Mobile security in Japan

NetAgent Co. Ltd.
Kenji Aiko

Presentation Outline

1.Mobile market in Japan

1.Smartphone and KEITAI

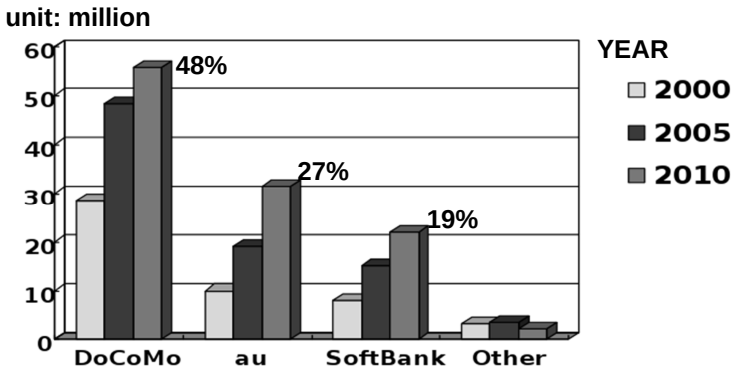
1.Web application security on mobile

1.Attacking mobile network

Mobile phone's share

There are 3 major carriers in Japan

- DoCoMo, au, and SoftBank

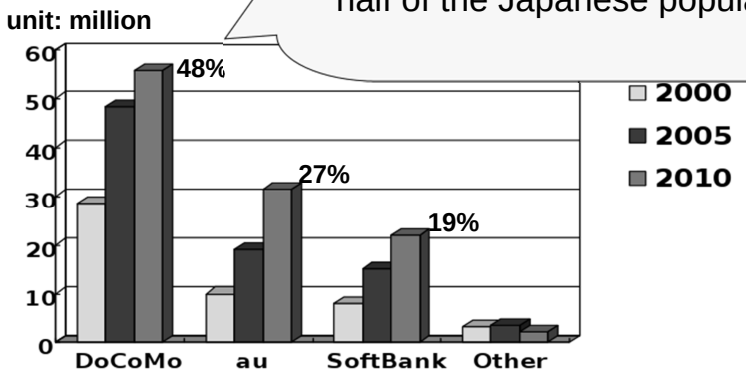


Mobile phone's share

There are 3 majo

- DoCoMo, au, and

"NTT DoCoMo" is a top of mobile market in Japan, they has about 60,000,000 users, it reaches the half of the Japanese population

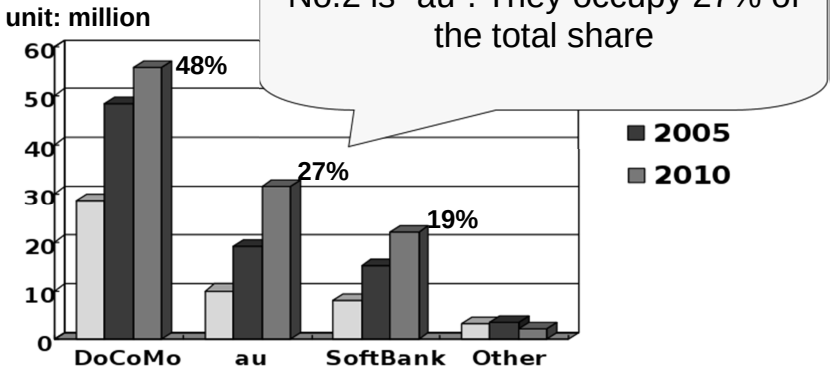


Mobile phone's share

There are 3 major carriers in Japan

- DoCoMo, au, and SoftBank

No.2 is "au". They occupy 27% of the total share

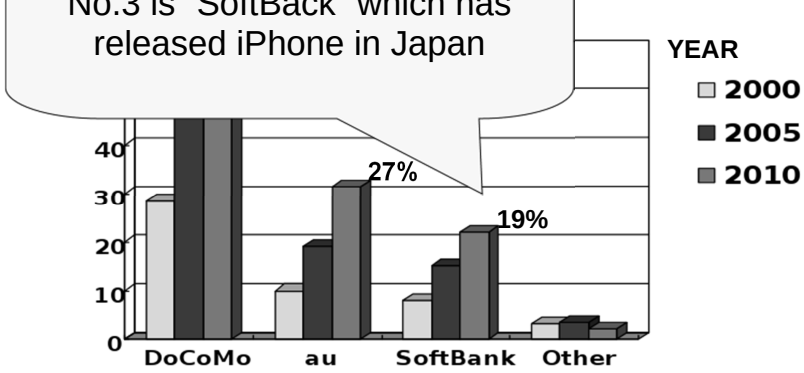


Mobile phone's share

There are 3 major carriers in Japan

- Docomo, au, and SoftBank

No.3 is "SoftBack" which has released iPhone in Japan

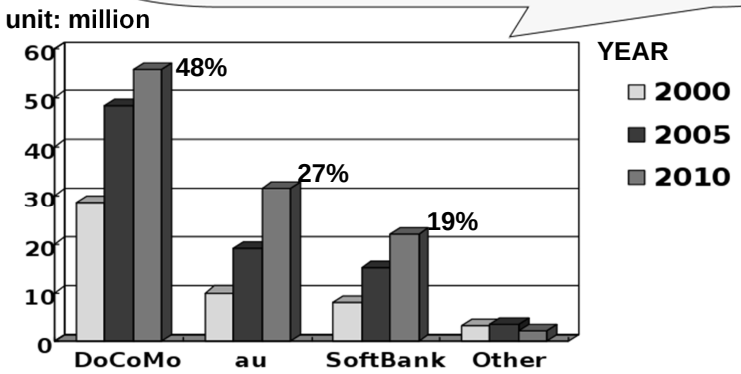


Mobile phone's share

There ar

- DoCom

The number of total mobile users is about 110 millions (It's so big a market)



Carriers provide 2 types of mobile phone

1. Smartphone
   - iPhone, Android, etc…
   - In short, it's general mobile in the world
2. Japan's original mobile phone (KEITAI)
   - The mobile which we call "KEITAI"
   - It accounts for 90% of mobile share in Japan

Carriers provide 2 types of mobile phone

1. Smar
   - Blac
   - In sh
2. Japan's original mobile phones (KEITAI)
   - The mobile which we call "KEITAI"
   - It accounts for 90% of mobile share in Japan

Today, I'll discuss about security of Japan's original mobile phone (KEITAI), because smartphone security of other country is similar

Presentation Outline

1. Mobile market in Japan
1. Smartphone and KEITAI
1. Web application security on mobile
1. Attacking mobile network

Difference between Smartphone and KEITAI

There are a little bit difference between Smartphone and KEITAI

It's the Individual Identification Number

Individual Identification Number

- KEITAI has unique number
  - It's like product number
  - Server uses it to recognize each user
- It is added in the HTTP header by Gateway when you connecting to HTTP server on KEITAI

How does the server get it?

The Gateway include “Individual Identification Number” into USER_AGENT

How does the server get it?

