66-G : __ __ __

Restoring the Privacy and Confidentiality of Users Over Mobile Collaborative Learning (MCL) Environment

Abdul Razaque & Khaled Elleithy
Wireless & Mobile Communication Laboratory
Department of Computer Science and Engineering
School of Engineering, University of Bridgeport, CT

Abstract

Rogue DHCP server spreads the wrong network parameters that create the bridge for attackers to expose confidentiality and privacy. Trojans like DNS-changing installs the rogue DHCP server and pollutes the network. It provides the chances for attackers to use compromised resources on network. Rogue DHCP server creates several problems to expose the privacy of legitimate users. Two important attacks are shown in figure 1. The poster focuses on two of most important issues.

Introduction

The rogue DHCP is unauthorized server that releases the incorrect IP address to users and sniffs the traffic illegally. The contribution specially provides privacy to users and enhances the security aspects of mobile supported collaborative framework (MSCF). The poster introduces multi-frame signature-cum anomaly-based intrusion detection system (MSAIDS) supported with novel algorithms, addition of new rules in IDS and mathematical model. The major target of contribution is to detect malicious attacks and blocks an illegal activities of rogue DHCP server and develop new application for medical.

Algorithm 1: Verifying DHP Server and detecting the attack

1. Input: MF =(FD, FS,FA & I)
2. Output : For every strategy I € FA, I € FS, D € FD)
3. D = Each valid DHCP Server
4.IP= Internet protocol address
5. N= Number of mobile devices
6. FD= Frame DHCP server
7. If D € FD
8. IP→ N
9. endif
10.S= Number of available signatures in signature based Intrusion detection system (SIDS)
11.FS= Frame of signatures
12.FS ⊆ SIDS
13.I= Number & Types of attacks
14.For (I=S; I ≤ FS; I++)
15.If I ⊆ FS
16.SIDS attack alert
17.endif
18.endfor
19.A= Number of signatures available in Anomaly based Intrusion detection system AIDS
20.FA= Frame of AIDS
21.FA ⊆ AIDS
22.For (I =A; I ≤ FA ; I ++)
23.If I ⊆ FA
24.AIDS raises alert
25.If (I ∉ FS & I ∉ FA)
No alert (No attack)
26.endif
27.endif
28.endfor

Calculation by using mathematical model

I. $TP = TP^2 + (TP^* FN) / TP + FP$

II. FN-FN= 0
If we get zero value that shows the false negative

III. FP= FNTP /TP

IV. TN-TN=0

Possible attacks of DHCP rogue server

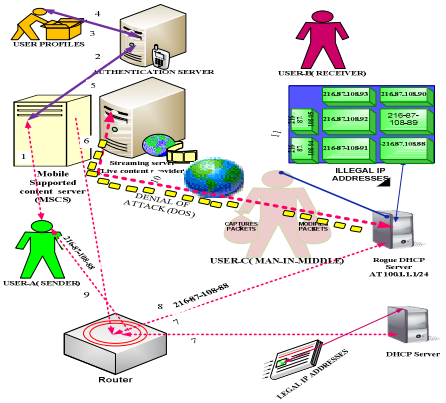

Figure 2.denial of service attack (DOS) attack

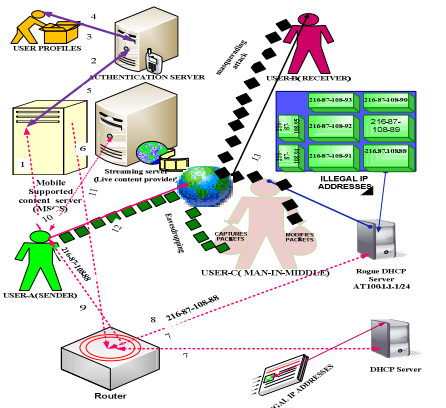

Figure 3. showing masquerading attack while sniffing traffic

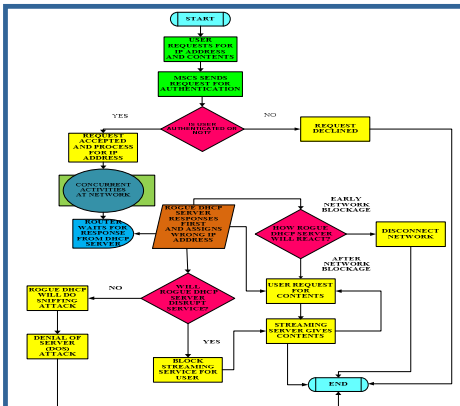

Figure 4.Behavior of DHCP Rogue during the attack

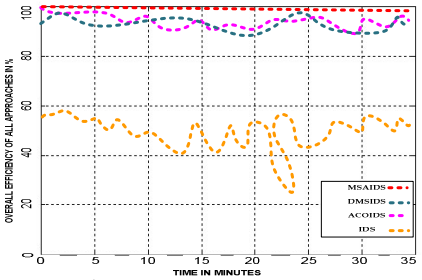

Figure 5.Comparison efficiency of all approaches

Algorithm 2: Detecting the types of alerts with AIDS

1.FS= Frame of signatures
2.FS ⊆ SIDS
3.Si = False Negative
4.Sj= True negative
5.Sk= True positive
6.Sk= False positive
7. 0 = don't match & 1= match
8.Sijkl = 1/d $\sum_{m=1}$ Sijkl
10.Sij = { 0, if i & j
11.No false negative & true positive
12.Sij = { 1, if i & j
13.false negative & true positive
14.Alert of attack
15.Skl = { 0, if k & l [do not match] & 1, if k & l [match]
16.Alert of true negative & false positive
17.No sign of attack
18.endif
19.endif
20.endif
21.endif

Algorithm 3: Determine the sing of attack or non-sign of attack

I. We select random odd prime number for TN and any even number for FN.
2. The value of FN must not be exceeded than TN.
3. Therefore, FN > 1 & FN< TN
4. Here, FN= {2, 4, 6, 8…} & TN= {3, 5, 7, 11, 13…}
5. Here sign of attack = ST, d = not exposed & b = exposed.
6. b and d has constant value 1.
7. Thus, ST = TN/ (TN+ d)/ FN (FN +b)
8. If value of ST > 1, it means there is no sign of attack, if the value of ST < 1 that is sign of attack.
9. endif
Assume FN = 2 & TN =3
BY applying the sign of attack formula:
ST = TN/ (TN+ d)/ FN (FN +b)
Substitute the values in given formula.
ST = 3/ (3+ 1) / 2(2+1)
ST = 9/8
ST= 1.125
ST > 1
Here, ST > 1 means there is no sign of attack and we will be able to determine that is True negative (TN).

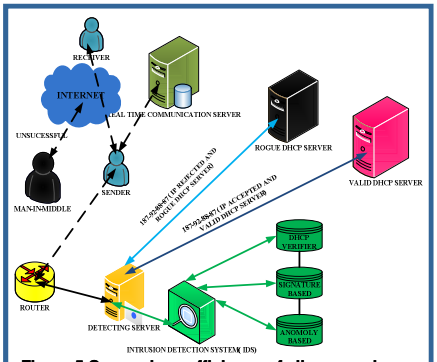

Figure 5.Comparison efficiency of all approaches

Conclusion

MSAIDS is presented in this poster. It controls malicious activities of DHCP rogue server to restore privacy of users during MCL. This research also boost the confidential level of the users. In future, the applications of this research will be implemented in medical field for detecting cancer and brain tumor.

Abdul Razaque , Khaled Elleithy," Restoring the privacy and confidentiality of users over Mobile collaborative learning (MCL) environment, IEEE Transaction, LTL-2011, VOL-09.