US 20160182533A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2016/0182533 A1**

(43) **Pub. Date: Jun. 23, 2016**

Purpura

(54) **COMPUTER DEFENSES AND COUNTERATTACKS**

(71) Applicant: **The Boeing Company**, Chicago, IL (US)

(72) Inventor: **William J. Purpura**, Anaheim, CA (US)

(73) Assignee: **The Boeing Company**

(21) Appl. No.: **14/574,076**

(22) Filed: **Dec. 17, 2014**

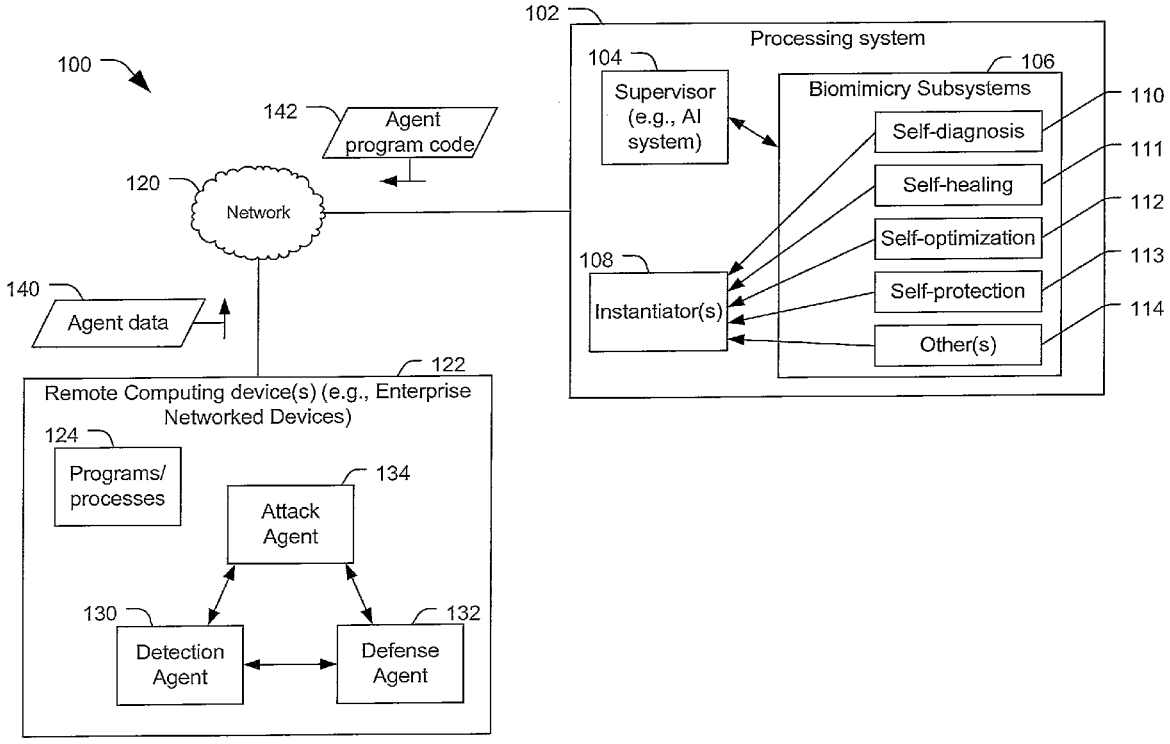
Publication Classification

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/145*** (2013.01)

(57) **ABSTRACT**

A method includes instantiating a first detection agent based on detection criteria, where the first detection agent includes first program code executable by a second computing device to monitor network activity. The method further includes sending the first program code of the first detection agent to the second computing device for execution. When the first program code of the first detection agent is executed at the second computing device, the first detection agent causes network activity data to be transmitted to a network monitor, and the network monitor updates the detection criteria based on the network activity data to generate updated detection criteria. The method also includes instantiating a second detection agent based on the updated detection criteria and sending second program code of the second detection agent to the second computing device for execution.



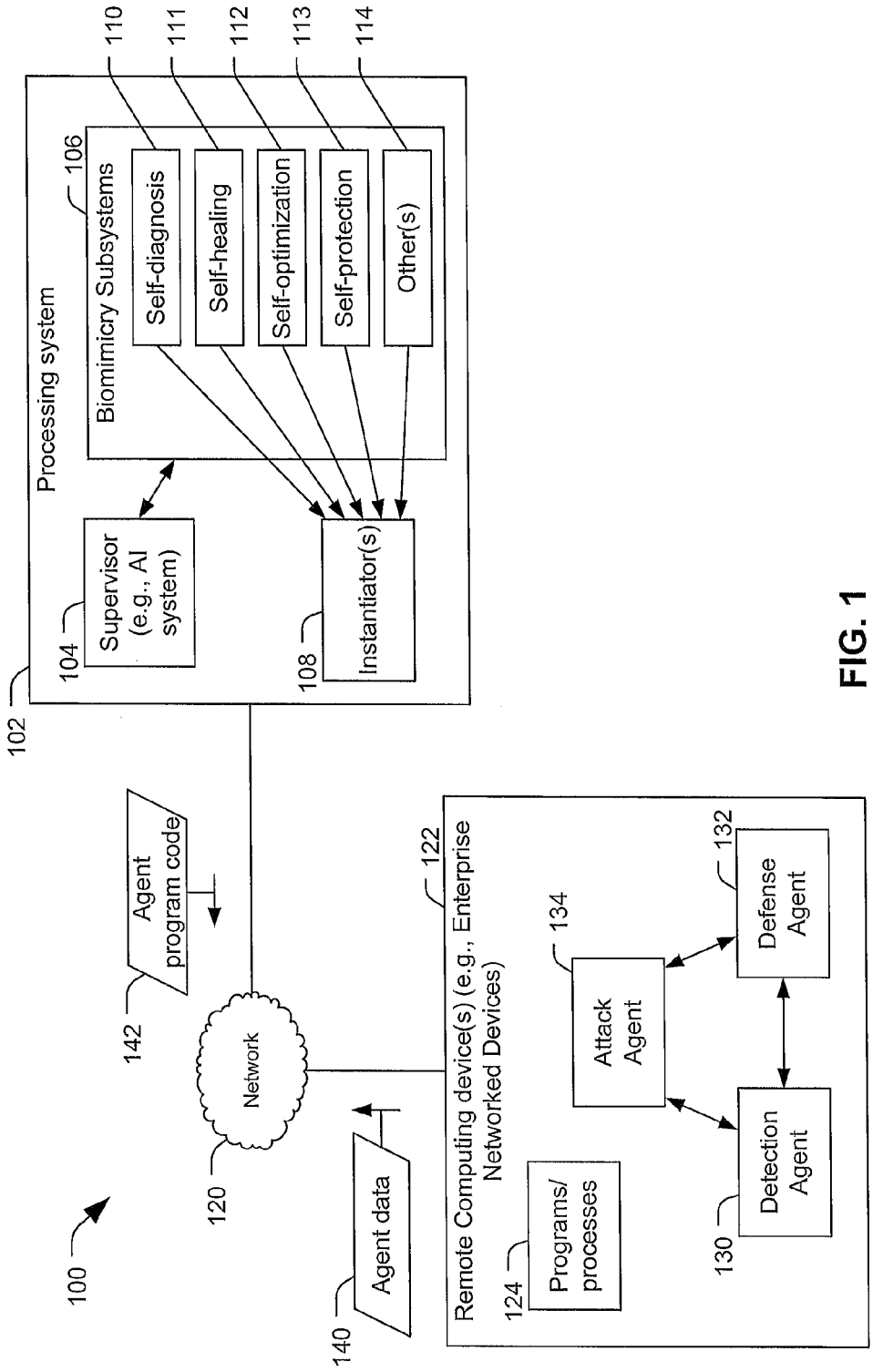

100
102
Processing system
104
Supervisor (e.g., AI system)
106
Biomimicry Subsystems
110
Self-diagnosis
111
Self-healing
112
Self-optimization
113
Self-protection
114
Other(s)
108
Instantiator(s)
120
Network
122
Remote Computing device(s) (e.g., Enterprise Networked Devices)
124
Programs/ processes
130
Detection Agent
132
Defense Agent
134
Attack Agent
140
Agent data
142
Agent program code

