3.1 Physical Security versus Logical Security

[Gol99] [IGD]

3.2 How to Hide a Logical Bomb

a) *What changes if $\mathbb{H}$ in their schemes is not a one-way function?*
For a function to be one-way it must be infeasible to get the input only with the knowledge of the image, but only by brute forcing all possible inputs which can take a very long time.
This is necessary for these schemes because otherwise it would be easy to compute N with $M = \mathbb{H}(N)$. Furthermore a preimage attack can be executed if the hash-function is not *one-way*, s.t. for any A it is easy to find a B which satisfies $\mathbb{H}(B) = A$ for any hash-function $\mathbb{H}$, because in these schemes there is no preimage resistance.

b) *How can the execution environment defend itself and other applications running on it against malicious code like this?*
For example, an agent could be designed such that it can only run in certain environments. It would then collect auditing data on certain types of machines or of the network it is currently in and can only carry out transactions or complete its task within a network of a certain vendor. An example for this would be a *directed virus*, which will carry out a special set of instructions only if it is run in a certain environment. The point of this idea is that without the explicit knowledge of the activation environment its "special instructions" would not reveal themself and cannot be determined [RS98].
The next "defense mechanisms" were found in [AB05] *(there are also more than the once described here)***:**
If an mobile agent would travel across a multi-hop network and visits many different platforms that can be not trust-worthy the agent could have been converted into a malicious one during its trip. Therefore a mobile agent should be able to maintain an authenticable record of the previously visited platforms such that the platform can make a decision on whether to run the mobile agent or not.
Another way to prevent malicious attacks would be *"Code Signing"*. It is used to verify that the code of the mobile agent was not altered or tempered with. For example it makes use of a digital signature and an one-way hash function. A current example for such a scheme would be Microsoft Authenticode which is usually used for signing code such as ActiveX controls and Java applets.

Bibliography

[AB05] ALFALAYLEH, Mousa ; BRANKOVIC, Ljiljana: An Overview of Security Issues and Techniques in Mobile Agents. In: *International Federation for Information Processing Digital Library; Communications and Multimedia Security;* 175 (2005), 10. `http://dx.doi.org/10.1007/0-387-24486-7_5`. – DOI 10.1007/0–387–24486–7_5. ISBN 0–387–24485–9

[Gol99] GOLLMANN, Dieter: *Computer Security*. USA : John Wiley & Sons, Inc., 1999. – ISBN 0471978442

[IGD] *Inside A Google Data Center: 2020 Version*. `https://datacenterfrontier.com/inside-a-google-data-center-2020-version/`. – Accessed: October 19, 2021

[RS98] RIORDAN, James ; SCHNEIER, Bruce: Environmental Key Generation Towards Clueless Agents. In: *Mobile Agents and Security*, 1998