Security & Privacy for Existing and Emerging Technologies

Franziska (Franzi) Roesner
Assistant Professor
University of Washington
franzi@cs.washington.edu
What security & privacy issues are we facing today?

This talk: secure communication for journalists (etc.)

What security & privacy issues will arise in the future, with emerging technologies?

This talk: security & privacy for augmented reality
Part 1: Computer Security for Journalists
Using encryption software was something I had long intended to do...

But [PGP] is complicated, especially for someone who had very little skill in programming and computers, like me...

It never became pressing enough for me to stop other things and focus on it.
Journalists can benefit from security tools...
… but don’t often use these tools in practice.
Goals: (1) Study the practices, constraints, and needs of journalists & lawyers, to guide (2) the design of new technical security/privacy tools.


Our Process: Collaboration between experts in the journalism, usability, and computer security communities.

Part 1: Interviews with individual journalists
Part 2: Interviews with organizational stakeholders (editors, IT staff)
Part 3: Design and prototype encrypted email tool
Part 4: Usability study + interviews with journalists and lawyers

[USENIX Sec '15] [PETS '16] [EuroS&P '17] [EuroS&P '17]
Goal: Study individual journalists to understand their general practices and constraints, and their computer security needs, concerns, and threat models.
Choice of communication technology is often **driven by the source** – and many sources are not tech-savvy.

[The source] probably understand[s] the threat model they’re under better than I would. **People’s first impression is that they would go by what the source feels comfortable doing. As opposed to stepping in and being paternalistic about it.**
Long-term sources are common, with trust built over time; **truly anonymous sources are rare.**

If I don’t know who they are and can’t check their background, **I’m not going to use the information they give.**
Tool Design and Prototype
Usable Encrypted Email?

Motivation: Journalists frequently use email with sources. Unfortunately, *usable encrypted email is a longstanding problem.*

Nikita Borisov @nikitab · Aug 12

"Why Johnny Can't Encrypt" wins the USENIX Security test of time award since Johnny still can't encrypt. #sec15 (congratulations Alma&Doug!)
Towards (More) Usable Encrypted Email

What’s different now?

Informally authenticating your contacts’ social media accounts is common.

**Keybase** leverages this: a public key directory with verifiable links to social media profiles.

https://keybase.io
Our Tool: Confidante

Compose Email

To:
Alice Johnson <alice.johnson.campaign2016@gmail.com>

Keybase Username of Recipient:
alicejohnson2016

Alice Johnson
@alicej_2016

Meow meow meow meow meow meow meow meow meow meow meow meow meow meow meow meow meow meow

Encrypt and Send

[MEOW] Meow meow meow

john.doe.campaign2016@gmail.com

2:09 PM (2 minutes ago)

-----BEGIN PGP MESSAGE-----
Version: Keybase OpenPGP v2.0.54
Comment: https://keybase.io/crypto

wcBMA9jR3syKJ+zuUAFQf+HugNh87APbSVXyZHiEBkJr1zXrZx4H3OQmgdWmbwX1t
eySiKaFAu9AbXnHhImlDH0QHldrLeEGIPU0V2MHNfW6TjaUJcdQKRWGM1Doqbmkw
LyfbvKNeckQw3ik4limekAowv4f6Ss1ZMi8EgiLk6yIO80h87C1cy6b0u184BY

Meow,
Meow meow

Message was signed by:

John Doe
@jdoecampaign16
@johndoecampaign

Reply
Usability Study

**Goals:** (1) *Evaluate design decisions* we made in Confidante, and (2) more generally, learn more about the *encrypted email use cases and security needs* for journalists and lawyers.

Compare with Mailvelope.
Using Keybase for automated key management is promising: easy to use, many errors avoided.

The easiest PGP experience I ever had … I could see, in a way that you never could with PGP before, [sending] a one-page instructional thing on how to set this up, and trust that [sources] could actually do it themselves.

