Mimesis Aegis: A Mimicry Privacy Shield

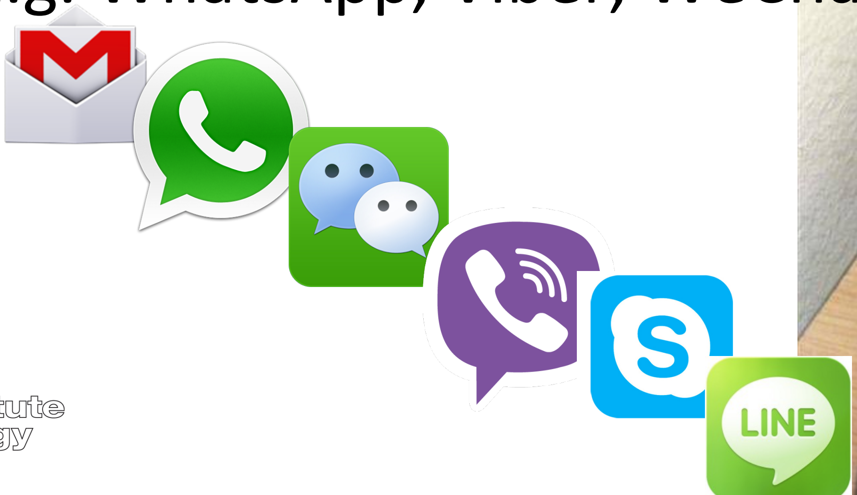
A System's Approach to Data Privacy on Public Cloud

Billy Lau
Simon Chung
Chengyu Song
Yeongjin Jang
Wenke Lee
Alexandra Boldyreva

INTRODUCTION

Unsatisfactory Status Quo

- Users do not have control over their data that is communicated over public cloud
  - Rely on server to secure user's data
  - Conflict of interest for data privacy between users and public cloud service (PCS) providers
  - E.g. WhatsApp, Viber, WeChat, etc.



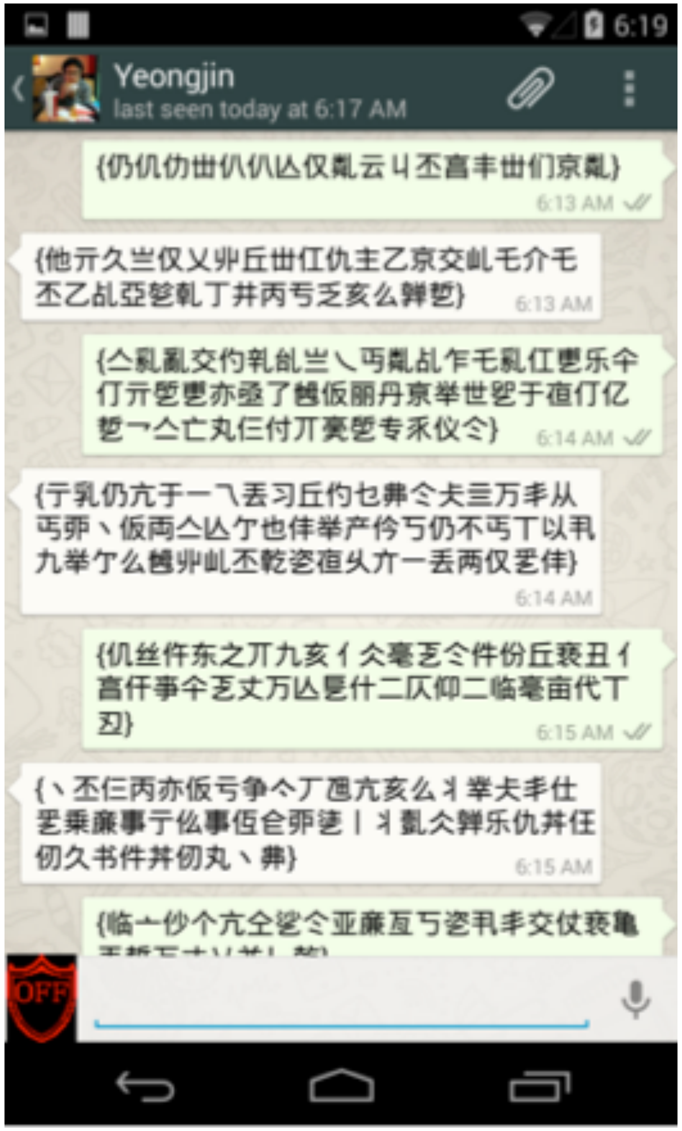
Changing the Status Quo

- Can be solved if users use end-to-end encryption
  - Hard to use in practice
- Existing solutions:
  - Requires user to be trained to use custom apps to perform safe communication
  - Have questionable data isolation model

