Example of essay on covert channels

Part A

Error message in the ICMP protocol is a truly a good example of a storage channel. As the writer argued, it is the information about the operating system, contained in the echoing message, which can be exploited by the hackers. The most prevalent attack that face is identity theft and password cracking. The typical purpose of error message is to send a report of any error that occurs during datagram processing by providing feedback on any problem within the communication environment. However, the error message does not make the IP reliable. The error message is not effective because it does not guarantee the delivery of datagram or return of control message. In some cases, the datagram is not delivered and there is no nitification. The writer's mitigation mechanism of entering a set of zero's in the fields that are reserved and eliminating critical information is the best for this situation.

Reference

Frankel et al, S. (Dec 2005). Guide to IPsec VPNs. NIST Special Publication 800-77 .
Harrington, J. (2009). Network Security: A Practical Approach. Academic Press.

Part B

As the writer argued, timing channel is a type of covert channel which depends on time. However, the example that the writer gave does not indicate an ideal example for a timing covert channel. An ideal example is a

case of a military base with two individuals operating at different levels of security. Since the only medium of communication is a single computer that is separate, the computer which transmits the signal can simply request the data to be sent from the other computers. It processes it and move to the next computer. Since they transmit binary signals continuously, the hackers can monitor and get the signal using time. When the computer sends the signal instantly, then the other computer operating at higher security can realize. The writer's recommendation of changing the algorithm and using the same CPU to confuse the hacker is suitable.

References

Bernard, L. (2010). Network and System Administration. NeXT Computer, Incorporated.

Perlman, R. (2000). Key Exchange in IPSec: Analysis of IKE, IEEE Internet Computing. Cengage.