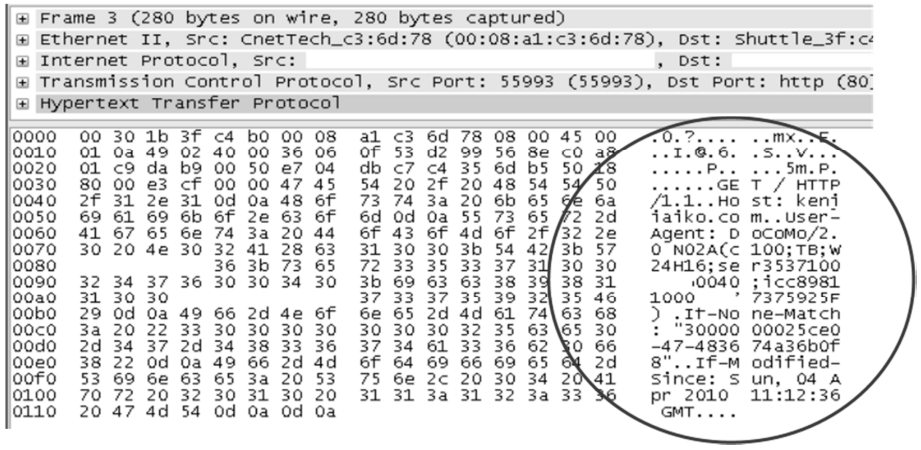
The Gateway include “Individual Identification Number” into USER_AGENT


```
⊞ Frame 3 (280 bytes on wire, 280 bytes captured)
⊞ Ethernet II, Src: CnetTech_c3:6d:78 (00:08:a1:c3:6d:78), Dst: Shuttle_3f:c
⊞ Internet Protocol, Src:                                  , Dst:
⊞ Transmission Control Protocol, Src Port: 55993 (55993), Dst Port: http (80
⊞ Hypertext Transfer Protocol

0000  00 30 1b 3f c4 b0 00 08  a1 c3 6d 78 08 00 45 00   .0.?.... ..mx..E.
0010  01 0a 49 02 40 00 36 06  0f 53 d2 99 56 8e c0 a8   ..I.@.6. .S..V...
0020  01 c9 da b9 00 50 e7 04  db c7 c4 35 6d b5 50 18   .....P.. ...5m.P.
0030  80 00 e3 cf 00 00 47 45  54 20 2f 20 48 54 54 50   ......GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 6b 65 6e 6a   /1.1..Ho st: kenj
0050  69 61 69 6b 6f 2e 63 6f  6d 0d 0a 55 73 65 72 2d   iaiko.co m..User-
0060  41 67 65 6e 74 3a 20 44  6f 43 6f 4d 6f 2f 32 2e   Agent: D oCoMo/2.
0070  30 20 4e 30 32 41 28 63  31 30 30 3b 54 42 3b 57   0 N02A(c 100;TB;W
0080                 36 3b 73  65 72 33 35 33 37 31 30 30   24H16;se r3537100
0090  32 34 37 36 30 30 34 30  3b 69 63 63 38 39 38 31       0040 ;icc8981
00a0  31 30 30                 37 33 37 35 39 32 35 46   1000    ' 7375925F
00b0  29 0d 0a 49 66 2d 4e 6f  6e 65 2d 4d 61 74 63 68   ) .If-No ne-Match
00c0  3a 20 22 33 30 30 30 30  30 30 30 32 35 63 65 30   : "30000 00025ce0
00d0  2d 34 37 2d 34 38 33 36  37 34 61 33 36 62 30 66   -47-4836 74a36b0f
00e0  38 22 0d 0a 49 66 2d 4d  6f 64 69 66 69 65 64 2d   8"..If-M odified-
00f0  53 69 6e 63 65 3a 20 53  75 6e 2c 20 30 34 20 41   Since: S un, 04 A
0100  70 72 20 32 30 31 30 20  31 31 3a 31 32 3a 33 36   pr 2010  11:12:36
0110  20 47 4d 54 0d 0a 0d 0a                            GMT....
```

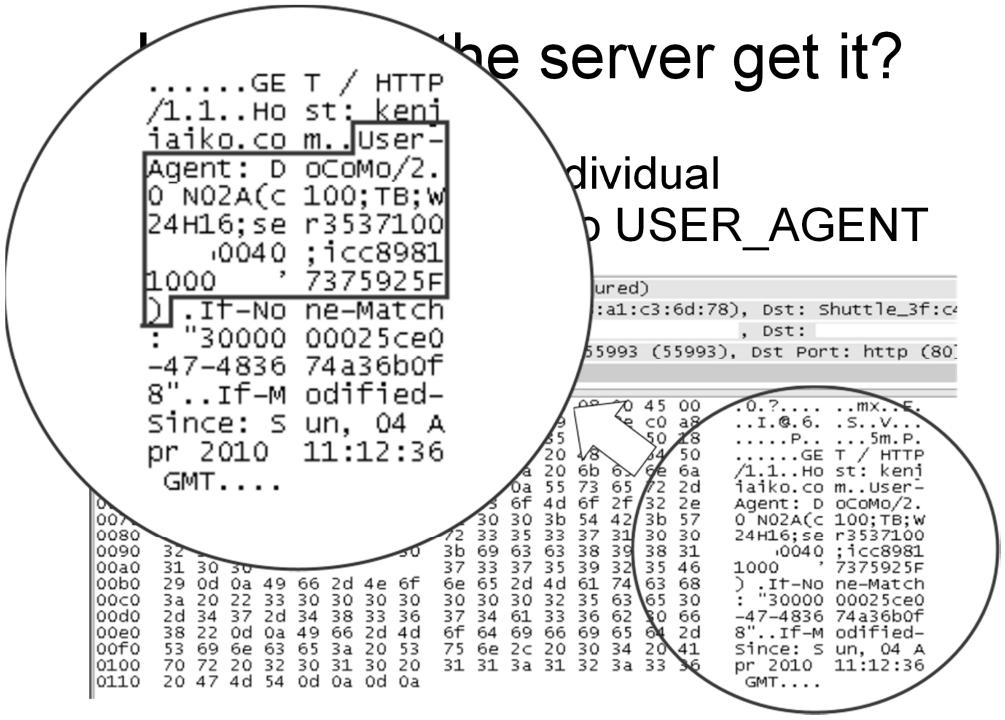

How does the server get it?