FIG. 1

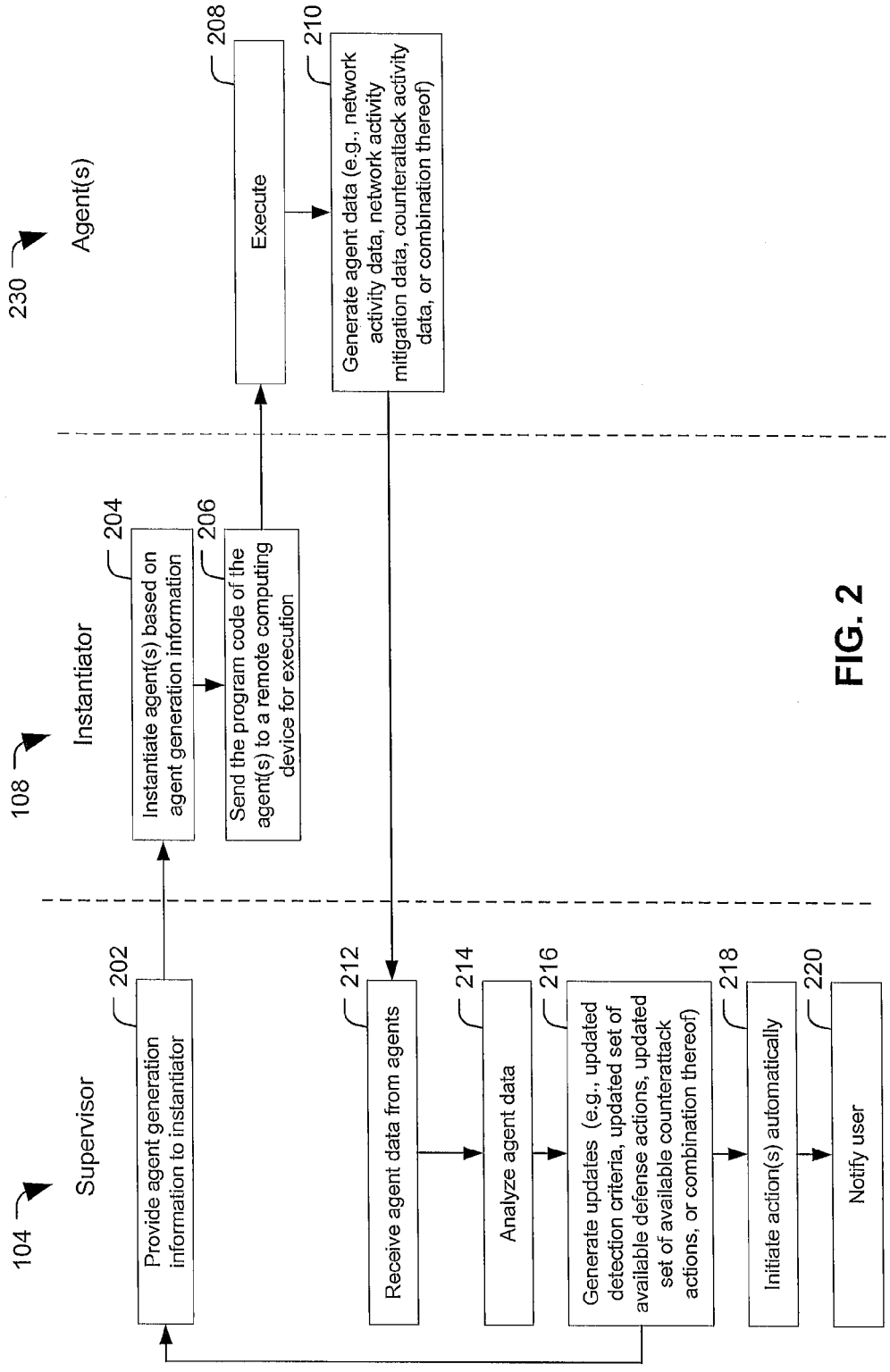

104
Supervisor
202
Provide agent generation information to instantiator
108
Instantiator
204
Instantiate agent(s) based on agent generation information
206
Send the program code of the agent(s) to a remote computing device for execution
230
Agent(s)
208
Execute
210
Generate agent data (e.g., network activity data, network activity mitigation data, counterattack activity data, or combination thereof)
212
Receive agent data from agents
214
Analyze agent data
216
Generate updates (e.g., updated detection criteria, updated set of available defense actions, updated set of available counterattack actions, or combination thereof)
218
Initiate action(s) automatically
220
Notify user

FIG. 2

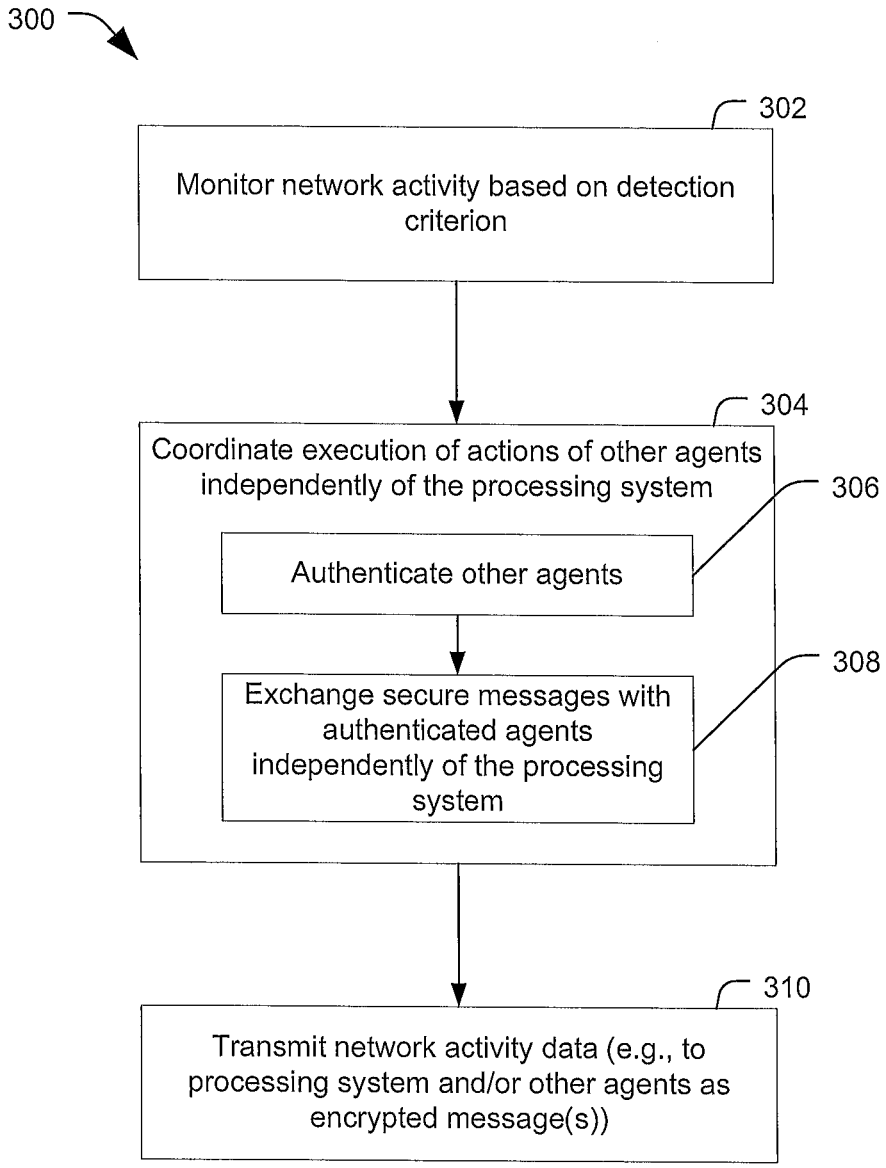

300
302
Monitor network activity based on detection criterion
304
Coordinate execution of actions of other agents independently of the processing system
306
Authenticate other agents
308
Exchange secure messages with authenticated agents independently of the processing system
310
Transmit network activity data (e.g., to processing system and/or other agents as encrypted message(s))

