Advances in Robotics & Automation

Keung HY, Adv Robot Autom 2014, 3:3
DOI: 10.4172/2168-9695.1000e122

Editorial Open Access

Risks Affecting Data Security

YAU Hon Keung*

Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Kowloon, Hong Kong

***Correspondence author:** YAU Hon Keung, Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Kowloon, Hong Kong. E-mail: honkyau@cityu.edu.hk

Rec Date: July 1 2014; **Acc Date:** July 5 2014; **Pub Date:** Dec 24, 2014

Introduction

From Acquisti [1], there are many kinds of risk affecting data security, so important decision predicating this analysis is what kind of adversary is to be considered such that any system are evaluated for resistance to various types of attacks.

Risk

Insider theft

As Jamsa [2] suggests, the risk of computer and data theft is very real, both from within the company and from those who can connect to the company. When it happens to have a data breach, it is important for the public to immediately understand broadly as to whether their personal information may be involved. The unaccomplished intended transparency of most breach laws encourages bad behavior on the part of companies who should be more concerned about the protection of the privacy of their customers. Consumers should know if they are at risk from even a small breach. The details of a breach help determine their risk factors as well as guide them in proactive measures.

Burglary

Burglary is a crime which is quite close to theft, and is the essence of which is entry into a building for the purposes of committing an offence.

There are a few points about the meaning of burglary

1. Breaking can be either actual, like by forcing open a door, or constructive, like by fraud or threats. Breaking does not require that anything be "broken" in terms of physical damage. A person who has permission to enter part of a house, but not another part, commits a breaking and entering when they use any means to enter a room where they are not permitted, so long as the room was not open to enter.
2. Entering can involve either physical entry by a person or the insertion of an instrument with which to remove property. Insertion of a tool to gain entry may not constitute entering by itself. It is required that entry occurs as a consequence of the breaking. House includes a temporarily unoccupied dwelling, but not a building used only occasionally as a habitation
3. Night time is defined as hours between half an hour after sunset and half an hour before sunrise. The law definition has been expanded in most jurisdictions, such that the building need not be a dwelling or even a building in the conventional sense, physical breaking is not necessary, the entry does not need to occur at night, and the intent may be to commit any felony or theft.

Hacks

Hacking is a very typical way in attacking Internet-connected system. There are a few approaches like Network enumeration which is discovering information about the intended target, vulnerability analysis to identify potential ways of attack and exploitation: attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.

In order to hack into computer systems, there are several tools and techniques used by computer criminals and security experts.

Security exploits

A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery which abuse security holes that may result from substandard programming practice.

Vulnerability scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners which check to see which ports on a specified computer are "open" or available to access the computer, and can also know what program or service is listening on that port, and its version number.

Password cracking

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.

Spoofing attack

A spoofing attack means that one program, system, or website successfully pretends to be another by falsifying data and so being treated as a trusted system by a user or another program. The purpose is to fool programs, systems, or users into revealing confidential information to the attacker such as user names and passwords.

Social engineering

Social Engineering is the art of getting persons to reveal sensitive information about a system. This is usually done by impersonating someone or by convincing people to believe you have permissions to obtain such information.

Trojan horse / Virus / Worm

A Trojan horse is a program which seems to be doing one thing, but is actually doing another like a spy. A Trojan horse can be used to set up a back door in a computer system such that the intruder can gain access later.

A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents just like a biological virus spreading by inserting itself into living cells.

A worm is also a self-replicating program like a virus. A worm is different from a virus that it propagates through computer networks without user intervention and it does not attach itself to an existing program.

Key loggers

A key logger is a tool designed to ―log‖ (record) every keystroke on an affected machine for later retrieval. Its purpose is to allow the intruder to gain access to confidential information typed on the affected machine, such as password or other private data. Some key loggers even uses virus, trojan, and rootkit-like methods in order to remain active and hidden. However, some key loggers are used in legitimate ways and sometimes to even enhance computer security like catching employee fraud on a computer used at a Point of Sale through collecting data.

References

1. Acquisti A, Gritzalis S, Lambrinoudakis C, Vimercati SC (2008) Digital Privacy: Theory, Technologies, and Practices. Auerbach Publications, NY.
2. Jamsa K (2002) Hacker Proof second edition. OnWord Press, Canada.