

Security and Privacy Enablers in the Framework of Privacy Flag

***Privacy-Flag - based Special Session
Infocom World 2016, Athens
November 02, 2016***

Evangelos Sfakianakis- *Hellenic Telecommunications Organization S.A. -OTE*
Ioannis Chochliouros- *Hellenic Telecommunications Organization S.A. -OTE*



**PRIVACY
FLAG**



Co-funded by the
European Union



Co-funded by the
Swiss Confederation

Privacy Flag Project Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments



PRIVACY FLAG

Content



Introduction



Data Protection and Privacy Concerns



Security and Privacy Enablers



Traffic Analysis - Website Fingerprinting



Traffic Analysis – Study



Co-funded by the
European Union



Co-funded by the
Swiss Confederation

Infocom World 2016 _ Athens, Greece, Nov.02, 2016
Privacy Flag - based Special Session



PRIVACY FLAG

Introduction



Personal data protection is a challenge both in terms of **privacy** and **exploitation** for **5G** and **IoT** environment.



The European Union protects citizens against unilateral collection and privacy of **personal data**:

- ❖ Including **IoT** and **smartphone application** and;
- ❖ Developed Applications outside the EU legal framework.
- *Inefficient to implement or extent a privacy top-down mechanism.*



Privacy-Flag intends to combine **crowd-sourcing technologies** together with privacy monitoring agents, innovative privacy risk assessment methodology and legal expertise to develop a **privacy protection framework** *enabling citizens to better control and protect their personal data.*



Privacy-Flag assessment tool will help citizens to **monitor** and **control** their **privacy** and **data exploitation**, *notifying them by a smartphone application, Website or a browser add-on.*





PRIVACY FLAG

Data protection and privacy concerns

Privacy Flag aims to effectively research the potential of crowdsourcing and legal expertise to empower the users to set the desired level of privacy, based on a simple -to understand- visualisation of the privacy level.

This will be realised *through a crowd-sourcing based process and a set of tools and solution(s)* enabling the users to “collectively assess and control the level of risk for their privacy” in the context of web applications, smart phones applications and IoT deployments.

It will provide a new paradigm of privacy risk assessment combining:

- (i) a Crowdsourcing model of risk identification and evaluation;
- (ii) a Universal Privacy Risk Area Assessment Tool resulting to the corresponding Universal Privacy Risk Area Assessment Methodology (UPRAAM)
- (iii) Distributed Agents (DAs) to monitor, assess and inform about the privacy risk level of any application;
- (iv) full anonymization and privacy technology for server connections;
- (v) legal expertise in privacy and personal data protection; personal data valuation mechanism, and;
- (vi) a voluntary legal binding mechanism for companies located outside of Europe.






PRIVACY FLAG

Security and Privacy Enablers - Intro

Privacy Flag creates technical enablers for security and privacy that will:

 **Provide** privacy protection mechanisms for users.

 **Contribute** towards the improvement of privacy protection and risk detection through collective user activities and reporting.

 **Help infuse privacy risk awareness**, as well as **privacy risk detection knowledge** to users in order to make them take a more active role in handling their own, as well as others' privacy.



Co-funded by the
European Union



Co-funded by the
Swiss Confederation

Infocom World 2016 _ Athens, Greece, Nov.02, 2016
Privacy Flag - based Special Session



PRIVACY FLAG

Security and Privacy Enablers

- Should not only be about anonymization (onion routing)
- It is believed that systems such as Tor are still vulnerable to **traffic analysis**
- **How to protect?**

State-of-the-Art: Tor

- Better Quality of Service ?
- Resistance to Traffic Analysis ?
- more specific Website Fingerprinting



Co-funded by the
European Union



Co-funded by the
Swiss Confederation

Infocom World 2016 _ Athens, Greece, Nov.02, 2016
Privacy Flag - based Special Session



PRIVACY FLAG

Traffic Analysis - Website Fingerprinting

Traffic Analysis

- ❖ Even if the data packets are encrypted, the packet flow may leak side-channel information
- ❖ Attacker is a local, passive observer of packet flow
- ❖ Utilizes timing information, packet sizes, power consumption, ...

Website Fingerprinting

- ❖ Belongs to the family of Traffic Analysis attacks
- ❖ Tries to identify the webpage someone is visiting by looking at the encrypted packets
- ❖ Uses machine learning



Co-funded by the
European Union



Co-funded by the
Swiss Confederation

Infocom World 2016 _ Athens, Greece, Nov.02, 2016
Privacy Flag - based Special Session



PRIVACY FLAG

Traffic Analysis – Study (1/2)



- Idea:** Infer information about the content of an encrypted transmission based on packet direction, ordering, size and timing
- *There was conducted a large-scale study about the feasibility of traffic analysis*

Goal: Identify countermeasures to constrain information leakage.