FIG. 3

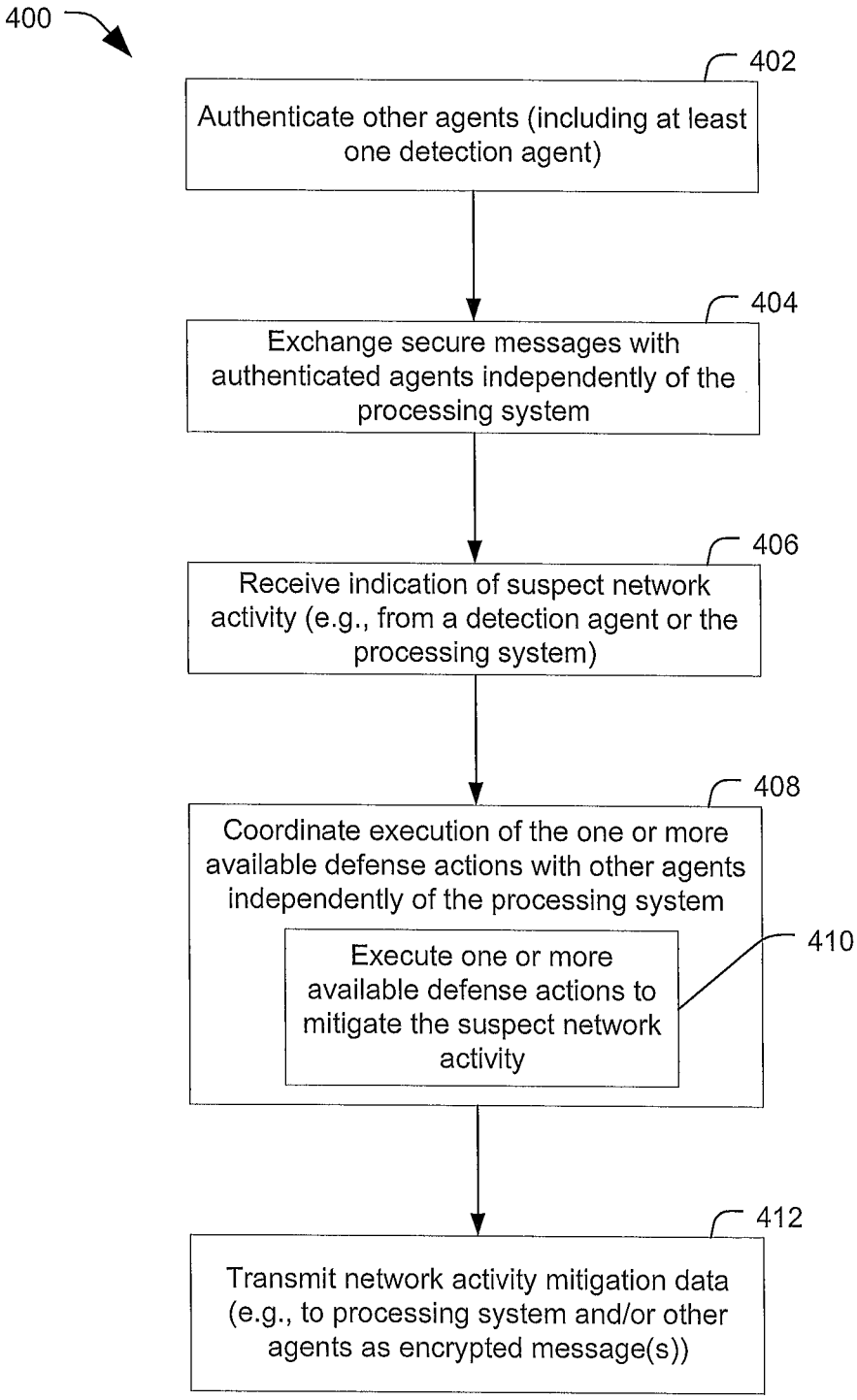

400
402
Authenticate other agents (including at least one detection agent)
404
Exchange secure messages with authenticated agents independently of the processing system
406
Receive indication of suspect network activity (e.g., from a detection agent or the processing system)
408
Coordinate execution of the one or more available defense actions with other agents independently of the processing system
410
Execute one or more available defense actions to mitigate the suspect network activity
412
Transmit network activity mitigation data (e.g., to processing system and/or other agents as encrypted message(s))

FIG. 4

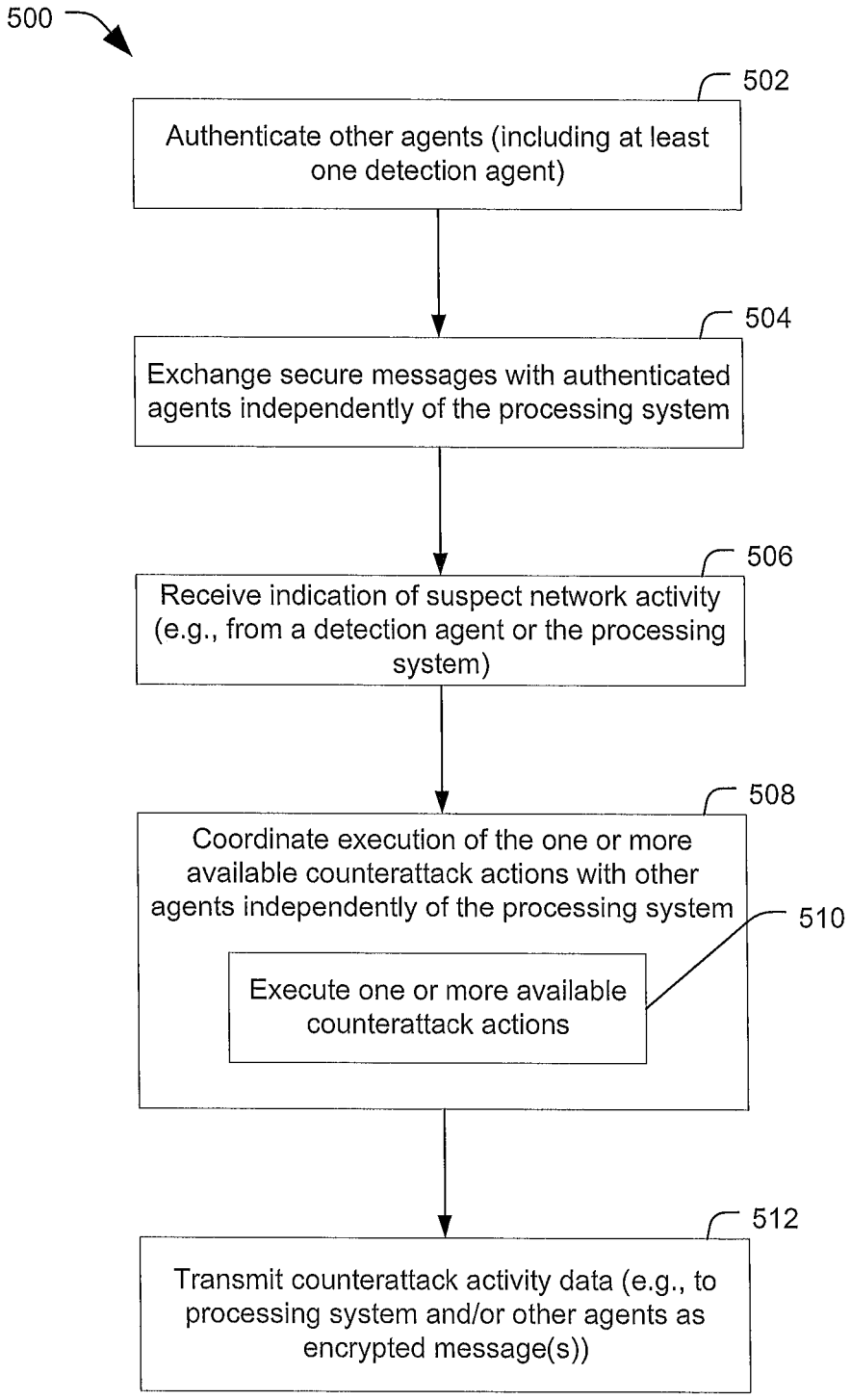

500
502
Authenticate other agents (including at least one detection agent)
504
Exchange secure messages with authenticated agents independently of the processing system
506
Receive indication of suspect network activity (e.g., from a detection agent or the processing system)
508
Coordinate execution of the one or more available counterattack actions with other agents independently of the processing system
510
Execute one or more available counterattack actions
512
Transmit counterattack activity data (e.g., to processing system and/or other agents as encrypted message(s))

