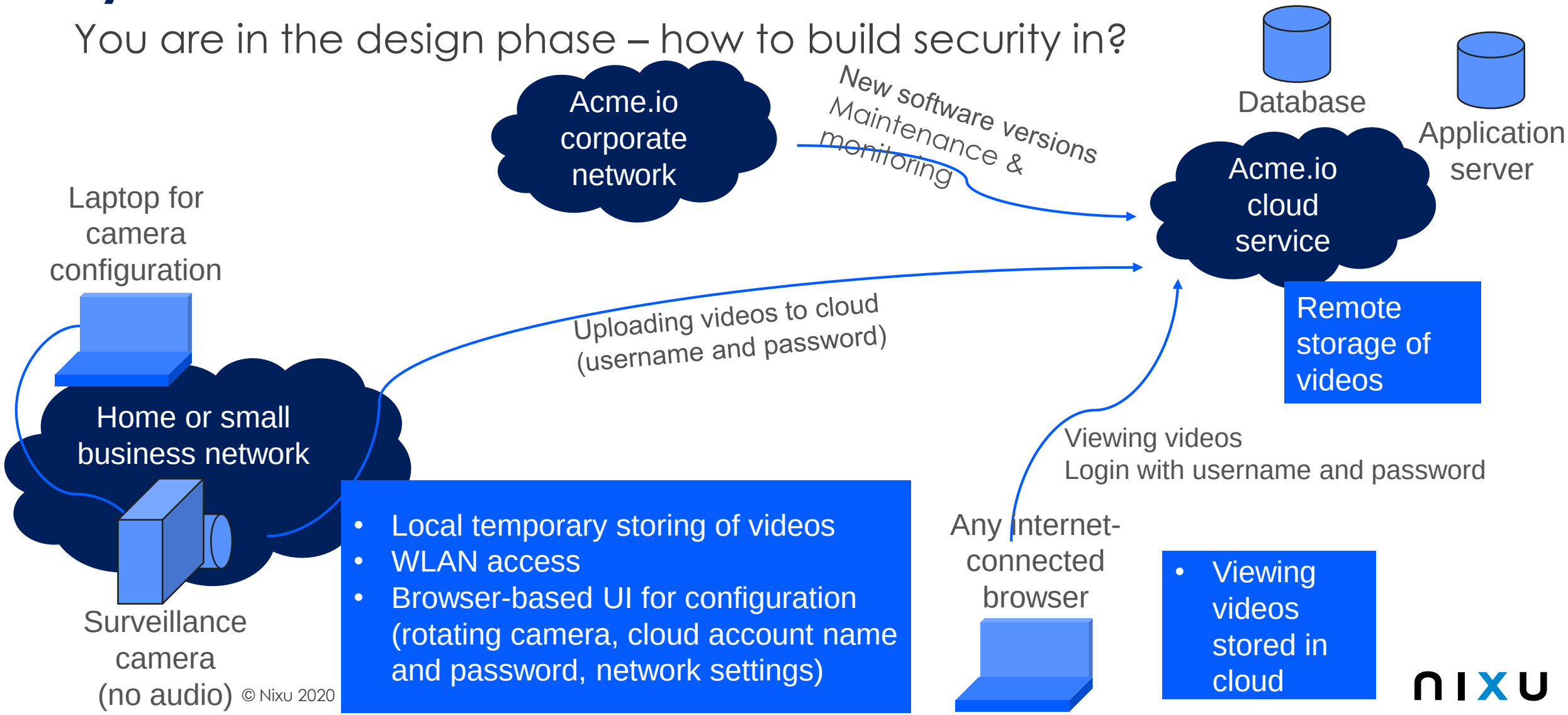
nixu
cybersecurity.

