WHAT IS CLAIMED IS:

1. A communication device comprising:

a processor; and

a memory coupled to the processor, the memory storing instructions, which when executed by the processor, cause the communication device to perform operations including:

determining that an update for a first software layer of an application installed on the communication device is available at a server;

sending a request for the update to the server, the request including a current identifier associated with a current version of the first software layer installed on the communication device;

receiving an updated version of the first software layer from the server that is encrypted using a current transport key embedded in the current version of the first software layer installed on the communication device;

decrypting the updated version of the first software layer using the current transport key embedded in the current version of the first software layer installed on the communication device; and

installing the updated version of the first software layer without updating a second software layer of the application.

2 . The communication device of claim 1, wherein the operations further include: subsequent to installing the updated version of the first software layer:

sending a request to the server for sensitive data, the request including an updated identifier associated with the updated version of the first software layer;

receiving the sensitive data encrypted using an updated transport key embedded in the updated version of the first software layer; and

decrypting the sensitive data using the updated transport key.

3. The communication device of claim 2, wherein the sensitive data is received in a message that includes a header and a payload containing the sensitive data, and wherein the operation of decrypting the sensitive data using the updated transport key comprises:

generating a one-time key by encrypting the header with the updated transport key; and

decrypting the sensitive data with the one-time key.

4. The communication device of claim 2, wherein the operation of decrypting the sensitive data using the updated transport key comprises:

generating a derived key using the updated transport key and a key derivation seed received from the server; and

decrypting the sensitive data with the derived key.

5. The communication device of claim 1, wherein the operation of determining that an update for the first software layer is available at the server comprises:

contacting the server to verify whether the application is up-to-date.

6. The communication device of claim 1, wherein the operation of determining that an update for the first software layer is available at the server comprises:

receiving a message notifying that the update for the first software layer is available.

7. The communication device of claim 1, wherein the current version of the first software layer is obfuscated using a first obfuscation seed, and the updated version of the first software layer is obfuscated using a second obfuscation seed that is different than the first obfuscation seed.

8. The communication device of claim 1, wherein the second software layer is written in a first programming language, and the first software layer is written in a second programming language that is different than the first programming language.

9. A method for updating an application installed on a communication device, wherein the application includes a first software layer and a second software layer, the method comprising:

determining, by the application, that an update for the first software layer is available at a server;

sending a request for the update to the server, the request including a current identifier associated with a current version of the first software layer installed on the communication device;

receiving an updated version of the first software layer from the server that is encrypted using a current transport key embedded in the current version of the first software layer installed on the communication device;

decrypting the updated version of the first software layer using the current transport key embedded in the current version of the first software layer installed on the communication device; and

installing the updated version of the first software layer on the communication device without updating the second software layer.

10. The method of claim 9, further comprising:

subsequent to installing the updated version of the first software layer:

sending a request to the server for sensitive data, the request including an updated identifier associated with the updated version of the first software layer;

receiving the sensitive data encrypted using an updated transport key embedded in the updated version of the first software layer; and

decrypting the sensitive data using the updated transport key.

11. The method of claim 10, wherein the sensitive data is received in a message that includes a header and a payload containing the sensitive data, and decrypting the sensitive data using the updated transport key comprises:

generating a one-time key by encrypting the header with the updated transport key; and

decrypting the sensitive data with the one-time key.

12. The method of claim 9, wherein determining, by the application, that an update for the first software layer is available at the server comprises:

contacting the server, by the application, to verify whether the application is up-to-date.

13. The method of claim 9, wherein determining, by the application, that an update for the first software layer is available at the server comprises:

receiving, by the application, a message notifying that the update for the first software layer is available.

14. The method of claim 9, wherein the current version of the first software layer is obfuscated using a first obfuscation seed, and the updated version of the first software layer is obfuscated using a second obfuscation seed that is different than the first obfuscation seed.

15. The method of claim 9, wherein the second software layer is written in a first programming language, and the first software layer is written in a second programming language that is different than the first programming language.

16. A server for providing an update to an application installed on a communication device, wherein the application includes a first software layer and a second software layer, the server comprising:

a processor; and

a memory coupled to the processor, the memory storing instructions, which when executed by the processor, cause the server to perform operations including:

receiving a request for an update to the first software layer of the application from the communication device, the request including a current identifier associated with a current version of the first software layer installed on the communication device;

determining, based on the current identifier, a current transport key that is associated with the current version of the first software layer installed on the communication device;

encrypting an updated version of the first software layer using the current transport key; and

transmitting the encrypted updated version of the first software layer to the communication device without transmitting an update to the second software layer of the application.

17. The server of claim 16, wherein the operations further include:

subsequent to transmitting the updated version of the first software layer:

receiving a request from the communication device for sensitive data, the request including an updated identifier associated with the updated version of the first software layer;

encrypting the sensitive data using an updated transport key embedded in the updated version of the first software layer; and

transmitting the encrypted sensitive data to the communication device.

18. The server of claim 17, wherein the sensitive data is transmitted in a message that includes a header and a payload containing the sensitive data, and the operation of encrypting the sensitive data using the updated transport key comprises:

generating a one-time key by encrypting the header with the updated transport key; and

encrypting the sensitive data with the one-time key.

19. The server of claim 17, wherein the operation of encrypting the sensitive data using the updated transport key comprises:

generating a derived key using the updated transport key and a seed; and

encrypting the sensitive data with the derived key.

20. The server of claim 16, wherein the current version of the first software layer is obfuscated using a first obfuscation seed, and the updated version of the first software layer is obfuscated using a second obfuscation seed that is different than the first obfuscation seed.