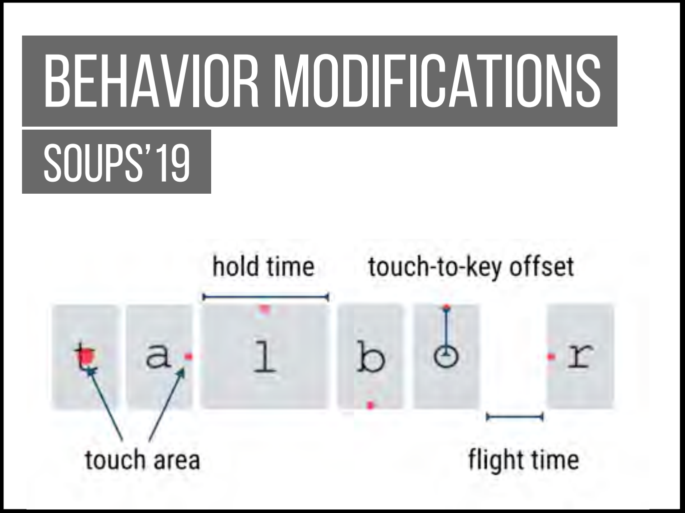
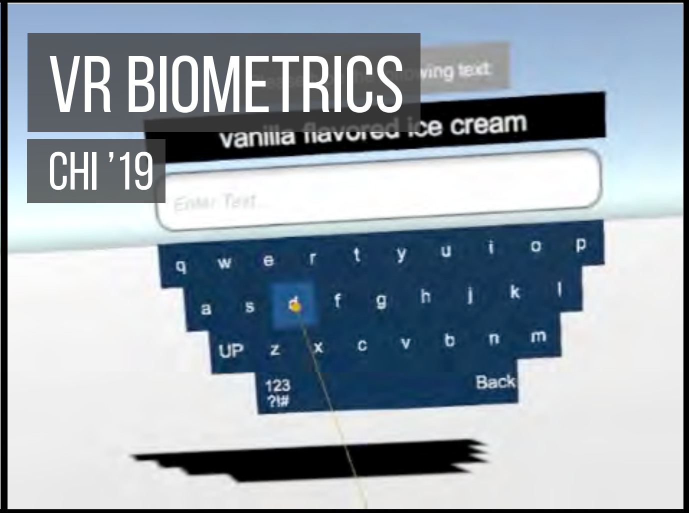
Security and Privacy for Technologies That Have Very Personal Data

Florian Alt



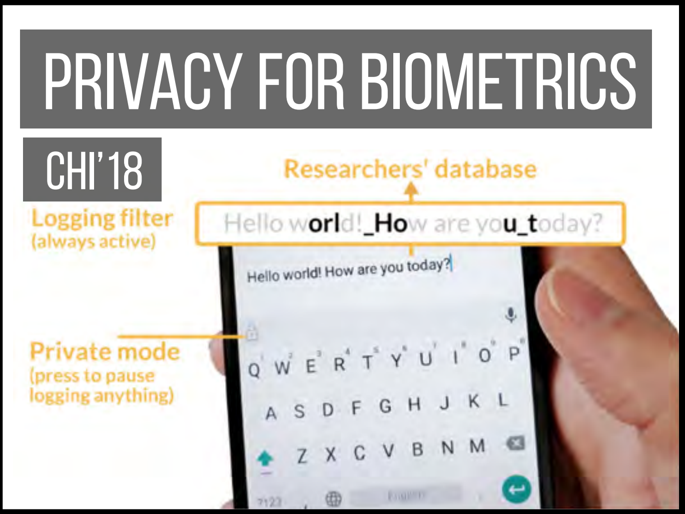
BEHAVIOR MODIFICATIONS
SOUPS’19

RE-AUTHENTICATION
SOUPS’19

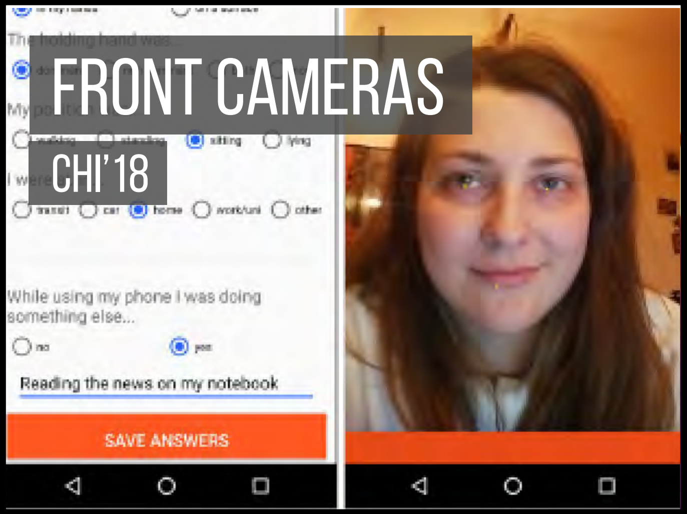


VR BIOMETRICS
CHI ’19

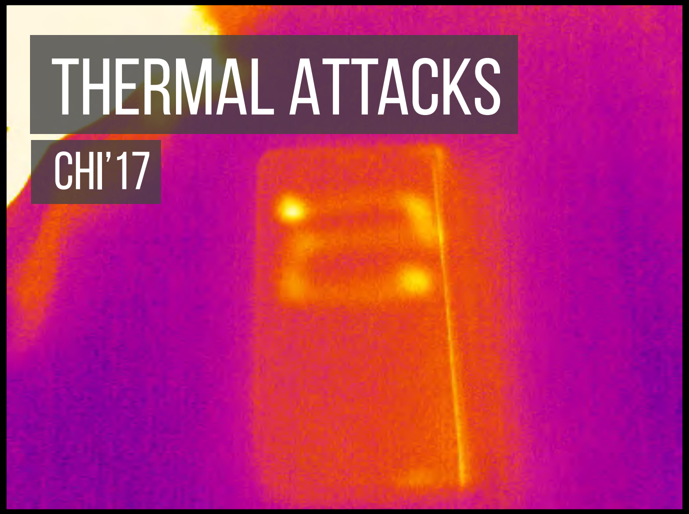
SMART HOME AUTH
EUROUSEC’19


Researchers' database
Logging filter
(always active)
Hello world!_How are you_today?
Hello world! How are you today?
Private mode
(press to pause logging anything)

PRIVACY FOR BIOMETRICS
CHI’18


While using my phone I was doing something else...
Reading the news on my notebook
SAVE ANSWERS

