EPFL

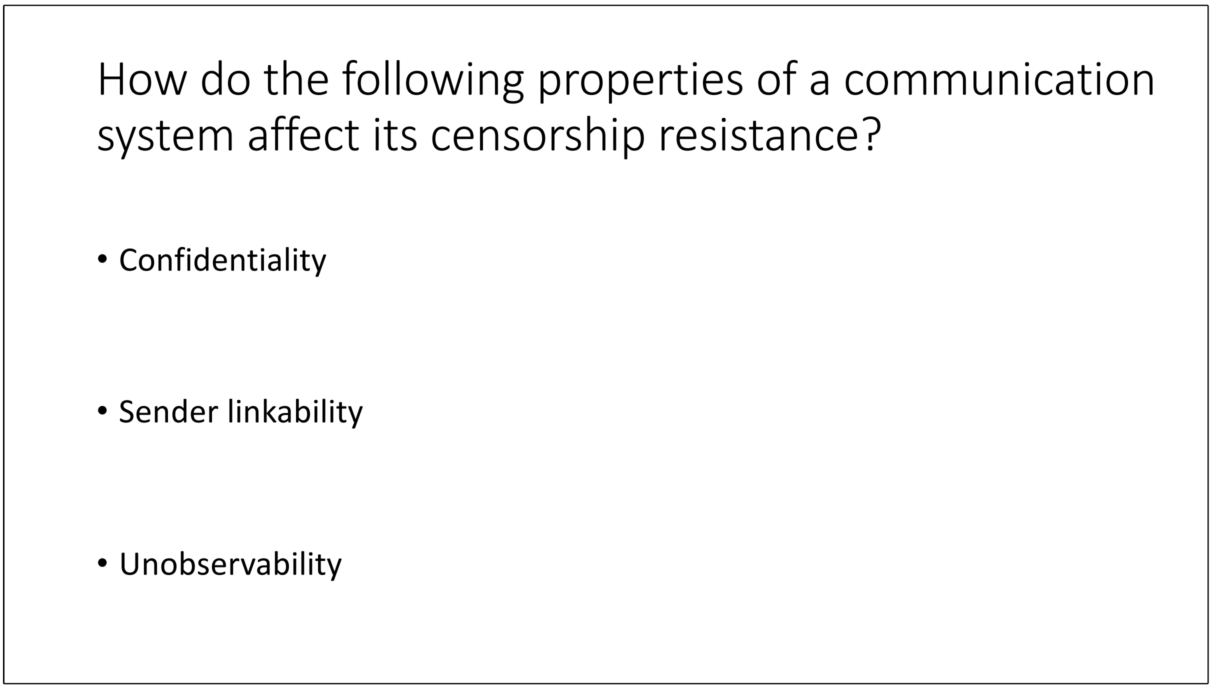
SPRING

SECURITY AND PRIVACY ENGINEERING LABORATORY

CS-523 Advanced topics on Privacy Enhancing Technologies

Censorship resistance
Live exercises

Theresa Stadler
SPRING Lab
theresa.stadler@epfl.ch



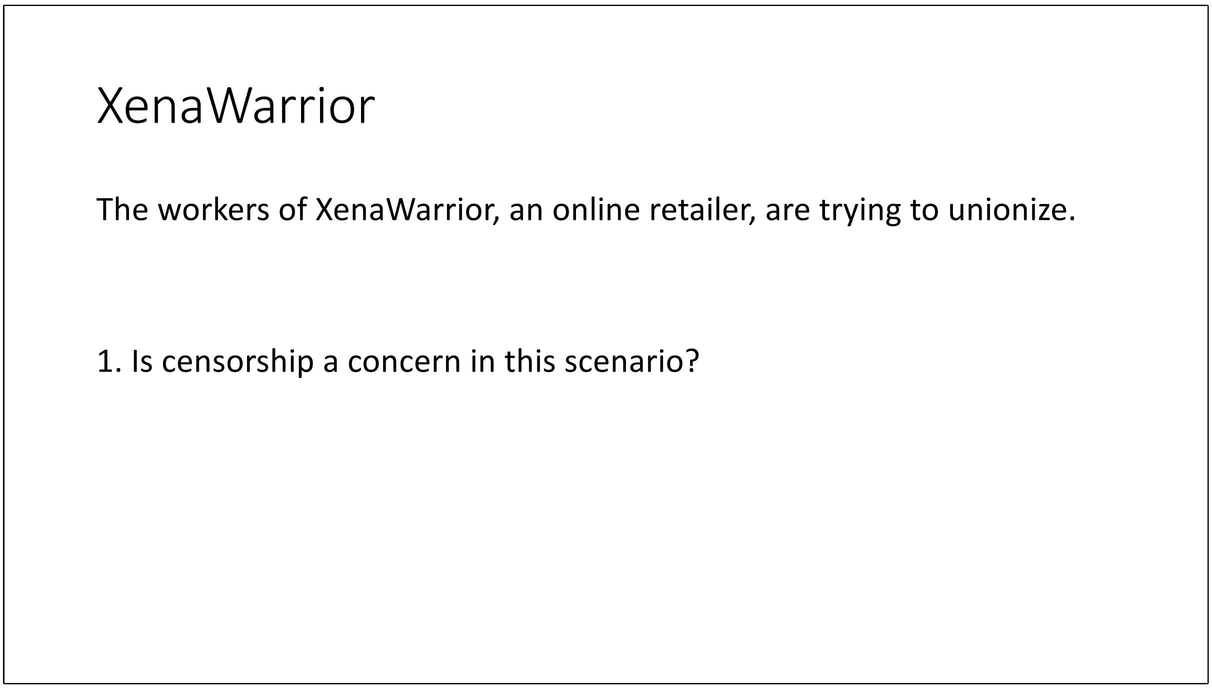
How do the following properties of a communication system affect its censorship resistance?

- Confidentiality
- Sender linkability
- Unobservability

Confidentiality of the content of communication such as messages or even search terms prevents content-based censorship, i.e., increase censorship resistance

Sender linkability: Revealing information related to the sender and more generally any metadata enables flow-based censorship.

Unobservability helps against censorship by making it harder for the censor to know whether there is even a flow that they should consider for censoring.