The Gateway include “Individual Identification Number” into USER_AGENT

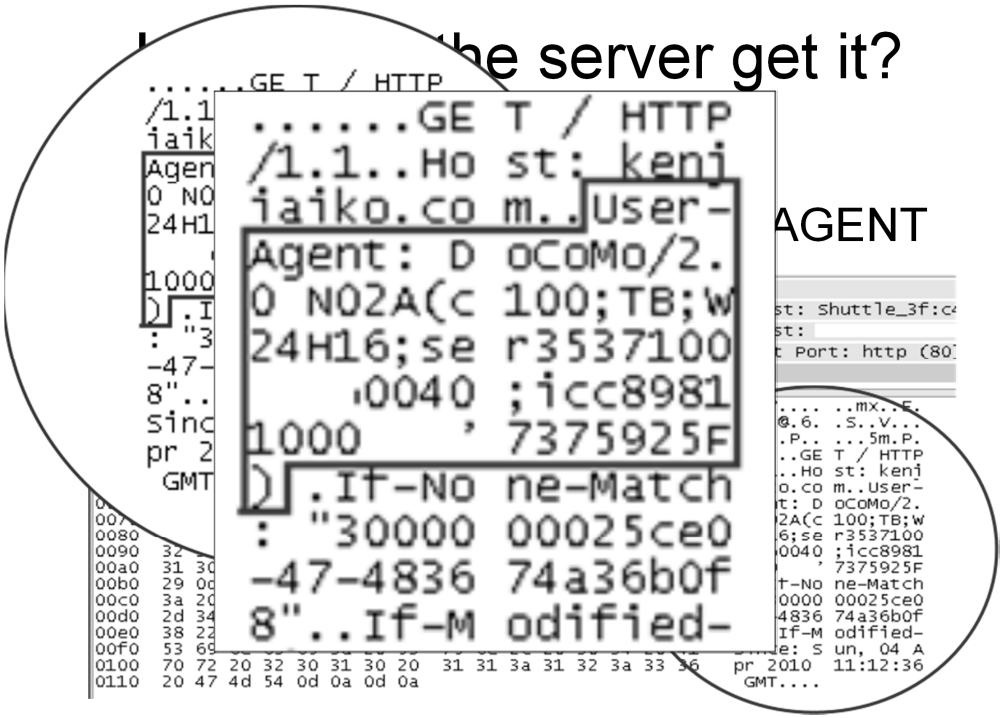


How does the server get it?

The Gateway include “Individual Identification Number” into USER_AGENT



he server get it?



AGENT

Why do you need it?

1. Carriers want to control the network to use the identification information of users in Gateway

1. Almost all of KEITAI don't have "Cookie" technology, so they use it like "Cookie"

Why do you need it?

1. Carriers want to control the network to use the identification information of users in Gateway

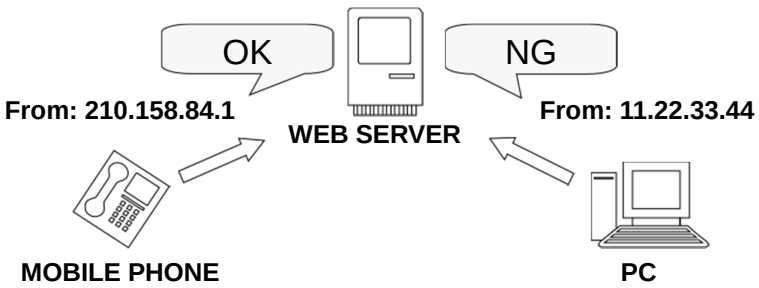
1. Almost all of K
technology, so

However, you are able to more easily change the HTTP request header from PC

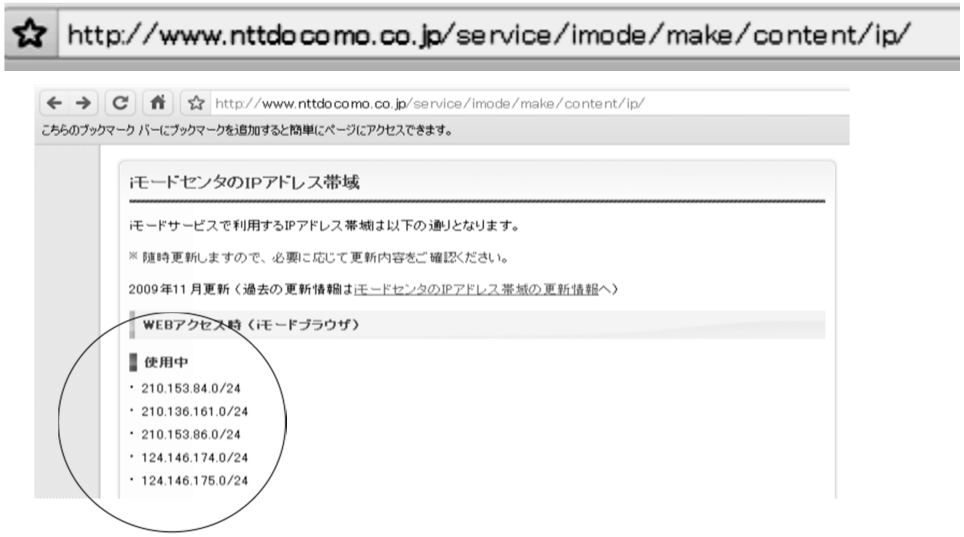
How to block access from PC?

Using IP address

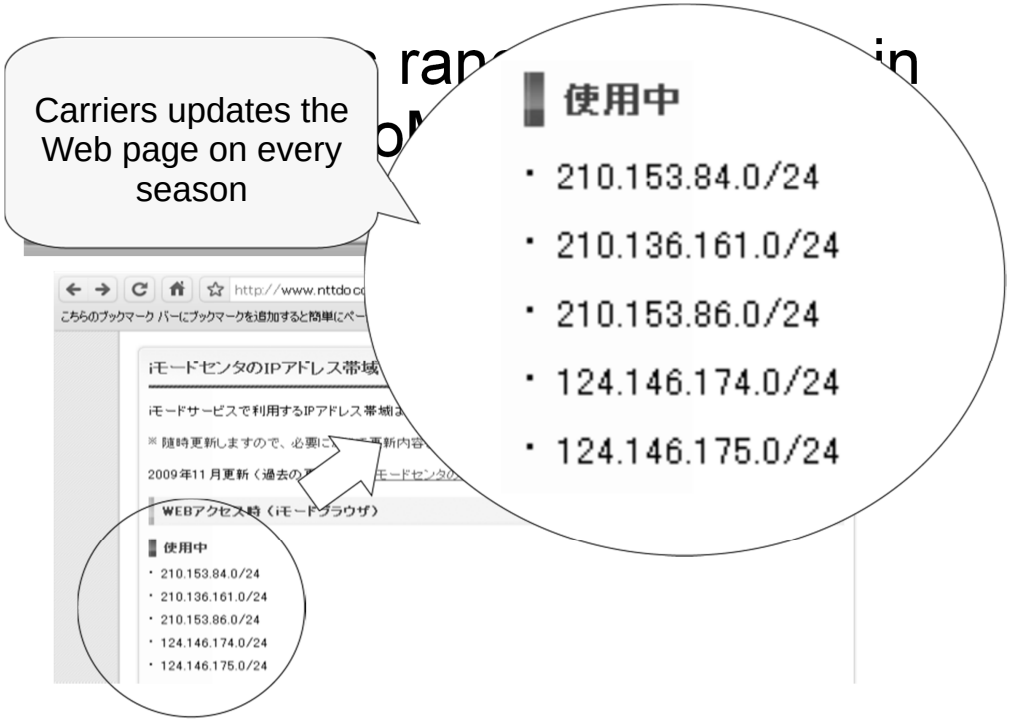
- Carriers are announcing the IP address range to use for accessing from KEITAI for Web application engineers on every season



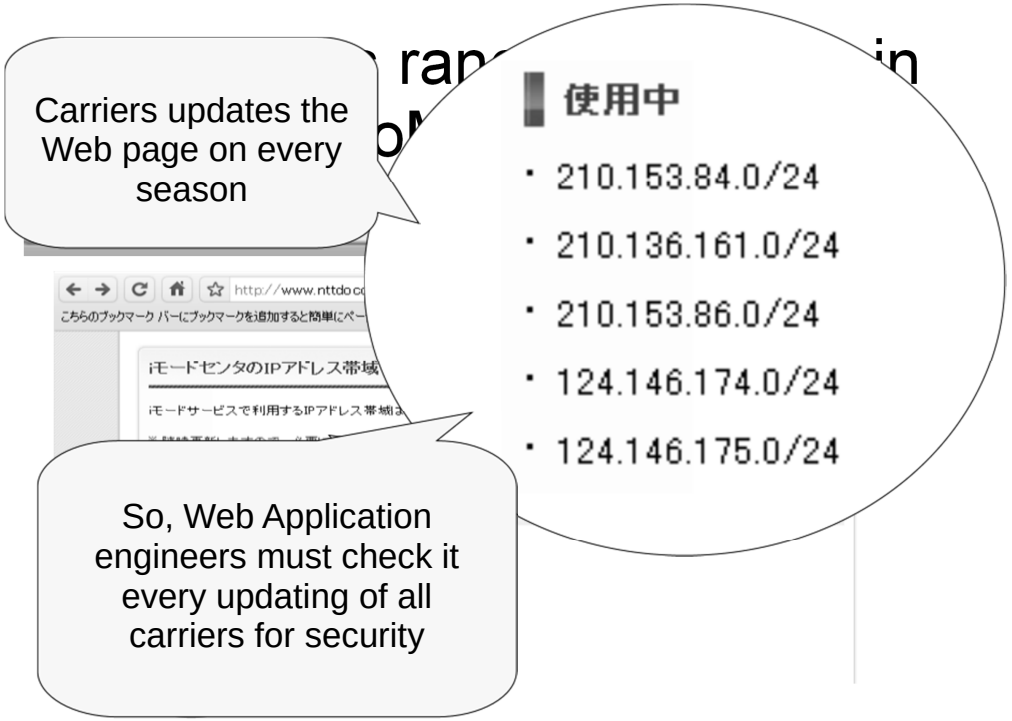
IP address range for mobile in DoCoMo Web site



Carriers updates the Web page on every season



Carriers updates the Web page on every season



So, Web Application engineers must check it every updating of all carriers for security

Presentation Outline

1.Mobile market in Japan

1.Smartphone and KEITAI

1.Web application security on mobile

1.Attacking mobile network

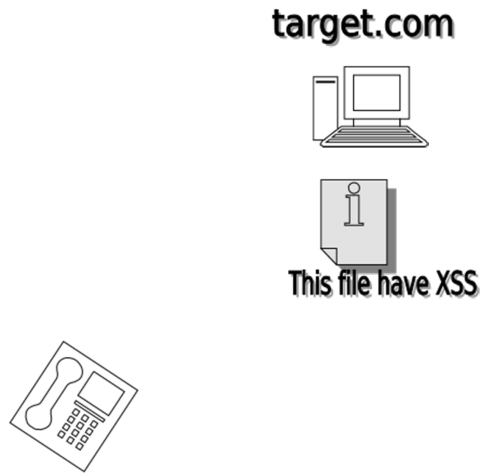
Web application security on mobile

In July 2009, DoCoMo released new KEITAI which has JavaScript-Engine

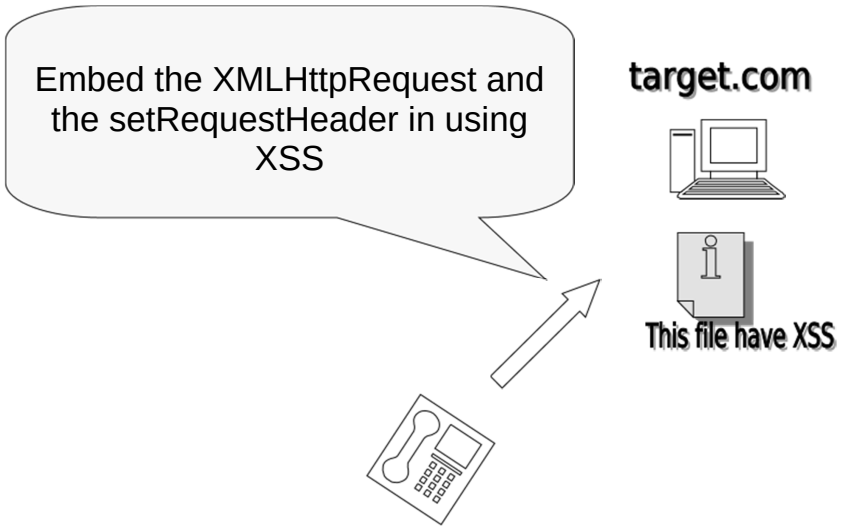
However, the JavaScript-Engine had 2 security issues

1. XSS + setRequestHeader

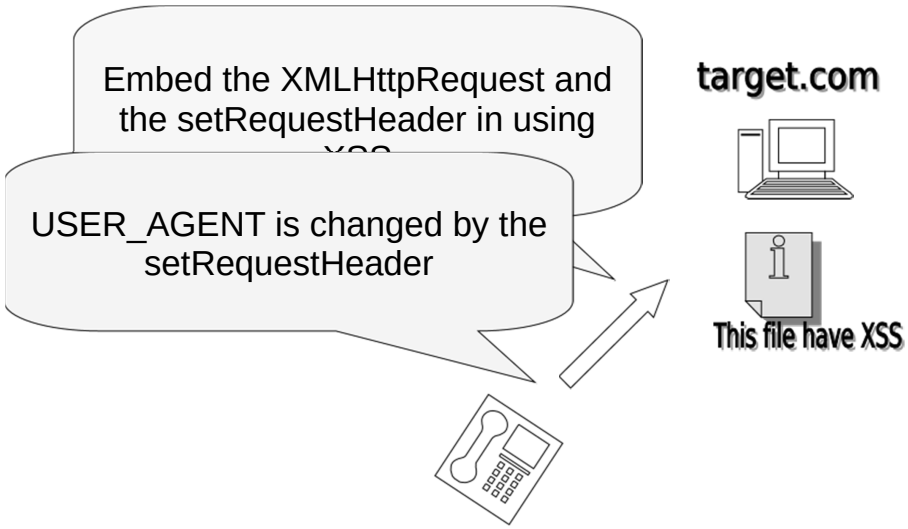
Attack process



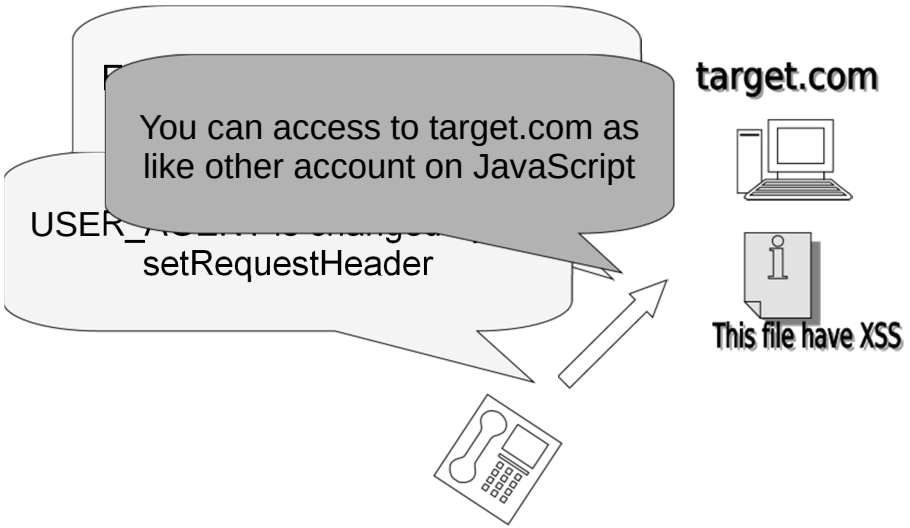
Attack process



Attack process



Attack process

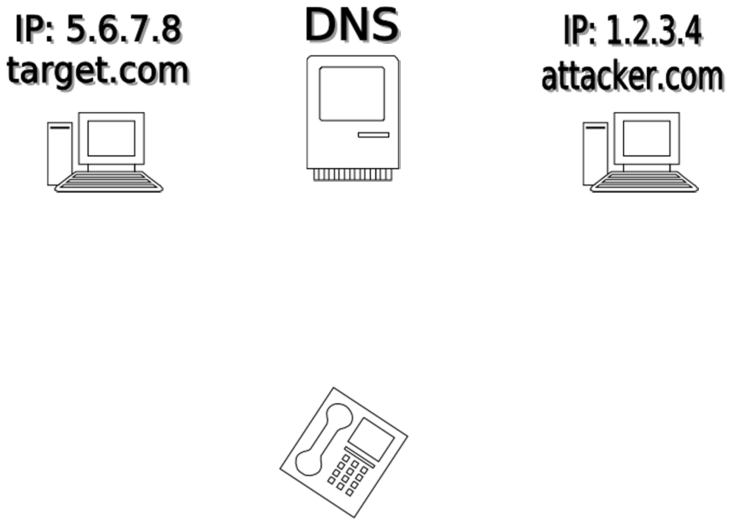


Critical damage by XSS only

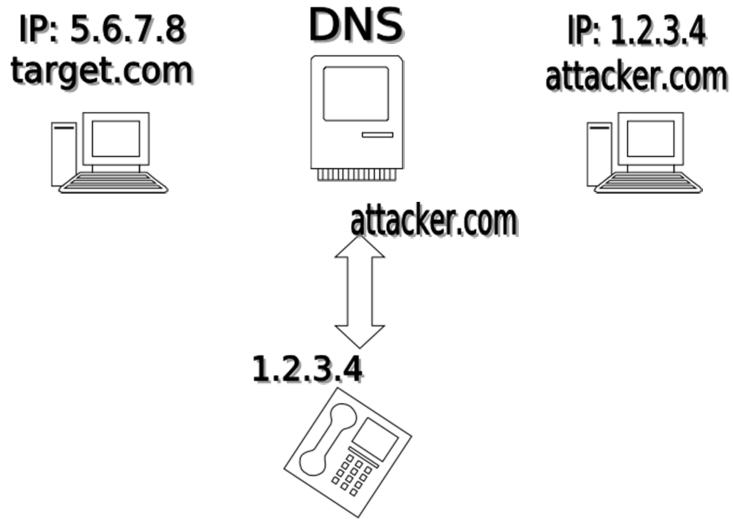
- This is quite simple a vulnerability, but DoCoMo couldn't notice before released the last "KEITAI" in July, 2009
- Researcher(Hiroshi Tokumaru) published it in August, 2009
  - DoCoMo corrected the part of function on JavaScript (setRequestHeader, etc…) in November, 2009

