“We know what you did this summer” Android Banking Trojans Exposing Its Sins in The Cloud

Siegfried Rasthofer (TU Darmstadt / CASED)
Eric Bodden (TU Darmstadt / Fraunhofer SIT)
Carlos Castillo (Intel Security)
Alex Hinchliffe (Intel Security)

Siegfried Rasthofer

- 3rd year PhD-Student at TU Darmstadt
- Research interest in Static-/dynamic code analyses
- Found 2 AOSP exploits, various App security vulnerabilities

Prof. Dr. Eric Bodden

- Professor at TU Darmstadt
- Research interest in Static-/dynamic code analyses
- Heading the Secure Software Engineering Group at Fraunhofer SIT and Technische Universität Darmstadt

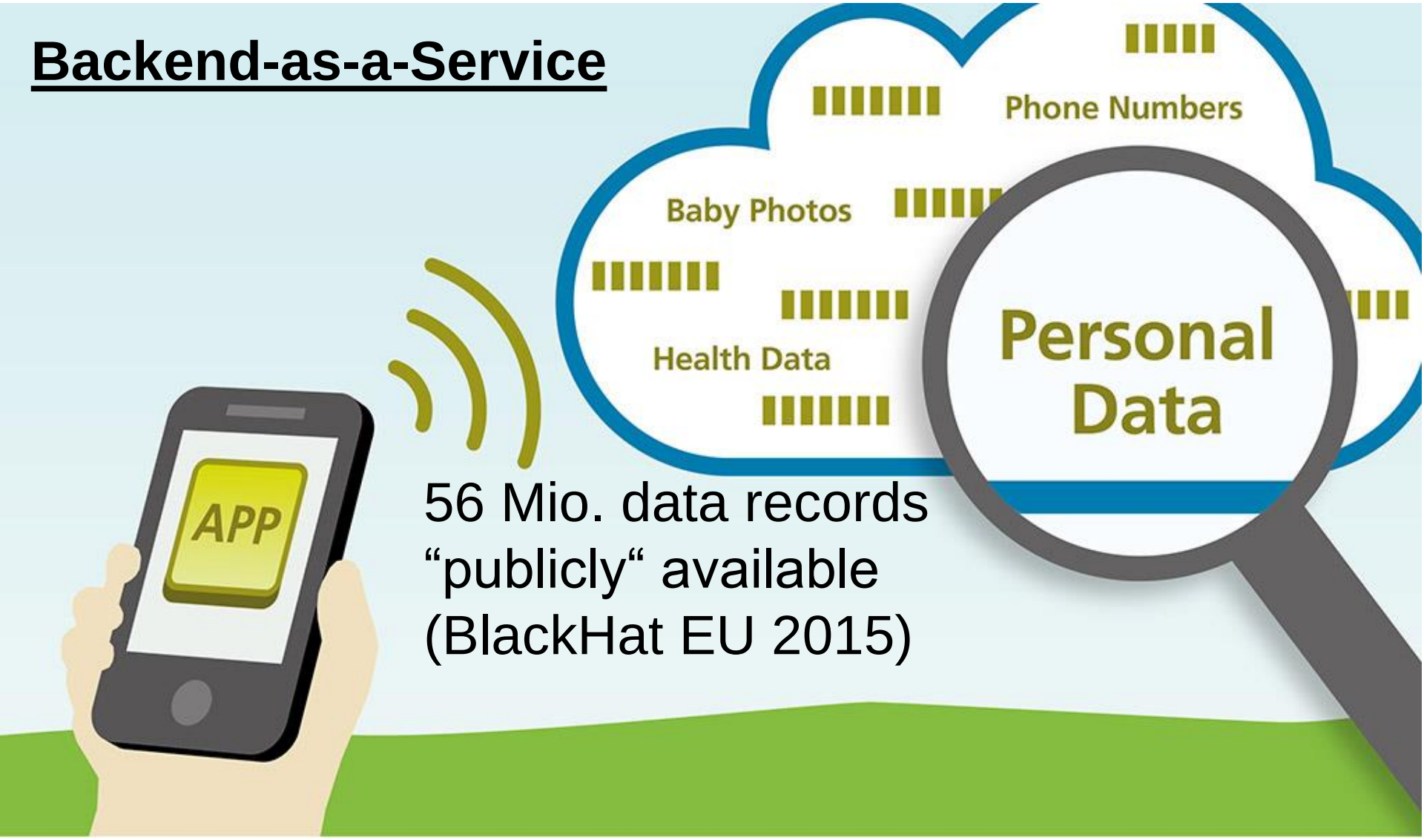
Carlos Castillo

- Mobile Security Researcher at Intel Security.
- Hacking Exposed 7 co-author (Hacking Android).
- ESET Latin America's Best Antivirus Research winner 2009.

Alex Hinchliffe

- Mobile Security Research Manager at Intel Security
- Co-developer of cloud based Anti-Malware technology, Artemis
- Project partner of MobSec, S^2Lab, Royal Holloway University, London

Backend-as-a-Service



56 Mio. data records “publicly“ available (BlackHat EU 2015)

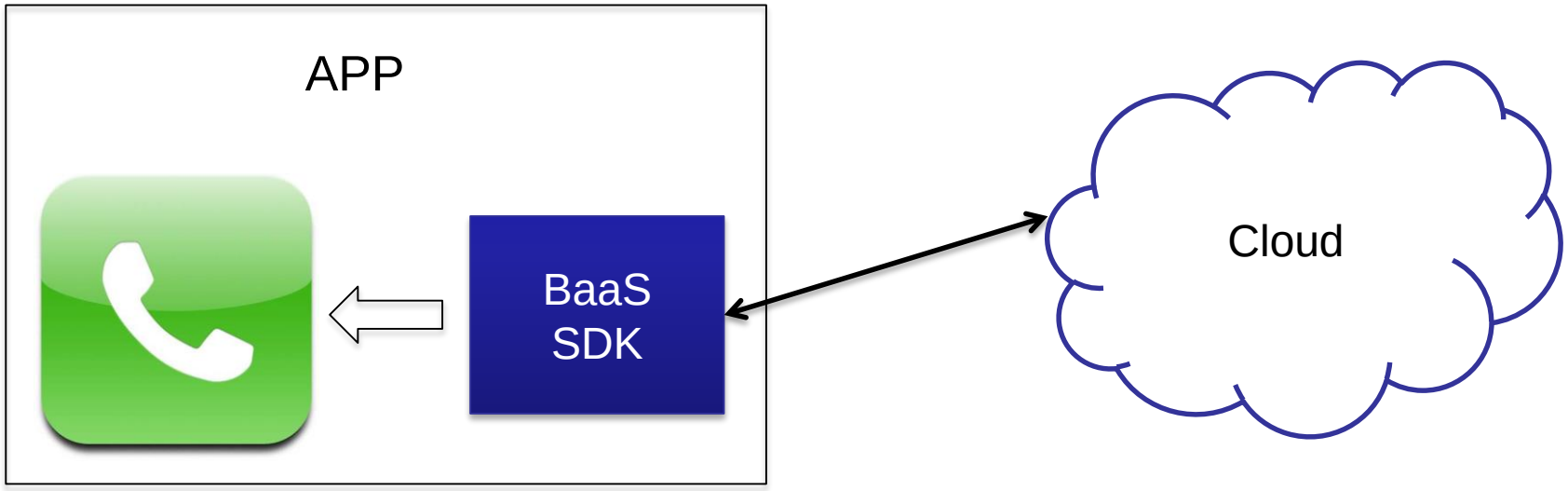
Backend-as-a-Service

TECHNISCHE UNIVERSITÄT DARMSTADT
SECURE SOFTWARE ENGINEERING GROUP
intel Security

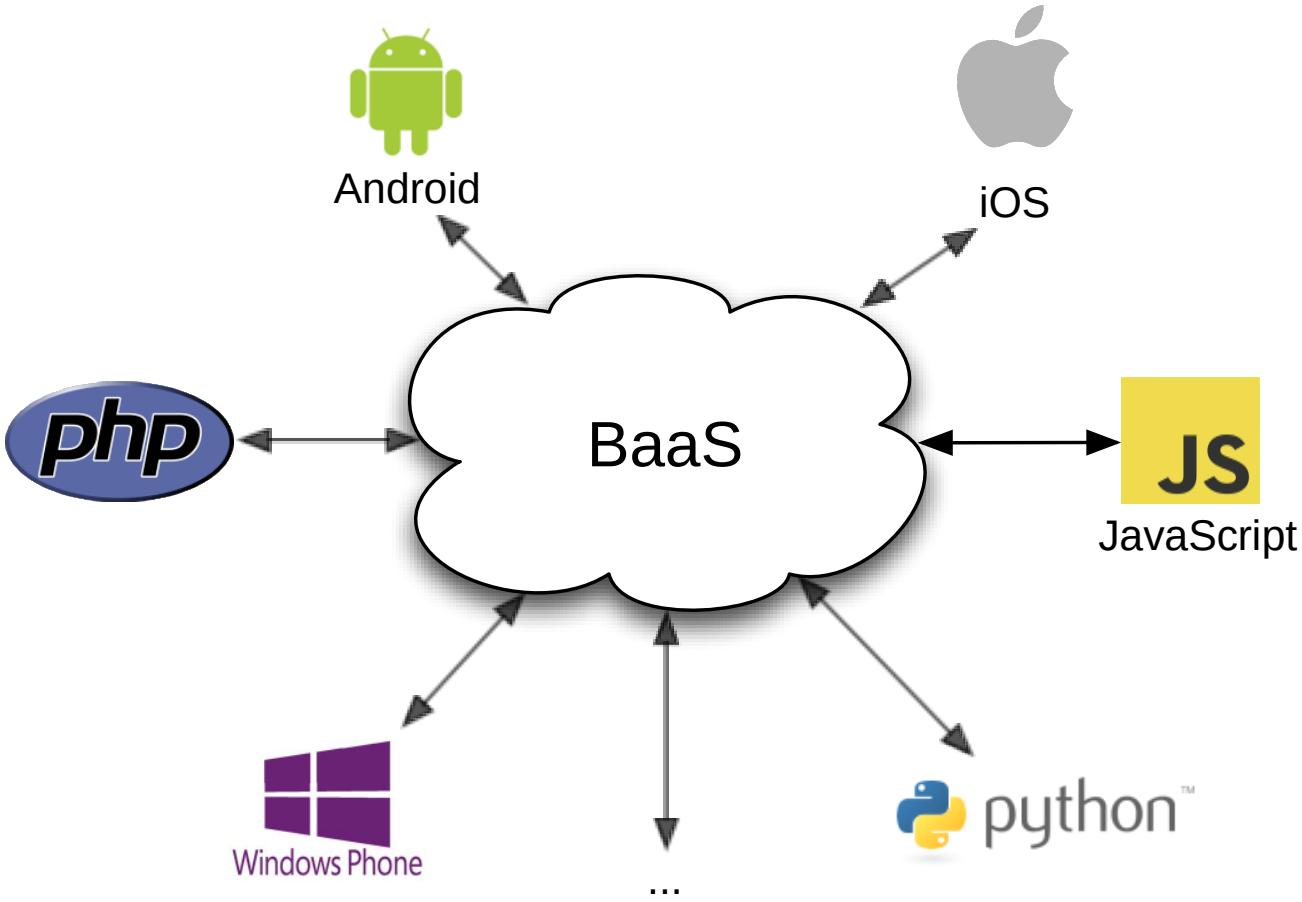
Agenda

- Backend-as-a-Service
- Developers exposing BaaS resources
- Android Malware using Facebook Parse
- Android/OpFake and Android/Marry
- Exposed Android Malware Facebook Parse accounts
- Financial Fraud by Android/Marry
- Responsible disclosure
- Conclusions

