

Using Crowdsourcing to Protect Web Privacy

Dr. Vasileios Vlachos (CTI)



**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

About CTI

-  One of the major R&D institutes in Greece
-  Has undertaken more than 85 R&D projects
-  The team involved in Privacy Flag works within CTI's Research Unit 1 (RU1) which consists of Faculty Members, 9 PhD Researchers and 20 Engineers-PhD Students
-  The CTI team is involved in relevant FP7 and national projects in the privacy/security, crowdsensing/crowdsourcing and IoT (PROTOS, ABC4Trust, IoT Lab)



CTI
computer
technology
institute & press



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG

Future Current threats

Third party tracker or advertising company



Cookies

Fingerprinting

Traffic analysis



PrivacyFlag AddOn User





PRIVACY FLAG

Smartphone Privacy Invasion in action

- It was revealed that the most commonly used flashlight apps are secretly stealing the users' personal information stored on their mobile devices.
- In reality these apps have put the security and privacy of smartphone users at risk just by requesting for fanatical permissions which naïve users adhere to.
- Downloading from Google Play doesn't ensure the security of any app.

Flashlight Apps	Super-Bright LED Flashlight	Brightest Flashlight Free	Tiny Flashlight + LED	Flashlight	Flashlight	Brightest LED Flashlight	Color Flashlight	High-Powered Flashlight	Flashlight HD LED	Flashlight: LED Torch Light
Permissions										
retrieve running apps	✓					✓		✓		
modify or delete the contents of your USB storage	✓	✓				✓		✓		
test access to protected storage	✓	✓				✓		✓		
take pictures and videos	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
view Wi-Fi connections	✓	✓				✓		✓	✓	
read phone status and identity	✓	✓			✓	✓		✓		
receive data from Internet	✓					✓		✓		
control flashlight	✓	✓	✓			✓	✓	✓	✓	
change system display settings	✓					✓		✓		
modify system settings	✓					✓		✓		
prevent device from sleeping	✓							✓		
view network connections	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
full network access	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
approximate location (network-based)	✓	✓						✓		
precise location (GPS and network-based)	✓	✓								
disable or modify status bar	✓	✓								
read Home settings and shortcuts	✓	✓		✓						✓
install shortcuts	✓	✓		✓						✓
uninstall shortcuts	✓	✓		✓						✓
control vibration	✓		✓							
prevent device from sleeping		✓	✓	✓		✓			✓	✓
write Home settings and shortcuts				✓						✓
disable your screen lock				✓						✓
read Google service configuration					✓				✓	



