

Introduction to IT Security - Exercise sheet 1

Vianney HERVY

0. Use of generative AI

This report was written in Typst¹, a LaTeX equivalent. To help me with the unfamiliar math syntax², symbols³ and the layout, I used Google's Gemini⁴. I also cross-checked the facts by submitting my work along with the slides. Finally, I checked the spelling and formulations.

1. User Authentication: Passwords

According to the instructions, there are 26 possible characters for each one of the 14 symbols of the password. This gives $26 \times \dots \times 26 = 26^{14} \approx 6.45 \cdot 10^{19}$ different passwords.

1.1. Base case

To get a specific password, it would take the attacker $6.45 \cdot 10^{19}$ attempts (number of passwords).

He can make $40000_{\text{tries/s}} \times 86400_{\text{s/day}} \approx 3.46 \cdot 10^9$ tries per day.

It would then take him $\frac{6.45 \cdot 10^{19} \text{ tries}}{3.46 \cdot 10^9 \text{ tries/day}} \approx 1.87 \cdot 10^{10}$ days.

This result is the worst case, if the targeted password is tried last. On average, it would take him approximately half that time (same order of magnitude)

1.2. Irregular distribution

The answer here depends on the attacker's strategy. The optimal one is to only test the 1,000 popular passwords and get 90% of the passwords in a fifth of a second. But having a correct password is not enough; the user has to match as well ("The right key is nothing without the right lock").

There are $5000 \times 90\% = 4500$ vulnerable users.

Each attempt is a user-password pair. The probability that that specific user has that specific password from the popular list is:

$$P(\text{User is vulnerable}) \times P(\text{User chose this password}) = 90\% \times \frac{1}{1000} = 0.0009$$

To get 90 passwords, the attacker would have to do $\frac{90}{0.0009} = 1 \cdot 10^5$ attempts

Given a 5000 rate, it would take him $\frac{100000_{\text{tries}}}{5000_{\text{tries/s}}} = 20$ seconds to find a matching pair.

1.3. Defense

Let $P_{\text{vulnerable}}$ (resp. P_{secure}) be the probability that the targeted account is vulnerable (resp. secure) and $P_{\text{success}|\text{vulnerable}}^{(n)}$ (resp. $P_{\text{success}|\text{secure}}^{(n)}$) the probability to guess correctly a vulnerable (resp. secure) password in n tries.

The total probability of success is:

$$P_{\text{success}}^{(n)} = \left(P_{\text{secure}} \times P_{\text{success}|\text{secure}}^{(n)} \right) + \left(P_{\text{vulnerable}} \times P_{\text{success}|\text{vulnerable}}^{(n)} \right)$$

¹<https://typst.app/>

²<https://typst.app/docs/reference/math/>

³<https://typst.app/docs/reference/symbols/sym/>

⁴<https://gemini.google.com/>

replacing with the values found earlier, we get

$$P_{\text{success}}^{(n)} = ((1 - 90\%) \times \frac{n}{26^{14}} + \left(90\% \times \frac{n}{1000}\right))$$

The chance of finding a “secure” password is negligible for the probable value of n we will get. The equation simplifies as such:

$$P_{\text{success}}^{(n)} \approx 0 + n \times 0.0009$$

We want

$$P_{\text{success}}^{(n)} \leq 1 - 60\%$$

thus

$$n \times 0.0009 \leq 0.4$$

therefore

$$n \leq \frac{0.4}{0.0009} \approx 444.444$$

But $n \in \mathbb{N}$ so the highest acceptable value is $n = 444$ attempts before shutting down the auth mechanism for this user.

This value is pretty high and no regular user would need so many attempts, n can be lowered to an eighth (56 attempts) to allow even safer authentication.

2. Access Control

2.1. Mobile Apps

Pinterest⁵ is a social media where users can view, share, comment and save “pins”. Pinterest requests access to the contacts (read), location (read), camera (read) and storage (read/write).

Too Good To Go⁶ connects customers to restaurants and stores to save unsold food surplus. The app requires the user’s location (read) and their calendar (write).

Bonjour RATP⁷ is the official app of the Parisian public transportation company. It requires access to the user’s location (read) and to their physical activity data (read)

All these permissions are grouped from the app’s perspective, the access rights are associated with the subject (the app). This is a capability list. Mobile systems use capability lists because each app runs in its own sandbox and needs only small, explicit permissions instead of complex resource-based rules. Capabilities are simpler for users and developers, enforce least privilege cleanly, and avoid the overhead of maintaining global access control lists. This model scales better, is easier to secure, and matches how mobile OS APIs are designed.

2.2. Role-based Access Control

Roles allow permission grouping to avoid granting the same permissions again and again.

Inheritance is also permitted, enabling simpler permission distribution and management. Roles may also be parameterized or hierarchized.

⁵<https://www.pinterest.com/>

⁶<https://www.toogoodtogo.com/>

⁷<https://www.bonjour-ratp.fr/en/>

In an application like Moodle, the users can be grouped by role with parameters: “student of [program]”, “lecturer of [subject]”, “head of [department]”. The permissions can be direct functions of these parameters: student can only read a course he is taking, lecturer can only write a course he is giving etc.

3. Application Whitelisting

1. Explain how application whitelisting works with WDAC (Windows Defender Application Control)

Windows Defender Application Control enforces application whitelisting by using a policy that defines trusted apps (via the publisher, package, etc). Every executable, script or driver is checked against this policy, allowing only verified (approved) apps to run and blocking all others. The philosophy is that an unknown app is considered potentially unsafe until proven otherwise.

2. Does WDAC restrict users/processes with respect to executing code ? How ?

Yes, WDAC restricts code execution by enforcing its policy on all user accounts and processes. When a user or a process attempts to run an app, WDAC checks if the whitelist allows the application. If it is not approved, the execution is denied.

3. Does WDAC restrict users/processes with respect to reading and writing files ? How ?

No, WDAC does not control read/write operations. Its scope is limited to the “execute” operation. However, it can prevent an application from running entirely, which indirectly prevents it from reading/writing files.

4. What are the different file rules that you can use with WDAC ?

WDAC supports publisher rules (verified via digital signatures), file hash rules (ensuring installed/downloaded content is identical to expected) and path rules (based on location in the file system).

5. What is the purpose of the audit mode in WDAC ?

WDAC Audit Mode is a mode where the policy is enforced only for logging. It does not block any application from running but it records events about what would have been blocked if the policy were enforced. It is like a “test playground” where to test rules and policies before applying them.

6. How do you debug WDAC policies, i.e., how do you find out that they are effective and where are WDAC events logged ?

Debugging WDAC policies relies on the Audit Mode to check effectiveness and identify missing policy rules. The WDAC events are systematically logged into the **Application and Services Logs\Microsoft\Windows\CodeIntegrity\Operational** event log.