring measuremen

SS7 & SIGTRAN


GL
MGC
SIP
MGC
SCP
SIP
GL
GL
GL
SIGTRAN
MEGACO
IP
SG
SS7
IP Phone
GL
GL
Ethernet
MGCP
PSTN
SG
RTP
MG
SS7
GL
MG
Voice
RTP
Voice
GL SS7 over IP (SIGTRAN) Analysis and Simulation

SS7 & SIGTRAN


Soft Switch
SIGTRAN
MGCP
Megaco
VoIP
SCP
A Link
STP
B Link
D Link
C Link
SS7
SSP
F-Link
E-Link
Analog Phone
FAX
T1, E1, T3, E3
2-Wire,
CAS, ISDN
Modem
PBX
GSM
GMSC
VLR
MSC
Abis
BSC
A
BTS
GL's SS7 Protocol Analysis and Simulation
GL's Digital Central Office Switch Simulator (DCOSS)
SS7 Protocol Stack
TCAP
ISUP
SCCP
TUP
MTP3
MTP2
MTP1
T1 or E1

SS7 Protocol Analysis

SS7 Protocol Analysis SS7 ITU

File View Capture Statistics Database Call Detail Records Configure Help

0 GoTo

Dev	TS...	Su...	Frame#	TIME (Relative)	Len	BSN	BIB	FSN	FIB	Sta...	SLC	DPC
1	20		0	00:00:00.000000	21	34	1	68	1		0	2.2.2
1	20		1	00:00:00.120500	21	34	1	69	1		0	2.2.2
1	20		2	00:00:00.193750	21	34	1	70	1		0	2.2.2
1	20		3	00:00:00.216000	21	34	1	71	1		0	2.2.2
1	20		4	00:00:00.281500	21	34	1	72	1		0	2.2.2
1	20		5	00:00:00.361500	21	34	1	73	1		0	2.2.2

```
Card1 TimeSlot=20 Frame=0 at 00:00:00.000000 OK Len=21
HDLC Frame Data + FCS
 ============ MTP2 Layer ============          =
  BSN                                          = .0100010 (34)
  BIB                                          = 1....... (1)
  FSN                                          = .1000100 (68)
  FIB                                          = 1....... (1)
  LI                                           = ..010011 MSU Format
 ============ MTP3 Layer ============          =
  Service Indicator                            = ....0101 ISDN User Part
  Priority Code                                = ..00.... Priority Code 0
  Sub-service field                            = 00...... International network
  DPC                                          = 2.2.2(00010010 ..010000)
  OPC                                          = 1.1.1(01...... 00000010 ....0010)
  Signalling Link Code                         = 0000.... (0)
 ============ ISUP Layer ============          =
  Circuit Identification Code                  = 00000001 ....0000 (1)
```

```
Hex Dump of the Frame Data
+-----------+-----------+-----------+----------     +---+---+---+--
A2 C4 13 05 12 50 02 02 01 00 0C 02 00 05 C2 10     ¢Ä   P        Å
00 00 0B C7 F8                                         Çø
```

Off-line Viewing | D:\Program Files\GL Communicatio | 2349 Frames

kpn

SS7 Protocol Analysis

SS7 Protocol Analysis SS7 ITU

File View Capture Statistics Database Call Detail Records Configure Help

Dev	TSlot	SubCh	Frame#	TIME (Relative)	Len	Error	BSN	BIB	FSN	FIB	St...	SLC	DPC	OPC	SCCP
1	23		0	00:00:00.000000	13		1	1	2	1		1	5.5.5	3.4.6	
2	23		1	00:00:00.728875	14		2	1	2	1		1	3.4.6	5.5.5	
1	23		2	00:00:06.101875	13		2	1	3	1		1	5.5.5	3.4.6	
2	23		3	00:00:06.845500	13		3	1	3	1		1	3.4.6	5.5.5	
1	23		4	00:00:17.390000	13		3	1	4	1		1	5.5.5	3.4.6	
2	23		5	00:00:18.115750	13		4	1	4	1		1	3.4.6	5.5.5	

Device #	Message Ty...	Frame Count(Message Ty...
1	Initial address (1)	2
1	Address complete ...	1
1	Answer (9)	1
1	Release (12)	2
1	Release Complete ...	1
1	Reset Circuit (18)	1
1	Blocking (19)	1
1	Unblocking (20)	1

Call ID	Call Status	Disp	Calling Num	Called Num	Call Start Date & Time	Call Duration	Release Complete Cause
0	C IaArR	1	9987095800	8978675400	2013-03-15 18:32:21.805000	00:00:06.843000	Normal call clearing
1	C IaA!!	3	9987095821	8978675421	2013-03-15 18:36:23.475375	00:00:24.091750	x00
2	C IrR	4	9987095804	8978675404	2013-03-15 18:37:11.966750	00:00:20.716625	Recovery on timer expiry

Off-line Viewing C:\Program Files (x86)\GL Communications Inc\tl 19 Frames

All the juicy info here :

- ✓ **Calling no.**
- ✓ **Called no**
- ✓ **Call duration**
- ✓ **Call duration**
- ✓ **Call status**

SS7 Protocol Attacks & Flows

Feel confident that NSA not interested in 'Good' people?.

NSA: We'll move your metadata into /dev/null when you stop suing us

November 29 set as cutoff date for further collection

NSA Not Interested in "Bad People"; It Listens to "Interesting ...