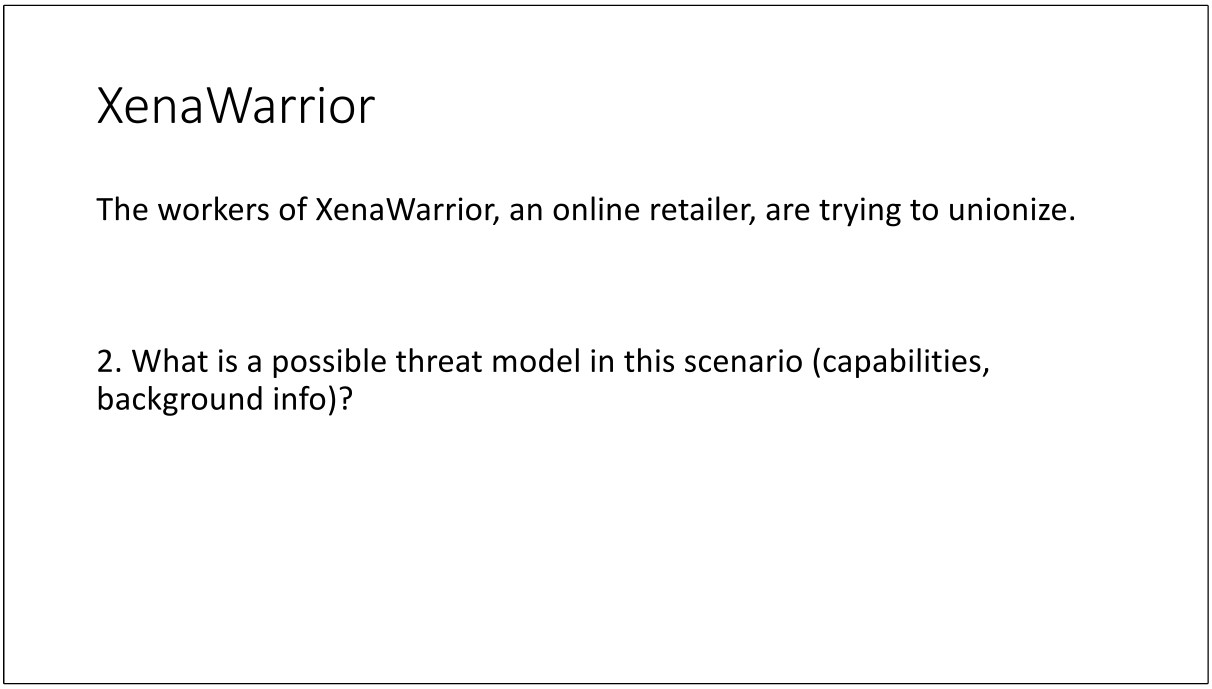


XenaWarrior

The workers of XenaWarrior, an online retailer, are trying to unionize.

1. Is censorship a concern in this scenario?

Yes, censorship is a concern. Xena Warrior is an online retailer, they cannot prevent all exchange of packets, but, for example if Xena Warrior wanted to forbid / slow down discussions among unionizers or restrict their access to information about their rights by using censorship techniques, that would be bad



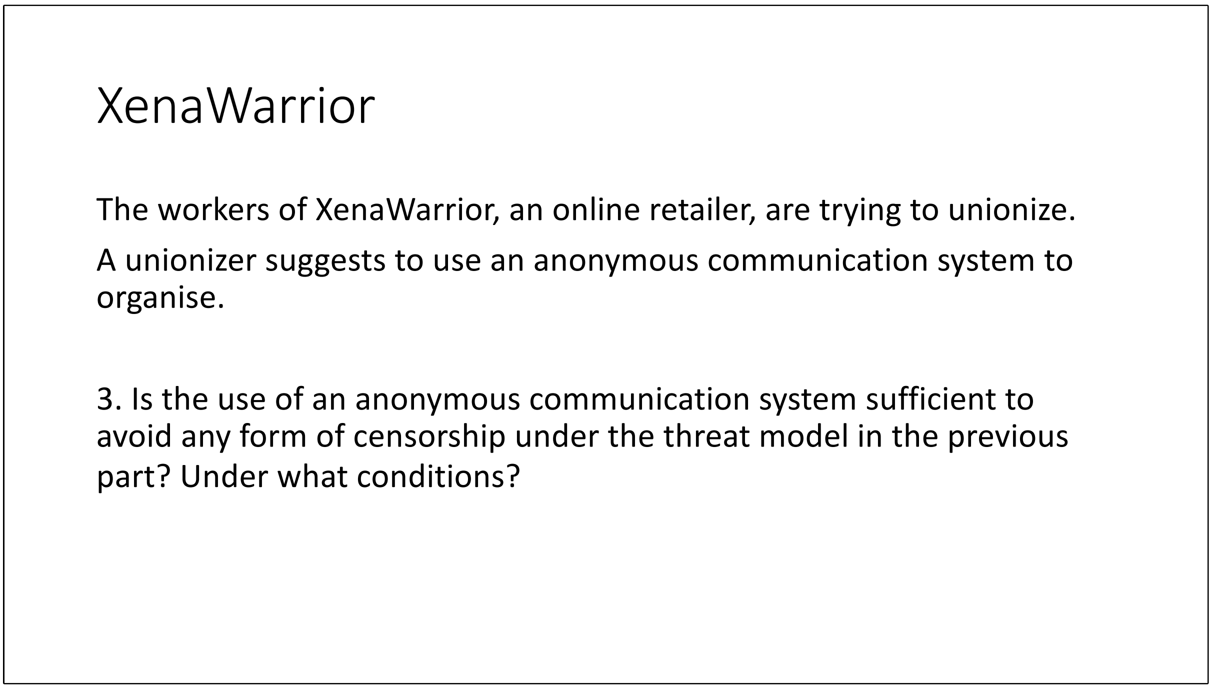
XenaWarrior

The workers of XenaWarrior, an online retailer, are trying to unionize.