PRIVACY FLAG

Smartphone Privacy Invasion in action

 XcodeGhost

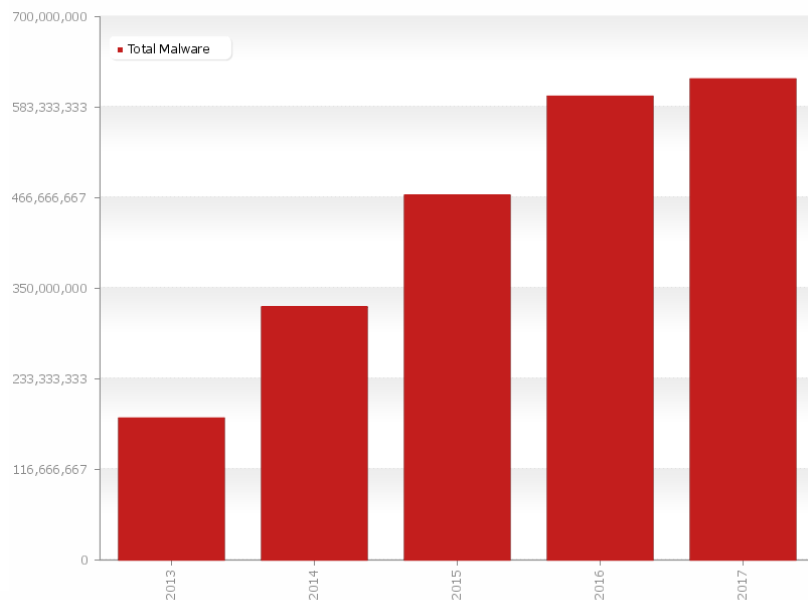




PRIVACY FLAG

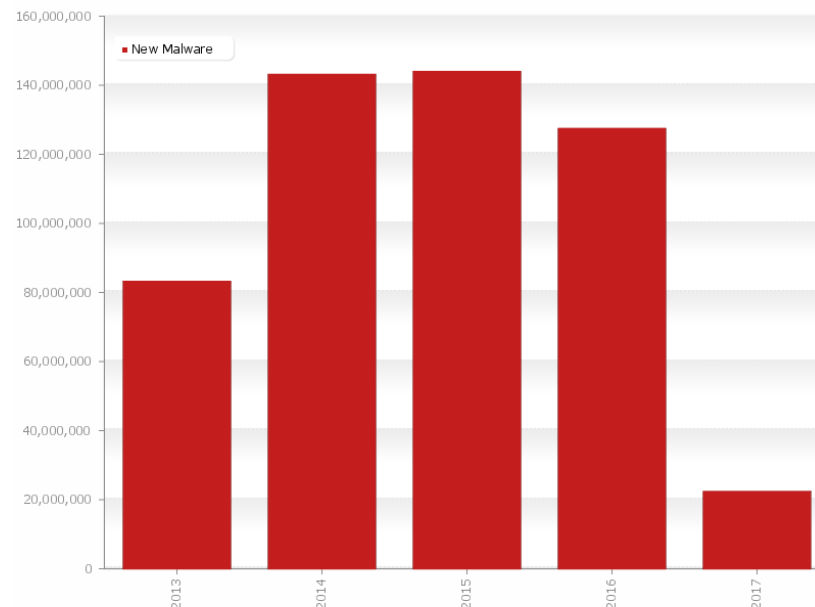
Smartphone Privacy Invasion in action

Total Malware (2013 – 2017)



Copyright © AV-TEST GmbH, www.av-test.org

New Malware (2013 – 2017)



Last update: 03-20-2017 10:38

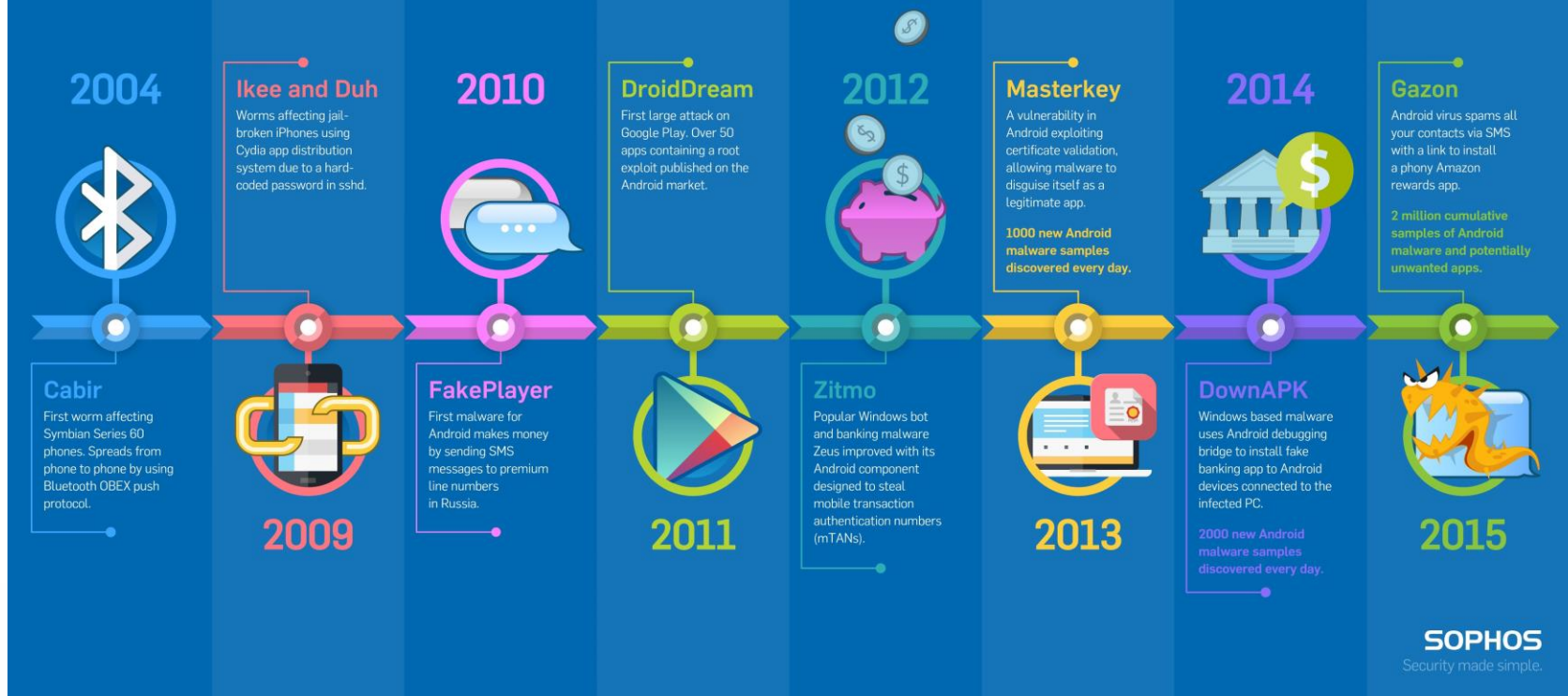
Copyright © AV-TEST GmbH, www.av-test.org