www.youtube.com/watch?v=BhrPVse9TnE

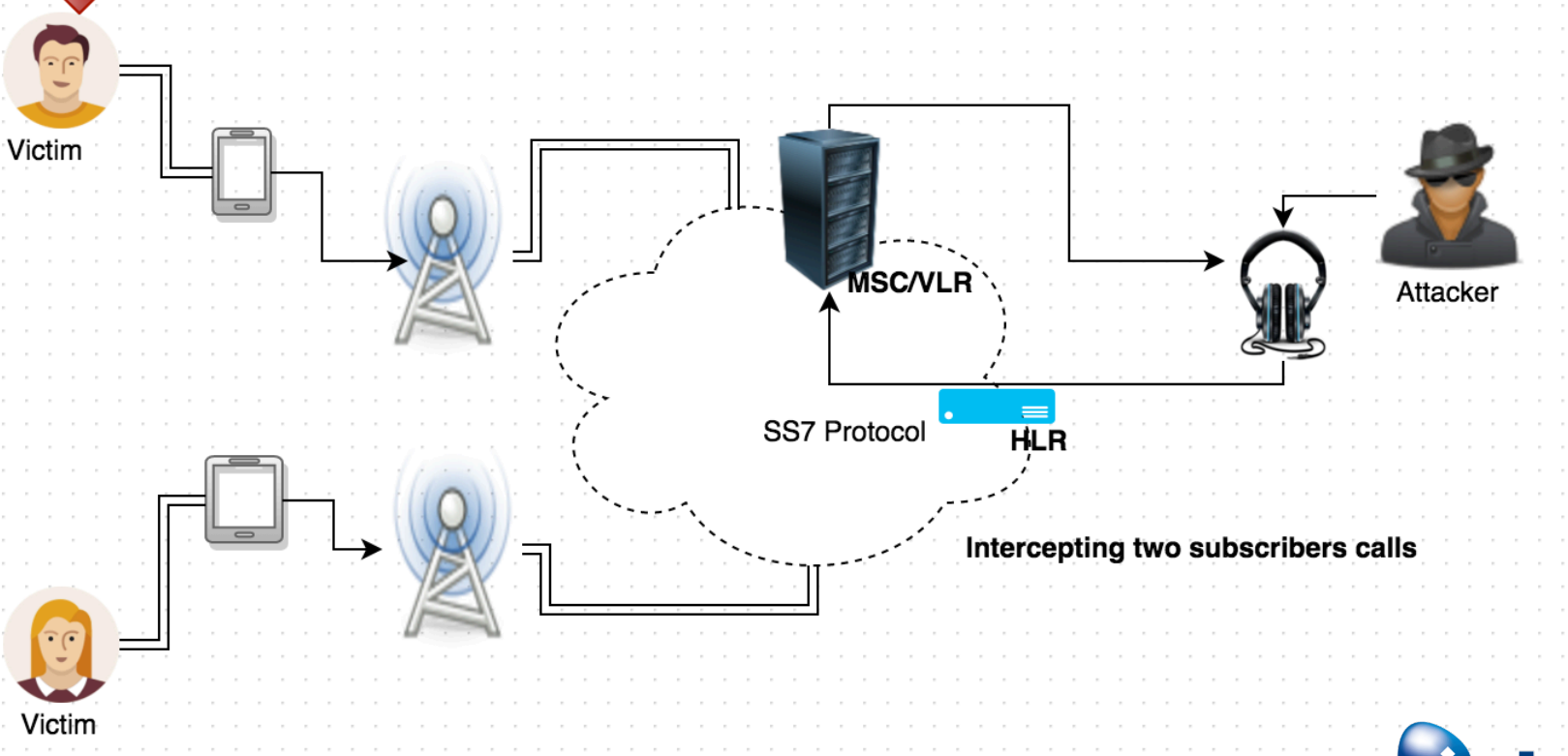
Feb 4, 2015 - Uploaded by Ken Campbell

Michael Hayden, former **NSA** Director, former Director of National Director of CIA has ...

SS7 Practical Attack Scenarios

1

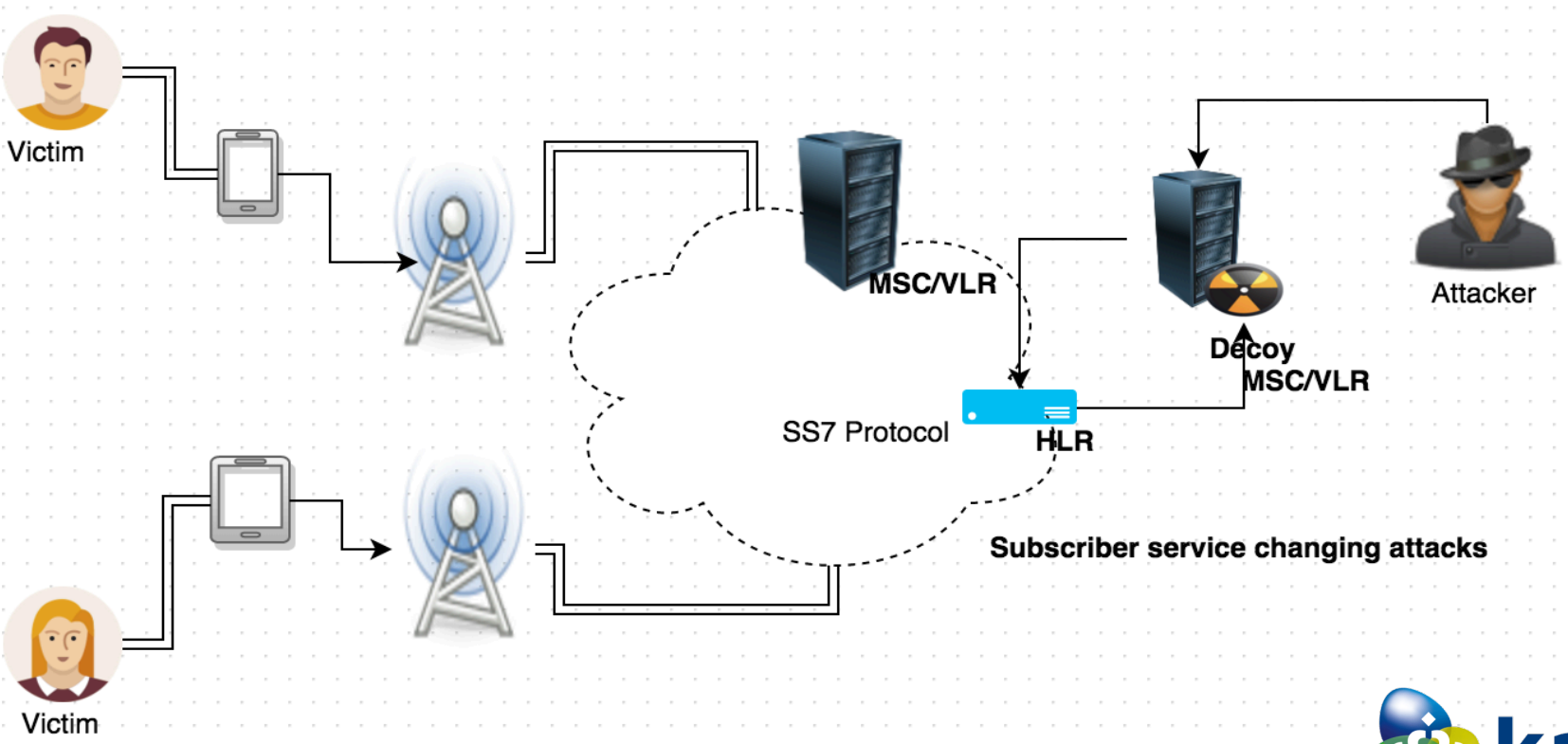
- Intercepting subscribers calls



SS7 Practical Attack Scenarios

2

- Subscriber service change attacks



SS7 Practical Attack Scenarios

3. Interception of SMS messages
4. Interception of outgoing calls
5. Redirection of incoming or outgoing calls
6. Making changes in user bills or balance

SS7 Practical Attack Scenarios

7

- Unblocking stolen mobile devices

Unblocking stolen mobile devices using SS7-MAP vulnerabilities

Exploiting the relationship between IMEI and IMSI for EIR access

Siddharth Prakash Rao[1, 2], Silke Holtmanns[1], Ian Oliver[1], Tuomas Aura[2]
[1]Nokia Networks
Espoo, Finland
{sid.rao, silke.holtmanns, ian.oliver}@nokia.com
[2]Department of Computer Science and Engineering
Aalto University, School of Science
Espoo, Finland
{siddharth.rao, tuomas.aura}@aalto.fi

IEEE August 2015, Nokia Researchers Espoo, Finland.

