COLLEGE OF SOCIAL & BEHAVIORAL SCIENCES
School of Information

Layer 8+ Privacy: Analog Hole Problems

Information Privacy with Applications

David Sidi (dsidi@email.arizona.edu)

Warm-up

- Write a couple of sentences on what the problem is that Narayanan and Shmatikov are trying to solve (you may just give an example)

Small mention of interesting things

- In the VM, caps lock and escape are switched
- Project proposals
- Assignment 1 progress

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

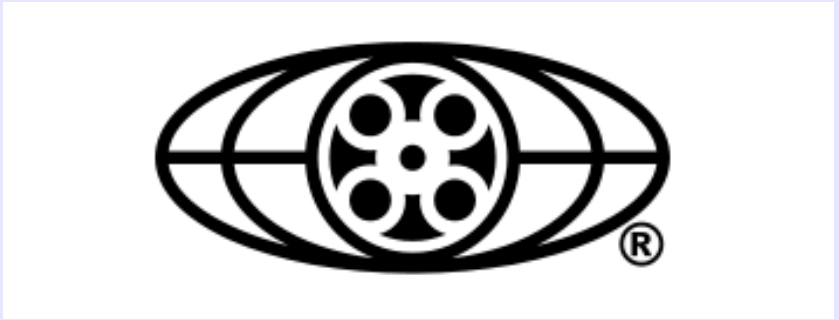
- in general copying stored information is often easy
  - VHS recorders, tape recorders, etc.
- on computers, copying in bulk is easy
  - a single person can distribute a work to zillions of others without much effort

Digital Restrictions Management / Digital Rights Management (DRM)

- broadly, DRM tries to control what 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

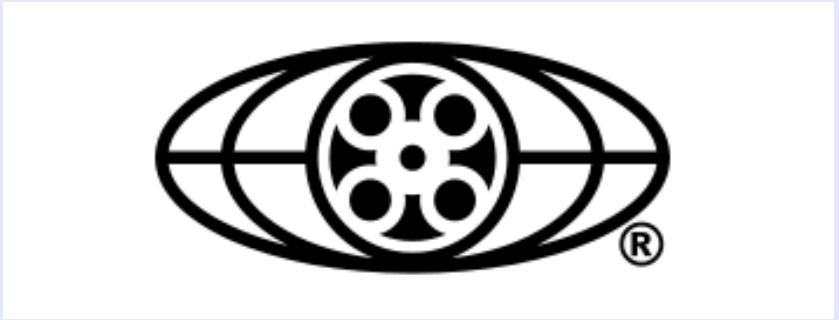
DRM has collateral damage

- Record companies et al. have in mind pirates as adversaries
- Advocacy groups have in mind legitimate users for whom DRM is malware



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



Controversial DRM examples

- John Deere tractors cannot be repaired without software codes
  - they 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

“DRM creates a damaged good; it prevents you from doing what would be possible without it. This concentrates control over production and distribution of media, giving DRM peddlers the power to carry out massive digital book burnings and conduct large scale surveillance over people's media viewing habits.

If we want to avoid a future in which our devices serve as an apparatus to monitor and control our interaction with digital media, we must fight to retain control of our media and software.”

https://www.defectivebydesign.org

Excerpt from EFF resignation letter from W3C

...In our campaigning on this issue, we have spoken to many, many members' representatives who privately confided their belief that the EME was a terrible idea (generally they used stronger language) and their sincere desire that their employer wasn't on the wrong side of this issue. This is unsurprising. You have to search long and hard to find an independent technologist who believes that DRM is possible, let alone a good idea. Yet, somewhere along the way, the business values of those outside the web got important enough, and the values of technologists who built it got disposable enough, that even the wise elders who make our standards voted for something they know to be a fool's errand.

We believe they will regret that choice. 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.

So we'll keep fighting to keep the web free and open. We'll keep suing the US government to overturn the laws that make DRM so toxic, and we'll keep bringing that fight to the world's legislatures that are being misled by the US Trade Representative to instigate local equivalents to America's legal mistakes.

We will renew our work to battle the media companies that fail to adapt videos for accessibility purposes, even though the W3C squandered the perfect moment to exact a promise to protect those who are doing that work for them.

We will defend those who are put in harm's way for blowing the whistle on defects in EME implementations.

It is a tragedy that we will be doing that without our friends at the W3C, and with the world believing that the pioneers and creators of the web no longer care about these matters.

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. It does this by isolating the function of playback of protected video content in the EME specification and integrating it in the Open Web Platform. Our analysis and testing of EME has shown no barriers to accessing captions, transcripts, or audio description of video. 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

Macrovision v. Sima

- 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
- 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”

Side-channel attacks

- van Eck phreaking
  - demonstration of keyboard eavesdropping ()
  - Noise Floor demo. (link @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

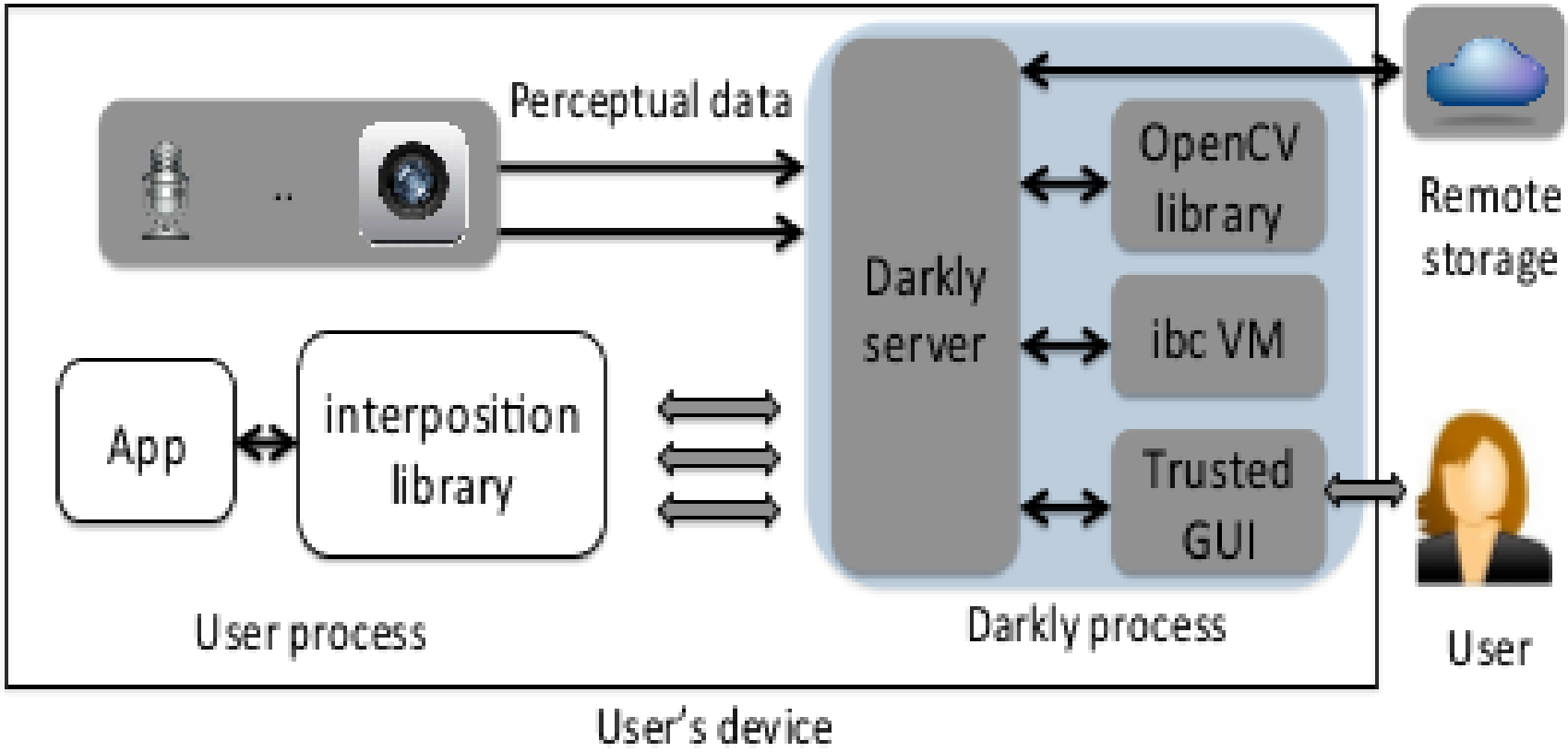
- Similar approaches to DRM exist
- Recording system must read marks embedded in the noise channel
  - macrovision, DCS, CGMS-A, VRAM (VEIL)
  - e.g. (CGMS-A): “a copy protection mechanism for analog television signals. It consists of a waveform inserted into the non-picture Vertical Blanking Interval (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 (for example, at home), and want to be sure that they 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