Imaginary IoT Camera System

Threat modeling example target

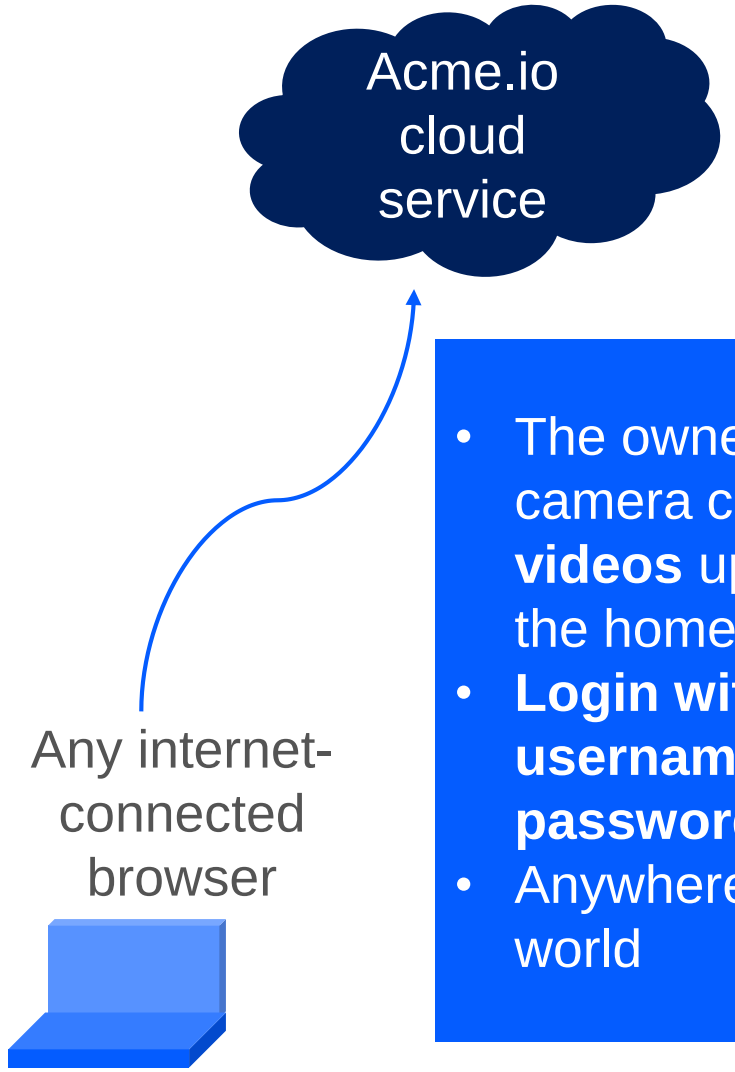
An imaginary home surveillance IoT camera system

You are in the design phase – how to build security in?



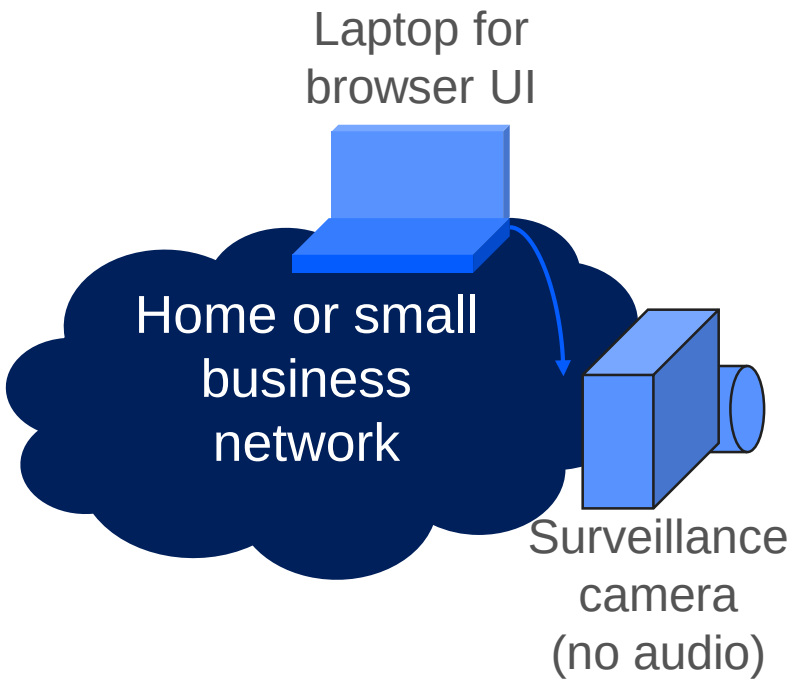
What threats can you find from the video cloud access?

- Camera owners can **view the videos** recorded by their home surveillance camera also **while travelling or when at work**
- Using a **browser**, they simply login to their Acme.io cloud account
- Authentication with **username and password**



What threats can you find from the camera features?

- Camera is connected to the home network with WLAN or Ethernet cable
- Camera has a **web-based configuration interface**
  - Network settings
  - Camera UI username and password
  - Rotating the camera
  - Video storage options (cloud account username and password, how many days the videos are kept before removal)
  - Updating firmware
- **Recorded videos are stored temporarily on the device** until storage limit is reached
  - **Videos are uploaded to cloud** when there's internet connectivity



- Local temporary storing of videos
- WLAN access
- Browser-based UI for configuration (rotating camera, cloud account name and password, network settings)

What threats can you find from development and operations?

- Drew **is a new developer** and is not familiar with all procedures yet
- Olive has been in the operations for ages and **does not like the job**
- SSH remote access to the servers