***Abstract*— The increase in usage of mobile phones and the relative increase in the number of mobile phone thefts have imposed an overhead on securely retrieving the stolen or missing devices. While the mobile security researchers try to figure out various mechanisms to track such devices, attackers on the other hand are trying to exploit weaknesses in the mobile network system to dissipate into the dark side with stolen devices. In this paper we present how the SS7- MAP protocol can be misused to help an attacker to unblock the device from the stolen list and use it normally.**

Keywords*— *SS7, MAP, EIR, Stolen Mobiles, IMEI

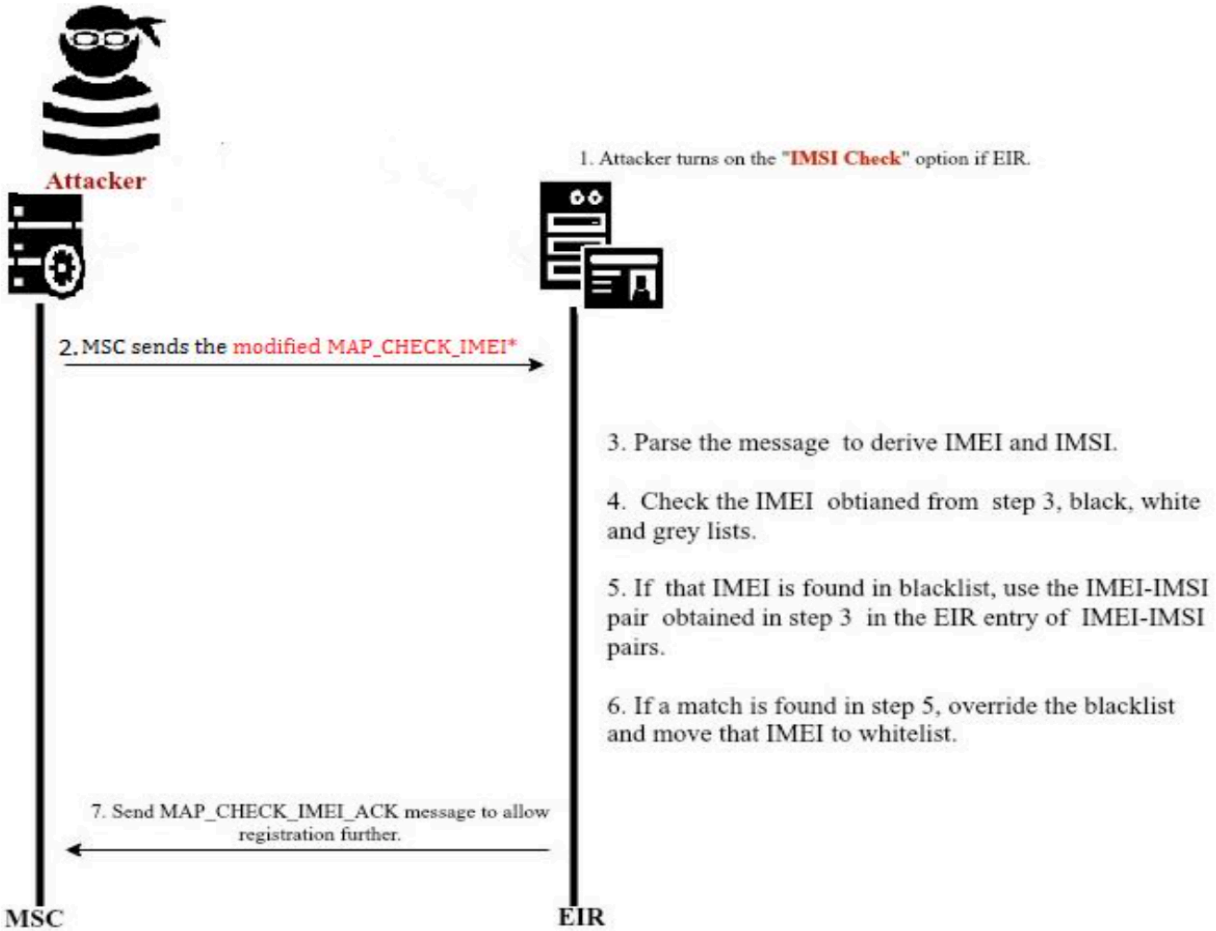
over stolen/missing devices and the private information on them. There exists a growing black market [3] where such devices are sold with least possibility of tracing them.

Signaling System No.7 (SS7) is a mobile backend protocol used for interconnectivity between mobile operator networks which enables roaming and cellular services across operator domains. This protocol is mainly used for communication between the network elements and between networks. Recent successful attacks on SS7 as per [4][5][6][7] and [8] haven proven that an attacker with privilege over the core mobile network can take control over users personal information such as billing data and Short Message Service (SMS) messages

SS7 Practical Attack Scenarios

7

- Unblocking stolen mobile devices



IEEE August 2015, Nokia Researchers Espoo, Finland.

Hacking Team after SS7 Hacks

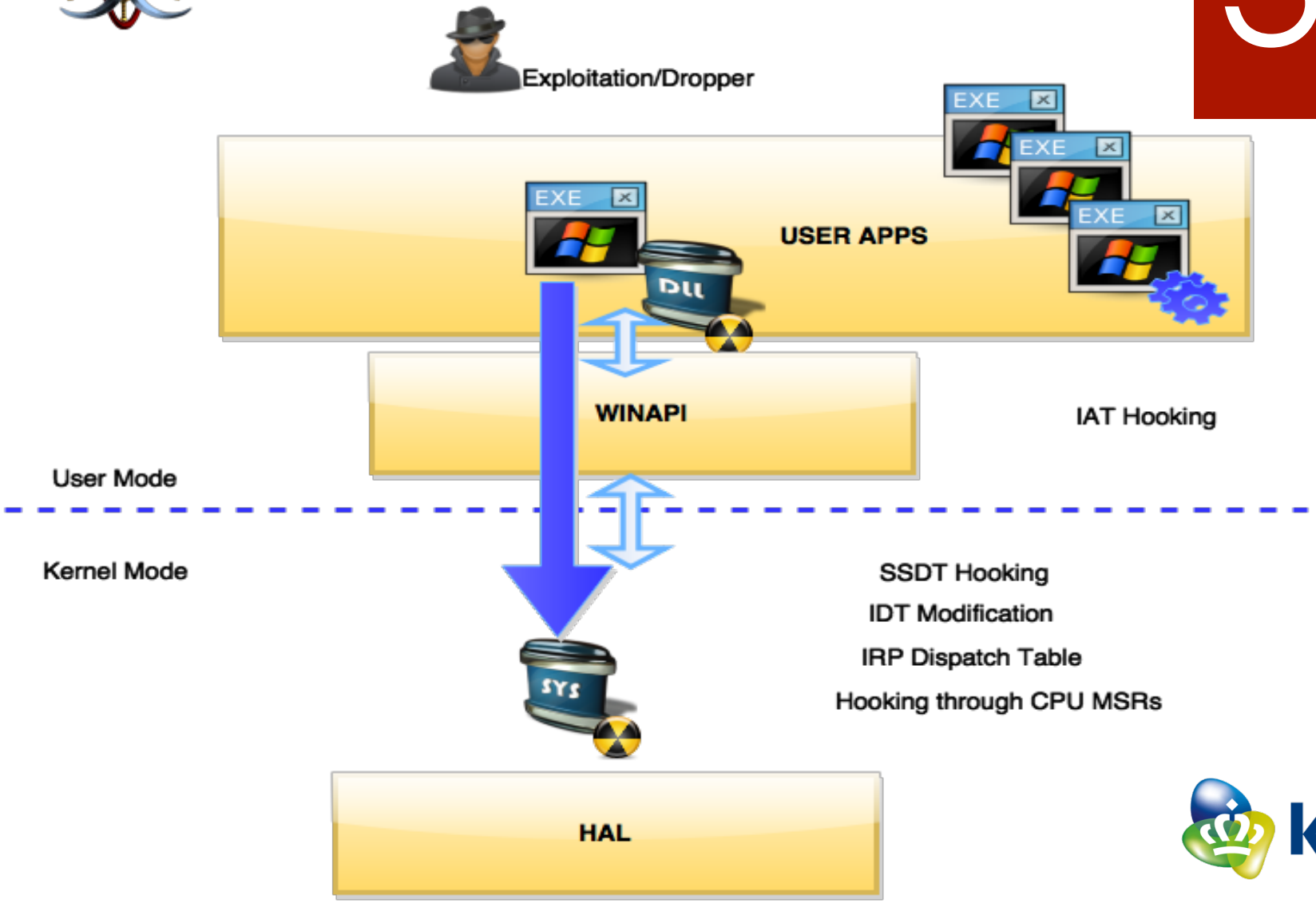
On 5 Sep, 2013, at 3:10 PM, Alberto Ornaghi <a.ornaghi@hackingteam.com> wrote:

