METHOD AND SYSTEM FOR RESPONDING TO A COMPUTER INTRUSION

Field of the Invention

The present invention relates in general to the field of data processing, and, in particular, to an improved data processing system and method for responding to a malicious intrusion using a graphical representation of the intrusion's effect.

Background of the Invention

Most modern enterprise networks include means for access by remote users, typically via the Internet. This access is designed to afford authorized users interaction with the network for purposes such as e-commerce, sharing content, and other electronic activities. Because these networks are designed to be easily accessible to authorized users, they are also prone to access by unauthorized users, specifically those with malicious intent for accessing the network. This malice is presenting in the form of an "intrusion" by the user. An intrusion is defined as a malicious electronic access of the network or a computer in the network. Examples of intrusions include viruses, unauthorized data mining (sometimes called "hacking of files"), and distributed denial of service (DDOS) attacks, in which a computer system is overloaded by the intrusion such that real work can no longer be performed.

An intrusion event is defined as the result (effect) of an intrusion. Examples of an intrusion event are data files being corrupted or illegally copied, system/computer crashes and system/computer slow-downs.

Countering intrusions is typically the job of a security administrator, an information technology specialist who monitors, with the aid of risk management software, a computer system for intrusions. While there are many known methods for detecting an intrusion and the intrusion event, managing responses to the intrusion is extremely complicated. That is, while detection of an event is well known and may be automatic, management and response actions are typically taken manually. Because of the complex nature of an intrusion, it is difficult for the security administrator to evaluate what type of intrusion is occurring, and how to respond appropriately.

Thus, there is a need for a method and system to assist the security administrator in responding to detected intrusions, preferably in an manner that is automatic or semi-automatic.

SUMMARY OF THE INVENTION

The present invention is directed to a method and system for managing an intrusion on a computer by graphically representing an intrusion pattern of a known past intrusion, and then comparing the intrusion pattern of a current intrusion with the past intrusion. If the known and current intrusions have some or all common results (intrusion events or commonly affected hardware), then a security administrator can execute scripted responses to heal damage caused by the current intrusion, or at least prevent the current intrusion from causing any further damage.

The intrusion pattern may either be based on intrusion events, which are the effects of the intrusion or activities that provide a signature of the type of intrusion, or the intrusion pattern may be based on hardware topology that is affected by the intrusion.

The intrusion pattern is graphically displayed to the security administrator, who can respond by executing scripted responses, which in a preferred embodiment are presented in pop-up windows associated with each node in the intrusion pattern. Alternatively, the response to the intrusion may be automatic, based on a pre-determined percentage of common features in the intrusion pattern of the known past intrusion and the current intrusion.

The above, as well as additional objectives, features, and advantages of the present invention will become apparent in the following detailed written description.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention will now be described in detail by way of example only with reference to the following drawings:

Figure 1 depicts a block diagram of a data processing system in a preferred embodiment of the present invention;

Figure 2a illustrates an intrusion pattern based on intrusion events of a many different intrusions, including a known past intrusion in a preferred embodiment of the present invention;

Figure 2b depicts an intrusion pattern based on intrusion events of an unknown current intrusion that matches an intrusion pattern of a known past intrusion in a preferred embodiment of the present invention;

Figure 3 is a flow chart of a preferred embodiment of the present invention for automatically running scripted responses for an unknown current intrusion in a preferred embodiment of the present invention;

Figure 4a illustrates an intrusion pattern based on affected hardware topology of a many different intrusions, including a known past intrusion in a preferred embodiment of the present invention; and

Figure 4b depicts an intrusion pattern based on affected hardware topology of an unknown current intrusion that matches an intrusion pattern of a known past intrusion in a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

With reference now to the figures, and in particular with reference to **Figure 1**, a data processing system **100**, capable of communication with a network (not shown), is depicted in accordance with a preferred embodiment of the present invention. Data processing system **100** may be, for example, one of the models of personal computers or servers available from International Business Machines Corporation of Armonk, New York. Data processing system **100** may include only a single processor or may be a multiprocessor (MP) system including a plurality of processors. A single processor system is shown in the example depicted. A second processor (not shown) may be added to the system depicted, either with a separate L2 cache or sharing L2 cache **108** with processor **102**. Processor **102** may be a superscalar reduced instruction set computing (RISC) processor including separate Level One (L1) instruction and data caches **104** and **106** within the processor.

Processor **102** is connected to Level Two (L2) cache **108**. L2 cache **108** is connected to system bus **110** for data processing system **100**. System memory **112** is also connected to system bus **112**, as is Input/Output (I/O) bus bridge **114**. I/O bus bridge **112** couples I/O bus **118** to system bus **110**,

relaying and/or transforming data transactions from one bus to the other. Other devices may also be connected to system bus **110**, such as memory-mapped graphics adapter **116**, which provides user interface information to a display **124**.

I/O bus bridge **114** is connected to I/O bus **118**, which may be connected to a variety of other devices such as an input device **126**, which may be a conventional mouse, a trackball, a keyboard, or the like, and a non-volatile storage **122**, such as a hard drive, a compact disk read-only memory (CD-ROM) drive, a digital video disk (DVD) drive, or similar like storage devices.

Also connected to I/O bus **118** is a networks adapter **120**, which provides a logical interface with a network, which may be a local area network (LAN), wide area network (WAN), the Internet or other network that affords communication with other computers in the network with data processing system **100**.

The exemplary embodiment shown in **Figure 1** is provided solely for the purpose of explaining a preferred embodiment of the present invention, and those skilled in the art will recognize that numerous variations are possible, both in form and function. For instance, data processing system **100** may include a sound card and audio speakers, other I/O devices and communication ports, and numerous other components.

With reference now to **Figure 2a**, illustrated are possible intrusion events caused by many different intrusions. The intrusion events are defined as effects or activities initiated by the intrusion. While depicted in a tree manner, these intrusion events are best understood by realizing that the intrusion events illustrated are interrelated. For example, consider an intrusion path **200**, which depicts intrusion events (shown in heavy circles) caused by an Intrusion A. Intrusion A, which for exemplary purposes may be a virus such as "Code Red," is an intrusion that affects multiple hosts **202** in creating a distributed denial of service **204** in a host computer **206**. Intrusion A is shown as being detected by a Snort **208**, which is an exemplary intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. Snort **208** can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, common gateway interface (CGI) attacks, server message block (SMB) probes, operating system (OS) fingerprinting attempts, and the like.

Intrusion A may also trigger a response from an intrusion detection system (IDS) **210**, which inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise the system. IDS **210** detected a network event **212**, which in the present example is Intrusion A, which is a type of intrusion event **214** identified by and affecting the entire system.

Note that Intrusion A also affects other parts of the computer system, as illustrated by intrusion path **200**. That is, Intrusion A also creates a host event **216**, which at system level **218** affects both a memory event **220** as well as a permission event **222**. Further, Intrusion A creates a perimeter event **224**, which is detected by firewall **226** as being both a scanning event **228** and also having a bad packet **230** of data. The bad packet **230** is a transmission control protocol (TCP) malformed protocol packet **232**, as depicted.

Thus, the pattern shown by intrusion path **200** having darkened heavy borders is a unique signature intrusion pattern for Intrusion A. Referring now to **Figure 2b**, there is depicted an intrusion path **201** based on intrusion events of an unknown current intrusion. The cause of the current intrusion is initially unknown. However, since the intrusion pattern is identical to that of Intrusion A of **Figure 2a**, the security administrator of the computer network or computer that has been intruded upon can recognize that the current intrusion is the same as, or at least acts in the same manner as, Intrusion A.

In a preferred embodiment of the present invention, associated with each node is a scripted response, such as scripted response **204a** associated with denial of service event **204**. The scripted response is a pre-scripted code for handling the intrusion event. For example, scripted response **204a** may be a program designed to isolate the intrusion that is overwhelming the computer system, and then disabling the intrusion. The scripted responses are depicted associated with each event describing node, and are preferably in an active window, such as a pop-up window, that initiates the scripted response simply by clicking on the active window with a mouse or similar pointing device. While scripted responses are depicted as single items, in an alternate preferred embodiment, a list of multiple suggested scripted responses are depicted and active in one or all of the nodes in the intrusion path **201**. The multiple scripted responses are preferably depicted with rankings, with one of the scripted responses having a highest ranking based on historical success using the

scripted response, the criticality of the intrusion, or other factors determined by the security administrator when developing a risk manager program for evaluating intrusions. For example, a risk manager program may determine that any intrusion that attacks mission critical data must be ensured of isolation, even if the isolation takes down non-affected parts of the computer system. In such a case, the highest suggested response would be to take down many areas of the computer system, and would be recommended as the highest suggested response.