PRIVACY FLAG

Smartphone Privacy Invasion in action

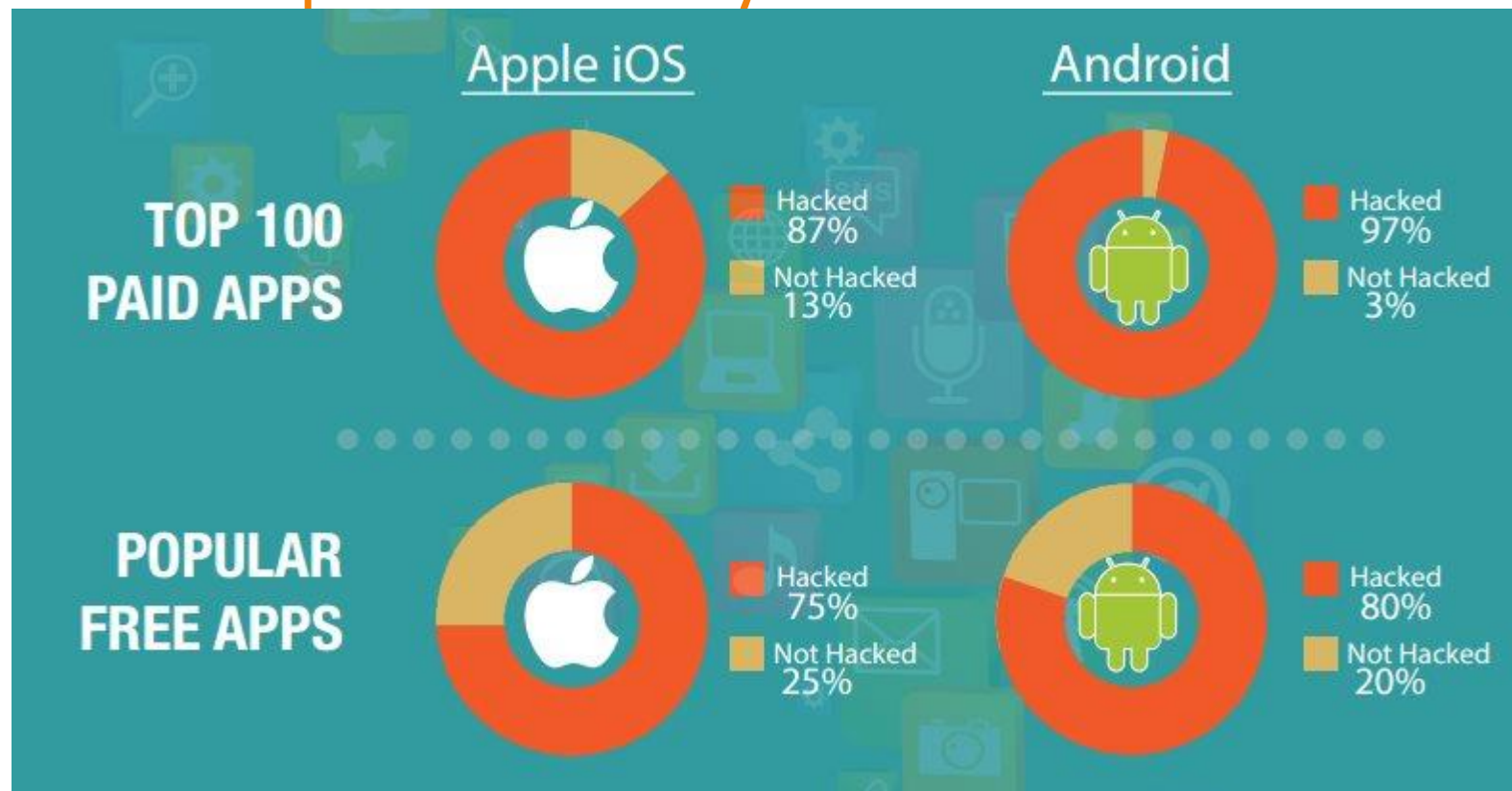
Malware Goes Mobile: Timeline of Mobile Threats, 2004 – 2015





