CLAIMS

1. A method of detecting compromised access points by a communications device, comprising: transmitting a first probe addressed to a server from the communications device via a first radio access technology; transmitting a second probe addressed to the server from the communications device via a second radio access technology that is different from the first radio access technology; receiving, by the communications device, a first probe reply from the server via the first radio access technology; receiving, by the communications device, a second probe reply from the server via the second radio access technology; and determining, by the communications device, whether an access point is a rogue access point based on a result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology.

2. The method of claim 1, further comprising taking an action in response to determining that the access point is a rogue access point based on the result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology.

3. The method of claim 2, wherein taking the action comprises terminating a network connection with at least one of: an access point of a first network; or an access point of a second network.

4. The method of claim 1, wherein determining whether the access point is a rogue access point based on the result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology further comprises: determining whether either the first probe reply or the second probe reply is malicious; and determining that the access point is a rogue access point in response to determining that either the first probe reply or the second probe reply is malicious.

5. The method of claim 1, wherein determining whether the access point is a rogue access point based on the result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology further comprises comparing connection results and connection parameters of the first probe reply to connection results and connection parameters of the second probe reply.

6. The method of claim 5, wherein the connection results indicate whether a secure connection was established between the communications device and the server.

7. The method of claim 5, wherein the connection parameters include characteristics of a security certificate.

8. The method of claim 5, wherein the connection parameters include a security level of any redirect uniform resource locators (URLs).

9. The method of claim 5, wherein the connection parameters include characteristics of domain

name system queries and results.

10. A communications device, comprising: a first transceiver configured to communicate with a first network via a first network connection; a second transceiver configured to communicate with a second network via a second network connection; a processor coupled to the first and second transceivers and configured with processor executable instructions to perform operations comprising: transmitting a first probe addressed to a server from the communications device via a first radio access technology; transmitting a second probe addressed to the server from the communications device via a second radio access technology that is different from the first radio access technology; receiving a first probe reply from the server via the first radio access technology; receiving a second probe reply from the server via the second radio access technology; and determining based whether an access point is a rogue access point based on a result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology.

11. The communications device of claim 10, wherein the processor is further configured with processor executable instructions to perform operations further comprising taking an action in response to determining that the access point is a rogue access point based on the result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology.

12. The communications device of claim 11, wherein the processor is further configured with processor executable instructions to perform operations such that taking the action comprises terminating a network connection with at least one of: an access point of the first network; or an access point of the second network.

13. The communications device of claim 10, wherein the processor is further configured with processor executable instructions to perform operations such that determining whether the access point is a rogue access point based on the result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology further comprises: determining whether either the first probe reply or the second probe reply is malicious; and determining that the access point is a rogue access point in response to determining that either the first probe reply or the second probe reply is malicious.

14. The communications device of claim 10, wherein the processor is further configured with processor executable instructions to perform operations such that determining whether the access point is a rogue access point based on the result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology further comprises comparing connection results and connection parameters of the first probe reply to connection results and connection parameters of the second probe reply.

15. The communications device of claim 14, wherein the connection results indicate whether a secure connection was established between the communications device and the server.

16. The communications device of claim 14, wherein the connection parameters include characteristics of a security certificate.

17. The communications device of claim 14, wherein the connection parameters include a security level of any redirect uniform resource locators (URLs).

18. The communications device of claim 14, wherein the connection parameters include characteristics of domain name system queries and results.

19. A communications device, comprising: means for transmitting a first probe addressed to a server from the communications device via a first radio access technology; means for transmitting a second probe addressed to the server from the communications device via a second radio access technology that is different from the first radio access technology; means for receiving a first probe reply from the server via the first radio access technology; means for receiving a second probe reply from the server via the second radio access technology; and means for determining whether an access point is a rogue access point based on a result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology.

20. The communications device of claim 19, further comprising means for taking an action in response to determining that the access point is a rogue access point based on the result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology.

21. The communications device of claim 20, wherein means for taking the action comprises means for terminating a network connection with at least one of: an access point of a first network; or an access point of a second network.

22. The communications device of claim 19, wherein means for determining whether the access point is a rogue access point based on the result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology further comprises: means for determining whether either the first probe reply or the second probe reply is malicious; and means for determining that the access point is a rogue access point in response to determining that either the first probe reply or the second probe reply is malicious.

23. The communications device of claim 19, wherein means for determining whether the access point is a rogue access point comprises based on the result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology further comparing connection results and connection parameters of the first probe reply to connection results and connection parameters of

the second probe reply.

24. A non-transitory processor-readable medium having stored thereon executable instructions causing a processor of a communications device to perform operations comprising: transmitting a first probe addressed to a server from the communications device via a first radio access technology; transmitting a second probe addressed to the server from the communications device via a second radio access technology that is different from the first radio access technology; receiving a first probe reply from the server via the first radio access technology; receiving a second probe reply from the server via the second radio access technology; and determining whether an access point is a rogue access point based on a result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology.

25. The non-transitory processor-readable medium of claim 24, wherein the stored processor-executable instructions are configured to cause the processor of the communications device to perform operations further comprising taking an action in response to determining that the access point is a rogue access point based on the result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology.

26. The non-transitory processor-readable medium of claim 25, wherein the stored processor-executable instructions are configured to cause the processor of the communications device to perform operations such that taking the action comprises terminating a network connection with at least one of: an access point of a first network; or an access point of a second network.

27. The non-transitory processor-readable medium of claim 24, wherein the stored processor-executable instructions are configured to cause the processor of the communications device to perform operations such that determining whether the access point is a rogue access point based on the result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology comprises: determining whether either the first probe reply or the second probe reply is malicious; and determining that the access point is a rogue access point in response to determining that either the first probe reply or the second probe reply is malicious.

28. The non-transitory processor-readable medium of claim 24, wherein the stored processor-executable instructions are configured to cause the processor of the communications device to perform operations such that determining whether the access point is a rogue access point based on the result of comparing the first probe reply received from the server via the first radio access technology to the second probe reply received from the server via the second radio access technology comprises comparing connection results and connection parameters of the first probe reply to connection results and connection parameters of the second probe reply.