FRONT CAMERAS
CHI’18

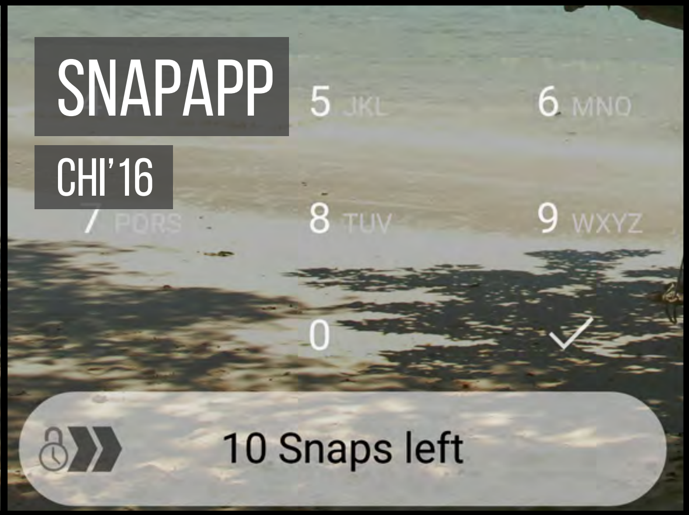


THERMAL ATTACKS
CHI’17

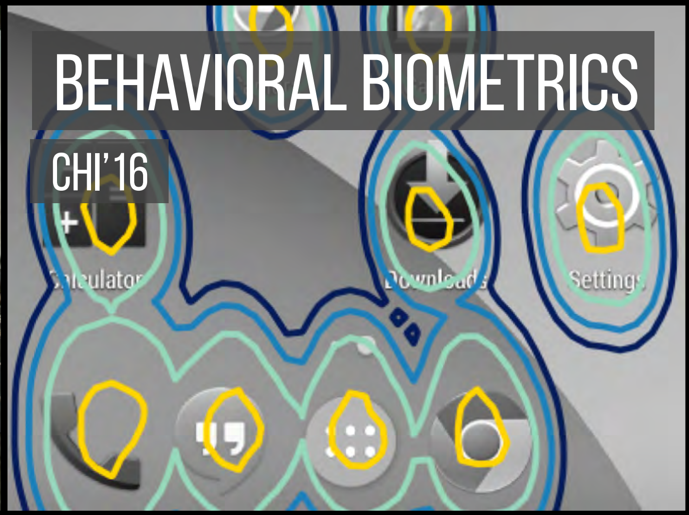
PROBUI
CHI’17

SHOULDER SURFING
CHI’17

VR AUTHENTICATION
USEC’17



SNAPAPP
CHI’16



BEHAVIORAL BIOMETRICS
CHI’16

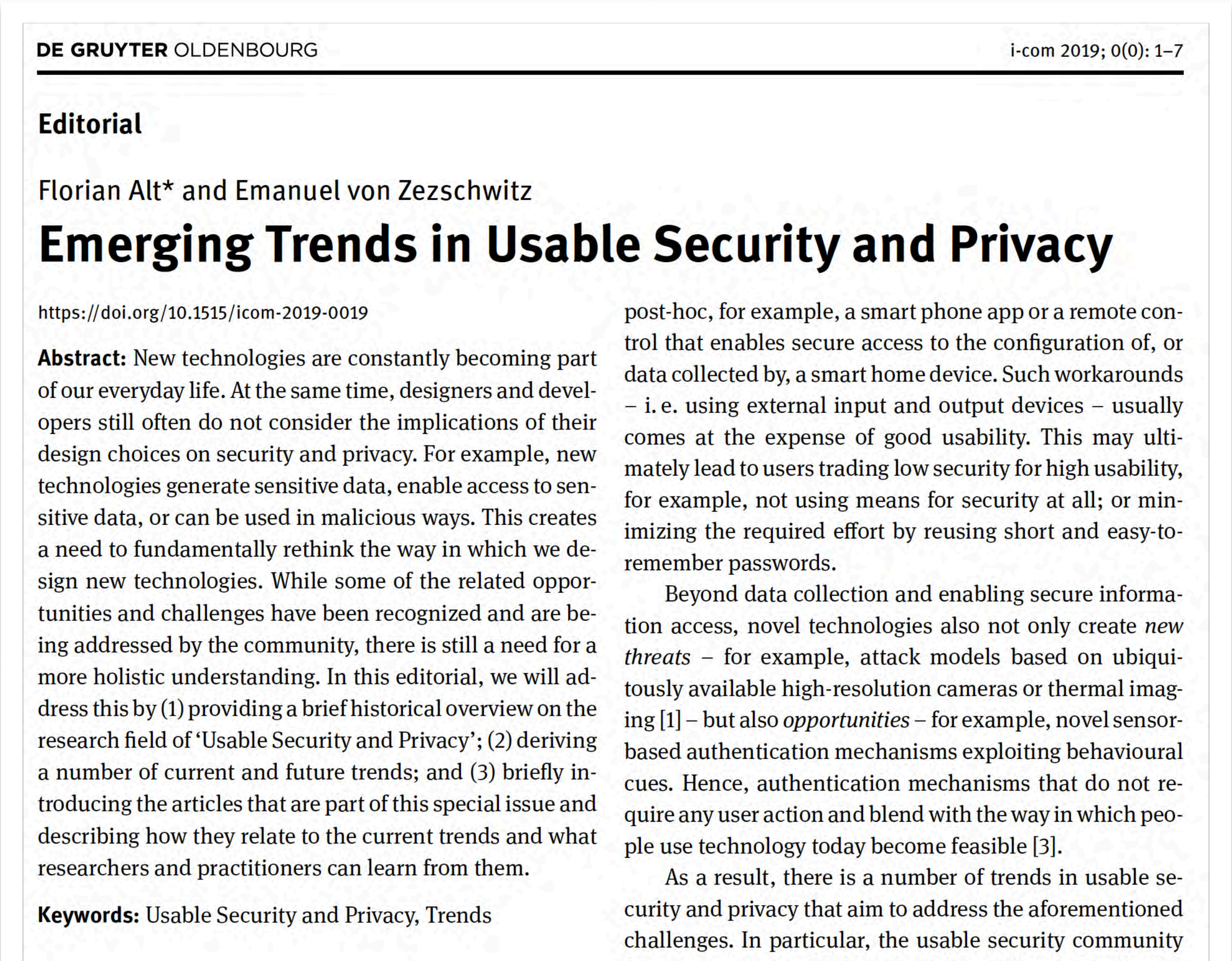
MEMORABILITY
MUM ’16

SMUDGESAFE
UBICOMP ’15

IN-THE-WILD
MOBILEHCI’15

GAZE AUTHENTICATION
CHI’14

TRENDS IN USABLE SECURITY



DE GRUYTER OLDENBOURG i-com 2019; 0(0): 1–7

Editorial

Florian Alt* and Emanuel von Zezschwitz

Emerging Trends in Usable Security and Privacy

https://doi.org/10.1515/icom-2019-0019

Abstract: New technologies are constantly becoming part of our everyday life. At the same time, designers and developers still often do not consider the implications of their design choices on security and privacy. For example, new technologies generate sensitive data, enable access to sensitive data, or can be used in malicious ways. This creates a need to fundamentally rethink the way in which we design new technologies. While some of the related opportunities and challenges have been recognized and are being addressed by the community, there is still a need for a more holistic understanding. In this editorial, we will address this by (1) providing a brief historical overview on the research field of 'Usable Security and Privacy'; (2) deriving a number of current and future trends; and (3) briefly introducing the articles that are part of this special issue and describing how they relate to the current trends and what researchers and practitioners can learn from them.

Keywords: Usable Security and Privacy, Trends

post-hoc, for example, a smart phone app or a remote control that enables secure access to the configuration of, or data collected by, a smart home device. Such workarounds – i. e. using external input and output devices – usually comes at the expense of good usability. This may ultimately lead to users trading low security for high usability, for example, not using means for security at all; or minimizing the required effort by reusing short and easy-to-remember passwords.

Beyond data collection and enabling secure information access, novel technologies also not only create *new threats* – for example, attack models based on ubiquitously available high-resolution cameras or thermal imaging [1] – but also *opportunities* – for example, novel sensor-based authentication mechanisms exploiting behavioural cues. Hence, authentication mechanisms that do not require any user action and blend with the way in which people use technology today become feasible [3].

As a result, there is a number of trends in usable security and privacy that aim to address the aforementioned challenges. In particular, the usable security community

Session Objectives

- Understanding Threats to Very Personal Data
- Protecting Very Personal Data
- Publishing Privacy / Security Research

Motivation

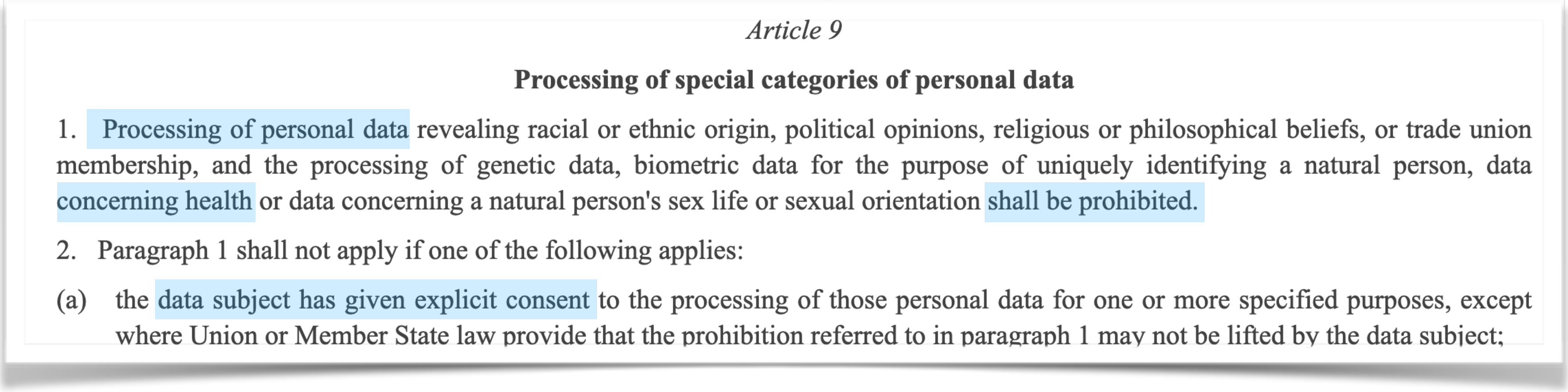
- Importance of protecting very personal data
  - often **not** possible to only decide **for yourself only** (genetic data will reveal information on your relatives)
  - **People might not want to know** their medical condition
    - psychological stress
    - medical consequences
- IT security and safety may be **opposing goals**
- Data **protection vs.** scientific **progress**

GDPR Principles

- **Lawful basis for processing**
  - explicit informed consent required for making data publicly available
  - can be revoked anytime
- **Responsibility and accountability**
  - subject must be informed about the extent of data collection
  - pseudonymization of data
  - right to view personal data and access to an overview how it is being processed
- **Data protection by design and by default**
  - highest possible privacy-settings by default
- **Right to erasure**
  - users can request their data to be erased within 30 days
- **Data breaches**
  - must be reported within 72 hours
- **Sanctions**
  - fines up to 20M US$ / 4% annual worldwide turnover

Medical Privacy

- **GDPR, Art. 9**



Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

- **Data Privacy Impact Assessment required** (needs documentation)
  - Description of planned processing
  - Assessment of necessity and proportionality
  - Risk assessment
  - Action planning (access protection, encryption, etc.)
- BMWi: Orientierungshilfe zum Gesundheitsdatenschutz (German only) https://www.bmwi.de/Redaktion/DE/Downloads/M-O/orientierungshilfe-gesundheitsdatenschutz.pdf?__blob=publicationFile&v=16

Privacy of Health Data in Other Countries

- **Medical Privacy Laws**
  existing in Australia, Canada, Turkey, UK, US, New Zealand, Netherlands
- **Example:**
  Health Insurance Portability and Accountability Act (HIPAA)
  - The **Privacy Rule**:
    national standards for when protected health information (PHI) may be used and disclosed
  - The **Security Rule:**
    specifies safeguards to protect confidentiality, integrity, and availability of electronic protected health information (ePHI)
  - The **Breach Notification Rule:**
    requirement for notifications (U.S. Department of Health & Human Services (HHS); the media) in case of a breach of unsecured PHI

HIPAA — Security Rule

- **Administrative Safeguards – Policies and procedures designed to clearly show how the entity will comply with the act**
  - Adopt **written set of privacy procedures**
  - Designate a **privacy officer** (developing and implementing required policies and procedures)
  - Clearly **identify employees or classes of employees who will have access** to PHI
  - Provide **training program** regarding the handling of PHI
  - Vendors to comply with HIPAA law requirements
  - **Data backup and disaster recovery procedure**
  - Routine and event-based audits
  - **Instructions for addressing and responding to security breaches**

HIPAA — Security Rule

- **Physical Safeguards – controlling physical access to data**
  - Govern the **introduction and removal of hardware and software**
  - Equipment taken out of service must be **disposed** of properly
  - Access to equipment containing health information should be carefully **controlled and monitored**.
  - Access limited to properly **authorized individuals** (sign-in and escorts).
  - Address **proper workstation use** (workstations not in high-traffic areas, screens not in direct view of public)
  - Contractors must be **fully trained** on physical access responsibilities

HIPAA — Security Rule

- **Technical Safeguards – controlling access to computers**
  - **Intrusion protection** (encryption of network traffic; access control)
  - Data **integrity** must be maintained (e.g., use of check sum, message authentication, digital signature)
  - **Authentication of entities** (passwords, two or three-way handshakes, telephone callback, tokens)
  - **Documentation** of
    - HIPAA practices (available to government)
    - Information technology (configuration of network components)
  - **Risk analysis** and **risk management**

Protecting Sensitive Data in (HCI) Studies

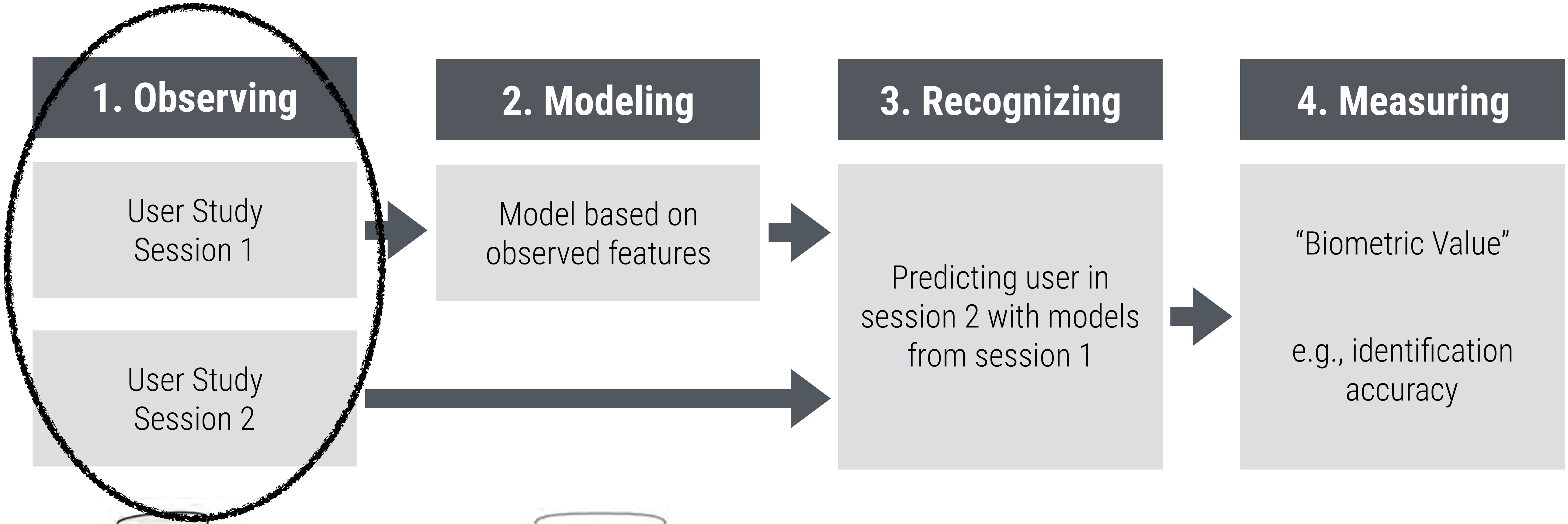
STUDYING NATURAL TYPING BEHAVIOR

— CHI 2018 —

Buschek, Bisinger, Alt. “ResearchIME: A Mobile Keyboard Application for Studying Free Typing Behaviour in theWild”.

