Cryptography & Network Security

Intruders

PRESENTED BY : RIYA KHATUN

Who are Intruders?

AN INTRUDER IS A PERSON WHO ATTEMPTS TO GAIN UNAUTHORIZED ACCESS TO A SYSTEM,
TO DAMAGE THAT SYSTEM,
OR TO DISTURB DATA ON THAT SYSTEM.

TYPES OF INTRUDERS

--INTRUDERS CAN BE CLASSIFIED IN THREE BROAD CATEGORIES

01 Masquerader

An unauthorized user who penetrates a system's access control to exploit other's account.

Most likely an outsider

02 Misfeasor

A legitimate user but accesses data, program or resources for which he/she is not authorized.

Generally an insider

03 Clandestine

An individual who seizes supervisory control and evades auditing and access control

May be an insider or outsider

EXAMPLES OF INTRUSIONS

01 Performing a remote root compromise of an e-mail server

02 Defacing a Web server

03 Guessing and cracking passwords

04 Copying a database containing credit card numbers

05 Viewing sensitive data, including payroll records and medica information, without authorization

06 Running a packet sniffer on a workstation to capture usernames and passwords

07 Using a permission error on an anonymous FTP server to distribute pirated software and music files

08 Dialing into an unsecured modem and gaining internal network access

09 Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password

AUDIT RECORD

A fundamental tool for intrusion

Basically, two plans are used :

Native audit records: Virtually all multiuser operating systems include accounting software that collects information on user activity. The advantage of using this information is that no additional collection software is needed. The disadvantage is that the native audit records may not contain the needed information or may not contain it in a convenient form.

Detection-specific audit records: A collection facility can be implemented that generates audit records containing only that information required by the intrusion detection system. One advantage of such an approach is that it could be made vendor independent and ported to a variety of systems. The disadvantage is the extra overhead involved in having, in effect, two accounting packages running on a machine

INTRUSION TECHNIQUES

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system.

Alternatively, the intruder attempts to acquire information that should have been protected.

With knowledge of some other user’s password, an intruder can log in to a system and exercise all the privileges accorded to the legitimate users.

INTRUSION DETECTION

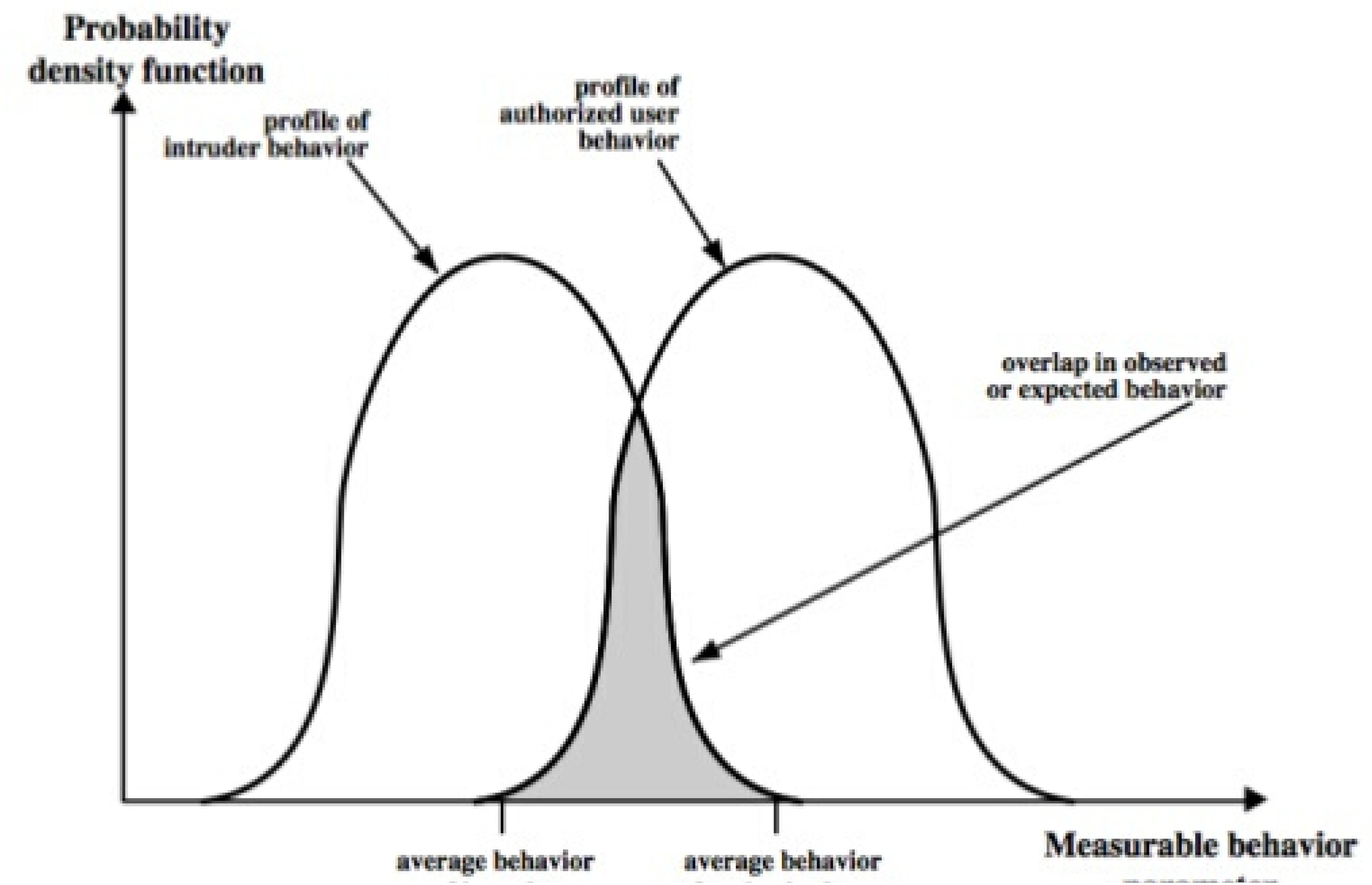
Inevitably, the best intrusion prevention system will fail. A system's second line of defense is intrusion detection, and this has been the focus of much research in recent years. This interest is motivated by a number of considerations, including the following:

1.If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.

2. An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.

3. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

INTRUSION DETECTION



Intrusions Preventions

An intrusion prevention system is typically configured to use a number of different approaches to protect the network from unauthorised access. These include:

--Signature-Based

--Anomaly-Based

--Policy-Based