End Points Malfeasance

Aditya K Sood
Handle : zeroknock
http://zeroknock.metaeye.org

[End Point Malfeasance]

Abstract

This article shows the advancement in the flaw that occur in the end point technology ie client/server transactions.In this the emphasis laid on the HTTP/HTTPS for undertaking rogue issues which become the further base of attacking on the network or protocol infeasibility. The issue discussed are of much importance when ever network problems are concerned.

We will discuss the core of end points directly.The issues will undertaken inadvertently.

Premature Truncation Of Connection:

This is quiet an interesting problem occur in the end point communication.The end point communication here refers to the client server architecture.The premature truncation relates the unauthorised closing of the connection by the client even the closing alert has not been recieved by the server.This sets the connection in immature state because no final alert checks for closing connection is being undertaken.The client automatically closes it.As a result of this truncation of data becomes possible.Due to this improper layout a virtual error state occurs..

Attack Base:

A] The session has not been fully matured. As a result the connection can be reused in certain way to initialise the same state of connection through server.

B] The attacker use this flaw. in the It becomes hard to understand whether the connection is closed by the attacker or server.

C] Due to this it becomes hard to find whether the data has been truncated by the server or attacker as anyone who has control over the machine will close the connection by issuing a rogue request and not waiting for the server alert.

The content length is always checked prior to the closing of connection by the server or by the client.This is clearly understated that if the connection is closed prematurely than the content length will get altered ie truncated to some extent.It is of concern to some extent because the content can be manipulated with MITM attacks and the length can be altered to perform the requisite work by the attackers. This issue is of great concern and have been exploited by the attackers to launch further third party attacks.

Dethroning Server's Identity

The dethroning of server identity certificate by the clients hold a crucial aspect.Actually it is possible by the client to ignore the server identity generically.what happen is that the connection is not completed fully and remain in the incomplete state which sets it for attack base.It rises complexity because if the crafty attacker owns a machine he can easily interpret the traffic and perform certain number of attacks such as MITM to let the work done by exploiting the connection which is not fully closed. As a result of this advancement has occured in the MITM attacks. Underlined is the some of the attacks which occur through the MITM.

A] Domain Manipulation:

This is a technique used by the attackers to manipulate the domain acceptance parameter to let the illicit domain to get accepted.As we know the metacharacters play a generic role in acceptance of domain as parameters are set according to that.A wildcard (*) character is used to accept the domain starting with specific entity and others of same kind.

Ex:- *.meta.com , A*.meta.com The attacker can easily manipulate the parameters that further result rogue domain acceptance.

B] Certificates Error Generation:
This is a very specific way to accept the unauthorised connection when the certificate parameters that are not same as that of client.This is a configuration problem because a error is generated if no match occurs and connection can or can not be terminated.The attacker uses this technique by removing check on the error acceptance as a result of which error prone connection or unauthorised connection get established and further attacks can be performed.

Data Blocks Encryption
This is prime importance when TLS security is concerned because the data block recieved from the client is encoded in a specific manner.After the decoding of message by the TLS server , this can be checked whether the message is formatted in right manner or not..It is a case of poor encryption as layer by layer data block is traversed to decode the content.
Ex: The Attack discovered by : Daniel is a perfect example of this.

Structure of RSA Encrypted Secret Message

```
struct {
        ProtocolVersion client_version;
        opaque random[46];
        } PreMasterSecret;
```

The attack takes advantage of the fact that by failing in different ways, a TLS server can be coerced into revealing whether a particular message, when decrypted, is properly PKCS#1 formatted or not.

Switching Between HTTP1.0 /HTTP1.1 /TLS:
This is the new blend that has been undertaken for security parameter to upgrade the normal connection to get upgraded to secure tansport layout.This occur in the underlined way:-

First of all options request is sent to server as:

```
Options * HTTP/1.1
Host : www.meta.com
Upgrade : TLS/1.0
Connection : Upgrade
```

The request is accepted by server and the required switching is done then:

```
GET http://<any file> HTTP/1.1
Host: www.meta.com
Upgrade: TLS/1.0
Connection: Upgrade
```

So in this way the required request is processed by the server.Sometimes a server require a request code as:

```
HTTP/1.1 426 Upgrade Required
Upgrade: TLS/1.0, HTTP/1.1
```

Connection: Upgrade

But the structure is of great security concern because if possible , the attacker can easily switch over between secure and insecure channels during the course of endpoint checks.That means after undertaking parameters the attacker can easily play with the upgrade entity.So no doubt security enhancement has been done but malfeasance occur at same time too.

Tunnel Anatomy:

The tunnel generation can not be considered to be as perfect solution for imparting security.This is very true in its context.The point of concern is authorisation.The presence of proxy in between source and destination makes the thing complex.The authorisation is very limited to a number of ports that means it not a distributed layout.The very basic port is 80.The proxy inclusion makes it very handy as well as point of concern.The data becomes opaque when travelling through the tunnel..The reverse connection to ports also become possible.

So all in all this is playing in both aspects.

Conclusion

The aim is to inspect the way of malfeasance occur in the end point communication that makes it attack prone.The stress is laid on the understanding of these hidden tags in the realm of providing security.