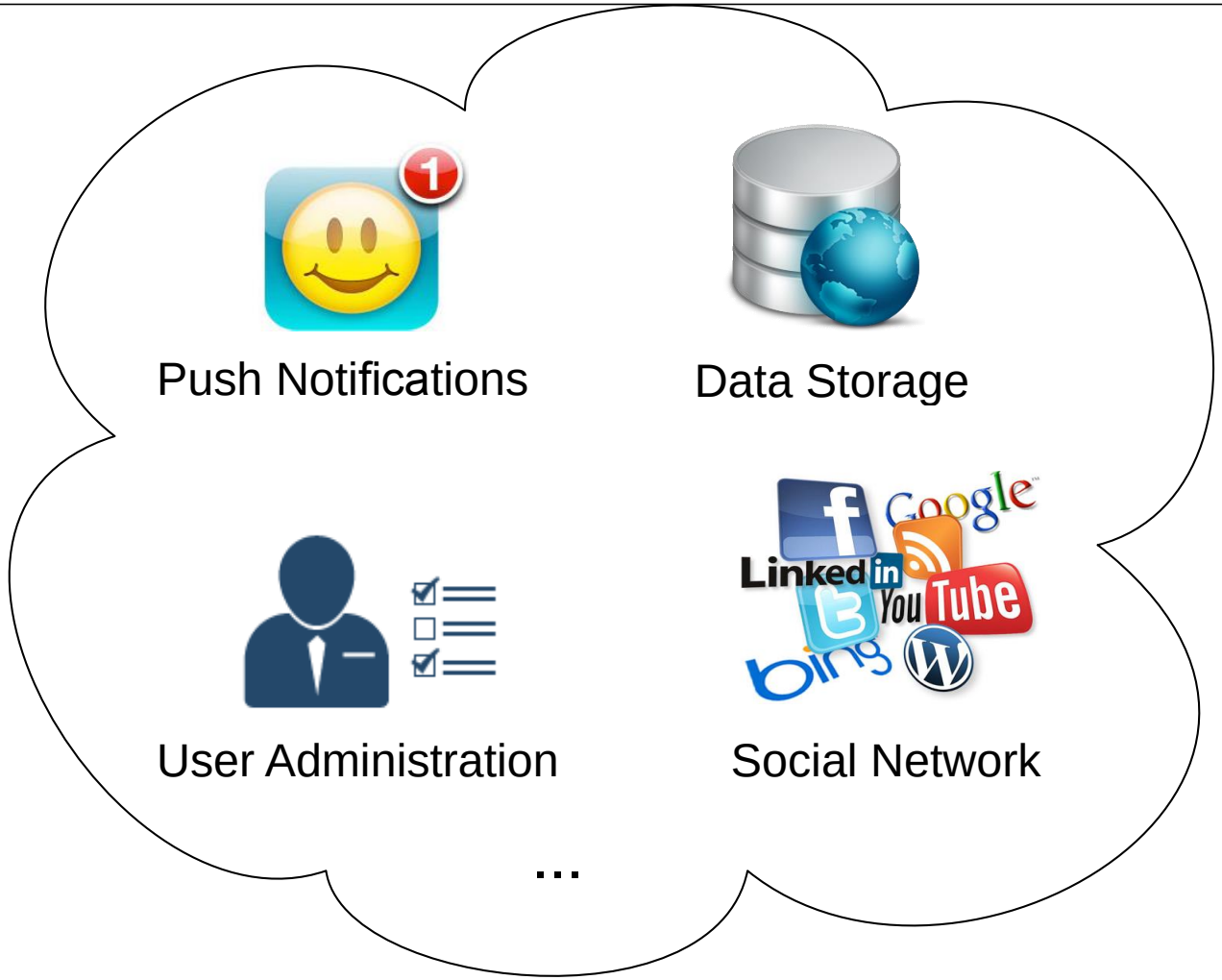
Backend-as-a-Service (1)



Backend-as-a-Service (2)



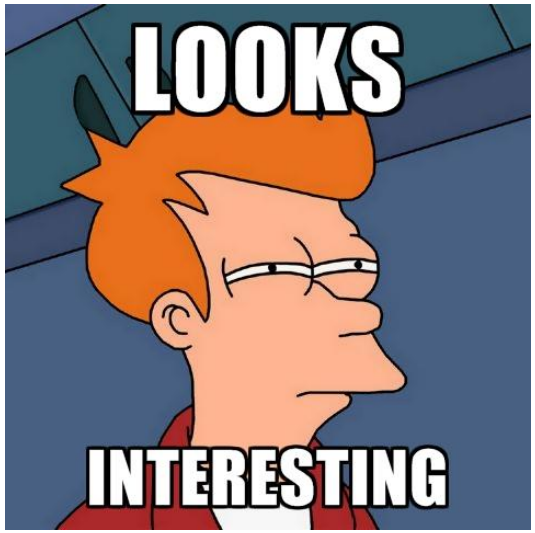
Backend-as-a-Service (3)



Amazon Tutorial

DB connection

```
AmazonS3Client s3Client = new AmazonS3Client(
        new BasicAWSCredentials("ACCESS_KEY_ID", "SECRET_KEY") );
```



"When you access AWS programmatically, you use an access key to verify your identity and the identity of your applications. An access key consists of an access key ID and a secret access key.

Anyone who has your access key has the same level of access to your AWS resources that you do."

Source: http://docs.aws.amazon.com/

App Authentication Model

Identification

"Hi, I am app <Application ID>"

Authentication

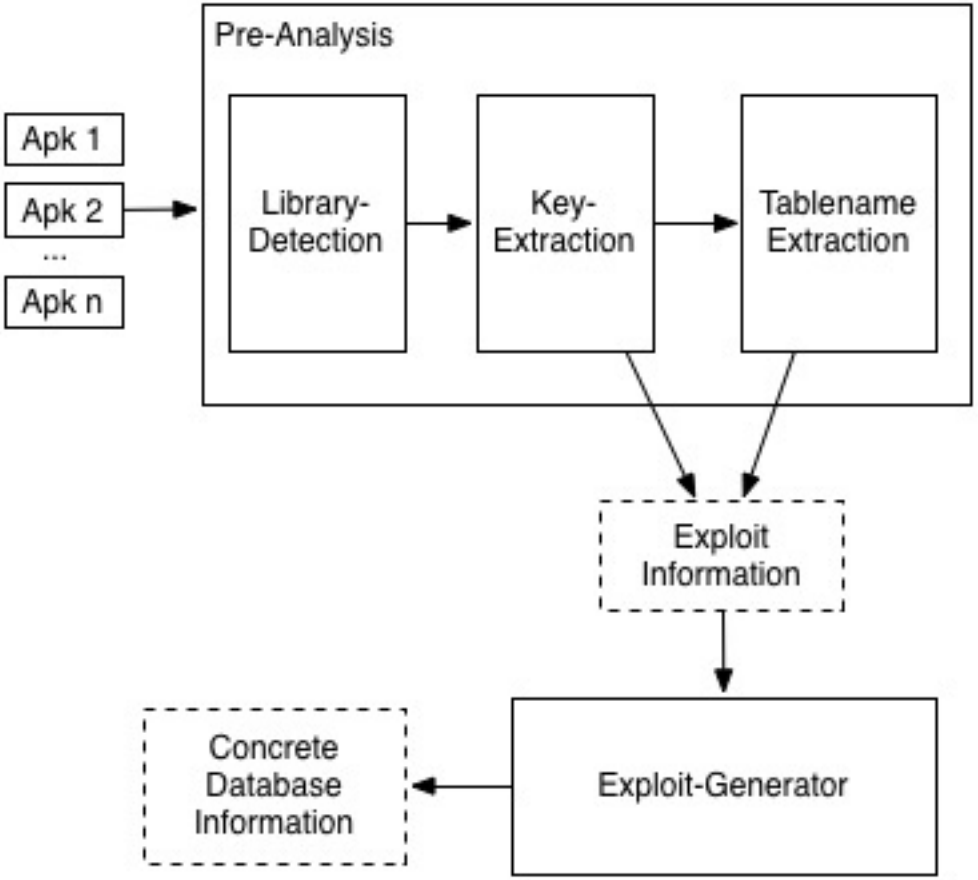
"My <Secret Key> is in the app" ???