PRIVACY FLAG

Smartphone Privacy Invasion in action



2014 results



PRIVACY FLAG

Web Privacy Invasion in action

Device fingerprinting is the capability of a site to identify a visiting user via configuration settings or other observable characteristics. In the "ideal" case, all web client machines would have a different fingerprint value (diversity), and that value would never change (stability). Panopticlick demonstrates the kind of information obtained:

Panopticlick

How Unique – and Trackable – Is Your Browser?

Your browser fingerprint appears to be unique among the 6,133,141 tested so far.



PRIVACY FLAG

Crowdsourcing monitoring of privacy risks with distributed agents

The Top25 Web Privacy Threat Matrix

	The problem to address	Output
1	Does the website provide data encryption (SSL/TLS)?	True / False
2	Does the website provide HSTS?	True / False
3	Is the encryption method (cipher suite) negotiated between client and server considered as secure?	True / False
4	What information does the website/server directly learn about a user (using forms)?	submitted information
5	Does the website use a trustworthy certification chain?	True / False
6	Does the website use Certificate pinning?	True / False
7	Which communication parties is data transferred to?	list of parties
8	Does the website use HTTP cookies?	[0...n]
9	Does the website use Third party cookies?	[0...n]
10	Does the site exploits users Web history?	True / False
11	Does the website use HTML5 Web SQL database	True / False
12	Does the website use LSOs?	[0...n]
13	Does the website use Supercookies?	[0...n]

	The problem to address	Output
14	Does the website use technologies with known security issues - PDF?	True / False
15	Does the website use known fingerprinting techniques?	[0...n]
16	Does the website use technologies with known security issues - Flash?	True / False
17	Does the website contain links to malicious sites (Google's Safe browsing API)?	[0...n]
18	Does the website use potentially dangerous advanced HTML5 APIs: Web Audio API?	True / False
19	Does the website use potentially dangerous advanced HTML5 APIs: WebRTC?	True / False
20	Does the website use potentially dangerous advanced HTML5 APIs: Geolocation (GPS)?	True / False
21	Does the website use technologies with known security issues - ActiveX?	True / False
22	Does the website use technologies with known security issues - Java?	True / False
23	Does the website use technologies with known security issues - Silverlight?	True / False
24	Does the website use HTML5 Local Storage?	True / False
25	Does the website comply with any known privacy policy eTrust, P3P, published privacy policy?	True / False



PRIVACY FLAG

Browsers: The weak link in Web Privacy

Browserscope is a community-driven project for profiling web browsers. The goals are to foster innovation by tracking browser functionality and to be a resource for web developers.