I think that any telco in the world could access SS7 signals to know where a phone number is located. If the have to call that number from a country, let's say UK, the UK's provider must know where the phone is attached to the global network since if the called one is in UK the call is not routed abroad and routed directly internally.
sounds plausible?
On Sep 5, 2013, at 09:03 , serge <s.woon@hackingteam.com> wrote:

To narrow down the possible whistleblower, I think the person has to be working in the telecom provider we subscribed to ... TIM?Location query from SS7 signalling can only indicate the location of the mobile phone at the time of query (we can verify this with NICE :-)). The records are clearly a database query as it is very systematic; twice per day at 1100h and 2300h. As the records started from one or two years back, either Mus and Marco.B have a common secret admirer (which I do not think so) or the person just query the records from the telco existing database knowing that their names are mentioned in controversial articles. We can compliant to TIM (I am not sure whether they will do anything about it) or just switch to another telco and monitor the situation.

Source: https://wikileaks.org/hackingteam/emails/emailid/343623

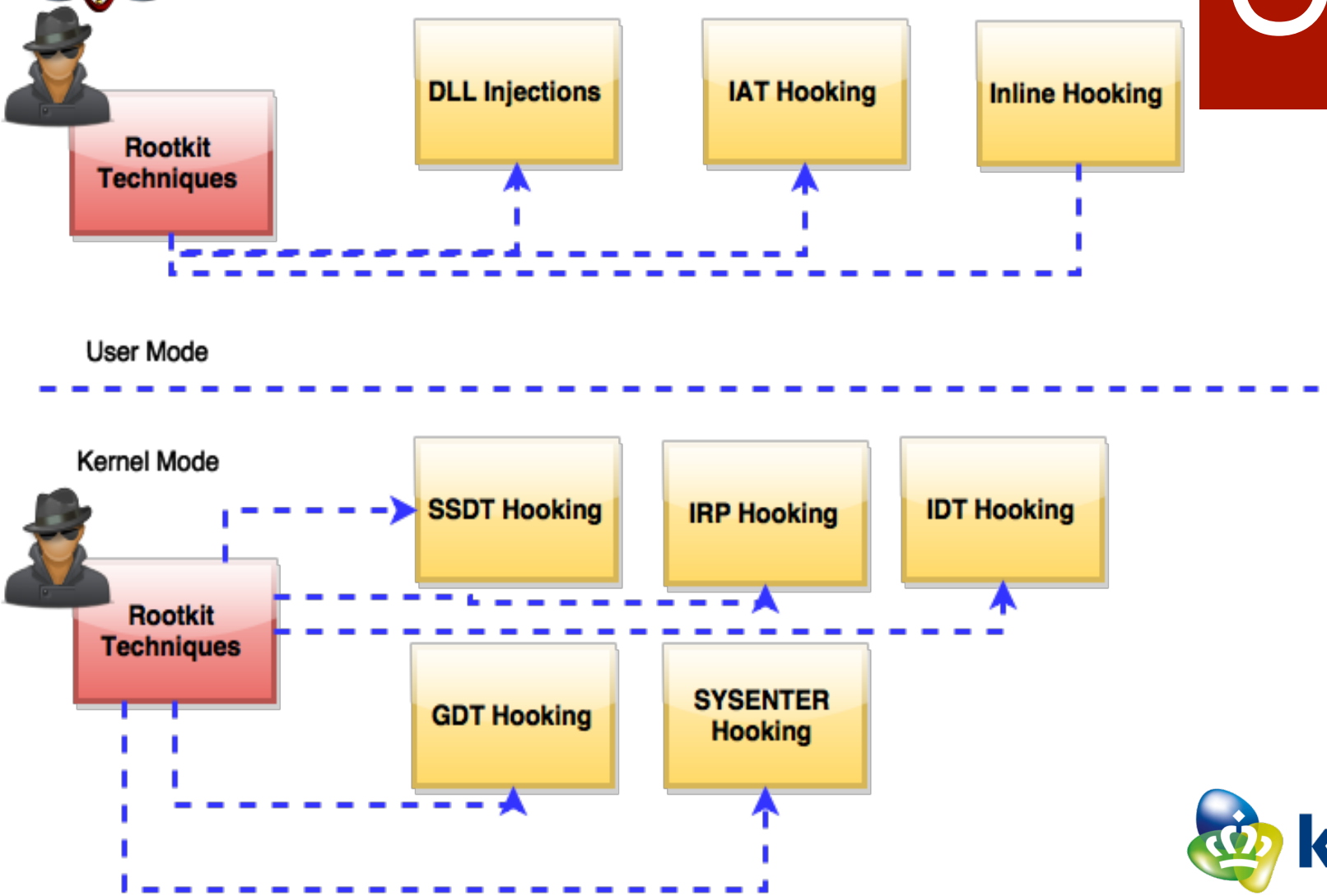
Rootkit Techniques



Hardware/Software Interception: Captain Hook Style Hacking

Captain Hook Style Hacking: *Intercepts every function, keeps a copy of the content for herself, and then let the function continue as it was supposed to …*

