CANAUX CACHES

Plan

- Introduction
- Definition
- Classification
- Canaux réseaux
- Detection d’un canal caché sur un réseau
- Modèles de sécurité des flux d’informations
- Conclusion

Introduction

- Depuis leur création les réseaux d’ordinateurs avaient pour but d’échanger des mails des données ou partager des informations entre chercheurs ou dans des locaux des entreprises les enjeux de la sécurité étaient alors négligeable.

Introduction

- Aujourd'hui avec les nouvelles technologies tous les services et tous les réseaux s'interconnectent, les données de toute personnes reliés à ce vaste réseau sont plus au moins accessibles à n'importe qui ainsi la sécurité des différents réseaux est devenu primordiale, pour assurer la sécurité des informations il a fallu alors restreindre le transit des données de ces réseaux.

Introduction

- Dès qu'on parle de transit d'informations , volontairement ou non cela se fait par un canal donc il est possible d'utiliser le flux autorisé pour faire transiter des données arbitraires dont le trafic est interdit , mettant ainsi en place un canal de communication caché d'où l'intérêt de la stéganographie par rapport à la cryptographie vu qu'elle cherche à dissimuler un message là ou la cryptographie cherche à préserver sa confidentialité .

Introduction

- Ainsi tout administrateur consciencieux sait que les canaux cachés existent, et qu'il ne peut pas grand chose pour les détecter. Néanmoins l'objet de toutes les convoitises en sécurité étant l'information, toute forme de fuite peut s'avérer néfaste.

Définition

- Canal caché ou « covert channel » en anglais est un chemin de communication qui n’a pas été initialement prévu et/ou qui n’est pas autorisé pour transférer de l’information et qui, par conséquent, viole la politique de sécurité mise en place. Signalons qu’un canal caché nécessite donc au moins deux intervenants : celui qui donne les informations et celui qui les reçoit.

Classification

- ***Covert storage channel*** : un processus dispose d'un accès, direct ou indirect, à un espace de stockage en écriture, pendant qu'un autre processus dispose d'un accès, direct ou indirect, à ce même espace de stockage, mais en lecture.

Classification

- ***Covert timing channel*** : ces canaux consistent pour l'utilisateur à mesurer la vitesse à laquelle s'exécute ses processus afin de déduire ce que font d'autres processus à ce moment alors qu'il ne peut pas les observer directement.

Classification

- ***Termination channel*** : un premier processus lance une tâche, le second récupère l'information en vérifiant que cette tâche est achevée ou non.

Classification

- ***Probabilistic channel*** : un processus modifie la distribution de probabilités d'un événement associé à une ressource, le second processus doit alors estimer cette distribution.

Classification

- ***Resource exhaustion channel*** : ce type de canal s'appuie sur la disponibilité ou non d'une ressource donnée.

Canaux réseaux

- Les Canaux cachés de la couche Réseau
- Les Canaux cachés au niveau de la couche transport
- Les Canaux cachés de la couche application

