Security issues and Open Source.

Experiences from using Linux and other open source in embedded networked devices

Fredrik Hugosson, PdM Core Video Platform,
Axis Communications AB

Axis, The market leader in network video

75.000 partnerships in **179** countries

1984 Founded as IT company

2061 Employees*

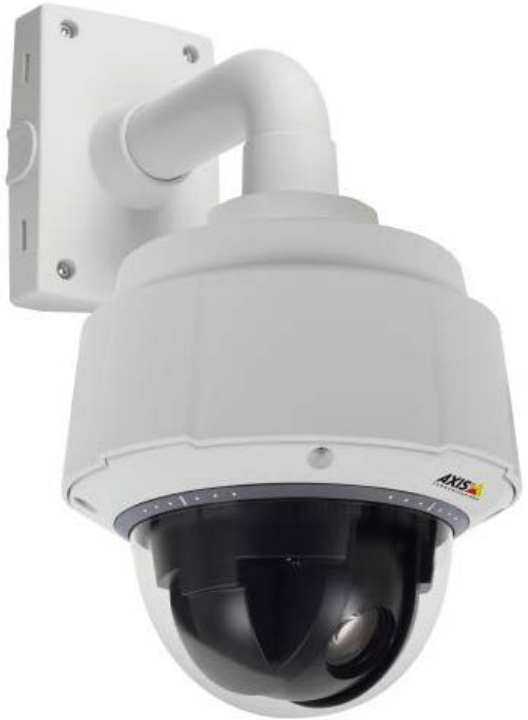
Own offices in **49** countries

Total sales: SEK **5,5 billion**

2014 except *Jun, 30 2015

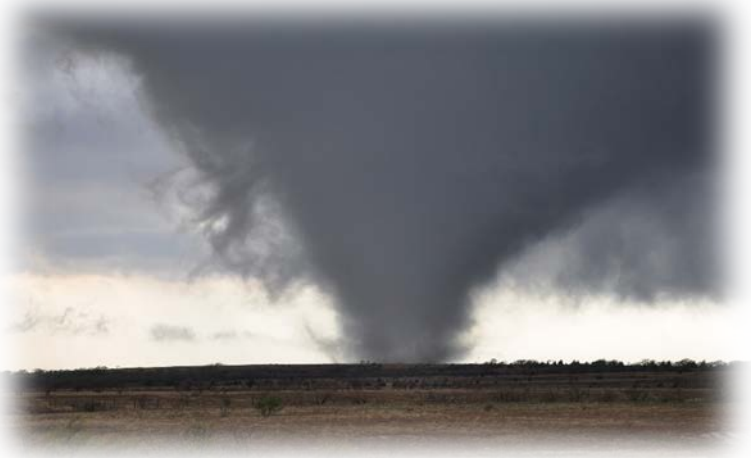
Axis long history with open source and network connectivity

- 1985 IBM mainframe print protocol converter
- 1989 Network print server for PCs
  - Using BSD TCP/IP stack, our own RTOS
- 1993 GCC ported to the CRIS architecture
  - Fully upstreamed 2001, binutils 2000
- 1996 Worlds 1st TCP/IP network camera
  - Based on print server code, many more pre-IoT devices
- 1999 Network Camera running Linux
  - Worlds 1st commercial embedded device with Linux
- 2008 First camera with GStreamer
- 2013 Entering IoT again
  - Door Controller, Horn Speaker
- 2015 Using Yocto/Poky/OpenEmbedded



Typical threats in IoT environments

- Threatscape
  - Worms
  - Malware
  - Default configurations
- Goals
  - Hinder normal operation, DoS
  - Bot-nets
    - Spam
    - Bitcoin mining
    - DDoS
  - Steal information
  - Launchpad for other attacks
    - Infect other devices
    - Disabling or destroying HW

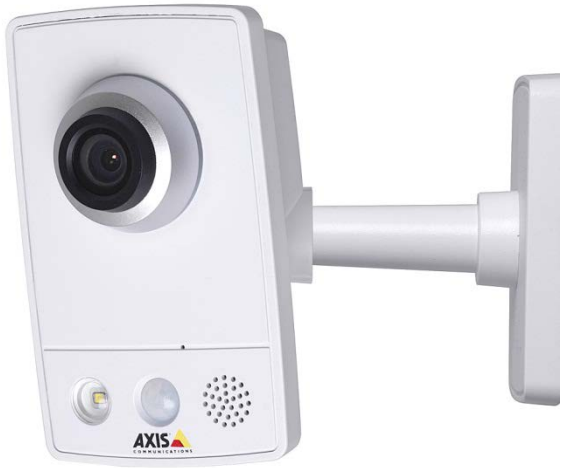


Open source and security

- Open means open! For everyone.
  - Code & Vulnerabilities & Patches
  - Widespread, BIG impact
- Possible problems are often reported “secretly”
  - A CVE is released when patches are ready/deployed, when information about the problem is leaked or directly if exploits are seen in the wild
- Exploits may appear in days or even hours after a CVE is released
- Focus on defense!
  - Fast updates with security patches

Good security practices for Linux

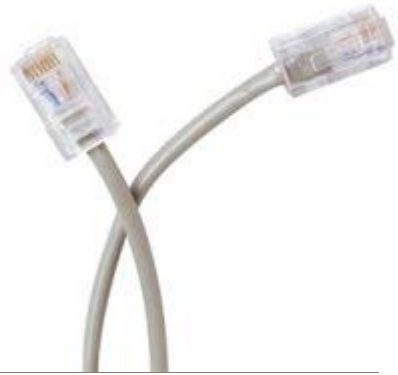
- Protect
  - Harden your system, use SELinux or SMACK
  - Sandbox unknown (or all) applications
  - Make your system secure by default
  - Take *extra* care of the parts handling updates of the system
- Limit possible damage
  - Run everything with as low privileges as possible. Keep the attack surface minimal
  - Use features such as No-Execute
  - Do not allow root user, no su, no sudo, nothing
  - Use multiple layers
    - Web/CGI-layer, service layer, system layer, kernel
    - Gives you more time to deploy a solution, lower probability of multiple interacting vulnerabilities
- Detect
  - Add an IDS (Intrusion Detection System)



Expected future needs

- > Manual tracking of CVEs
- > Same flow as service packs
- > Manual deployment
- > Not part of service agreements
- > Update disrupts normal service

- > Automation or service
- > Faster security patch flow
- > Automated deployment
- > Required by customers/operators
- > No disruption of service



Opportunities for us, you, anyone

- Supporting Poky/Yocto-based distributions with automated CVE announcements
- Technology for continuous updates of firmware
- Technology for disruption-free updates of devices
- Security-as-a-service, supplier of updates to IoT devices, selling to:
  - Manufacturers
  - Operators
  - End-users
- Collaborate!


Megapixel
Quality
Ease of use
Network video
Reliability
open
Innovation
Easy installation
Protect
support
integration
Secure
Thank you
Service all the way
Image usability
Thermal
Convergence
HDTV
Access control
World Leader
Competence
Intelligent
Quality
Partners
Focus
Cameras
Safe
Outdoor
Video encoder
Global