Identification

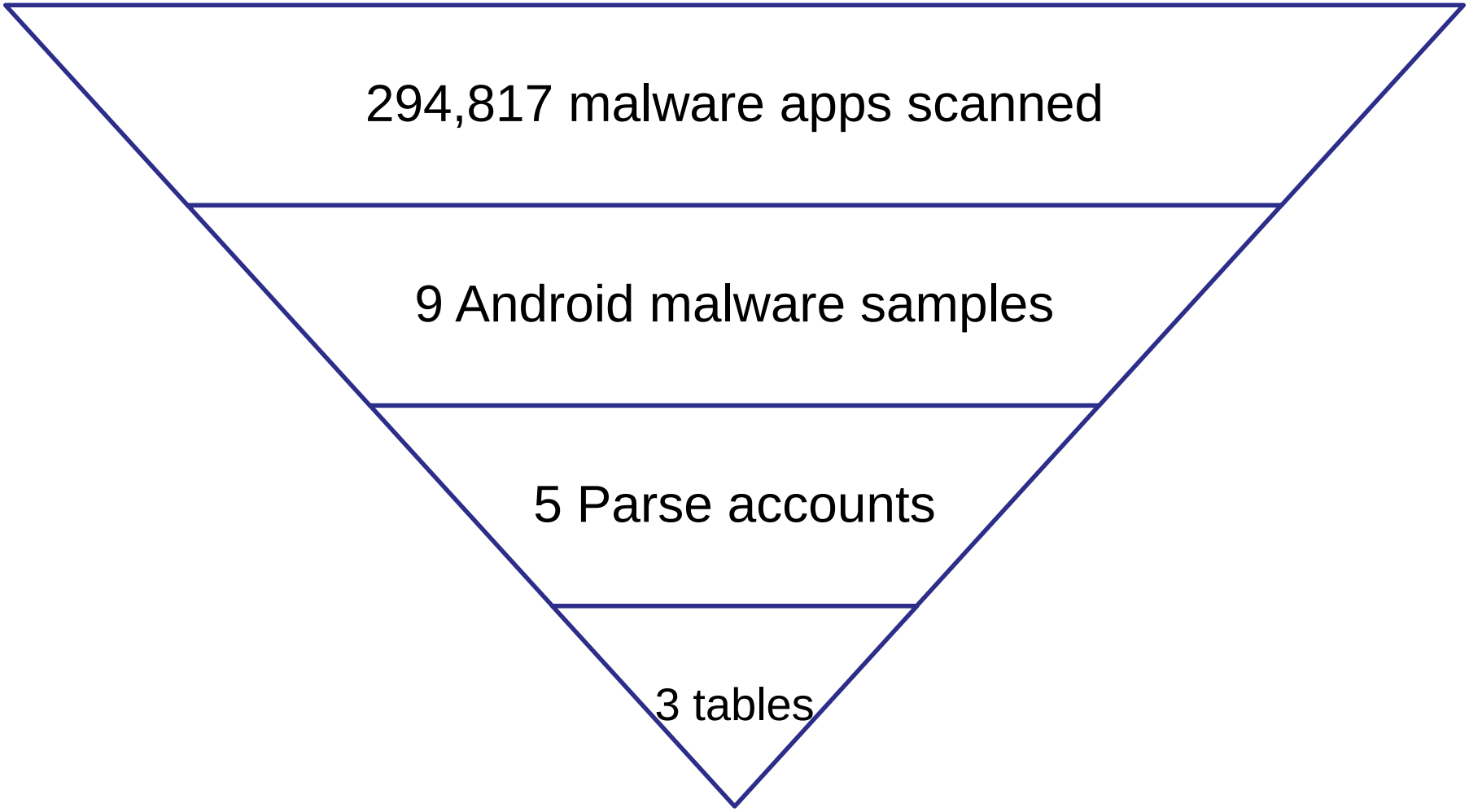
??
=

Authentication

HAVOC: Automatic Exploit Generator



Malware using Facebook‘s Parse

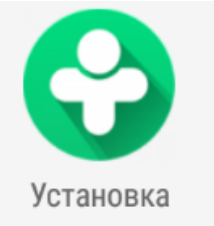


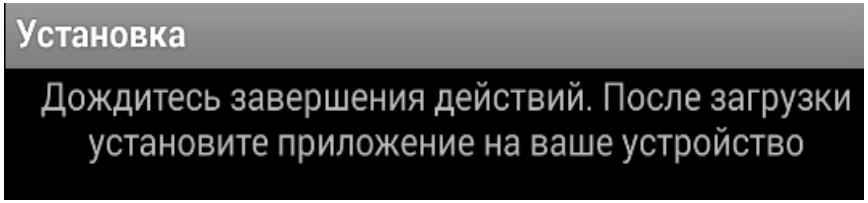
TECHNISCHE UNIVERSITÄT DARMSTADT

SECURE SOFTWARE ENGINEERING GROUP

intel Security

OpFake – App Execution





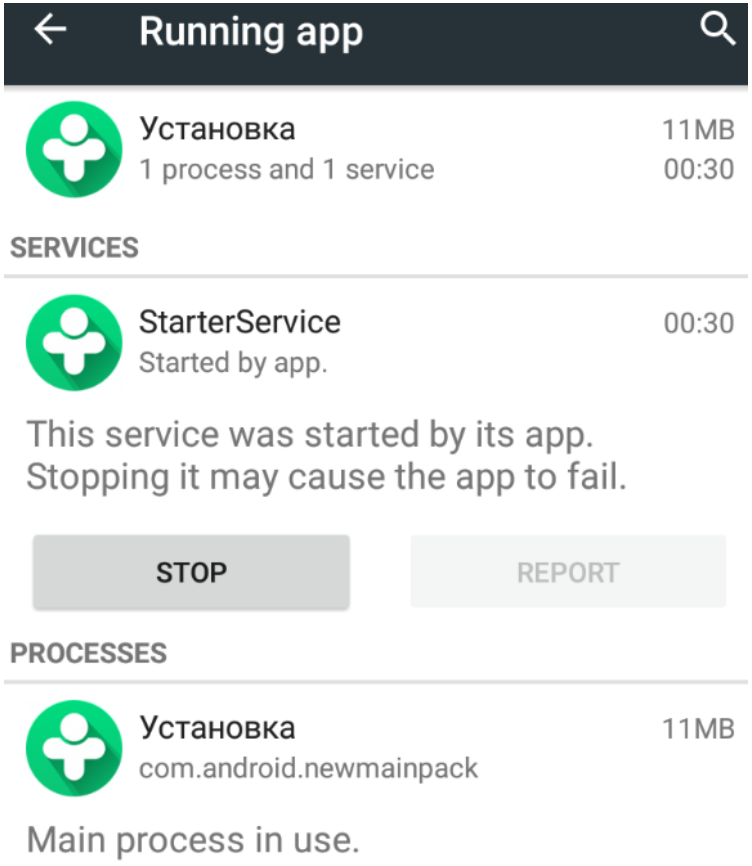
Icon Hidden

OpFake – MainService Started

Phone Rings

OR

Boot Completed



TECHNISCHE UNIVERSITÄT DARMSTADT

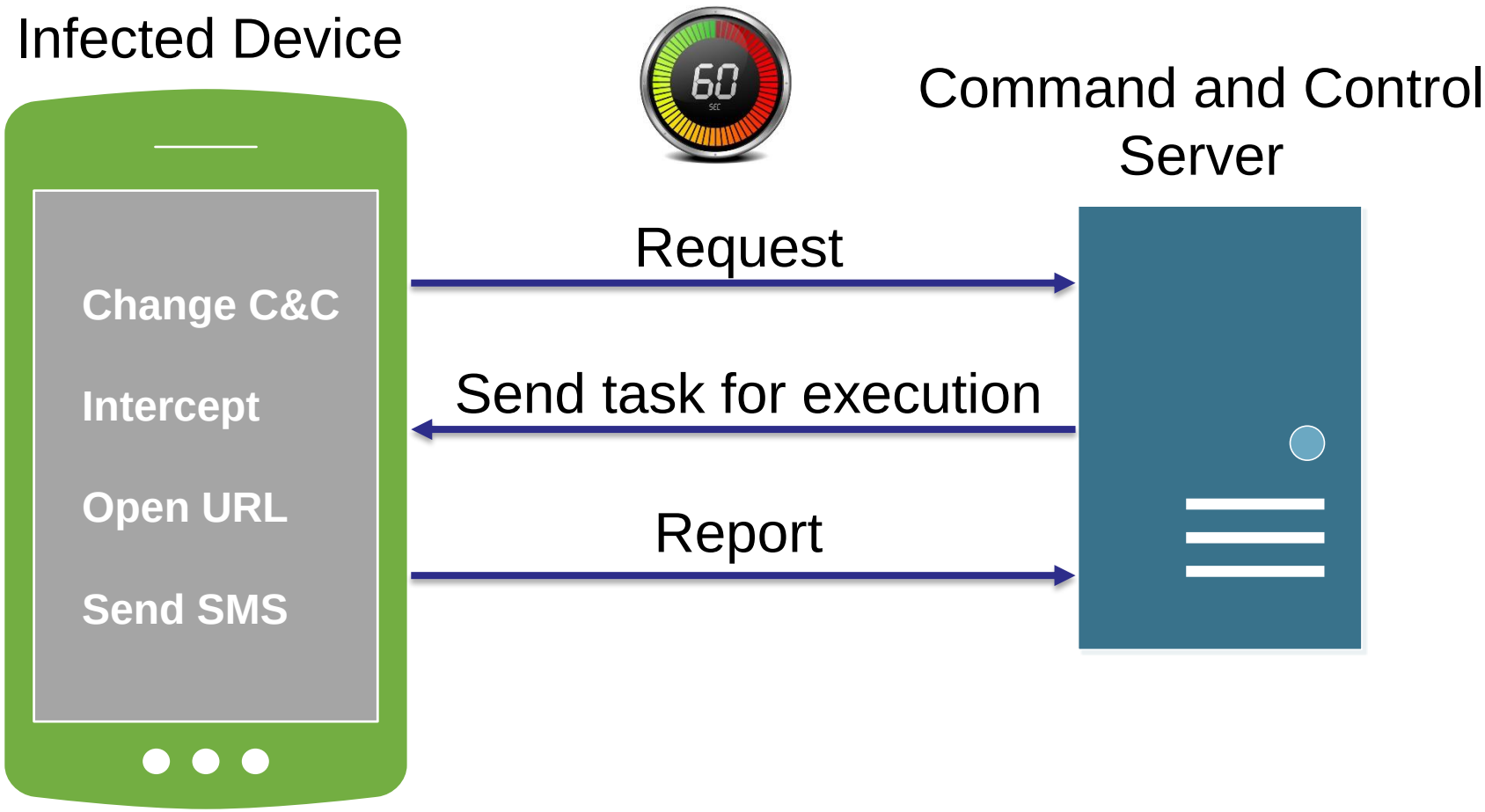
SECURE SOFTWARE ENGINEERING GROUP

intel Security

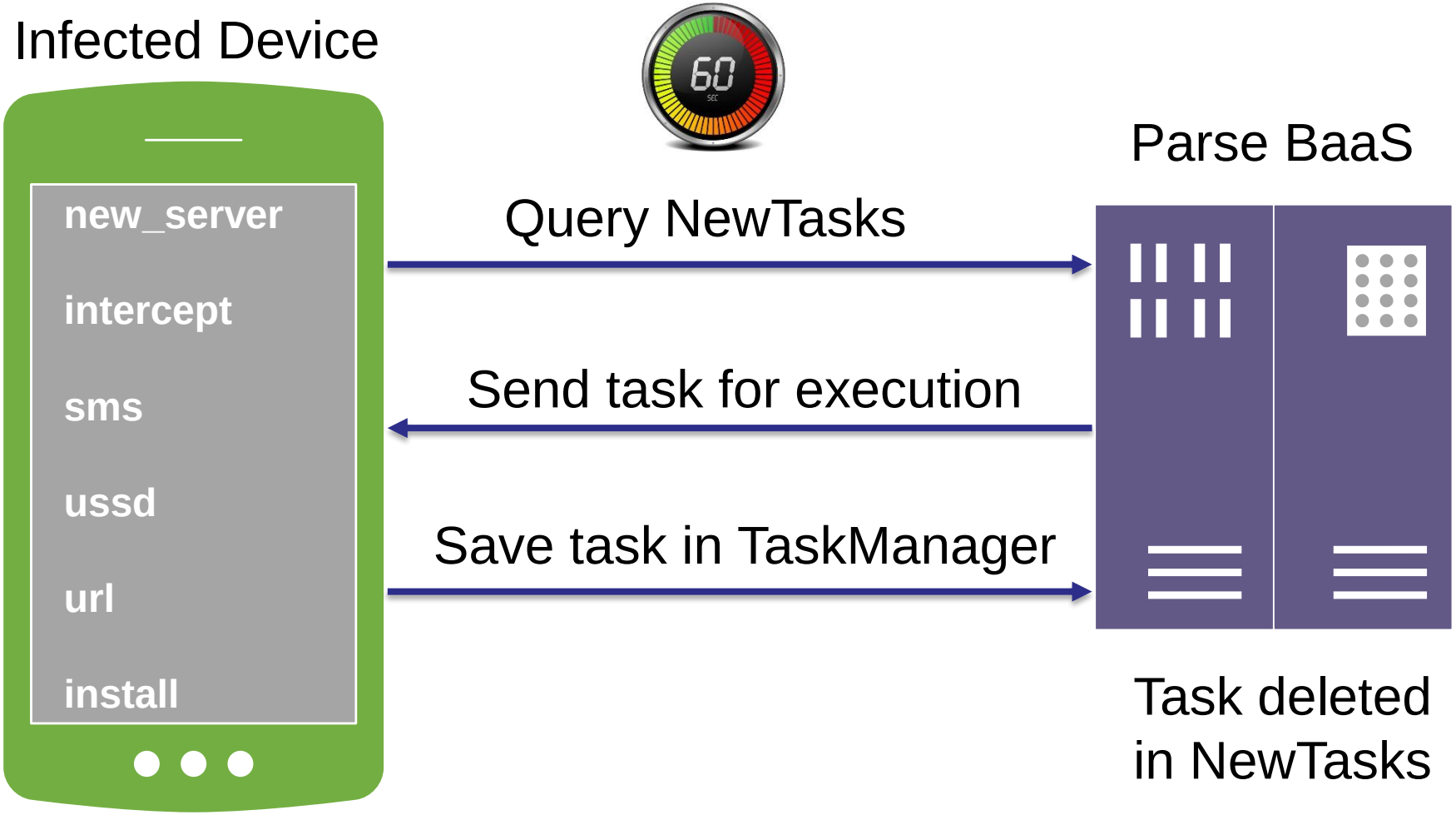
OpFake – Main Service Functionality

Subscribe to Push Notifications	Leak device data to a remote C&C server	Save installation data in Parse	Schedule a System Alarm
• D-<device_id> • “Everyone” • Country • “welcome”	• IMEI • Country • Phone Number • Network Operator • Balance	• Device data • device is rooted? • device is active?	• Execute code every 60 seconds

OpFake – “Traditional” C&C cycle



OpFake – Parse C&C cycle



TECHNISCHE UNIVERSITÄT DARMSTADT
SECURE SOFTWARE ENGINEERING GROUP
intel Security

OpFake – SMS Received

Save data in Parse SmsReceiver table

- origin
- content
- IMEI
- type
- is_card

Send message data to Parse Push channel “T”

- IMEI
- origin
- content
- type (incoming)

OpFake – Intercept flag

Intercept is ON

- Check if it is a response from a previous command
- Find the executed task in TaskManager Parse table
- Update the record with the response

Intercept is OFF

- Leak SMS message to remote server
- If origin is a specific network operator, extract balance

NewTasks Schema

NewTask Record				
imei	task	objectId	createdAt	updatedAt

sms			
origin	destination	content	date

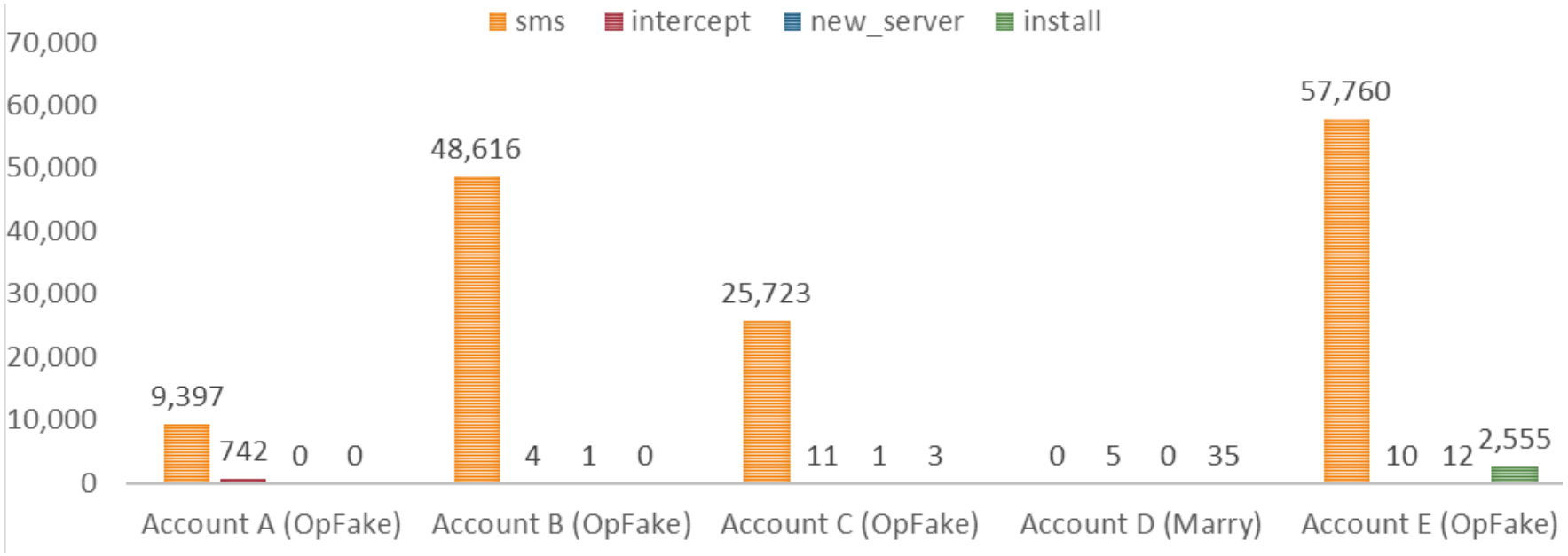
intercept	
values (on/off)	date

new_server		
imei	URL	date

install			
imei	URL of the APK	date	package name

Exposed Malware Parse.com Accounts

NewTasks – Commands received but never consumed



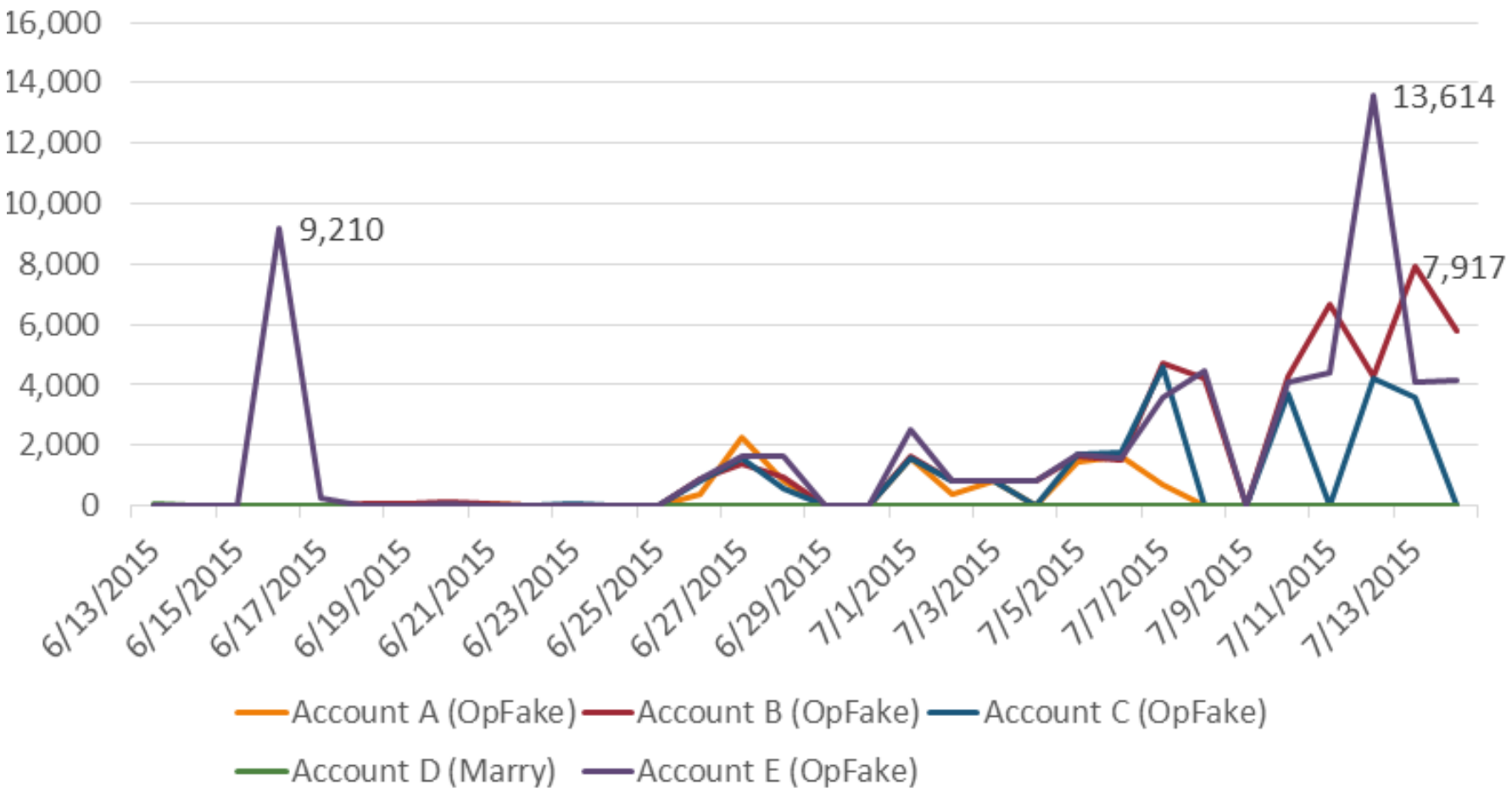
TECHNISCHE UNIVERSITÄT DARMSTADT

SECURE SOFTWARE ENGINEERING GROUP

intel Security

Exposed Malware Parse.com Accounts

NewTasks – Command created by date



TECHNISCHE UNIVERSITÄT DARMSTADT

SECURE SOFTWARE ENGINEERING GROUP

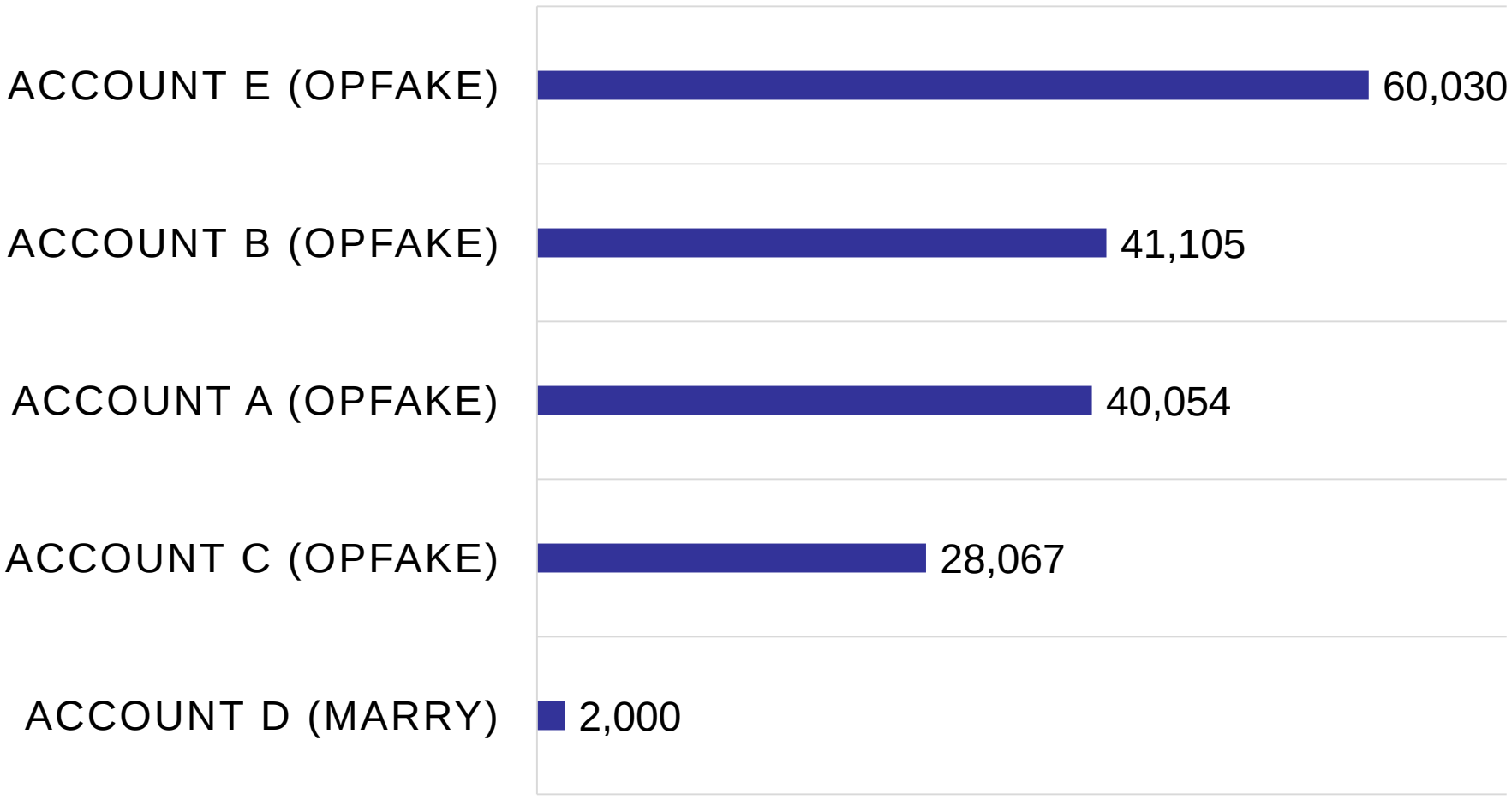
intel Security

SmsReceived Schema

SmsReceived Record							
body	from	objectId	intype	is_card	updatedAt	type	createdAt

Exposed Malware Parse.com Accounts

Number of Intercepted SMS messages in SmsReceiver Parse table



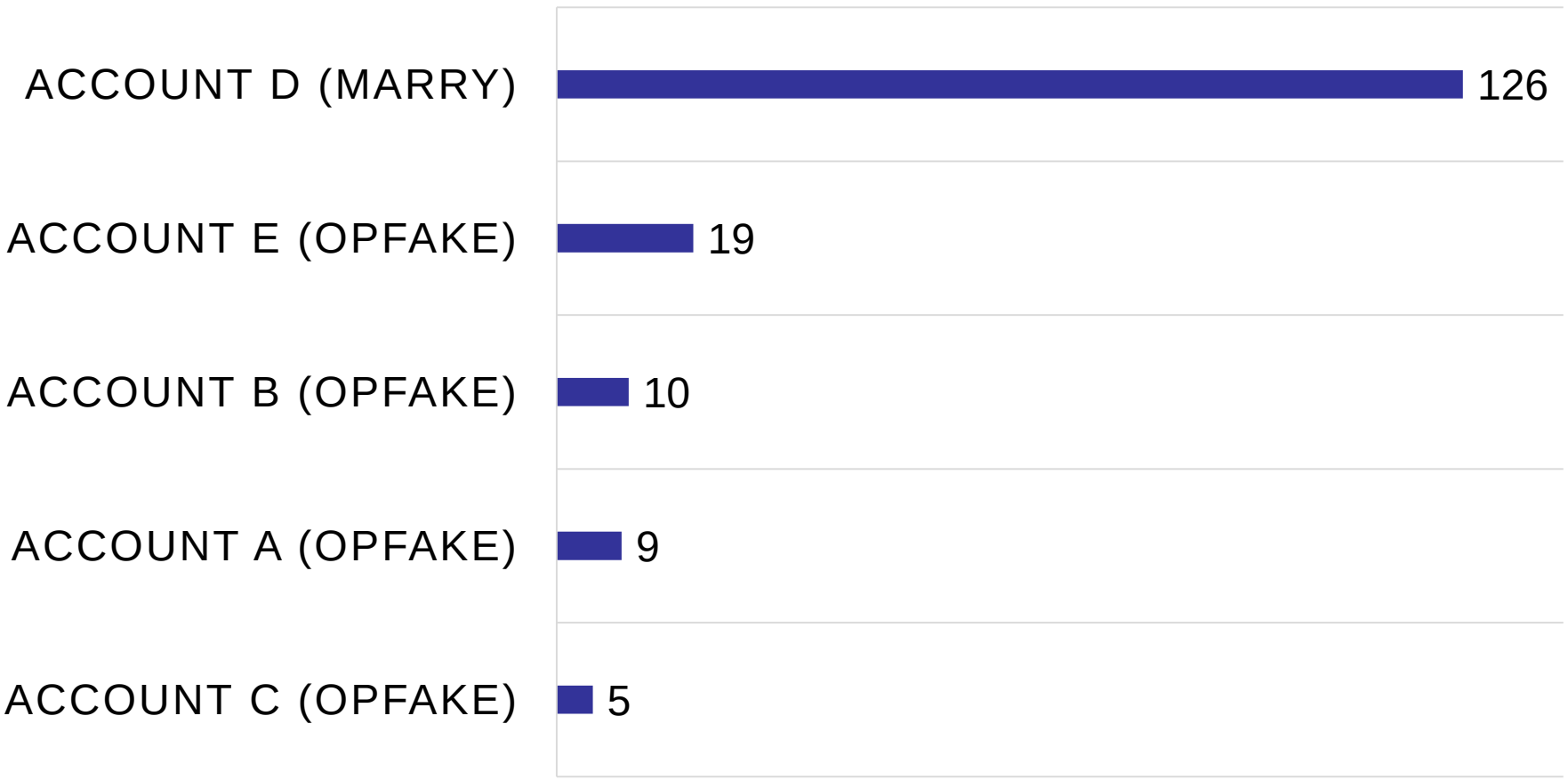
TECHNISCHE UNIVERSITÄT DARMSTADT

SECURE SOFTWARE ENGINEERING GROUP

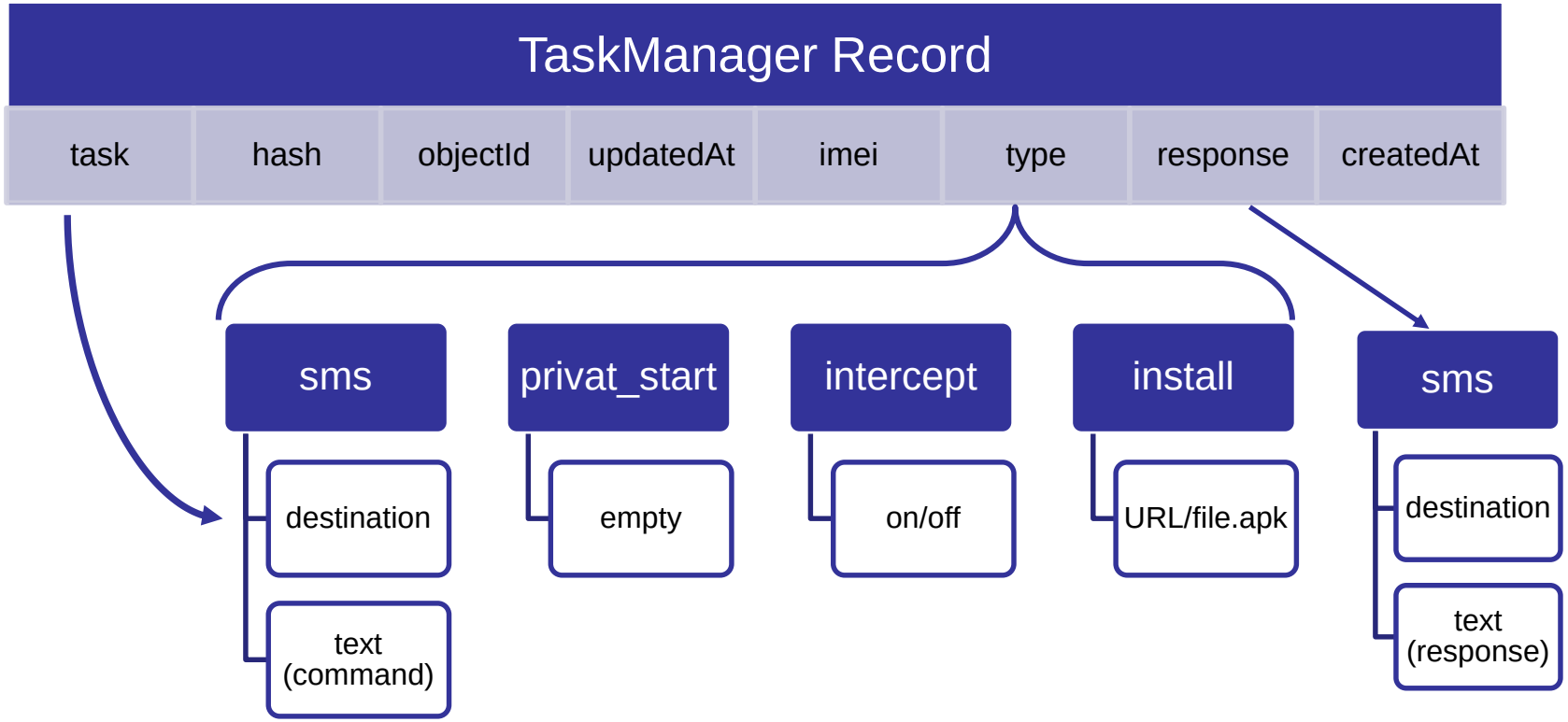
intel Security

Exposed Malware Parse.com Accounts

Number of credit cards numbers in SMS messages in SmsReceiver



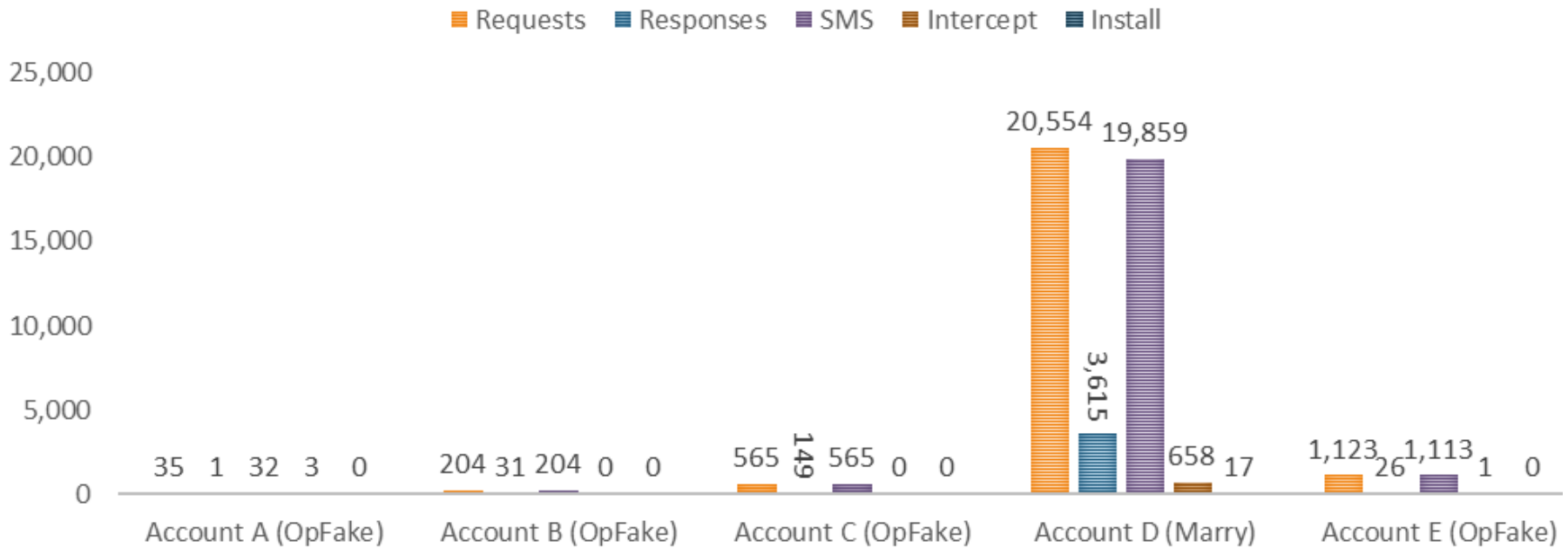
TaskManager Schema



TECHNISCHE UNIVERSITÄT DARMSTADT