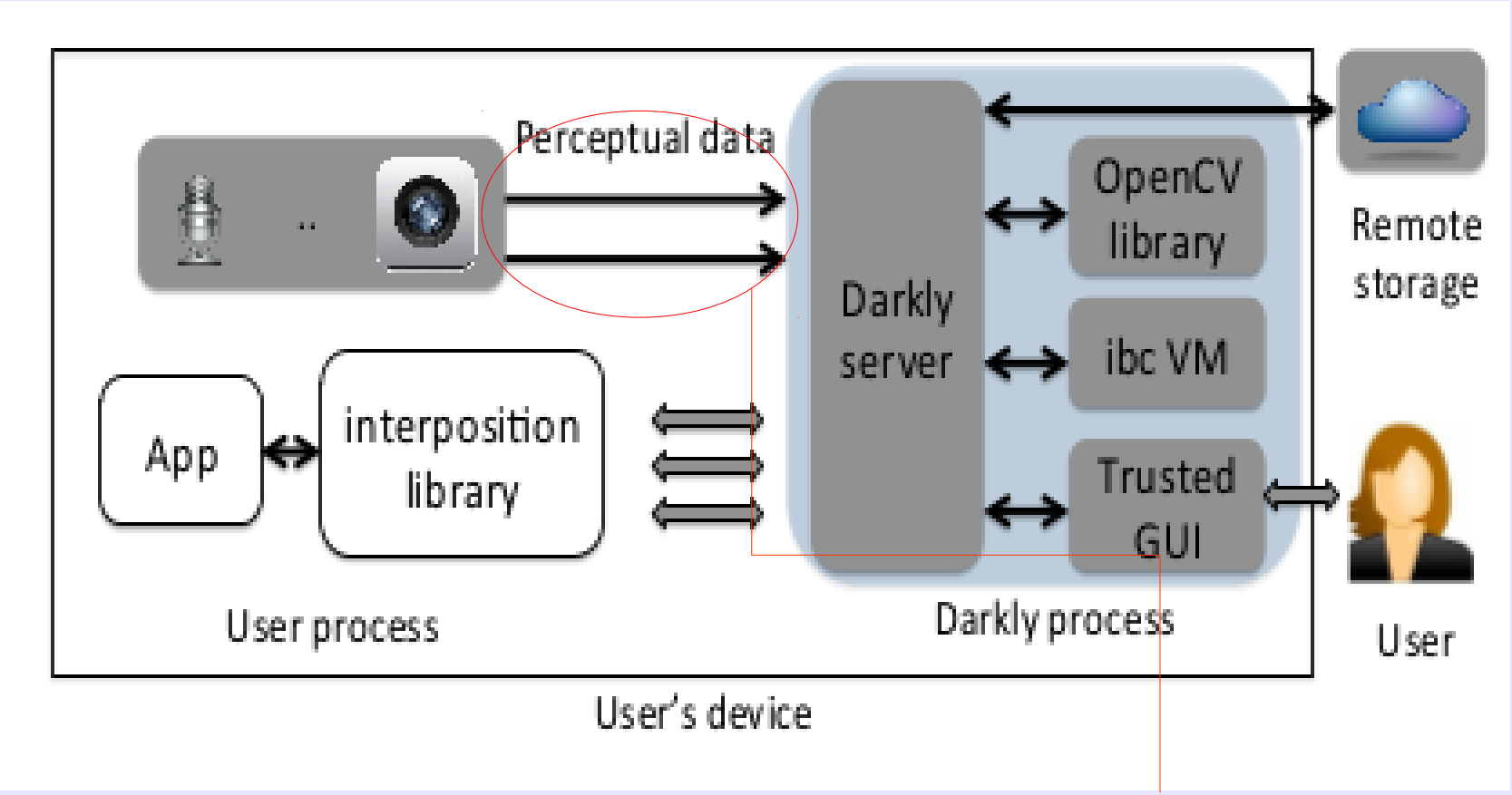
Infrastructural approaches

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



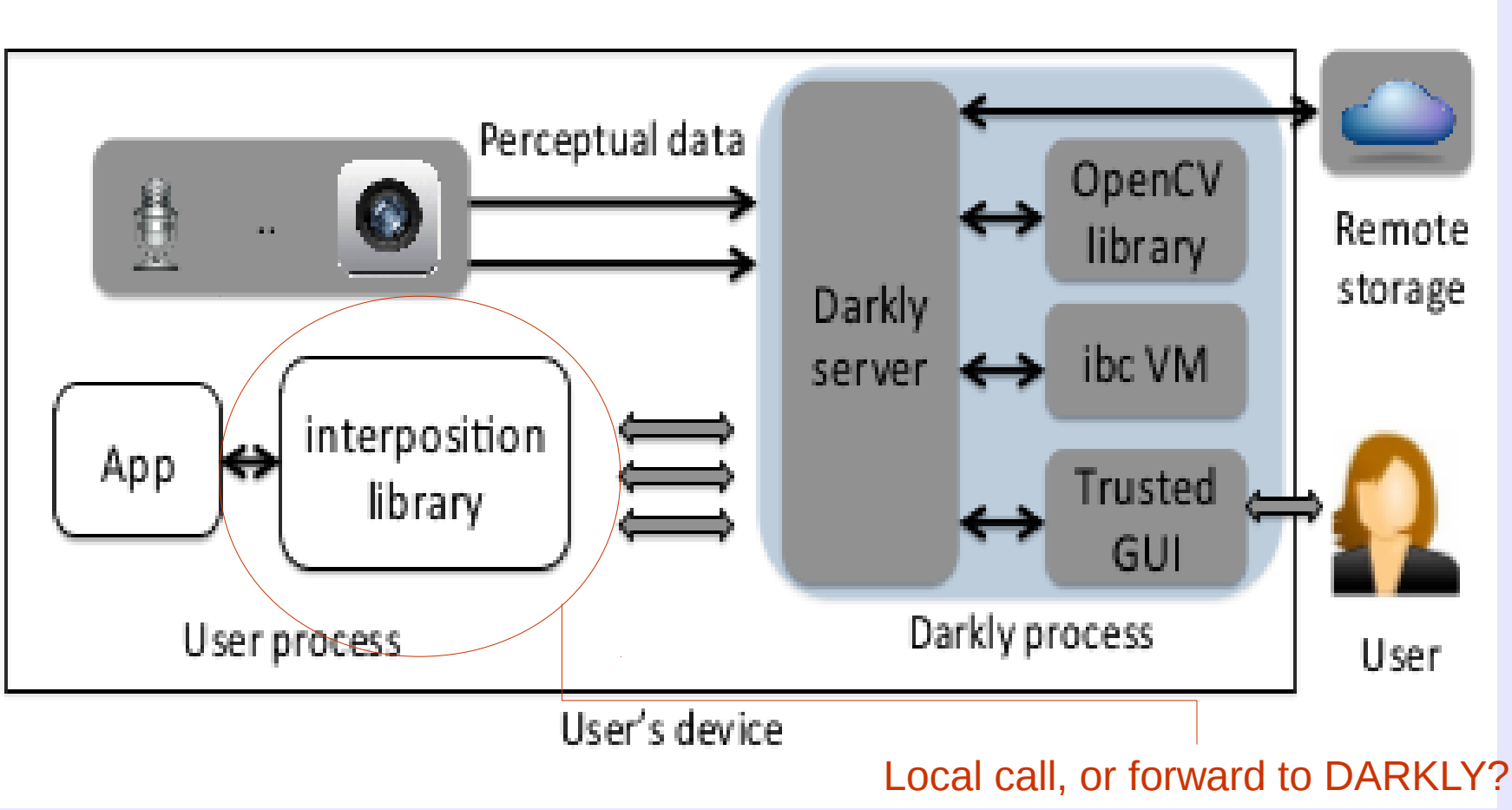
