Hijacking mobile data connections

Black Hat Europe 2009

Cristofaro Mune
Roberto Gassirà
Roberto Piccirillo

Agenda

- Provisioning & WAP primer
- Forging Messages
- Demo: Remote provisioning
- Provisioning: Process and Issues
- Attack scenario and exploiting
- Final Demo
- Wrap-Up

Poll

Who, among the audience, has an Internet capable phone?

Please raise your hands!!

Net in your hands...et

- ***Business:*** Mobile Operators business models mostly based on data revenues.
- ***Users:*** Information reachability everywhere
- ***Technical:*** Faster speeds, improved UIs
- ***Social:*** Smartphones are cool !!!

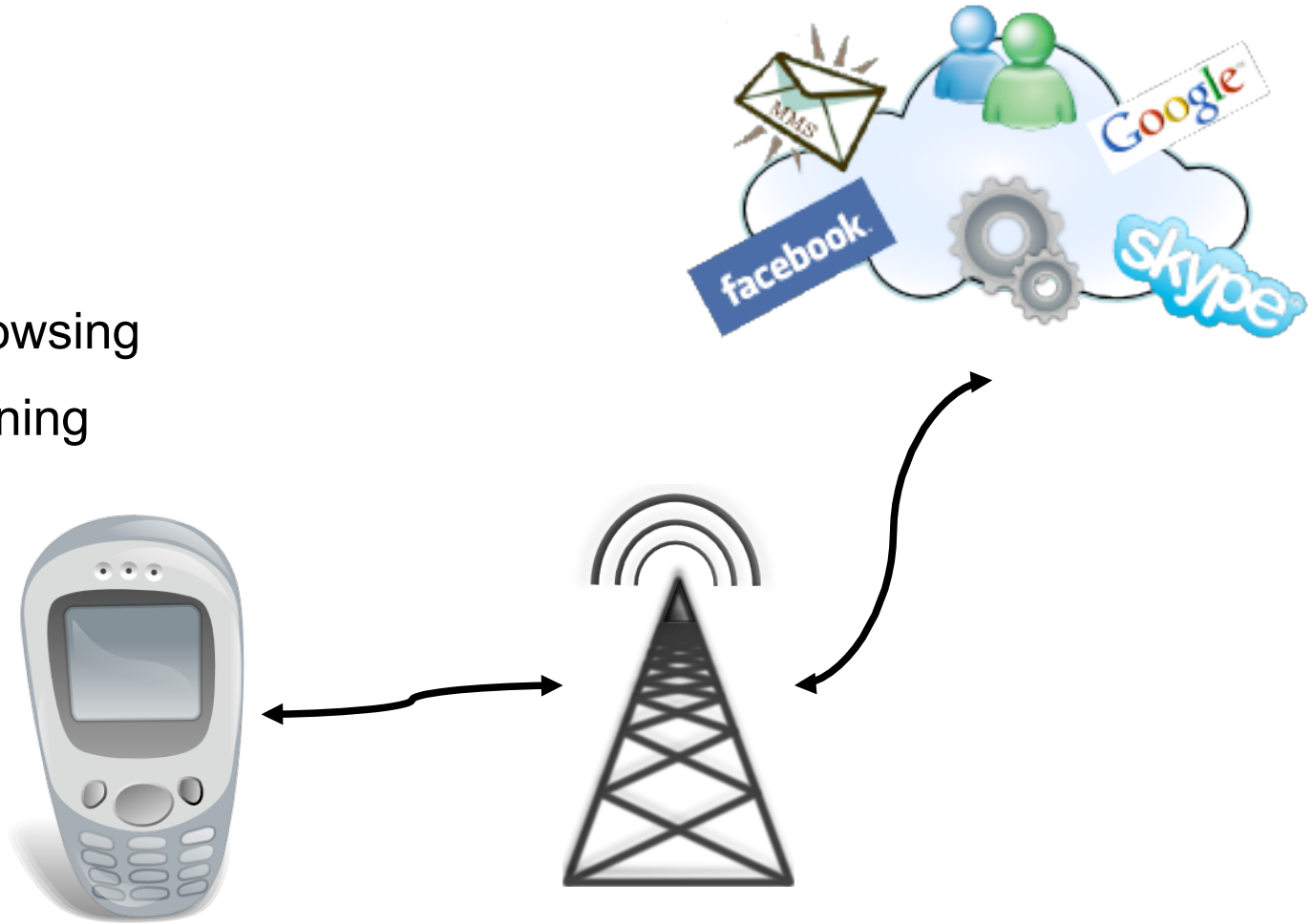
Provisioning

- Mobile Equipment must be configured to inter-operate with mobile infrastructures and services.
- "*Provisioning is the process by which a WAP client is configured with a minimum user interaction.*"
- Provisioning is performed using WAP architecture capabilities.
- *Normally* performed by mobile operators...

WAP Architecture

- "*Wireless Application Protocol defines industry-wide specification for developing applications that operate over wireless communication networks*".

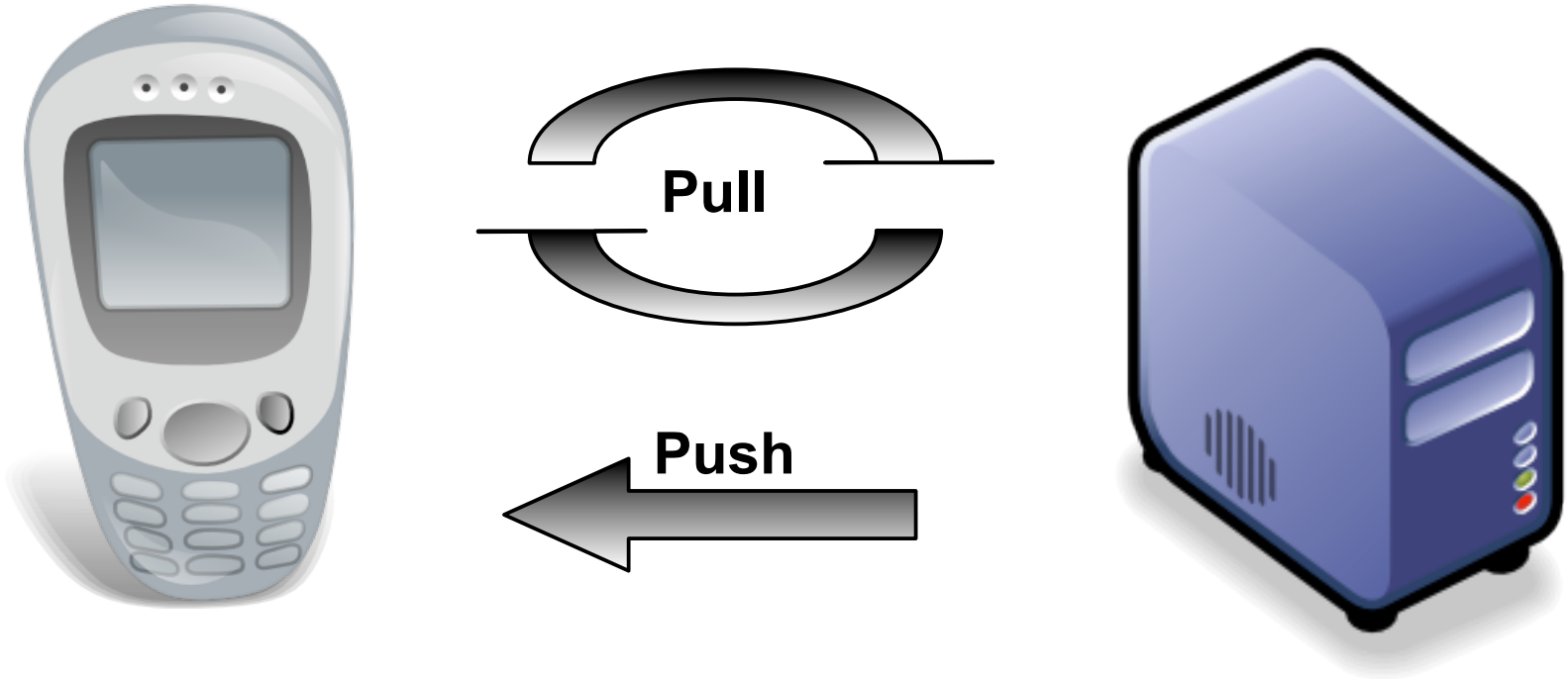
- Application?
  - MMS
  - Web Browsing
  - Provisioning
  - ...



WAP Communication

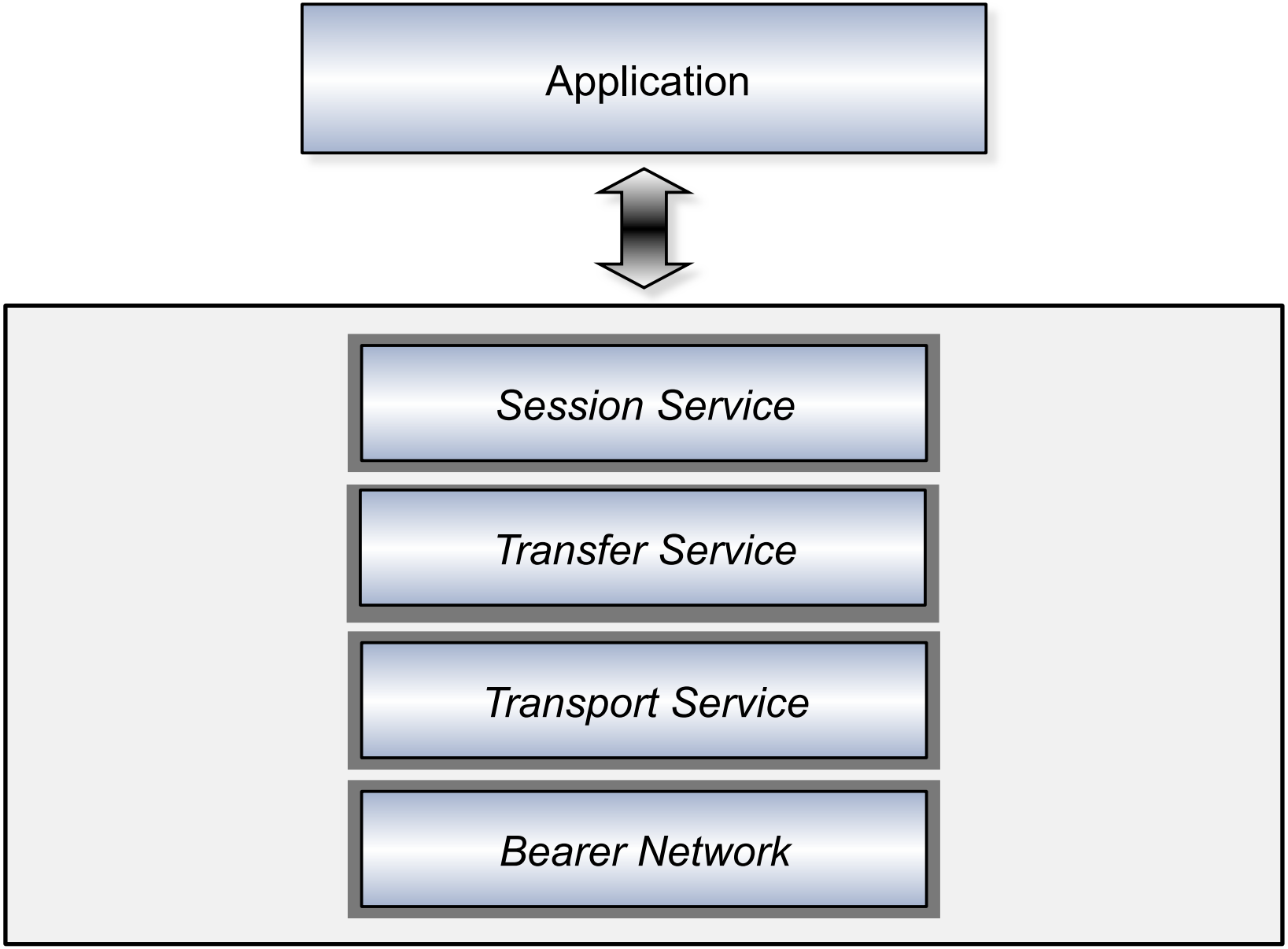
- WAP specifies communication protocol framework.

- WAP communication is based on two models:



- Push Model is normally used to send unsolicited data from server to the client.

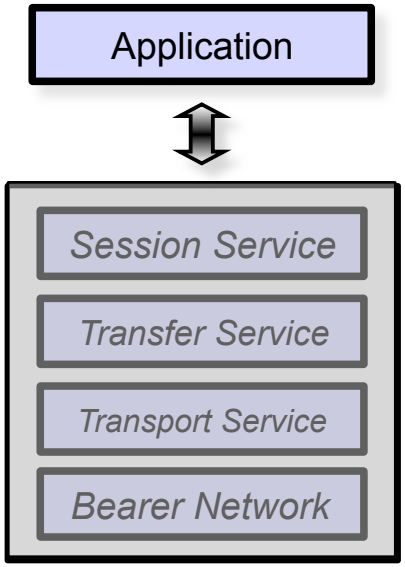
Protocol Framework



Let's build a provisioning message

Application - Provisioning Document

- A Provisioning Document provides parameters related to:
  - Network Access Points, application specific configuration etc.



- Use cases:
  - Provide configuration to new customers
  - Reconfigure mis-configured phones
  - Enable new services

- Provisioning Document is encoded in Wap Binary XML format (WBXML).

Binary Encoding Example

```
1 <wap-provisioningdoc>
2   <characteristic type="NAPDEF">
3     <parm name="NAME" value="bh"/>
4     <parm name="NAPID" value="bh_NAPID_ME"/>
5     <parm name="BEARER" value="GSM-GPRS"/>
6     <parm name="NAP-ADDRESS" value="apn.bh.com"/>
7     <parm name="NAP-ADDRTYPE" value="APN"/>
8   </characteristic>
9 </wap-provisioningdoc>
```

XML provisioning document is encoded in WBXML

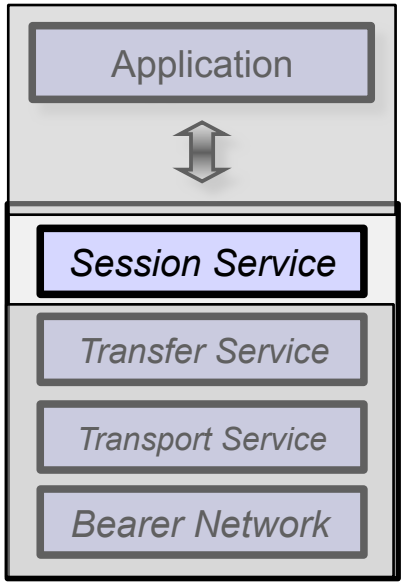
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	03	0B	6A	00	45	C6	55	01	87	07	06	03	62	68	00	01	..j.EÆU.‡...bh..
00000010	87	10	06	AB	01	87	09	06	89	01	87	08	06	03	61	70	‡..«.‡..‰.‡...ap
00000020	6E	2E	62	68	2E	63	6F	6D	00	01	87	14	01	01	01		n.bh.com..‡....

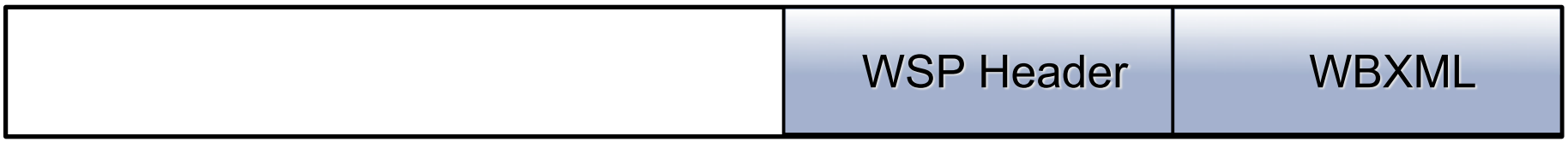
Offset: 4 = 69 Block: n/a Size: n/

	WBXML

Session Service - WSP

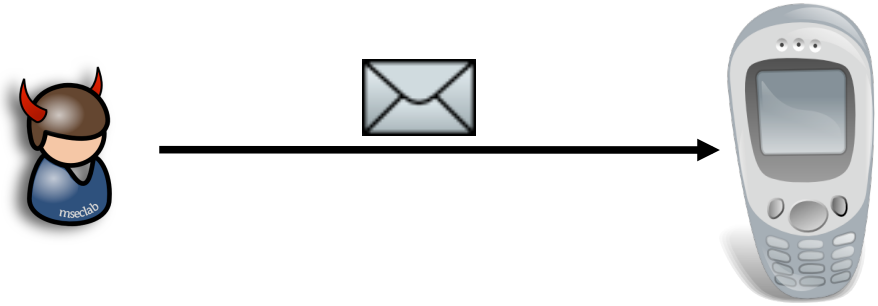
- WSP provides connectionless service PUSH.
- Delivering provisioning document requires:
  - Media type: *application/vnd.wap.connectivity-wbxml*
- … security information is usually required:
  - SEC parameter to specify security mechanism
  - Security mechanism related information





Security Purpose

- Message Authentication protects from accepting malicious messages from untrusted sources.

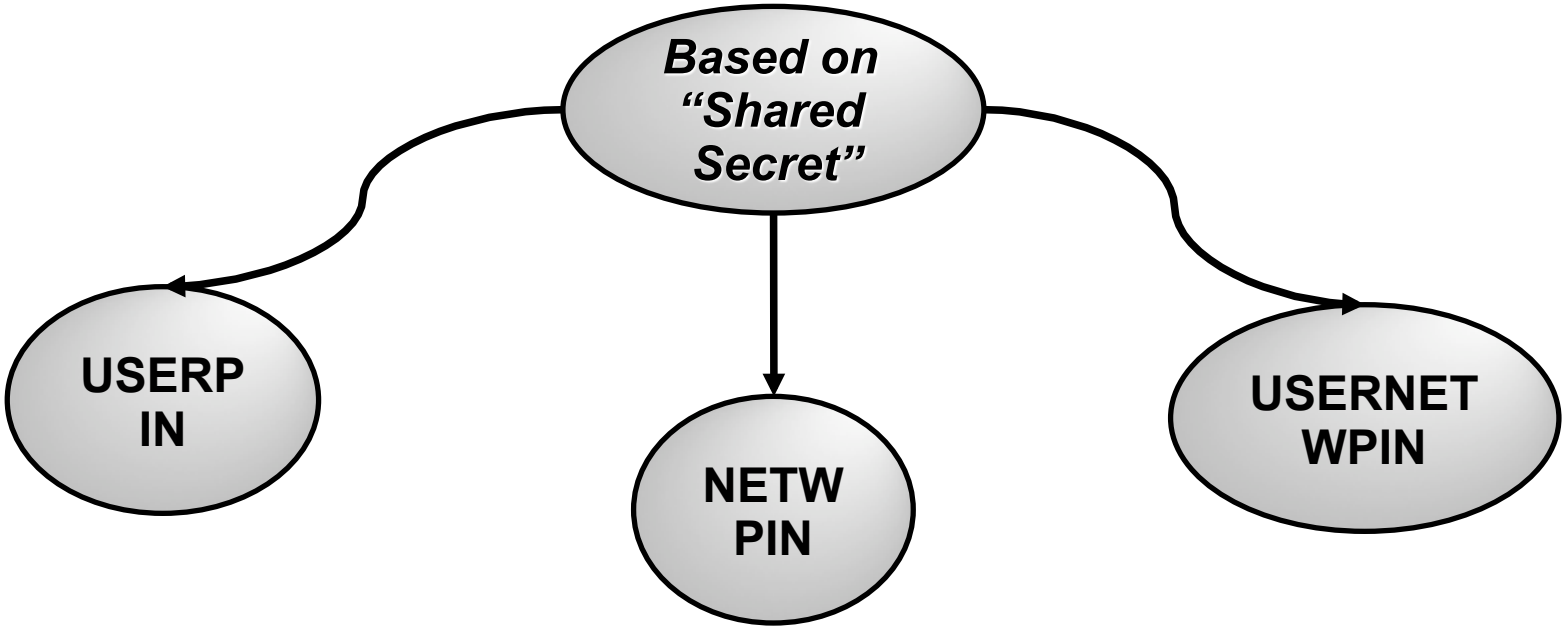


- Messages with no authentication may be discarded.

- Security based on HMAC to preserve sender authentication and document integrity.

Security Mechanism

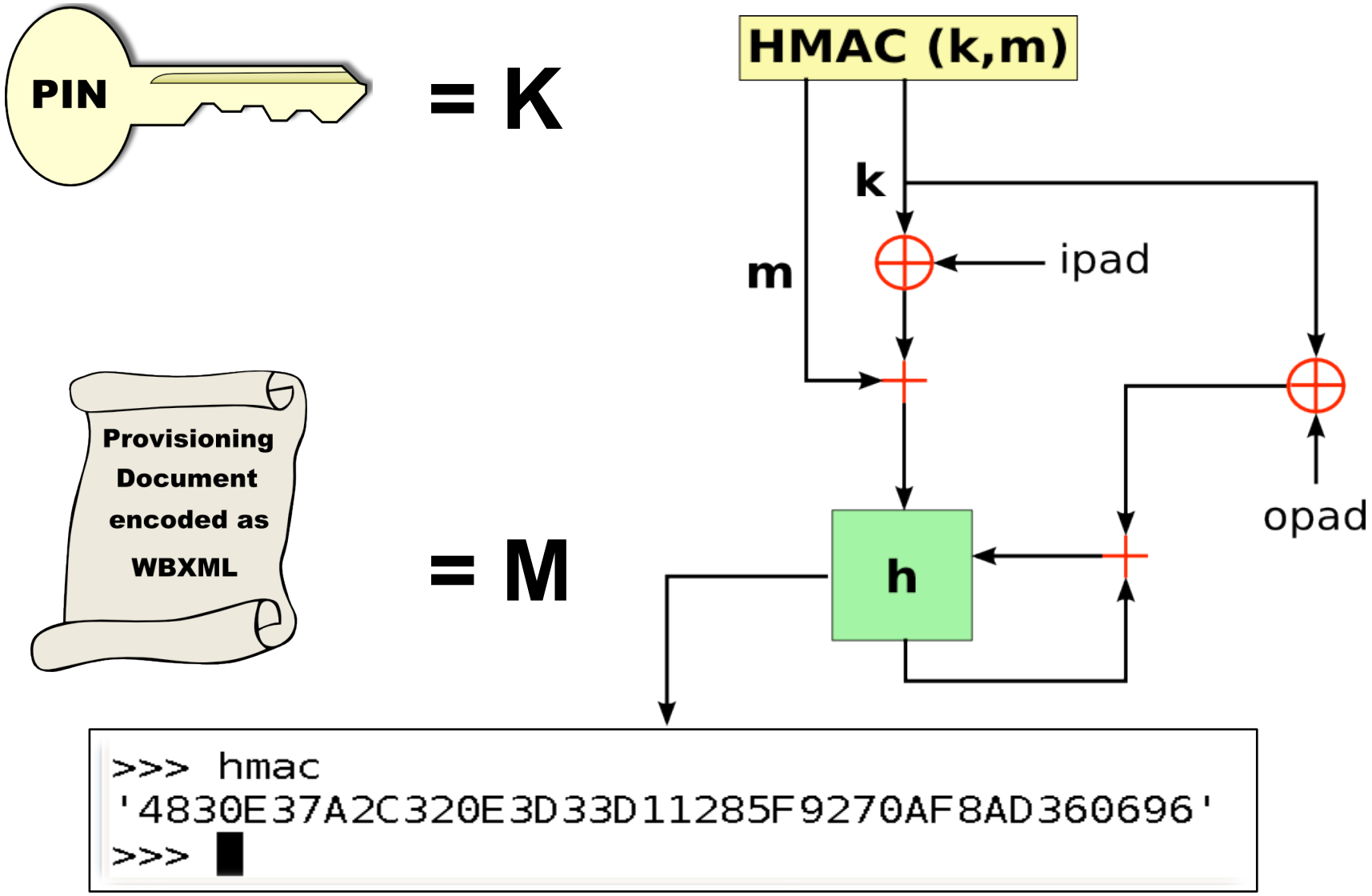
- Security mechanism used is typically based on “Shared Secret”