Note that intrusion paths need not be identical to provide the security administrator information on how to respond to the intrusion. That is, if the known and unknown intrusions have a certain number of commonalities in their intrusion paths, the security administrator may initiate a response that will cure most, if not all, of the detrimental effects of the current unknown intrusion.

In one embodiment of the present invention, each scripted response is manually selected by the security administrator for each node in the intrusion path **201**. Alternatively, a setting may be selected to automatically initiate a highest suggested response for all nodes in response to an intrusion, as described in the flow chart of **Figure 3.** As described in block **302**, a current intrusion is detected, preferably by a risk manager capable of detecting an intrusion according to characteristics of the intrusion. Such characteristics may include known packets of mischievous header information or other data received, actions taken by software or hardware in the computer system characteristic of an intrusion, such as scanning all computers in a network for Internet protocol (IP) address, sudden computer performance degradation or CPU usage, and like events or conditions. The intrusion events of the current intrusion are compared with those of a known intrusion, as described in block **304**. A determination is made, as illustrated at query block **306**, as to whether a pre-determined percentage of common event nodes are found in both the unknown current intrusion and the known historical intrusion. That is, the intrusion pathways of the known and current intrusions are compared. If the known past and unknown current intrusions have a significant number of common event nodes, then scripted responses for all nodes are automatically run, as described for block **310**. If there are not enough common event nodes between the known and unknown intrusions, then the security administrator is prompted to manually select a scripted response for each event node.

The determination to automatically run all scripted responses can also be determined by a risk management program on the computer system that classifies intrusions to determine whether an automatic response should be activated. For example, if the risk management program determines that the current intrusion is of a known classification type, or is or a known severity that could cause the entire system to crash, an automatic scripted response may be initiated. In a preferred embodiment, the severity of the intrusion is matched with a severity of the results of a scripted response. That is, a severe intrusion is matched to a scripted response that may have a severe impact on the system, such as preemptively bringing down a part of the system, but the severe impact may be justified due to the severe nature of the intrusion and the potential harm the intrusion may cause.

Similarly, if the risk management program has been designed to understand that the expected response time for the security administrator to respond is likely to be so long that significant damage is done to the system before the security administrator responds, an automatic scripted response may be initiated. Likewise, if a particular intrusion path has historically resulted in execution of specific scripted responses a significant number of times (or only once), then the risk management program can automatically initiate execution of the scripted responses based on this history.

In addition to common event patterns, as illustrated in **Figures 2a** and **2b**, intrusions also have signatures regarding what hardware in a hardware topology is affected. With reference now to **Figure 4a**, there is depicted hardware that may be affected by an intrusion. An intrusion path **400**, identified in the figure by bold bordered boxes, identified hardware topology of a computer system that is affected by Intrusion A, described above in **Figure 2a**. Thus, Intrusion A causes an anomaly in an enterprises computer system's intranet **402**, which is affected by a local area network (LAN) A **404** in intranet **402**. Within LAN A **404** are affected servers **406**, personal computers (PC's) **408** and intrusion detection system (IDS) hardware **410**. Within servers **406** is an affected web server **416**, whose portal B **418** is also affected by Intrusion A. Similarly, all PC's running Windows® based operating systems are affected and shown as Windows® based **414** PC's. Likewise, IDS hardware **410** running Snort enabled hardware **412** registers an event that Intrusion A has been detected. Thus, the hardware shows a signature intrusion pattern in a manner analogous to that of the intrusion event intrusion pattern described above with **Figures 2a** and **2b**.

With reference now to **Figure 4b**, the hardware topology intrusion path **401** depicts that pattern caused by Intrusion A. When a current unknown intrusion occurs having a same or similar pattern as shown by hardware topology intrusion path **401**, the security administrator responds in a manner similar to that described for the intrusion event intrusion pattern above. Thus, each event node in the hardware topology intrusion path **401** includes an associated active window containing scripted response(s), which are analogous to those described above in describing **Figures 2a** and **2b**. As with scripted responses for intrusion events, the scripted responses described in the hardware topology intrusion path **401** may be singular, as depicted, or may be a list of suggested scripted responses, which list is preferably scored such that a highest scripted response is advocated. The scripted responses may be initiated manually or automatically in a manner analogous to that described above for intrusion event intrusion paths.