2. DNS Rebinding

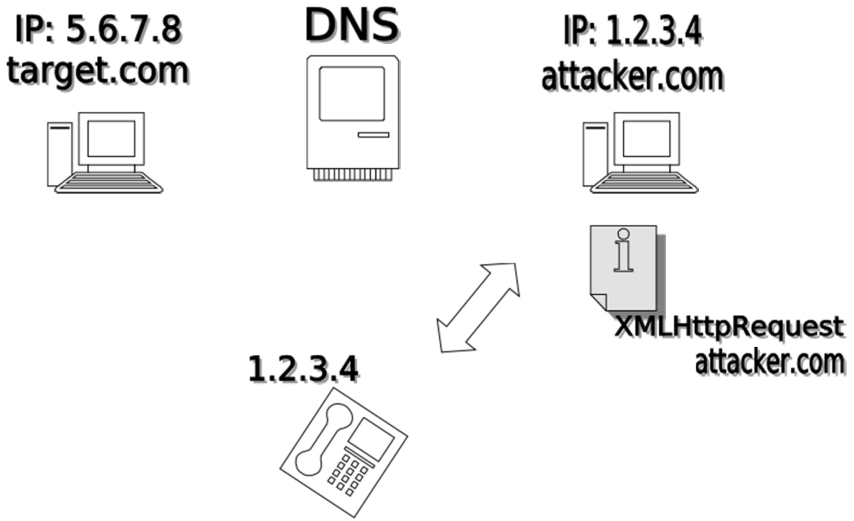
Attack process



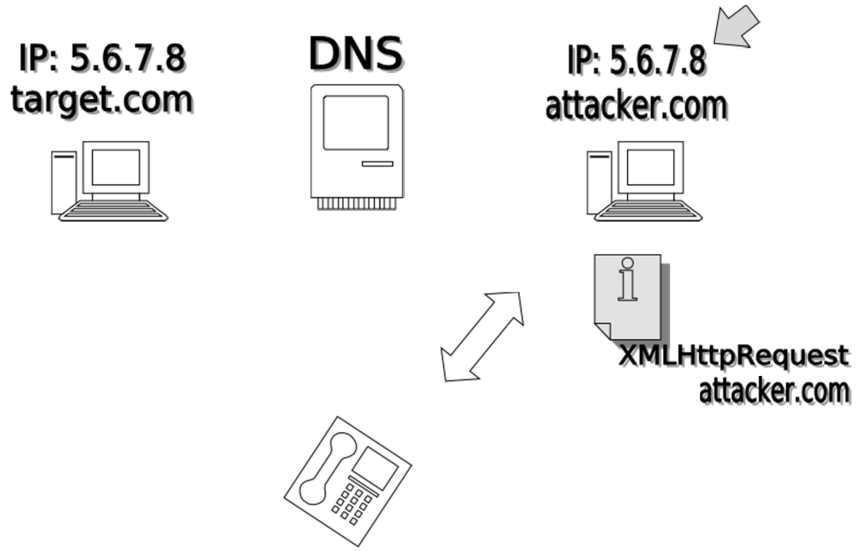
Attack process



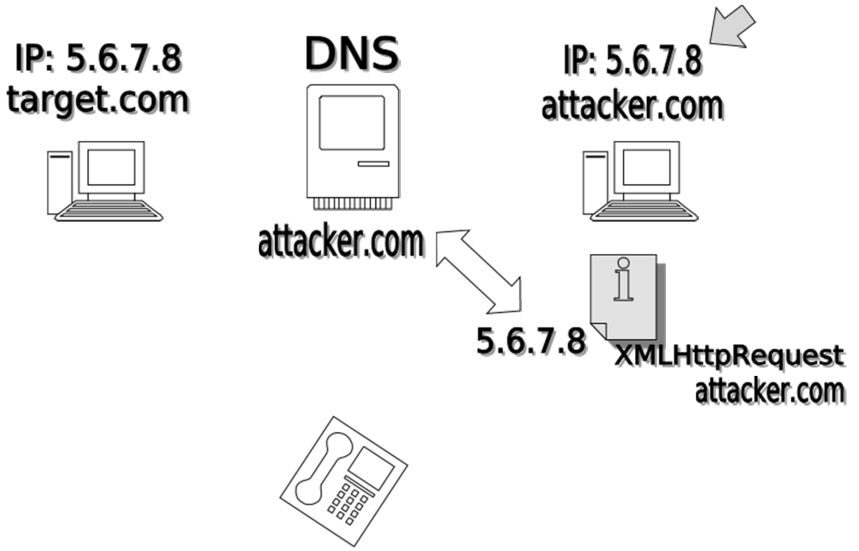
Attack process



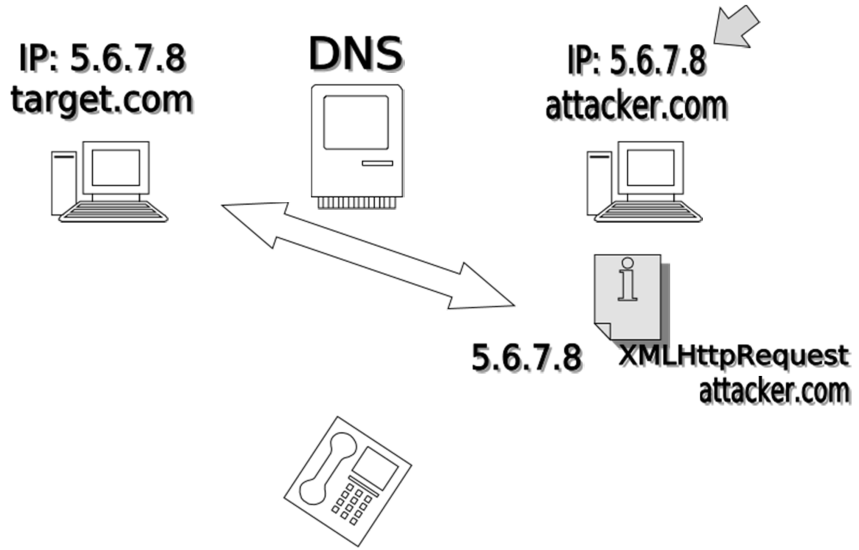
Attack process



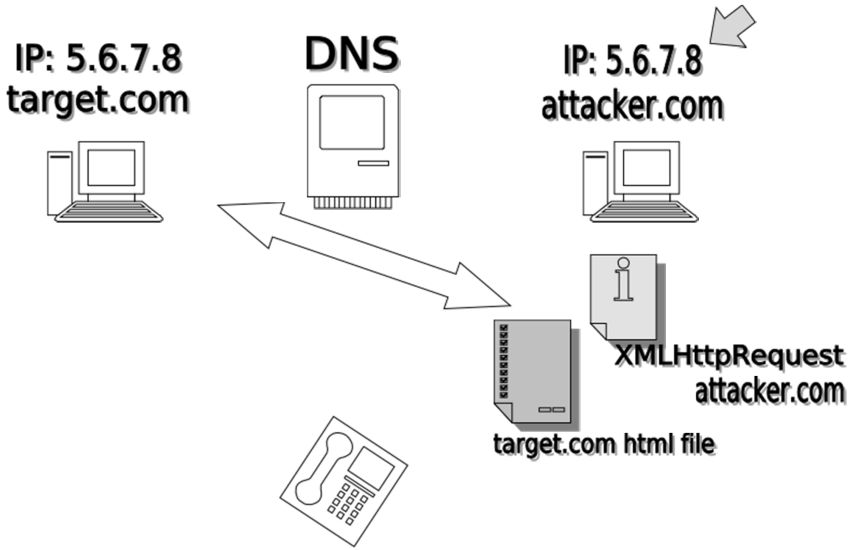
Attack process



Attack process



Attack process



Unsecure DNS

- Attacker can pass same-origin-policy of JavaScript for using DNS Rebinding on KEITAI
- The Mobile phone network in Japan don't cache DNS packets (I don't know why…)
- Carriers haven't corrected it yet

