**EndpointLock Enhanced Encryption (EPL SDK-EE)**

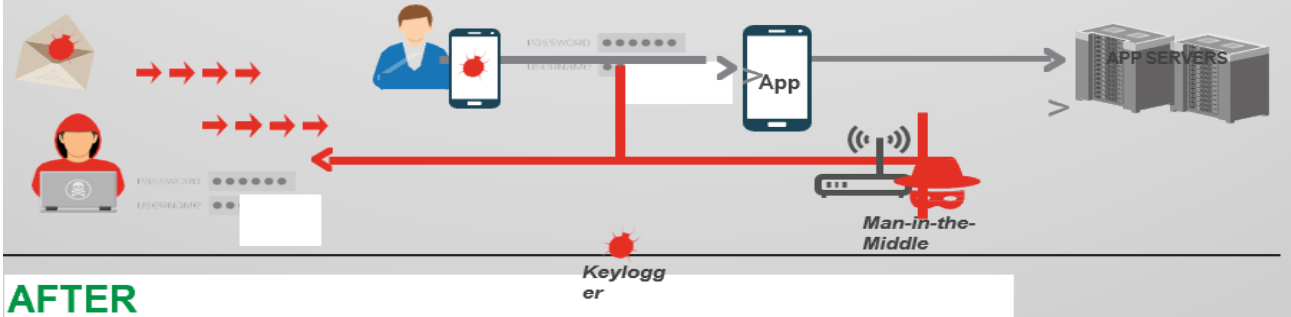
- The enhanced version provides the functionality to force the use of the encrypted keyboard on text input fields (all or some) within the partner/customer app
- The device user does not have to go through a setup/configuration process to authorize the use of the encrypted keyboard on the device
- The device user would not need to manually switch to the encrypted keyboard as this would be forced by the App and the EndpointLock SDK
- The encryption of the keystrokes would be extended to the actual key handling of the text field within the host application.
- This version requires the partner/customer to make some minor changes to the actual text entry fields within the app (to configure/force the text fields to use a specific keyboard)

**EndpointLock End-to-End Encryption (EPL SDK-ETEE)**

- The end-to-end version of the EndpointLock SDK extends the encryption of the keystrokes beyond the device app to the servers of the mobile application owner
- App data would be encrypted all the way to the partner/customer server- side platforms and the only way to decrypt the data would be to communicate with the EPL server-side platforms via an endpoint API
- This version of the SDK would require a communication path to be established between the partner/customer server-side applications and the EPL server-side endpoints
- There is detailed development required by the partner/customer to facilitate this extremely secure end- to-end encryption within the partner/customer server-side platform(s).
- This integration is much more involved as changes would be required by the partner/customer to not only the app but also to servers handling the processing of the app data (the partner/customer server- side platform)

## BEFORE

1. *Hacker sends email infected with zero day malware containing keylogger and/or spyware.*
2. *App User downloads the keylogger, logs into his app and begins to enter PII.*
3. *Hacker retrieves credentials and PII from the keylogger.*
4. *Hacker uses the stolen credentials to log into the user's accounts.*
5. *Threat of MITM attack also exists when using an unsecure router such as public WiFi hotspot.*




## AFTER

1. *Hacker sends email infected with zero day malware containing keylogger and/or spyware.*
2. *App User downloads the keylogger, logs into his app and begins to enter PII.*
3. *All keystrokes are encrypted by the app's embedded Secure Keyboard.*
4. *Hacker receives encrypted data completely unreadable and useless.*
5. *Man-in-the-Middle threat is prevented.*

***All data stays fully encrypted from the moment it is typed, until it reaches the app servers***