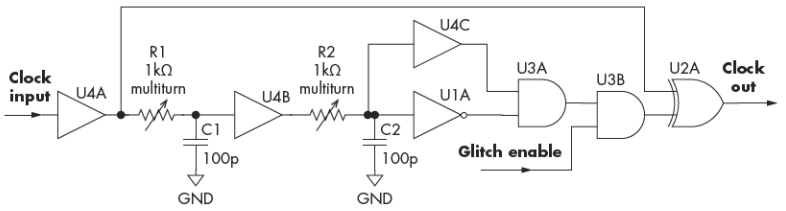
The Hardware Hacking Handbook

Breaking Embedded Security with Hardware Attacks

by Colin O'Flynn and Jasper van Woudenberg

errata updated to print 4

Page	Error	Correction	Print corrected
10	A Xenium ICE modchip on the left in Figure 1-4 is soldered to the main Xbox PCB in order to perform its attack. The board automates a **fault injection** attack to load arbitrary firmware.	A Xenium ICE modchip on the left in Figure 1-4 is soldered to the main Xbox PCB in order to perform its attack. The board automates a **hardware** attack to load arbitrary firmware.	Pending
50	This means if no other devices are talking, both lines will sit at logic one, and any device can take ownership of the bus by pulling down the **SCA** line.	This means if no other devices are talking, both lines will sit at logic one, and any device can take ownership of the bus by pulling down the **SDA** line.	Print 2
51	Figure 2-11 shows the STOP conditions on the **SCA** and SCL lines.	Figure 2-11 shows the STOP conditions on the **SDA** and SCL lines.	Print 2
51	I first tell the EEPROM from which memory address I want to read (which is a write operation—that is, a **one** on the eighth bit), then I have to tell the EEPROM to send the data at that memory location (which is a read operation—that is, a **zero** on the eighth bit)	I first tell the EEPROM from which memory address I want to read (which is a write operation—that is, a **zero** on the eighth bit), then I have to tell the EEPROM to send the data at that memory location (which is a read operation—that is, a **one** on the eighth bit)	Print 4
52	A complete sequence on **SCA** between a controller device and an EEPROM looks like the following:	A complete sequence on **SDA** between a controller device and an EEPROM looks like the following:	Print 2
52	As long as the controller keeps toggling **SDA** and acknowledging at the right time, the EEPROM will continue to send successive bytes of data to the controller.	As long as the controller keeps toggling **SCL** and acknowledging at the right time, the EEPROM will continue to send successive bytes of data to the controller.	Print 4
156	Figure replacement	 *Figure 5-10: Generating clock glitches using analog delay lines*	Print 2
426	This kit in particular includes the **TP910** test leads, which have a very fine point to easily probe QFN packages.	This kit in particular includes the **TL910** test leads, which have a very fine point to easily probe QFN packages.	Pending

Page	Error	Correction	Print corrected
426	The **TP910** test leads have the disadvantage that the thin and flexible cable is likely to be bent on smaller radii and eventually develops internal openings, especially near the end where flexing is most pronounced.	The **TL910** test leads have the disadvantage that the thin and flexible cable is likely to be bent on smaller radii and eventually develops internal openings, especially near the end where flexing is most pronounced.	Pending
427	Figure A-1: Fluke **TP910** test leads with pogo pin (left) on QFN IC pad and sharp probe to pierce solder mask (right)	Figure A-1: Fluke **TL910** test leads with pogo pin (left) on QFN IC pad and sharp probe to pierce solder mask (right)	Pending