Canaux réseaux

- Les Canaux cachés de la couche Réseau

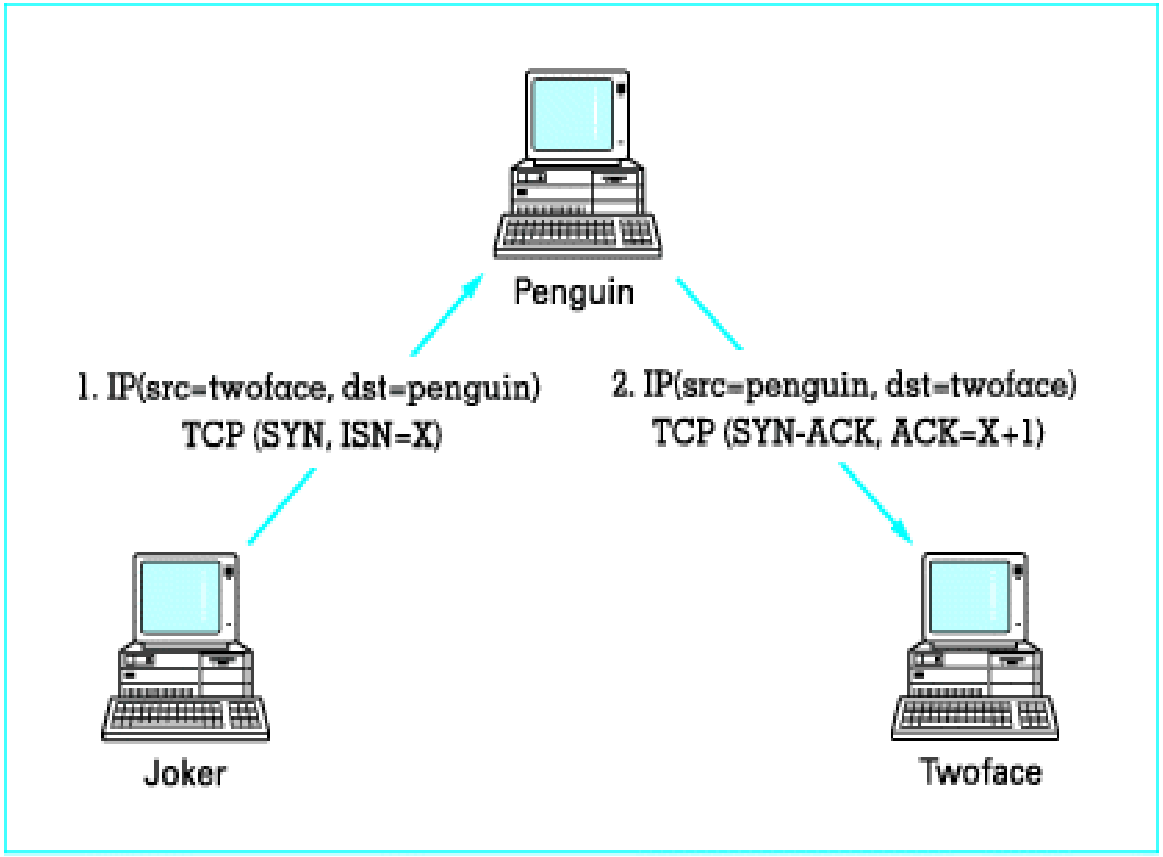
- Champs identification
- Champs Flags
- Champs options…

Canaux réseaux

- Les Canaux cachés au niveau de la couche transport

- Champs Syn (entête TCP)
- ICMP…

Canal caché par rebond



Canaux réseaux

- Les Canaux cachés de la couche application

- http: User-Agent, Referer, Cookie
- DNS: ID, QDCOUNT, ANCOUNT, NSCOUNT, ARCOUNT, QNAME, NAME

Détection d’un canal cache

16:03:38.931022 192.168.1.2 > 81.91.65.187:icmp: echo request (DF)0x0000 4500 . .0x0010 . . . . @ . . . @ . . T 0054 0000 4000 4001 e5e8 c0a8 0102E . 515b 41bb 0800 ee34 6e5a 0100 3a9e c33eQ [A . . . . 4 n Z . . : . . >0x0020 S E T S E C R E T C R . . af34 0e00 4352 4554 5345 4352 4554 5345. 4 C R S E C R E T S E E T E0x0030 4352 4554 5345 4352 4554 5345 4352 4554C R E T S E C R E T C R E T0x0040 5345 4352 4554 5345 4352 4554 5345 4352S E C R0x0050 4554 5345E T S E S E