Presentation Outline

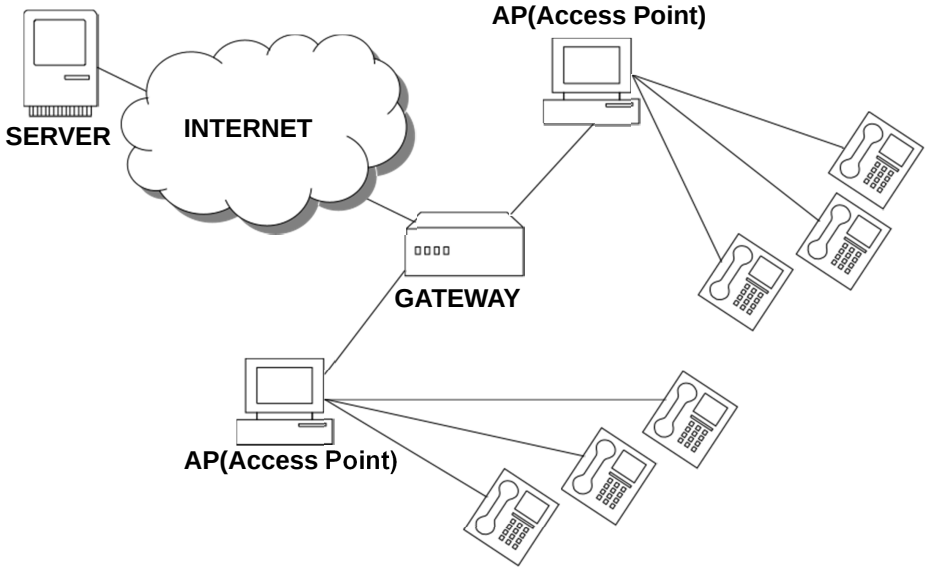
1.Mobile market in Japan

1.Different between smart phone and

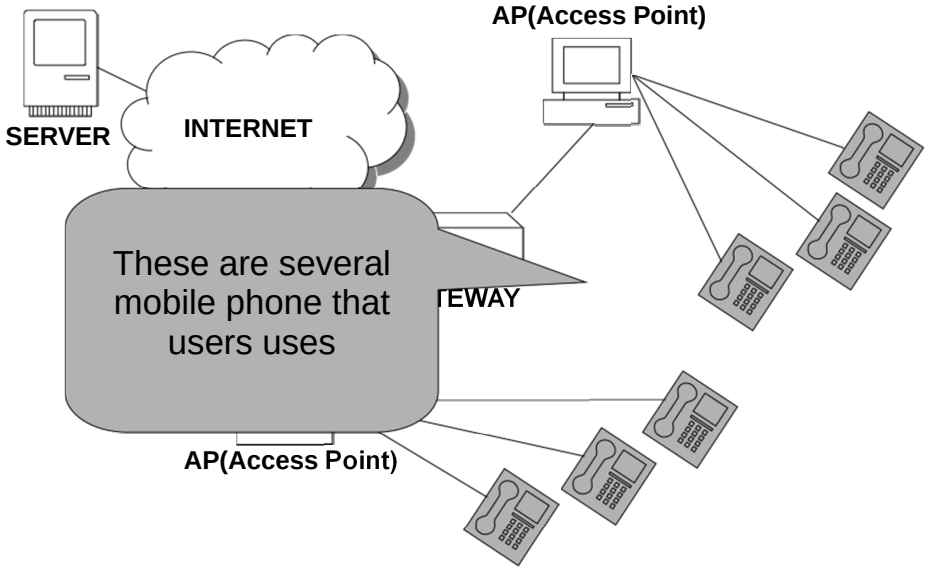
1.Web application security on mobile

1.Attacking mobile network

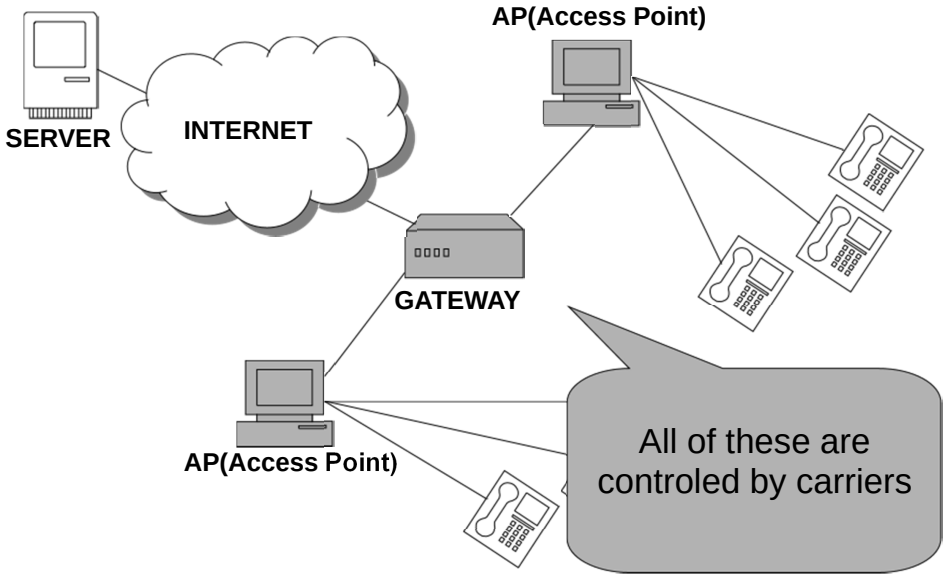
Mobile Network



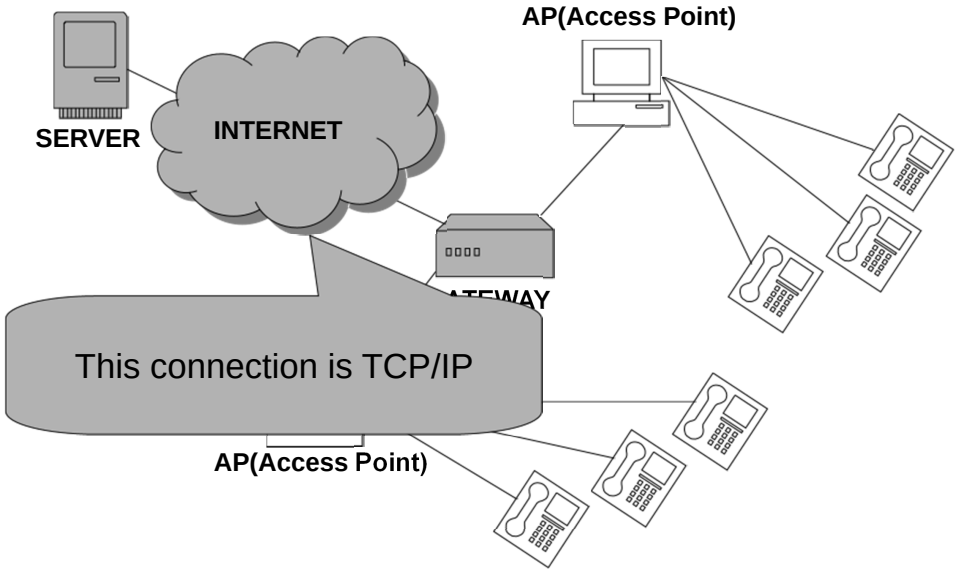
Mobile Network



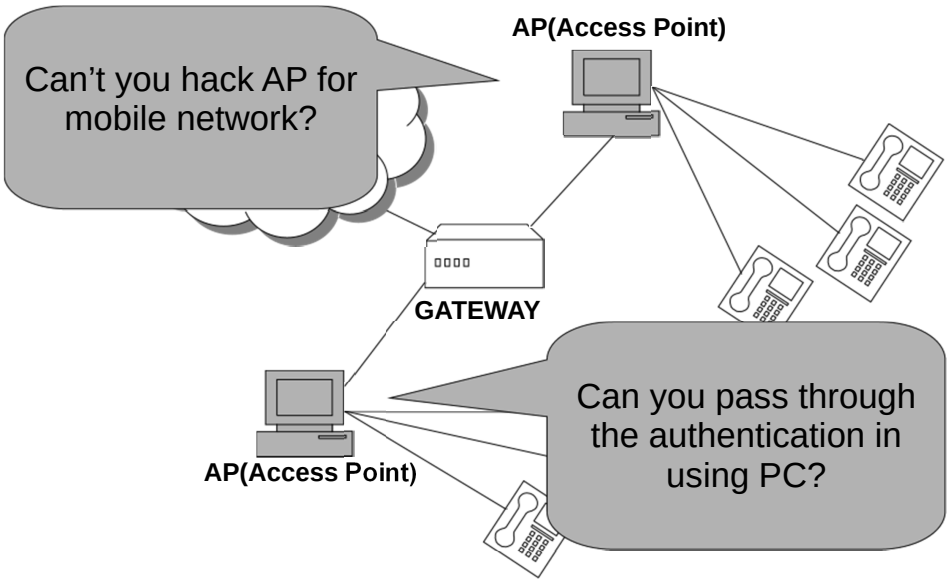
Mobile Network



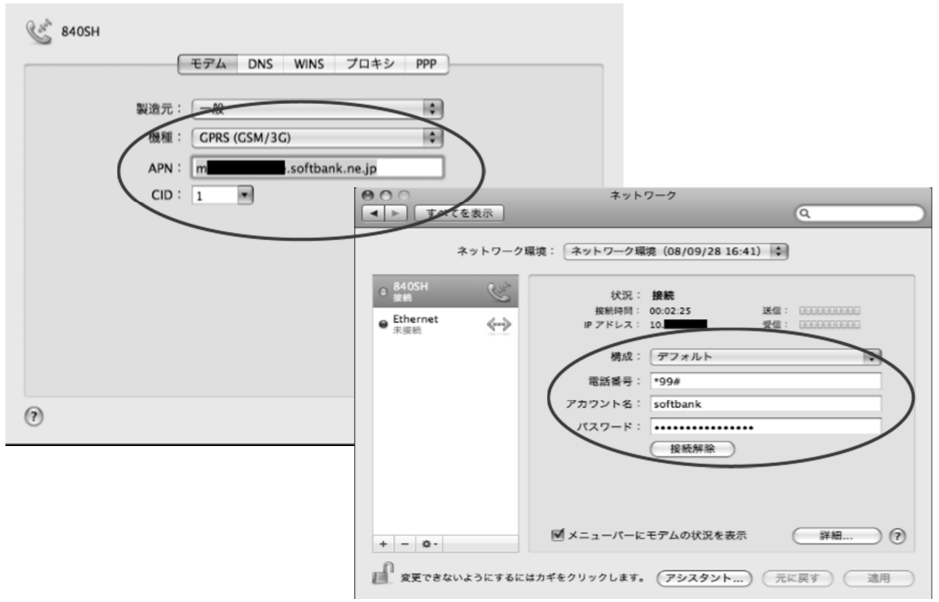
Mobile Network



Mobile Network