Top Browsers																			
name	score	postMessage	JSON.parse	toStaticHTML	httpOnly cookies	X-Frame-Options	X-Content-Type-Options	Block reflected XSS	Block location spoofing	Block JSON hijacking	Block XSS in CSS	Sandbox attribute	Origin header	Strict Transport Security	Block cross-origin CSS attacks	Cross Origin Resource Sharing	Block visited link sniffing	Content Security Policy	# Tests
<input type="checkbox"/> Chrome 32 →	15/17	yes	yes	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	797
<input type="checkbox"/> Firefox 26 →	13/17	yes	yes	no	yes	yes	no	no	yes	yes	yes	yes	no	yes	yes	yes	yes	yes	873
<input type="checkbox"/> IE 9 →	13/17	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	no	no	yes	yes	yes	no	3640
<input type="checkbox"/> IE 10 →	14/17	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	no	yes	yes	yes	no	1291
<input type="checkbox"/> IE 11 →	14/17	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	no	yes	yes	yes	no	2325
<input type="checkbox"/> Safari 7.0.1 →	14/17	yes	yes	no	yes	yes	no	yes	yes	yes	yes	yes	yes	no	yes	yes	yes	yes	57
<input checked="" type="checkbox"/> Chrome 34 →	16/17	yes	yes	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	793
<input type="checkbox"/> Firefox 27 →	13/17	yes	yes	no	yes	yes	no	no	yes	yes	yes	yes	no	yes	yes	yes	yes	yes	604
<input type="checkbox"/> Android 2.3 →	10/17	yes	yes	no	no	yes	no	no	yes	yes	yes	yes	yes	no	yes	yes	no	no	494
<input type="checkbox"/> Android 4 →	12/17	yes	yes	no	yes	yes	no	no	yes	yes	yes	yes	yes	no	yes	yes	yes	no	1415
<input type="checkbox"/> Blackberry 7 →	13/17	yes	yes	no	yes	yes	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	26
<input checked="" type="checkbox"/> Chrome Mobile 18 →	16/17	yes	yes	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	58
<input type="checkbox"/> IEMobile 9 →	13/17	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	no	no	yes	yes	yes	no	33
<input type="checkbox"/> IEMobile 10 →																			0
<input type="checkbox"/> iPhone 7 →																			0
Compare Browsers																			
● We think you're using Chrome 46.0.2490 12406 tests from 15 browsers Downloads: json pickle csv Link to this page																			



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG

Browsers: Security != Privacy

All modern browsers have a “Do not track” option

Chrome



- Has discrete privacy settings
- Google stores a lot of information on their servers but none of it is used to identify users according to google
- There is no clear indication for the duration these data are stored.

Firefox



- Clearly explains in their privacy policy what information is collected based on the features used.
- All of the information sent is opt-in, not opt-out, and none of it is personally identifiable
- The privacy policy also includes information about what Mozilla shares with third parties upon request.

Other browsers:



- Opera collects very little information and all of it is stored as aggregate
- Apple has a global privacy policy, as well as a commitment to customer privacy
- Internet explorer has different privacy policies with each new version

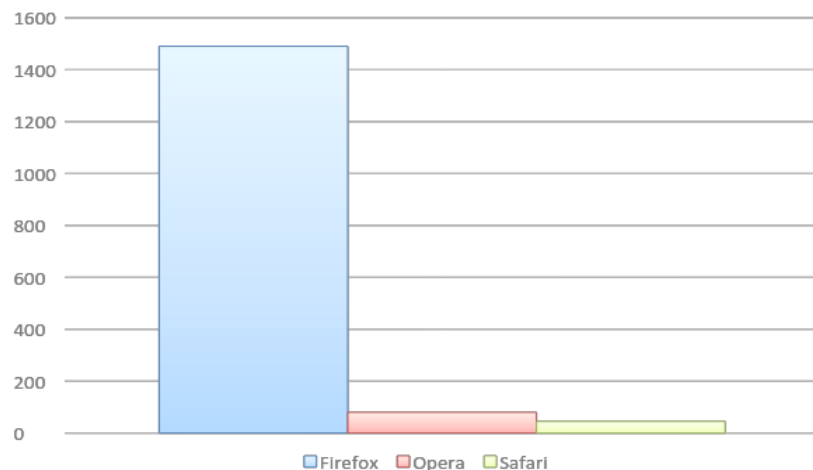
Bottomline: Firefox is the most privacy enabled browser, with a clear privacy policy. But, in essence all browsers are similar regarding privacy issues.



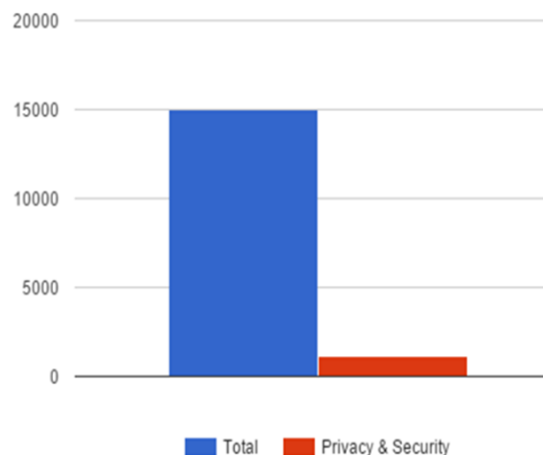
PRIVACY FLAG

Browsers: The weak link in Web Privacy

Number of privacy and security related add-ons



Browser overall AddOns



Mozilla Firefox AddOns

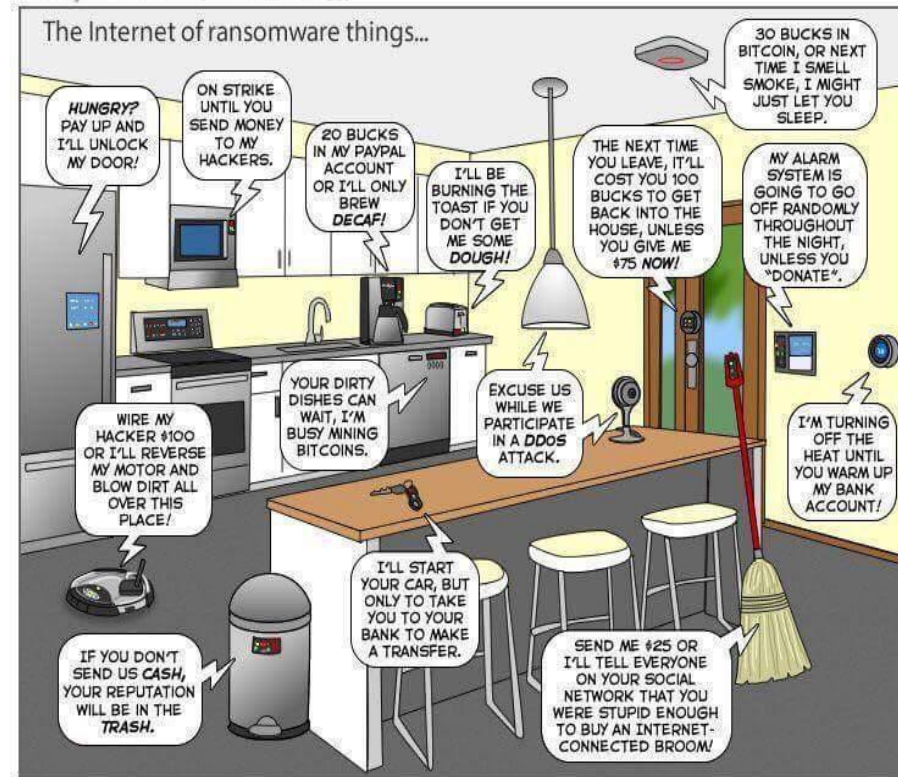


PRIVACY FLAG

lessons NOT learned: IoT (in)security

- ☎ “Internet of things” becomes part of our life
 - ❖ Animate and inanimate will be interconnected
 - ❖ Unique identification between each other
- ☎ Billion devices are connected already
- ☎ More and more devices will be connected in the near future
- ☎ The more the devices the largest the **ATTACK** surface