- “USERPIN”: key is numeric PIN code chosen by the sender
- “NETWPIN”: key is IMSI
- “USERNETWPIN”: hybrid approach

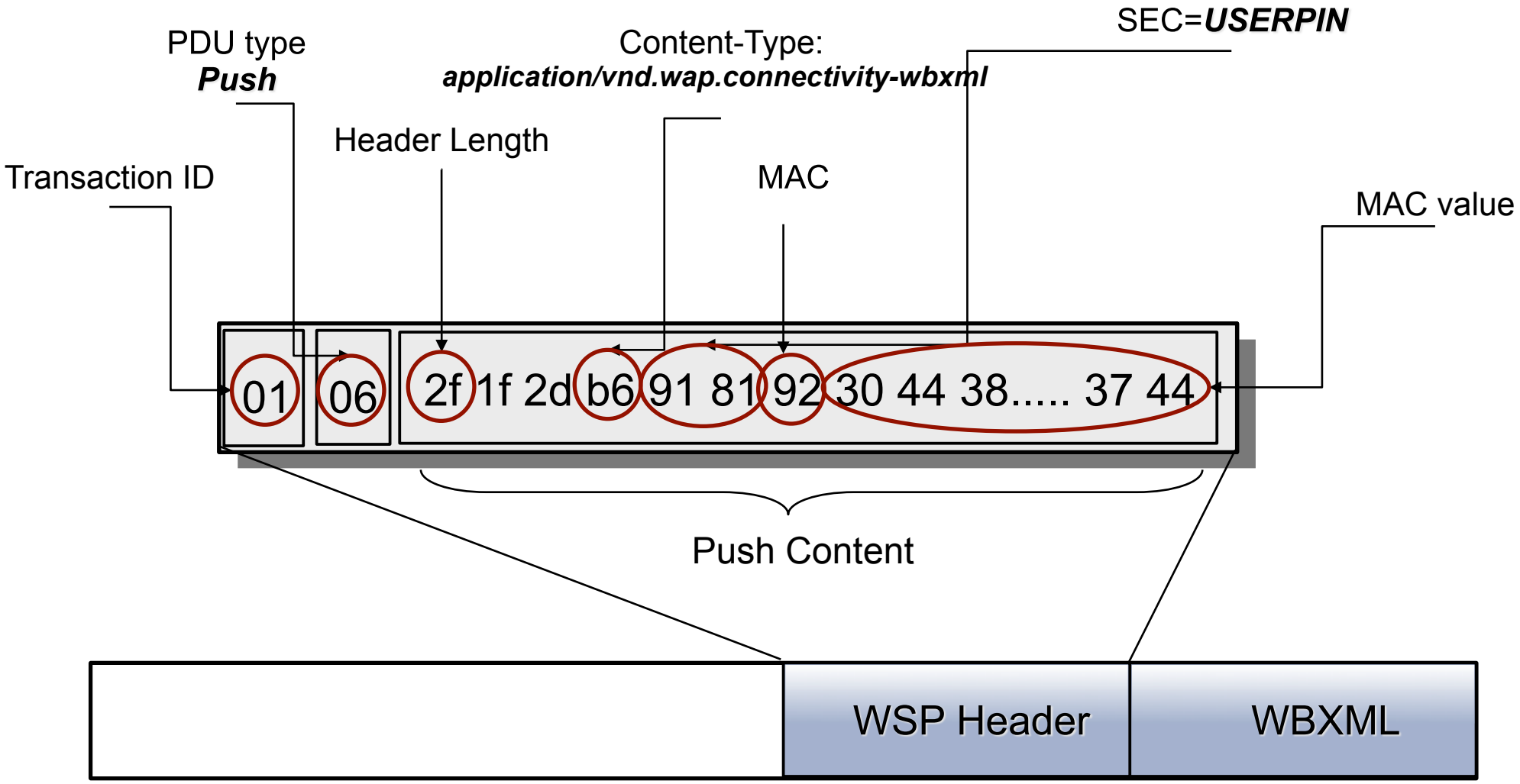
Security Mechanism: USERPIN

- It's based on HMAC algorithm



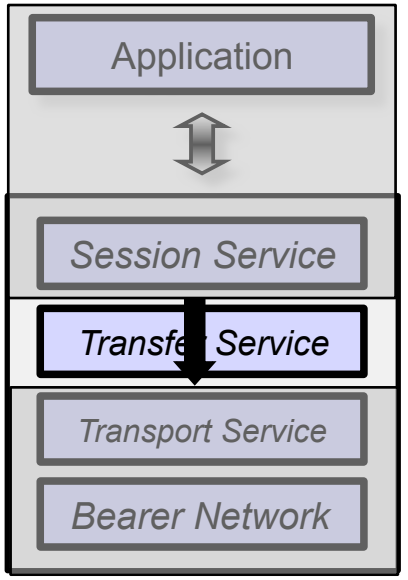
WSP Primitive Push

- Push primitive is used for sending unsolicited information from server to client

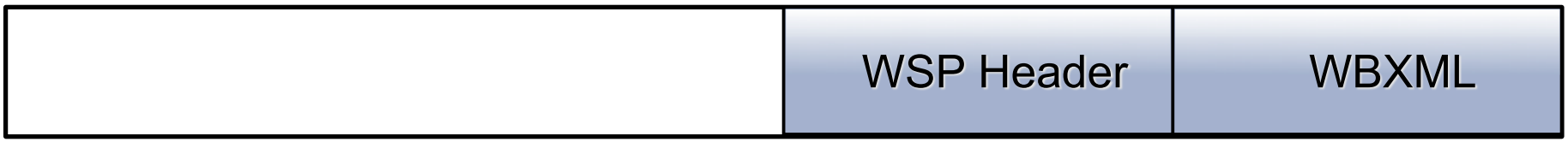


Transfer Service

- Transfer services provide reliable connection-oriented communications.
  - Offers services necessary for interactive request/ response applications

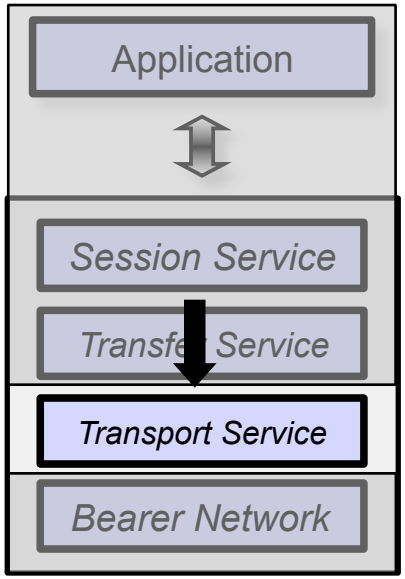


- Transfer service is not required by provisioning process.
  - Configurations are sent without using this layer



Transport Service - WDP

- WDP provides connectionless datagram transport service.
- WDP support is mandatory on any WAP compatible handset.
- WDP can be mapped onto a different bearer.
- WDP over GSM SMS is used to send the message.

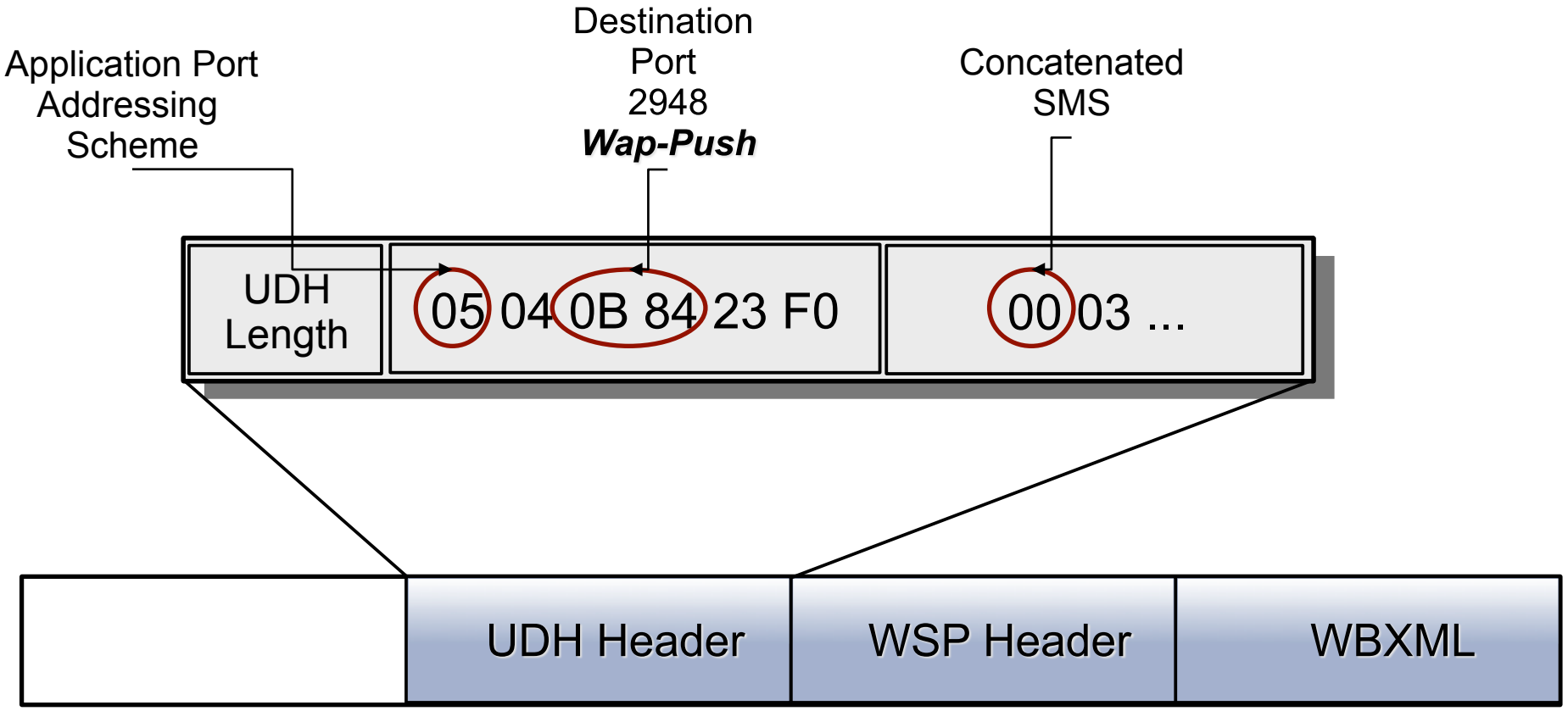


	WDP Header	WSP Header	WBXML

WDP over GSM-SMS

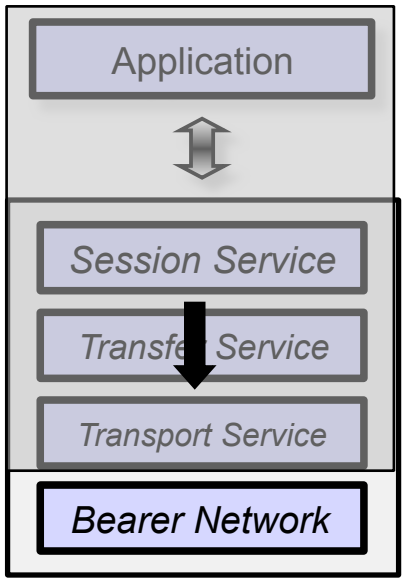
- WDP over GSM-SMS header is defined using UDH headers.

