Computer Security (COM-301)

Adversarial thinking and threat modelling

Live exercise solving

STRIDE analysis

After the release of the COVID-19 vaccine, life is back to normal. The EPFL bar, Satellite, is re-opening. In order to celebrate this event, Satellite decides to have a special offer where if a student buys a beer, they get an additional free beer. If a professor buys a beer, they also get a free beer. There is an extra condition that this offer is only valid up to a purchase of three beers for professors. Students do not have a limit on this offer; they can purchase as many beers as they want and they get a free beer for every purchase.

When a customer orders a beer at the bar, the bartender first checks their CAMIPRO for their status (student/professor). The bartender updates a logbook with the customer's ID, status, and the number of beers that they have purchased. If they are eligible for free beer, they provide the free beer along with the purchase.

Perform a STRIDE analysis of this scenario. Write **three** possible threats (three letters of STRIDE). For each threat, describe what can go wrong and suggest a possible countermeasure to it.

Backdooring encryption

EU encryption ban follows the terrorist attack

In the EU Council of Ministers, a resolution was made ready within five days, obliging platform operators such as WhatsApp, Signal and Co to create master keys for monitoring E2E-encrypted chats and messages.

From **Erich Moechel**

The terrorist attack in Vienna is used in the EU Council of Ministers to enforce a ban on secure encryption for services such as WhatsApp, Signal and many others in the fast-boiling process. This emerges from an internal document dated November 6th from the German Presidency to the delegations of the member states in the Council, which ORF.at has received.

ANNEX

Draft Council Declaration on Encryption

Security through encryption and security despite encryption

1. Preamble: Security through encryption and security despite encryption

The European Union fully supports the development, implementation and use of strong encryption. Encryption is a necessary means of protecting fundamental rights and the digital security of governments, industry and society. At the same time, the European Union needs to preserve the ability of law enforcement and judicial authorities to exercise their lawful powers, both online and offline.

According to the European Council conclusions, 1-2 October 2020, EUCO 13/20 *the EU will leverage its tools and regulatory powers to help shape global rules and standards.* It was agreed to use funds under the Recovery and Resilience Facility to advance objectives such as *enhancing the EU's ability to protect itself against cyber threats, to provide for a secure communication environment, especially through quantum encryption, and to ensure access to data for judicial and law enforcement purposes.*

Would this be secure?

How can this system be exploited by an adversary?