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon.com/joyoftech

joyoftech.com



PRIVACY FLAG

lessons NOT learned: IoT (in)security

SHODAN

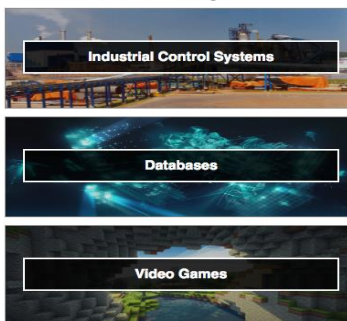
EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

TAKE A TOUR

FREE SIGN UP

Featured Categories



Top Voted

7,843	Webcam best ip cam search I have found yet.	
webcam	surveillance	cams
		2010-03-15
2,841	Cams admin admin	
cam	webcam	
		2012-02-06
1,746	Netcam Netcam	
netcam		
		2012-01-13

Meet the "Mirai" IoT Botnet



briankrebs
@briankrebs

Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen. 665 Gbps. Site's still up. #FAIL
3:02 AM - 21 Sep 2016

Largest DDoS attack the Internet has ever seen!
665 Gbps!

Source KrebsOnLine: <https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/>
Bashlight + Mirai botnets > 1.400.000 bots
@665 Gbps DDoS
Previous max: 363 Gbs DDoS