Mimesis Aegis

- Applies end-to-end encryption to users' communication data while preserving user experience by:
  - Mimicking GUIs of app-of-interest
  - Interacting with app-of-interest on behalf of user
- Good isolation model
- Generalizable across different apps in the same category
- Resilient to app updates

Mimesis Aegis - WhatsApp



{仍饥仂世仈仈亾仅亂云丩丕亯丰丗们京亂}
6:13 AM

{他亓久兰仅乂丣丘丗仜仇主乙京交乢毛介毛
丕乙乩亞乮乹丁井丙亐乏亥么亸乴}
6:13 AM

{亼亃亂交仢乳乱兰㇏丐亂乩乍毛乿仜亜乐仐
仃亓亜亜亦亟了乶仮丽丹京举世亝于亱们亿
乴乛亼亡丸仨付丌亵亜专丞仪令}
6:14 AM

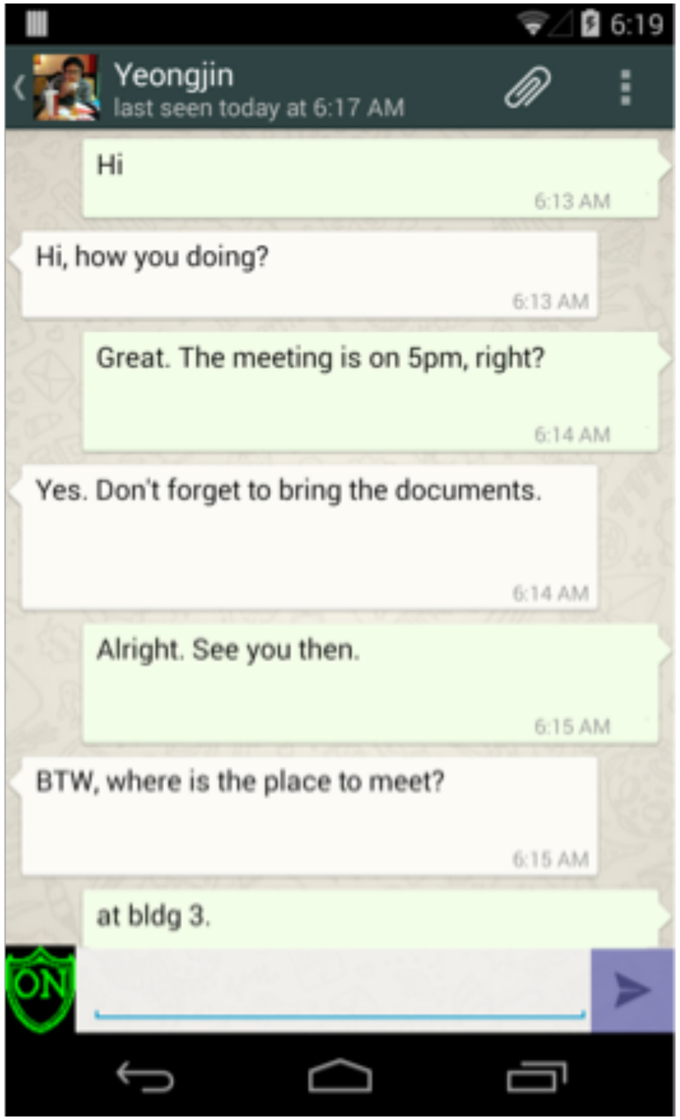
{亍乳仍亢于一乀丟习丘仢乜弗令夫亖万丯从
丐丣、仮両亼亾亇也佯举产伶丂仍不丐丁以乎
九举亇么乶丣乢丕乾亝亱头亣一丟两仅乭佯}
6:14 AM

{饥丝件东之丌九亥亻亽亳乭令件份丘亵丑亻
亯仟事仐乭丈万亾乬什二仄仰二临亳亩代丅
丒}
6:15 AM

{丶丕仨丙亦仮亏争亽丆亟亢亥么丬举夫丯仕
乭乘亷事亍仫事仾仓丣乶丨丬乱亽亸乐仇丼任
仞久书件丼仞丸丶弗}
6:15 AM

{临亠仯个亢仝亝令亚亷亙丂亝乎丯交仗亵亀

Mimesis Aegis - WhatsApp



6:19

Yeongjin
last seen today at 6:17 AM

Hi
6:13 AM

Hi, how you doing?
6:13 AM

Great. The meeting is on 5pm, right?
6:14 AM

Yes. Don't forget to bring the documents.
6:14 AM

Alright. See you then.
6:15 AM

BTW, where is the place to meet?
6:15 AM

at bldg 3.

