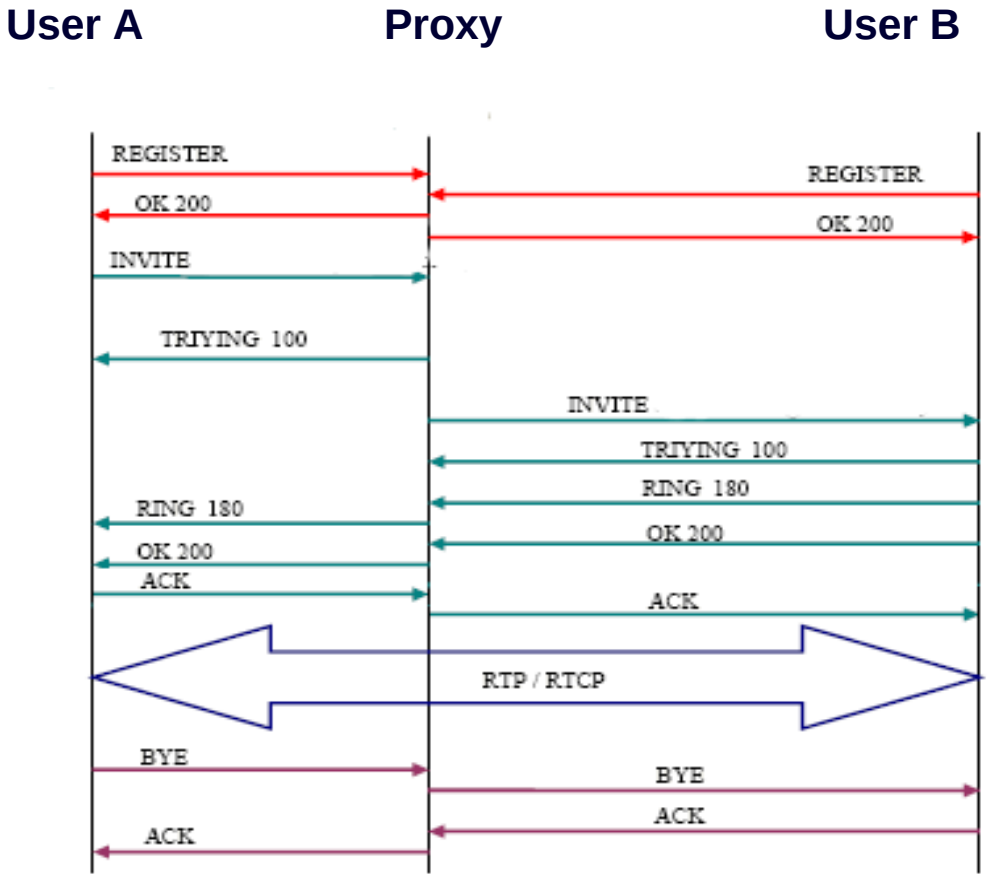
VoIP Attack
2008.11.05

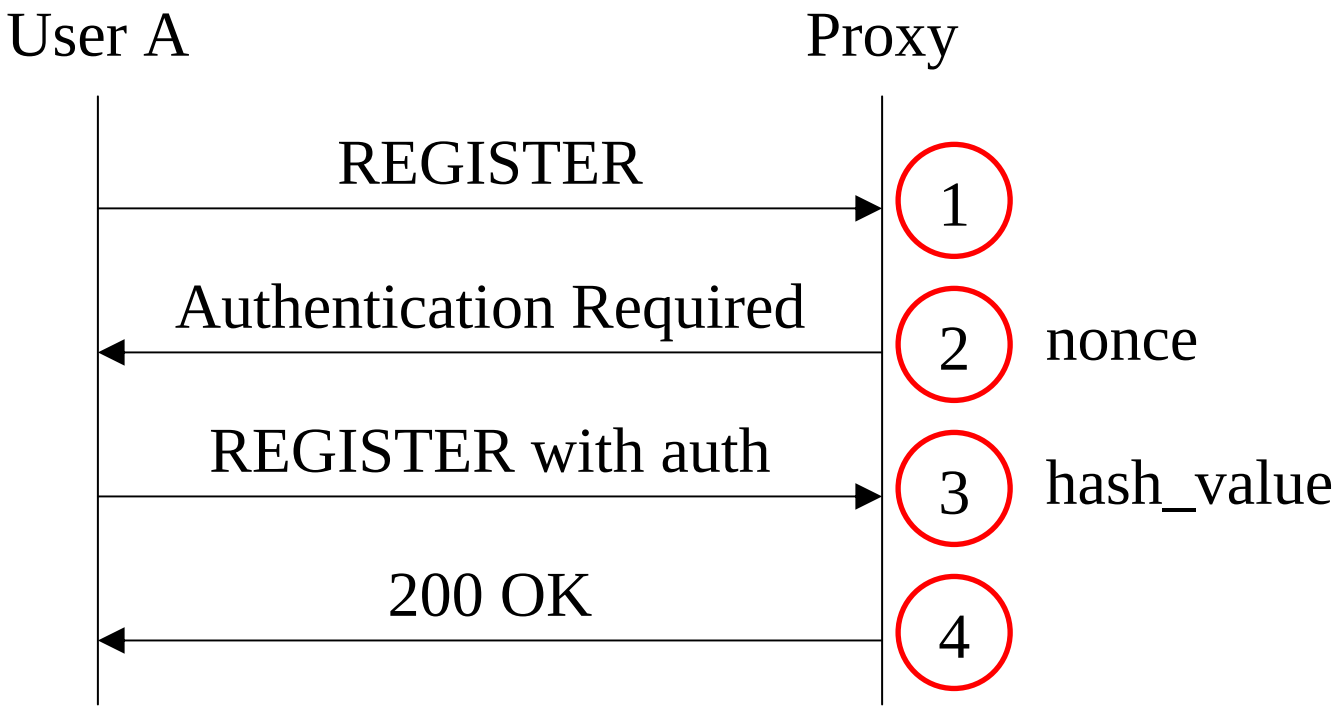
http://www.netlab.co.kr

SIP Flow Chart



http://www.en.voipforo.com/SIP/SIP_example.php

SIP Authentication Register



hash_value = hash_function(username, password, nonce, …);

Nonce value from Proxy to user always changes whenever it is passed through network to protect from MITM attack, so it is hard for attacker to guess password from hash value.

SIP Register Flow Chart

REGISTER sip:service.com SIP/2.0

Via: SIP/2.0/UDP 192.168.123.157:5060;branch=z9hG4bK782861688

From: "07012345678" <sip:77012345678@service.com>;tag=1548311646

To: " 07012345678 " <sip: 77012345678@service.com >

Proxy-Require: com.appliance_provider.firewall

Call-ID: 9999117224@192.168.123.157

CSeq: 2 REGISTER

Contact: <sip:7012345678@192.168.123.157:61291;maddr=125.111.222.223>;expires=3600

Proxy-Authorization: Digest username="7012345678", realm="Realm",
nonce="MTIyNTgyMjM4MjY1OTZjMzI4NTU3N2RlMGY5YTIyMGYwZWFmYWRlMDdlZjAw",
uri="sip:service.com", response="**8ce5e1e9c121baxxxxdf536d50b76347**", algorithm=MD5,
cnonce="234abcc436e2667097e7fe6eia53e8dd", qop=auth, nc=00000001

…

Is attacker able to guess password from hash value(shown in **response** field)?

Guessing password using brute-force attack

Attacker can get information userame and hash value from packet capturing, but it is not easy for him to infer password from hash value directly. So attacker would like to use **brute-force attack method**.

hash(“7012345678”, …, “0000”) = response?

hash(“7012345678”, …, “0001”) = response?

hash(“7012345678”, …, “0002”) = response?

hash(“7012345678”, …, “0003”) = response?

…

http://www.google.com/search?q=sipcrack

http://www.codito.de

How to protect from brute-force attack

If you can not avoid attack,

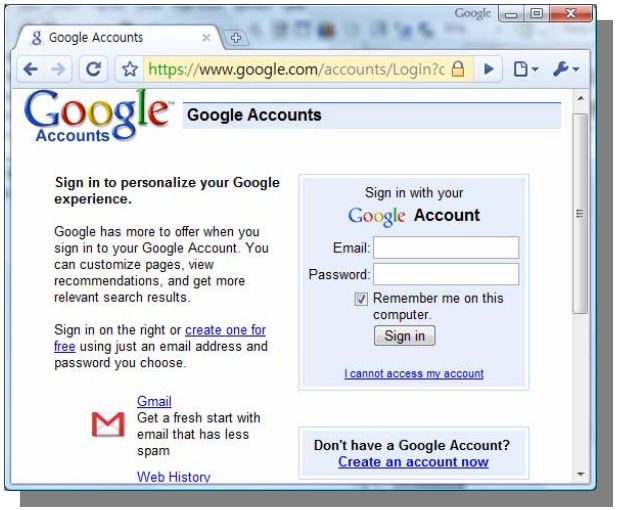
long password can be good enough!!!

