Seminar on Privacy in Ubiquitous Computing

Mehmed Mustafa
Institute of Computer Science
University of Göttingen
mehmed.mustafa@stud.uni-goettingen.de

Chris Warin
Institute of Computer Science
University of Göttingen
chris.warin@stud.uni-goettingen.de

***Abstract*—This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Index Terms*—privacy, bystander, privacy enhancing technology**

I. Introduction

Today's society is filled with technological devices that are capable of gathering data from people, such as smartphones [1], surveillance cameras [2], *Augmented Reality* (AR) devices [3] or *Internet of Things* (IoT) devices [1]. Although these devices been causing a number of concerns regarding the privacy of users, another topic—that is less publicly discussed, but as important—is the privacy of bystanders, i.e. the people that are around users using these devices, and of which personal information can be collected without their knowledge or consent.

A common real-life example could be a person taking a picture in a busy street, where the faces of bystanders are recognizable. The picture can later be posted on social media, and neither the posting or the taken picture have been made with the knowledge nor consent of the bystanders [3]. The data that are collected from bystanders can come from different mediums (i.e. pictures, videos, audio), and can be of different nature (i.e. face, voice, location). This results in pervasiveness in bystanders' privacy and touches several domains, namely economical, social, legal, and technological.

In the past, several attempts have been made in order to ensure the privacy of bystanders; technological attempts (e.g. gaussian blur, pixelisation [4]), as well as partial solutions to avoid privacy issues (e.g. forbidding the use of cameras in certain places[3]). However, these have been proven either inefficient [4] or insufficient [3].

This report focuses on the different technologies that address the pervasiveness in the privacy of bystanders. Section II lists different real-life examples of bystanders' privacy being compromised. Section III goes over different technologies that ensure different aspects of the privacy of bystanders. Section IV describes the current limitations and challenges that these technologies are facing, whether they are technological or not. Finally, section V concludes this report.

II. Bystanders' privacy pervasiveness

Give real-life examples and why they are problematic.

A. Videos and images

Surveillance cameras, smartphone photos/videos in the street capturing bystanders

B. Audio

Google Home / Amazon Alexa in a household: other members are also listened

C. Location

Pervasive location information in apps (e.g. French StopCovid app recenses more contacts' location information than announced)

D. Others

IoT, see example in 2.b

III. Technologies for ensuring the privacy of bystanders

A. PriSurv System

Video surveillance systems are necessary for a safe and secure community, which explains why they are widely deployed. However, high deployment rate of these systems in public places leads to privacy invasion of the objects being recorded. Solution of this problem is a challenging task because privacy and security should be balanced appropriately and when possible in real-time. There are several other studies on privacy based on video surveillance. Two studies proposed image processing methods in order to protect the privacy of objects [5][6]. In some other studies the privacy protection of objects depends either on the authority of objects or observers [7][8]. Privacy information can be embedded by using digital watermarking technology in a such way that only predefined authorized viewers will have access to it [9]. However, these solutions are not flexible enough, because the sense of privacy of different objects is not considered. For example, object A may want his or her privacy to be protected from observer A, but not from observer B.

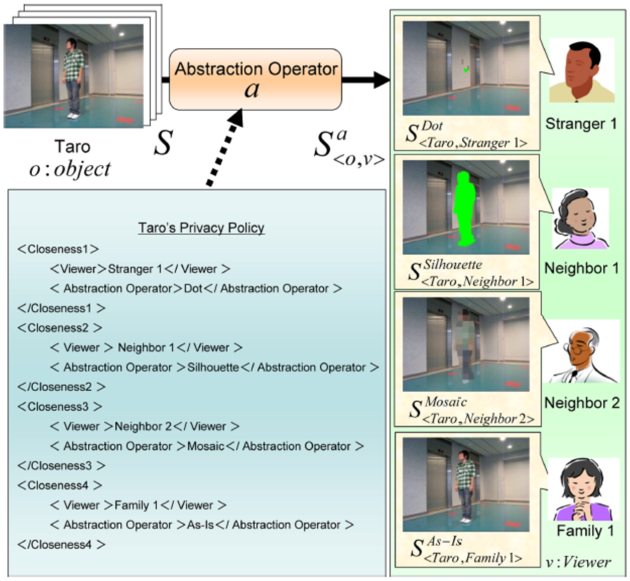
Taro
$o: object$
S
Abstraction Operator
a
$S^{a}_{<o,v>}$
Taro's Privacy Policy
<Closeness1>
<Viewer>Stranger 1</ Viewer >
< Abstraction Operator>Dot</ Abstraction Operator >
</Closeness1 >
<Closeness2 >
< Viewer > Neighbor 1</ Viewer >
< Abstraction Operator >Silhouette</ Abstraction Operator >
</Closeness2 >
<Closeness3 >
< Viewer >Neighbor 2</ Viewer >
< Abstraction Operator >Mosaic</ Abstraction Operator >
</Closeness3 >
<Closeness4 >
< Viewer >Family 1</ Viewer >
< Abstraction Operator >As-Is</ Abstraction Operator >
</Closeness4 >
$S^{Dot}_{<Taro,Stranger 1>}$
Stranger 1
$S^{Silhouette}_{<Taro,Neighbor 1>}$
Neighbor 1
$S^{Mosaic}_{<Taro,Neighbor 2>}$
Neighbor 2
$S^{As-Is}_{<Taro,Family 1>}$
Family 1
$v: Viewer$

