Zadanie nr 6

Bezpieczeństwo przesyłania danych

Jak wiemy, w profesjonalnych sieciach przemysłowych stosowane są różnorodne metody weryfikacji poprawności przesyłanych danych. Dość powszechnie stosowana jest metoda nadmiarowej redundancyjnej sumy kontrolnej (CRC). Metoda ta jest wykorzystywana między innymi w sieciach: MODBUS, PROFIBUS, HART, CAN, Foundation Fieldbus, itd. Istnieje jednak pewne skończone prawdopodobieństwo, że jeśli mimo to przesyłana ramka komunikacyjna zostanie zniekształcona to odebrana suma kontrolna będzie poprawna. Taka ramka zostanie poprawnie przyjęta przez urządzenie odbiorcze, co może mieć poważne konsekwencje. Możemy w tym przypadku stwierdzić, że zostało narażone bezpieczeństwo przesyłu danych. Zwykle, obok CRC, systemy komunikacyjne wykorzystują uzupełniające metody weryfikacji poprawności przesyłania danych np. bity parzystości, kontrolę zakresu wartości określonych pól ramki komunikacyjnej itp.

Opis sytuacji

Pewien haker należący do organizacji Against War zdobył informację, że dynamiczny kod dostępu do tajnego składu broni masowej zagłady pewnej organizacji militarnej przesyłany jest siecią Modbus RTU.
Informacje szczegółowe, które dodatkowo zdobył są następujące:

- jednostka master wysyła kod rozkazem o kodzie 0x10
- system zamków magazynu jest obsługiwany przez jednostkę slave o stałym adresie 0x0A
- kod dostępu jest kodem128 bitowym
- jednokrotne podanie niewłaściwego kodu do zamka wiąże się z jego automatycznym zniszczeniem.
- poprawność samego kodu jest weryfikowana dodatkowo przez CRC, która dla zmylenia wyznaczana jest tak jak standardowa CRC w specyfikacji sieci Modbus.

Skaner, który został zainstalowany przez przyjaciół hakera tuż przy jednostce master zarejestrował ramkę z nieczytelnym kodem dostępu do składu broni o postaci:

Pole adresu		0x0A
Pole funkcji		0x10
Adres pierwszego rejestru kodu		0x0000
Adres ostatniego rejestru kodu		0x0008
Liczba bajtów pola danych		0x12
Pole danych	kod	0x????
	kod	0x????
	kod	0x????
	kod	0x????
	kod	0x????
	kod	0x????
	kod	0x????
	kod	0x????
	CRC kodu	0xA77C
	CRC ramki	0x????

Zadanie 6
a) Odtworzyć kod dostępu do zamka składu broni.
b) Ile jest możliwych kodów dostępu? Odpowiedź udowodnić.
c) Proszę o komentarz, jakie informacje należałoby zdobyć, aby kod został wyznaczony w sposób jednoznaczny.

Punktacja:

Zadanie 6 a	4 punkty
Zadanie 6 b	4 punkty
Zadanie 6 c	2 punkty