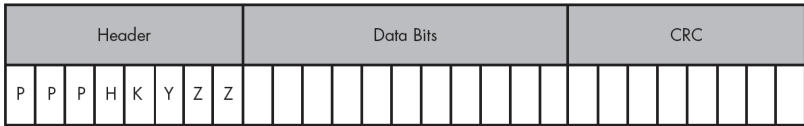



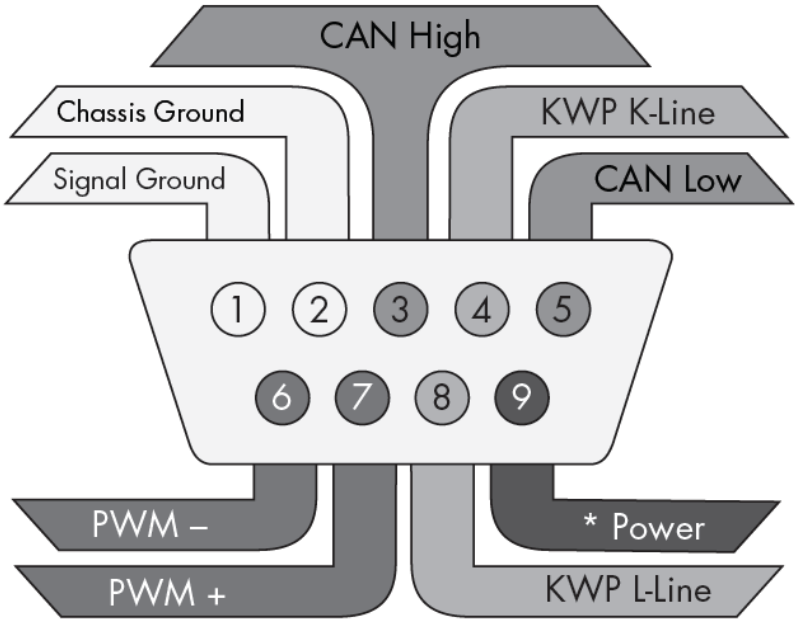
The Car Hacker's Handbook

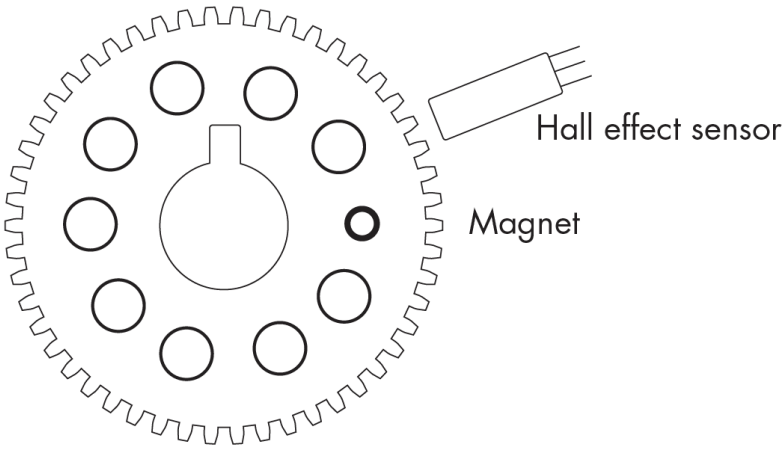
A Guide for the Penetration Tester

by Craig Smith

errata updated to print 10

Page	Error	Correction	Print corrected
19	... it won't break if another packet transmits extended CAN packets it won't break if another sensor transmits extended CAN packets ...	Print 5
19	When looking at extended packets in a network dump, you'll see that unlike standard packets, extended packets use substitute remote request (SRR) in place of the remote transmission request (RTR) with SSR set to 1.	When looking at extended packets in a network dump, you'll see that unlike standard packets, extended packets use substitute remote request (SRR) in place of the remote transmission request (RTR) with SRR set to 1.	Print 5
22	Figure 2-6 replacement	 <p>The diagram shows a CAN bus frame structure. It is divided into three main sections: Header, Data Bits, and CRC. The Header section contains 7 bits labeled P, P, P, H, K, Y, Z, Z. The Data Bits section contains 24 bits. The CRC section contains 15 bits.</p>	Print 5
24	Figure 2-9 replacement	 <p>The diagram shows a CAN bus response structure. It is divided into two main sections: Header and Response. The Header section contains 3 bits labeled Break, SYNC, ID. The Response section contains 4 fields: Data (0-8 bytes) and Checksum.</p>	Print 5
25	MOST divided into the seven layers of the OSI model. The OSI layers are in the right column.	MOST divided into the seven layers of the OSI model. The OSI layers are in the left column.	Print 5