Infrastructural approaches

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



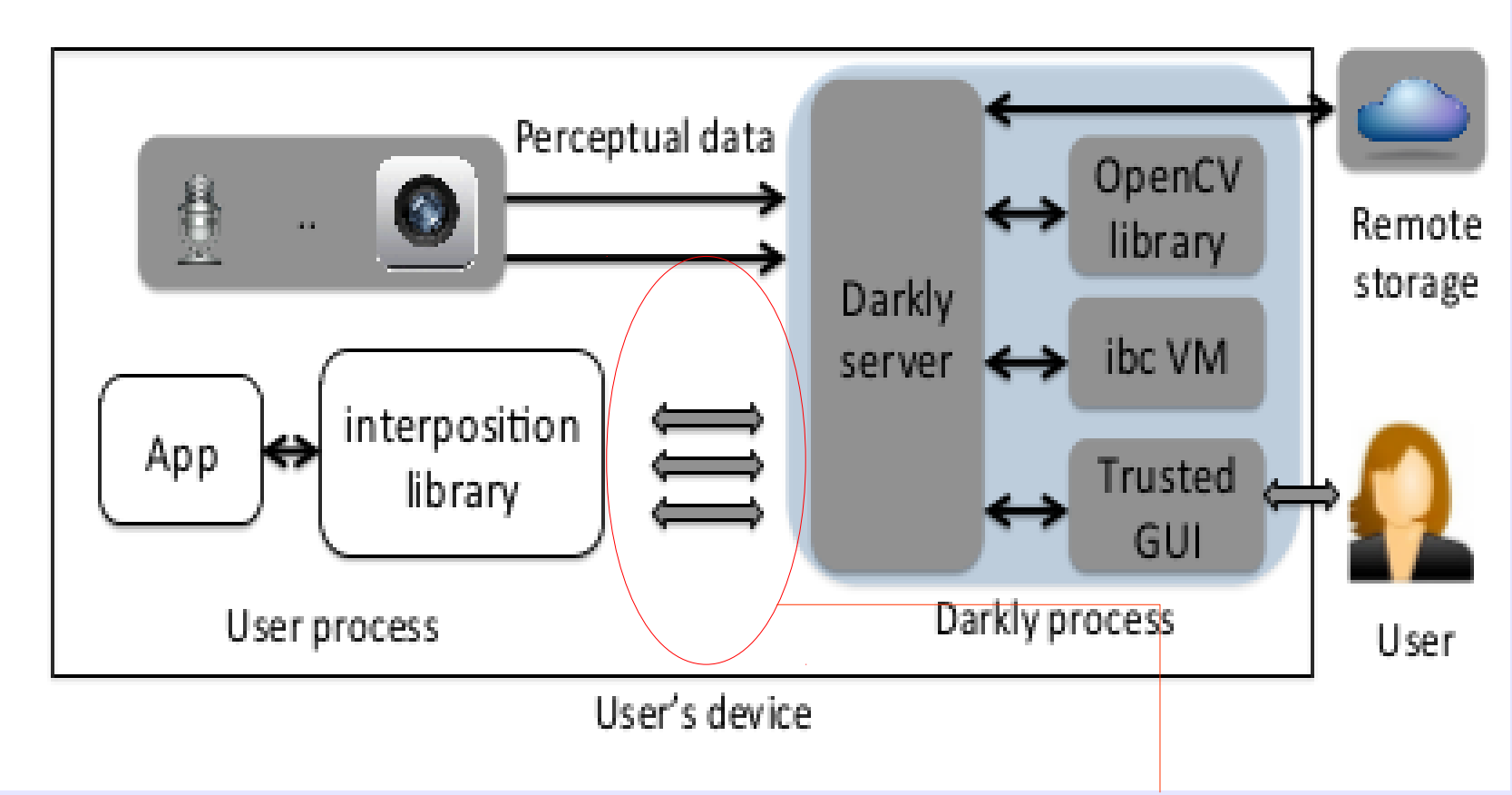
Infrastructural approaches

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



Infrastructural approaches

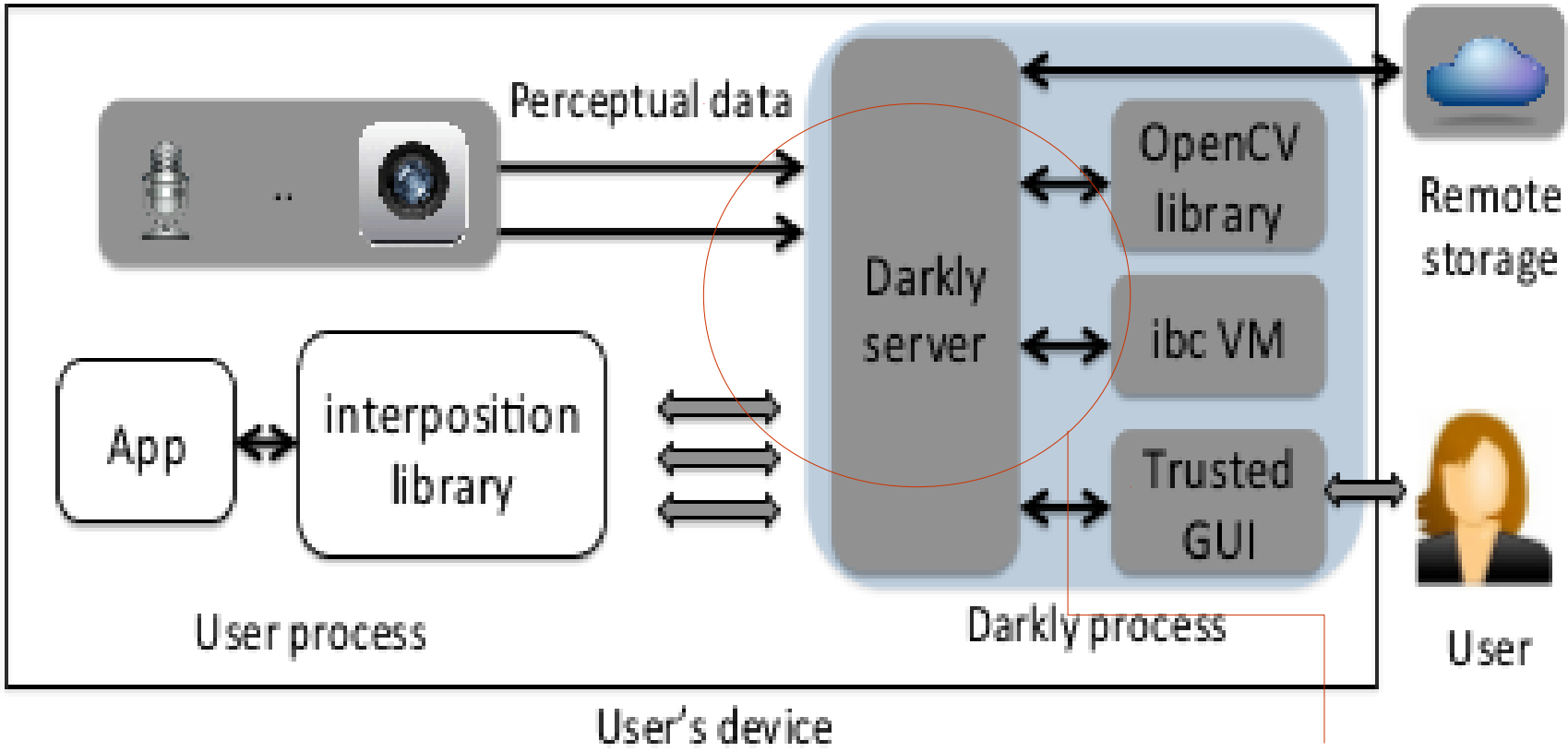
- “the application will never have access to the raw pixels”
  - opaque references