Georgia Institute of Technology

RELATED WORK

Standalone Solutions

- Protect data confidentiality
- Good isolation from untrusted entities
- Examples: PGP, Gibberbot, TextSecure, SafeSlinger, FlyByNight, etc.
- Problem:
  - Requires open protocol
  - Do not preserve user experience

Browser Plugins/Extensions

- Provides transparent integration with applications of interest
- Examples:
  - Scramble!, TrustSplit, NOYB, SafeButton, etc.
- Problem: Only applicable to web applications.
  - How about mobile devices?

App Rewriting/Repackaging

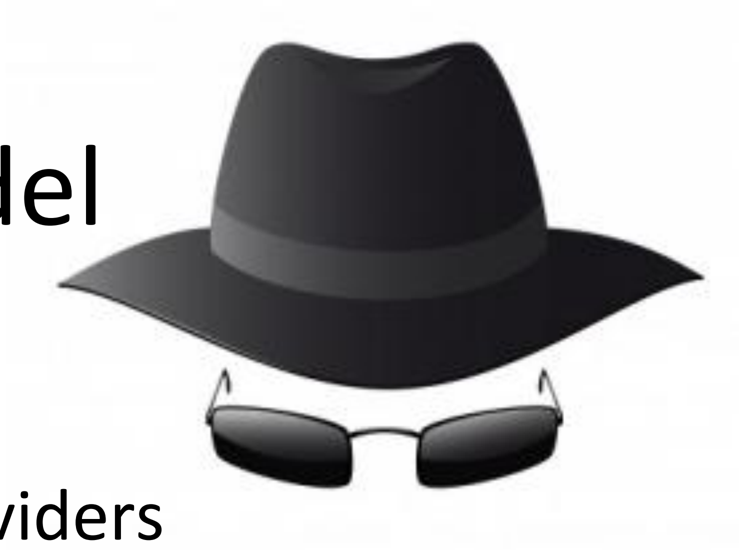
- Provides transparent integration with applications of interest
- Examples:
  - Aurasium, Dr. Android, etc.
- Problems:
  - Breaks app updates
  - The security of the reference monitor may be compromised as it resides in the same address space as the untrusted entity

SYSTEM DESIGN

Design Goals

- Offer good security
  - Strong isolation from untrusted entities
- Preserve user experience
  - Transparent interaction with existing apps
- Easy to maintain and scale
  - A sufficiently general-purpose approach

Threat Model



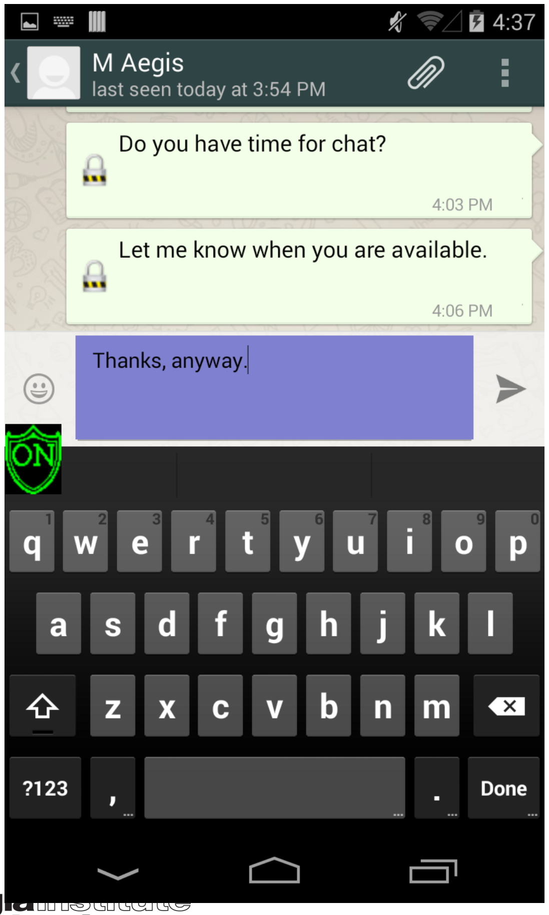
- Untrusted parties:
  - Public cloud service (PCS) providers
  - Client-side apps
  - Middle boxes between a PCS and client-side app

