Introduction to Computer Security

Matt Bishop

AAddison-Wesley

Boston • San Francisco • New York • Toronto • Montreal
London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

Contents

Cybersecurity Fundamentals â€“ Introduction to Cybersecurity. Cybersecurity Firewall: How Application Security Works? Cybersecurity Threats and State of Our Digital Privacy.Â Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system. There are various types of computer security which is widely used to protect the valuable information of an organization. What is Computer Security and its types? One way to ascertain the similarities and differences among Computer Security is by asking what is being secured. For example Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications). Integrity: In lay usage, information has integrity when it is timely, accurate, complete, and consistent.Â 1. Introduction. deliberate or inadvertent unauthorized manipulation of the system."7 The definition of integrity has been, and continues to be, the subject of much debate among computer security experts. Availability: A "requirement intended to assure that systems work promptly and service is not denied to authorized users."8. Computer security, cybersecurity or information technology security (IT security) is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.[1].Â Failed offensive strategy[edit]. The National Security Agency (NSA) is responsible for both the protection of U.S. information systems and also for collecting foreign intelligence.[10] These two duties are in conflict with each other. Protecting information systems includes evaluating software, identifying security flaws, and taking steps to correct the flaws, which is a defensive action.