any opaque references?

Infrastructural approaches

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



declassifiers (e.g., sketching transform)

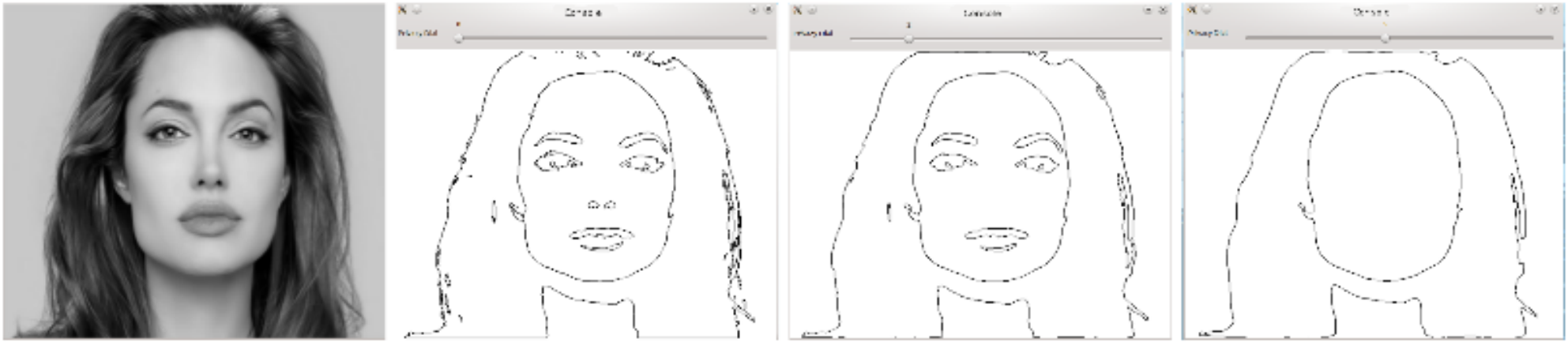


Figure 2. Output of the sketching transform on a female face image at different privacy levels.

