### AUTHENTICATION USAGE MODEL

The authentication usage model represents the usage of an authentication system. The independent variables that must be sampled to determine the usage of an authentication system are the average data transmitted during an authentication (x1) and the average network speed for a single authentication (x2). The average data transmitted is the average of request and response data for a single authentication and the average network speed is the average upload and download speed for a single authentication. The dependent variable that must be sampled is the time taken for an authentication (y).

The goal of modelling the dependent and independent variables is to arrive at a mathematical relationship between y and the two independent variables x1 and x2. It is expected that the relationship will be Y=c1(x2/x1) +c2, where c1 and c2 are system constants. In addition to that, some system constants that will aid threat analysis must be determined. These are the total number of valid authentications, the expected authentications within a time frame, the minimum authentications within a time frame and the maximum authentications within a time frame.

The mathematical relationship between y, x1 and x2 is the normal usage model of the authentication system. After this relationship has been determined, various occurrences that deviate from this relationship can be used to analyze threats. For instance, any occurrence that is not equal to the average usage is a threat. Additionally, any occurrence that indicates a change outside an acceptable threshold is a threat. The acceptable threshold is a range within which changes in the systems are deemed normal. Such a range is composed of the average usage and standard deviation.

### SESSION USAGE MODEL

A session usage model represents a single user’s behavior before his session expires. To determine the mathematical model for a user’s session, two main independent variables must be sampled. These are size of session data accumulated (x1), and number of user actions (x2). The dependent variable that must be sampled is time spent before session expires (y). The session usage model is expected to be made up of two micro usage models. The mathematical representation of the micro usage models are expected to be Y=c1x1+c2 where c1 and c2 are systems constants and Y=c1x2+c2 where c1 and c2 are system constants.

In addition to the two mathematical functions, some system constants that will aid threat analysis must be determined. These include average user actions, average size of data accumulated, average time spent. These constants can be determined from the data set used to determine the usage model.

The two mathematical relationships represent the session usage model. Both are linear functions. It is expected that as user actions increase the time spent also increases. It is also expected that as data accumulated increase times spent also increases.

### MEMORY USAGE MODEL

The memory usage model represents the usage of memory space in a system. The independent variables that must be sampled are number of application programs running (x1), and the number of system processes running (x2). The dependent variable that must be sample is amount of memory space being used(y). The mathematical relationship between x1, x2, and y is expected to be y=c1x1+c2x2+c3 where c1 is the average memory space for programs, c2 is the average memory space for processes and c3 is the average memory being used when no process or program is running.

In addition to these, some system constants that aid threat analysis must be determined. These include the minimum and maximum memory space for programs and the minimum and maximum memory space for processes. The mathematical relationship between x1, x2, and y is the memory usage model. When determined, the memory usage model can be used to analyze changes in the memory usage that indicate threats in the system.

### CPU USAGE MODEL

The CPU usage model represents CPU usage in a system. The independent variables that must be sampled are the number of application programs running (x1), and number of system processes running (x2). The dependent variable that must be sampled is amount of CPU power being used (y). The mathematical relationship between x1, x2, and y is expected to be y=c1x1+c2x2+c3 where c1 is the average CPU power being used for programs, c2 is the average CPU power being used for processes and c3 is average CPU power being used when no process or program is running. In addition to these, some system constants that aid threat analysis must be determined. These include the minimum and maximum CPU power for programs and the minimum and maximum CPU power for processes. The mathematical relationship between x1, x2 and y is the CPU usage model. When determined, the CPU usage model can be used to analyze changes in the CPU usage that indicate threats in the system.

### HOST USAGE MODEL

The host usage model is composed of four independent variables. Memory usage (x1), session usage (x2) and CPU usage (x3), derived from their respective usage models. The dependent variable that must be sampled in the time host spent on host (y). Any relationship determined between the dependent and the independent variables is the host usage model. The resulting host usage model is denoted y=f (x1,x2, x3).

### SERVER USAGE MODEL

The server usage model is made up of the CPU time being used, the memory space being used and the number of processes running. These variables are used to form two different micro usage models. As such, there are two dependent variables, CPU time and memory space. The independent variable for both micro usage models is the number of processes running.

### BATTERY USAGE MODEL

The battery usage model is made up of the average usage of CPU, average memory usage and the average usage of how a session behaves in the system. These are the independent variables. The dependent variable is the battery lifespan. The independent variables are derived from their respective micro usage models.

### DEVICE USAGE MODEL

The device usage model is made up of a battery usage model, a host usage model, and the time spent on the device. The usage models that make up the device usage model compute the average micro usage and try to relate that with the time spent on the device. The time spent on the device is the dependent variable.

### PORT USAGE MODEL

The port usage model is made up of the time elapsed during communication, number of programs that use the port and the number of paired ports. The number of paired ports is the dependent variable and the remaining variables are the independent variables.

### NETWORK USAGE MODEL

The network usage model is made up of average port usage, average server usage average host usage, the average size of data transmitted on the network, and time spent on the network. The first three variables are the independent variables. The remaining two are the dependent variables. As such two micro usage models make up the network usage model.

### PROGRAM USAGE MODEL

To determine the program usage model, the dependent and independent variables that must be sampled are time spent using program (y), and number of functions used (x). In addition to that, the following constants must also be determined. Minimum functions used and maximum functions used. The relationship between y and x determined after sampling various x and y values is the program usage model denoted by y=f(x).

### AGGRESSIVE USAGE DETECTOR

This model is a utility that detects aggressive behavior on a system. It is modelled just like the various micro usage models. Various factors that determine aggressive behavior during system usage are used to determine the mathematical representation of this utility. Aggressive behavior includes aggressive use of major system resources, and aggressive use of system components with limited resources.

The average aggressive behavior and its standard deviation are determined. Any system occurrence that indicates the average aggressive behavior, or the average aggressive behavior plus its standard deviation or the average aggressive behavior minus its standard deviation is considered a threat and must be halted, alerted or stored for audit purposes.

### FALSE ALARM DETECTOR

The false alarm detector is a utility that detects normal system usage that otherwise may be deemed threats. Occurrences that meet the criteria for false alarms are normal usage that seems to put the entire usage of the system into a false state of vibration or anarchy. Such usage occurrences are as such prioritized as normal optimal usage. The remedy for the vibrations such usage occurrences cause is delay in other normal usage occurrences in the system.

The state and magnitude of other system occurrences plus the state and magnitude of the normal optimal usage determine the impact of the perceived anarchy. To increase convenience with which the system for which this utility is developed, the average delay time and its standard deviation must be detected. This utility is part of the normal usage. The utility is modelled just like the aggressive usage detector.