CHI ’18

BUILDING A BEHAVIORAL BIOMETRICS SYSTEM



1. Observing

User Study Session 1

User Study Session 2

2. Modeling

Model based on observed features

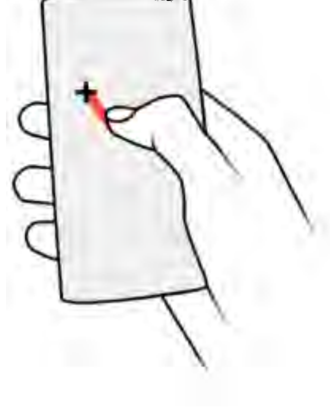
3. Recognizing

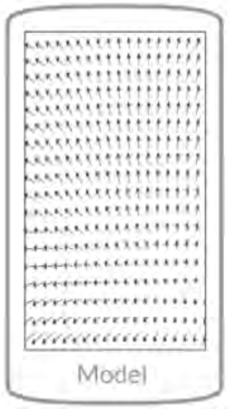
Predicting user in session 2 with models from session 1

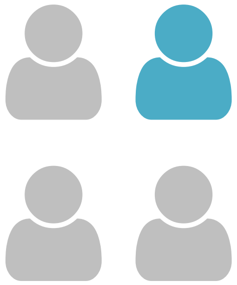
4. Measuring

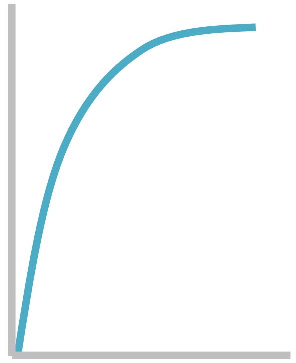
"Biometric Value"

e.g., identification accuracy



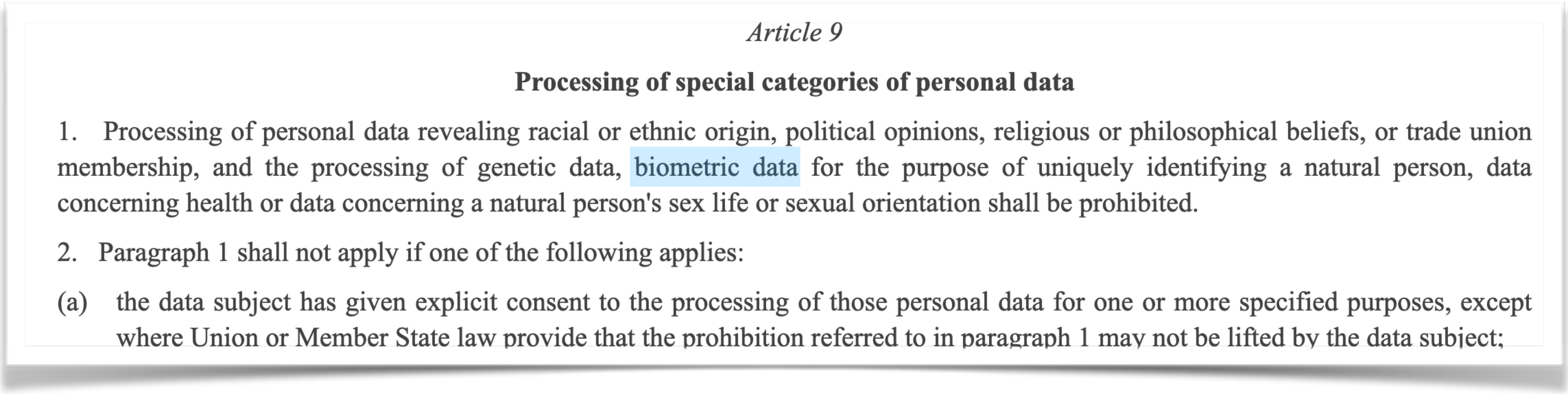






Medical Privacy

- **GDPR, Art. 9**



Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

- **Privacy impact assessment required** (needs documentation)
  - Description of planned processing
  - Assessment of necessity and proportionality
  - Risk assessment
  - Action planning (access protection, encryption, etc.)
- BMWi: Orientierungshilfe zum Gesundheitsdatenschutz (German only) https://www.bmwi.de/Redaktion/DE/Downloads/M-O/orientierungshilfe-gesundheitsdatenschutz.pdf?__blob=publicationFile&v=16

APPROACH

1. What to log?

Literature Review

Data & Requirements

2. How to log?

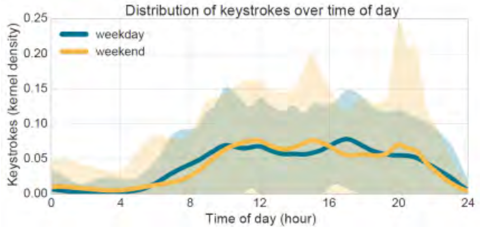
Filter concepts

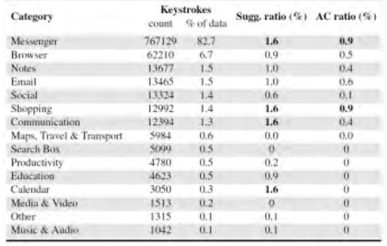
Online Survey

Filter & parameters

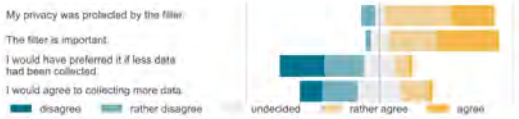
3. System

4. Study



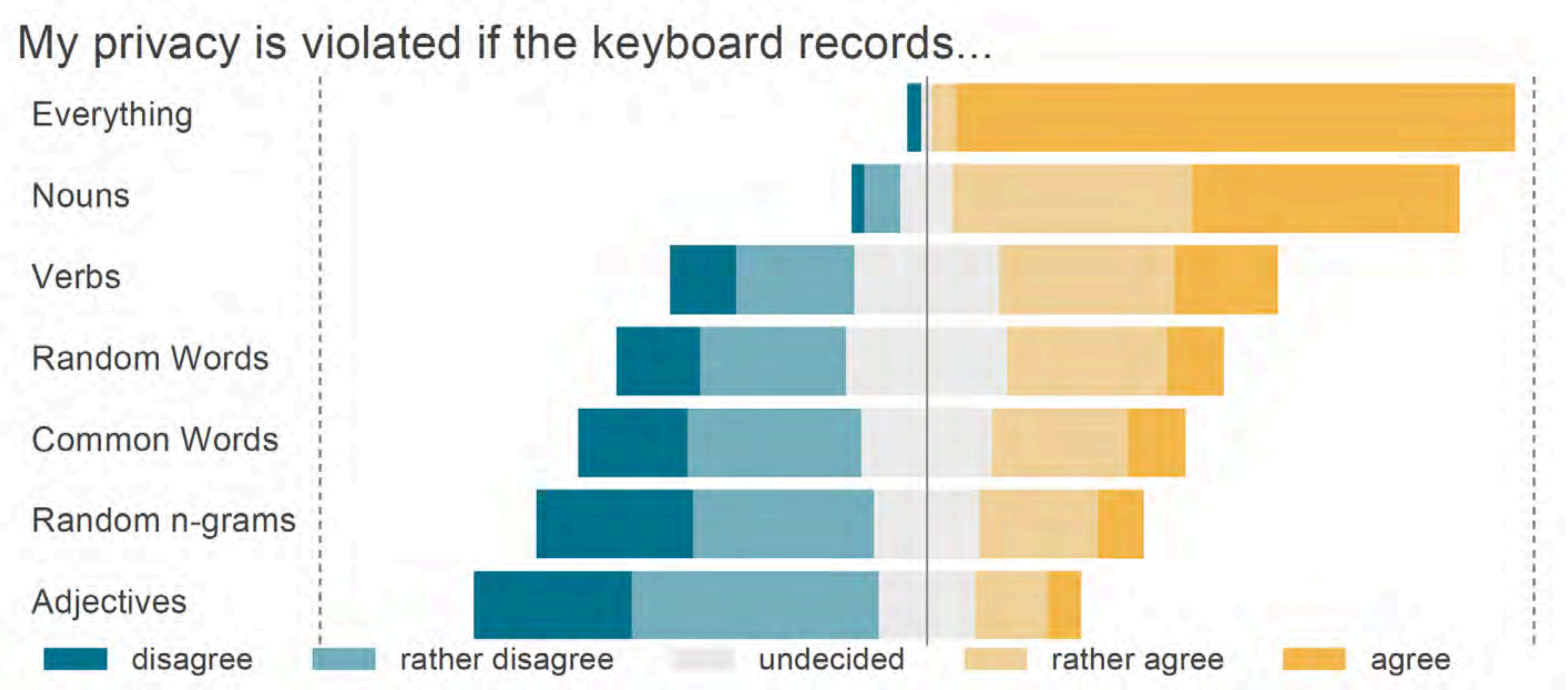


Category	Keystrokes count	Keystrokes % of data	Sugg. ratio (%)	AC ratio (%)
Messenger	767129	82.7	**1.6**	**0.9**
Browser	62210	6.7	0.9	0.5
Notes	13677	1.5	1.0	0.4
Email	13465	1.5	1.0	0.6
Social	13324	1.4	0.6	0.1
Shopping	12992	1.4	**1.6**	**0.9**
Communication	12394	1.3	**1.6**	0.4
Maps, Travel & Transport	5984	0.6	0.0	0.0
Search Box	5099	0.5	0	0
Productivity	4780	0.5	0.2	0
Education	4623	0.5	0.9	0
Calendar	3050	0.3	**1.6**	0
Media & Video	1513	0.2	0	0
Other	1315	0.1	0.1	0
Music & Audio	1042	0.1	0.1	0