1 number : only 1 second.

8 number : 10^8 seconds.

N alnum character : about (10 + 26 + 26) ^N seconds.

SIP Auto Provision



User inputs username and password directly to use the web service.

Have you ever inputted SIP account information whenever you would like to use VoIP phone service?

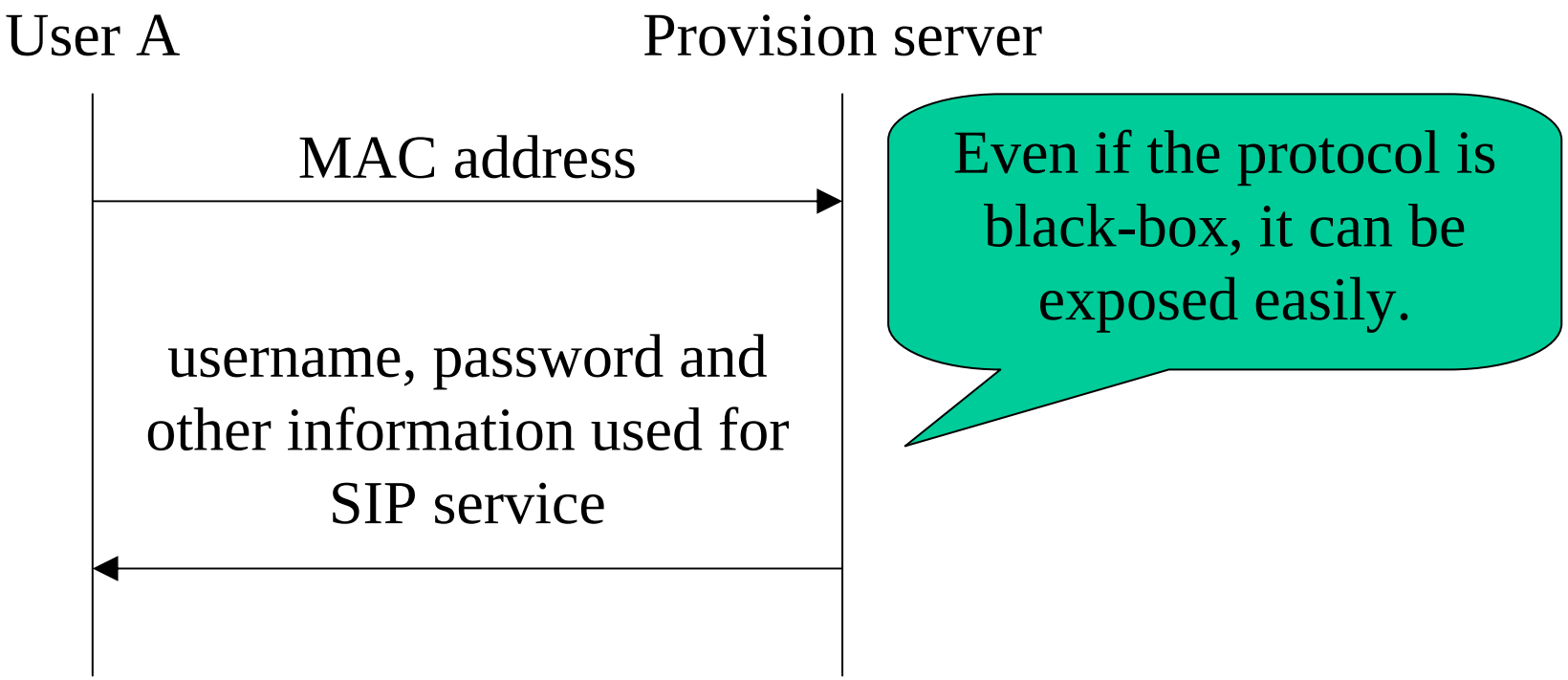
Image from : http://www.ctintegrators.com/cti/telephones.htm

Is auto provision safe or not?

Auto provision service is convenient.

But IS IT SAFE?

Sample of SIP auto provision



Auto provision can be dangerous, and moreover it is difficult for service provider to change auto provisioning algorithm unless hardware firmware is upgraded.

Some problems of Korean SIP service

Standard cipher algorithm for VoIP(SIP over TLS, SRTP and so on) is not widely-used yet.

