CLAIMS

1. A security appliance configured to protect a client device against computer security threats, wherein the client device is configured to connect wirelessly to an administration device, wherein connecting comprises the client device emitting availability notifications and the administration device initiating peer-to-peer connections with the client device by responding to the respective availability notifications, the security appliance being separate from the client device and the administration device, and further having a hardware processor configured to:

   monitor wireless communication between the client device and the administration device to determine a notification pattern specific to the client;

   in response to detecting a first wireless communication comprising an availability notification, determine whether the first wireless communication fits a notification pattern;

   in response, if the first wireless communication does not fit the notification pattern, transmit a second wireless communication configured to initiate a peer-to-peer connection with the sender of the first wireless communication, the second wireless communication further configured to include an identifier of the administration device; and

   in response to transmitting the second wireless communication, perform a security action to protect the client device or the administration device.

2. The security appliance of claim 1, further characterized by having the hardware processor configured to determine whether the first wireless communication fits the notification pattern according to a time interval separating the first wireless communication from a previously-detected wireless communication comprising another availability notification emitted by the client device.

3. The security appliance of claim 2, further characterized by having the hardware processor configured to:

compare a difference between a size of the time interval and a reference interval size characteristic of the client device to a pre-determined threshold; and
in response, determine whether the first wireless communication fits the notification pattern according to a result of the comparison.

4. The security appliance of claim 1, further characterized by having the hardware processor configured to determine whether the first wireless communication fits the notification pattern according to a notification frequency specific to the client device, the notification frequency determined according to a count of availability notifications emitted by the client device within a pre-determined time interval.

5. The security appliance of claim 1, further characterized by having the hardware processor configured to determine whether the first wireless communication fits the notification pattern according to an indicator of a signal-to-noise ratio of a carrier signal of the first wireless communication.

6. The security appliance of claim 1, wherein:
the notification pattern comprises a pattern of hopping between carrier signal frequency bands; and
further characterized by having the hardware processor configured to determine whether the first wireless communication fits the pattern of hopping according to a frequency of a carrier signal of the first wireless communication and further according to another frequency of another carrier signal of another availability notification previously received from the client device.

7. The security appliance of claim 1, further characterized by having the hardware processor configured, in preparation for determining whether the first wireless communication fits the notification pattern, to:
detect a plurality of availability notifications emitted by the client device; and
in response, determine the notification pattern according to the plurality of availability notifications.

8. The security appliance of claim 1, wherein the security action comprises maintaining the peer-to-peer connection active for a pre-determined amount of time.

9. The security appliance of claim 1, wherein the security action comprises transmitting a set of surrogate data to the sender of the first wireless communication over the peer-to-peer connection.

10. A computer-implemented method of protecting a client device against computer security threats, wherein the client device is configured to connect wirelessly to an administration device, wherein connecting comprises the client device emitting availability notifications and the administration device initiating peer-to-peer connections with the client device by responding to the respective availability notifications, the method being performed by a security appliance separate from the client device and the administration device, and the employing a hardware processor of the security appliance to:

monitor wireless communication between the client device and the administration device to determine a notification pattern specific to the client;

in response to detecting a first wireless communication comprising an availability notification, determine whether the first wireless communication fits the notification pattern;

in response, if the first wireless communication does not fit the notification pattern, transmit a second wireless communication configured to initiate a peer-to-peer connection with a sender of the first wireless communication, the second wireless communication further configured to include an identifier of the administration device; and

in response to transmitting the second wireless communication, perform a security action to protect the client device or the administration device.

11. The method of claim 10, further characterized by employing the hardware processor to determine whether the first wireless communication fits the notification pattern

according to a time interval separating the first wireless communication from a previously-detected wireless communication comprising another availability notification emitted by the client device.

12. The method of claim 11, further characterized by employing the hardware processor to:
compare a difference between a size of the time interval and a reference interval size characteristic of the client device to a pre-determined threshold; and
in response, determine that the first wireless communication fits the notification pattern if the difference is smaller than a pre-determined threshold.

13. The method of claim 10, further characterized by employing the hardware processor to determine whether the first wireless communication fits the notification pattern according to a notification frequency specific to the client device, the notification frequency determined according to a count of availability notifications emitted by the client device during a pre-determined time interval.

14. The method of claim 10, further characterized by employing the hardware processor to determine whether the first wireless communication fits the notification pattern according to an indicator of a signal-to-noise ratio of a carrier signal of the first wireless communication.

15. The method of claim 10, wherein:
the notification pattern comprises a pattern of hopping between carrier signal frequency bands, the pattern of hopping specific to the client device; and
further characterized by employing the hardware processor to determine whether the first wireless communication fits the pattern of hopping according to a frequency of a carrier signal of the first wireless communication and further according to another frequency of another carrier signal of another availability notification previously received from the client device.

16. The method of claim 10, further characterized by employing the hardware processor, in preparation for determining whether the first wireless communication fits the notification pattern, to:
detect a plurality of availability notifications emitted by the client device; and
in response, determine the notification pattern according to the plurality of availability notifications.

17. The method of claim 10, wherein the security action comprises maintaining the peer-to-peer connection active for a pre-determined amount of time.

18. The method of claim 10, wherein the security action comprises transmitting a set of surrogate data to the sender of the first wireless communication over the peer-to-peer connection.

19. A non-transitory computer-readable medium storing instructions which, when executed by a hardware processor of a security appliance, cause the security appliance to protect a client device against computer security threats, wherein the client device is configured to connect wirelessly to an administration device, wherein connecting comprises the client device emitting availability and the administration device imitating peer-to-peer connections with the client device be responding to the respective availability notifications, the security appliance being separate from the client device and the administration device and the instructions cause the security appliance to:
monitor wireless communication between the client device and the administration device to determine a notification pattern specific to the client device;
in response to detecting a first wireless communication comprising an availability notification, determine whether the first wireless communication fits the notification pattern;
in response, if the first wireless communication does not fit the notification pattern, transmit a second wireless communication configured to initiate a peer-to-peer connection with the sender of the first wireless communication, the second wireless

communication further configure to include an identifier of the administration device; and

in response to transmitting the second wireless communication, perform a security action to protect the client device or the administration device.