user device with specific instructions or data (e.g., misinformation to provide to access requests) for responding to the security threat.

One embodiment provides a system comprising a server and a user device. The server is configured to manage cyber security for a plurality of user devices belonging to an enterprise. The user device comprises an interface component configured to communicate with the server over a network; a hardware processor that implements a machine learning function configured to monitor user interactions with the user device over time to establish a use profile, to detect anomalous use of the user device based on a variance from the use profile, to input the anomalous use into the machine learning function to determine that the anomalous use is representative of a security threat to the enterprise, to control the user device to automatically initiate recording behavior of the security threat in memory based on an output of the machine learning function, and to report the behavior of the security threat to the server via the interface; and another user device managed by the server that is associated with the user device. The machine learning function is configured, in response to detecting the anomalous use of the user device, to send an instruction to the another user device to validate whether an authorized user is in proximity of the another user device. The server is configured to analyze the behavior of the security threat to profile attack patterns for the user devices belonging to the enterprise.

Another embodiment provides a method comprising communicating, via an interface component of a user device, with a server that manages cyber security for a plurality of user devices belonging to an enterprise; implementing a machine learning function with a processor of the user device; monitoring user interactions with the user device over time to establish a use profile; detecting anomalous use of the user device based on a variance from the use profile; and identifying another user device managed by the server that is associated with the user device. In response to detecting the anomalous use of the user device, the method includes sending an instruction to the another user device to validate whether an authorized user is in proximity of the another user device. The method also includes determining the anomalous use is representative of a security threat to the enterprise based on input of the anomalous use into the machine learning function; controlling the user device to automatically initiate recording behavior of the security threat based on an output of the machine learning function; reporting the behavior of the security threat to the server; and analyzing, at the server, the behavior of the security threat to profile attack patterns for the user devices belonging to the enterprise.

Another embodiment provides a non-transitory computer readable medium embodying programmed instructions executed by a processor. The instructions direct the processor to communicate, via an interface component of a user device, with a server that manages cyber security for a plurality of user devices belonging to an enterprise; implement a machine learning function with the user device; monitor user interactions with the user device over time to establish a use profile; detect anomalous use of the user device based on a variance from the use profile; and identify another user device managed by the server that is associated with the user device. In response to detecting the anomalous use of the user device, the instructions direct the processor to send an instruction to the another user device to validate whether an authorized user is in proximity of the another user device; determine the anomalous use is representative of a security threat to the enterprise based on input of the anomalous use into the machine learning function; control the user device to automatically initiate recording behavior of the security threat in memory based on an output of the machine learning function; report the behavior of the security threat to the server; and analyze, at the server, the behavior of the security threat to profile attack patterns for the user devices belonging to the enterprise.

Another embodiment provides an apparatus comprising a hardware processor configured to detect anomalous use of a user device based on historical use of the user device, to identify another user device that is associated with the user device, to send an instruction to the another user device to validate whether an authorized user is in proximity of the another user device in response to detecting the anomalous use of the user device, to input information of the anomalous use into a machine learning function, to determine a characteristic of a cyber threat from an output of the machine learning function, to initiate recording behavior of the cyber threat in memory based on the characteristic, and to report the behavior of the cyber threat to a server that manages cyber security for the user device and other user devices belonging to an enterprise.

Another embodiment provides a method comprising detecting anomalous use of a user device based on historical use of the user device; and identifying another user device that is associated with the user device. In response to detecting the anomalous use of the user device, the method includes sending an instruction to the another user device to validate whether an authorized user is in proximity of the another user device. The method also

includes inputting information of the anomalous use into a machine learning function; determining a characteristic of a cyber threat from an output of the machine learning function; initiate recording behavior of the cyber threat based on the characteristic; and reporting the behavior of the cyber threat to a server that manages cyber security for the user device and other user devices belonging to an enterprise.

There is also disclosed a system that includes a server configured to manage a plurality of user devices over a network, and a user device that includes an interface and a processor. The interface is configured to communicate with the server over the network, and the processor implements a machine learning function configured to monitor user interactions with the user device over time to establish a use profile, to detect anomalous use of the user device based on a variance from the use profile, to determine whether the anomalous use is representative of a security threat, and to instruct the user device to perform one or more automatic actions to respond to the security threat.

