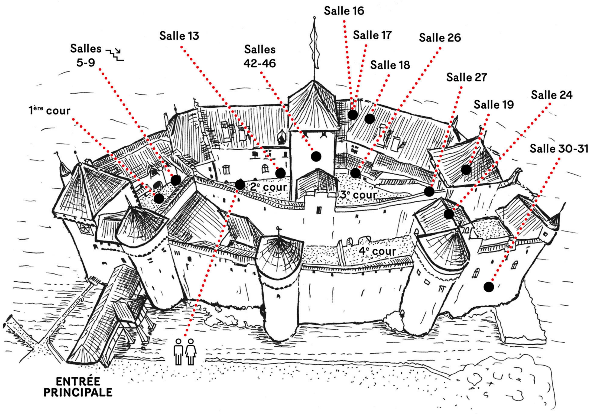
Institute of Computer Science, University of Bern
Privacy and Data Security, HS 2021

Prof. Christian Cachin
Orestis Alpos, Luca Zanolini

Exercise 3

3.1 Physical security versus logical security (6pt)

1. **Physical security:** Read the following brief article on the security of data centers and watch the embedded promotion video "6 layers of security" by Google:
   `https://datacenterfrontier.com/inside-a-google-data-center-2020-version/`
   It is not a coincidence when this reminds you of a medieval castle, like the spectacular Château de Chillon (image from `www.chillon.ch`):



2. **Logical security:** Read Section 3.4 in Gollmann's textbook [Gol11] (linked vial ILIAS).
3. **Integrated view;** Compare a diagram of Google's "six layers" or Chillon's four rings with the "layer" model of logical security shown in class and in the textbook [Gol11]. You will recognize that the concentric rings in the physical-security models are in the reverse orientation with respect to the logical-security models:

   > The most valuable entity to protect is in the innermost physical ring and obtains its security from the outer rings. In the logical model, though, the application is at the top of the stack of layers and gains its security from the layers below.

   Develop a combined and integrated model of physical and logical security for computing services with their physical realization. We suggest you create a graphical model and explain it with a few sentences.

⟹

3.2 How to hide a logical bomb (4pt)

Get the paper "Environmental Key Generation towards Clueless Agents" by Riordan and Schneier [RS98] and read sections 1–3. The paper is also available from Schneier's website under `https://www.schneier.com/academic/archives/1998/06/environmental_key_ge.html`

The term "mobile agent" may surprise you, but this was in an era when, for the first time, it became common that code was sent over a network from one computer to another and executed immediately there. This is so common today it no longer has a special name.

a) What changes if $\mathcal{H}$ in their schemes is not a one-way function? (If necessary, read up on one-way functions and hash functions.)

a) How can the execution environment defend itself and other applications running on it against malicious code like this?

References

[Gol11] D. Gollmann, *Computer security (3. ed.)*, Wiley, 2011.

[RS98] J. Riordan and B. Schneier, *Environmental key generation towards clueless agents*, Mobile Agents and Security (G. Vigna, ed.), Lecture Notes in Computer Science, vol. 1419, Springer, 1998, pp. 15–24.