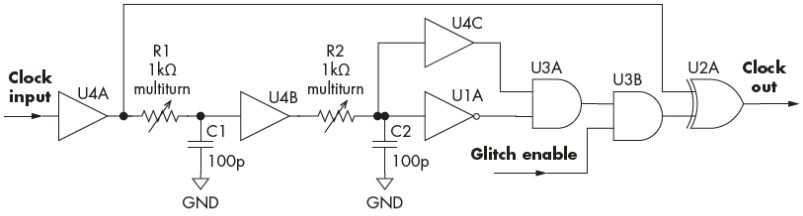
The Hardware Hacking Handbook

Breaking Embedded Security with Hardware Attacks

by Colin O'Flynn & Jasper van Woudenberg

Errata updated to print 5

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.	Print 5
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
57	*Addition*	Tools for toggling port pins on a device given a BSDL file exist; well-known examples include UrJTAG (open source) and TopJTAG (low-cost with free trial, GUI based). **Note that some users have had trouble receiving TopJTAG licenses, so check that the project is still alive before proceeding.**	Print 5
156	*Figure replacement*	 *Figure 5-10: Generating clock glitches using analog delay lines*	Print 2

Page	Error	Correction	Print corrected
169	`printf("%d %d %d %d\n", cnt, i, j, k++);`	`printf("%d %d %d %d\n", i, j, cnt, k++);`	Print 5
289	The difference at each point is much **larger** for the correct password.	The difference at each point is much **smaller** for the correct password.	Print 5
297	The Hamming weight of 0xA4 is 3 because 0xA4 is **10010100** in binary and in it are three ones.	The Hamming weight of 0xA4 is 3 because 0xA4 is **10100100** in binary and in it are three ones.	Print 5
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.	Print 5
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.	Print 5
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)	Print 5
448	*Addition*	Many other commercial software for boundary scan are thousands of dollars and don't work as well as TopJTAG. **Note that some users have had trouble receiving TopJTAG licenses, so check that the project is still alive before proceeding.**	Print 5