There is also disclosed an apparatus that includes a processor configured to detect anomalous use of a user device based on historical use of the user device, to input information of the anomalous use into a machine learning function, and to determine a characteristic of a cyber threat from an output of the machine learning function. The processor is also configured to determine an automatic action for the user device to perform based on the characteristic of the cyber threat, and to instruct the user device to perform the automatic action to respond to the cyber threat.

Other exemplary embodiments (e.g., methods and computer-readable media relating to the foregoing embodiments) may be described below. The features, functions, and advantages that have been discussed can be achieved independently in various embodiments or may be combined in yet other embodiments further details of which can be seen with reference to the following description and drawings.

Description of the Drawings

Some embodiments of the present disclosure are now described, by way of example only, and with reference to the accompanying drawings. The same reference number represents the same element or the same type of element on all drawings.

FIG. 1 illustrates an enterprise network environment in an exemplary embodiment.

CLAIMS

1. A system comprising:

a server configured to manage cyber security for a plurality of user devices belonging to an enterprise; and

a user device comprising:

an interface component configured to communicate with the server over a network;

a hardware processor that implements a machine learning function configured to monitor user interactions with the user device over time to establish a use profile, to detect anomalous use of the user device based on a variance from the use profile, to input the anomalous use into the machine learning function to determine that the anomalous use is representative of a security threat to the enterprise, to control the user device to automatically initiate recording behavior of the security threat in memory based on an output of the machine learning function, and to report the behavior of the security threat to the server via the interface; and

another user device managed by the server that is associated with the user device,

wherein the machine learning function is configured, in response to detecting the anomalous use of the user device, to send an instruction to the another user device to validate whether an authorized user is in proximity of the another user device, and

wherein the server is configured to analyze the behavior of the security threat to profile attack patterns for the user devices belonging to the enterprise.

2. The system of claim 1 wherein:

the server is configured to detect that the user device is compromised by the security threat, and to postpone invalidating communication of the user device to the server via the network for a period of time; and

the machine learning function operating on the user device is configured to record and report the behavior of the security threat to the server over the network via the interface component during the period of time.

3. The system of claim 1 wherein:

the behavior of the security threat includes one or more of keystroke data, audio data, image data, application use data, or file access request data.

4. The system of claim 1 wherein:

the machine learning function is configured to restrict capability of the user device to enable increased amounts of data collection related to the behavior of the security threat.

5. The system of claim 1 wherein:

the machine learning function is configured to instruct the user device to activate at least one hardware component including one of a microphone, a camera, and a network interface component, and to record the behavior of the security threat by monitoring the at least one hardware component.

6. The system of claim 1 wherein:

the user device includes a wireless interface component; and

the machine learning function is configured to instruct the user device to activate the wireless interface component to spoof a wireless network, to collect information of a wireless device that connects to the wireless network, and to report the information of the wireless device to the server over the network.

7. The system of claim 1 wherein:

the machine learning function is configured to identify sensitive information stored in memory of the user device that is susceptible to the security threat, to identify an incorrect data set in the memory of the user device that is associated with the sensitive information, and to provide the incorrect data set in response to a request to access the sensitive information.

8. The system of claim 7 further comprising:

a remote server that implements a machine learning system configured to receive information regarding the behavior of the security threat, and to provide the incorrect data set for

the user device based on a characteristic of the security threat output from the machine learning system.

9. The system of claim 1 wherein:

the hardware processor implements the machine learning function in one of a protected memory on top of an operating system kernel of the user device, or a hardware abstraction layer of the user device.

10. A method comprising:

communicating, via an interface component of a user device, with a server that manages cyber security for a plurality of user devices belonging to an enterprise;

implementing a machine learning function with a processor of the user device;

monitoring user interactions with the user device over time to establish a use profile;

detecting anomalous use of the user device based on a variance from the use profile;

identifying another user device managed by the server that is associated with the user device;

in response to detecting the anomalous use of the user device, sending an instruction to the another user device to validate whether an authorized user is in proximity of the another user device;

determining the anomalous use is representative of a security threat to the enterprise based on input of the anomalous use into the machine learning function;

controlling the user device to automatically initiate recording behavior of the security threat based on an output of the machine learning function;

reporting the behavior of the security threat to the server; and

analyzing, at the server, the behavior of the security threat to profile attack patterns for the user devices belonging to the enterprise.

