CS3840 Computer Security Homework 5 2017

Name: Nick Kvigne

1. Consider an SQL statement:

SELECT id, forename, surname FROM authors WHERE forename = ‘john’ AND surname = ‘smith’

1. What is this statement intended to do?

This will get the id, forename and surname from the authors table of all records with the forename ‘john’ and surname ‘smith’.

**b.** Assume that the forename and surname fields are being gathered from user-supplied input, and suppose the user responds with:

Forename: jo’hn

Surname: smith

What will be the effect?

The forename will be entered in as jo, since the apostrophe ends the input, so that record will not be gathered by the previous SQL statement.

**c.** Now suppose the user responds with:

Forename: jo’; drop table authors--

Surname: smith

What will be the effect?

The author table will be deleted.

1. Consider the following fragment:

*legitimate code*

ifdata is Friday the 13th;

crash\_computer();

*legitimate code*

What type of malware is this?

Logic Bomb

1. Assume a future where security countermeasures against DoS attacks are much more widely implemented than at present. In this future network, antispoofing and directed broadcast filters are widely deployed. Also, the security of PCs and workstations is much greater, making the creation of botnets difficult.
2. Do the administrators of server systems still have to be concerned about, and take further countermeasures against, DoS attacks?

Yes, they do need to be concerned about these attacks.

1. If so, what types of attacks can still occur, and what measures can be taken to reduce their impact?

DoS attacks could still occur. These attacks could just use nonspoofed addresses, which could still be used in these attacks.