- UDH header contains information for port addressing and concatenated short messages



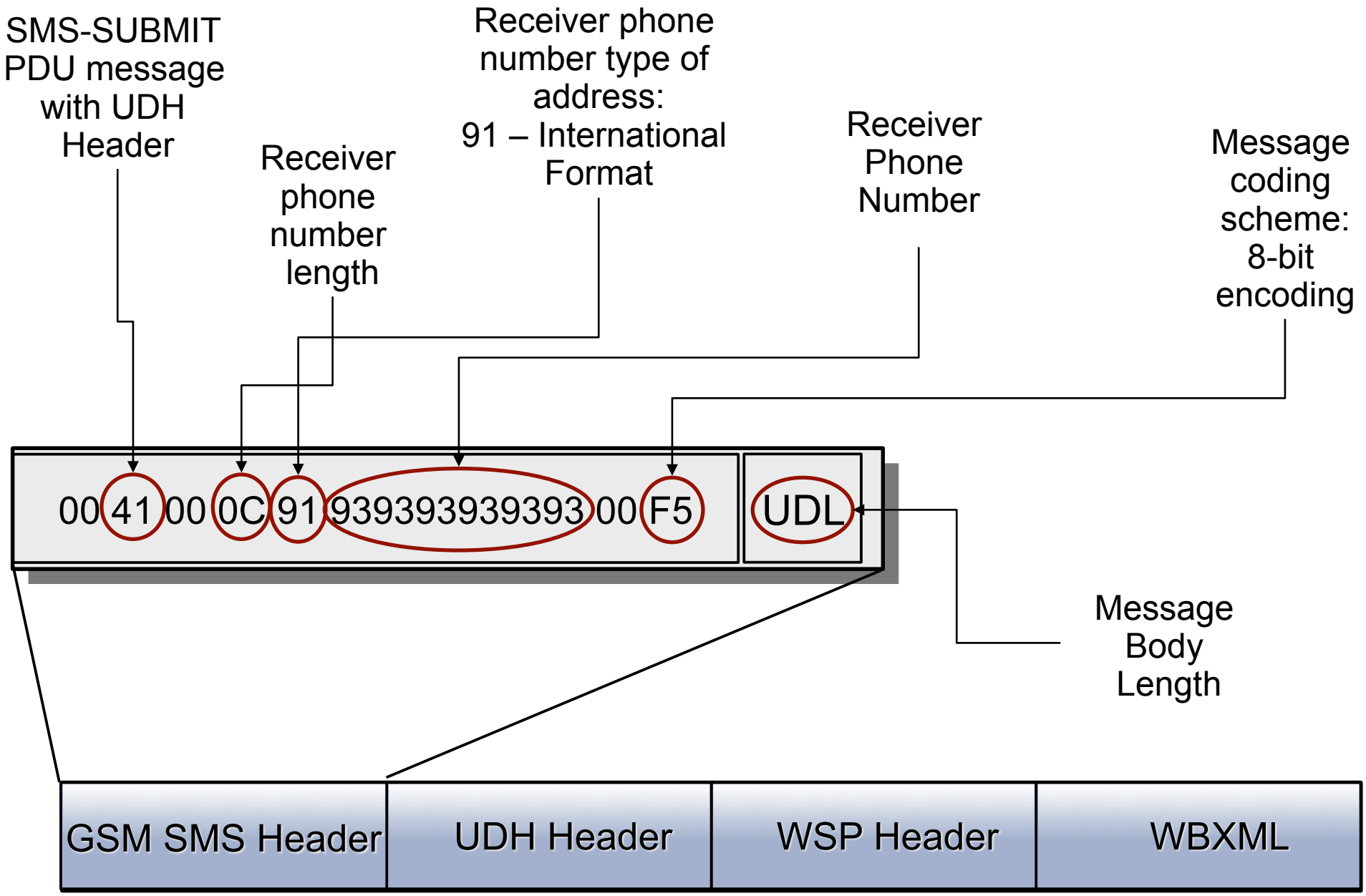
Bearer Network – GSM SMS

- GSM SMS PDU mode supports binary data transfer.
- Uncompressed 8-bit encoding scheme is used.
- Concatenated SMS is needed to send a payload larger than 140 bytes.
- Performed tests suggest that no restrictions are imposed on sending SMS-encapsulated provisioning messages.