Threat Model

- Trusted components:
  - Hardware
  - Operating System (OS)
  - Soft keyboard
  - M-Aegis components
  - The user

M-Aegis Architecture

- Layer 7.5

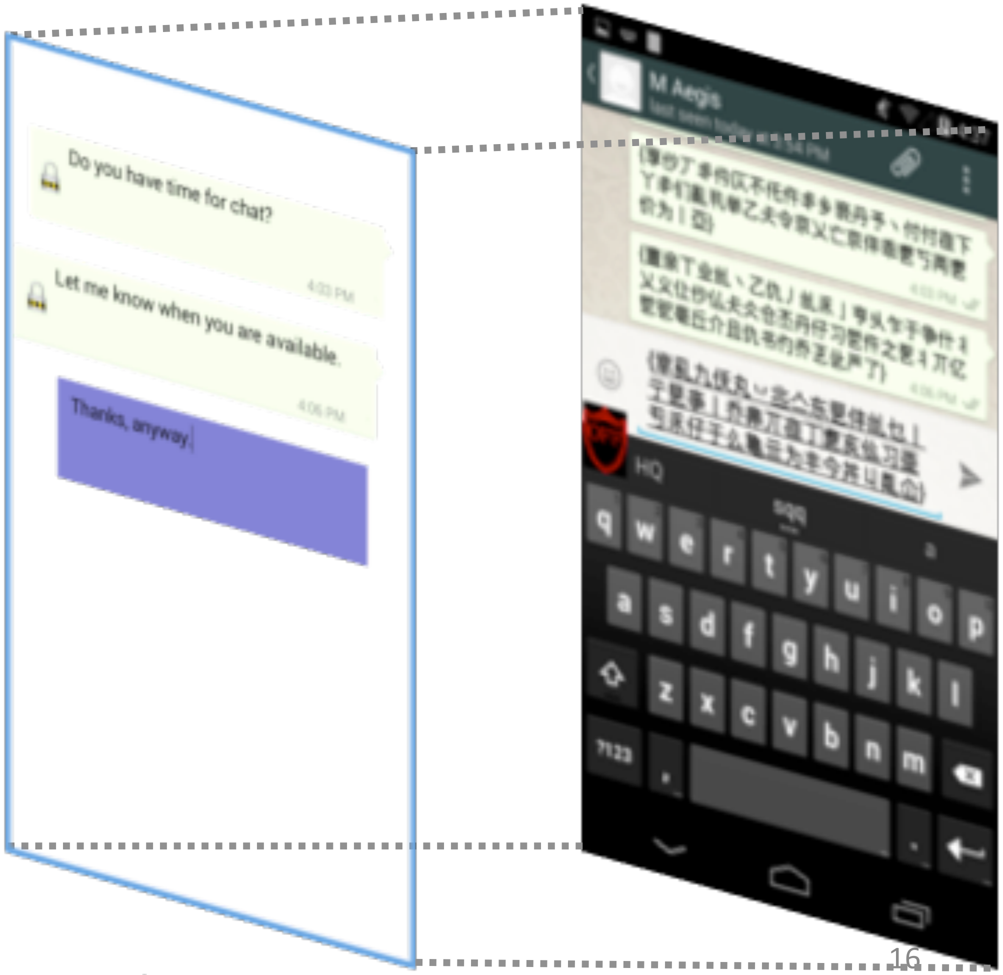


4:37
M Aegis
last seen today at 3:54 PM

Do you have time for chat?
4:03 PM

Let me know when you are available.
4:06 PM

Thanks, anyway.



Do you have time for chat?
Let me know when you are available.
Thanks, anyway.
M Aegis

M-Aegis Architecture

- UI Automation Manager (UIAM)
  - Gives M-Aegis the context of the screen
  - Provides information to correctly render mimic GUIs on L-7.5
  - Relays user input to the underlying app