User does not know his own SIP account.

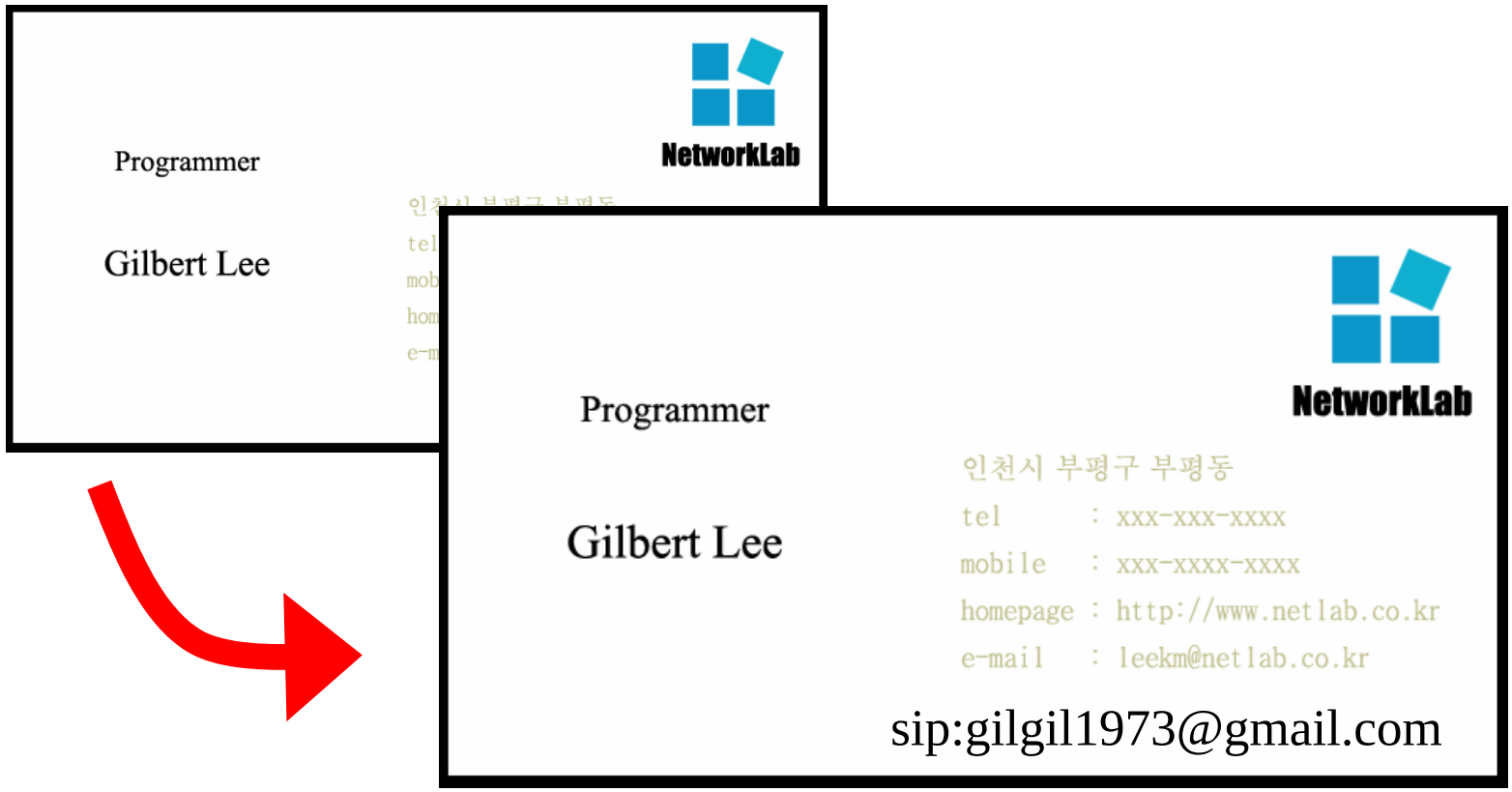
User can not change his password.

He can not help using device exclusively.

Passwords of the specific SSID devices are all the same. Hidden SSID and its password are fixed and can not be changed. It can be dangerous because they are all the same.. What happens if it is exposed?

SIP terminal, Access point device, SIP service and internet service are different.

What is SIP?



SIP comes from not telephone but internet.

All IP age will come true sometime.

Thank you

author : gilgil

homepage : http://www.gilgil.net

email : gilgil1973 at gmail.com

messenger : gilgil1973 at gmail.com