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG

Traffic Analysis – Study (2/2)

- **All previous studies limited to unrealistic datasets**
 - Only popular websites
 - Small data set size
- **PF Compiled *realistic* data sets**
 - Hundreds of thousands websites retrieved by real users
 - Combined different sources (Twitter, Google Trends, ...)
- Applied all state-of-the-art attacks

Results:

- The attack was by far not as severe as presumed!
- It does not scale to realistic universe sizes
- **Efficient countermeasures are feasible!**

Web Analytics Tools



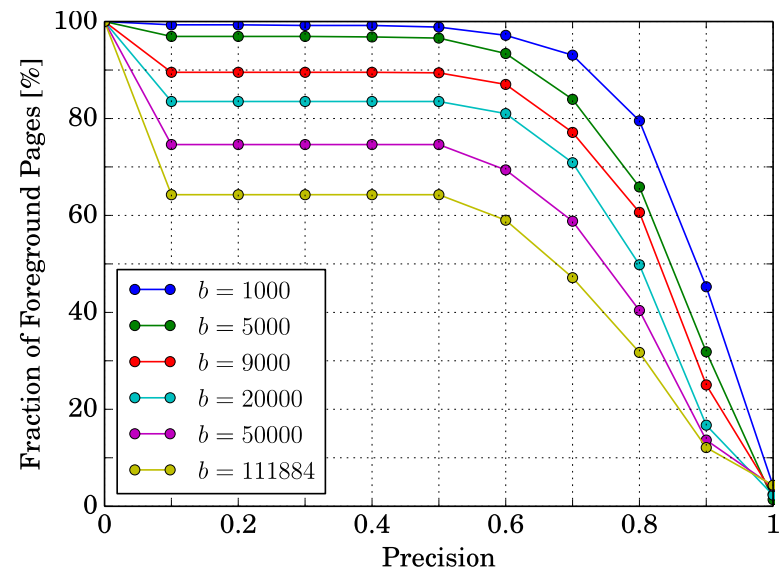
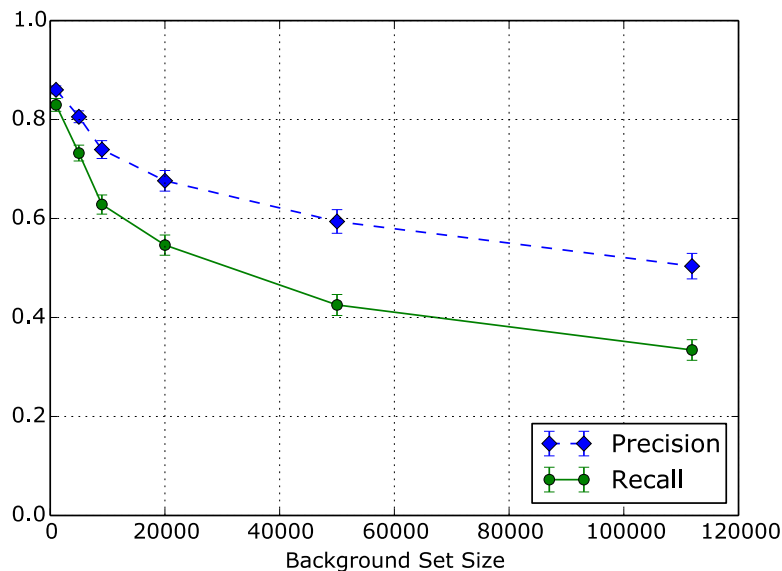
Co-funded by the
European Union



Co-funded by the
Swiss Confederation

Infocom World 2016 _ Athens, Greece, Nov.02, 2016
Privacy Flag - based Special Session

The attack is by far not as severe as presumed!
It does not scale to realistic universe sizes



Efficient countermeasures are feasible!



PRIVACY FLAG

Thank you!

www.privacyflag.eu

For more information:

Dr. Ioannis P. CHOCHLIOUROS
Head of Research Programs Section, Fixed
Coordinator of the Privacy Flag Project

E-Mail: ichochliouros@oteresearch.gr; ic152369@ote.gr;

Mr. Evangelos Sfakianakis
Research Programs Section, Fixed
E-Mail: esfak@oteresearch.gr;



Co-funded by the
European Union



Co-funded by the
Swiss Confederation

Infocom World 2016 _ Athens, Greece, Nov.02, 2016
Privacy Flag - based Special Session



National and Kapodistrian
University of Athens



HWCommunications
Cyber Security and Resilience



**PRIVACY
FLAG**



Co-funded by the
European Union



Co-funded by the
Swiss Confederation