Figure 1. PriSurv simple run case [10].

Some objects may not want a privacy protection at all. PriSurv system [10] can adaptively protect privacy of objects and disclosure their visual information according to the privacy policies of the different objects. PriSurv is a video surveillance system, which is defined by visual abstraction and protects the privacy of objects appearing within a video depending who observes the video. Closeness between objects and observers determines the privacy policies to be used.

1) Simple run case: Figure 1 is an example run case of PriSurv, which shows how visual abstraction is used in order to protect the privacy of an object appearing within an image. Let o, a, v and S denote an object, an abstraction operator, a viewer and an original image, respectively. In the example, "Taro" is the object which appears within the original image and is monitored by "Stranger 1", "Neighbor 1", "Neighbor 2" and "Family 1" which are the different viewers. Since the closeness between the object and viewers is different, different abstraction operators are used for hiding the visual information of the object. In the example, these operators are "Dot", "Silhouette", "Mosaic" and "As-Is", just 4 out of 12 possible. Each viewer then receives a privacy protected version of the original image which is denoted by $S^{a}_{<o,v>}$. A simplified version of Taro's privacy policy, which is a part of the abstraction operator, is also available to give better understanding how the closeness is defined.

2) System overview: Figure 2 shows the architecture of the PriSurv system. It consists of three main parts: Video Server, Main Server and Network. It also has six different components: Analyzer, Profile Generator, Profile Base, Access Controller, Abstractor and Video Data Base. Analyzer, which is a part of the video server, is responsible for identifying different objects. Each identifiable object must have own *Radio-frequency identification* (RFID)-tag. The surveillance area is divided into smaller N x N areas and the location area of each RFID-tag is determined by an RFID-reader. Each object inside the original image is extracted and then identified separately by comparing the obtained visual data with the binary images of each object. Profile Generator is used for setting up privacy policies for different members of the system. Each member's personal information such as name, age, gender and address and privacy policy stored securely inside the Profile Base. Profile Generator is also responsible for converting data taken from the GUI to *Extensible Markup Language* (XML) based syntax. The profile of each member can be updated only by them and other members have no access to this data. Access Controller determines what is the closeness relationship between a requesting viewer and an object to be monitored by reading XML based privacy policies of the object stored inside the Profile Base. Once the types of abstraction operators are extracted, Access Controller sends them to the Abstractor. Abstractor is a processor for images which does visual abstraction by using abstraction operators. Video Data Base stores past video data and makes it available to viewers after appropriate visual abstractions are performed.

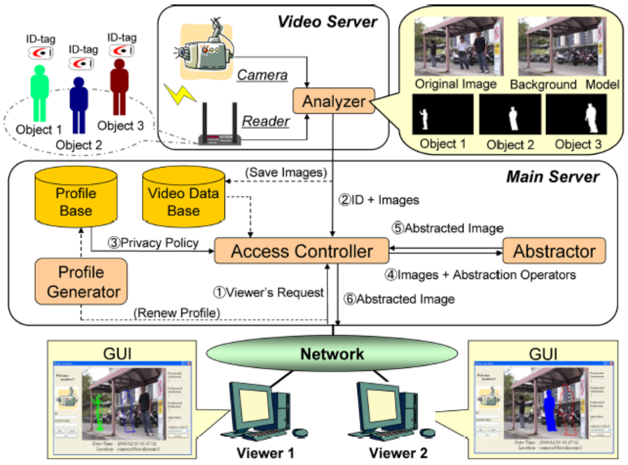

Figure 2. PriSurv system overview [10].

