Systemsicherheit

1. **Risks in Electronic Payment:**

   From your personal experience: Which risks are involved in electronic payment systems? Start with thinking about the vulnerabilities of today's methods, procedures, and mechanisms you are familiar with. Here are two possible scenarios:

   (a) Paying with a debit card (e.g. EC Maestro): starting with its use in a shop and ending with the money withdrawal from your bank account.

   (b) Home banking using a static (e.g. snail-mailed) or dynamically generated transaction authentication number (TAN), e.g. sent from your bank via SMS (mTAN) or using a smartphone app (pushTAN).

   What are the advantages of smart cards (such as your thoska), carrying a microprocessor for cryptographic computations?

   Solution: Electronic payment involves theft of data or money. Hackers may get access to bank accounts and use it the same way as the normal user but with different intentions (get rich). To prevent hacking of accounts, banks use different ways of defense.

   While paying with a debit card, the user must provide the card (physical item) and the pin code (knowledge). To prevent bruteforce attacks, a bank account is locked after a short number of invalid pin codes.

   Home banking uses a password (knowledge) and a TAN via Mail/Phone to have the possibility of hackers minimized.

2. **Buffer Overflow Attacks:**

   Which vulnerabilities are exploited by a buffer overflow attack? How can you counter buffer overflow attacks? How could you at least mitigate the effects of successful buffer overflow attacks?

   Solution: Buffer overflow attacks aim to trick the softwar to execute futher attack code and exploit whatever the hacker needs. To prevent buffer overflow, one must check the maximum possible length of the input versus the users input. To mitigate any successfull attack, a programm should be contained and not have access to further information or programms but the necessary.

3. **Data vs. Information:**

   (a) What is the difference between data and information?

   (b) What are the consequences for systems security?

   Solution: Data is a collection of values like characters, numbers or other data types. Unprocessed data have little to no meaning to a human. Information is processed data so a human can read, understand and use it.

4. **Root Kits:**

   Which special properties of root kits make them so extremely dangerous?

   Solution: Invisible, total sustainable takeover of a complete IT system. Root Kits are a comprehensive tool kit for fully automated attacks on all levels of the software stack.

5. **NI: Dynamic Properties:**

   Similar to HRU, an NI model is basically formalized through a deterministic automaton. Can we also use it to analyze HRU Safety (no matter if by proof or by simulation)?

   If yes: How would HRU Safety for NI be defined (in prose)? If no: What extension of the NI model in the lecture would be required to enable Safety analysis?

   Solution:

6. **NI: Motivation:**

   Which security problem do NI models address? Name two modern application scenarios where this problem is highly relevant!

   Solution:

7. **BLP and Biba:**

   What's the difference in terms of goals and formalism between the BLP and the Biba model?

   Solution:

8. **BLP: Lattice vs. ACM:**

   (a) Why does the BLP model contain both: (1) a lattice, which is mapped to subjects and objects via cl, and (2) an ACM?

   (b) What problem might occur from using both (1) and (2)?

   Solution:

9. **DAC vs. MAC:**

   (a) What is the difference between discretionary (DAC) and mandatory access control (MAC)?

   (b) What are the weaknesses of discretionary access control systems?

   Solution:

10. **TAM: Type System:**

    How is the type system in TAM formally represented within the HRU-based automaton? Which parts of the type system may change during runtime?

    Solution:

11. **TAM: Motivation:**

    What is the goal of the TAM security model?

Solution:

12. **RBAC ACF:**

    As with any AC model, the formal components of RBAC are designed to enable access control decisions. However, in the ACF definition of RBAC0 (which is the basis for ACFs of the other RBAC96 models), the component UA is not included. Why?

    Solution:

13. **RBAC Safety:**

    How can we analyze RBAC safety? Which information is needed for this, and is it provided by RBAC96 models?

    Solution:

14. **IBAC vs. RBAC vs. ABAC:**

    What is the key difference between IBAC and RBAC models? How about ABAC models then?

    Solution:

15. **HRU Safety Undecidability:**

    Given HRU Safety is undecidable, what is the actual merit of this model? What can we do to handle the undecidability problem in practice?

    Solution:

16. **HRU: Unix Read:**

    How do we model a read operation, such as for a Unix-OS file system, in HRU? Remember that this operation neither modifies the subject set, nor the object set, nor the ACM.

    Solution:

17. **ACM vs. HRU:**

    What is the idea that distinguishes an ACM from an HRU model? How is it formally represented?

    Solution:

18. **HRU: Output Function:**

    Why does an HRU automaton not have an output function?

Solution:

19. **Core-based Model Engineering:**

Assume you have to design the security policy for a very simple hospital information system, including

- users in roles such as physician, nurse, etc.
- legal information flows between these roles
- one operation to change a user's roles.

Re-use the model abstractions you know from chapter 3 to express this policy as a core-based model by answering the following questions:

(a) Which formal components do you need beyond the actual model core? (2 sets and 2 relations should suffice!)

(b) What is the core specialization?

(c) What is the core extension?

(d) What are possible pre- and post-conditions of the only operation?

Solution:

20. **Common Model Core:**

What is the common model core shared by models such as HRU, DRBAC, BLP, Brewer-Nash, and NI?

Solution:

21. **Hybrid Models:**

Name the semantical concepts from AC, IF and/or NI models that can be found in

- the Brewer-Nash model
- the LR-CW model
- the the MLS-CW model.

Compare how these three models express allowed information flows according to the CW policy.

Solution: