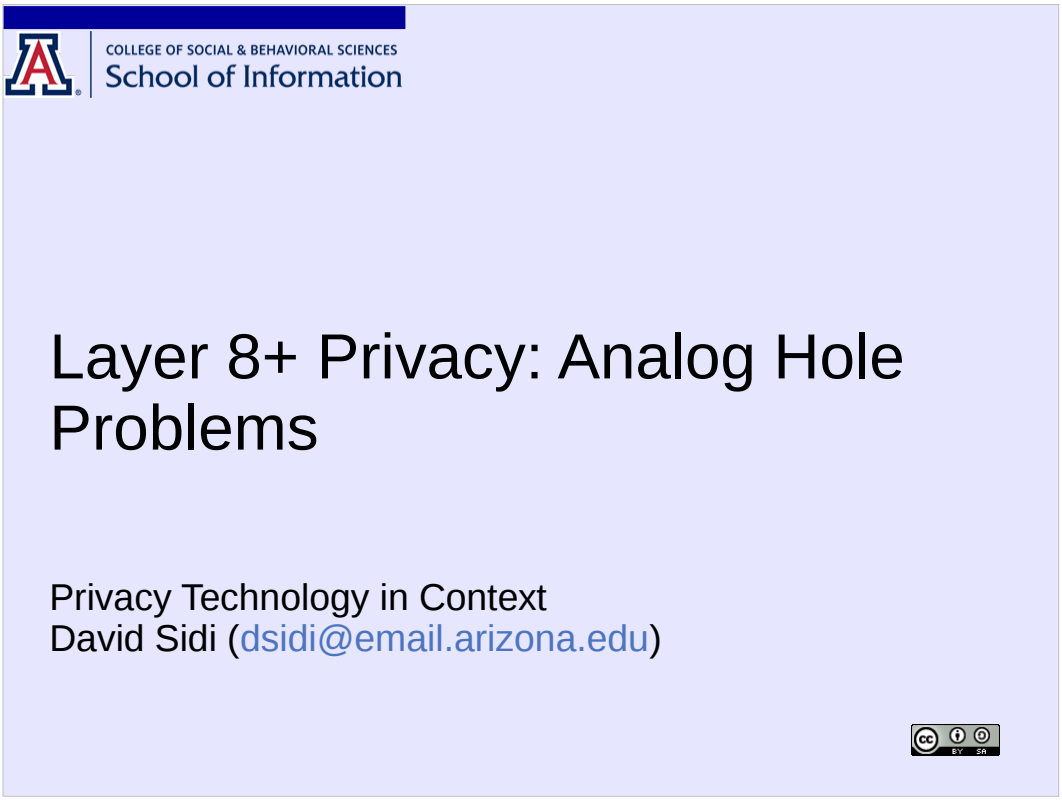
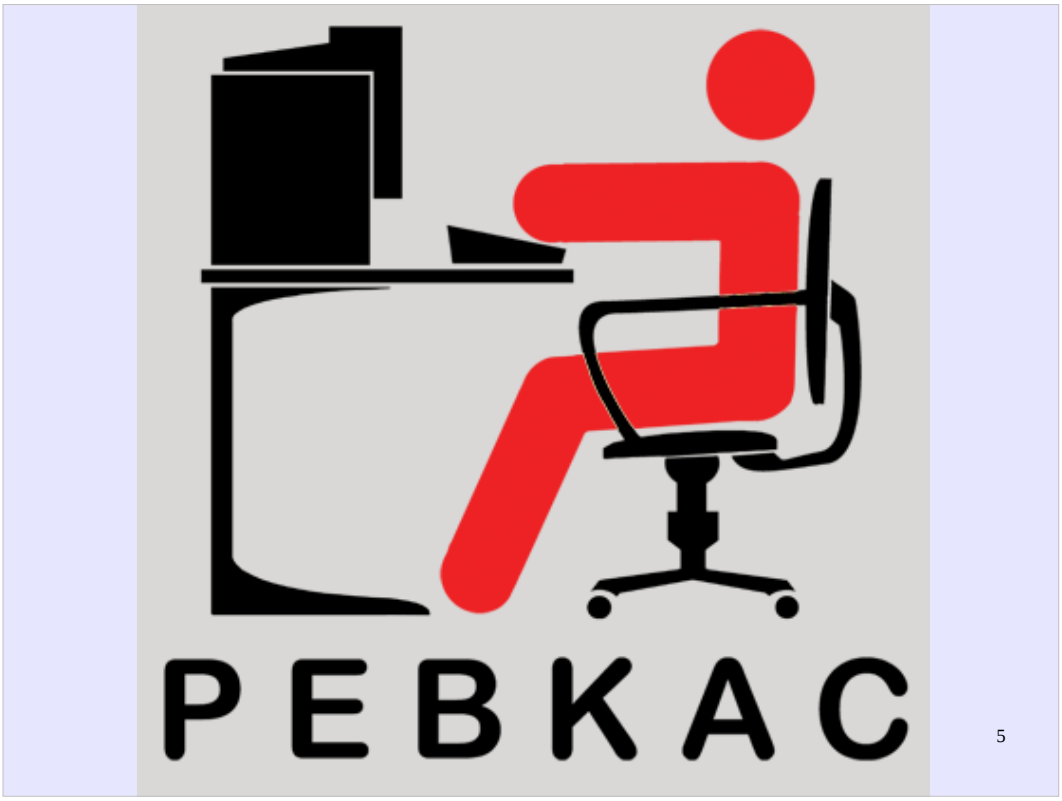


Today we start discussion of a class of problems centered on passive, physical access to communications.

Small mention of interesting things

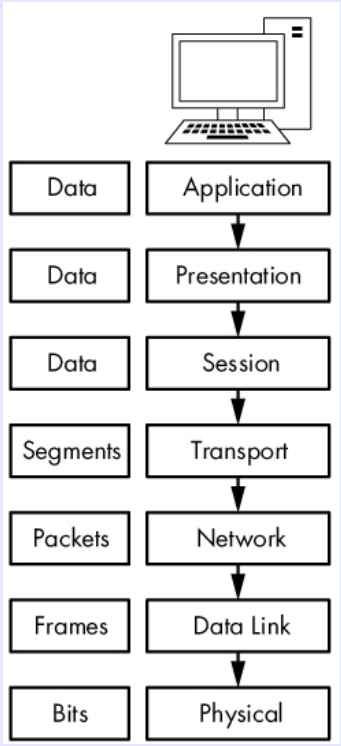
- Schedule:
  - Dont forget: server assignment by tonight; write-up by tomorrow night
  - programming assignment on the 22nd, final server assignment on the 27th, and a write up for the 29th
- You'll need the VM for the next assignment, so set it up
  - (sidenote: In the VM, caps lock and escape are switched)



- PEBCAK: Problem exists between computer and chair
- “A colleague once told me about a user who complained that he could not access a network resource. The issue was the result of the user’s entering an incorrect password. My colleague referred to this as a layer 8 issue. Layer 8 is the unofficial user layer. This term is commonly used among those who live at the packet level.” Practical Packet Analysis
- *Chortle.* Anyway, ‘funny’ and ‘serious’ are not contrary; you can have both

8+?

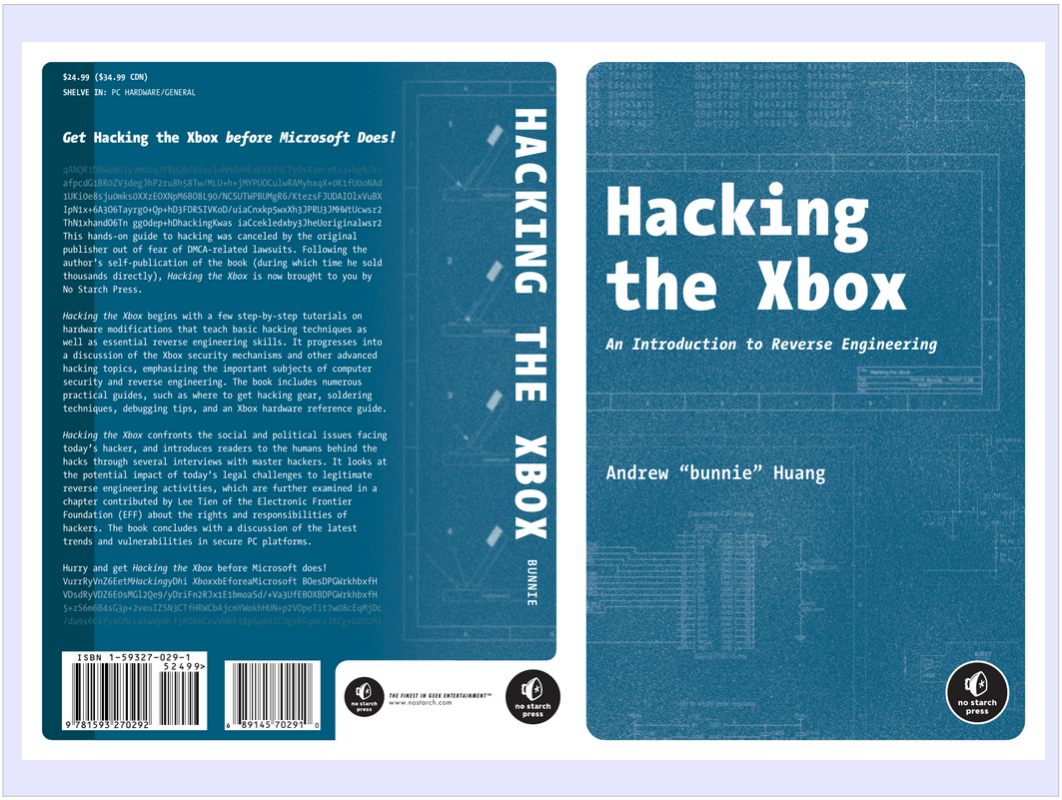
The ~~Seven~~-Layer OSI Model



- *Users sit on top of the OSI model*
- *Users* communicate using networking technology---not just computers
- There is a layer eight
- Moreover, there are higher level organizations that communicate through us: there are layers above eight
-
- There are a class of privacy problems that I think we can identify in the extended reference model, to do with information available at *displaytime*

A problem for paid content delivered on computers: easy bulk copying

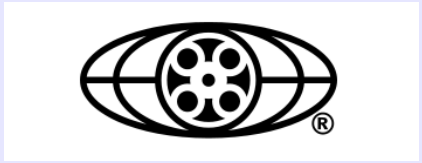
- getting a copy onto a computer of information available at display time is generally easy, using recording devices (this image is from the days of VHS recording)
- once in that form on a computer, copying in bulk is easy
  - a single person can distribute a work to zillions of others without much effort
  - So far, this is not quite a privacy worry, though you may see a connection already



- broadly, DRM tries to control copying and what else can be done with digital media in the hands of an adversary
- There are non-cryptographic and cryptographic variants, as well as prevention- and mitigation-focused approaches
- Record companies et al. have in mind pirates as adversaries here, while
- Advocacy groups have in mind legitimate users for whom DRM is malware
- (quote from bunnie)

DRM has collateral damage

- DRM cannot tell what your intentions are if you want unencumbered access to the data it tries to protect, so everyone is prevented that access
  - successfully circumventing DRM is illegal, whatever your purposes, according to the DMCA's section 1201



Section 1201 of the DMCA makes it illegal to bypass DRM or give others the means of doing so. 1201 gives technology manufacturers the power to cast clouds of legal uncertainty over common uses of their products. It gives content owners and other powerful entities an unfair weapon against innovation by others. It's a law that needs fixing.

- there are several Controversial examples of DRM
- John Deere tractors cannot be repaired without software access codes
  - some farmers have turned to Ukranian firmware instead
- The W3C approved Encrypted Media Extensions (EME) as a web standard
  - Lobbied by Google, Microsoft, Netflix, Apple, CTA, MPAA (which includes Disney, Fox, NBCUniversal, Paramount, Sony Pictures and Warner Bro studios)
  - EFF resigned in response

Excerpt from EFF resignation letter from W3C

...Today, the W3C bequeaths a legally unauditable attack-surface to browsers used by billions of people. They give media companies the power to sue or intimidate away those who might re-purpose video for people with disabilities. They side against the archivists who are scrambling to preserve the public record of our era. The W3C process has been abused by companies that made their fortunes by upsetting the established order, and now, thanks to EME, they'll be able to ensure no one ever subjects them to the same innovative pressures.
...
Effective today, EFF is resigning from the W3C.

Thank you,

Cory Doctorow
Advisory Committee Representative to the W3C for the Electronic Frontier Foundation

Counterpoint: Advantages of EME

Conforming EME implementations will protect users and provide a model for privacy and security which is superior to native platform alternatives. However, in the current software architecture, in particular the closed CDM implementations, this specification cannot technically enforce a complete protection for users. Nevertheless, the specification sets clear expectation for those protections.

...As mentioned earlier, plugins have historically been used for features that were not available in the Open Web Platform, e.g. Graphic APIs, camera/phone access, audio/video, protected video content, or faster animations. This meant that DRM-related code was loaded for every page that used Adobe Flash or Microsoft Silverlight, even when there was no encrypted video or even any video at all.

...By developing EME as an extension, W3C is reducing the number of pages that load access to decryption technology. EME has the benefit that all interactions happen within the Web browser and moves the responsibility for interaction from the plugins or third-party applications to the browser. The EME API mitigates the interactions with DRM within the browser itself, limits the access from third-party DRM systems, reducing their exposure for security vulnerabilities or leakage of sensitive user data.

EME improves accessibility of encrypted online video, in contrast to many existing mechanisms, by operating at a level that does not interfere with transmission or control of accessibility information.

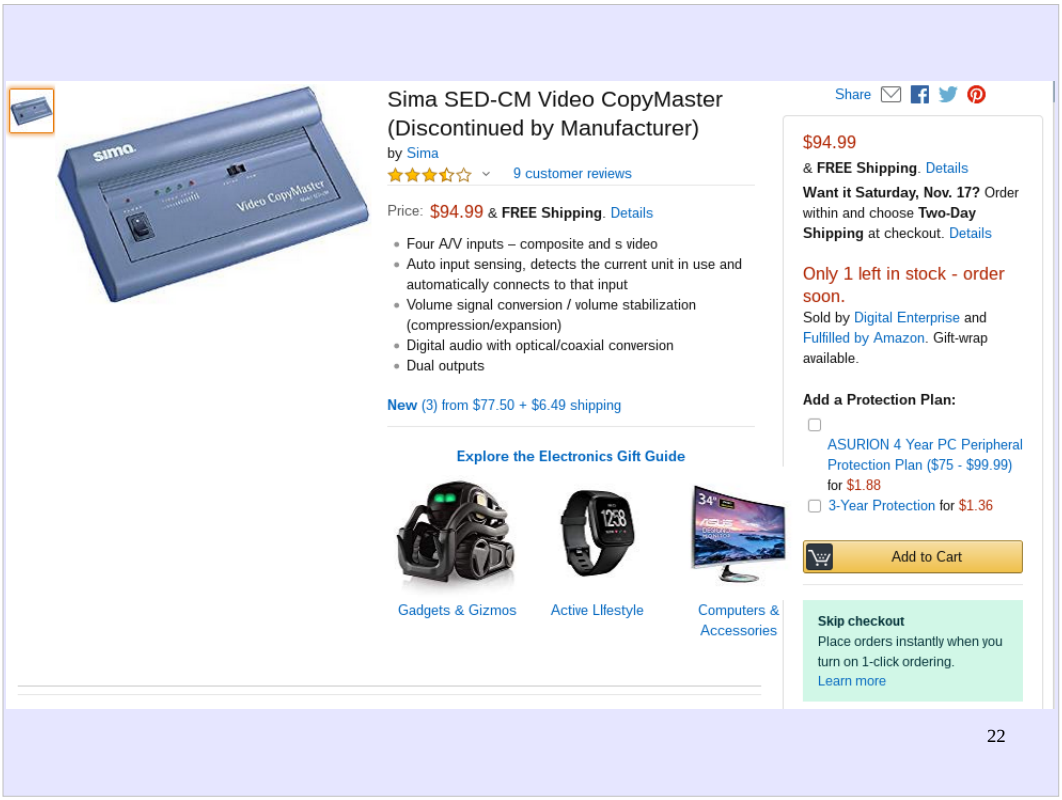
Applications conforming to EME ensure that accessibility information will either be transmitted in the clear; or, if encrypted, then decrypted along with the primary video file. Additionally, for the specific issues raised in the formal objections, many video functionalities necessary for accessibility are provided in the Open Web Platform. For instance, access to the video controls, time-scale modification, discovery and activation/deactivation of alternative content, use of secondary screen are all functionalities provided by the HTML specification or some of its extensions. These and future accessibility enhancements of the Open Web Platform can be leveraged.

...

Together with MSE, EME is just one piece of W3C's larger vision for media tuning which includes HTML5 as well as TTML (for which W3C won an Emmy Award in 2016) as well as other specifications. The Open Web Platform, of which HTML5 is a cornerstone, also includes CSS, DOM, SVG and Web APIs.

All these specifications are open, royalty-free technologies which enable developers to build rich interactive experiences, powered by vast data stores, that are available on any device.

https://www.w3.org/2017/07/EME-backgrounder.html



- Sima makes products for converting analog signals to digital for recording purposes
- The Macrovision DRM, which involves signals invisibly embedded in the analog output, is not preserved in the copies
- Macrovision says this circumvents their copyright protection, violating the DMCA
- Users say it helps them to make legitimate backups, and tinker to create new technologies (see “Hacking the Xbox,” again)
- Case resulted in a settlement

How is DRM like malware? How is it different? (2 min)

The analog hole problem

“The music industry frets about what is known as the analog hole, which arises from the simple fact that digital music must be converted to an analog signal at some point if it is to be enjoyed. It is very difficult, if not impossible, to prevent people from capturing these analog signals, re-digitizing them, and distributing them on the Internet, stripped of DRM.”

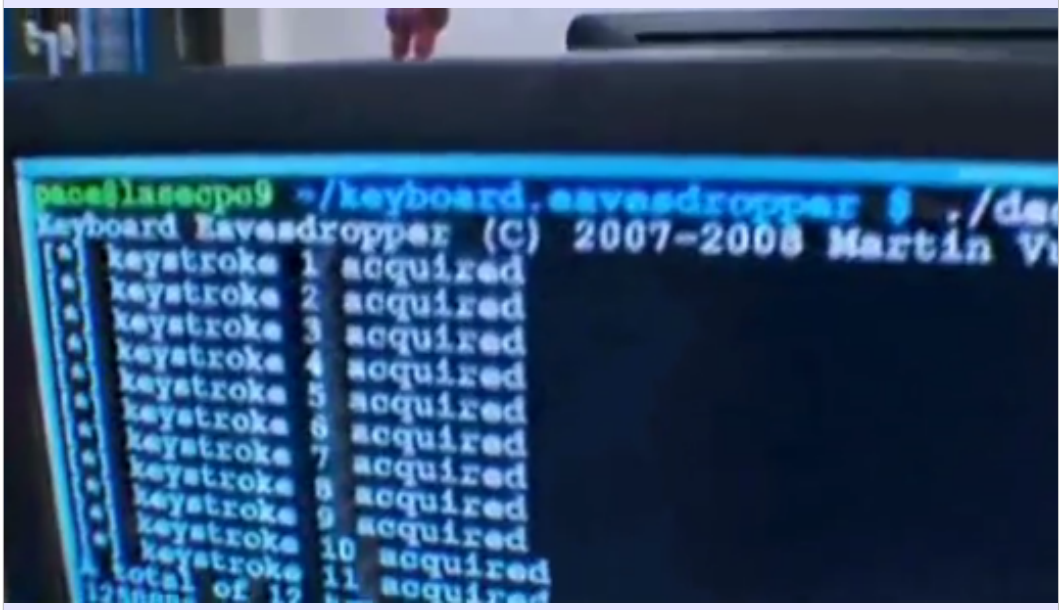
Sicker et al., “The analog hole and the cost of music’

‘Analog hole’ is a misnomer

- Recording with pixel scraping with Audials (link)
- Recording from buffers
  - Data-processing operations, and specifically decryption operations, are carried out on buffers of data
  - Everybody uses known media codecs (coming up with new codecs is hard, and there are patents)
  - You can tell the difference between encrypted and decrypted content based on their entropy
  - See Wang et al., ‘Steal this movie: Automatically bypassing DRM Protection in Streaming Media Services’

Wang et al. II: Electric Boogaloo

- The analog hole is a general security and privacy hole!
- “To showcase our optimizations, we have also evaluated our approach against GPG, an open-source cryptographic suite”



- Examples of the security implications
- van Eck phreaking
  - demonstration of keyboard eavesdropping (https://www.youtube.com/watch?v=AFWgIAgMtiA)
  - Noise Floor demo. (https://www.youtube.com/watch?v=_g9yUiAHiFo @3:38 - 5:00, 17:35. 23:17-26:35, 29:23 - 36:10)
- TEMPEST
  - testing lab is nearby, at Fort Huachuca

Wang et al. II: Electric Boogaloo

- The analog hole is a general security and privacy hole!
- “To showcase our optimizations, we have also evaluated our approach against GPG, an open-source cryptographic suite”

Wang et al. II: Electric Boogaloo

- The analog hole is a general (old and venerable) security and privacy hole
- “To showcase our optimizations, we have also evaluated our approach against GPG, an open-source cryptographic suite”
- What to do?

Infrastructural approaches

- Personalized Privacy Assistants (link)
  - A registry of IoT devices that respects users requests about how their data will be handled
- A good idea for those willing to participate in the registry (which is probably a lot of device owners, and participation could be made compulsory in some contexts)
- No good if the IoT device owner spurns the registry, or if they try to use it to mislead

Infrastructural approaches

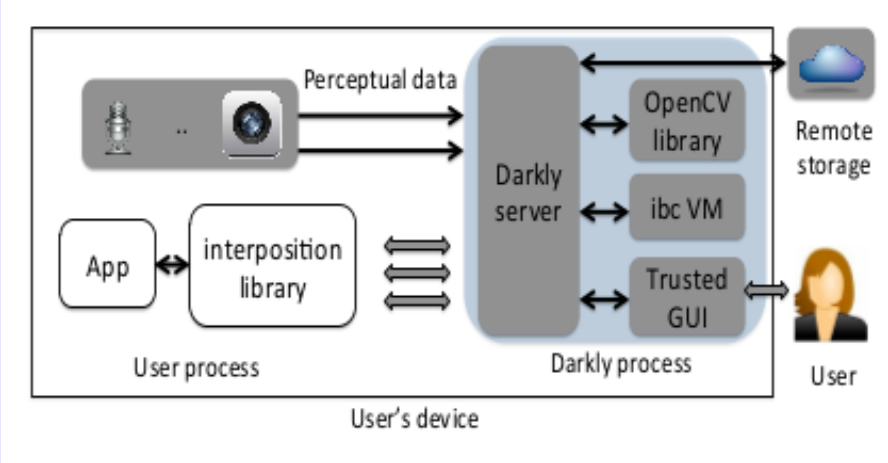
- Similar approaches to DRM exist
- Recording system must read marks embedded in the noise channel
  - macrovision, DCS, CGMS-A, VRAM (VEIL)
  - e.g. (CGMS-A): “a copy protection mechanism for analog television signals. It consists of a waveform inserted into the non-picture Vertical Blanking Interval (VBI) of an analogue video signal. If a compatible recording device (for example, a DVD recorder) detects this waveform, it may block or restrict recording of the video content.” (wikipedia)
- But the DMCA "does not require manufacturers of consumer electronics, telecommunications or computing equipment to design their products affirmatively to respond to any particular technological measure.”

Infrastructural approaches

- Suppose you own devices with perceptual capabilities and want to be sure that the apps that use those capabilities don’t misbehave
- Darkly (@ 31:49 - 43:00)
- Trust includes
  - device operating system
  - the hardware of its perceptual sensors
- Trust does not include a third party application running on your device

Infrastructural approaches

- "the application will never have access to the raw pixels"
  - opaque references

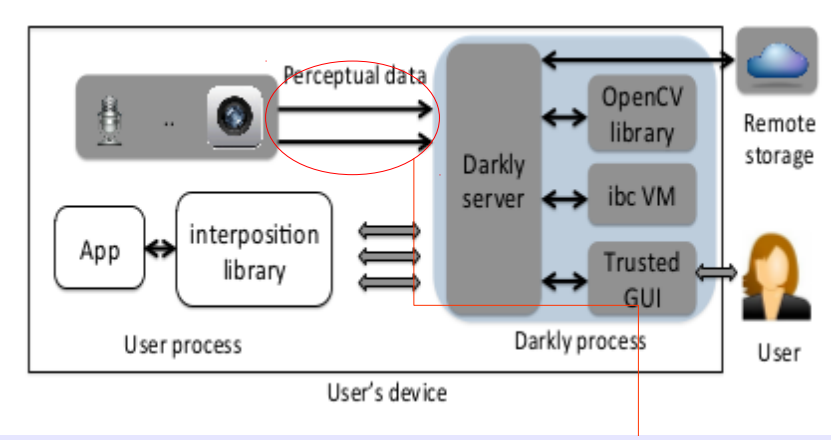


The triple arrows are standard OS user isolation, which we'll clarify in a second
Input to Darkly is trusted: sensors, OS, HW

To block direct access to raw images, DARKLY replaces
pointers to image data with opaque references that cannot
be dereferenced by applications. Applications can still pass
them as arguments into OpenCV functions, which dereference them internally and access the data.

Infrastructural approaches

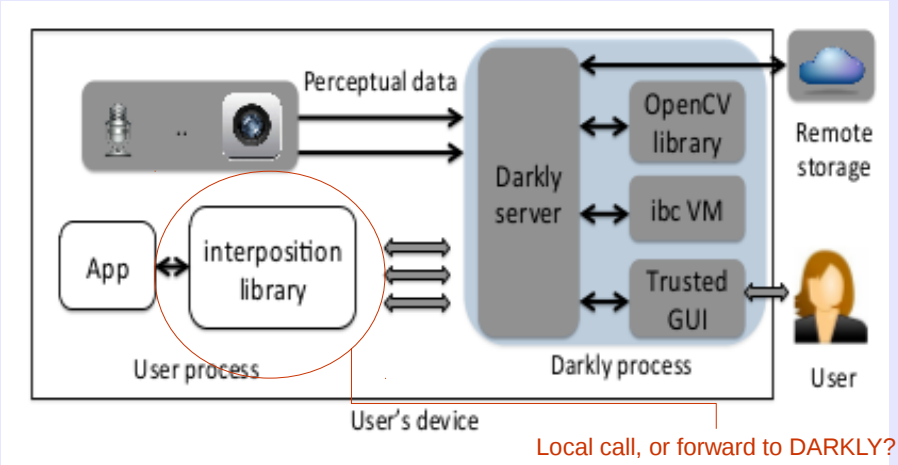
- “the application will never have access to the raw pixels”
  - opaque references



To block direct access to raw images, DARKLY replaces pointers to image data with opaque references that cannot be dereferenced by applications. To distinguish opaque references and real pointers,
D ARKLY exploits the fact that the lower part of the address space is typically reserved for the OS code, and therefore all valid pointers must be greater than a certain value. For example, in standard 32-bit Linux binaries, all valid stack and heap addresses are higher than 0x804800. The values of all opaque references are below this address. It only does this for the pixel data inside the data structures; it leaves metadata alone.

Infrastructural approaches

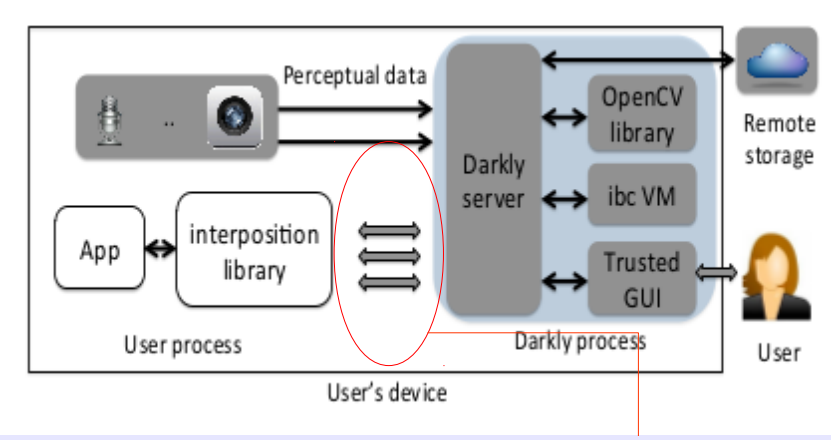
- "the application will never have access to the raw pixels"
  - opaque references



For each call made by an application to an OpenCV function, the interposition library must decide whether to execute it within the application or forward it to the trusted D ARKLY server running as a separate "user" on the same device (only this server has access to camera inputs).

Infrastructural approaches

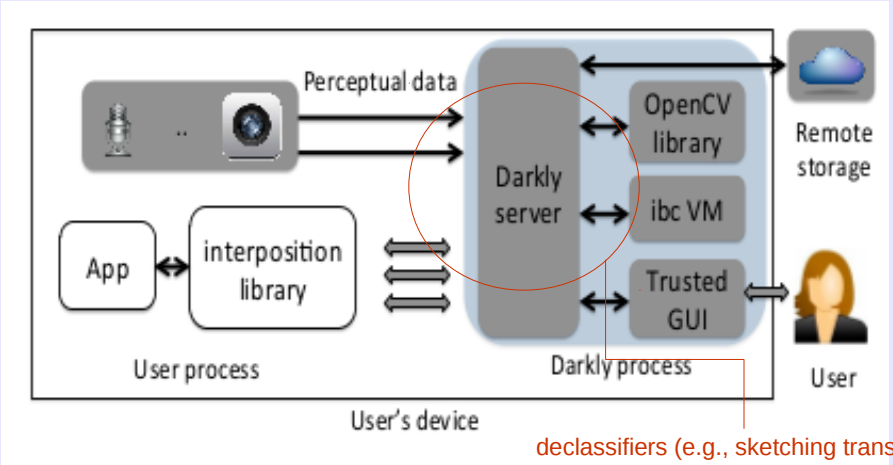
- "the application will never have access to the raw pixels"
  - opaque references



If there is at least one argument with an opaque reference, executing the function requires access to the image. The interposition library marshals the local arguments and opaque references, and forwards the call to D ARKLY for execution. If none of the arguments contain an opaque reference, the function does not access the image and the interposition library simply calls the function in the local OpenCV library.

Infrastructural approaches

- “the application will never have access to the raw pixels”
  - opaque references



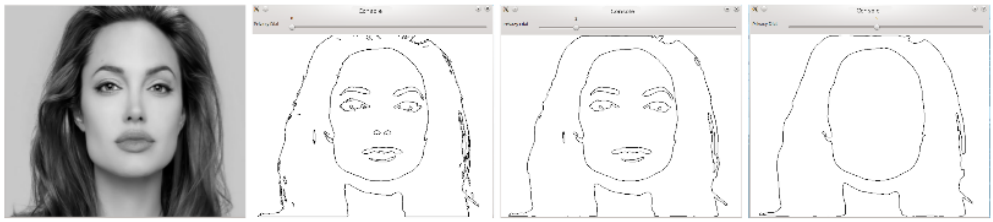


Figure 2. Output of the sketching transform on a female face image at different privacy levels.