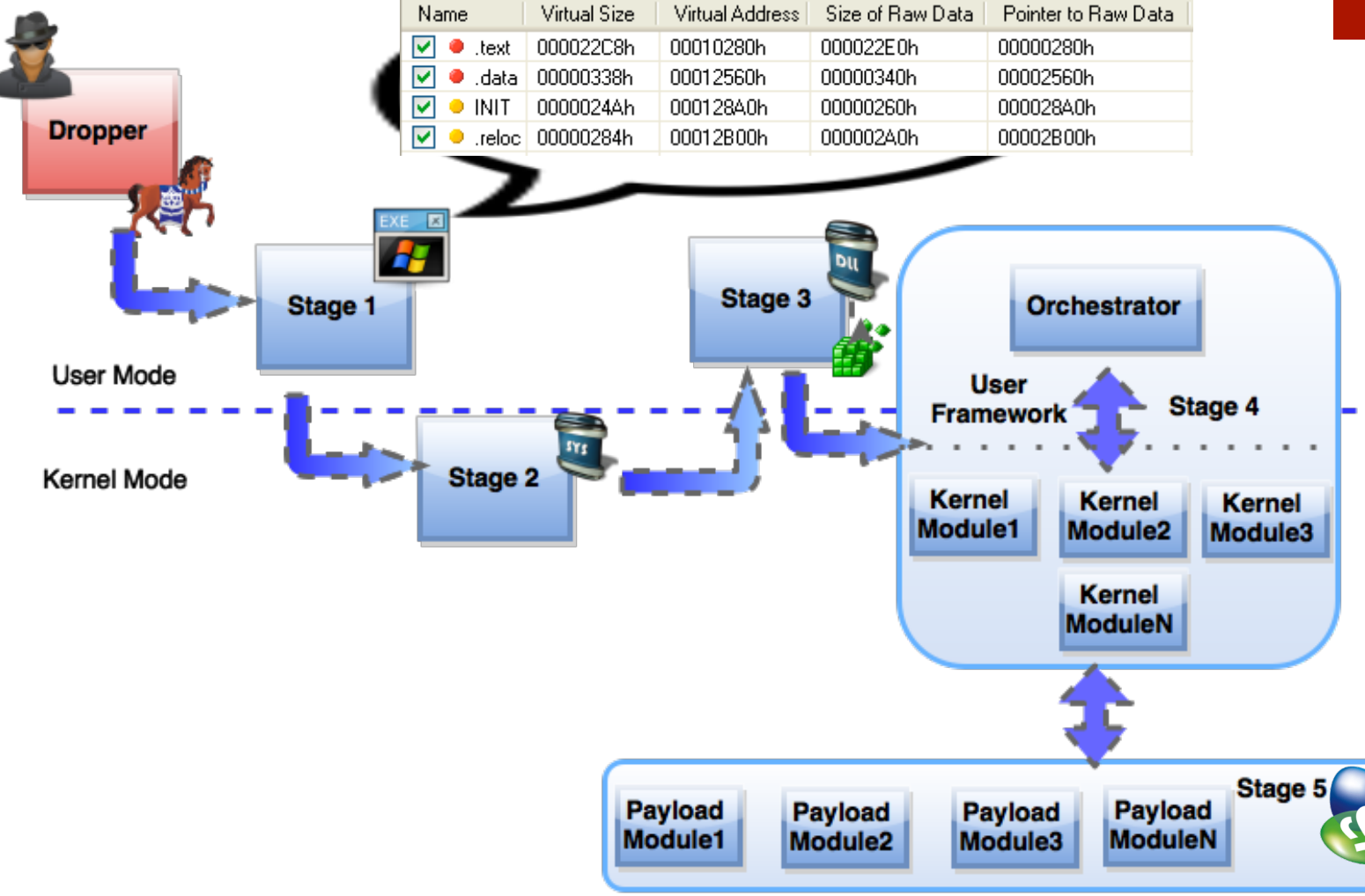
Rootkit Techniques



Regin Platform Structure

REGIN FRAMEWORK

Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data
.text	000022C8h	00010280h	000022E0h	00000280h
.data	00000338h	00012560h	00000340h	00002560h
INIT	0000024Ah	000128A0h	00000260h	000028A0h
.reloc	00000284h	00012B00h	000002A0h	00002B00h



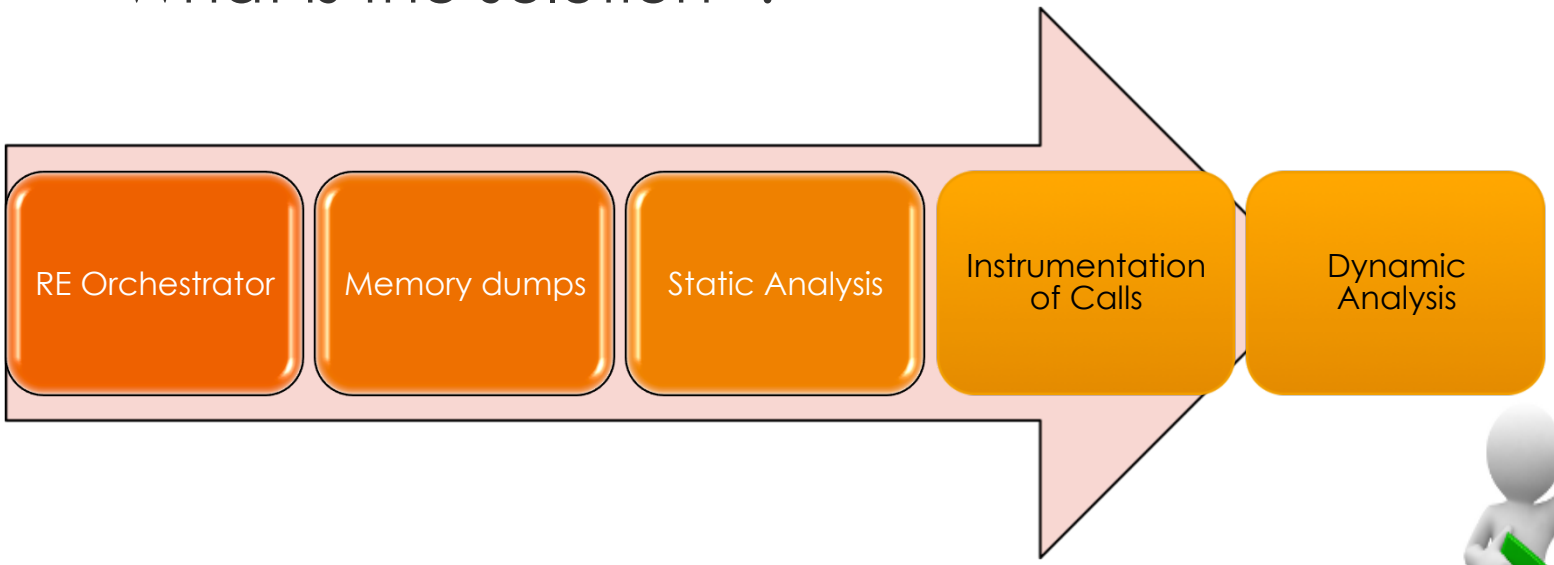
Regin Platform Analysis

- Challenges, Hurdles & Difficulties:

- No one had the dropper when started analysis
- Multi stage and encrypted framework structure
- Modules are invoked via SOA structure by the framework
- Malware data are stored inside the VFS
- Researched GSM Networks had no indication of compromise ☺