FIG. 5

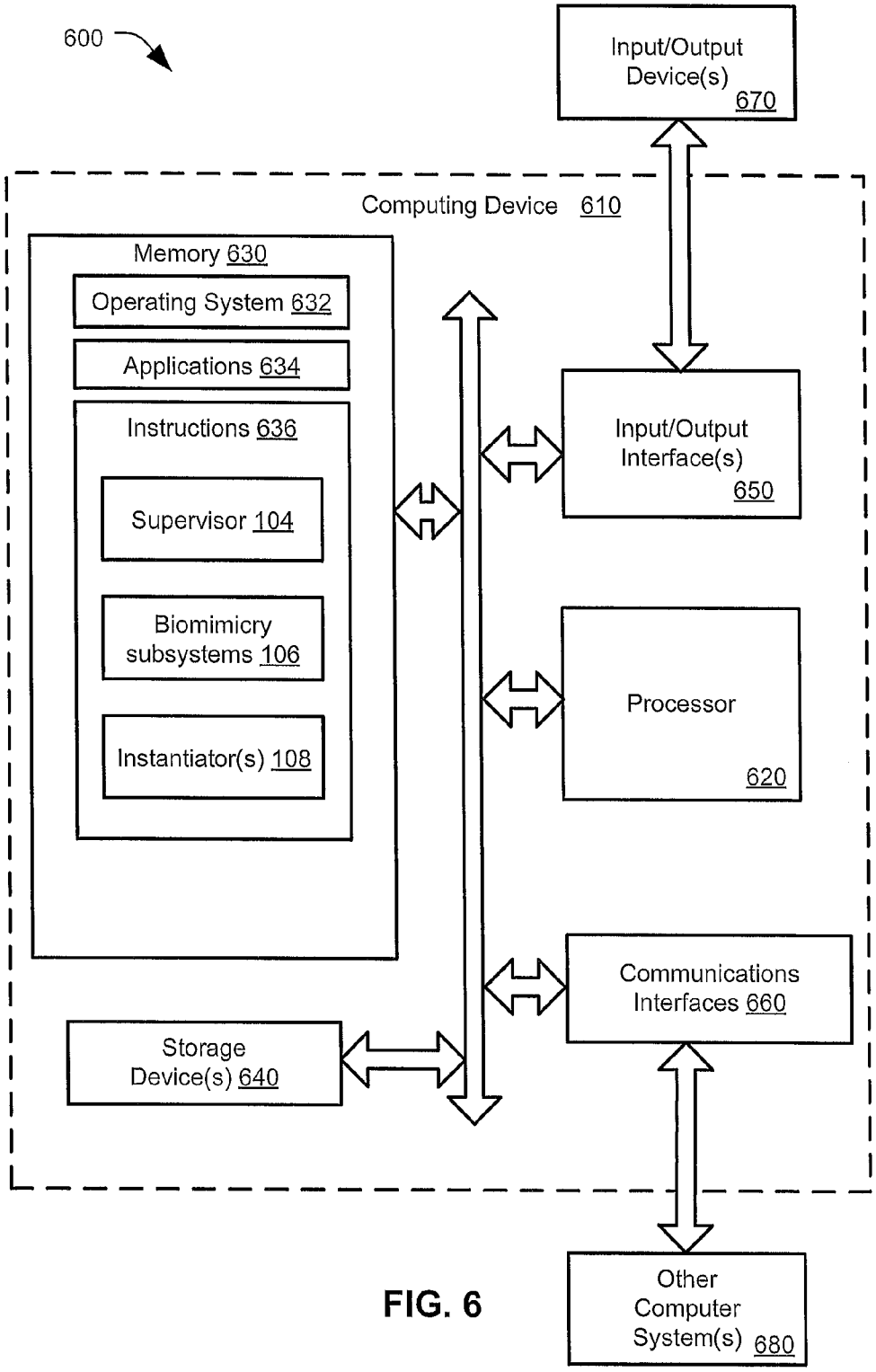

600
Input/Output Device(s) 670
Computing Device 610
Memory 630
Operating System 632
Applications 634
Instructions 636
Supervisor 104
Biomimicry subsystems 106
Instantiator(s) 108
Input/Output Interface(s) 650
Processor 620
Communications Interfaces 660
Storage Device(s) 640
Other Computer System(s) 680

FIG. 6

COMPUTER DEFENSES AND COUNTERATTACKS

FIELD OF THE DISCLOSURE

[0001] The present disclosure relates to systems and methods to defend computers and networks, as well as to conduct counterattacks.

BACKGROUND

[0002] Computer and network security typically focuses on defending a computer or a system of computers against attacks. New types of attacks are regularly developed. Accordingly, computer and network security providers frequently update monitoring software and other software to keep pace with the new types of attacks.

[0003] As a result of conventional methods of updating software after detection and analysis of a new type of attack, computer systems and networks are vulnerable for a period of time after the development of each new type of attack. Taking steps to reduce response times to new attack types may reduce vulnerability of computer systems and networks to attacks.

SUMMARY

[0004] In a particular embodiment, a system includes a processing system having one or more processors and memory accessible to the processing system. The memory stores instructions executable by at least one processor of the one or more processors to cause the at least one processor to perform operations including instantiating a first detection agent based on detection criteria. The first detection agent includes first program code executable by a second processor to monitor network activity. The operations also include sending the first program code of the first detection agent to a remote computing device for execution. When the first program code of the first detection agent is executed at the remote computing device, the first detection agent causes network activity data to be transmitted to the processing system, and the processing system updates the detection criteria based on the network activity data to generate updated detection criteria. The operations further include instantiating a second detection agent based on the updated detection criteria and sending second program code of the second detection agent to the remote computing device for execution.

[0005] In another particular embodiment, a method includes instantiating a first detection agent based on detection criteria, the first detection agent including first program code executable by a second computing device to monitor network activity. The method also includes sending the first program code of the first detection agent to the second computing device for execution. When the first program code of the first detection agent is executed at the second computing device, the first detection agent causes network activity data to be transmitted to a network monitor, and the network monitor updates the detection criteria based on the network activity data to generate updated detection criteria. The method also includes instantiating a second detection agent based on the updated detection criteria and sending second program code of the second detection agent to the second computing device for execution.

[0006] In another particular embodiment, a computer-readable storage device stores instructions that are executable by a processor to cause the processor to perform operations including instantiating a first detection agent based on detection criteria. The first detection agent includes first program code executable by a remote computing device to monitor network activity. The operations further include sending the first program code of the first detection agent to the remote computing device for execution. When the first program code of the first detection agent is executed at the remote computing device, the first detection agent causes network activity data to be transmitted to a network monitor, and the network monitor updates the detection criteria based on the network activity data to generate updated detection criteria. The operations also include instantiating a second detection agent based on the updated detection criteria and sending second program code of the second detection agent to the remote computing device for execution.

[0007] The features, functions, and advantages that have been described can be achieved independently in various embodiments or may be combined in yet other embodiments, further details of which are disclosed with reference to the following description and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. **1** is a diagram that illustrates a first particular embodiment of a computer defense and counterattack system;

[0009] FIG. **2** is a diagram that illustrates a method of computer defense that may be performed by the system of FIG. **1**;

[0010] FIG. **3** is a flow chart of a first particular embodiment of a method associated with a computing agent

[0011] FIG. **4** is a flow chart of a second particular embodiment of a method associated with a computing agent

[0012] FIG. **5** is a flow chart of a third particular embodiment of a method associated with a computing agent; and

[0013] FIG. **6** is a block diagram that illustrates a particular embodiment of a computing system of a computer defense and counterattack system.

DETAILED DESCRIPTION

[0014] Particular embodiments of the present disclosure are described below with reference to the drawings. In the description, common features are designated by common reference numbers throughout the drawings.

[0015] The figures and the following description illustrate specific exemplary embodiments. It will be appreciated that those skilled in the art will be able to devise various arrangements that, although not explicitly described or shown herein, embody the principles described herein and are included within the scope of the claims that follow this description. Furthermore, any examples described herein are intended to aid in understanding the principles of the disclosure and are to be construed as being without limitation. As a result, this disclosure is not limited to the specific embodiments or examples described below, but by the claims and their equivalents.

[0016] Embodiments described herein enable decentralized monitoring of and responding to network threats, which may improve response times to particular types of attacks. For example, a cyber defense system may utilize agents (executing at a plurality of computing devices) to autonomously gather information, perform defensive actions, perform offensive actions (e.g., counterattacks), or a combination thereof. Detection agents may gather information from many computing devices, such as computing devices coupled to an

enterprise network (e.g., client computers, routers, servers, control systems, etc.) and computing devices remote from the enterprise network (e.g., a computer suspected of threatening activity, etc.). Detection agents may send the information to other agents associated with the cyber defense system, to a controller (or supervisor) of the cyber defense system, or both. The controller may be a centralized or decentralized (e.g., distributed) system that analyzes the information and causes actions to be taken at one or more network devices. For example, the controller may be an artificial intelligence system that analyzes the information to detect potential threats and coordinates response actions at the enterprise network. Other agents associated with the cyber defense system may include other detection agents, attack agents, or defense agents.

[0017] Detection agents gather and report network activity data based on detection criteria. For example, a detection agent may execute at a computing device to gather information descriptive of processes executing at the computing device, to gather information descriptive of network communications from the perspective of the computing device, etc. Defense agents perform actions to reduce or mitigate a perceived threat. For example, a defense agent may execute at a computing device to perform a defense action (such as to close a network connection, to terminate an executing process, etc.). Attack agents perform offensive actions directed to a perceived source of a threat. For example, an attack agent executing at a computing device may perform actions such as causing a network connection of another device to be terminated or overwhelmed (e.g., a denial of service attack), to take over control of the other device, etc.

[0018] After deployment, a set of agents (e.g., detection agents, defense agents, and/or attack agents) may cooperate with one another independently of the cyber defense system. For example, a set of agents deployed by the cyber defense system may detect threats and take offensive or defensive action related to detected threats without input from the cyber defense system. The agents may provide information to the cyber defense system, such as descriptions of detected or suspicious network activity, response actions taken, results of response actions, etc. The information provided to the cyber defense system may enable the cyber defense system to generate (e.g., instantiate or compile) new agents that are better capable of detecting or dealing with a particular threat, to send agents to new or different computing systems, or to otherwise improve protection of a network associated with the cyber defense system.

[0019] The controller may remotely control, disable or replace the agents as needed. For example, in response to information received from a detection agent that indicates existence of a new type of attack, the controller may cause one or more new agents (e.g., new detection agents, new defense agents, new attack agents, or a combination thereof), to be instantiated and sent to a remote computing device for execution to replace or to supplement agents already executing at the remote computing device ("old agents"). When the new agents replace the old agents, the controller may cause the old agents to be deactivated. The new agents may be configured to respond to the new type of attack (e.g., may include program code that is executable to perform actions to mitigate the new type of attack). Alternately, the controller may send a signal that causes one or more agents that are already deployed (e.g., old agents) to activate to address the new type of attack if the controller determines that the old agents are capable of responding to the new type of attack. Thus, the cyber defense system enables fast and tailored response to new threats.

[0020] FIG. **1** illustrates a first particular embodiment of a computer defense and counterattack system **100**. The system **100** includes a processing system **102** of a cyber defense system. The processing system **102** may include one or more computing devices or processors. For example, the processing system **102** may include a single computing device, such as a server device, or may be a distributed system including multiple computing devices. The processing system **102** may be coupled via a network **120** to one or more remote computing devices **122**. For example, the remote computing devices **122** may include one or more devices of an enterprise network that is protected by the processing system **102**, one or more computing devices associated with suspicious activity (e.g., a perceived threat), other computing devices, or a combination thereof. The remote computing devices **122** may include client computing devices (e.g., an end user device or a work station) or other types of computing devices (e.g., routers, switches, servers, control systems, or other computing devices).