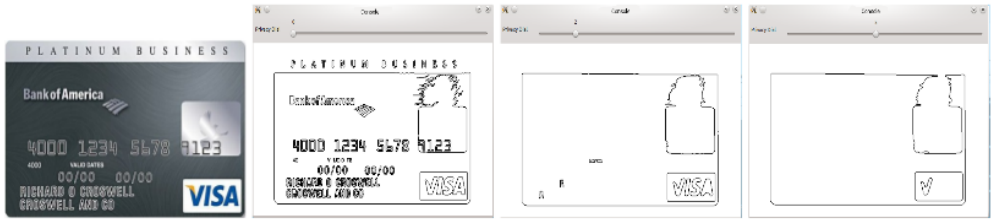
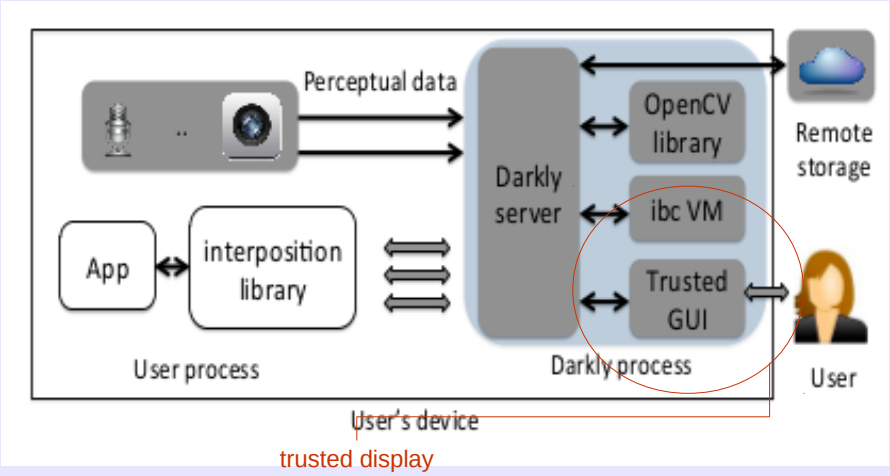


Figure 3. Output of the sketching transform on a credit card image at different privacy levels.

Infrastructural approaches

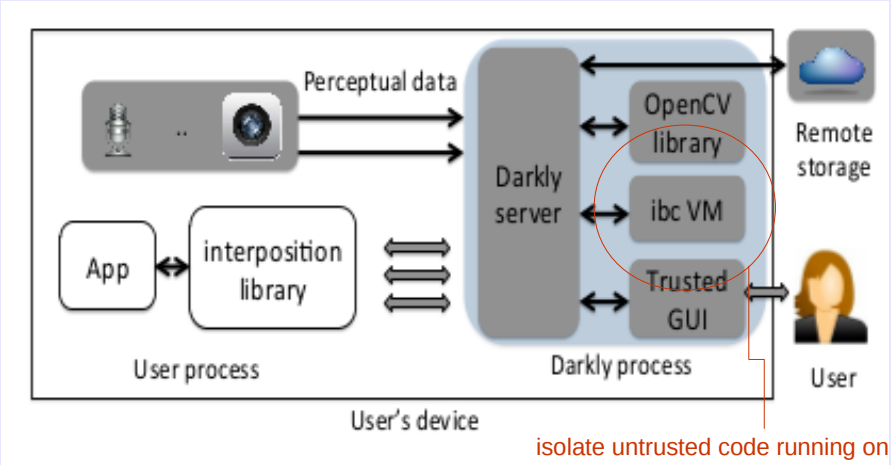
- "the application will never have access to the raw pixels"
  - opaque references



The trusted display serves a dual purpose:
(1) an application can use it to show images to which it does not have direct access, and (2) it shows to the user
the privacy-transformed features and objects released to the
application by declassifiers (see Section VIII).

Infrastructural approaches

- “the application will never have access to the raw pixels”
  - opaque references



ibc programs cannot access D ARKLY ’s or OpenCV’s internal state, and can only read or write through a few D ARKLY functions

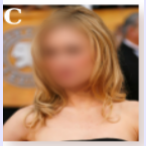
Infrastructural approaches

- Architecture is general in principle, but in practice lots of OpenCV specific tinkering required
  - “DARKLY exploits the fact that most OpenCV data structures for images and video include a separate pointer to the actual pixel data. For example, IplImage’s data pointer is stored in the imageData field; CvMat’s data pointer is in the data field. For these objects, DARKLY creates a copy of the data structure, fills the meta-data, but puts the opaque reference in place of the data pointer. Existing applications can thus run without any modifications as long as they do not dereference the pointer to the pixels”

To block direct access to raw images, DARKLY replaces pointers to image data with opaque references that cannot be dereferenced by applications. Applications can still pass them as arguments into OpenCV functions, which dereference them internally and access the data.

Infrastructural approaches

- Not always clear what a system needs to perform its work, and manual intervention is problematic
  - “The sketch of an image is intended to convey its high-level features while hiding more specific privacy-sensitive details. A loose analogy is publicly releasing statistical aggregates of a dataset while withholding individual records.”
  - May reduce performance in unexpected ways
  - May reduce privacy in unexpected ways
    - Not always intuitive what privacy protections are guaranteed by different transformations of visual input: sketching transform
    - Example: Gaussian blur



Preventative approaches

- Bodyguard FLARE home security camera (link. Also, among the funniest videos I've seen)
- A depolarized monitor matched to polarizing glasses (link)