SECURE SOFTWARE ENGINEERING GROUP
intel Security

Exposed Malware Parse.com Accounts

TaskManager – Command Executed

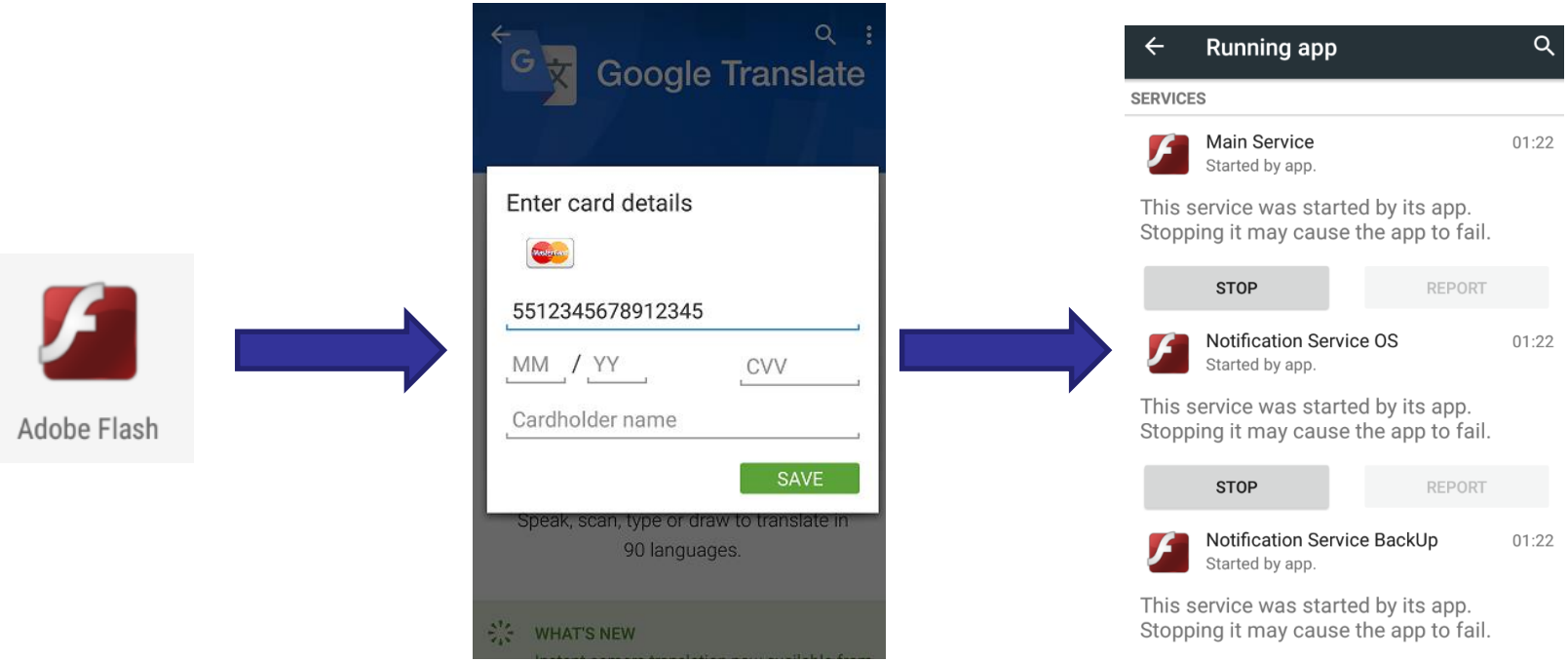


TECHNISCHE UNIVERSITÄT DARMSTADT

SECURE SOFTWARE ENGINEERING GROUP

intel Security

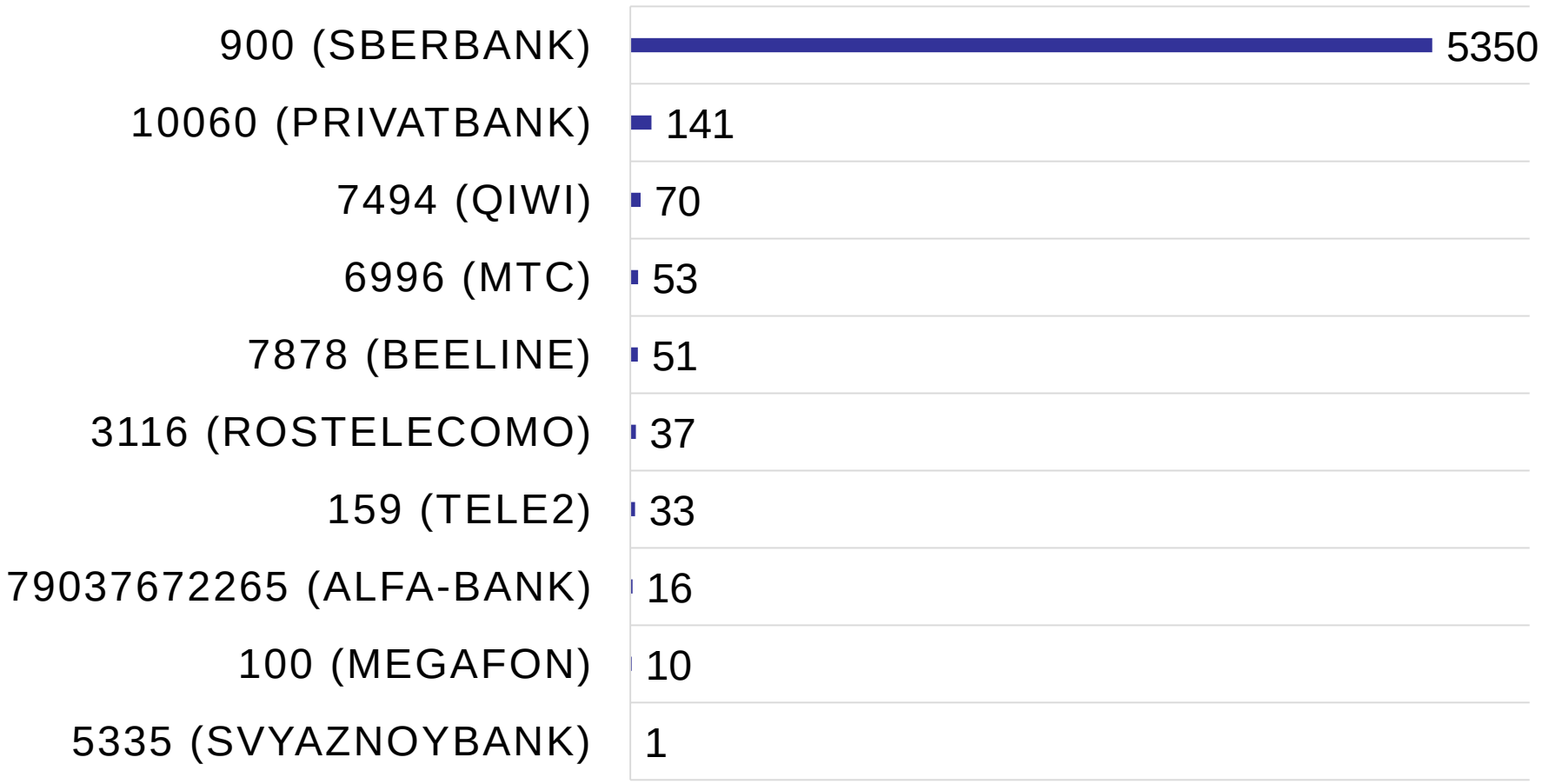
Android/Marry



TECHNISCHE UNIVERSITÄT DARMSTADT
SECURE SOFTWARE ENGINEERING GROUP
intel Security

Exposed Malware Parse.com Accounts

Number of SMS requests by targeted companies in Account D (Marry)