Possible Logging Approaches

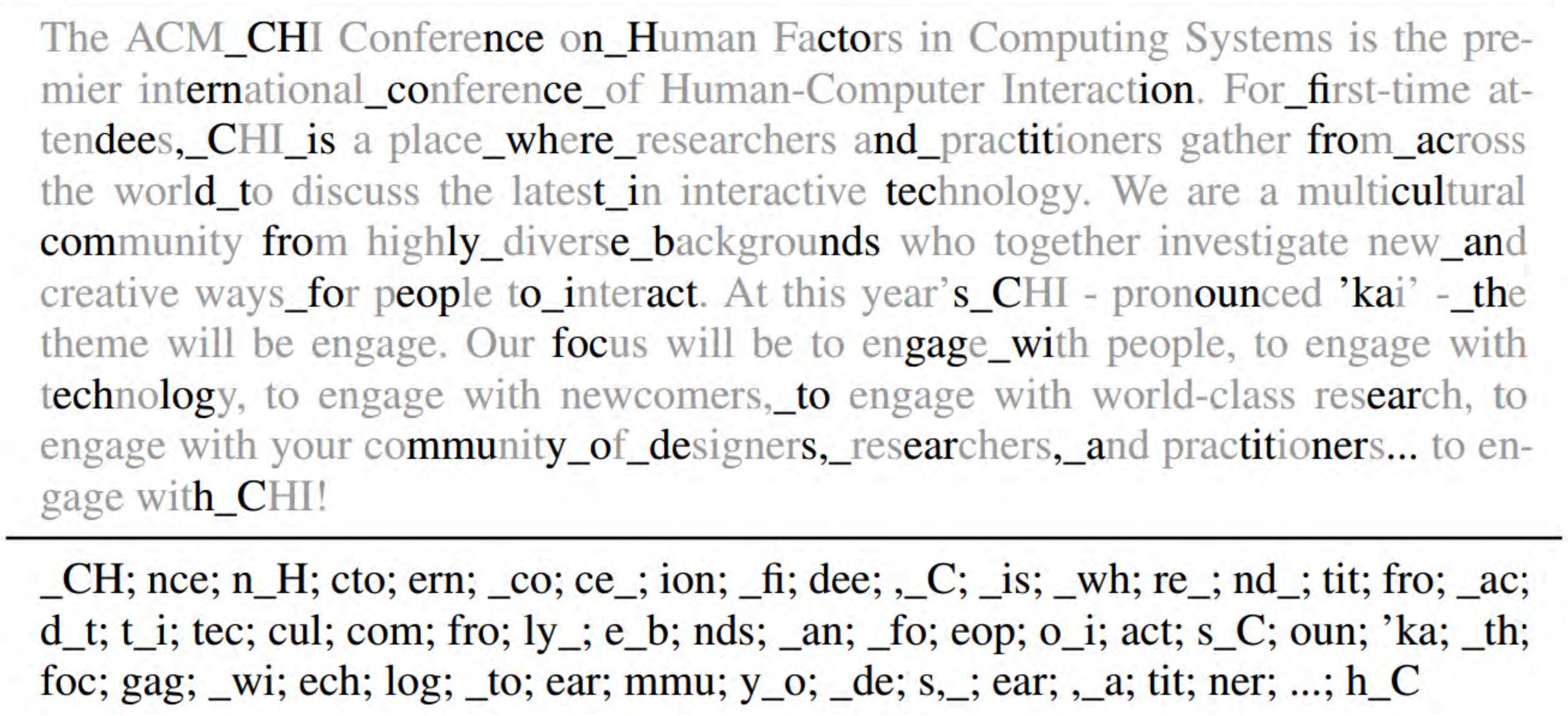
- everything (naive approach)
- single characters
- only nouns
- only verbs
- only adjectives
- random words
- most common 400 words
- random n-grams



FILTERING

RANDOM N-GRAM FILTER

- Log text-revealing data only for some touches
- n-gram with chance p
- minimum 1 character gap



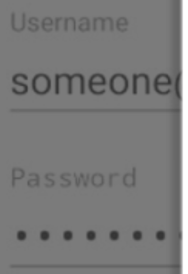
The ACM_CHI Conference on_Human Factors in Computing Systems is the premier international_conference_of Human-Computer Interaction. For_first-time attendees,_CHI_is a place_where_researchers and_practitioners gather from_across the world_to discuss the latest_in interactive technology. We are a multicultural community from highly_diverse_backgrounds who together investigate new_and creative ways_for people to_interact. At this year's_CHI - pronounced 'kai' -_the theme will be engage. Our focus will be to engage_with people, to engage with technology, to engage with newcomers,_to engage with world-class research, to engage with your community_of_designers,_researchers,_and practitioners... to engage with_CHI!

_CH; nce; n_H; cto; ern; _co; ce_; ion; _fi; dee; ,_C; _is; _wh; re_; nd_; tit; fro; _ac; d_t; t_i; tec; cul; com; fro; ly_; e_b; nds; _an; _fo; eop; o_i; act; s_C; oun; 'ka; _th; foc; gag; _wi; ech; log; _to; ear; mmu; y_o; _de; s,_; ear; ,_a; tit; ner; ...; h_C

no pa

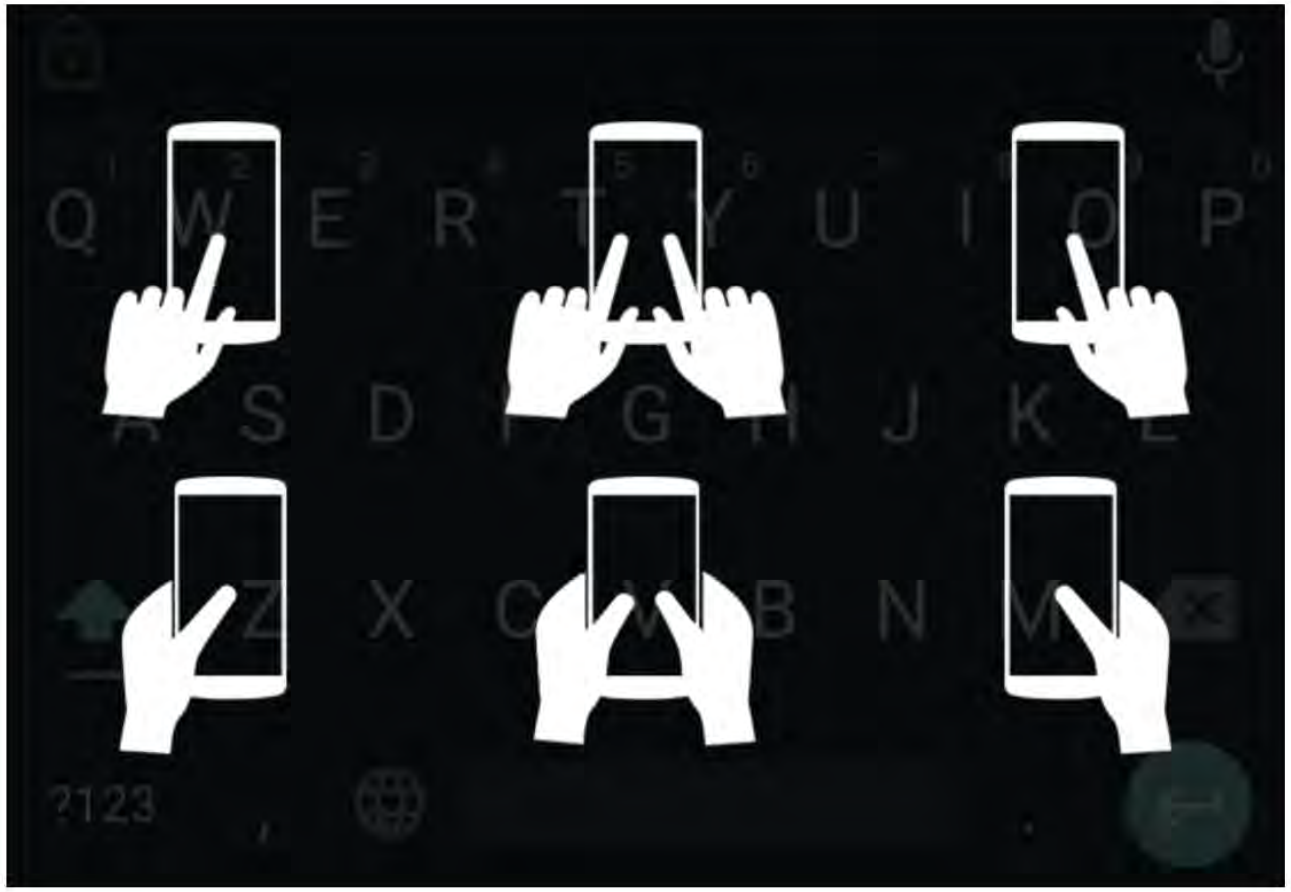
ntrol

de” button



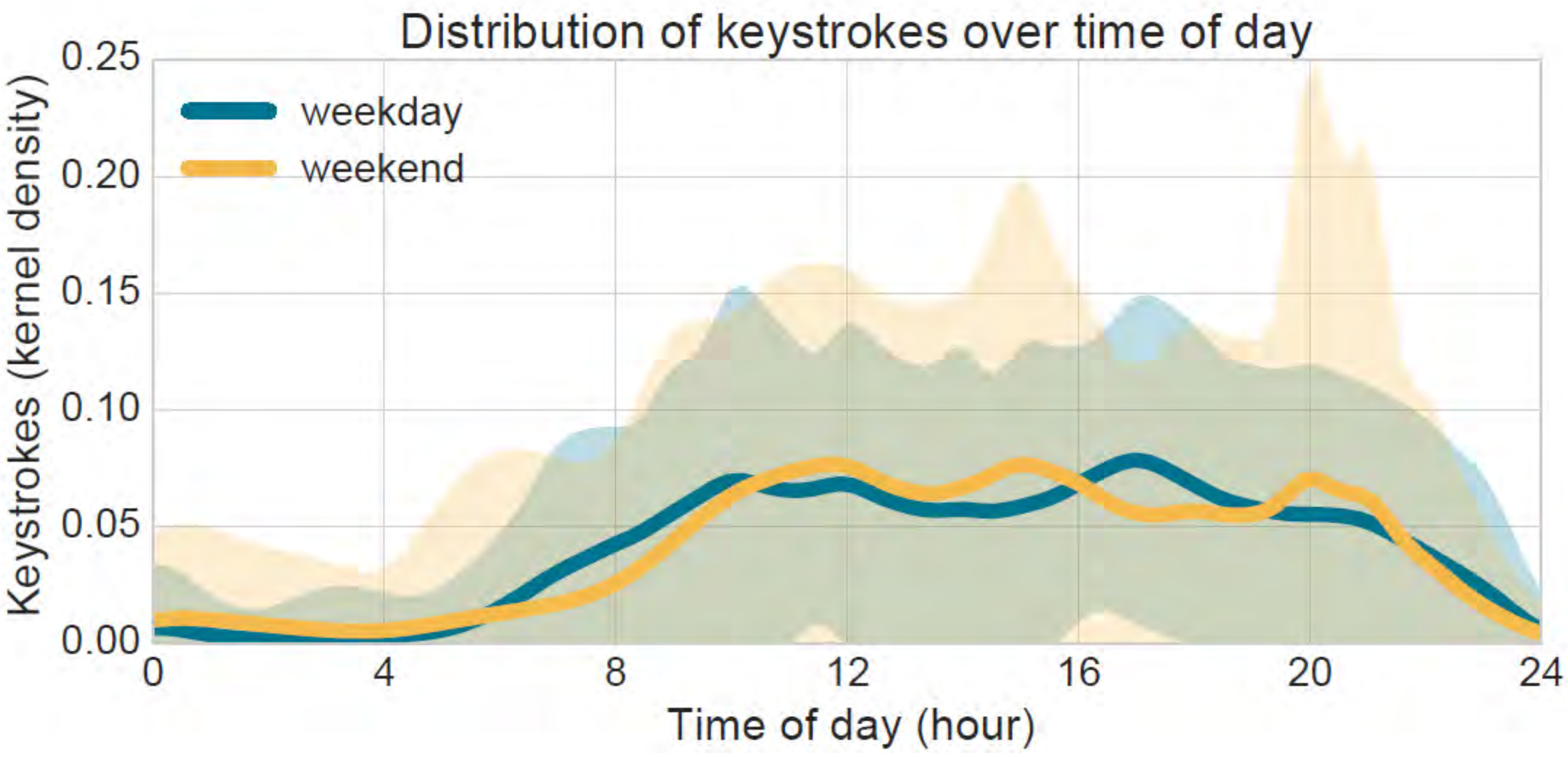
EXPERIENCE SAMPLING INTEGRATION

- Keyboard overlay
- When opening
- Limited frequency
- Select posture



DATA SET (N=30, 3 WEEKS)