[0021] The processing system **102** may include a plurality of subsystems, which are depicted as distinct functional blocks in FIG. **1**. For example, the subsystems may include a supervisor application **104** (e.g., a controller), a biomimicry subsystem **106** and/or instantiators **108**. Representation of the subsystems as functional blocks in FIG. **1** is intended to simplify description of different actions associated with or performed by the subsystems and is not meant to imply that distinct software or hardware is associated with each functional block. To illustrate, functions described as performed by the supervisor application **104** may be executed by a first computing device, functions described as performed by the biomimicry subsystems **106** may be executed at a second computing device, and functions described as performed by the instantiators **108** may be executed at a third computing device. Alternatively, the functions performed by the supervisor application **104**, functions performed by the biomimicry subsystems **106**, and functions performed by the instantiators **108** may be executed at a single computing device. Other combinations are also possible, such as execution of the functions performed by the supervisor application **104** and the instantiators **108** at a first computer and execution of the functions performed by the biomimicry subsystems **106** at a second computer. Further, any or all of the functional blocks may be executed in whole or in part at multiple computing devices. To illustrate, functions performed by the supervisor application **104** may be executed at multiple computing devices such that each of the multiple computing devices independently performs all of the functions or such that each of the multiple computing devices performs a subset of the functions.

[0022] In a particular embodiment, the supervisor application **104** may include an artificial intelligence (AI) system that is adapted to process information to assess network security, to make determinations regarding options for responding to network security issues, to provide an interface to users (such as network security administrators), or a combination thereof. The biomimicry subsystems **106** may include subsystems that provide specific functionality to the network to sustain or improve operation of the network. For example, the biomimicry subsystems **106** may include a self-diagnosis subsystem **110** that is adapted to identify and diagnose (e.g., identify potential causes of) network performance concerns,

such as connectivity issues (e.g., loss of a communication connection), reduced data rates, etc. As another example, the biomimicry subsystems **106** may include a self-healing system **111** that is adapted to perform actions to attempt to repair network performance concerns detected by the self-diagnosis subsystem **110**. To illustrate, the self-healing system **111** may attempt to re-establish a lost data connection or attempt to reroute data to avoid the lost data connection. As another example, the biomimicry subsystems **106** may include a self-optimization subsystem **112** adapted to perform optimization operations, such as load balancing, to improve operation of the network or operation of specific subsystems of the network. As yet another example, the biomimicry subsystems **106** may include a self-protection subsystem **113**. The self-protection subsystem **113** may be adapted to perform computer monitoring, defense actions, and attack actions as described herein. The biomimicry subsystems **106** are not limited to the specific subsystems described above. Rather, the biomimicry subsystems **106** may include other subsystems **114** in addition to or instead of the subsystems **110-113** described above.

[0023] The instantiators **108** are adapted to generate (e.g., instantiate or compile) executable code based on parameters or instructions provided by various subsystems of the biomimicry subsystems **106**. To illustrate, the self-optimization subsystem **112** may provide parameters or instructions to the instantiators **108** to generate code that is executable at a remote computing device, such as the remote computing device **122**, to optimize (or improve in some respect) performance of the remote computing device or performance of the network **120**. As a specific example, the performance may be improved by changing a quality of service parameter associated with particular network communications to or from the remote computing device **122**. In another example, the instantiators **108** may be adapted to generate executable code of various cyber security agents at the direction of, or based on, parameters or criteria provided by the self-protection subsystem **113**. The cyber security agents may include detection agents **130**, attack agents **134**, defense agents **132** or a combination thereof. The program code generated by the instantiators **108** may be executable on a particular platform (e.g., an operating system of a particular remote computing device) or may be cross-platform compatible.

[0024] Agents generated by the instantiators **108** may be sent as agent program code **142** via the network **120** to remote computing devices, such as the remote computing devices **122**. The remote computing devices **122** may execute the agent program code **142** to perform actions based on the agent program code **142**. To illustrate, when the agent program code **142** corresponds to a detection agent **130**, the remote computing device **122** may execute the detection agent **130** to monitor network activities, to monitor activities or processes implemented by one or more programs or processes **124** executing on the remote computing device **122**, or to perform other monitoring actions based on detection criteria specified by the agent program code **142** of the detection agent **130**. The detection agent **130** may generate data, such as agent data **140**, which may be transmitted from the remote computing device **122** via the network **120** to the processing system **102**. The supervisor application **104** may analyze the agent data **140** and may take one more actions based on the agent data **140**. For example, the supervisor application **104** may provide instructions to the biomimicry subsystems **106** to utilize one or more of the biomimicry subsystems **106** to generate additional agents, to generate different types of agents, or to provide agents to different computing devices (e.g., other remote computing device).

[0025] In another example, when the agent program code **142** corresponds to an attack agent **134**, the remote computing device **122** may execute the agent program code **142** to perform one or more counterattack actions specified by the agent program code **142** of the attack agent **134**. To illustrate, the attack agent **134** may receive information from the detection agent **130** and may perform a counterattack action based on the information received from the detection agent **130**.

[0026] In a particular embodiment, the detection agent **130** may provide information to the attack agent **134** independently of the processing system **102**. For example, a detection agent executing at a particular remote computing device (such as the detection agent **130** executing at the remote computing device **122**) may provide information via encrypted communications directly to an attack agent (such as the attack agent **134**) executing at the same remote computing device or executing at a different remote computing device. The attack agent **134** may perform a counterattack action without awaiting an instruction from the supervisor application **104** or other components of the processing system **102**.

[0027] As another example, when the agent program code **142** corresponds with a defense agent **132**, the remote computing device **122** may execute the agent program code **142** to perform one or more defense actions specified by the agent program code **142** of the defense agent **132**. To illustrate, the defense agent **132** may perform defense actions responsive to information received from a detection agent executing at a particular remote computing device (such as the detection agent **130** executing at the remote computing device **122**). To illustrate, the detection agent **130** may detect suspicious activity and provide a communication via an encrypted message to the defense agent **132**. The defense agent **132** may take a defense action, such as terminating a process executing at the remote computing device **122**, based on the encrypted message.

[0028] Defense agents and attack agents (such as the defense agent **132** and the attack agent **134**) may also interact with one another to coordinate activities independently of the processing system **102**. To illustrate, the defense agent **132** may provide a secure communication to the attack agent **134** indicating that the defense agent **132** has or will perform a particular defense action. The attack agent **134** may perform a counterattack action responsive to the communication. Similarly, the detection agent **130** may take actions based on information provided by the attack agent **134**, the defense agent **132**, or both. To illustrate, the detection agent **130** may monitor particular network activities or particular programs or processes **124** based on secure communications (from the attack agent **134**, the defense agent **132**, or both) that particular actions have been performed or will be performed by the corresponding agents. Thus, each agent **130-134** executing at the remote computing device **122** may take action independently of the processing system **102** and/or in coordination with other agents at the remote computing device **122** to provide cyber security to the network **120**.

[0029] In operation, the supervisor application **104** may cause the self-protection subsystem **113** to instruct the instantiators **108** to instantiate (e.g., compile) a detection agent based on particular detection criteria. In a particular embodiment, the detection criteria may specify, for example, particu-

lar types of network activity to be monitored, particular circumstances under which information is to be to provided to other agents or to the processing system **102**, types of information to be reported, timing of gathering or reporting information, or combinations thereof. The detection agent may be instantiated as program code that is executable by a processor to monitor network activity. For example, the detection agent **130** may correspond to or include the agent program code **142**.

[0030] The processing system **102** may send the agent program code **142** to a remote computing device, such as the remote computing device **122**, for execution. When the agent program code **142** corresponding to the detection agent **130** is executed at the remote computing device **122**, the detection agent **130** gathers information, such as network activity data, and transmits the information, e.g., as the agent data **140**, to the processing system **102**, to other agents (e.g., the defense agent **132** or the attack agent **134**), or both. The processing system **102** may take actions based on the agent data **140**. For example, the supervisor application **104** may analyze the agent data **140** to determine updated detection criteria. The updated detection criteria may be provided to the self-protection subsystem **113** which may cause the instantiators **108** to generate an updated detection agent which may be transmitted, as agent program code **142**, to the remote computing device **122** or to another remote computing device for execution. When executed, the updated detection agent may supplement the detection agent **130** or may replace the detection agent **130**. The detection agent **130** may be adapted to detect network activity based on a first network detection criterion, and the updated detection agent may be adapted to detect network activity based on a second detection criteria that is distinct from the first detection criteria. For example, the detection agent **130** may detect network activity associated with a connection to the network **120**, and the updated detection agent may detect network activity associated with a specific program or process of the programs or processes **124** executing at the remote computing device **122**.

[0031] In a particular embodiment, the supervisor application **104** may perform an analysis of the agent data **140** and may initiate one or more actions automatically, i.e., without human intervention, based on the analysis. Additionally, the supervisor application **104** may notify a human operator of the agent data **140**, of results of analysis of the agent data **140**, of actions automatically performed based on the agent data **140** or the results of the analysis, or a combination thereof.