It’s no different to use than just using Gmail directly.

If something like this caught on, I could see putting my Keybase on my business card, or putting it in the signature line of my email.
Security concerns and usability challenges remain...

For example:
- Lack of trust ("too easy")
- Drawing suspicion
- No metadata protection
- Private key management

Because this is so easy… it really feels like there must be something wrong… [PGP is] a rite of passage.

[Sources]… would say “Is this actually going make it more likely for this to raise a red flag with my employer?”
Journalists and lawyers have **different operational constraints** and **different threat models**.

**Examples:** Sources vs. clients, Technical vs. legal protections

**Attorney-client privilege** is... sacrosanct.

If I have a document that’s a privileged document, *if somebody breaks into my office and looks at it, that doesn’t defeat the privilege*. But if I leave it out where somebody walking by can see it, that could. So you’d have to take **reasonable precautions**.
Conclusions (Part 1)

**Study and test with target user groups:** Our tools must be informed by their security needs and operational constraints.

**One size doesn’t fit all:** Different groups may need *entirely different tools*.

**Going forward:** Study these and other user groups and build/evaluate tools in those contexts.
Part 2: Security & Privacy for Augmented Reality
Augmented Reality (AR)

Our definition:
Computer-generated audio, visual, and/or haptic feedback is overlaid on the user’s perception of the real world in real-time.
Current and Emerging AR
Future AR Systems

Today vs. Tomorrow

One app at a time vs. Many concurrent apps
Few, trusted developers vs. Tons of third-party apps
App on by command vs. Background apps
2D annotations vs. 3D virtual objects
Synthetic annotations vs. Virtual object interactions

Security and privacy?
Challenges along two axes:
1. Single AR app, Multiple apps, Multiple systems
2. Input, Output, Data access

Identifying Security & Privacy Challenges

Challenges along two axes:
1. Single AR app, Multiple apps, Multiple systems
2. Input, Output, Data access

Input Privacy

Input Privacy

- Jana et al., USENIX Security ’13
- Roesner et al., CCS ’14
- Templeman et al., NDSS ’14
- Raval et al., MobiSys ’16
Output Security

Raw Input → Trusted Input Module → Filtered Input

AR App → Sensory Output
Hyper Reality (https://www.youtube.com/watch?v=YJg02ivYzSs)
A buggy or malicious app might…

- Obscure another app’s virtual content to hide or modify its meaning
- Obscure important real-world content, such as traffic signs or cars
- Disrupt the user physiologically, such as by startling them
Output Security

Raw Input

Trusted Input Module

Filtered Input

App Outputs

App Outputs

Trusted Output Module

Constrained Output

Output Security

- Lebeck et al., HotMobile '16
- Lebeck et al., IEEE S&P '17
Arya: AR Objects and Output Policies in Action

“Real world” Buggy or malicious apps

In-game purchases available!
Ad! Ad! Ad!
You’ve got mail!
Name: Alice  Role: CEO
"Real world" Buggy or malicious apps Policies enforced

OS enforces output policies
Emerging AR platforms raise new security and privacy risks, including **input privacy** and **output security**.

Our **Arya prototype** introduces an output security module to constrain output from buggy or malicious AR applications.

We must (and can still!) address security & privacy challenges in AR technologies **before these platforms become widespread and entrenched**.

[https://ar-sec.cs.washington.edu](https://ar-sec.cs.washington.edu)
Thanks to many collaborators!

Ada Lerner (UW)
Eric Zeng (UW)
Mitali Palekar (UW)
Kelly Caine (Clemson)
Susan McGregor (Columbia)
Kiron Lebeck (UW)
Kimberly Ruth (UW)
Yoshi Kohno (UW)
What security & privacy issues are we facing today?

What security & privacy issues will arise in the future, with emerging technologies?

- franzi@cs.washington.edu
- @franziroesner
- https://www.franziroesner.com