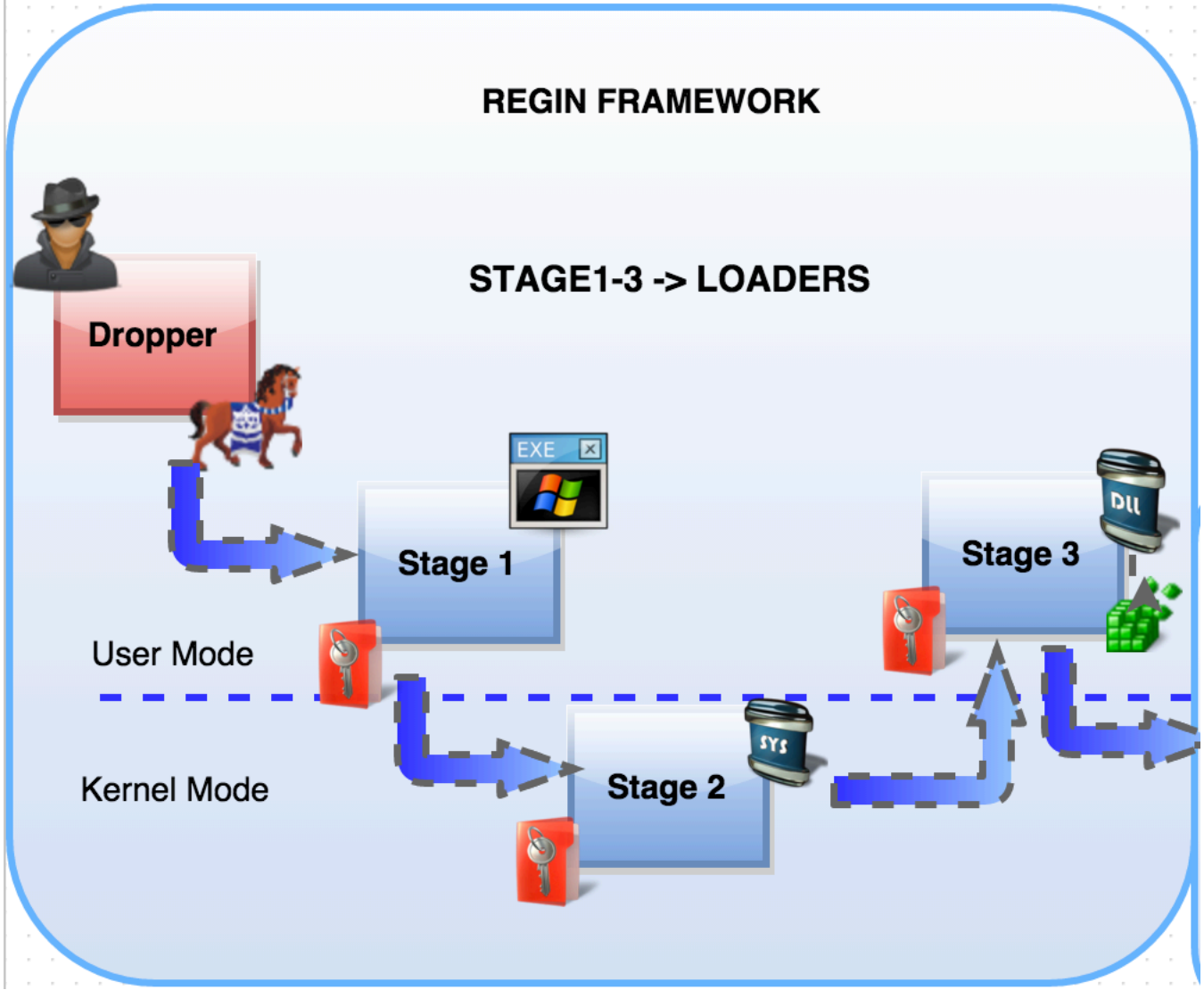
Regin Platform Analysis

- What is the solution ?

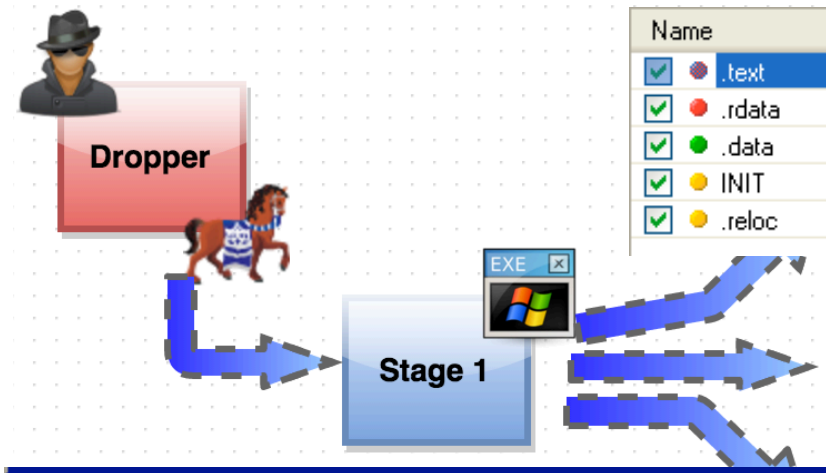


Check similar work & the write up:
http://artemonsecurity.com/regin_analysis.pdf

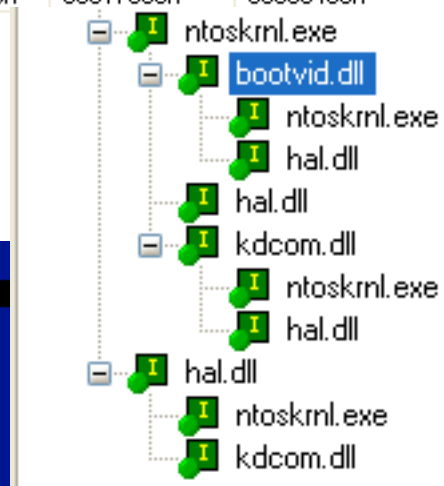
Regin Platform Stages



Regin Platform – Stage 1



Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data
.text	00002578h	00011000h	00002600h	00000400h
.rdata	00000104h	00014000h	00000200h	00002A00h
.data	0000033Ch	00015000h	00000400h	00002C00h
INIT	000002E0h	00016000h	00000400h	00003000h
.reloc	00000396h	00017000h	00000400h	00003400h



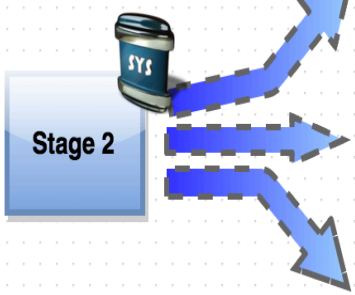

```
extrn memcpy
extrn RtlTimeToTimeFields
extrn ExSystemTimeToLocalTime
extrn KeQuerySystemTime
extrn ExFreePool
extrn NtBuildNumber
extrn ZwQuerySystemInformation
extrn ZwCreateFile
extrn memset
extrn ZwQueryInformationFile
extrn ExAllocatePoolWithTag
```