- 5.9 million keyboard events
- 28 million sensor readings
- 1 million keystrokes (200,000 non-redacted)
- 7000 experience sampling answers



Session Objectives

- **Understanding Threats to Personal Data**
- **Protecting Personal Data**
- Publishing Privacy / Security Research

Threats to Personal Data

- **Data types:**
  - Gaze
  - EMG
  - EEG
  - Cardio-vascular Responses
  - Bio Markers
- **Questions:**
  - What are possible threats that result from access to the data or information derived from the data?
  - How can the threats be mitigated?

The World Café Method

- Five stations at which a particular topic is discussed for 5 minutes
- Host to introduce the topic of the station
- Host and group members share insights and results from prior discussions (5 rounds)
- Presentation of results to all participants

World Café — Threats to Personal Data

- **Data types (hosts):**
  - Gaze (Jesse) — 1
  - EMG (Jakob) — 2
  - EEG (Thomas) — 3
  - Cardio-vascular Responses (Jasmin) — 4
  - Bio Markers (Luke) — 5
- **Questions:**
  - What are possible threats that result from access to the data or information derived from the data? (Rounds 1—3)
  - How can the threats be mitigated? (Rounds 4—5)

Session Objectives

- Understanding Threats to Personal Data
- Protecting Personal Data
- **Publishing Privacy / Security Research**

CHI — Human Factors in Computing Systems

- https://chi2021.acm.org/
- ACM Flagship Venue on Human-Computer Interaction
- Submission Deadline: mid September (17.09.2020)
- Conference: May
- Subcommittee: Privacy, Security
- Next year in Yokohama

CHI 2021 May 8-13, 2021 Yokohama, Japan

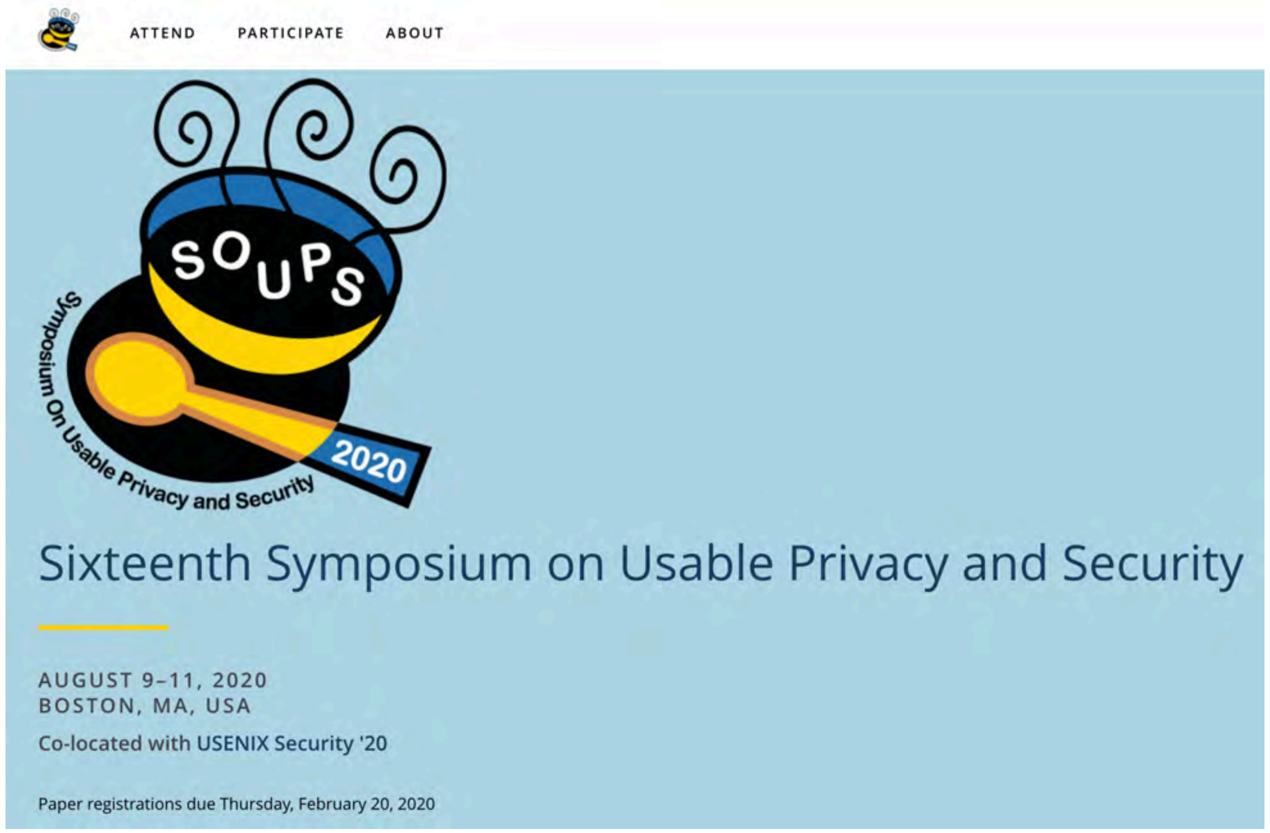
CHI 2021

May 8-13, 2021 Yokohama, Japan

Deadlines
Thursday Sep. 10, 2020
Papers : Title, abstract, authors, subcommittee choice, and all other metadata

SOUPS — Symposium on Usable Privacy and Security

- https://www.usenix.org/conference/soups2020
- Premier Venue for Usable Privacy and Security Research
- Deadline: end February (26.02.2020)
- Symposium Date: mid August
- Topics:
  - Novel security and privacy mechanisms
  - Empirical studies
  - Systematization of knowledge papers
- This year in Boston



Sixteenth Symposium on Usable Privacy and Security

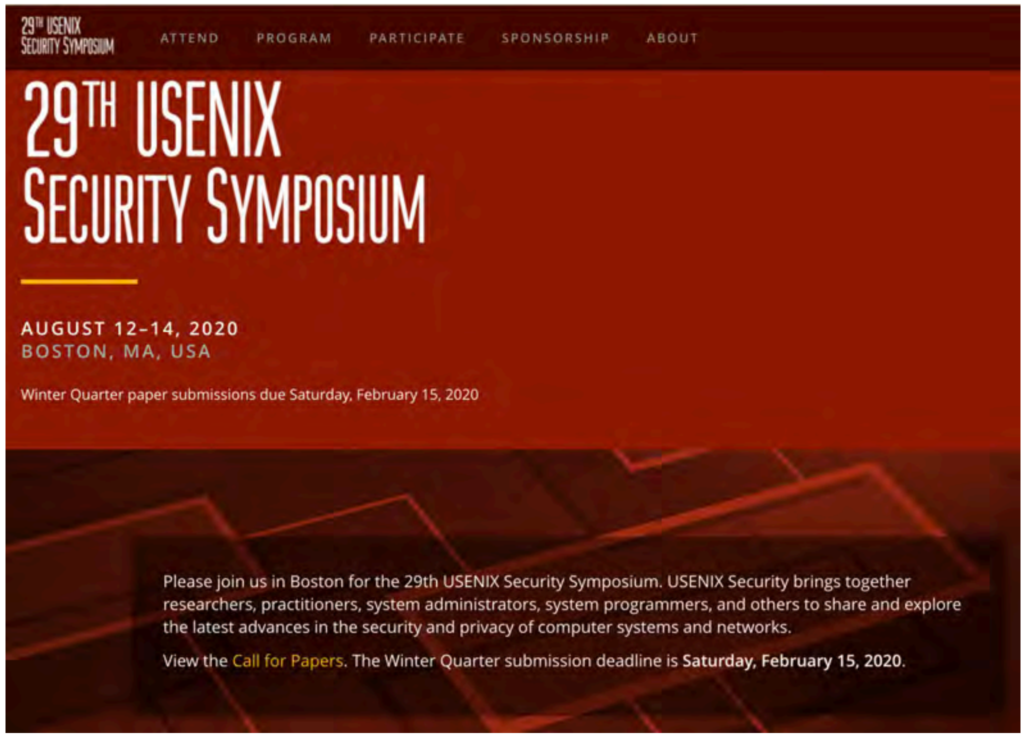
AUGUST 9–11, 2020
BOSTON, MA, USA

Co-located with USENIX Security '20

Paper registrations due Thursday, February 20, 2020

USENIX Security

- https://www.usenix.org/conference/usenixsecurity20
- Four deadlines: 15th February/May/August/November
- Symposium Date: mid August
- Relevant Topics:
  - Usable Security and Privacy
  - Social issues and security
    - Research on computer security law and policy
    - Ethics of computer security research
    - Research on security education and training
- SOUPS as co-located event
- This year in Boston