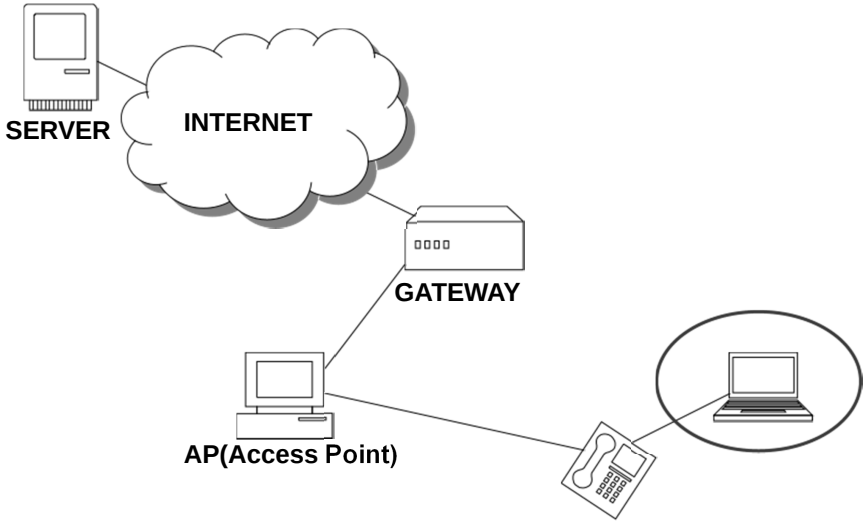
Set information for APN



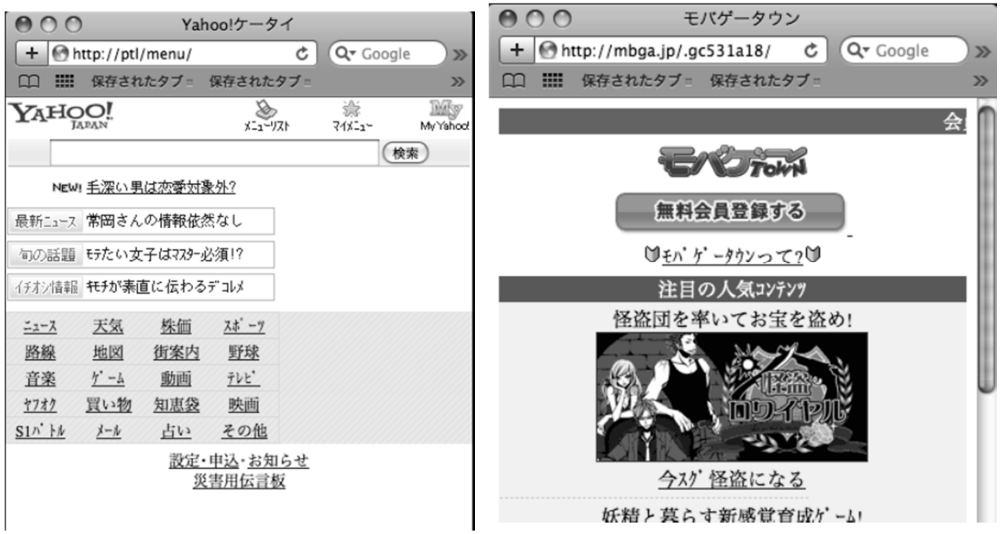
Connect with KEITAI

A KEITAI is set for Internet-Tethering

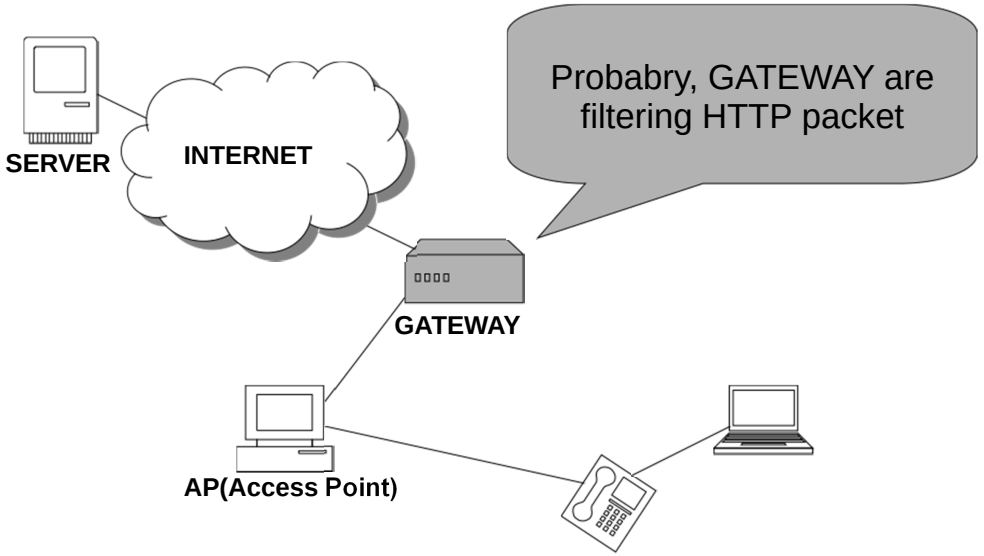
Mobile Network



Access mobile site from PC



Mobile Network



Conclusions

- Is the mobile world safety or not?
  - Though it’s safer than PC, but it isn’t sufficient
- Is it safer more than PC forever?
  - I don’t think so, mobile becomes unsafe if it gets many functionalities like PC

Any Questions?