SnoopSpy 2 for POC2007

2007.11.10

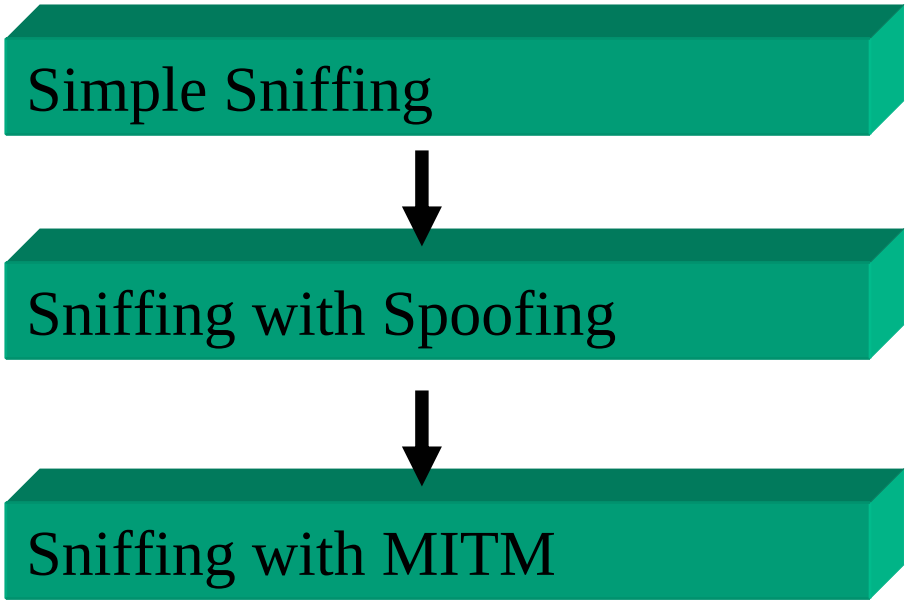
http://www.snoopspy.com

Overview

This document explains the MITM (Man In The Middle) attack concept, and analyzes sniffing-related cipher code examples.

Evolving of sniffing attacks

Packet sniffing attacks have been developed in connection with various techniques for a long time.



Promiscuous mode, TCP/IP and so on

ARP spoofing, IP spoofing and so on

Proxy, Version rollback and so on

Can I decrypt enciphered code?

Do you want to sniff?

Sniffing often requires not only high level technical skills but also original ideas.

How can I analyze this encrypted code?

MITM for SSL - What is SSL?

SSL (Secure Sockets Layer) is a protocol developed by Netscape for transmitting private documents via Internet.

from : http://www.webopedia.com/TERM/S/SSL.html

cf : http://www.ietf.org/rfc/rfc2246.txt?number=2246

MITM for SSL - What is Secure Server?

A Web server that supports any of the major security protocols, like SSL, that encrypt and decrypt messages to protect them against third party tampering.