29TH USENIX SECURITY SYMPOSIUM

AUGUST 12–14, 2020
BOSTON, MA, USA

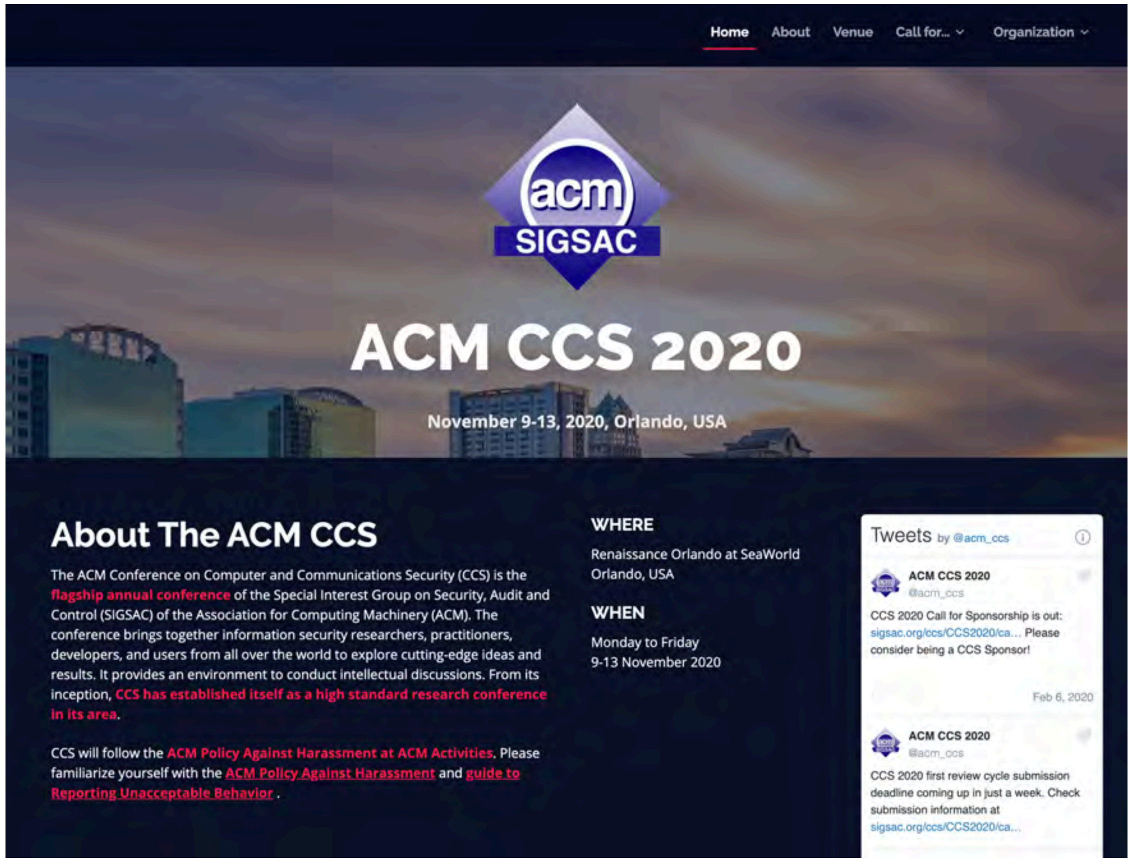
Winter Quarter paper submissions due Saturday, February 15, 2020

Please join us in Boston for the 29th USENIX Security Symposium. USENIX Security brings together researchers, practitioners, system administrators, system programmers, and others to share and explore the latest advances in the security and privacy of computer systems and networks.

View the Call for Papers. The Winter Quarter submission deadline is **Saturday, February 15, 2020**.

ACM CCS — Computer and Communication Security

- https://www.sigsac.org/ccs/CCS2020/
- ACM Flagship Conference on Security
- Submission Deadlines:
  January and May (with revision cycles)
- Conference Date: November
- Relevant Area:
  Usability and Measurement
  (Serge Egelman)
- This year in Orlando



ACM CCS 2020

November 9-13, 2020, Orlando, USA

About The ACM CCS

The ACM Conference on Computer and Communications Security (CCS) is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM). The conference brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results. It provides an environment to conduct intellectual discussions. From its inception, CCS has established itself as a high standard research conference in its area.

CCS will follow the ACM Policy Against Harassment at ACM Activities. Please familiarize yourself with the ACM Policy Against Harassment and guide to Reporting Unacceptable Behavior .

WHERE

Renaissance Orlando at SeaWorld
Orlando, USA

WHEN

Monday to Friday
9-13 November 2020

Tweets by @acm_ccs

ACM CCS 2020
@acm_ccs
CCS 2020 Call for Sponsorship is out: sigsac.org/ccs/CCS2020/ca... Please consider being a CCS Sponsor!
Feb 6, 2020

ACM CCS 2020
@acm_ccs
CCS 2020 first review cycle submission deadline coming up in just a week. Check submission information at sigsac.org/ccs/CCS2020/ca...

IEEE S&P — Symposium on Security and Privacy

- https://www.ieee-security.org/TC/SP2020/
- IEEE Flagship Conference on Security
- Submission Deadlines:
  every first of the month (2 month review cycle, with revisions)
- Symposium Date: May
- Relevant Area:
  Usable security and privacy
- Next Symposium in San Francisco

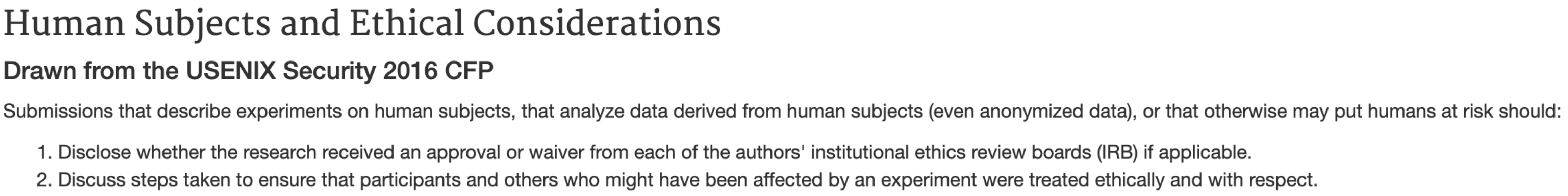
MAY 18-20, 2020 AT THE HYATT REGENCY, SAN FRANCISCO, CA

41st IEEE Symposium on Security and Privacy

Sponsored by the IEEE Computer Society Technical Committee on Security and Privacy in cooperation with the International Association for Cryptologic Research

Since 1980, the IEEE Symposium on Security and Privacy has been the premier forum for presenting developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field. The 2020 Symposium will mark the 41st annual meeting of this flagship conference.

The Symposium will be held on May 18-20, 2020, and the Security and Privacy Workshops will be held on May 21, 2020. Both events will be in San Francisco, CA at the Hyatt Regency.



Human Subjects and Ethical Considerations

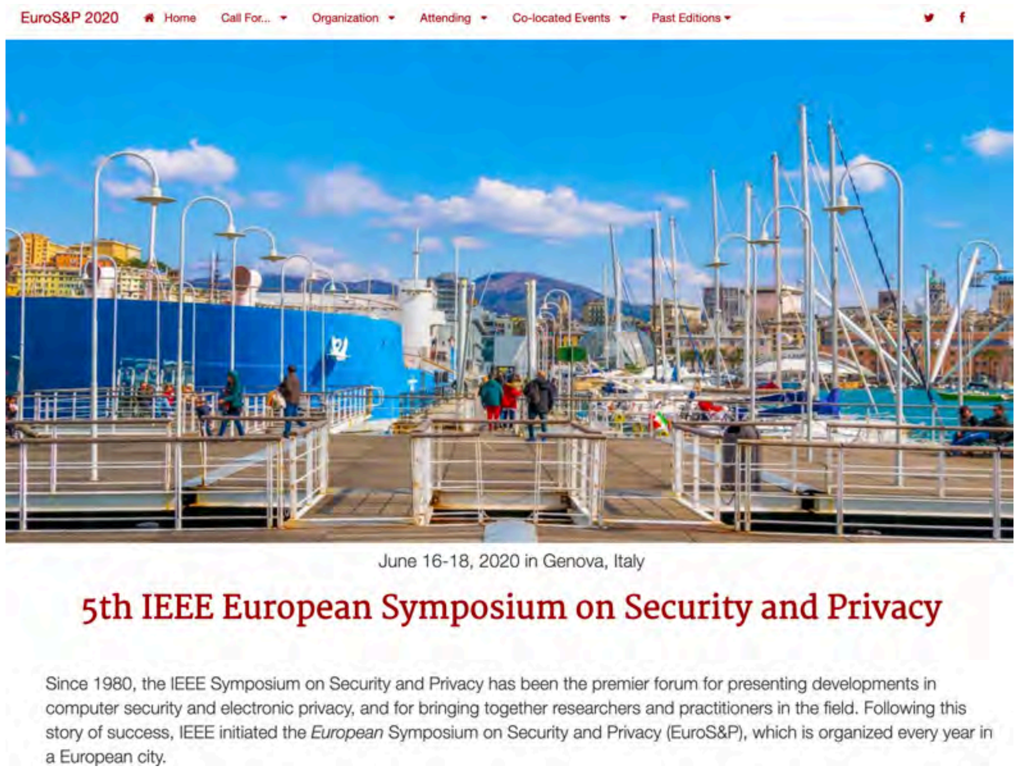
Drawn from the USENIX Security 2016 CFP

Submissions that describe experiments on human subjects, that analyze data derived from human subjects (even anonymized data), or that otherwise may put humans at risk should:

1. Disclose whether the research received an approval or waiver from each of the authors' institutional ethics review boards (IRB) if applicable.
2. Discuss steps taken to ensure that participants and others who might have been affected by an experiment were treated ethically and with respect.

IEEE Euro S&P — European Symposium on Security & Privacy

- https://www.ieee-security.org/TC/SP2020/
- Submission Deadline: November
- Conference Date: June
- Relevant Area: Human aspects of security and privacy
- Strong presence of Usable Security Researchers in the PC
- This year in Genova



