Security.

InputStickUtility Android application.

InputStickUtility Android application requires following permissions:

- *Bluetooth Admin* - turn Bluetooth power on/off,
- *Bluetooth* – connect to InputStick,
- *Vibrate* – to notify user about removing InputStick form USB port (option).
- *Location* – required by Android 6.0 to scan for nearby Bluetooth devices. Can be revoked after adding InputStick device.

Application does not require any unnecessary privileges. It is not allowed to send any data over the Internet. InputStickUtility does not log any data that it sends to or received from InputStick.

Pairing PIN.

Bluetooth 2.1 version is protected by 4 digit pairing PIN. PIN can be changed with InputStickUtility application. Default PIN: 1234.
In Bluetooth 4.0 version, PIN protection is disabled by default due to bug in Android OS (system will ask user to provide PIN before every connection attempt). It is recommended to use password protection on protocol level. InputStickUtility will not allow to set PIN for BT4.0 device, however it is possible to enable PIN protection by sending *CMD Set Pin*.

Pairing PIN can be restored with following procedure:

- Plug InputStick into USB port, use Windows PC*.
- Make sure it is recognized by the OS (should appear in Device Manager).
- Within next 20 seconds press NumLock, CapsLock or ScrollLock key 20 times (use other keyboard).
- Pairing PIN will be restored to 1234 (BT2.1 version) or disabled (BT4.0 version). **Firmware v0.98 and later will also remove password protection, unless user disabled *"Simple restore"*.**
- InputStick will flash all keyboard LEDs: OFF→ON→OFF.
- Remove InputStick from USB port.

* Windows keeps global state of keyboard LEDs (NumLock, CapsLock, ScrollLock), what allows InputStick to see changes made using other keyboards. Linux and OS X keep separate state of keyboard LEDs for each connected keyboard device.

Password protection and authentication.

InputStick can be password protected using 128bit key. When password protection is enabled, most commands (most importantly: keyboard and mouse actions) can be executed only after successful authentication. This prevents from using InputStick to remotely control USB host it is currently plugged into. The key is also used to encrypt transmitted data using AES-128 algorithm.

Restoring defaults.

"Simple restore" - since v0.98 firmware release, password protection is by default removed when pairing PIN is restored. If *"Simple restore"* is disabled, more time consuming procedure is required (see below).

If user forgets the password, InputStick can be restored to factory defaults using InputStickUtility application. To minimize risk of unauthorized person successfully performing restore defaults procedure to gain access to your InputStick, it requires:

- Android device with Bluetooth and InputStickUtility application,
- PC running Windows OS*,
- enough time (10 minutes),
- physical access to InputStick (must be removed from USB port),

* Windows keeps global state of keyboard LEDs (NumLock, CapsLock, ScrollLock), what allows InputStick to see changes made using other keyboards. Linux and OS X keep separate state of keyboard LEDs for each connected keyboard device.

Restore procedure consists of 10 steps:

- InputStick asks user to set specified state of keyboard LEDs (NumLock, CapsLock, ScrollLock),
- user must use other keyboard (or software method) to set specified state,
- after 60 seconds state of the LEDs is verified. If it is correct, procedure moves to next step, if not, restore procedure results in failure and must be started over again.

After all steps are completed, InputStick erases password protection, all user settings and goes into infinite loop. It must be removed from USB port before it can be used again.

If unauthorized person is able to successfully complete restore procedure and as a result remove password protection, user will be notified about this fact by InputStickUtility application during next connection attempt.

Following features are available since 0.97 firmware version.

Custom Bluetooth pairing PIN.

Default Bluetooth pairing PIN (1234) can be changed using InputStickUtility application. After setting new PIN InputStick must be removed from USB port. User will be asked for new pairing PIN during next connection attempt.

Restoring Bluetooth pairing PIN.

If user forgets pairing PIN, it can be restored to default value (1234):

- plug InputStick into USB port,
- press CapsLock key 15 times (within 30 seconds time),
- InputStick will confirm restoring Bluetooth pairing PIN (to 1234) by toggling keyboard LEDs,
- wait 5 seconds,
- remove InputStick form USB port.

Just like in case of restoring factory defaults, this procedure also requires physical access to the InputStick device and PC running Windows OS.

If unauthorized person is able to successfully restore Bluetooth pairing PIN to 1234, your Android device will ask you to enter new pairing PIN during next connection attempt.

Locked state.

When InputStick is in “locked” state, it is not possible to set password protection or change Bluetooth pairing PIN. This mechanism is designed to protect unauthorized person from taking over your InputStick device.
InputStick is put into “unlocked” state if Bluetooth connection is established during first 30 seconds after powering up or when password protection is already set.
InputStick is “locked” after 30 seconds passes from powering up and password protection is not set, as well as each time Bluetooth connection is lost. In such case it is necessary to unplug InputStick from USB port and plug again, before setting password or changing PIN.

Any potential attach can be successful only during first 30 seconds after InputStick is plugged into USB port, provided that attacker manages to establish Bluetooth connection before user. Otherwise it requires physical access to the InputStick device.