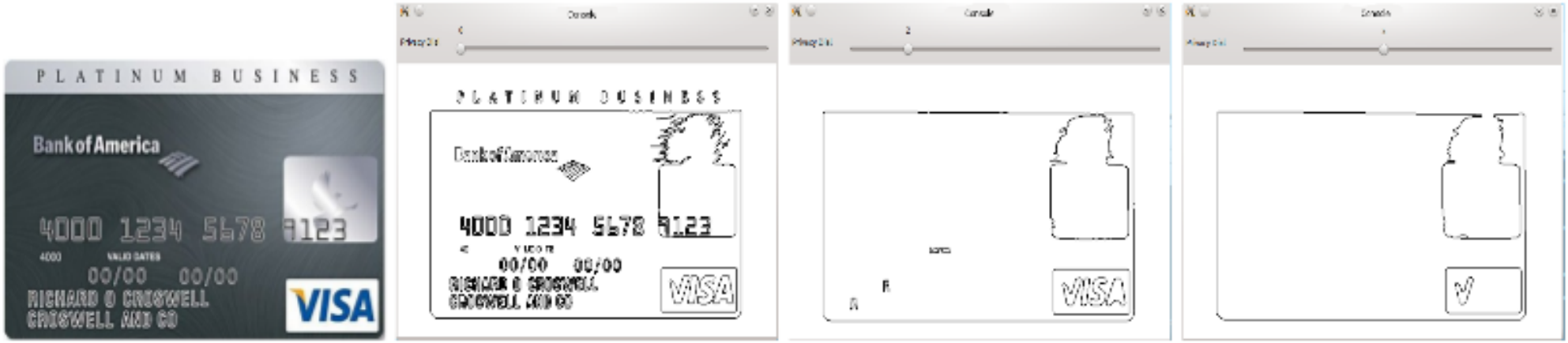
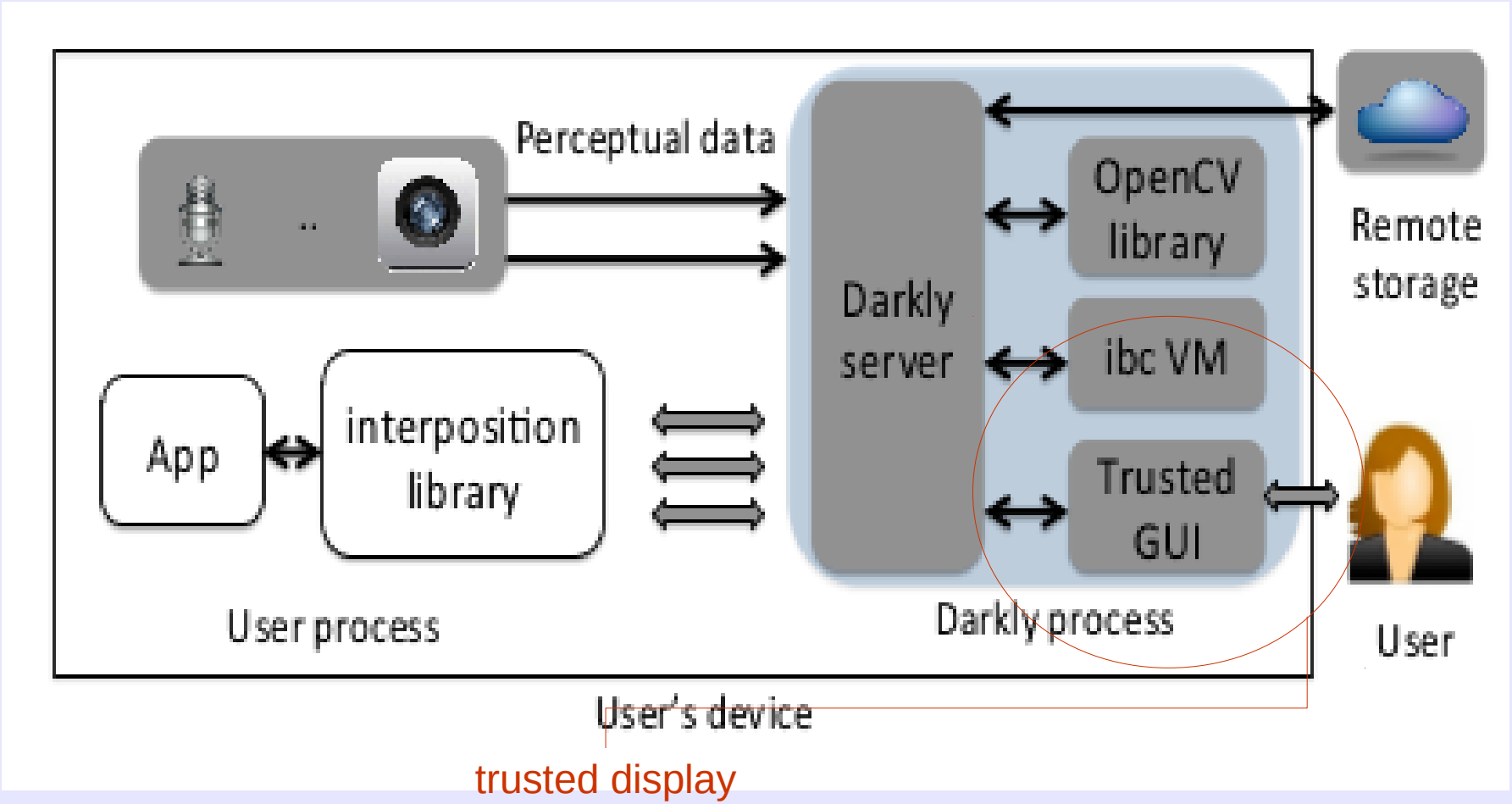


Figure 3. Output of the sketching transform on a credit card image at different privacy levels.