B. Sharing of Multi-Subject and Interdependent Data

Reference [11]

C. Cardea Framework

Reference [3]

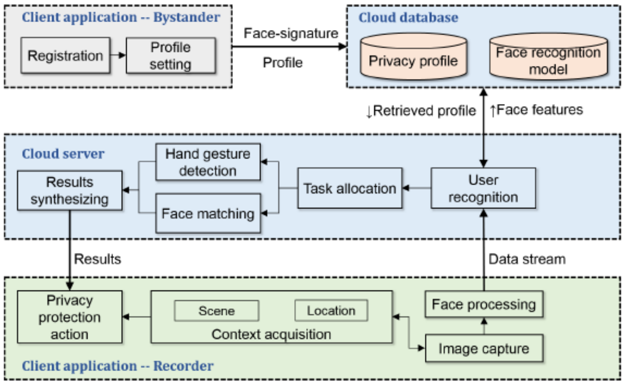

Figure 3. Cardea framework overview [3].

D. Others - More specific Audio or Location based technologies should be found

IV. Limitations and challenges of privacy ensuring technologies

A. Cardea (user contribution)

Willingly putting your personal data on a cloud to avoid having your privacy invaded by others can be seen as counter productive

B. Example 2

C. Example 3

D. (optionally) Ideas that could fix these limitations

V. Conclusion

Table I
Table Type Styles

Table Head	**Table Column Head**		
	Table column subhead	***Subhead***	***Subhead***
copy	More table copy[a]		

[a]Sample of a Table footnote.

References

Please number citations consecutively within brackets [3]. The sentence punctuation follows the bracket [4]. Refer simply to the reference number, as in [2]—do not use "Ref. [2]" or "reference [2]" except at the beginning of a sentence: "Reference [1] was the first . . ."

Number footnotes separately in superscripts.[10] Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [1]. Papers that have been accepted for publication should be cited as "in press" [11]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.[12]

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [11].

Abbreviations and Acronyms

IoT *Internet of Things*
AR *Augmented Reality*
RFID *Radio-frequency identification*
XML *Extensible Markup Language*

References

[1] Y.-H. Lu, A. Cavallaro, C. Crump, G. Friedland, and K. Winstein, "Privacy protection in online multimedia," in *Proceedings of the 25th ACM international conference on Multimedia*, pp. 457–459, 2017.

[2] T. Denning, Z. Dehlawi, and T. Kohno, "In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2377–2386, 2014.

[3] J. Shu, R. Zheng, and P. Hui, "Cardea: Context-aware visual privacy protection from pervasive cameras," *arXiv preprint arXiv:1610.00889*, 2016.

[4] F. Dufaux and T. Ebrahimi, "A framework for the validation of privacy protection solutions in video surveillance," in *2010 IEEE International Conference on Multimedia and Expo*, pp. 66–71, IEEE, 2010.

[5] A. Cavallaro, O. Steiger, and T. Ebrahimi, "Semantic video analysis for adaptive content delivery and automatic description," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 15, pp. 1200–1209, 11 2005.

[6] I. Kitahara, K. Kogure, and N. Hagita, "Stealth vision for protecting privacy," vol. 4, pp. 404–407 Vol.4, 09 2004.

[7] J. Wickramasuriya, M. Alhazzazi, M. Datt, S. Mehrotra, and N. Venkatasubramanian, *Privacy-protecting video surveillance*. 02 2005.

[8] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y. Li, A. Ekin, J. Connell, C.-F. Shu, and M. Lu, "Enabling video privacy through computer vision," *Security & Privacy, IEEE*, vol. 3, pp. 50–57, 06 2005.

[9] W. Zhang, S.-c. Cheung, and M. Chen, "Hiding privacy information in video surveillance system," pp. 868–871, 01 2005.

[10] N. Chinomi and B. Ito, "Prisurv: Privacy protected video surveillance system using adaptive visual abstraction," in *Advances in Multimedia Modeling*, pp. 144–154, 2008.

[11] A.-M. Olteanu, K. Huguenin, I. Dacosta, and J.-P. Hubaux, "Consensual and privacy-preserving sharing of multi-subject and interdependent data," in *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS)*, pp. 1–16, Internet Society, 2018.

[12] S. Aditya and O. Druschel, "I-pic: A platform for privacy-compliant image capture," 2016.