Unprocessed data | Strings | View 1 | View 2 | View 3 | View 4

```
00011088                    jmp_ntoskrnl.exe!_except_handler3:
00011088  FF2578400100                jmp     [ntoskrnl.exe!_except_handler3]
0001108E                    SUB_L0001108E:
0001108E  8BFF                        mov     edi,edi
00011090  55                          push    ebp
00011091  8BEC                        mov     ebp,esp
00011093  83EC20                      sub     esp,00000020h
00011096  8B450C                      mov     eax,[ebp+0Ch]
00011099  C645FF00                    mov     byte ptr [ebp-01h],00h
```

kpn

Regin Platform – Stage 2




```
ObjectAttributes= OBJECT_ATTRIBUTES ptr -34h
DestinationString= UNICODE_STRING ptr -1Ch
ValueName= UNICODE_STRING ptr -14h
Length= dword ptr -0Ch
KeyHandle= dword ptr -8
ResultLength= dword ptr -4

mov     edi, edi
push    ebp
mov     ebp, esp
sub     esp, 34h
push    esi
mov     esi, ds:RtlInitUnicodeString
push    edi
push    offset SourceString ; "\\REGISTRY\\Machine\\System\\CurrentCon"
lea     eax, [ebp+DestinationString]
xor     edi, edi
push    eax             ; DestinationString
mov     [ebp+ResultLength], edi
call    esi ; RtlInitUnicodeString
push    offset word_163E6 ; SourceString
lea     eax, [ebp+ValueName]
push    eax             ; DestinationString
call    esi ; RtlInitUnicodeString
lea     eax, [ebp+DestinationString]
mov     [ebp+ObjectAttributes.ObjectName], eax
lea     eax, [ebp+ObjectAttributes]
push    eax             ; ObjectAttributes
push    0F003Fh         ; DesiredAccess
```

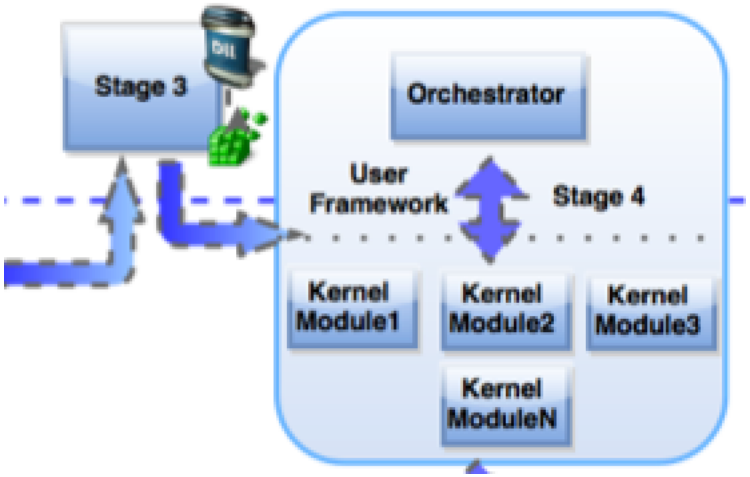
```
120         RegistryPatha = RtlWriteRegistryValue(
121                           1u,
122                           SourceString.Buffer,
123                           Destination.Buffer,
124                           1u,
125                           ValueData,
126                           (unsigned __int16)v18 + 2);
127         if ( RegistryPatha < 0 )
128           break;
129       }
130       Destination.Length -= DestinationString.Length;
131       ObjectName.Length -= DestinationString.Length;
```

Regin Platform – Stage 2


```
12  ResultLength = 0;
13  RtlInitUnicodeString(
14    &DestinationString,
15    L"\\REGISTRY\\Machine\\System\\CurrentControlSet\\Control\\Session Manager\\Memory Management");
16  RtlInitUnicodeString(&ValueName, &word_163E6);
17  ObjectAttributes.ObjectName = &DestinationString;
18  ObjectAttributes.Length = 24;
19  ObjectAttributes.RootDirectory = 0;
20  ObjectAttributes.Attributes = 64;
21  ObjectAttributes.SecurityDescriptor = 0;
22  ObjectAttributes.SecurityQualityOfService = 0;
23  result = ZwOpenKey(&KeyHandle, 0xF003Fu, &ObjectAttributes);
24  if ( !result )
25  {
26    if ( ZwQueryValueKey(KeyHandle, &ValueName, KeyValueFullInformation, 0, 0, &ResultLength) == -1073741789 )
27    {
28      Length = ResultLength;
29      v1 = sub_12892(ResultLength, PagedPool);
30      if ( v1 )
31      {
32        if ( !ZwQueryValueKey(KeyHandle, &ValueName, KeyValueFullInformation, (PVOID)v1, Length, &ResultLength)
33          && *(_DWORD *)(v1 + *(_DWORD *)(v1 + 8)) == 1 )
34        byte_19B79 = 1;
35      sub_12952((PVOID)v1, Length);
```

```
85  memset(v5, 0, ObjectName.MaximumLength);
86  RtlAppendUnicodeToString(&ObjectName, L"\\Device\\");
87  RtlAppendUnicodeToString(&ObjectName, v16.Buffer);
88  v14 = ExAllocatePoolWithTag(0, 4 * v12, 0x206B6444u);
89  if ( v14 )
90  {
91    v22 = 0;
92    for ( Value = 0; Value < v12; ++Value )
93    {
94      RegistryPatha = RtlIntegerToUnicodeString(Value, 0xAu, &DestinationString);
```

Regin Platform – Stage 3 & 4



ExAllocatePoolWithTag routine

The **ExAllocatePoolWithTag** routine allocates pool memory of the specified type and returns a pointer to the allocated block.

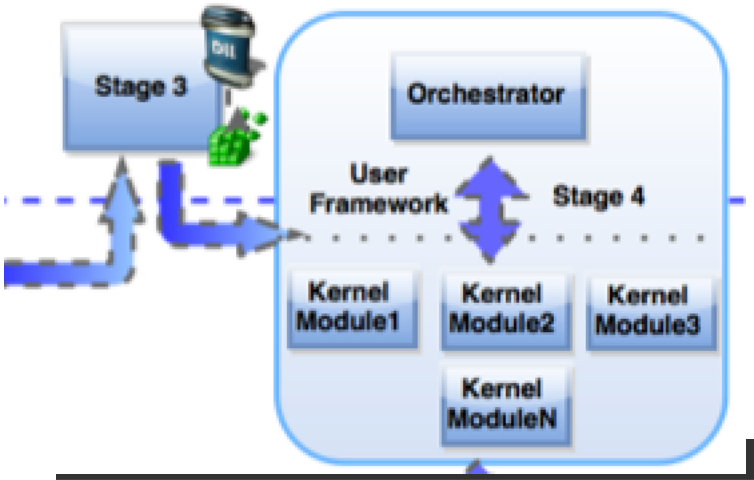
Syntax

C++

```
PVOID ExAllocatePoolWithTag(
  _In_ POOL_TYPE PoolType,
  _In_ SIZE_T    NumberOfBytes,
  _In_ ULONG     Tag
);
```

```
00029232 aNtoskrnl_exe   db 'ntoskrnl.exe',0
0002923F                 align 10h
00029240 unk_29240       db  3Ah ; :            ; DATA XREF: seg000:000291C8↑o
00029241                 align 2
00029242 aExallocatepool db 'ExAllocatePoolWithTag',0
00029258 unk_29258       db  47h ; G            ; DATA XREF: seg000:000291C4↑o
00029259                 align 2
```