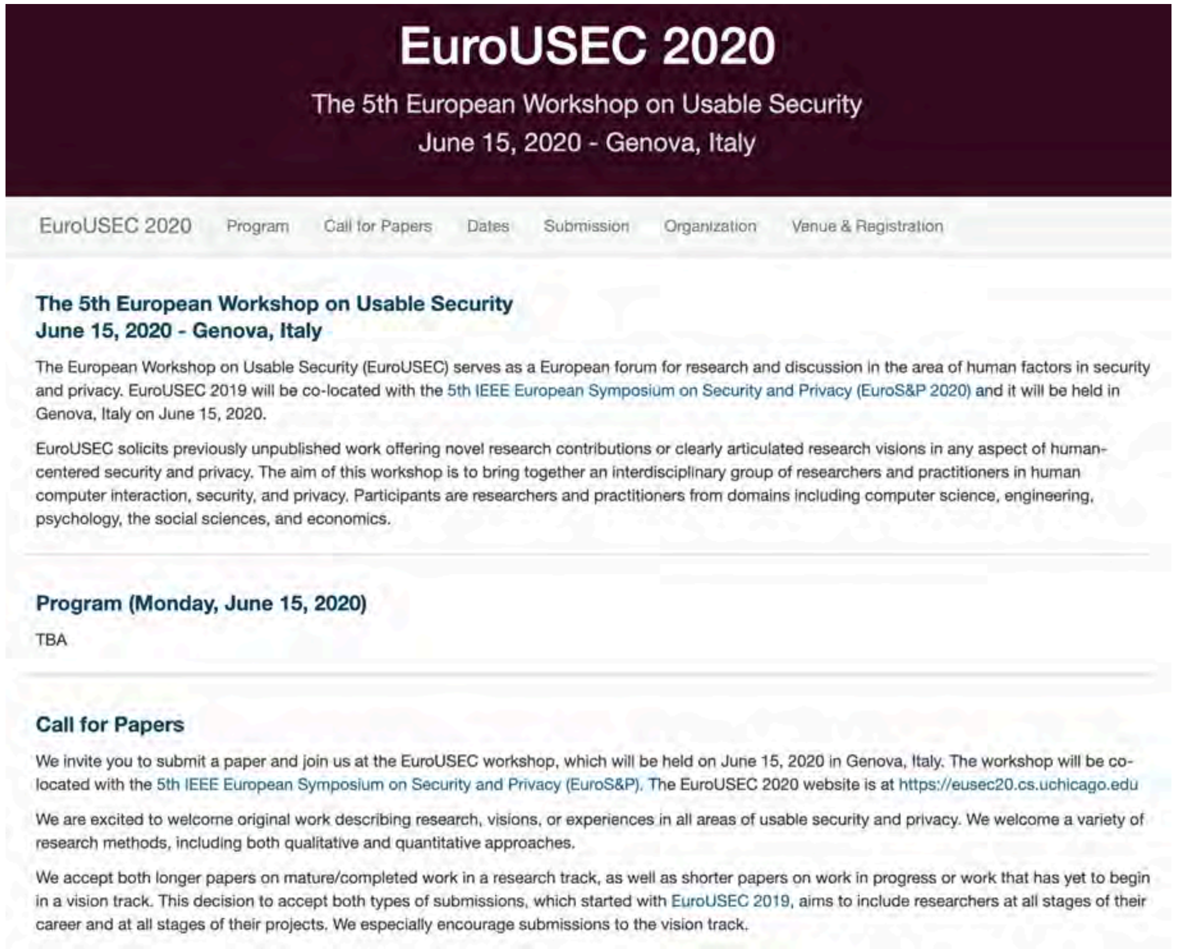
June 16-18, 2020 in Genova, Italy

5th IEEE European Symposium on Security and Privacy

Since 1980, the IEEE Symposium on Security and Privacy has been the premier forum for presenting developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field. Following this story of success, IEEE initiated the *European* Symposium on Security and Privacy (EuroS&P), which is organized every year in a European city.

EuroUSEC — Usable Security Workshop

- https://eusec20.cs.uchicago.edu/
- Submission Deadline: March (16.3.2020)
- Workshop Date: June (co-located with Euro S&P)
- Great venue to get to know the usable security community
- This year in Genova



EuroUSEC 2020

The 5th European Workshop on Usable Security
June 15, 2020 - Genova, Italy

The 5th European Workshop on Usable Security
June 15, 2020 - Genova, Italy

The European Workshop on Usable Security (EuroUSEC) serves as a European forum for research and discussion in the area of human factors in security and privacy. EuroUSEC 2019 will be co-located with the 5th IEEE European Symposium on Security and Privacy (EuroS&P 2020) and it will be held in Genova, Italy on June 15, 2020.

EuroUSEC solicits previously unpublished work offering novel research contributions or clearly articulated research visions in any aspect of human-centered security and privacy. The aim of this workshop is to bring together an interdisciplinary group of researchers and practitioners in human computer interaction, security, and privacy. Participants are researchers and practitioners from domains including computer science, engineering, psychology, the social sciences, and economics.

Program (Monday, June 15, 2020)

TBA

Call for Papers

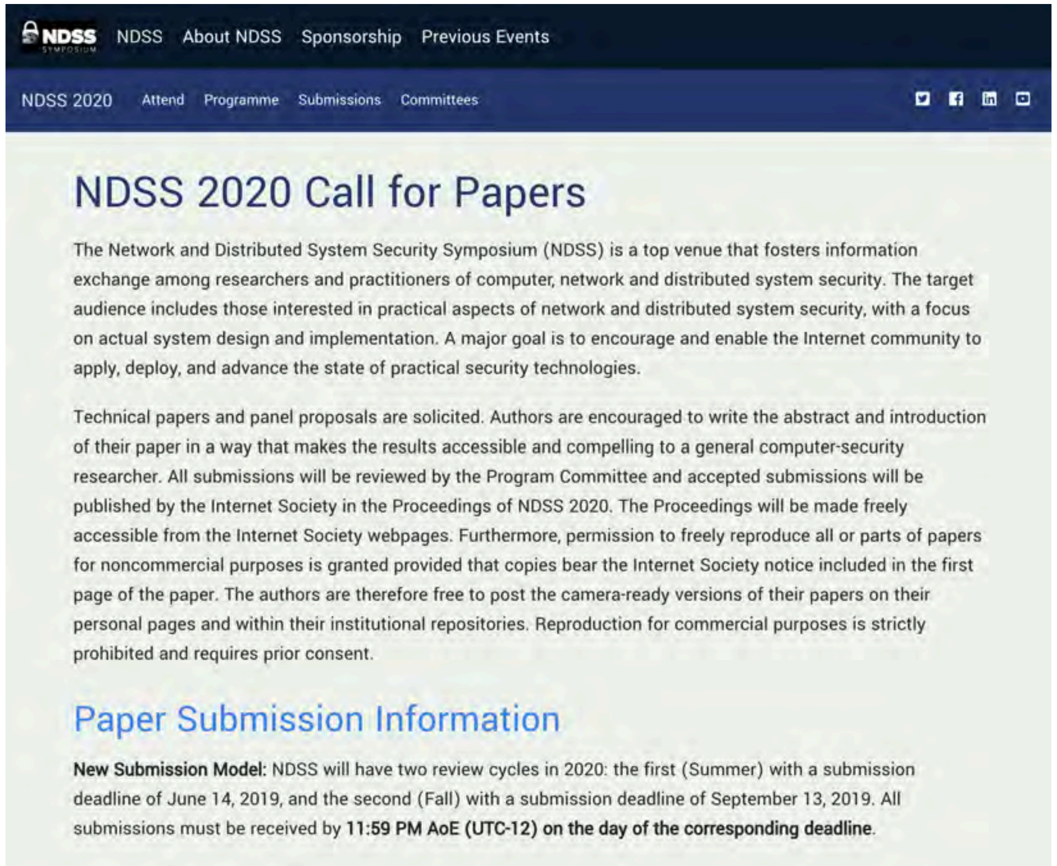
We invite you to submit a paper and join us at the EuroUSEC workshop, which will be held on June 15, 2020 in Genova, Italy. The workshop will be co-located with the 5th IEEE European Symposium on Security and Privacy (EuroS&P). The EuroUSEC 2020 website is at https://eusec20.cs.uchicago.edu

We are excited to welcome original work describing research, visions, or experiences in all areas of usable security and privacy. We welcome a variety of research methods, including both qualitative and quantitative approaches.

We accept both longer papers on mature/completed work in a research track, as well as shorter papers on work in progress or work that has yet to begin in a vision track. This decision to accept both types of submissions, which started with EuroUSEC 2019, aims to include researchers at all stages of their career and at all stages of their projects. We especially encourage submissions to the vision track.

NDSS — Network and Distributed System Security Symposium

- https://www.ndss-symposium.org/ndss2020/call-for-papers/
- Submission Deadlines: May and August
- Symposium Date: February
- Relevant Area: Usable security and privacy
- Location this year: San Diego



NDSS 2020 Call for Papers

The Network and Distributed System Security Symposium (NDSS) is a top venue that fosters information exchange among researchers and practitioners of computer, network and distributed system security. The target audience includes those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation. A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of practical security technologies.

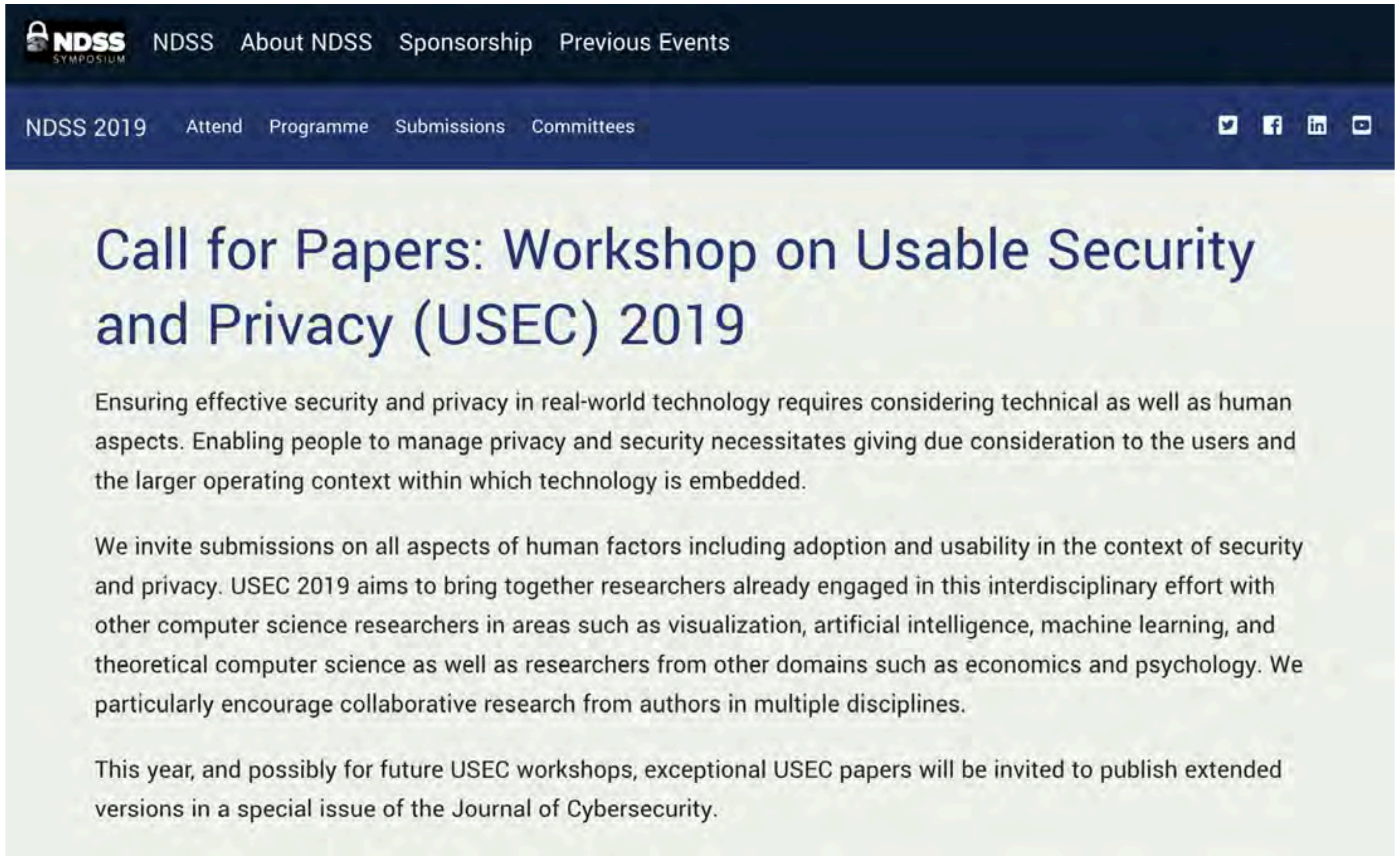
Technical papers and panel proposals are solicited. Authors are encouraged to write the abstract and introduction of their paper in a way that makes the results accessible and compelling to a general computer-security researcher. All submissions will be reviewed by the Program Committee and accepted submissions will be published by the Internet Society in the Proceedings of NDSS 2020. The Proceedings will be made freely accessible from the Internet Society webpages. Furthermore, permission to freely reproduce all or parts of papers for noncommercial purposes is granted provided that copies bear the Internet Society notice included in the first page of the paper. The authors are therefore free to post the camera-ready versions of their papers on their personal pages and within their institutional repositories. Reproduction for commercial purposes is strictly prohibited and requires prior consent.