Page	Error	Correction	Print corrected
33	Figure 2-19 replacement		Print 5
43	<pre># sudo insmod ./can-isotp.ko</pre>	<pre>\$ sudo insmod ./can-isotp.ko</pre>	Print 5
45	<pre>addr.can_ifindex = ifr.ifr_ifindex;</pre>	<pre>addr.can_ifindex = ifr.ifr_ifindex; bind(s, (struct sockaddr *)&addr, sizeof(addr));</pre>	Print 5
55	(If the response fails, you should see a 0x7F instead of the positive + 0x40 response.)	(If the response fails, you should see a 0x7F instead of the positive + 0x40 response.) You can send a request to 0x7DF and it should generate a response from all listening ECUs. This response value will be anything from 0x7E8 to 0x7EF. If you want to address just one ECU directly, you subtract 8 from the response value; for example, if you see a response of 0x7E8 you can use 0x7E0 to query only that ECU.	Print 5
95	It's a good idea to make a list of part numbers to feed to Google, datasheet.com , or something similar, to obtain a copy of the data sheet.	It's a good idea to make a list of part numbers to feed to Google, datasheets.com , or something similar, to obtain a copy of the data sheet.	Print 5
109	The result is the vector table shown in Figure 6-15, which looks sane enough: all addresses are above the 0x8000 entry point specified. Notice that the reset vector (0xFFFFE, RES-vector) has a pointer to the RESET_entry at 0xBE6D.	The result is the vector table shown in Figure 6-15, which looks sane enough: all addresses are above the 0x8000 entry point specified. Notice that the reset vector (0xFFFFE, RES_vector) has a pointer to the RESET_entry at 0xBE6D.	Print 5

Page	Error	Correction	Print corrected
121	Figure 7-6 replacement	 <p>The diagram shows a circular gear with 12 teeth. Inside the gear, there are 12 small circles arranged in a ring. A larger circle is in the center. A rectangular component labeled 'Hall effect sensor' is positioned to the right of the gear, with a line pointing to one of the small circles. Below the gear, the word 'Magnet' is written, with a line pointing to the same small circle.</p>	Print 5
125	Every so often a CAN signal shows up that resets the values to 00 00 and stops the speedometer from moving.	Every so often a CAN signal shows up that resets the values to 00 00 and stops the tachometer from moving.	Print 5
129	If you look up the model number in conjunction with the ST code, you'll learn that the STM32F407Vx series is an ARM Cortex M4 chip with support for Ethernet, USB, two CANs, and LIN as well as JTAG and Serial Wire Debug.	If you look up the model number in conjunction with the ST code, you'll learn that the STM32F407Vx series is an ARM Cortex M4 chip with support for Ethernet, USB, two CANs, and LIN as well as JTAG and Serial Wire Debug.	Print 5
163	The algorithm in Listing 9-3 reads in a byte at ❶, multiplies it by 5 at ❷, and then, at ❸, adds it to the hash to calculate the final sum.	The algorithm in Listing 9-3 reads in a byte at ❶, shifts left by 5 at ❷, and then, at ❸, adds it to the hash to calculate the final sum.	Print 5
195	<pre data-bbox="178 990 1008 1120">\$ gcc -o temp_shellcode temp_shellcode.c \$ ls -l temp_shell -rwxrwxr-x 1 craig craig 8722 Jan 6 07:39 temp_shell \$./temp_shellcode</pre> <p>Now run <code>candump</code> in a separate window on <code>vcan0</code>, as shown in the next listing. The temp_shellcode program should send the necessary CAN packets to control the temperate gauge.</p>	<pre data-bbox="1045 990 1879 1120">\$ gcc -o temp_shell temp_shell.c \$ ls -l temp_shell -rwxrwxr-x 1 craig craig 8722 Jan 6 07:39 temp_shell \$./temp_shell</pre> <p>Now run <code>candump</code> in a separate window on <code>vcan0</code>, as shown in the next listing. The temp_shell program should send the necessary CAN packets to control the temperate gauge.</p>	Print 5
207	The main ID is the common ID with the shortest average interval—in this case, signal 0x143 at 0.009998 ms .	The main ID is the common ID with the shortest average interval—in this case, signal 0x143 at 0.009998 s .	Print 5
211	In FSK, a high-frequency signal is a 0 , and a low-frequency signal is a 1 .	In FSK, a high-frequency signal is a 1 , and a low-frequency signal is a 0 .	Print 5
214	As mentioned, sensors generally transmit around once a minute, but rather than waiting 60 seconds for the sensor to send a packet, an attacker can send a 125 kHz activation signal to the TPMS device with an SDR to elicit a response.	As mentioned, sensors generally transmit around once a minute, but rather than waiting 60 seconds for the sensor to send a packet, an attacker can send a 125 kHz activation signal to the TPMS sensor with an SDR to elicit a response.	Print 10

Page	Error	Correction	Print corrected
214	To improve your chances of capturing signals, send the activation signal to wake up the device as it passes.	To improve your chances of capturing signals, send the activation signal to wake up the sensor as it passes.	Print 10
236	The two empty 28-pin sockets in the lower-left corner have been added to the original ECU.	The two 28-pin sockets in the lower-left corner have been added to the original ECU.	Print 3