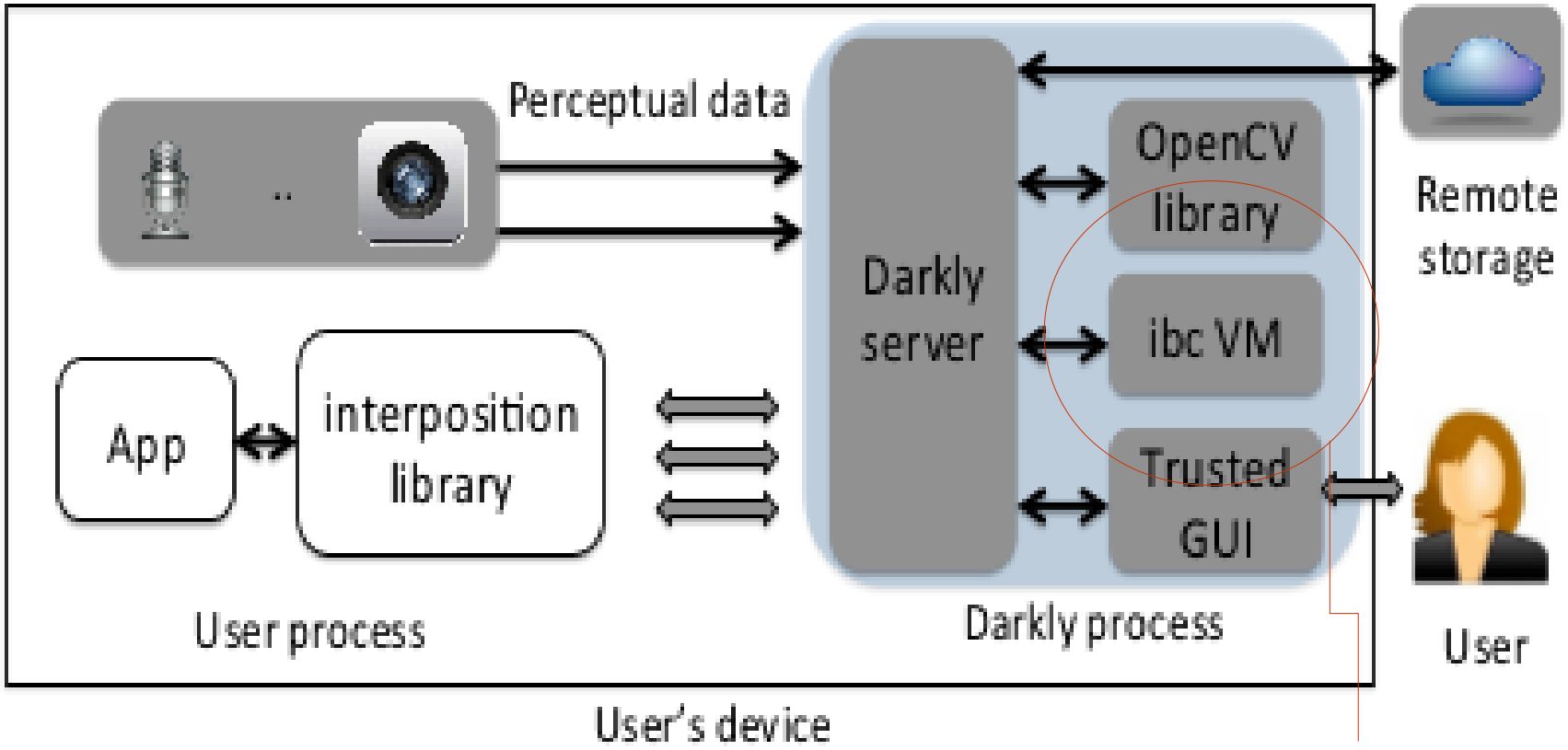
Infrastructural approaches

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



Infrastructural approaches

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



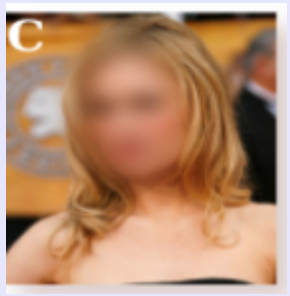
isolate untrusted code running on raw input

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”

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)