[0032] Additionally or in the alternative, during operation, the processing system **102** may cause a defense agent to be instantiated. For example, the supervisor application **104** may instruct the self-protection subsystem **113** to generate one or more defense agents. The self-protection subsystem **113** may provide instructions and/or criteria to the instantiators **108** to cause the instantiators **108** to generate one or more defense agents. A particular defense agent may be sent, as the agent program code **142**, via the network **120** to the remote computing device **122** for execution as the defense agent **132**. When the defense agent **132** is executed at the remote computing device **122**, the defense agent **132** may perform mitigation activities and may cause network activity mitigation data to be transmitted, as agent data **140**, to the processing system **102** or to other agents. The network activity mitigation data may indicate actions taken by the defense agent **132**, suspicious activity that triggered the defense actions, responses to the defense actions, or any combination thereof.

[0033] Additionally or in the alternative, during operation, the processing system **102** may cause one or more attack agents to be instantiated. For example, the supervisor application **104** may instruct the self-protection subsystem **113** to cause one or more attack agents to be instantiated by the instantiators **108** based on particular criteria. A particular attack agent may be transmitted, as agent program code **142**, via the network **120** to a remote computing device, such as remote computing device **122**, for execution. The attack agent **134**, when executed by the remote computing device **122**, may automatically perform offensive actions, such as a counterattack. The particular actions that are performed by the attack agent **134** may be specified by the agent program code **142** corresponding to the attack agent **134**. Additionally, the attack agent **134** may cause counterattack activity data to be transmitted, as agent data **140**, to the processing system **102** or to other agents. The counterattack activity data may indicate actions taken by the attack agent **134**, activity that triggered the actions, responses to the actions, or any combination thereof.

[0034] In a particular embodiment, the supervisor application **104** may cause the self-protection subsystem **113** to have instantiated an updated (or new) agent based on the agent data **140** received from an agent executing at a remote computing device (such as one of the agents **130-134** executing at the remote computing device **122**). The updated (or new) agent may be instantiated to have functionality or capabilities different from or in addition to the agent that provided the agent data **140**. For example, the agent data **140** may be received from a detection agent, such as the detection agent **130**, and the updated (or new) agent may include a defense agent, an attack agent, or a detection agent with different or additional detection criteria. As another example, the agent data **140** may be received from a defense agent, such as the defense agent **132**, and the updated (or new) agent may include a detection agent, an attack agent, or a defense agent capable of performing different defense actions or performing defense actions in a different manner or in response to different criteria than the defense agent that sent the agent data **140**. As yet another example, the agent data **140** may be received from an attack agent, such as the attack agent **134**, and the updated (or new) agent may include a detection agent, a defense agent, or an attack agent capable of performing different counterattack actions or performing counterattack actions in a different manner or in response to different criteria than the attack agent that sent the agent data **140**. Further, more than one update (or new) agent may be generated based on the agent data **140**.

[0035] As a specific example, when the agent data **140** is received at the processing system **102**, the supervisor application **104** may analyze the agent data **140** and determine appropriate counterattack measures or counterattack processes to be implemented by an attack agent based on the agent data **140**. The supervisor application **104** may provide information indicating the particular counterattacks or the particular threat that triggered instantiation of the attack agent to the self-protection subsystem **113**. The self-protection subsystem **113** may cause one or more attack agents to be instantiated by the instantiators **108** and transmitted as agent program code **142** to the remote computing device **122** or another remote computing device.

[0036] While executing at the remote computing device, various agents, such as the detection agent **130**, the defense agent **132**, and the attack agent **134** may act independently of

the processing system **102** to coordinate activities, such as detection activities, counterattack activities and defense activities. Additionally, the agents **130-134** may share information with one another via secure communications and may provide agent data **140** to the processing system **102**. Information provided to the supervisor application **104** may enable the supervisor application **104** to analyze actions performed by the agents, to analyze data detected by the agents, to update operation of the agents (e.g., by instantiating and distributing new agents), or to modify operation of the agents (e.g., by sending secure messages to the agents to cause the agents to cease operation or to transition from a dormant state to an active state). For example, the processing system **102** may cause the agents **130-134** to be instantiated with a shared encryption key that enables the agents **130-134** to share secured communications with one another or with the processing system **102**.

[0037] Accordingly, the agents **130-134** may operate in a "fire and forget" manner (e.g., may perform actions autonomously or in coordination with one another) to provide cyber security for a network associated with the processing system **102**. The agents **130-134** may be configured to infiltrate other systems (e.g., the remote computing device **122**) to monitor, degrade, destroy and/or control the other systems. In a particular embodiment, one or more of the agents **130-134** may hibernate or await execution until particular circumstances are present (such as arrival of a particular time or date, receipt of a wake up signal, execution of a particular program or process, etc.). For example, the attack agent **134** may execute responsive to detection of particular network activities by the detection agent **130**. Thus, one or more of the agents **130-134** may cause execution of another agent responsive to actions detected at the remote computing device independently of the processing system **102**. While hibernating or while executing, the agents **130-134** may emulate trusted components of the remote computing device **122** to avoid detection (e.g., by the remote computing device **122** or by other cyber defense systems). An example of emulating a trusted component is for one or more of the agents **130-134** to mirror a normal operational rhythm of a trusted device by monitoring the typical operational signature (e.g., rhythm) of the trust device before the agent commences active operation based on the signature (or rhythm).

[0038] FIG. **2** illustrates a particular embodiment of a method that may be performed by the system **100** of FIG. **1**. FIG. **2** illustrates the supervisor application **104**, the instantiators **108** and one or more agents **230**. The one or more agents **230** may include detection agents, defense agents, attack agent, or a combination thereof. In a particular embodiment, the supervisor application **104** may provide agent generation information via one or more biomimicry subsystems **106** to the instantiators **108**, at **202**. The instantiators **108** may generate agent program code based on the agent generation, at **204**. The instantiators **108** may send the agent program code to a remote computing device for execution, at **206**. At **208**, the one or more agents **230** may be executed at the remote computing device. While executing, the one or more agents **230** may generate agent data, such as network activity data, network activity mitigation data, or counterattack data, at **210**. The agent data may be sent to other agents, to the supervisor application **104**, or both.

[0039] The supervisor application **104** may receive the agent data from the one or more agents, at **212**. The supervisor application **104** may analyze the agent data, at **214**, and may generate updates to agent generation information, at **216**. For example, the updates may include updated detection criteria, an updated set of defense actions, an updated set of available counterattack actions, or combination thereof. Additionally or in the alternative, the supervisor application **104** may initiate one or more actions automatically, at **218**. For example, the supervisor application **104** may perform actions at a local computing device, such as one or more processing devices of the processing system **102** of FIG. **1**. To illustrate, the supervisor application **104** may change settings or other programs or processes executing at the computing device. The supervisor application **104** may also, or in the alternative, notify a user, at **220**. For example, the supervisor application **104** may notify a network security administrator of information received via the agent data, results of analysis of the agent data, actions automatically performed by the supervisor application **104**, or a combination thereof. After generating updates, at **216**, the supervisor application **104** may provide updated agent data to the instantiators **108**, at **202**. Thus, the supervisor application **104**, the instantiators **108** and the one or more agents **230** may collaborate and take actions independently to provide network security to an enterprise network.

[0040] FIG. **3** is a flow chart of a particular embodiment of a method **300** that may be performed by a detection agent executing at a computing device, such as the remote computing device **122**. The method **300** includes monitoring network activity based on detection criteria, at **302**. For example, the detection agent **130** executing at the remote computing device **122** of FIG. **1** may monitor particular activity or actions on a network (such as the network **120**), particular processes or programs executing at the remote computing device **122** (such as the programs and processes **124**), or other activities based on detection criteria specified by the agent program code **142** of the detection agent **130**.

[0041] The method **300** also includes, at **304**, coordinating execution of actions with other agents independently of the processing system. For example, the detection agent may authenticate other agents, at **306**, via secure communication and may exchange secure messages with authenticated agents independently of the processing systems, at **308**. The secure messages may be used by the detection agent and the other agents to coordinate activities and to provide information to the processing system. For example, the agents **130-134** of FIG. **1** may include authentication information that may be used to exchange authentication information between the agents **130-134**. The agents **130-134** may include encryption information (such as shared key or public key/private key data) that may be used to send secure (e.g., encrypted) information between the agents **130-134**, or to the processing system **102**.

[0042] The method **300** also includes, at **310**, transmitting network activity data via encrypted messages to the processing system, to other agents, or both. Thus, the process flow illustrated in FIG. **3** may enable a detection agent executing at a remote computing device to detect suspicious activity based on detection criteria and to notify the processing system and/or other agents to the suspicious activity. The processing system may use the network activity data to generate a new agent (e.g., a new detection agent, a new defense agent, or a new attack agent) based on updated criteria (e.g., new detection criteria, a new set of available defense actions, a new set of available attack actions, or new criteria for executing or selecting particular available actions). The new agent may be

provided to the remote computing device or to another computing device for execution. Additionally or in the alternative, other agents may use information provided by the defense agent to select and/or execute particular response actions, such as counterattack actions or defense actions.