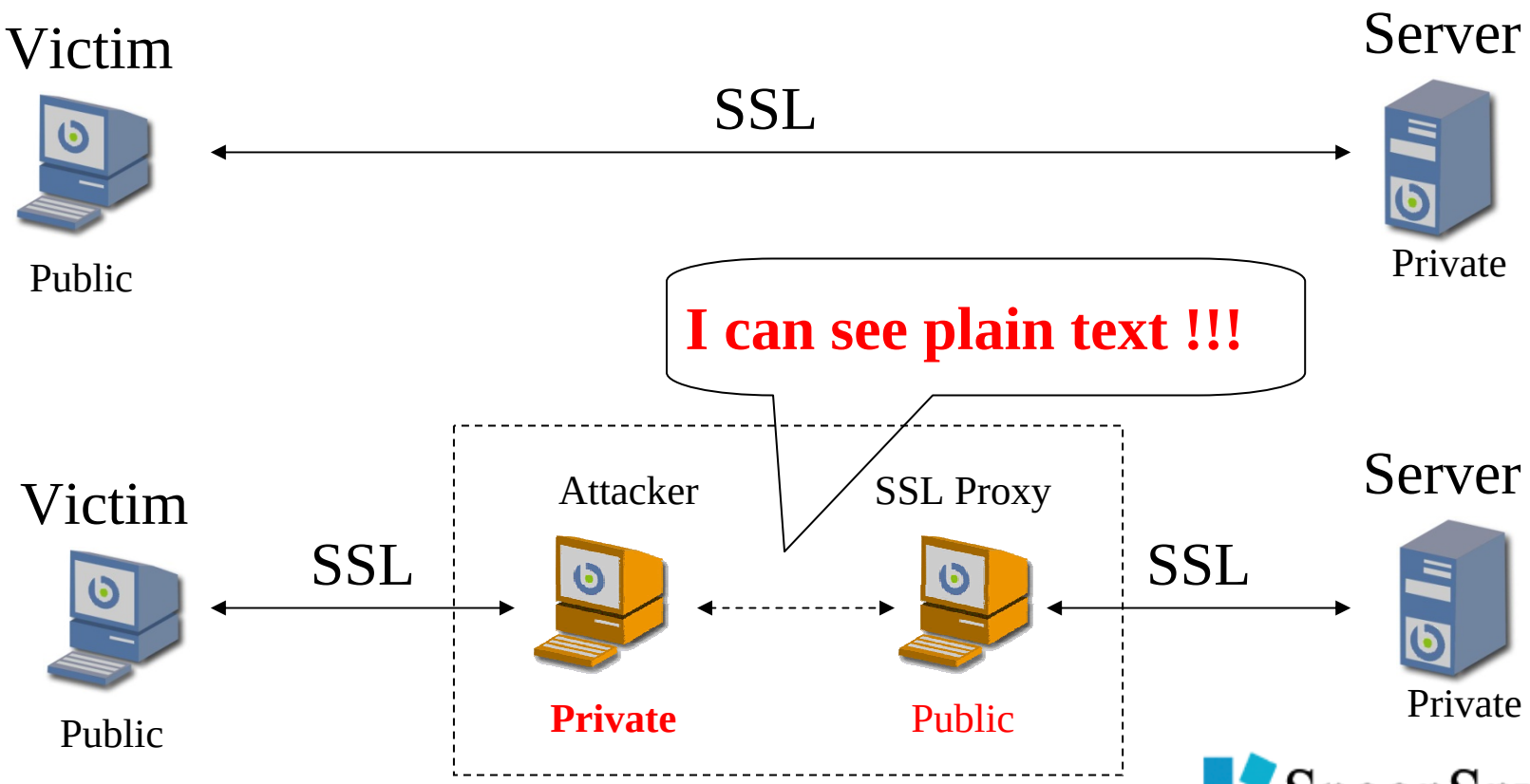
from : http://www.webopedia.com/TERM/S/secure_server.html

MITM for SSL - What is SSL MITM attack?

The attacker must be positioned between the victim and the server.

The attacker intercepts packets and routes them to the SSL Proxy.

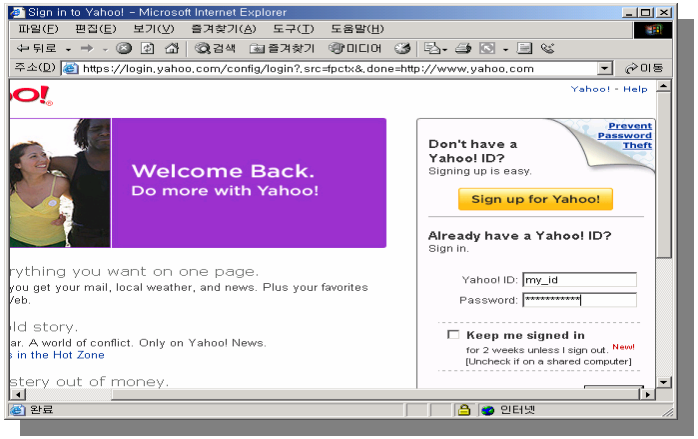
The SSL Proxy changes the SSL key value in order to get the decrypted information.



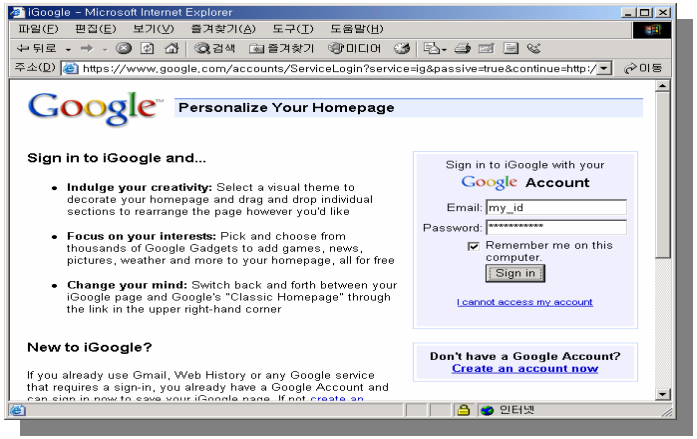
MITM for SSL - Examples

Is SSL communication safe or not? What do you think?