As with the graphical display of intrusion events described and depicted above with **Figure 2a** and **2b**, intrusion paths of known and unknown intrusions need not be identical to provide the security administrator information on how to respond to the intrusion. That is, if the known and unknown intrusions have a certain number of commonalities in their intrusion paths, the security administrator may initiate a response that will cure most, if not all, of the detrimental effects of the current unknown intrusion.

The scripted response to the intrusion may be initiated by the security administrator either locally or remotely, in response to a notification. For example, the security administrator may receive a notification on a cellular phone or personal digital assistant (PDA) informing her of the intrusion event. The security administrator may then activate some or all of the scripted responses electronically by clicking an interactive window in the PDA, such that the input is recognized by a risk management program for the computer system to initiate the requested scripted response(s).

The preferred embodiment described above presents a method and means for creating and graphically representing an intrusion pattern of a known intrusion for comparison to an current intrusion, which may be known or unknown by the risk management program of the computer system. After the current intrusion is identified according to its signature intrusion path which is graphically represented, scripted responses are initiated to respond to and control the intrusion. The scripted responses may be based

on historical data for the known intrusion. The known and current intrusions may be the same or different, and suggested scripted responses are graphically suggested in association with some or all of the event or hardware nodes in the intrusion path affected by the current intrusion. The scripted response may be a single choice for each event/hardware node in the intrusion path, or may be chosen from a list of ranked suggested scripted responses.

Programs defining functions of the preferred embodiment can be delivered to a data storage system or computer system via a variety of signal-bearing media, which include, without limitation, non-writable storage media (e.g. CD-ROM), writable storage media (e.g. a floppy diskette, hard disk drive, read/write CD-ROM, optical media), and communication media, such as computer and telephone networks including Ethernet. Such signal-bearing media, when carrying or encoding computer readable instructions that direct method functions of the present invention, represent alternative embodiments of the present invention.

CLAIMS

1. A method for managing an intrusion on a computer, the method comprising:

graphically representing an intrusion path of a known intrusion, the graphical representation including a scripted response at a node in the intrusion path;

matching a current intrusion of the computer to the graphical representation of the known intrusion according to at least one common feature in the intrusion path of the known intrusion and the current intrusion; and

responsive to the matching of the known intrusion and the current intrusion, initiating the scripted response, which is capable of responding to the current intrusion.

2. The method of claim 1, wherein the intrusion pattern is based on intrusion events.

3. The method of claim 1, wherein the intrusion pattern is based hardware topology affected by the known intrusion.

4. The method of claim 1, wherein the scripted response for the current intrusion is based on historical data for the known intrusion.

5. The method of claim 1, further comprising:

automatically performing the method described in claim 1 according to one of:

an expected response time for manually initiating the scripted response;

a severity of the current intrusion, wherein the scripted response is at a severity level appropriate to the severity of the current intrusion; and

a type classification of the current intrusion.

6. A system for managing an intrusion on a computer, the system comprising:

means for graphically representing an intrusion pattern of a known intrusion, the graphical representation including a scripted response at a node in the intrusion path;

means for matching a current intrusion of the computer to the graphical representation of the known intrusion according to at least one common feature in the intrusion path of the known intrusion and the current intrusion; and

means for initiating a scripted response for the current intrusion according to the matching of the known intrusion and the current intrusion.

7. The system of claim 6, wherein the intrusion pattern is based on a hardware topology affected by the known intrusion.

8. The system of claim 6, wherein the scripted response for the current intrusion is based on historical data for the known intrusion.

9. The system of claim 6, further comprising:

means for automatically performing the method described in claim 15 according to one of:

an expected response time for manually initiating the scripted response;

a severity of the current intrusion, wherein the scripted response is at a severity level appropriate to the severity of the current intrusion; and

a type classification of the current intrusion.

10. A computer usable medium for managing an intrusion on a computer, the computer usable medium comprising:

computer program code for graphically representing an intrusion pattern of a known intrusion, the graphical representation including a scripted response at a node in the intrusion path;

computer program code for matching a current intrusion of the computer to the graphical representation of the known intrusion according to at least one common feature in the intrusion path of the known intrusion and the current intrusion; and

computer program code for initiating a scripted response for the current intrusion according to the matching of the known intrusion and the current intrusion.