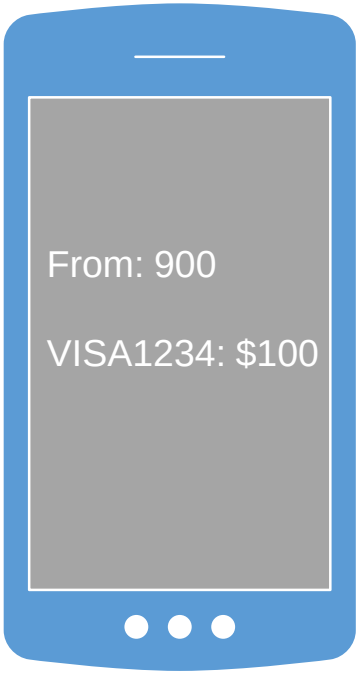


TECHNISCHE UNIVERSITÄT DARMSTADT

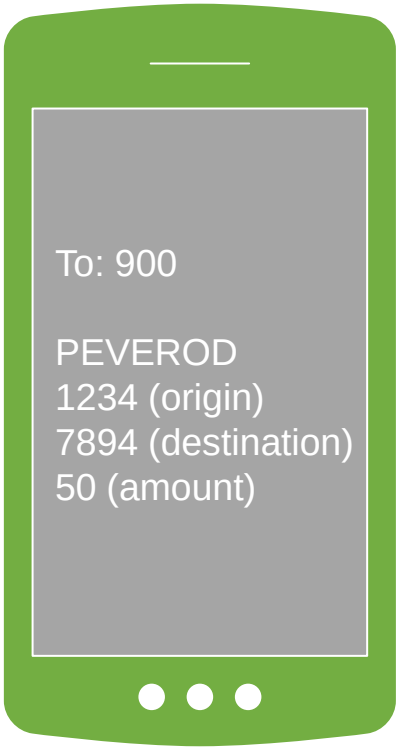
SECURE SOFTWARE ENGINEERING GROUP

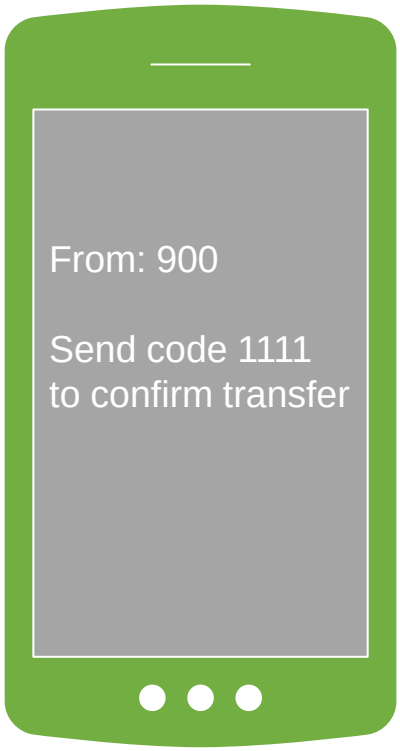
intel Security

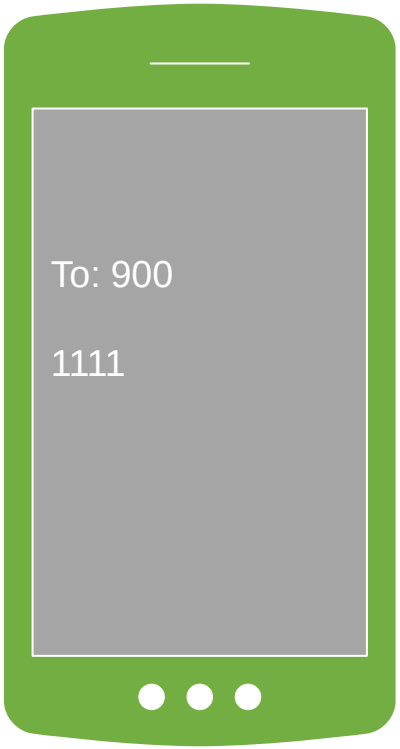
Sberbank SMS Banking Commands in TaskManager



Sberbank SMS Banking Commands in TaskManager



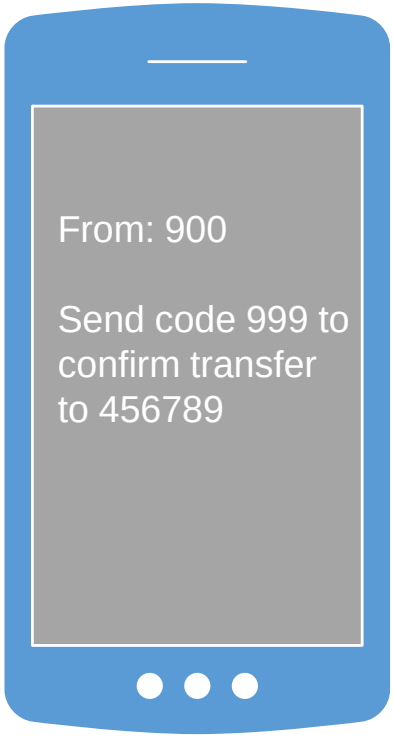




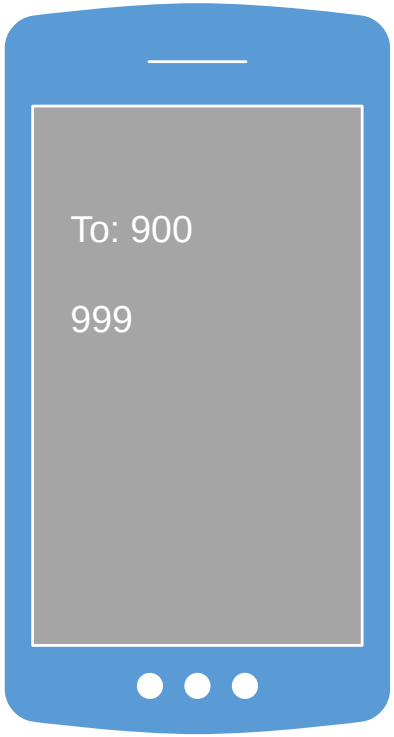
Sberbank SMS Banking Commands in TaskManager