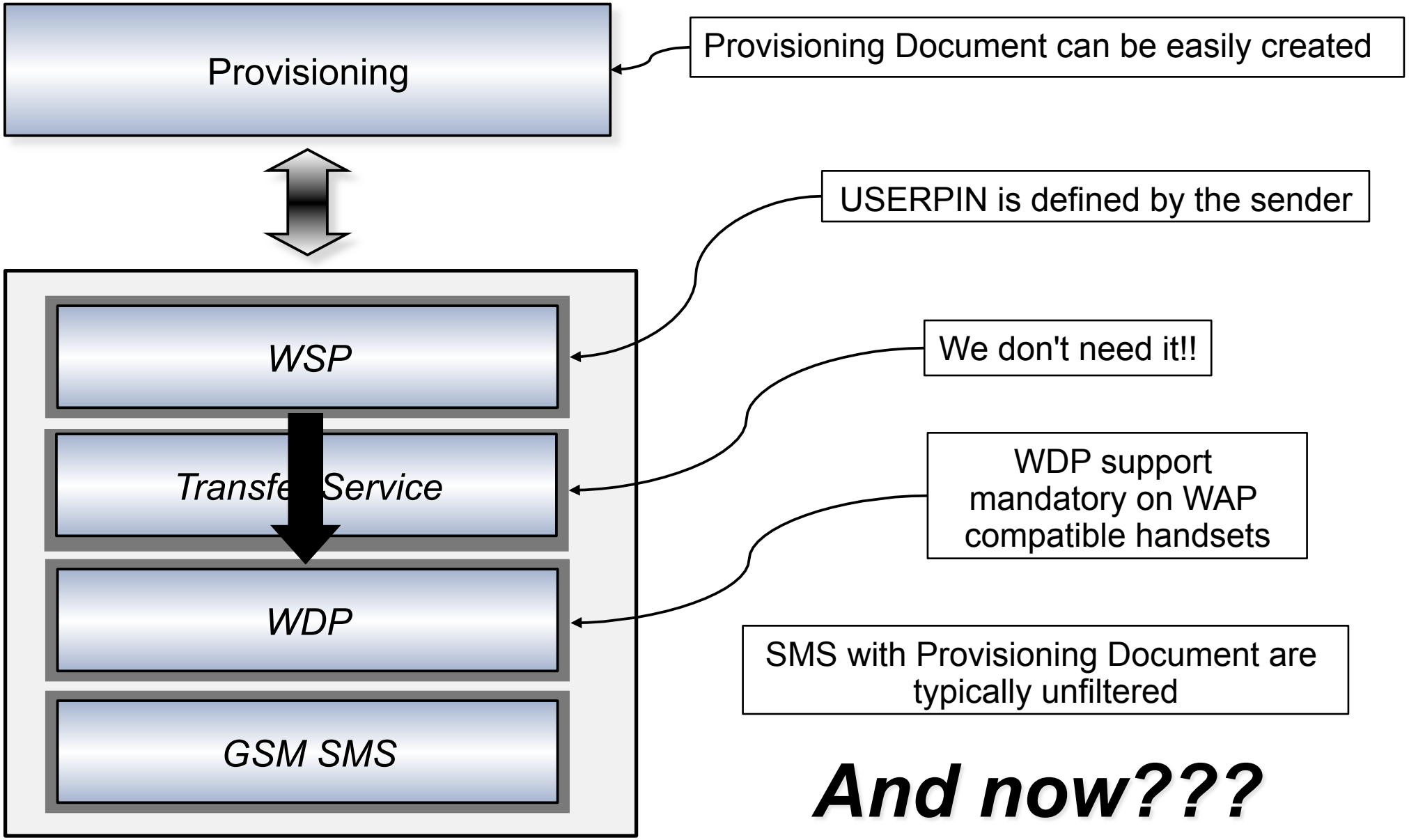


GSM SMS Header	UDH Header	WSP Header	WBXML

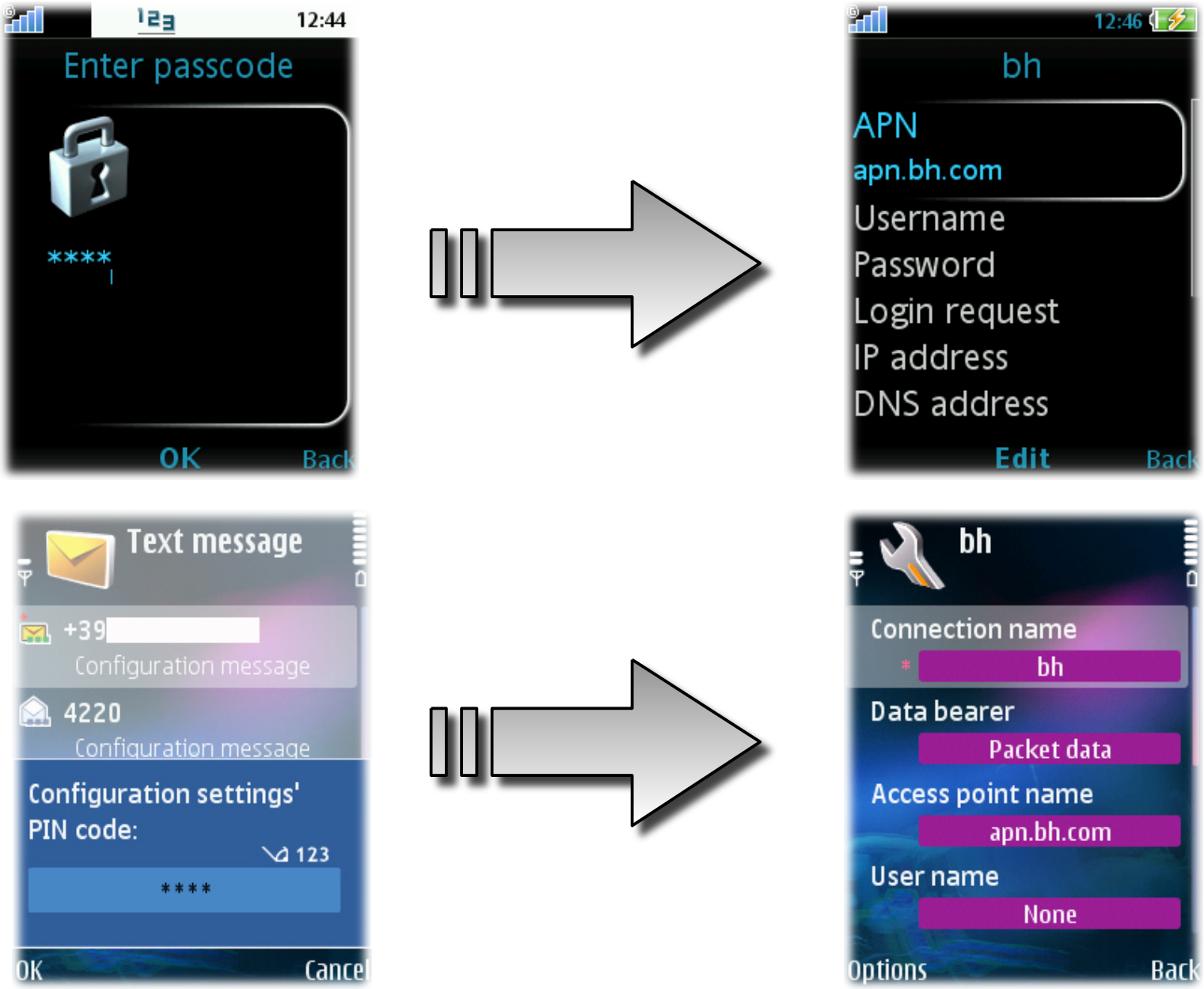
GSM SMS Header



Building a message



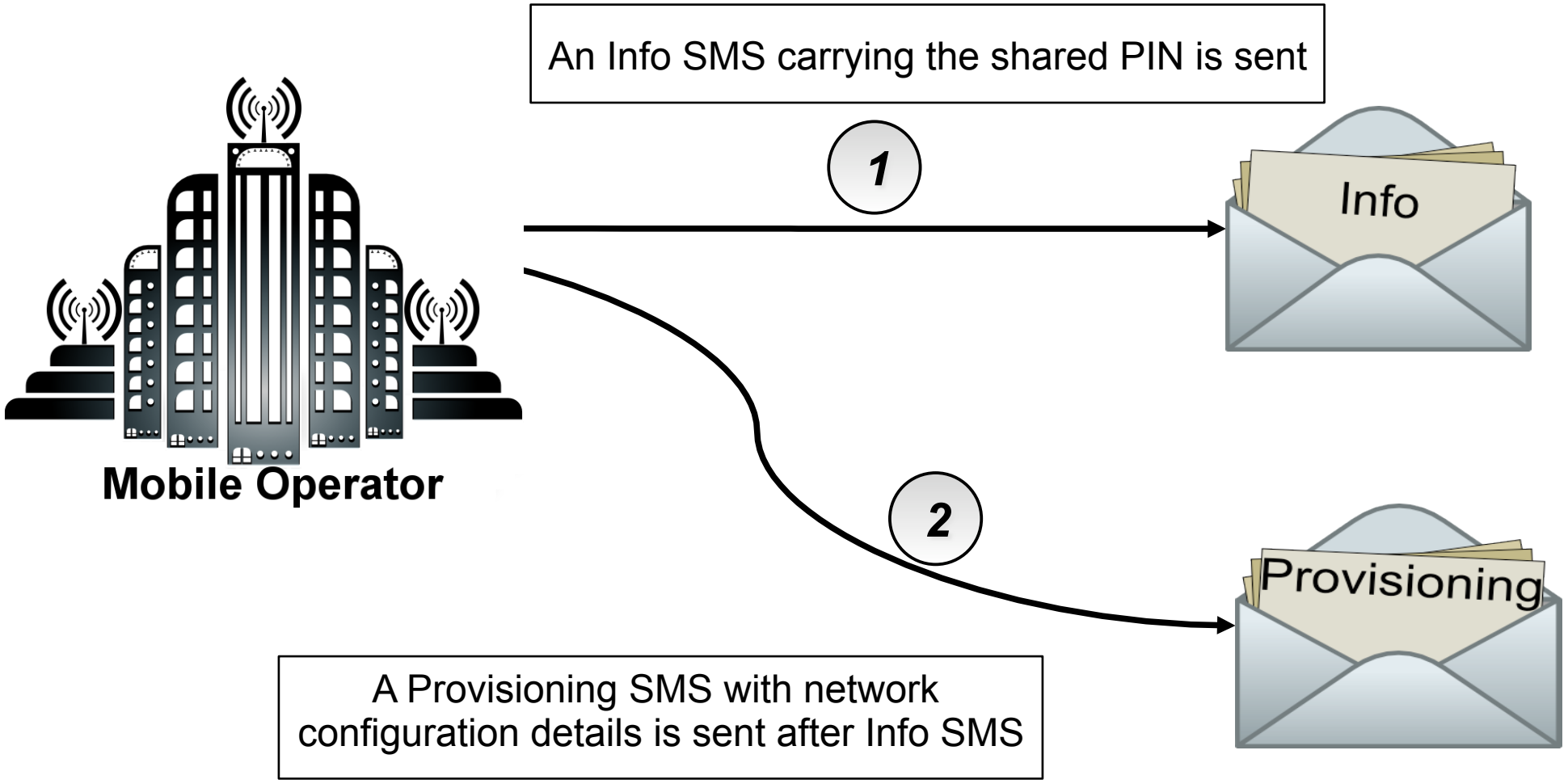
Demo: Profile Installation



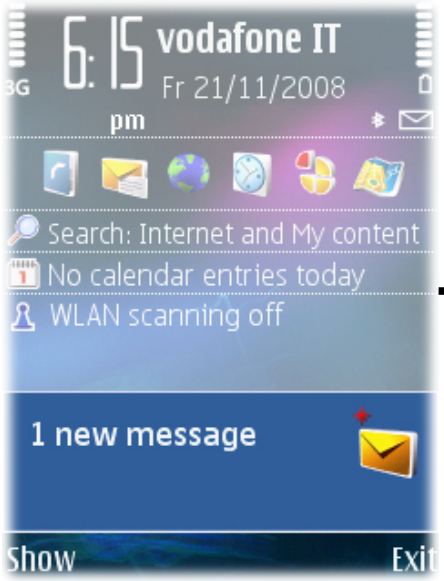
Provisioning Process

Mobile Operator Provisioning

- Many operators use USERPIN shared secret.



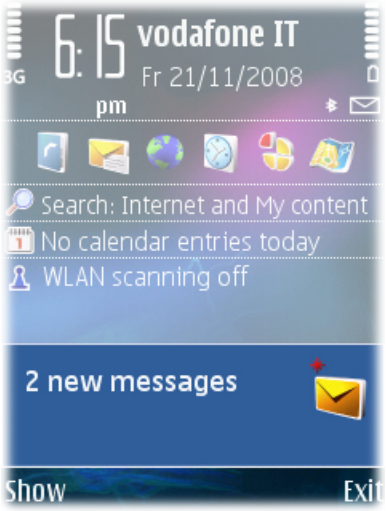
Info SMS



User takes a note of the pin

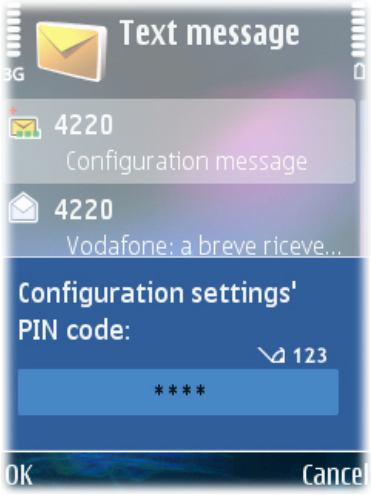
Operator Number used when sending Info SMS

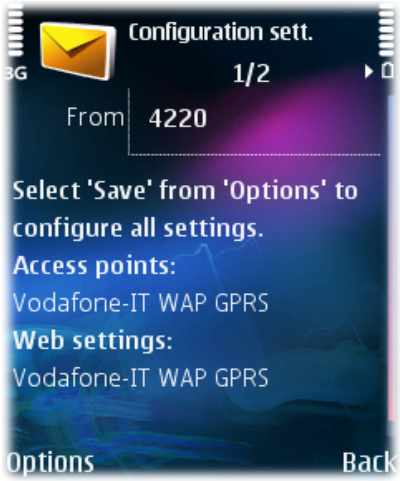
Provisioning SMS



1 The device receives a new SMS notification.

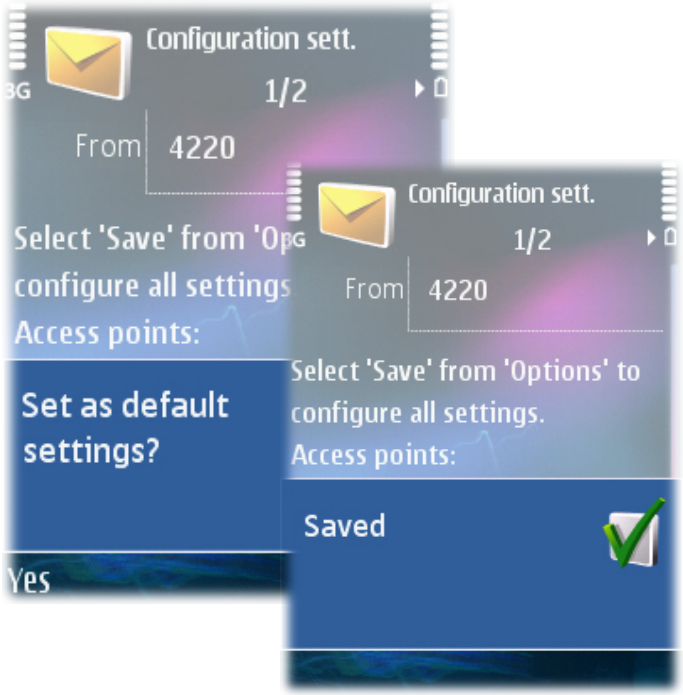
2 User types PIN provided by the Info SMS.





3 New settings overview is showed to the user.

Provisioning SMS

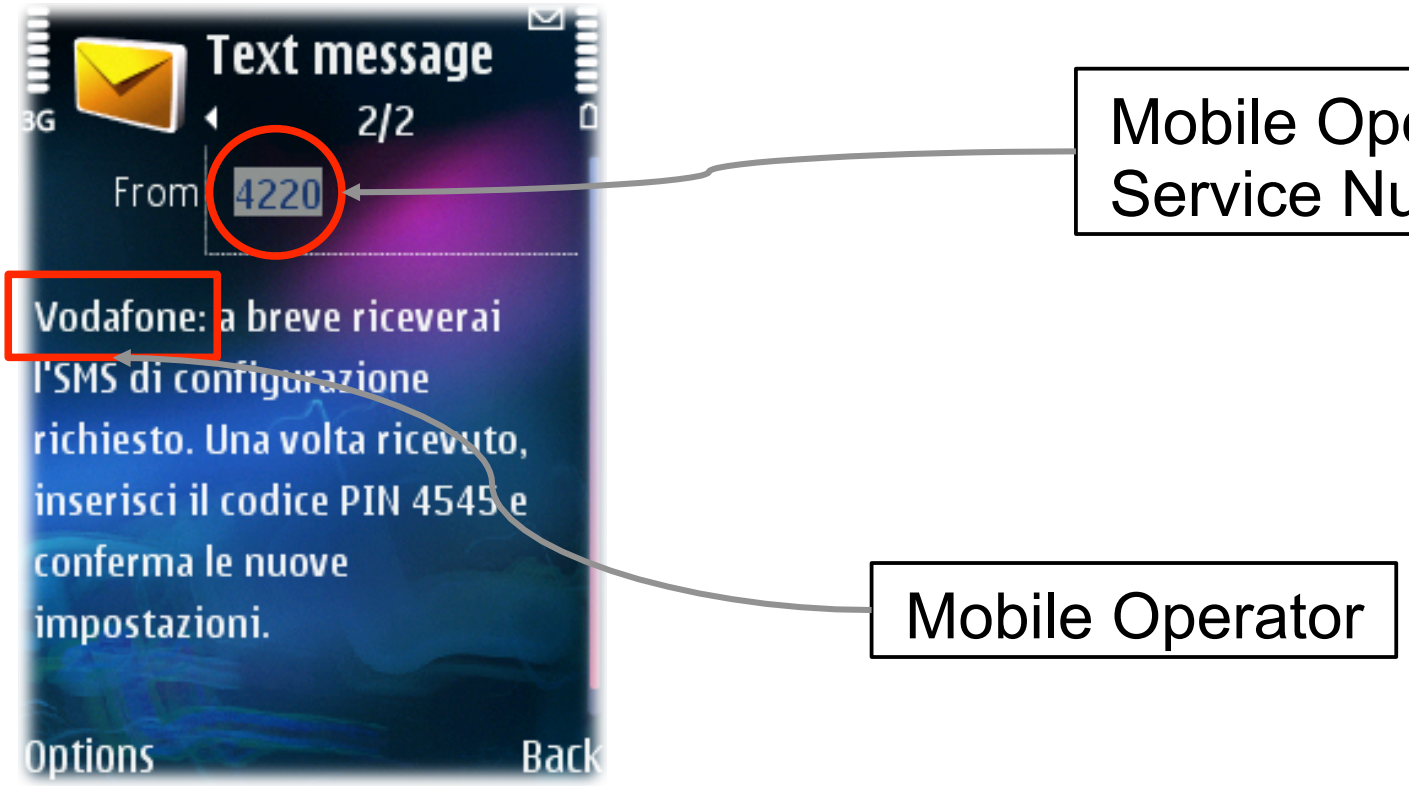


4 UI asks to use the new settings as default.

5 Settings are installed as a new Access Point.

Provisioning Issues

- User relies mostly on visual information to trust the received Info SMS.