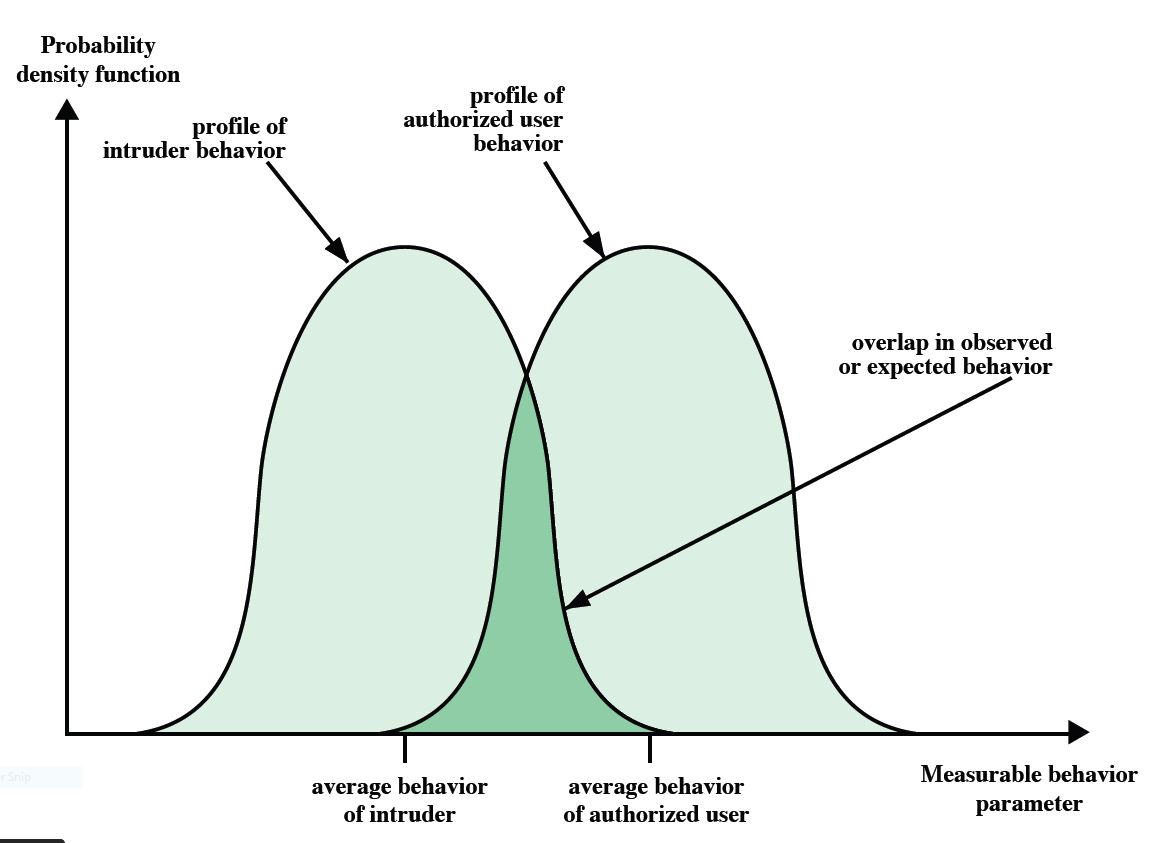
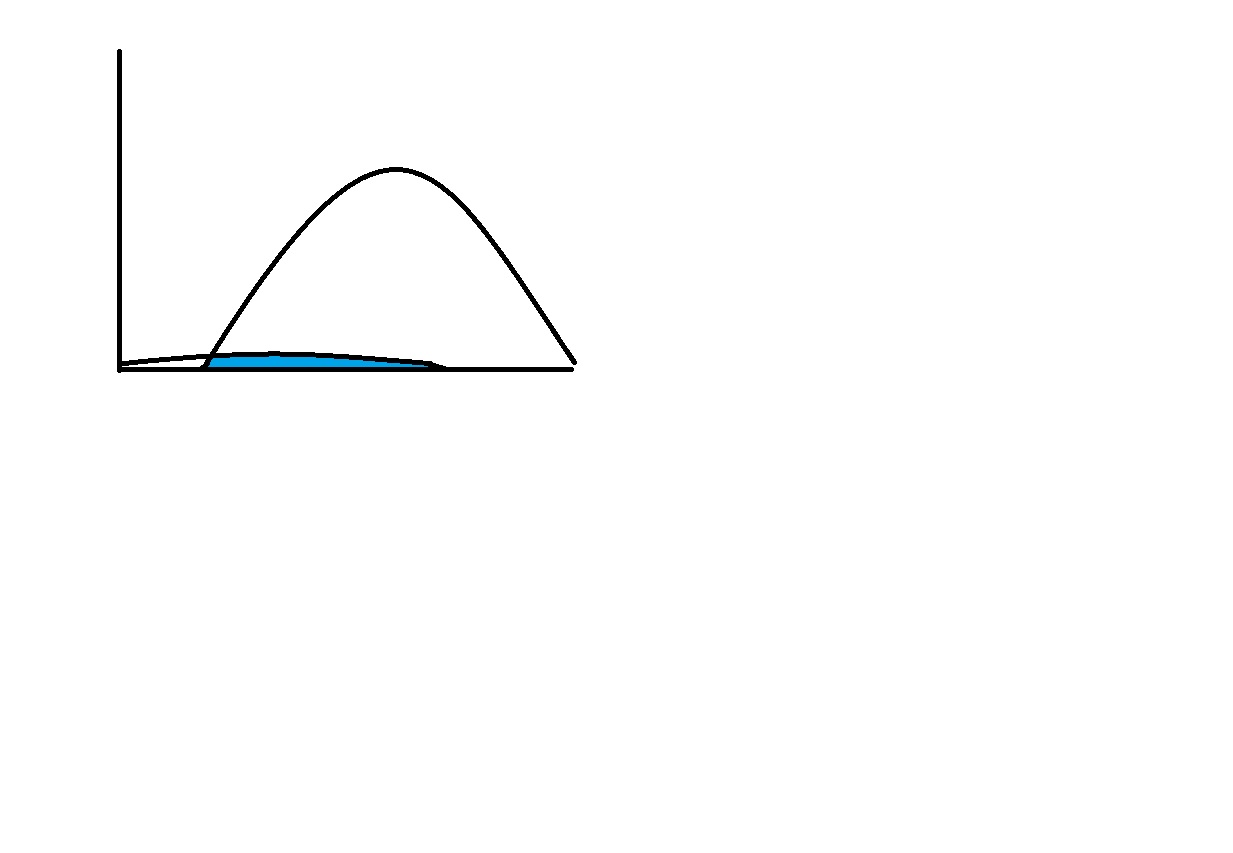


Figure 8.1

1. The overlapping area of the two probability density functions of Figure 8.1 (above) represents the region in which there is the potential for false positives and false negatives. Further, Figure 8.1 is an idealized and not necessarily representative depiction of the relative shapes of the two density functions. Suppose there is 1 actual intrusion for every 1000 authorized users, and the overlapping area covers 1% of the authorized users and 50% of the intruders.
2. Sketch such a set of density functions and argue that this is not an unreasonable depiction.



With all the security measures in place, most of the authorized users should be getting through, yet there is always a small chance for a very small percentage of those users to be intruders.

1. What is the probability that an event that occurs in this region is that of an authorized user? Keep in mind that 50% of all intrusions fall in this region.

1000 \* 1% = 10 authorized

1 \* 50% = .5 unauthorized

10 / 10.5 = 95.24%