Phone 456789

Phone 123456

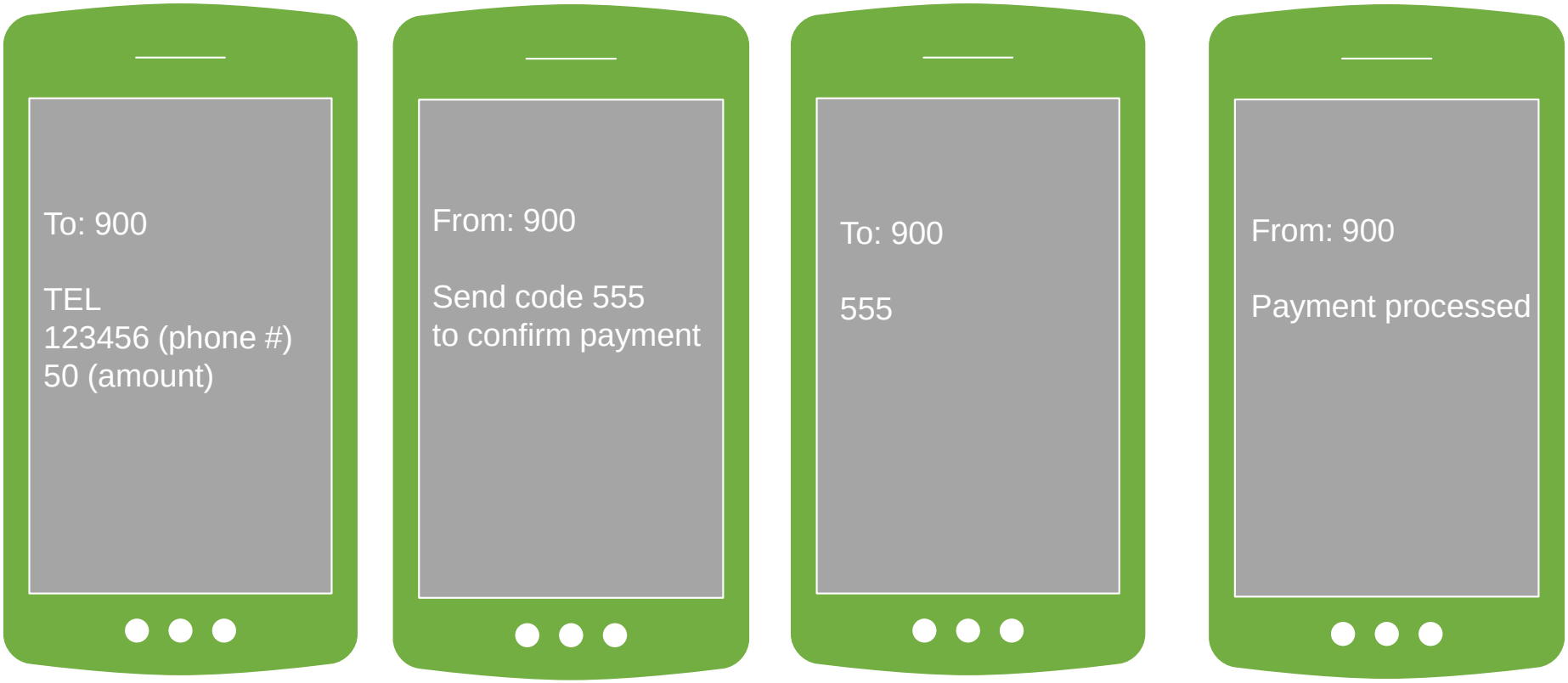


Phone 123456



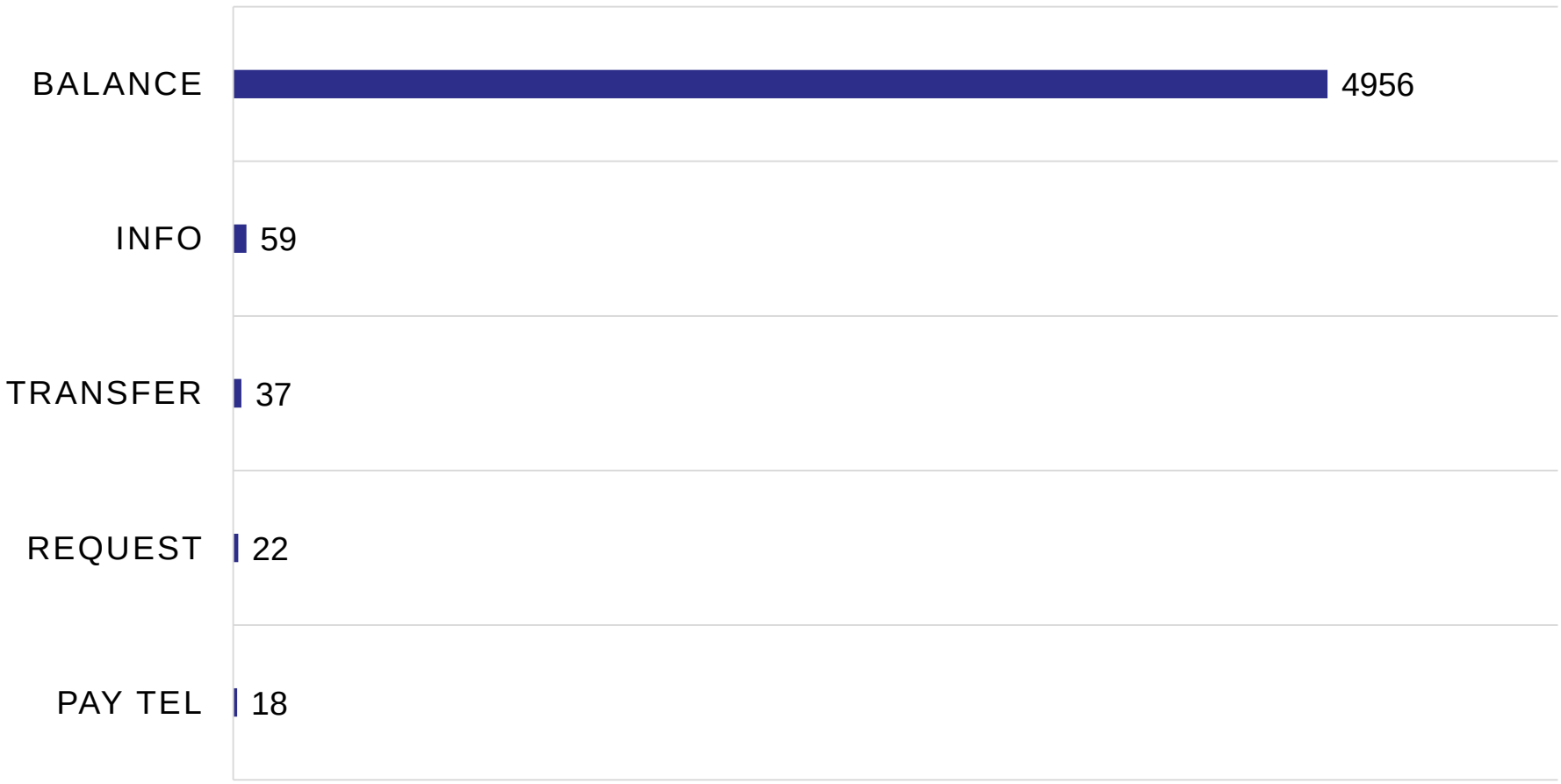
Phone 456789

Sberbank SMS Banking Commands in TaskManager



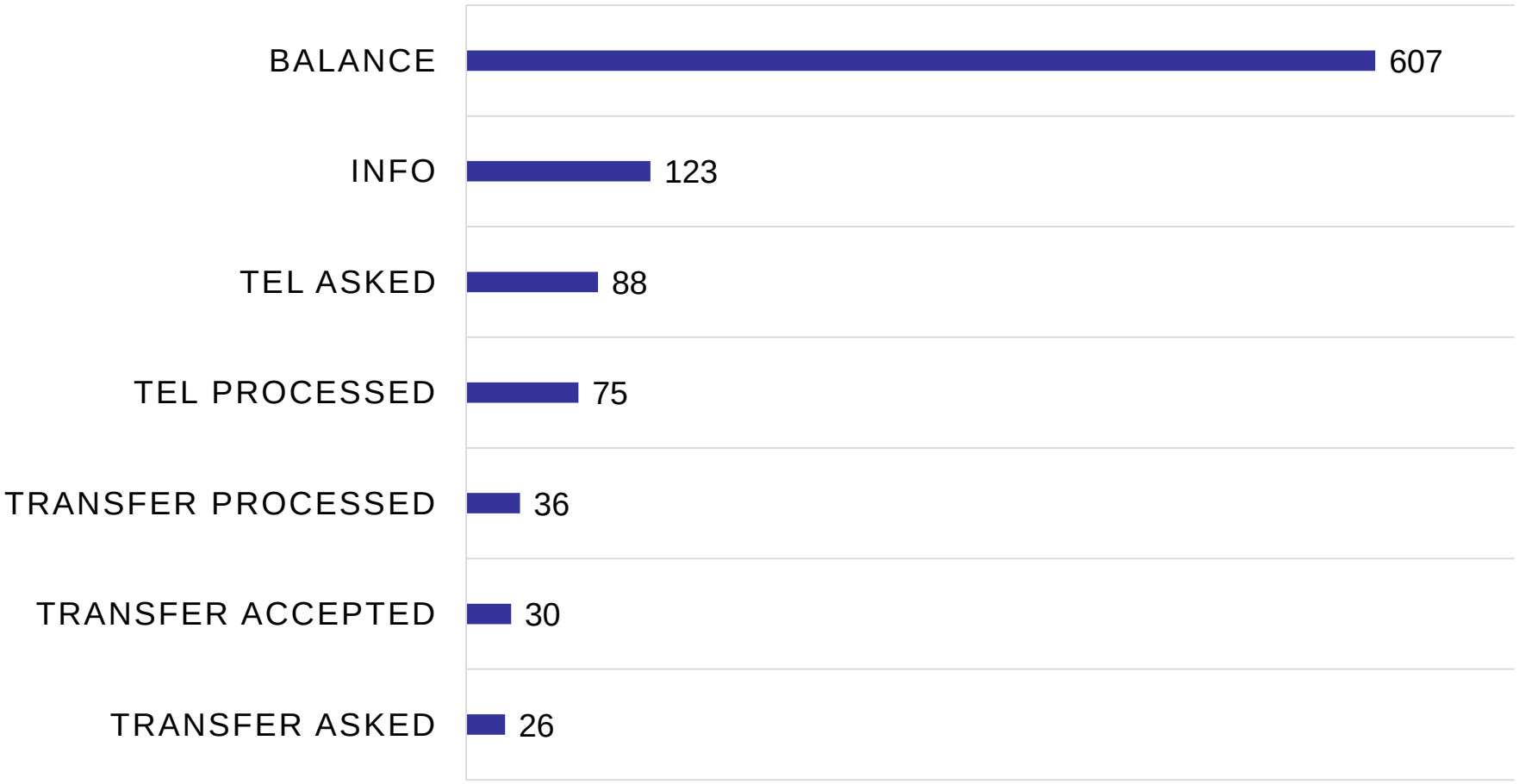
Exposed Malware Parse.com Accounts

Top Sberbank Commands – Task (TaskManager table) in Account D



Exposed Malware Parse.com Accounts

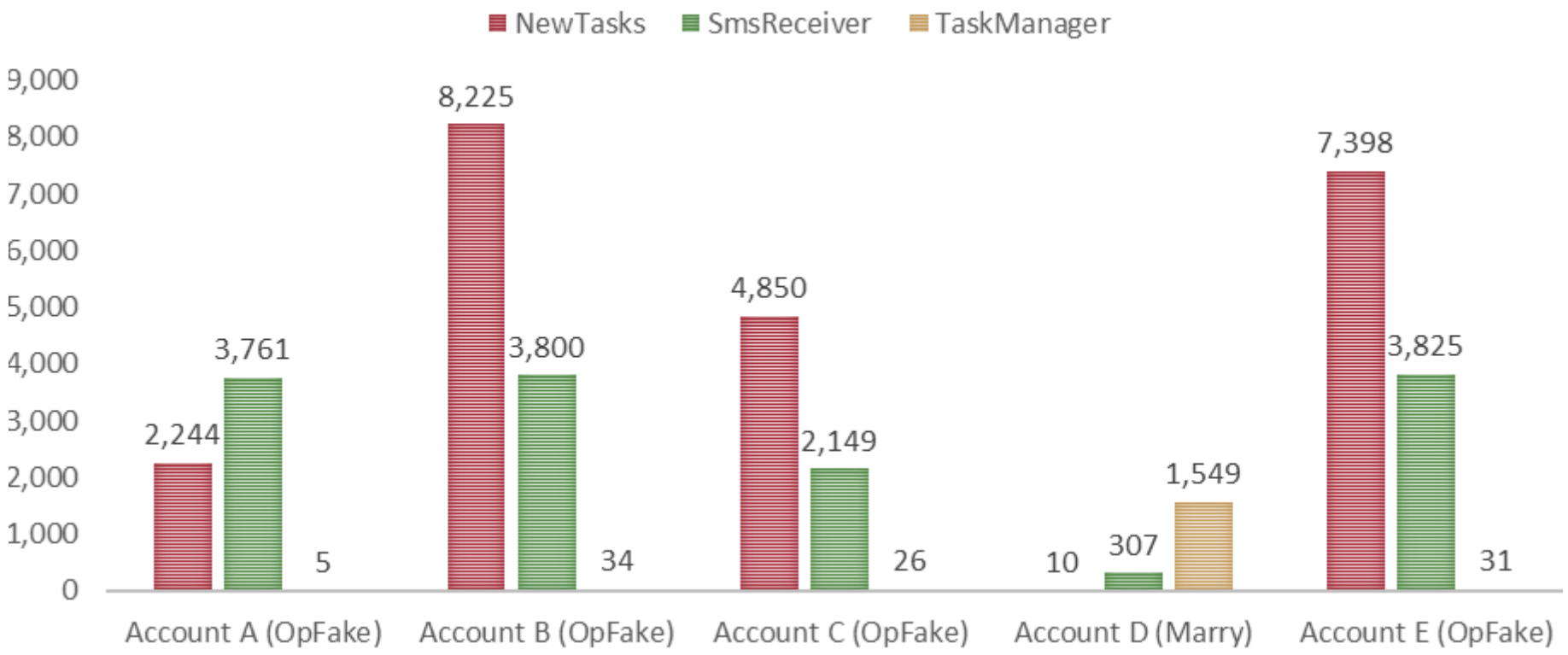
Top Sberbank fraud responses – Task (TaskManager table) - Account D



TECHNISCHE UNIVERSITÄT DARMSTADT
SECURE SOFTWARE ENGINEERING GROUP
intel Security

Exposed Malware Parse.com Accounts

Unique Device IDs per table



TECHNISCHE UNIVERSITÄT DARMSTADT
SECURE SOFTWARE ENGINEERING GROUP
intel Security

Responsible Disclosure

2015-08-03: Reported finding to Facebook
2015-08-05: Facebook replied with "*... This issue does not qualify as a part of our bounty program...*"

2015-08-05: Facebook asked for more details
2015-08-06: We provided more details and Facebook blocked all Parse accounts
2015-08-28: Facebook offered room for collaboration

Facebook's responsible disclosure system only works with a Facebook account

Conclusions

- Android Banking Trojans stores and exposes its data in BaaS solutions
- By default no authentication is needed to access BaaS data
- Android Banking Trojans are actively performing financial fraud via SMS.
- In less than a month, thousands of people were victims of financial fraud

Siegfried Rasthofer
Secure Software Engineering Group
Email: siegfried.rasthofer@cased.de
Blog: http://sse-blog.ec-spride.de
Website: http://sse.ec-spride.de
Twitter: @CodeInspect

Carlos Castillo
Intel Security
Email: carlos.castillo@intel.com
Twitter: @carlosacastillo