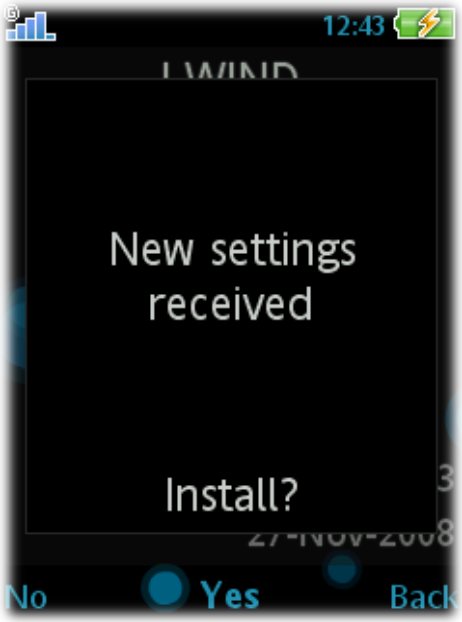
- Info SMS content can be easily forged.

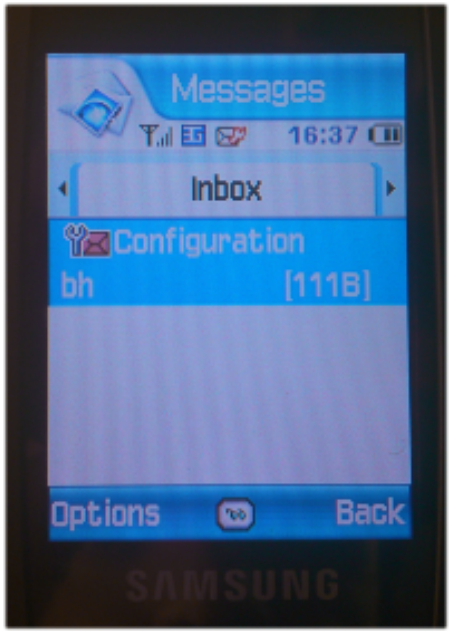
Provisioning SMS typically not filtered!

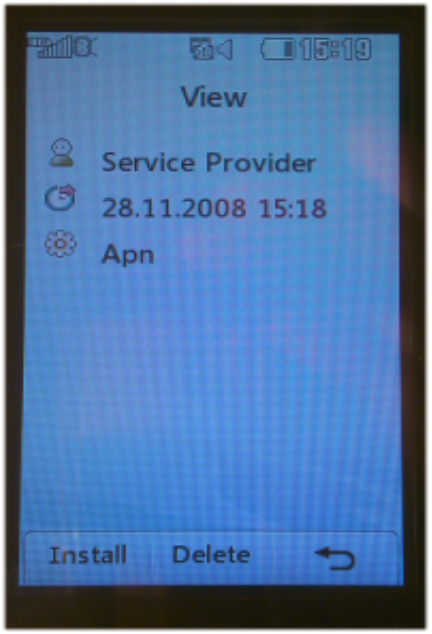
UI Issues

- UI designed to be user friendly …

- … but this could lead to confusing or hidden information:
  - Few technical details on provisioning content
  - Message source may be hidden or wrongly reported





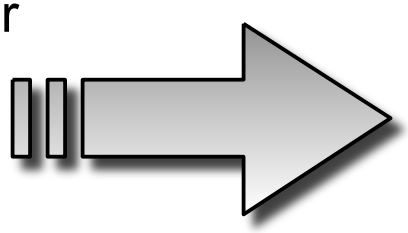


Attack for L(a)unch

Appetizer Preparation

Issue:

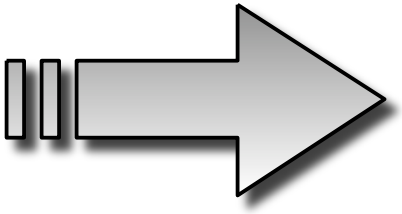
Handset displays phone number of Info SMS sender



Suspicious users may not accept the configuration message

Solution:

SMS sender spoofing



Info SMS could appear as legitimate and sent by Operator

Cooking: SMS spoofing

Bulk SMS Gateway

We provide SMS Gateways, Telecom Operators, Integrators and end-users with easy-to-use tools to facilitate their messaging workflow. We have various services to suit your needs:

Bulk SMS Gateway allows messages to be broadcasted to target mobile users via their handheld devices in any specified geographical area. This service is especially useful for applications in marketing, advertising, promotions, announcements and disseminating public information.

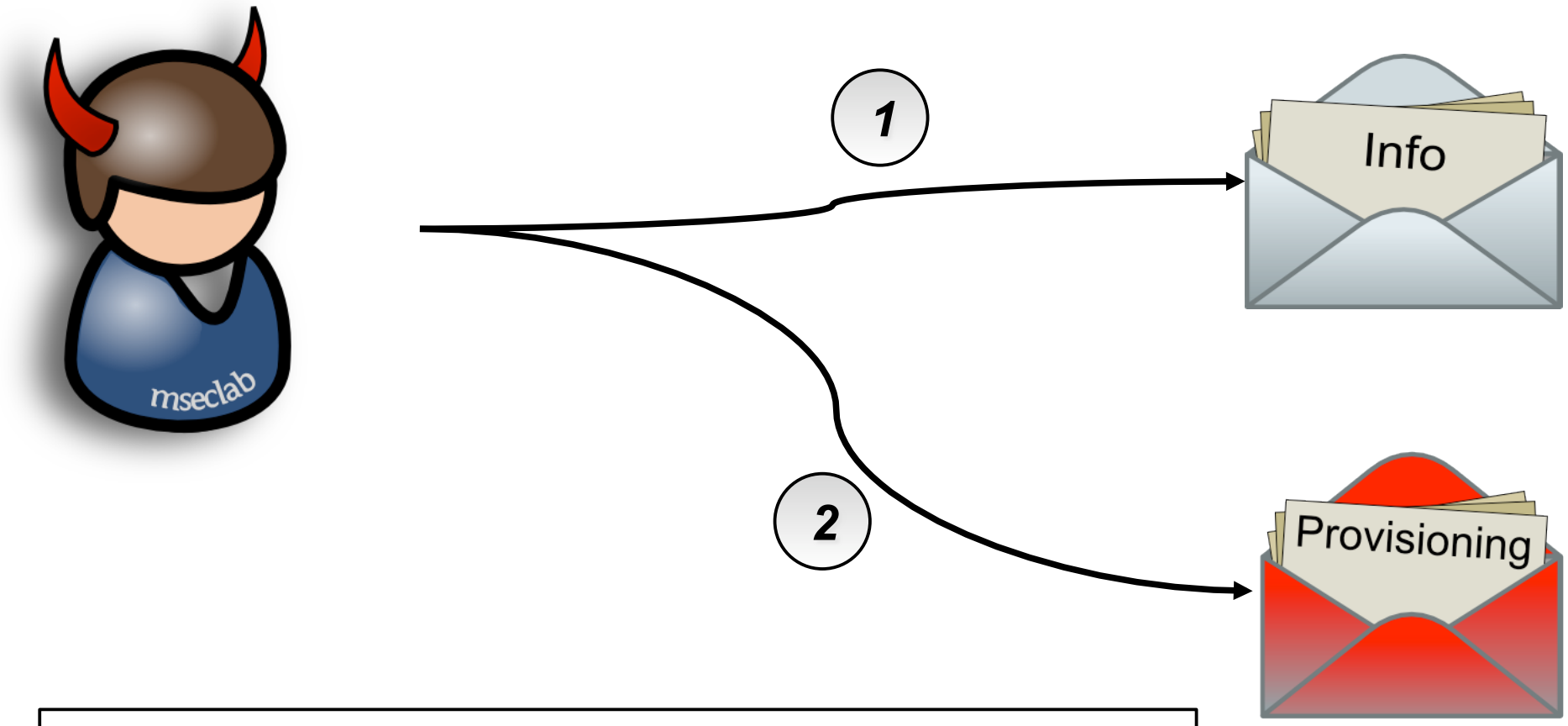
SMS Features

Union Vector Technologies is able to provide the following features with our SMS services:

- **Delivery Report**: Track the status of each message to confirm delivery to intended recipients
- **Dynamic/Fixed Sender ID**: Tag messages with either Dynamic Sender ID (your choice of Alphanumeric, Shortcode or International) or Fixed Sender ID (pre-specified longcode or shortcode)

Attack Scheme

Spoofed Info SMS carrying the PIN is sent (with Mobile Operator Service number)



Attacker Provisioning SMS is sent after Info SMS

Variations and Issues

- Different attack "*flavours*", depending on the handset:
  - Attacker configuration is ***automatically*** installed as the default
  - User is ***asked*** at ***installation time*** if the configuration has to be installed as the default
  - User is ***asked*** at ***connection time*** which configuration should be used for connection
- In some cases (eg: customized handsets) it may not be possible to change the default configuration
- Additional operations may be required from user

Appetizer Recipe

No Push Messages filtering in place: both on handset and network

+

Some UIs do not show enough information to users

=

Tricks users into accepting malicious configurations

Next choice...

- Provisioning message provides data connection parameters.

- If a victim accepts a malicious message, connection parameters are under attacker control

- Multiple interesting choices :
  - APN
  - DNS address
  - Proxy

Which is the best one???

Main Course Preparation

The parameter that seems to provide the best control of a victim is...

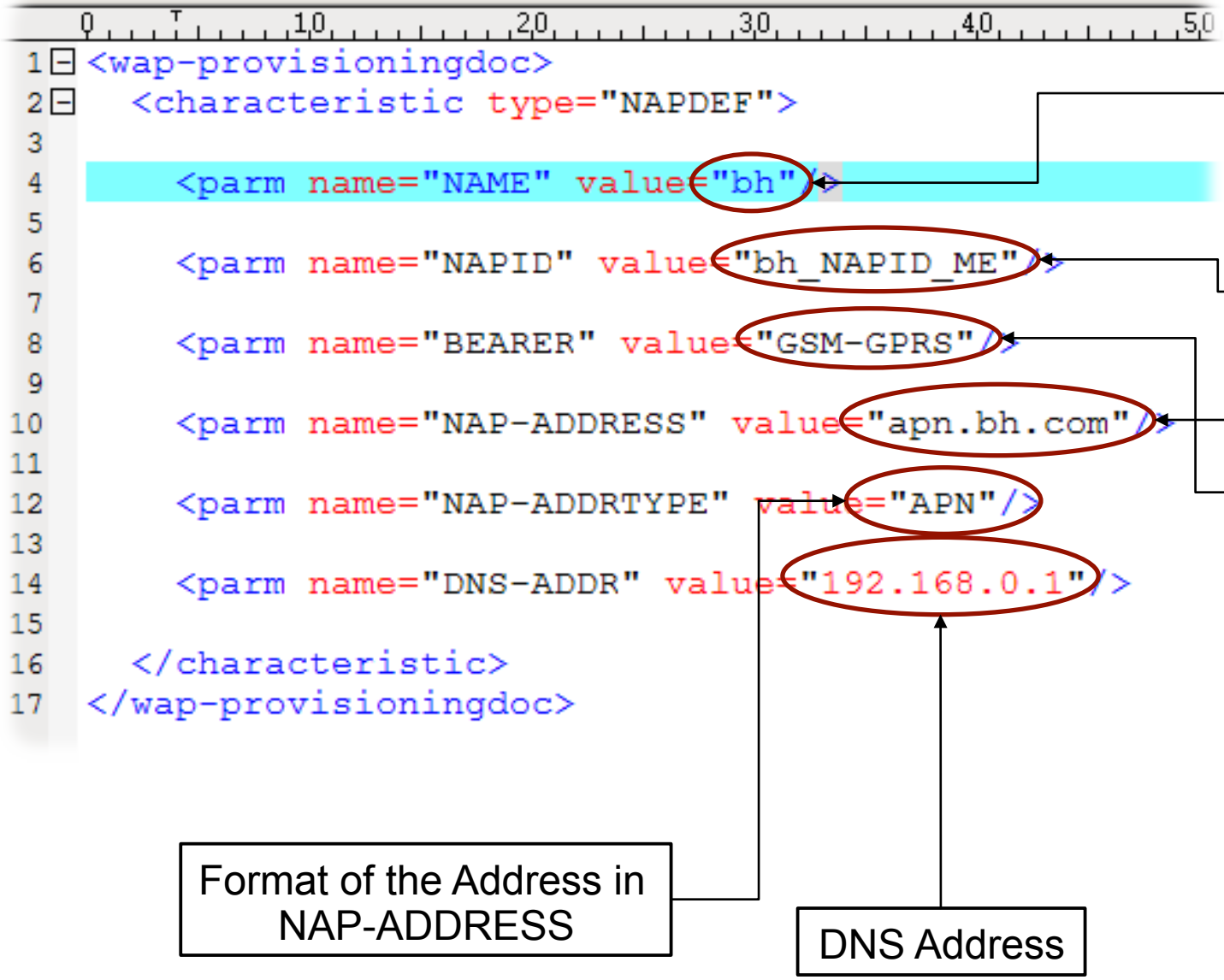
“DNS-ADDR”

Let's start cooking...

DNS Subverting

- "*Domain Name System (DNS) is used to map between hostnames and IP addresses.*"
- "DNS-ADDR" parameter indicates the DNS IP address used by the data connections.
- By adding the DNS-ADDR parameter to the default data connection, the DNS can be subverted.
- Victim DNS queries are then directed toward an attacker-chosen DNS server.

XML example with DNS



But...

Are DNS queries allowed to exit an Operator Network??

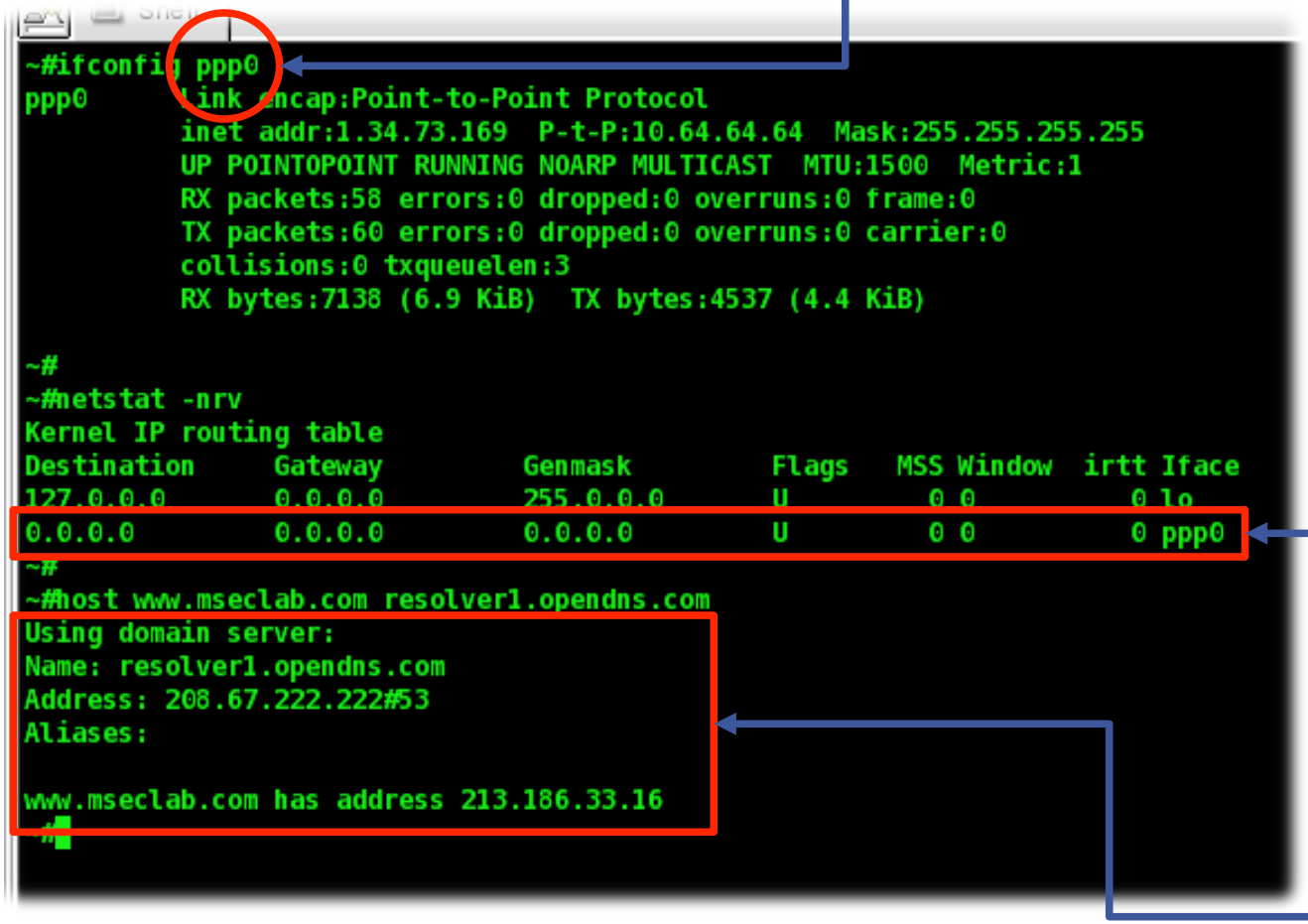
- The operator may force the use of specific DNS server

Tests have been performed on all the Operator Networks we had access to …

and the answer is...

Escaping the matrix

Definitely YES!!!



Dial-up using Handset as Modem

Default route via Mobile Operator Network

Successful query to external DNS server (OpenDNS)

Main Course Recipe

Modify default DNS in victim's phone

Operator networks allow queries to external DNS server

Redirection of victim DNS queries

0wning DNS

- Subverting DNS query toward attacker controlled DNS server yields the same effects of DNS poisoning attack.

- DNS poisoning threats have been widely explored:
  - Traffic redirection
  - Phishing
  - MITM attack
  - SSL attack

- All DNS queries, ***for ANY domain (!!)***, are completely under attacker control.

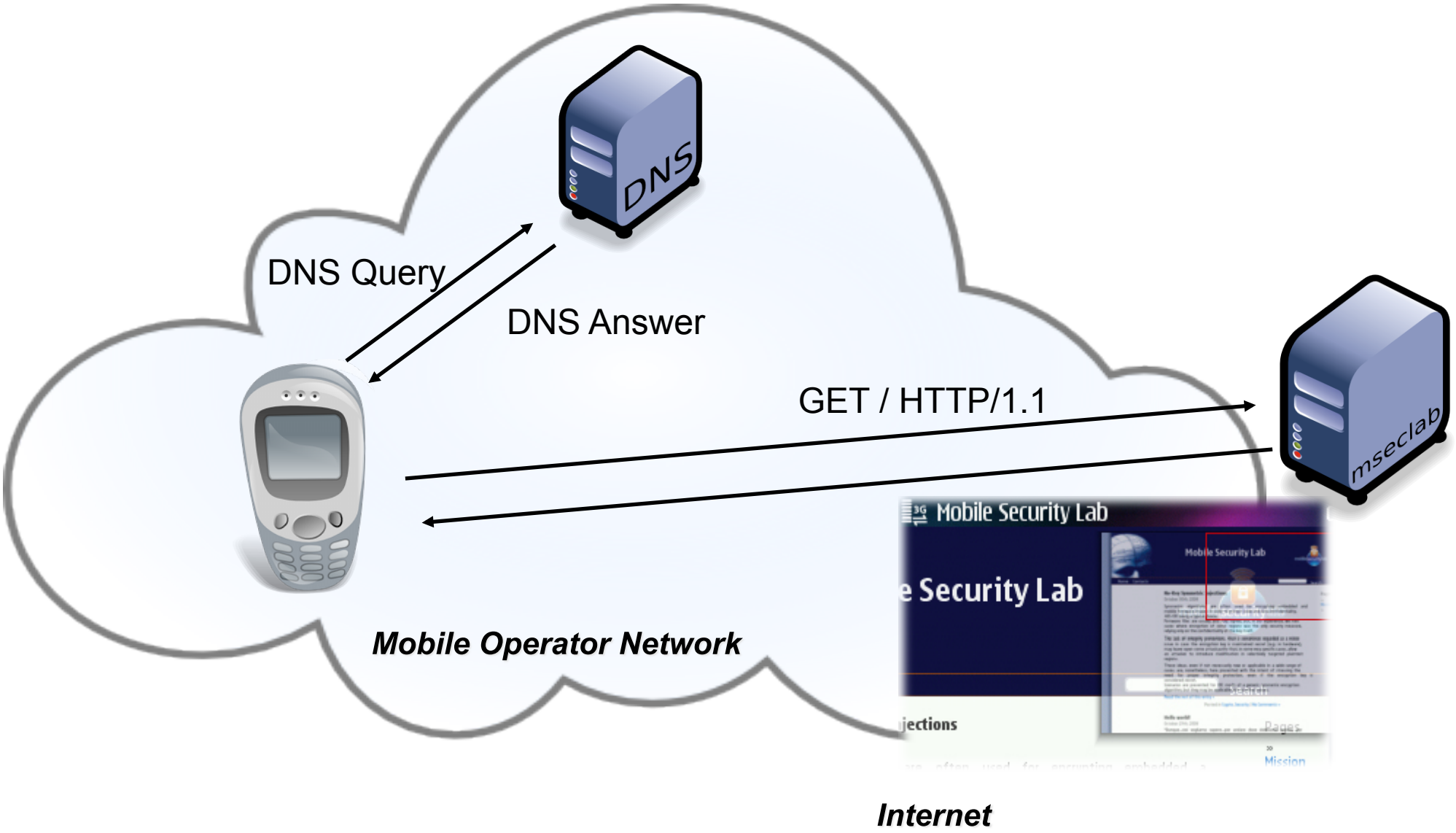
Next choice

- Most inviting options is HTTP:
  - Many mobile applications and services are based on HTTP protocols:
    - Browsers
    - Messaging
    - ...
  - Some Mobile Operators business models are based on providing services via internal HTTP web sites.