[0043] FIG. **4** is a flow chart of a particular embodiment of a method **400** that may be performed by a defense agent executing at a computing device, such as the defense agent **132** executing at the remote computing device **122** of FIG. **1**. The method **400** may include, at **402**, authenticating one or more agents, such as one or more detection agents executing at the same remote computing system as the defense agent or executing at another computing system. For example, the defense agent **132** of FIG. **1** may authenticate other agents (e.g., the agents **130** and **134**) via secure communication and may exchange secure messages with authenticated agents independently of the processing systems **102**. The secure messages may be used by the defense agent **132** and the other agents **130** and **134** to coordinate activities and to provide information to the processing system **102**. To illustrate, as explained above, the agents **130-134** of FIG. **1** may include authentication information that may be used to exchange authentication information between the agents **130-134**. The agents **130-134** may include encryption information (such as shared key or public key/private key data) that may be used to send secure (e.g., encrypted) information between the agents **130-134**, or to the processing system **102**.

[0044] The method **400** may also include, at **404**, exchanging secure messages with one or more authenticated agents independently of the processing system. For example, two or more agents executing at the same remote computing system may exchange secure messages at the remote computing system without transmitting messages via a network, such as the network **120** of FIG. **1**. As another example, an agent executing at a first remote computing system may provide information to an agent executing at a second remote computing system via a secure message without providing the information to the processing system or via a broadcast sent to both the processing system and the other agent.

[0045] The method **400** also includes, at **406**, receiving an indication of suspect network activity. For example, the detection agent **130** or the processing system **102** may provide information to the defense agent **132**. The information may indicate suspect network activity based on detection criteria, the information may direct the defense agent **132** to perform particular defensive actions, or both.

[0046] The method **400** also includes, at **408**, coordination of one or more available defense actions with other agents independent of the processing system. For example, the defense agent **132** may coordinate selection or execution of a particular defense action with selection or execution of another defense action by another defense agent (not shown) executing at the remote computing device **122** or executing at another computing device. The defense action may be selected from a set of available defense actions that include actions that the defense agent **132** is capable of performing based on agent program code **142** of the defense agent **132**. As another example, the defense agent **132** may coordinate selection or execution of a particular defense action with selection or execution of a particular counterattack action by the attack agent **134**. As yet another example, the defense agent **132** may coordinate selection or execution of a particular defense action with the detection agent **130**. To illustrate, the detection agent **130** may send a secure message to the defense agent **132** that triggers selection and/or execution of the particular defense action by the defense agent **132**.

[0047] The method **400** also includes, at **410**, executing the one or more available defense actions to mitigate the suspect network activity. For example, the defense agent **132** may execute a defense action to block a network connection, to reroute data, to isolate (e.g., sandbox) a program or process, etc.

[0048] The method **400** may also include, at **412**, transmitting network activity mitigation data to the processing system, to other agents, or to both, as encrypted messages. For example, before, during or after execution of a particular defense action, the defense agent **132** may provide information to the processing system **102** or to the other agents **130** and **134** identifying the particular action to be performed, indicating a response to the particular action, or providing other information related to the particular action.

[0049] Thus, the process flow illustrated in FIG. **4** may enable a defense agent executing at a remote computing device to autonomously perform one or more defense actions of a set of available defense action and to notify the processing system and/or other agents of actions taken or results of such actions. The processing system may use the information received from the defense agent to generate new or updated agent criteria, which may be used to instantiate a new agent (e.g., a new detection agent, a new defense agent or a new attack agent) based on updated criteria (e.g., new detection criteria, a new set of available defense actions, a new set of available attack actions, or new criteria for executing or selecting particular available actions). The new agent may be provided to the remote computing device or to another computing device for execution. Additionally or in the alternative, other agents may use the information provided by the defense agent to select and/or execute other response actions, such as counterattack actions.

[0050] FIG. **5** is a flow chart of a particular embodiment of a method **500** that may be performed by an attack agent executing at a computing device, such as the attack agent **134** executing at the remote computing device **122** of FIG. **1**. The method **500** may include, at **502**, authenticating one or more agents, such as one or more detection agents executing at the same remote computing system as the defense agent or executing at another computing system. For example, the attack agent **134** of FIG. **1** may authenticate other agents (e.g., the agents **130** and **132**) via secure communication and may exchange secure messages with authenticated agents independently of the processing systems **102**. The secure messages may be used by the attack agent **134** and the other agents **130** and **132** to coordinate activities and to provide information to the processing system **102**. To illustrate, as explained above, the agents **130-134** of FIG. **1** may include authentication information that may be used to exchange authentication information between the agents **130-134**. The agents **130-134** may include encryption information (such as shared key or public key/private key data), which may be used to send secure (e.g., encrypted) information between the agents **130-134**, or to the processing system **102**.

[0051] The method **500** may also include, at **504**, exchanging secure messages with one or more authenticated agents independently of the process system. For example, two or more agents executing at the same remote computing system may exchange secure messages at the remote computing system without transmitting messages via a network, such as the network **120** of FIG. **1**. As another example, an agent execut-

ing at a first remote computing system may provide information to an agent executing at a second remote computing system via a secure message without providing the information to the processing system or via a broadcast sent to both the processing system the other agent.

[0052] The method **500** also includes, at **506**, receiving an indication of suspect network activity. For example, the detection agent **130** or the processing system **102** may provide information to the attack agent **134**. The information may indicate suspect network activity based on detection criteria, may direct the attack agent **134** to perform particular defensive actions, or both.

[0053] The method **500** also includes, at **508**, coordination of one or more available counterattack actions with other agents independent of the processing system. For example, the attack agent **134** may coordinate selection or execution of a particular counterattack action with selection or execution of another counterattack action by another attack agent (not shown) executing at the remote computing device **122** or executing at another computing device. The available counterattack actions may include actions that the attack agent **134** is capable of performing based on agent program code **142** of the attack agent **134**. As another example, the attack agent **134** may coordinate selection or execution of a particular counterattack action with selection or execution of a particular defense action by the defense agent **132**. As yet another example, the attack agent **134** may coordinate selection or execution of a particular counterattack action of an available counterattack action with the detection agent **130**. To illustrate, the detection agent **130** may send a secure message to the attack agent **134** that triggers selection and/or execution of the particular counterattack action by the attack agent **134**.

[0054] The method **500** also includes, at **510**, executing the one or more available counterattack actions. For example, the attack agent **134** may execute a counterattack action to terminate a program or process, to isolate (e.g., sandbox) a program or process, to take over control of a program, a process or a computing device, etc.

[0055] The method **500** may also include, at **512**, transmitting counterattack activity data to the processing system, to other agents, or both, as encrypted messages. For example, before, during or after execution of a particular available counterattack action, the attack agent **134** may provide information to the processing system **102** or to the other agents **130** and **132** identifying the particular action to be performed, indicating a response to the particular action, or providing other information related to the particular action.

[0056] Thus, the process flow illustrated in FIG. **5** may enable an attack agent executing at a remote computing device to autonomously perform one or more counterattack actions of a set of available counterattack action and to notify the processing system and/or other agents of actions taken or results of such actions. The processing system may use the information received from the attack agent to generate new or updated agent criteria, which may be used to instantiate a new agent (e.g., a new detection agent, a new defense agent or a new attack agent) based on updated criteria (e.g., new detection criteria, a new set of available defense actions, a new set of available attack actions, or new criteria for executing or selecting particular available actions). The new agent may be provided to the remote computing device or to another computing device for execution. Additionally or in the alternative, other agents may use the information provided by the attack agent to select and/or execute other response actions, such as defense actions.

[0057] Referring to FIG. **6**, a block diagram of a computing environment is shown and generally designated **600**. The computing environment **600** includes a computing device **610** to support embodiments of computer-implemented methods and computer-executable program instructions (or code) according to the present disclosure. For example, the computing device **610**, or portions thereof, may execute instructions to provide security for a network. In a particular embodiment, the computing device **610** may include, may be included with, or may correspond to the system **100** of FIG. **1**. For example, the computing device **610** may execute the supervisor application **104** (or a portion thereof when the supervisor application **104** is a distributed application), may execute the biomimicry subsystems **106** (or a portion thereof when the biomimicry subsystems **106** are distributed), may execute the instantiators **108** (or a portion thereof when the instantiators **108** are distributed), or a combination thereof. Alternatively, the computing device **610** may include or correspond to the remote computing device **122**, which may execute one or more agents, such as the agents **130**-**134**.

[0058] The computing device **610** may include a processor **620** of FIG. **1**. The processor **620** may communicate with a memory **630**. The memory **630** may include volatile memory devices (e.g., random access memory (RAM) devices), nonvolatile memory devices (e.g., read-only memory (ROM) devices, programmable read-only memory, and flash memory), or both. The memory **630** may store data and/or instructions that are executable by the processor **620**. For example, the memory **630** may store an operating system **632**, which may include a basic/input output system for booting the computing device **610** as well as a full operating system to enable the computing device **610** to interact with users, other programs, and other devices. The memory **630** may include one or more application programs **634**. For example, the application programs **634** may correspond to the programs and processes **124** of FIG. **1**. The memory **630** may include instructions **636** corresponding to the supervisor application **104**, the biomimicry subsystems **106**, the instantiators **108**, or a combination thereof.

[0059] The processor **620** may communicate with one or more storage devices **640**. For example, the one or more storage devices **640** may include nonvolatile storage devices, such as magnetic disks, optical disks, or flash memory devices. The storage devices **640** may include both removable and non-removable memory devices. The storage devices **640** may be configured to store an operating system, images of operating systems, applications, and program data. In a particular embodiment, the memory **630**, the storage devices **640**, or both, include tangible, non-transitory computer-readable media.

