Examples of exam questions connected to the lecture on program security

2011-10-25

Problem 5

This morning's edition of the newspaper Metro had a short report on a statement made to the press by Pia Lindström of the Swedish Theft Prevention Association (Stöldskyddsföreningen – SSF). It is reported to be in connection with the fact that many people choose to hide their valuables and cash in such places as in the freezer or sewn into the curtains. The quote was (in translation from the Swedish) "All of these presumed clever places that one might think of have also been thought of by those who would steal from you " (Metro2010).

This advice is analogous to a principle that is well understood in the field of IT Security. Describe and explain that principle, and give an example of a realistic scenario (preferably a true history scenario if you are able to quote any such) where failure to apply this principle has resulted in a security breach of an IT system.

References

Metro2010 (Attributed to) TT, 2010. "Alla de här fiffiga ställen..." .Metro Stockholm, 25 Oct. p.3f

2011-12-19

Problem 3

Explain how the application of Saltzer and Schroeder's principles for the design of security systems might help to avoid the common vulnerabilities of

- buffer overflows
- poorly configured firewalls

Be specific in which principles you consider to be the most relevant and why.

Problem 5

A private computer user has noted that there are many firewall products available and she asks you for advice on how to choose and run firewalls for the small number of computers she has in her home network. Her main worries are that some software might not be dependable.

Give well motivated objective advice that can be of use in selecting a trustworthy firewalls, as well as some measures that are reasonable to take to ensure that the firewall systems run securely.

You may assume that the user is an enthusiastic computer user, i.e., not entirely naïve and willing to go to reasonable effort to learn. You should not assume that firewalls will run on any particular operating system.

Problem 4

Describe each of the following IT security related terms. Also, for each of these terms further illustrate the concept by choosing a closely connected IT security concept and explaining the relationship between the concepts. Furthermore, give an example of an application of these tools/threats/concepts. Give concrete examples wherever possible. Structure each of your answers with headings *description*, *relationship to [your chosen related concept]*, and *example.*

Some students may find it helpful to use the pre-printed problem 4 answer sheet for their answer. Those who choose not to should take care to follow the above instructions extra carefully.

Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem

- Hard Certificate
- **Saltzer and Schroeder's Principle of Psychological Acceptability**
- Phishing
- **Buffer Overflow**

2012-12-20

Problem 4

Describe each of the following IT security related terms. Also, for each of these terms further illustrate the concept by choosing a closely connected IT security concept and explaining the relationship between the concepts. Furthermore, give an example of an application of these tools/threats/concepts. Give concrete examples wherever possible. Structure each of your answers with headings *description*, *relationship to [your chosen related concept]*, and *example.*

Some students may find it helpful to use the pre-printed problem 4 answer sheet for their answer. Those who choose not to should take care to follow the above instructions extra carefully.

Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem

- Public Key Infrastructure (PKI)
- **Cross Site Scripting**
- The Common Criteria
- DMZ

2012-12-20

Problem 5

Imagine open source firewall software that is very small and effective and that is designed to run on a machine that is dedicated for the purpose, i.e. only a minimal operating system and the firewall runs on the hardware. The firewall itself is run with the minimal privileges required in order to read and write to its two network interfaces. In order to configure the firewall the administrator enters a sequence of rules, each one with a match part, and an action part. If any incoming package matches the match part, then it is handled according to the action part.

An example of such a rule (taken out of the context where the included variables have been defined and where lines beginning with '#' are comments) is (in an adaption from [Andre01]):

```
# In Microsoft Networks you will be swamped by broadcasts. These lines
# will prevent them from showing up in the logs.
#

$SECIFIREWALL -A udp_packets -p UDP -i $INET_IFACE -d $INET_BROADCAST \
--destination-port 135:139 -j DROP
```

If an incoming package does not match any of the rules it is passed (unaltered) through the firewall.

Given this description, give fully motivated suggestions as to which of Saltzer and Schroeder's Design Principles for Security Systems may not have been sufficiently followed in the design of this firewall software and explain briefly how this may negatively effect the security of the system.

The principles are (as summarised in [Bishop05]):

The Principle of Least Privilege
The Principle of Fail-Safe Defaults
The Principle of Economy of Mechanism
The Principle of Complete Mediation
The Principle of Open Design
The Principle of Separation of Privilege

The Principle of Least Common Mechanism
The Principle of Psychological Acceptability

2013-08-12

Problem 3

Give an illustrative and realistic example of the importance and value of the security principle of *defence in depth*.

This is not a principle that is represented in Saltzer and Schroeder's list of principles for the design of security systems. They do however have at least one closely related concept. Relate the principle of defence in depth to any similar principles that are included in Saltzer and Schroeder's list.

2011-08-25

Problem 5

If you have built a secure software system, two possible ways to convince customers that your security is good may be to distribute the system as open source, and to Common Criteria certify your system. Discuss advantages and weaknesses of these two schemes for assuring customers of your system's security.

2010-11-27

Problem 5

Saltzer and Schreoder's principles for the design and implementation of security mechanisms are summarised as:

- The Principle of Least Privilege
- The Principle of Fail-Safe Defaults
- The Principle of Economy of Mechanism
- The Principle of Complete Mediation
- The Principle of Open Design
- The Principle of Separation of Privilege
- The Principle of Least Common Mechanism
- The Principle of Psychological Acceptability

Pick the three principles that you consider would be most important for the design of a secure and efficient firewall, and fully motivate the choice that you make including reasons why other principles are assumed to be less important.