Let's focus on HTTP traffic redirection and MITM attack!!!

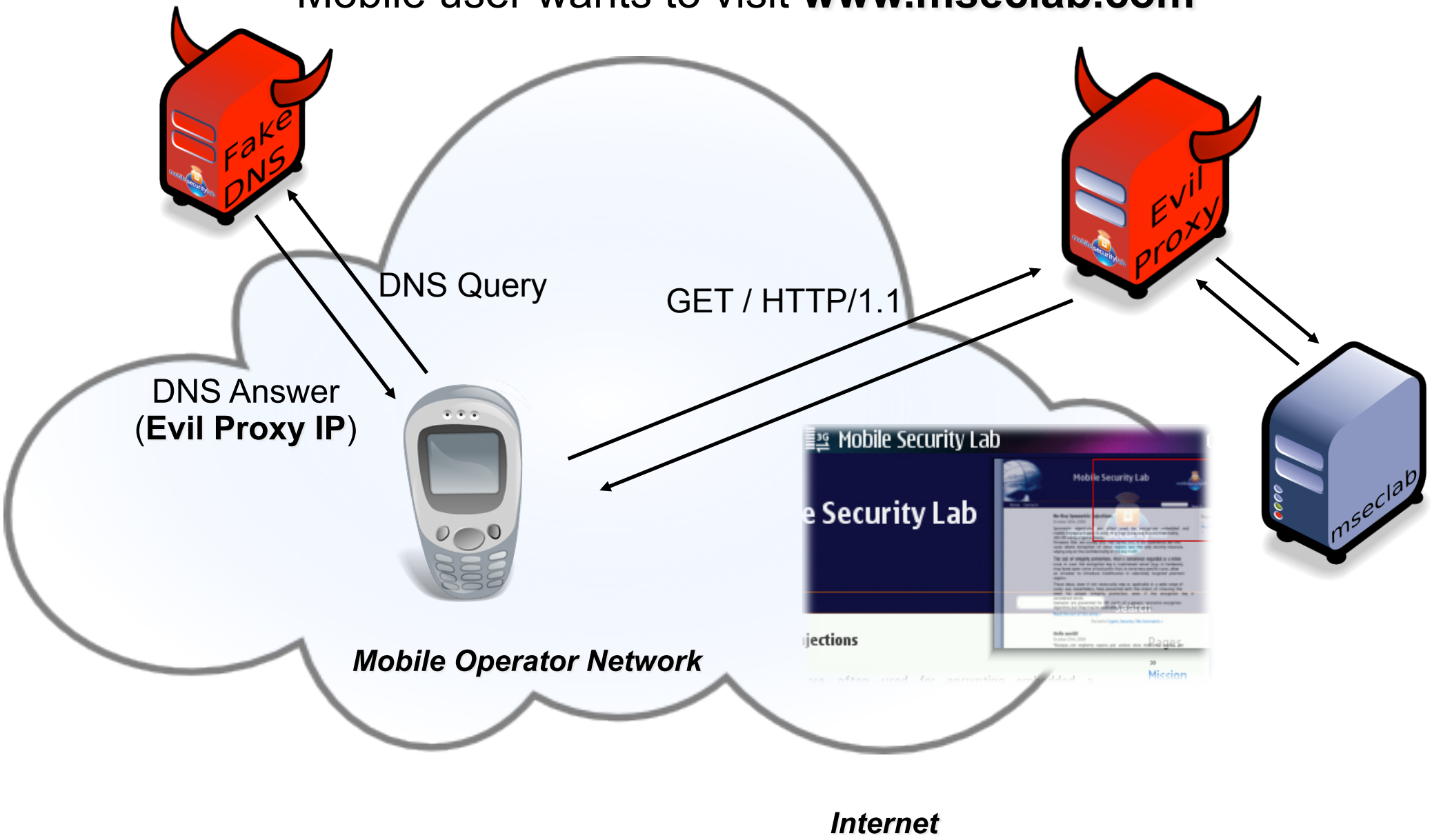
Standard HTTP transaction

Mobile user wants to visit **www.mseclab.com**



Redirect HTTP transaction

Mobile user wants to visit **www.mseclab.com**



XML with APPLICATION settings

```
1  <wap-provisioningdoc>
2    <characteristic type="NAPDEF">
3
4      <parm name="NAME" value="bh"/>
5
6      <parm name="NAPID" value="bh_NAPID_ME"/>
7
8      <parm name="BEARER" value="GSM-GPRS"/>
9
10     <parm name="NAP-ADDRESS" value="apn.bh.com"/>
11
12     <parm name="NAP-ADDRTYPE" value="APN"/>
13
14     <parm name="DNS-ADDR" value="192.168.0.1"/>
15
16   </characteristic>
17
18   <characteristic type="APPLICATION">
19
20     <parm name="APPID" value="w2"/>
21
22     <parm name="NAME" value="bh"/>
23
24     <parm name="TO-NAPID" value="bh_NAPID_ME"/>
25
26   </characteristic>
27 </wap-provisioningdoc>
```

DNS Address

Used to define Application Parameters

Browsing Applications Identifier defined by OMNA

Link to APN defined

Dessert Recipe

WBXML provisioning message (setting handset DNS address to Fake DNS)

+

Fake DNS (answering any query with Evil Proxy IP Address)

+

Evil Proxy (intercepting and forwarding the HTTP traffic)

=

Owning victim data traffic by means of _DNS control_

Serving the meal ...

Evil Proxy How-to

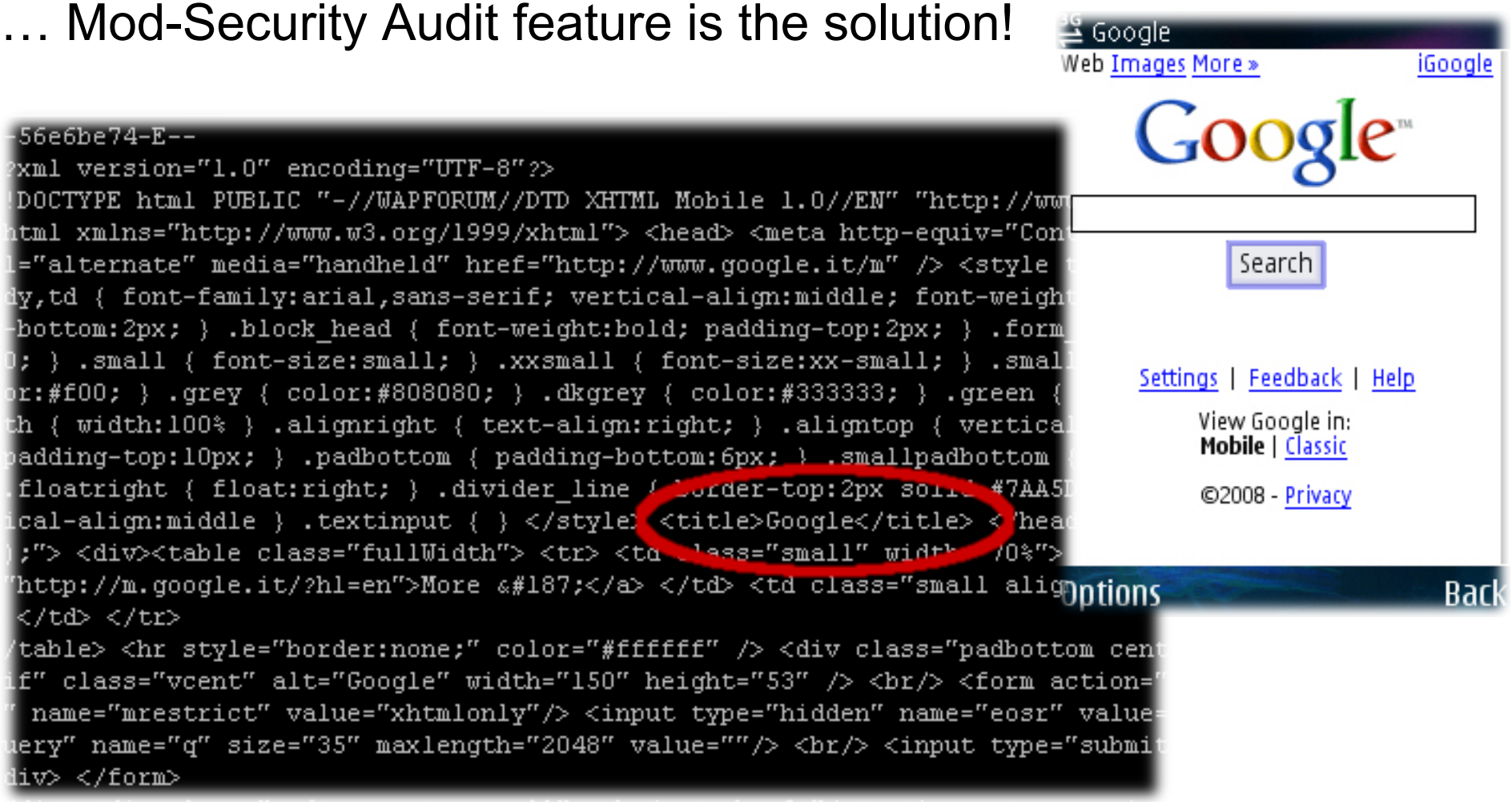
- Transparent proxy is just what we need.
- Apache+Mod-Proxy is a good starting point:

- Mod-Rewrite is used for proper redirection.

```
RewriteRule (.*) http://%{HTTP_HOST}$1 [P]
```

Mod-Security Power

- Now we are able to redirect the HTTP traffic as we want!
- It would be cool to access the traffic...
- … Mod-Security Audit feature is the solution!



Demo

[Hijacking remote mobile user browsing]

WARNING: Mobile connections on the test handsets will be monitored!!!

so…

Do NOT enter personal information or URL!!!

What can be achieved?

- User monitor and profiling

- Hijacking and control of application specific data traffic
  - IM, VoIP, Social Networks

- Traffic Injection
  - Redirection to 3rd party websites
  - Advertisements (→ Spamming)
  - Modification of served web pages

Focus on Issues

- The attack does not rely on the exploitation of a single vulnerability

- Issue at the 'system' level:
  - Small overlooked details concur in allowing a deeper exploitation

- The following made this attack possible:
  - Lack of Provisioning message filtering
  - UIs do not provide a sufficient level of details
    - Spoofing sharpen the issue!
  - Mobile Operator Networks allow use of external DNS servers

Countermeasures

- Filter external provisioning messages:
  - Network side
  - Handset Side (may be ineffective in case of spoofing)
- UI Improvements:
  - Provide proper detail level and warnings
  - May be ineffective in case of message spoofing
- Deny access to external DNS servers:
  - Could make the attack more difficult
  - May be unsuitable for some Operators
  - If used alone may cause massive connectivity DoS

Future Research

- Future research will focus on:
  - Application Data Hijacking
  - HTTPS traffic snooping
  - Malicious Payload Injection
  - Targeting Mobile Operator internal networks
  - Botnets

Thanks !!!

Mobile Security Lab
research@mseclab.com

Q&A

References

- OMA - Provisioning Architecture Overview v1.1
- OMA - WAP Architecture v12
- OMA - Push Architectural Overview v3
- OMA - Provisioning Content v1.1
- OMA – Provisioning Bootstrap v1.1
- OMA - Binary XML Content Format Specification v1.3
- OMA - Wireless Session Protocol Specification v5
- OMA - OMNA WSP Content Type Numbers
- OMA - Wireless Datagram Protocol Specification v14
- 3GPP - TS 03.40 Technical realization of the Short Message Service (SMS) v7.5.0
- Apache HTTP Server Project
- ModSecurity: Open Source Web Application Firewall