2. What is a possible threat model in this scenario (capabilities, background info)?

Examples of adversaries:

NSA = global passive adversary, could know the jobs of workers
Xena Warrior = local and active, could know the jobs but also the schedules of workers, their relationships, etc



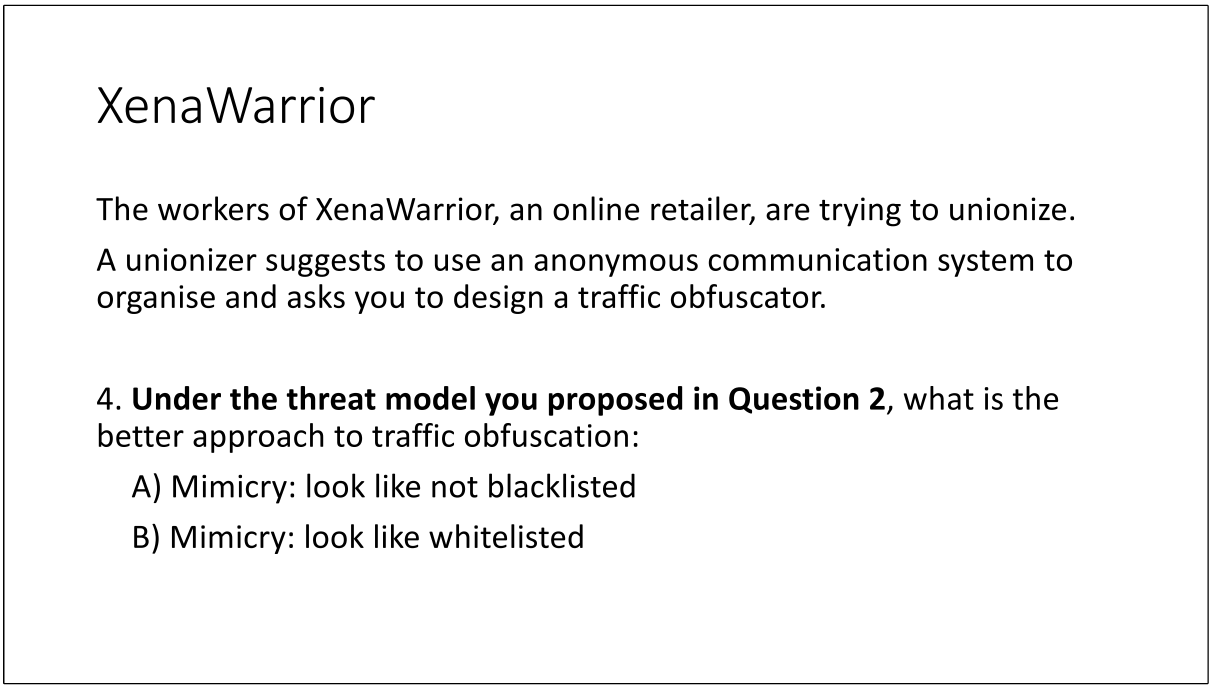
XenaWarrior

The workers of XenaWarrior, an online retailer, are trying to unionize.

A unionizer suggests to use an anonymous communication system to organise.

3. Is the use of an anonymous communication system sufficient to avoid any form of censorship under the threat model in the previous part? Under what conditions?

Anonymous communication by itself does not (necessarily) protect against censorship. The anonymous communication protocol is typically recognizable and/or different from retail exchange and can thus be censored. For example with Tor, the Tor nodes have public IP address and the handshake and certificates are special.



XenaWarrior

The workers of XenaWarrior, an online retailer, are trying to unionize.

A unionizer suggests to use an anonymous communication system to organise and asks you to design a traffic obfuscator.

4. **Under the threat model you proposed in Question 2**, what is the better approach to traffic obfuscation:

A) Mimicry: look like not blacklisted

B) Mimicry: look like whitelisted

(Both answers could be valid provided a good justification)

For NSA: look like not blacklisted could work, though it may become recognizable if it does not look for anything else

For Xena: look like whitelisted may be more effective, especially if you look like a whitelisted tool that Xena uses on their daily business and therefore they will not want to block.