Paper Submission Information

New Submission Model: NDSS will have two review cycles in 2020: the first (Summer) with a submission deadline of June 14, 2019, and the second (Fall) with a submission deadline of September 13, 2019. All submissions must be received by **11:59 PM AoE (UTC-12) on the day of the corresponding deadline**.

USEC — Usable Security Workshop

- http://www.usablesecurity.net/USEC/
- Submission Deadline: November
- Workshop Date: February (co-located with NDSS)
- Location this year: San Diego
- Quite competitive



Call for Papers: Workshop on Usable Security and Privacy (USEC) 2019

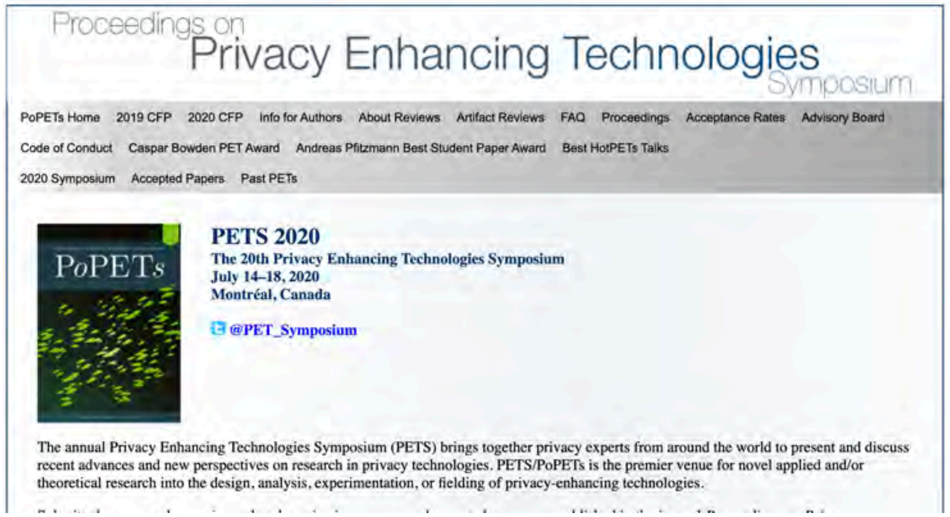
Ensuring effective security and privacy in real-world technology requires considering technical as well as human aspects. Enabling people to manage privacy and security necessitates giving due consideration to the users and the larger operating context within which technology is embedded.

We invite submissions on all aspects of human factors including adoption and usability in the context of security and privacy. USEC 2019 aims to bring together researchers already engaged in this interdisciplinary effort with other computer science researchers in areas such as visualization, artificial intelligence, machine learning, and theoretical computer science as well as researchers from other domains such as economics and psychology. We particularly encourage collaborative research from authors in multiple disciplines.

This year, and possibly for future USEC workshops, exceptional USEC papers will be invited to publish extended versions in a special issue of the Journal of Cybersecurity.

PETS — Privacy Enhancing Technologies Symposium

- https://petsymposium.org/
- Deadlines:
  4 deadlines (last day of May / August / November / February)
- Follows a journal approach (similar to IMWUT)
- Symposium Date: July
- Topics:
  - Technical approaches to privacy
  - Human factors, usability, and user-centered design of privacy technologies
- This year: Montreal



Proceedings on Privacy Enhancing Technologies Symposium

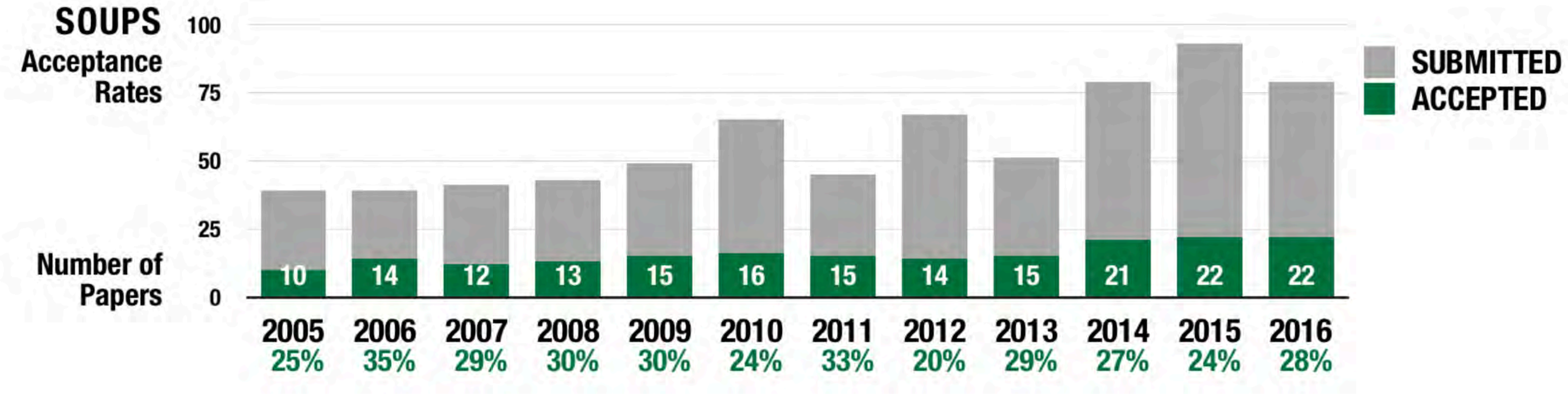
PETS 2020
The 20th Privacy Enhancing Technologies Symposium
July 14–18, 2020
Montréal, Canada

@PET_Symposium

The annual Privacy Enhancing Technologies Symposium (PETS) brings together privacy experts from around the world to present and discuss recent advances and new perspectives on research in privacy technologies. PETS/PoPETs is the premier venue for novel applied and/or theoretical research into the design, analysis, experimentation, or fielding of privacy-enhancing technologies.

Conference Rankings

- http://faculty.cs.tamu.edu/guofei/sec_conf_stat.htm
- https://scholar.google.es/citations?view_op=top_venues&hl=en&vq=eng_computersecuritycryptography



Describe your Threat Model

Example

We assume an attacker that is already in possession of the user's password pattern (the shape). That is, the first security barrier has already been breached. How the attacker got this information is of no concern for this work. In addition, the attacker managed to retrieve the mobile device (e.g. using pickpocketing) and wants to gain access to valuable information on it. For this, as for other commercial systems, the attacker has three tries until the device will be blocked.

The approach presented in this work relies on implicit authentication and has been designed to provide security against such an attack. Thus, even after losing the mobile device and the authentication credential, the proposed system should still provide the required security.

How to write research papers in security and privacy

- Evaluation **subject** (Model, Protocol, Process, Tool, Theory)
- Evaluation **attribute** (e.g., usability of evaluation subject; usually several ones)
- Evaluation **approach**
  - Empirical
    - Participants (simulation, humans, system)
    - Type of study (observational, interventional)
    - Type of data (self-reported, observed, automated)
    - Number of study conditions and subjects
    - Comparison (historical, generated data, none)
  - Proof
  - Discussion / Argumentation

Security Literature Review Paper Review Rubric

Version 2.0

Morgan Burcham and Jeffrey Carver*

***Department of Computer Science**
University of Alabama
carver@cs.ua.edu

August 30, 2016

Abstract

This document contains the definition of a rubric used to classify security research papers. First we define five dimensions used to classify each paper: a) Evaluation Subject - what is being analyzed in the paper, b) Evaluation Subject Source - whether the Evaluation Subject was first introduced in the current paper or elsewhere and by whom, c) Evaluation Attribute - what aspect of the Evaluation Subject is being studied, and d) Evaluation Approach - how the authors evaluated the properties of the Evaluation Subject. For each Evaluation Approach (Empirical, Proof, and Discussion), we define a *Completeness Rubric* containing a series of questions a reviewer can answer to help determine the completeness of the report from a Science of Security perspective.

1. Introduction

Our work has focused on the use of this rubric in conjunction with security papers to determine the completeness of the information provided in the literature. In order for the security research community to move forward, such literature should contain enough details to aid in scientific tasks such as replication, meta-analysis, and theory building. In the review process, we used the Nvivo data analysis software. We created an Nvivo template for all reviewers. In this template, we created nodes for every item in the rubric. Reviewers would import the security papers into the Nvivo template file. As the reviewers read the papers, they would answer all rubric items by marking the appropriate text and selecting the correct node corresponding to each rubric item.

2. Paper Characterization

This section defines the five dimensions used to characterize each paper. Note that the relationship between *evaluation subject* and *evaluation approach* is many-to-many. That is, there could be multiple *evaluation subjects* in each paper and each *evaluation subject* could have multiple *evaluation approaches*. In the case of *multiple evaluation subjects*, the reviewer will simply mark all subjects that apply and select the corresponding *evaluation approaches* for each subject. In the case of *multiple instances* of the *same evaluation subject*, the reviewer will make a note to that effect on the paper. The reviewer will classify the *evaluation approach* for each instance of the subject. In the case of *multiple instances* of the *same evaluation approach*, the reviewer should make a note to that effect on the paper. For each *rubric answer for the evaluation approach*, the reviewer will select the appropriate answer in each instance. For example, if a paper uses multiple Proofs to evaluate a Protocol, the reviewer will mark the individual

http://carver.cs.ua.edu/Studies/SecurityReview/Rubric.html

Some more Information on Publishing Security Research

- https://petsymposium.org/reviews.php
- Morgan Burcham, Mahran Al-Zyoud, Jeffrey C. Carver, Mohammed Alsaleh, Hongying Du, Fida Gi- lani, Jun Jiang, Akond Rahman, Özgür Kafalı, Ehab Al-Shaer, and Laurie Williams. Characterizing scientific reporting in security literature: An analysis of ACM CCS and IEEE S&P papers. In Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp, HoTSoS, pages 13–23, New York, NY, USA, 2017. ACM.
- Jeffrey C. Carver, Morgan Burcham, Sedef Akinli Kocak, Ayse Bener, Michael Felderer, Matthias Gander, Jason King, Jouni Markkula, Markku Oivo, Clemens Sauerwein, and Laurie Williams. Establishing a baseline for measuring advancement in the science of security: An analysis of the 2015 IEEE Security & Privacy proceedings. In Proceedings of the Symposium and Bootcamp on the Science of Security, HotSos '16, pages 38–51, New York, NY, USA, 2016. ACM.