[0060] The processor **620** may also communicate with one or more input/output interfaces **650** that enable the computing device **610** to communicate with one or more input/output devices **670** to facilitate user interaction. The input/output interfaces **650** may include serial interfaces (e.g., universal serial bus (USB) interfaces or Institute of Electrical and Electronics Engineers (IEEE) 1394 interfaces), parallel interfaces, display adapters, audio adapters, and other interfaces. The input/output devices **670** may include keyboards, pointing devices, displays, speakers, microphones, touch screens, and other devices.

[0061] The processor **620** may communicate with other computer systems **680** (e.g., the remote computing device **122** of FIG. **1**) via the one or more communications interfaces **660**. The one or more communications interfaces **660** may include wired interfaces (e.g., Ethernet), wireless interfaces (e.g., an interface that operates according to a standard of the IEEE 802 family of standards), other wireless communication interfaces, or other network interfaces. The other computer systems **680** may include host computers, servers, workstations, and other computing devices. The computing device **610** may send agent program code for execution to the other computer systems **680** via the one or more communications interfaces **660**. Similarly, the computing device **610** may receive agent data from agents executing at the other computer systems **680** via the one or more communications interfaces **660**.

[0062] Although only one computing device **610** is illustrated in FIG. **6**, in particular embodiments, the supervisor application **104**, the biomimicry subsystems **106**, the instantiators **108**, or portions thereof, may be distributed among multiple computing devices, e.g., as a distributed computing system.

[0063] Examples described above illustrate but do not limit the disclosure. It should also be understood that numerous modifications and variations are possible in accordance with the principles of the present disclosure. Accordingly, the scope of the disclosure is defined by the following claims and their equivalents.

[0064] The illustrations of the examples described herein are intended to provide a general understanding of the structure of the various embodiments. The illustrations are not intended to serve as a complete description of all of the elements and features of apparatus and systems that utilize the structures or methods described herein. Many other embodiments may be apparent to those of skill in the art upon reviewing the disclosure. Other embodiments may be utilized and derived from the disclosure, such that structural and logical substitutions and changes may be made without departing from the scope of the disclosure. For example, method steps may be performed in a different order than shown in the figures or one or more method steps may be omitted. Accordingly, the disclosure and the figures are to be regarded as illustrative rather than restrictive.

[0065] Moreover, although specific examples have been illustrated and described herein, it should be appreciated that any subsequent arrangement designed to achieve the same or similar results may be substituted for the specific embodiments shown. This disclosure is intended to cover any and all subsequent adaptations or variations of various embodiments. Combinations of the above embodiments, and other embodiments not specifically described herein, will be apparent to those of skill in the art upon reviewing the description.

[0066] The Abstract of the Disclosure is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, various features may be grouped together or described in a single embodiment for the purpose of streamlining the disclosure. As the following claims reflect, the claimed subject matter may be directed to less than all of the features of any of the disclosed examples.

What is claimed is:

1. A system comprising:

a processing system including one or more processors;

memory accessible to the processing system, wherein the memory stores instructions executable by at least one processor of the one or more processors to cause the at least one processor to perform operations comprising:

instantiating a first detection agent based on detection criteria, wherein the first detection agent includes first program code executable by a second processor to monitor network activity;

sending the first program code of the first detection agent to a remote computing device for execution, wherein, when the first program code of the first detection agent is executed at the remote computing device, the first detection agent causes network activity data to be transmitted to the processing system, and wherein the processing system updates the detection criteria based on the network activity data to generate updated detection criteria;

instantiating a second detection agent based on the updated detection criteria wherein the second detection agent includes second program code; and

sending second program code of the second detection agent to the remote computing device for execution.

2. The system of claim **1**, wherein the operations further comprise executing a supervisor application, wherein the supervisor application is executable to perform operations comprising:

performing analysis of data received from one or more agents executing at one or more remote processors;

initiating one or more actions automatically, without human intervention, based on the analysis; and

notifying a human operator of results of the data, results of the analysis, actions taken, or a combination thereof.

3. The system of claim **1**, wherein the first program code of the first detection agent further includes instructions to authenticate other agents and to exchange secure messages with the other agents independently of the processing system.

4. The system of claim **1**, wherein the first program code of the first detection agent is configured to monitor first detection criterion and is not configured to monitor second detection criterion, and wherein the second program code is executable by the second processor to monitor the second detection criterion.

5. The system of claim **1**, wherein the operations further comprise:

instantiating a first defense agent based on a set of available defense actions, wherein the first defense agent includes third program code executable by the second processor to mitigate suspect network activity; and

sending the third program code of the first defense agent to the remote computing device for execution to mitigate particular suspect network activity that is detected by a particular detection agent.

6. The system of claim **5**, wherein the operations further comprise:

instantiating a second defense agent based on the updated detection criteria after the processing system generates updated detection criteria; and

sending fourth program code of the second defense agent to the remote computing device for execution.

7. The system of claim **5**, wherein, when the first defense agent is executed at the remote computing device, the first

defense agent causes suspect network activity mitigation data to be transmitted to the processing system, and wherein the processing system updates the detection criteria to generate the updated detection criteria further based on the suspect network activity mitigation data.

8. The system of claim **5**, wherein, when the first defense agent is executed at the remote computing device, the first defense agent causes suspect network activity mitigation data to be transmitted to the processing system, and wherein the processing system updates the set of available defense actions to generate an updated set of available defense actions based on the suspect network activity mitigation data.

9. The system of claim **5**, wherein the first detection agent is configured to communicate detection data to the first defense agent at the remote computing device, wherein the detection data identifies suspect network activity detected by the first detection agent, and wherein the first defense agent is configured to automatically select and execute a particular defense action, independently of the processing system, based on the detection data.

10. The system of claim **5**, wherein the set of available defense actions includes a first subset of available defense actions and a second subset of available defense actions, and wherein the third program code of the first defense agent is configured to execute the first subset of available defense actions and is not configured to execute the second subset of available defense actions.

11. The system of claim **10**, wherein the operations further comprise:

instantiating a second defense agent including fourth program code executable by the second processor to execute one or more defense actions of the second subset of defense actions; and

sending the fourth program code of the second defense agent to the remote computing device.

12. The system of claim **1**, wherein the operations further comprise:

instantiating a first attack agent based on a set of available counterattack actions, wherein the first attack agent includes fifth program code executable by the second processor to execute a counterattack based on suspect network activity; and

sending the fifth program code of the first attack agent to the remote computing device for execution based on the suspect network activity detected by a particular detection agent.

13. The system of claim **12**, wherein the operations further comprise:

instantiating a second attack agent based on the updated detection criteria after the processing system generates updated detection criteria; and

sending sixth program code of the second attack agent to the remote computing device for execution.

14. The system of claim **12**, wherein, when the first attack agent is executed at the remote computing device, the first attack agent causes counterattack activity data to be transmitted to the processing system, and wherein the processing system updates the set of available counterattack actions to generate an updated set of available counterattack actions based on the counterattack activity data.

15. A method comprising:

instantiating, at a first computing device, a first detection agent based on detection criteria, wherein the first detection agent includes first program code executable by a second computing device to monitor network activity;

sending the first program code of the first detection agent to the second computing device for execution, wherein, when the first program code of the first detection agent is executed at the second computing device, the first detection agent causes network activity data to be transmitted to a processing system, and wherein the processing system updates the detection criteria based on the network activity data to generate updated detection criteria;

instantiating, at the first computing device, a second detection agent based on the updated detection criteria; and

sending second program code of the second detection agent to the second computing device for execution.

16. The method of claim **15**, further comprising:

instantiating at least one additional agent, the at least one additional agent including a defense agent, an attack agent, or both; and

sending program code of the at least one additional agent to the second computing device for execution.

17. The method of claim **16**, further comprising, before instantiating the at least one additional agent, selecting operations to be performed by the at least one additional agent based on the network activity data, wherein the program code of the at least one additional agent includes instructions executable by the second computing device to perform the selected operations.

18. A computer-readable storage device storing instructions that are executable by a processor to cause the processor to perform operations comprising:

instantiating a first detection agent based on detection criteria, wherein the first detection agent includes first program code executable by a remote computing device to monitor network activity;

sending the first program code of the first detection agent to the remote computing device for execution, wherein, when the first program code of the first detection agent is executed at the remote computing device, the first detection agent causes network activity data to be transmitted to a processing system, and wherein the processing system updates the detection criteria based on the network activity data to generate updated detection criteria;

instantiating a second detection agent based on the updated detection criteria; and

sending second program code of the second detection agent to the remote computing device for execution.

19. The computer-readable storage device of claim **18**, wherein the operations further comprise executing at supervisor application, wherein the supervisor application is executable to perform operations comprising:

performing analysis of data received from one or more agents executing at one or more remote computing devices;

initiating one or more actions automatically, without human intervention, based on the analysis; and

notifying a human operator of results of the data, results of the analysis, actions taken, or a combination thereof.

20. The computer-readable storage device of claim **18**, wherein the first program code of the first detection agent further includes instructions to authenticate other agents, to exchange secure messages with the other agents, and to send the network activity data as one or more encrypted messages to the processing system and to one or more other agents.

* * * * *