Modèle

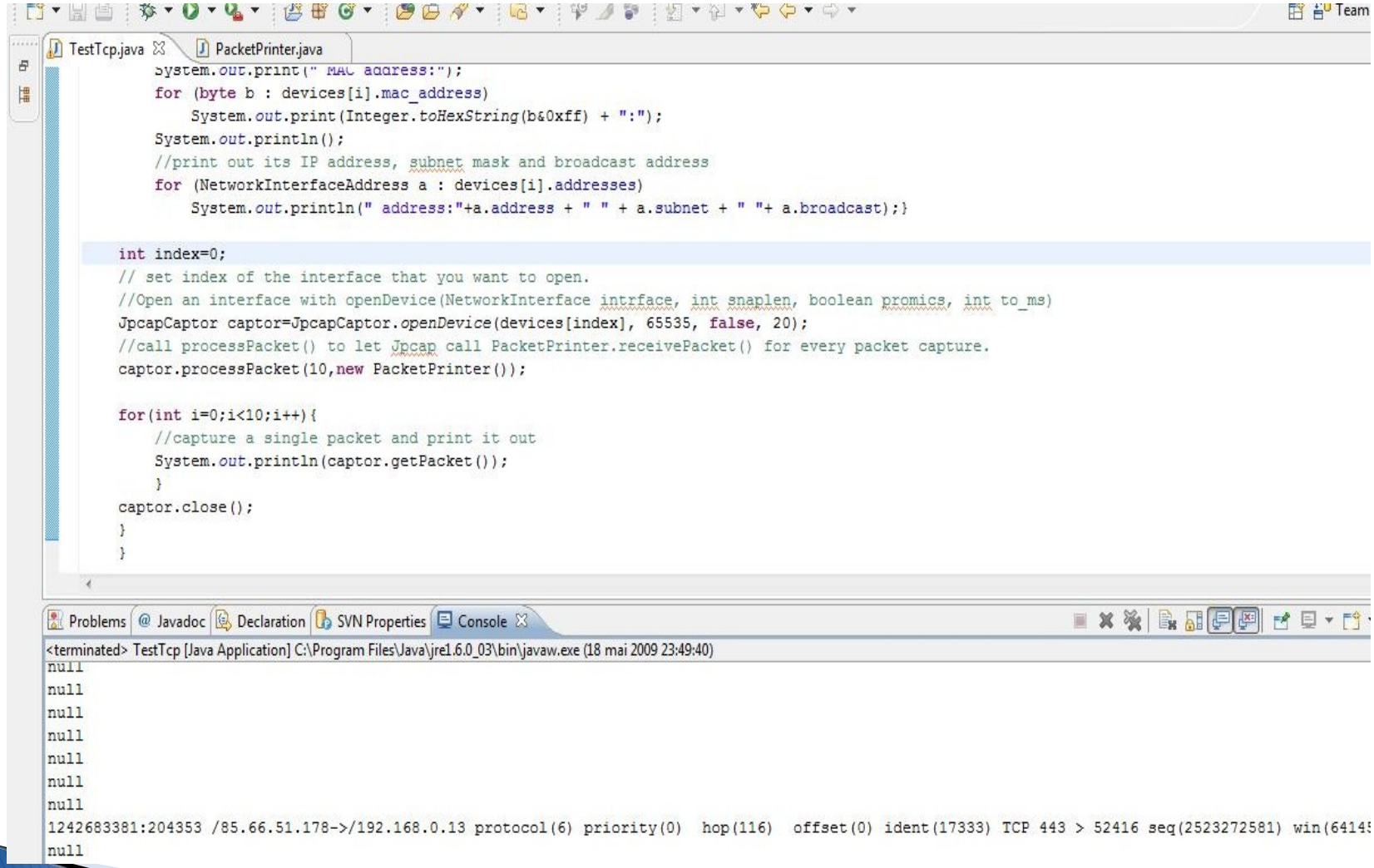
- **Modèle classique de Bell et LaPadula**
- **Modèle de non-interférence**
- **La non-interférence caractérisée par un système de types**

Conclusion

- A ce jour un grand nombre de recherches dédiés aux canaux cachés sont disponible en tant qu'articles ou en tant qu'outils mais en tant que aspects pratique et application, on n'a pas encore une stratégie efficace pour éliminer le transit des informations avec ses canaux cachés.

- Ainsi dans notre projet on a essayer de faire une approche global sur les canaux cachés pour mieux comprendre leur problématique, de plus on a essayer de programmer et d'implémenter l'exemple abordé dans la section canaux réseaux.

conclusion


TestTcp.java
PacketPrinter.java
System.out.print(" MAC address:");
for (byte b : devices[i].mac_address)
System.out.print(Integer.toHexString(b&0xff) + ":");
System.out.println();
//print out its IP address, subnet mask and broadcast address
for (NetworkInterfaceAddress a : devices[i].addresses)
System.out.println(" address:"+a.address + " " + a.subnet + " "+ a.broadcast);}
int index=0;
// set index of the interface that you want to open.
//Open an interface with openDevice(NetworkInterface intrface, int snaplen, boolean promics, int to_ms)
JpcapCaptor captor=JpcapCaptor.openDevice(devices[index], 65535, false, 20);
//call processPacket() to let Jpcap call PacketPrinter.receivePacket() for every packet capture.
captor.processPacket(10,new PacketPrinter());
for(int i=0;i<10;i++){
//capture a single packet and print it out
System.out.println(captor.getPacket());
}
captor.close();
}
}
Problems
Javadoc
Declaration
SVN Properties
Console
<terminated> TestTcp [Java Application] C:\Program Files\Java\jre1.6.0_03\bin\javaw.exe (18 mai 2009 23:49:40)
null
null
null
null
null
null
null
1242683381:204353 /85.66.51.178->/192.168.0.13 protocol(6) priority(0) hop(116) offset(0) ident(17333) TCP 443 > 52416 seq(2523272581) win(64145
null