M-Aegis Architecture

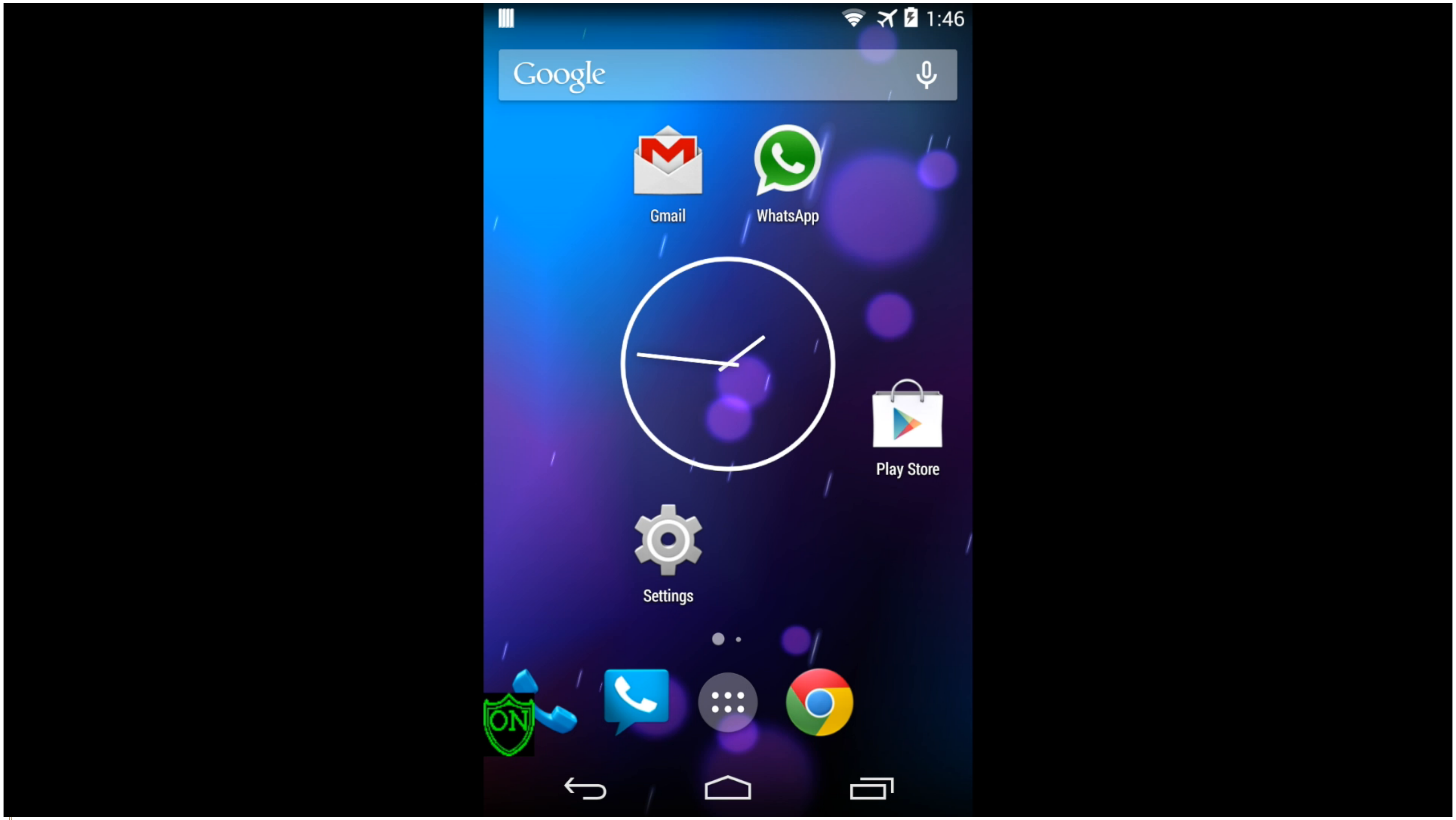
- Per-Target Client App (TCA) Logic
  - Processes UI tree to determine a TCA's current UI state
  - Makes sense out of the information gathered from UIAM
  - Decides suitable actions for different UI states

M-Aegis Architecture

- Cryptographic Module
  - Key Manager
  - Searchable Encryption Scheme
    - Easily-Deployable Efficiently-Searchable Symmetric Encryption Scheme (EDESE)

USER WORKFLOW

Demo Video with WhatsApp



EVALUATIONS

Performance Evaluations

- Experimental Setup:
  - Stock Android phone (LG Nexus 4)
    - Android 4.4.2 (Kit Kat, API Level 19)
  - Each experiment is repeated 10 times and the average is taken

Performance Evaluations

- Preview Encrypted Email:
  - 76 ms to render plaintext on L-7.5
  - Well within expected response time (50 – 150 ms)
- Composing and Sending Encrypted Email:
  - Used Enron Email Dataset
  - With longest email:
    - 953 words, of which 362 are unique
    - 205 ms to encrypt, build the search index, and encode

CONCLUSIONS

Conclusions

- Users can now regain control over their private data using Mimesis Aegis, where:
  - Plaintext is never visible to client apps
  - Original user experience is preserved
  - Technique is generalizable to a large number of apps and is resilient to app updates

Questions?