Regin Platform – Stage 3 & 4



C++

```
VOID KeStackAttachProcess(
  _Inout_ PRKPROCESS   Process,
  _Out_   PRKAPC_STATE ApcState
);
```

Hex View-1 | Structures | Enums | Imports

```
:000294E1                 db    3
:000294E2 aPsterminatesys db 'PsTerminateSystemThread',0
:000294FA                 db  22h ; "
:000294FB                 db    2
:000294FC aKeunstackdetac db 'KeUnstackDetachProcess',0
:00029513                 align 4
:00029514                 db 0F0h ; =
:00029515                 db    2
:00029516                 db  50h ; P
:00029517 aScreatesystemt db 'sCreateSystemThread',0
:0002952B                 align 4
:0002952C                 db  1Eh
:0002952D                 db 2, 4Bh, 65h
:00029530 aStackattachpro db 'StackAttachProcess',0
:00029543                 align 4
:00029544                 db  60h ; `
:00029545                 db 4, 5Ah, 77h
:00029548                 db  4Fh ; O
:00029549 aPenprocess     db 'penProcess',0
:00029554                 db 0F3h ; =
:00029555                 db    2
8| 00029548: seg000:00029548|
```

Regin Platform – Stage 3 & 4 – How to Weaponize it ?

1. Register a call-back function to a process
2. Log the PID of the target process
3. Obtain PEB via **ZwQueryInformation()** for base adresses of the modules
4. Obtain the EP via **PsLookupProcesByProcess**()
5. Get inside to the process context via **KeStackAttachProcess()** referenced by EP
6. Read PEB and other data in process context

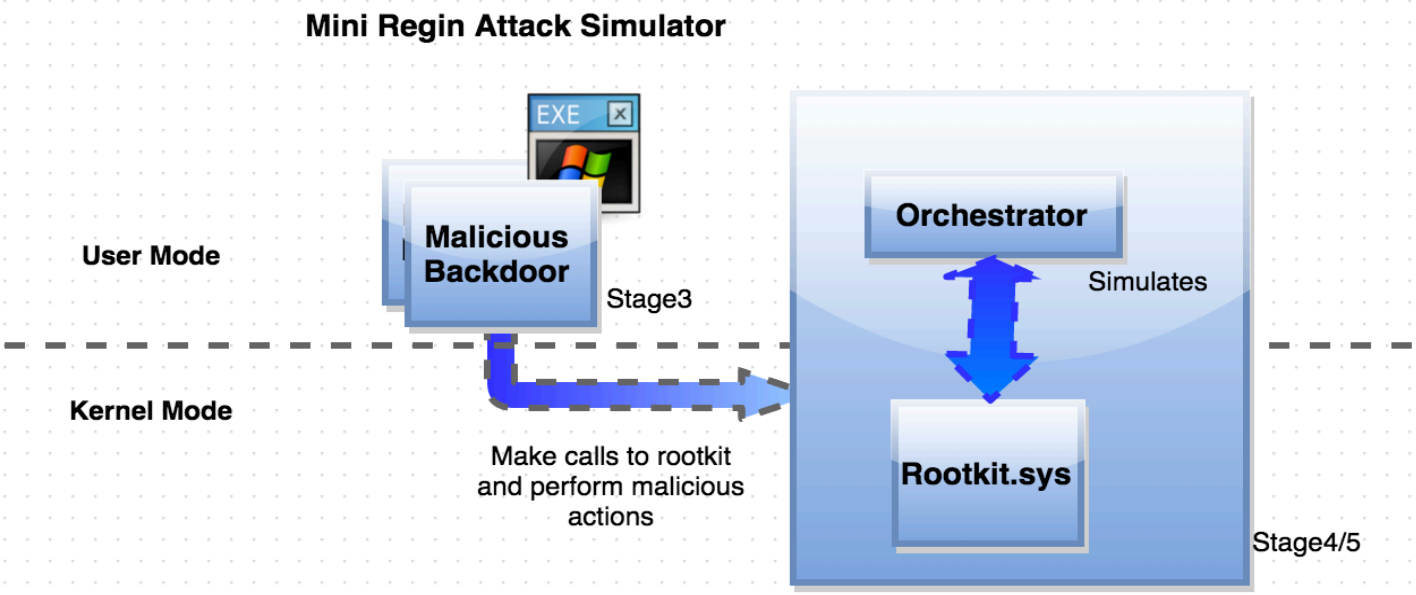
Regin Platform – Stage 3 & 4 – How to Weaponize it ?


```
InitializeObjectAttributes(&ObjectAttributes, NULL, OBJ_KERNEL_HANDLE, NULL,
    NULL);

clientID.UniqueProcess = hProcessId;
clientID.UniqueThread = NULL;


__try{


    status = ZwOpenProcess(&hProcessHandle, DesiredAccess, &ObjectAttributes,
        &clientID);

    status = ZwQueryprocess(hProcessHandle, ProcessBasicInformation,
        (PVOID)&BasicInfoReal, sizeof(PROCESS_BASIC_INFORMATION), &SizeReturned);

    status = PsLookupProcessByProcessId(hProcessId, &ep);

    __asm{
        mov eax, ep
            mov eax, [eax]
            mov myPwnProcess, eax
    }

    KeStackAttachProcess(&myPwnProces, ka_state);
```

Uruborus < Regin < Duqu2

Uruborus	Regin	Duqu2
Encrypted VFS	Encrypted VFS	Encrypted VFS #2
PatchGuard Bypass	Fake Certificate	Stolen Certificate
Multiple Hooks	Orchestrator SOA	Orchestrator SOA
AES	RC5	Camellia 256, AES, XXTEA
Backdoor/Keylogger Mod	Advanced Network/ File Mods	More Advanced Network/File/USB Mods

Regin Attack Simulation



Mini Regin Attack Simulator
Covert Channel Data Exfiltration
Run as a thread of legitimate app's address space
Orchestrator simulator and partial SOA
File system, registry and network calls hooking
Backdoor/Keylogger Mod

Demo

Questions ?

Thank you very much for your attention

References

- http://denmasbroto.com/article-5-gprs-network-architecture.html
- http://docstore.mik.ua/univercd/cc/td/doc/product/wireless/moblwrls/cmx/mmg_sg/cmxgsm.htm
- http://4g-lte-world.blogspot.nl/2013/03/gprs-tunneling-protocol-gtp-in-lte.html
- http://labs.p1sec.com/2013/04/04/ss7-traffic-analysis-with-wireshark/
- http://www.gl.com/ss7_network.html
- http://www.slideshare.net/mhaviv/ss7-introduction-li-in
- http://www.gl.com/ss7.html