Joshua Main-Smith
November 15, 2020

Legal Aspects, Security Policy, Trusted Platform

1. (10 points) The table below is the categorization of eCrime from US CERT.

For each of the cybercrimes cited, indicate whether it falls into the category of *computer as target*, *computer as storage device*, or *computer as communications tool*. In the case of computer as target, indicate whether the crime is primarily an attack on *data integrity*, *system integrity*, *data confidentiality*, *privacy*, or *availability*. Give a short justification for each answer.

Cybercrime	Category	Target Subcategory Attack on..	Justification
Malicious code	target / communication	data integrity	Depending on the purpose of the malware, it could be used to gain access to a target machine or (as has been more common recently) be used to mine cryptocurrency (a botnet of zombies accomplishing this).
Unauthorized access	target	data confidentiality	An attacker can gain unauthorized access to a computer for the purpose of pivoting to another computer of interest, or it could be the primary target. Most attackers are outsiders that would have access to confidential information. Data integrity could be at stake in the event of ransomware.
Spam	communication		The primary purpose of spam is to expose the user to services that are being sold.
Spyware	target	privacy	Spyware is frequently used to acquire the private information on a user's computing device. Keylogging would be such a technique. This would violate the user's right to privacy.
Denial of service	target	availability	The primary purpose of DoS is to deny an authorized user from using a given service,

			making it unavailable. This could be used to mount further attacks while a given critical service is unavailable.
Credit card fraud	target	data confidentiality	Only individuals with roper authorization should have access to credit card information. Credit card fraud is a breach of this confidentiality.
Phishing	target	data confidentiality	The primary purpose of phishing attacks is to gain access to confidential information, namely user credentials.
Theft of customer information	target	data confidentiality	Customer information should only be viewable by authorized individuals (customer, company, etc). A breach (such as credit card information of customers from a retailer) would be a violation of data confidentiality.
Theft of intellectual property	target	availability	The purpose of IP is to make it available to customers for those who have a right to use (such as a paying customer). Theft of IP makes the work available to those who don't have a right to use.
Exposure of information	target	privacy	A person has a right to privacy. Intentional exposure of a person's private information without their prior authorization would be a breach of their right to privacy.
Identity theft	target	data confidentiality	A customer/employee's identity should be confidential and readable only for those who have authorization. A breach in this would be a breach in data confidentiality.
Sabotage	target	system integrity	Intentionally destroying system information would deny the

			system of accurate information, thereby leading to a breach in system integrity.
Botnets	target / communication	availability	Botnets are used as a means to an end. One method could be the use of several computers for the purpose of crypto mining. Another could be for the use in a DoS attack, making a service for a company unavailable.
Website defacement	target	data integrity	The accuracy of the website is in question when there is defacement, thereby leading to a breach in data integrity.
Extortion	communication		Here, an attacker has probably gained access to sensitive information and is demanding payment, probably through cryptocurrency, in exchange for non-disclosure of said sensitive information.

2 (10 points) The necessity of the "no read up" rule for a multilevel secure system is fairly obvious. What is the importance of the "no write down" rule?

The "no write down" rule is important so that sensitive information from levels containing more sensitive information doesn't leak down to categories with less sensitive information. An example of where this could go wrong is the case in which an attacker has gained control of a high level system. An attacker could craft malware that, when applied to the high level system, could successfully propagate to lower level systems by writing to them. This is a current method of malware writers to systems. By taking control of, say, the antivirus of the system it could have complete control of the system (as the antivirus does). Preventing systems from writing down would prevent the cascade of malware propagation from occurring.

3. (10 points)

Documents can have the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the compartments A, B, and C. Specify what type of access (read, write, both, or neither) is allowed in each of the following situations.

a) Paul, cleared for (TOP SECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).
Neither

b) Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }).
Neither

c) Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).
Read

d) Sammi, cleared for (TOP SECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, { A }).
Read

e) Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }).
Write

4. (10 points) A noted computer security expert has said that without integrity, no system can provide confidentiality.

a) Assume the system provides no integrity controls. Do you agree with the noted computer security expert? Justify your answer.

Integrity is the prevention of intentional or accidental unauthorized changes. Confidentiality is the prevention of individuals from accessing unauthorized information. No integrity controls would mean that there would be no way for an industry to verify that information hasn't been altered and therefore there would be no guarantee that confidentiality has been maintained. If there is no way of knowing if confidentiality has been maintained, then an organization couldn't accurately claim to keep confidentiality.

b) Now suppose the system has no confidentiality controls. Can this system provide integrity without confidentiality? Again, justify your answer.

Confidentiality requires persons to be authenticated to perform some task (read, write, etc.). If there are no confidentiality controls, then an individual, that would otherwise be deemed unauthorized, could write to data violating integrity (John Doe giving himself a raise, e.g.). So, integrity can't be guaranteed without confidentiality.