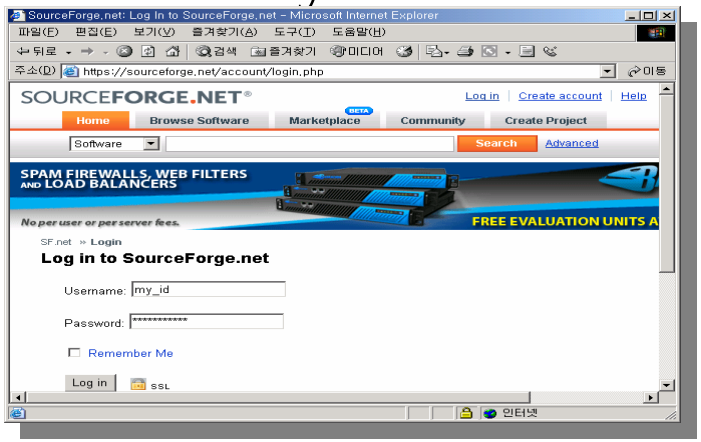
Portal



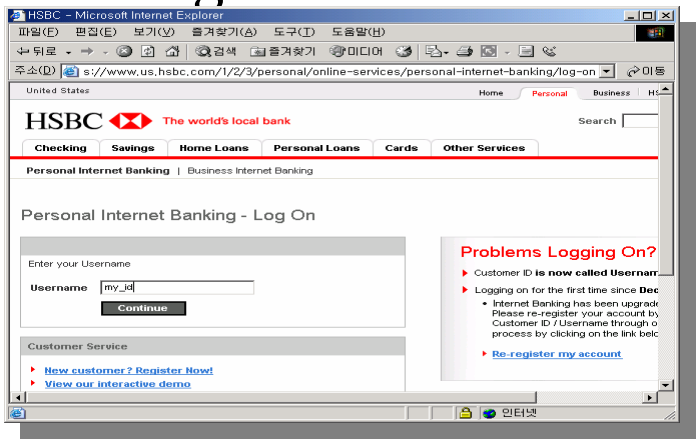
Mail



Community



Banking



SnoopSpy

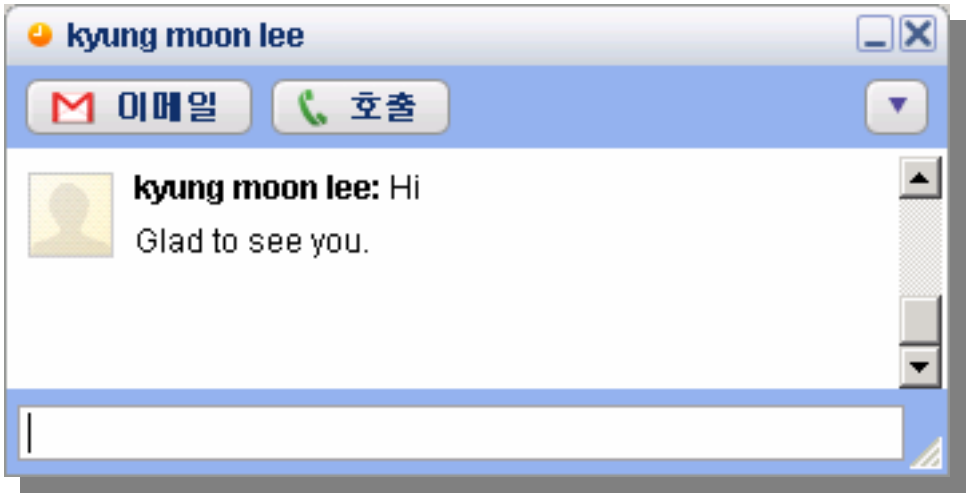
MITM for SSL – Just for fun

Change packet from “https://” to “http://” . ☺

MITM for Messenger – Plain Text Messages

Nothing to talk about!!!

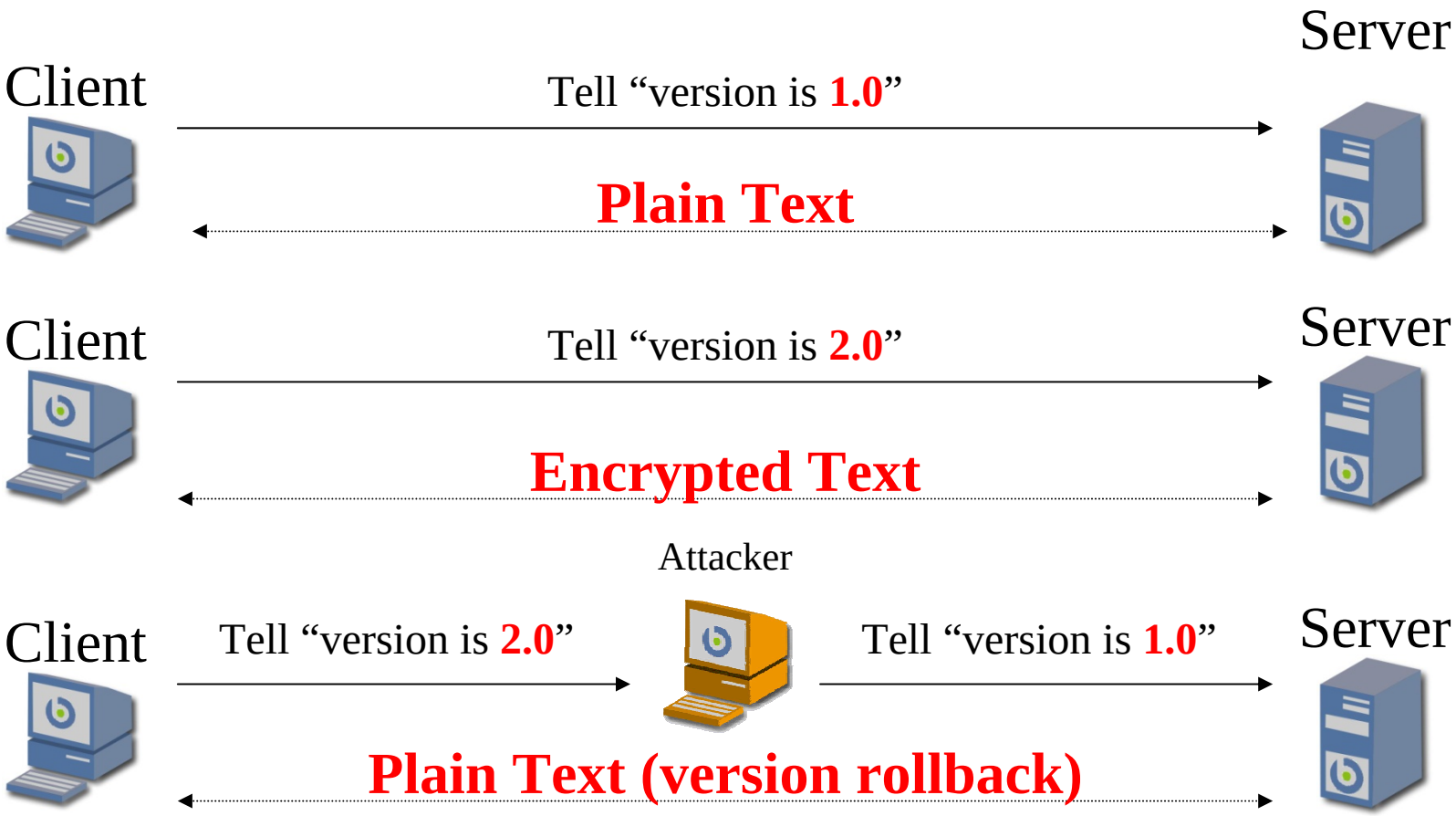
What you need to know is just XML, ASCII, UTF, Base64 and so on.




```
<message to="gilgil1973@gmail.com/Talk.v9322223B16" type="chat" id="40"
from="gilgil1975@gmail.com/Talk.v93C2DF76C2"><body>Glad to see you</body><active
xmlns="http://jabber.org/protocol/chatstates"/><nos:x value="disabled" xmlns:nos="google:nosave"/><arc:record
otr="false" xmlns:arc="http://jabber.org/protocol/archive"/></message>
```

MITM for Messenger – Encrypted Messages

There are many messengers that support encrypted chatting for security. So, what should I do if I want to see the full details of a conversation?



MITM for VoIP

RTP voice sessions between two VoIP terminals can be exposed and be modified.

MITM for FPS

Would an MITM attack also be possible for online games like FPS (First Person Shooter)? How can I beat other users in the game? Generally, packets about players' positions are transferred through UDP, not TCP.

What would happen if the data packet (UDP) containing my position was delayed in transmission to other users?

Conclusion

Hackers attack what is worth attacking.

Is your web site or service being attacked?

Don’t get angry. It means your service is worth attacking.

Why don’t you think about what you should do for security, and try to hear hackers’ voices?

Thank you

Author	gilgil
Email	gilgil1973@gmail.com
Home	http://www.gilgil.net
	http://www.gilgil.co.kr
	http://www.snoopspy.com