Motivation

Internet use: required

In the past, children's internet use was optional, e.g. games and entertainment

Children's internet use is increasingly required, e.g. homework, communicating with family members

Children must use internet unsupervised

Unsupervised Use is Risky

Children encounter content that

- They cannot handle
- Exploits them

And parents cannot be present to intervene or instruct.

Previous work

Focus: identify “bad” content and deny it
Means:

- List bad sites
- Automatically classify content
- Humans classify content

This is beyond the means of most families.

Commercial Services

Classify content (often with some human aid)

- e.g. OpenDNS

Overwhelmed with today's large volumes of content

Black Hats continually invent new means to circumvent

“Outsourcing” classification prevents family-specific policies

- Phobias
- Parental instruction needed

Assumption that classification errors are acceptable because children's internet use is

Commercial Services

Common justifications for misclassification

False positives: acceptable because children's internet use is optional.

False negatives: acceptable because children should always be supervised

Frustration feeds denial... or paranoia

- “Filtering content would be unethical”
- “I've raised my children to be able to handle everything”
- “It is a risk we have to run these days.”
- “It won't happen to us.”

Or

“I just don't let my children use a computer at all unless I'm standing over their shoulder.”

“The Internet is just full of bad things. We don't even have a computer.”

An opposite approach

Parents define the sites children may visit without supervision

Other internet activity must wait for parental intervention.

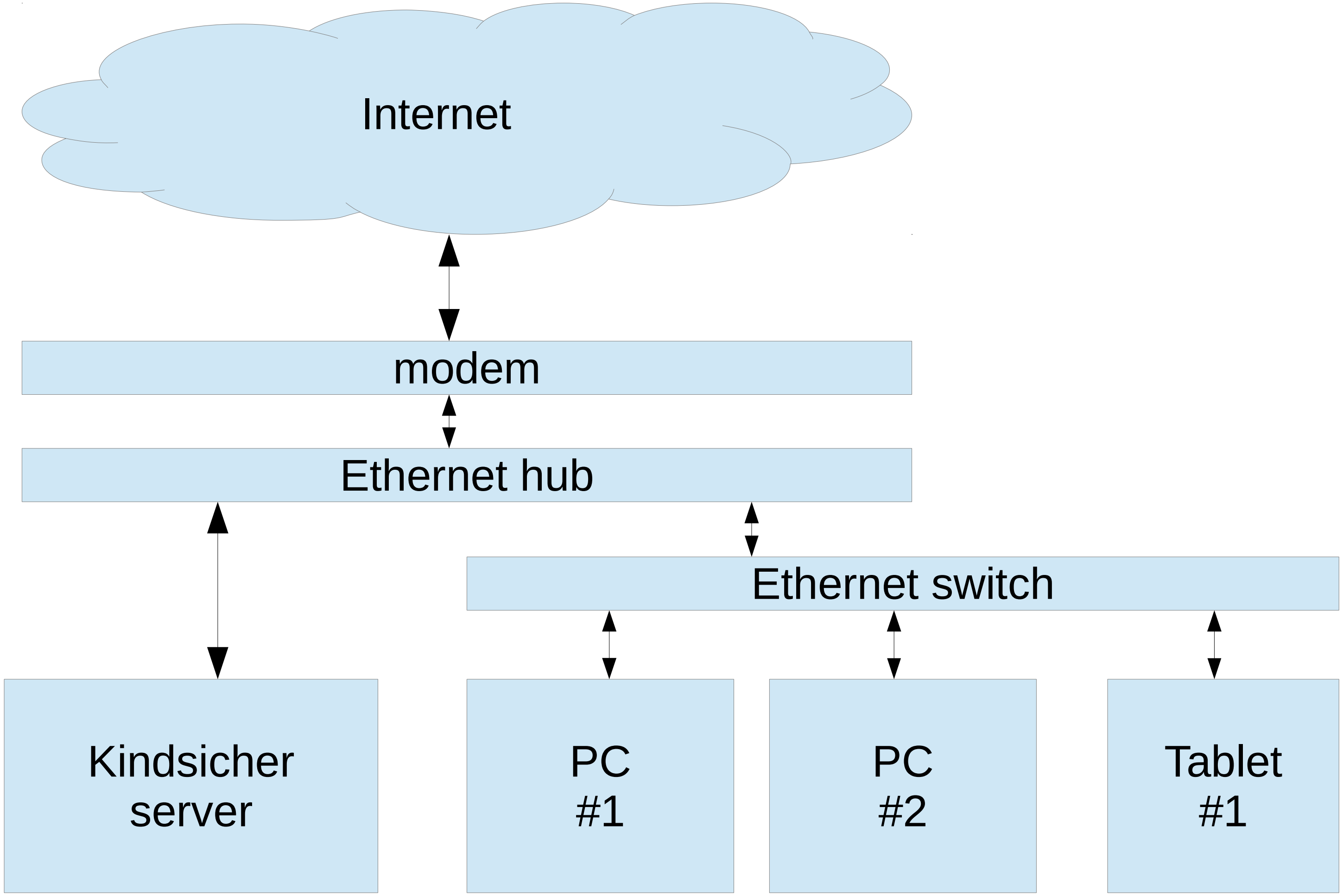
Example

Parents might decide their children may do these things on their own:

- Visit the school website (for homework)
- Visit Grandpa's blog in India
- Visit a few trusted game sites
- Visit Weather Underground
- Visit sites related to our faith
- Visit city Park and Recreation's website
- Visit National Geographic's website

Go get a parent to do other things.

Implementation



Threat Model

External:

- “Black Hat” site tries to mix its content with legitimate content
  - No advantage unless they mix it with an explicitly permitted site
- Weblink uses internet address, not domain name (e.g. http://155.98.65.24)
  - No advantage unless parents approved the address

Threat Model

Internal:

- Child enters an internet address into web browser (e.g. http://155.97.137.55)
  - No advantage unless parents approved the address
- Teenager rearranges network wiring
  - May require parents putting Kindsicher server, ethernet hub and modem in a locked cabinet
- Friend brings laptop or tablet to home
  - No advantage, Kindsicher is implemented as part of network infrastructure, no “client” component needed

title