11. The method of claim 10 further comprising:

responsive to detecting that the user device is compromised by the security threat, postponing, at the server, an invalidation of communication of the user device to the server via a network for a period of time; and

reporting the behavior of the security threat to the server over the network via the interface component during the period of time.

12. The method of claim 10 wherein further comprising:

the behavior of the security threat includes one or more of keystroke data, audio data, image data, application use data, or file access request data.

13. The method of claim 10 further comprising:

identifying sensitive information stored in memory of the user device that is susceptible to the security threat;

identifying an incorrect data set in the memory of the user device that is associated with the sensitive information; and

providing the incorrect data set in response to a request to access the sensitive information.

14. A non-transitory computer readable medium embodying programmed instructions executed by a processor, wherein the instructions direct the processor to:

communicate, via an interface component of a user device, with a server that manages cyber security for a plurality of user devices belonging to an enterprise;

implement a machine learning function with the user device;

monitor user interactions with the user device over time to establish a use profile;

detect anomalous use of the user device based on a variance from the use profile;

identify another user device managed by the server that is associated with the user device;

in response to detecting the anomalous use of the user device, send an instruction to the another user device to validate whether an authorized user is in proximity of the another user device;

determine the anomalous use is representative of a security threat to the enterprise based on input of the anomalous use into the machine learning function;

control the user device to automatically initiate recording behavior of the security threat in memory based on an output of the machine learning function;

report the behavior of the security threat to the server; and

analyze, at the server, the behavior of the security threat to profile attack patterns for the user devices belonging to the enterprise.

15. The computer readable medium of claim 14 wherein the instructions further direct the processor to:

in response to detecting that the user device is compromised by the security threat, postpone, at the server, an invalidation of communication of the user device to the server via a network for a period of time; and

report the behavior of the security threat to the server over the network via the interface component during the period of time.

16. The computer readable medium of claim 14 wherein:

the behavior of the security threat includes one or more of keystroke data, audio data, image data, application use data, or file access request data.

17. The computer readable medium of claim 14 wherein the instructions further direct the processor to:

identify sensitive information stored in memory of the user device that is susceptible to the security threat;

identify an incorrect data set in the memory of the user device that is associated with the sensitive information; and

provide the incorrect data set in response to a request to access the sensitive information.

18. An apparatus comprising:

a hardware processor configured to detect anomalous use of a user device based on historical use of the user device, to identify another user device that is associated with the user device, to send an instruction to the another user device to validate whether an authorized user is in proximity of the another user device in response to detecting the anomalous use of the user device, to input information of the anomalous use into a machine learning function, to determine a characteristic of a cyber threat from an output of the machine learning function, to initiate recording behavior of the cyber threat in memory based on the characteristic, and to report the

behavior of the cyber threat to a server that manages cyber security for the user device and other user devices belonging to an enterprise.

19. The apparatus of claim 18 wherein:

the hardware processor is configured, in response to determining that the characteristic of the cyber threat includes a threat to access a type of data via the user device, to instruct the user device to provide disinformation to respond to a request to access the type of data.

20. The apparatus of claim 18 wherein:

the hardware processor is configured, in response to determining that the characteristic of the cyber threat includes a threat to information leakage of data stored in memory of the user device, to instruct the user device to erase the data.

21. The apparatus of claim 18 wherein:

the hardware processor implements the machine learning function in a server that is remote from the user device.

22. A method comprising:

detecting anomalous use of a user device based on historical use of the user device;
identifying another user device that is associated with the user device;

in response to detecting the anomalous use of the user device, sending an instruction to the another user device to validate whether an authorized user is in proximity of the another user device;

inputting information of the anomalous use into a machine learning function;

determining a characteristic of a cyber threat from an output of the machine learning function;

initiate recording behavior of the cyber threat based on the characteristic; and

reporting the behavior of the cyber threat to a server that manages cyber security for the user device and other user devices belonging to an enterprise.

23. The method of claim 22 further comprising:

establishing, with the machine learning function, a communication pattern received by the device over a network interface;

detecting an intrusion event sequence in the communication pattern with the machine learning function; and

generating a graphical simulation of the intrusion event sequence.