Source: <http://www.shodanhq.com/>



Co-funded by the
European Union



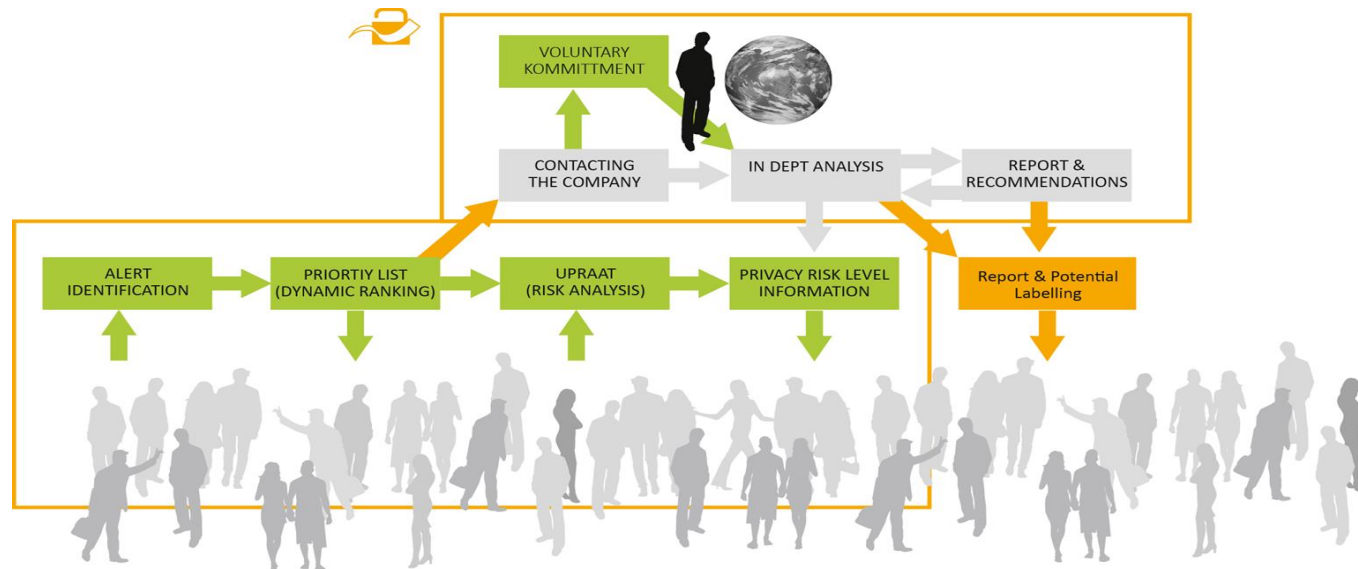
Co-funded by the
Swiss Confederation



PRIVACY FLAG

Privacy Challenges

-  None of the above solutions provides a holistic approach (web, mobile, IoT)
-  Techno-legal challenges
-  Technical vs Human solution





PRIVACY FLAG



About PrivacyFlag

MAIN GOALS OF THE PROJECT



Privacy Flag is developing a highly scalable privacy monitoring and protection solution with:

- Crowdsourcing mechanisms to identify, monitor and assess privacy-related risks;
- Privacy monitoring agents to identify suspicious activities and applications;
- Universal Privacy Risk Area Assessment Tool and methodology tailored on European norms on personal data protection;
- Personal Data Valuation mechanism;
- Privacy enablers against traffic monitoring and fingerprinting;
- User friendly interface informing on the privacy risks when using an application or website.



Privacy Flag is building a global knowledge database of identified privacy risks, together with online services to support companies and other stakeholders in becoming privacy-friendly, including:

- In-depth privacy risk analytical tool and services;
- Voluntary legally binding mechanism for companies located outside Europe to align with and abide to European standards in terms of personal data protection;
- Services for companies interested in being privacy friendly;
- Researching the potential for standardization, labelling and certification.



Privacy Flag will work in close interaction with standardization bodies and will actively disseminate towards the public and specialized communities, such as ICT lawyers, policy makers and academics.

11 European partners, including SMEs and a large telco operator, bring their complementary technical, legal, societal and business expertise; strong links with standardization bodies and international fora; and outcomes from over 20 related research projects. It intends to pave the way to a privacy defenders community.

News



National and Kapodistrian University of Athens



Co-funded by the European Union







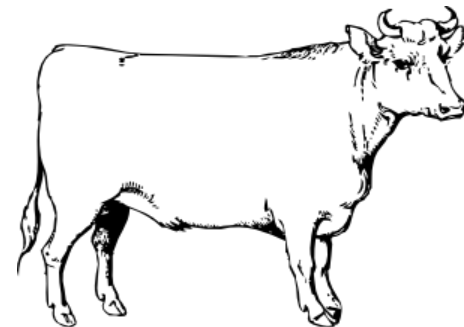
Co-funded by the Swiss Confederation



PRIVACY FLAG

Advantages of crowdsourcing






-  Mobilizes large crowds of people who **volunteer** to contribute towards the collection of environmental data and information or their behavior itself.
-  The experimenters can derive **useful global information** about the evolution of a physical phenomenon or explain an observed macroscopic behavior of the crowd population itself
-  Collecting data from a large number of individuals leads to **accurate intelligence**.
-  **Example:** 800 people estimated the weight of a slaughtered and dressed ox, with 99% accuracy of the true weight.





PRIVACY FLAG

Crowdsourcing Issues

-  **Crowdsourcing** characterizes large scale experimental set-ups which engage large numbers of individuals.
-  For people to be willing to engage in the crowdsourcing scheme they need to **trust** the crowdsourcing authority.
-  Individuals can be offered diverse **incentives** (monetary or other) to compensate for their participation and the use of their mobile phones and other devices
-  **Machine learning** and other techniques can be used to process the individuals' data and extract useful information
-  Using internet enabled devices, they interact with specialized information systems that collect and process information.

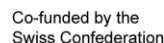
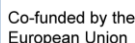
AND NOW: TOP BUSINESS BESTSELLER
...and thought provoking as The Tipping Point by
Malcolm Gladwell... The Wisdom of Crowds rings far and wide.
—The Boston Globe

THE WISDOM
OF CROWDS
JAMES
SUROWIECKI
WITH A NEW AFTERWORD BY THE AUTHOR





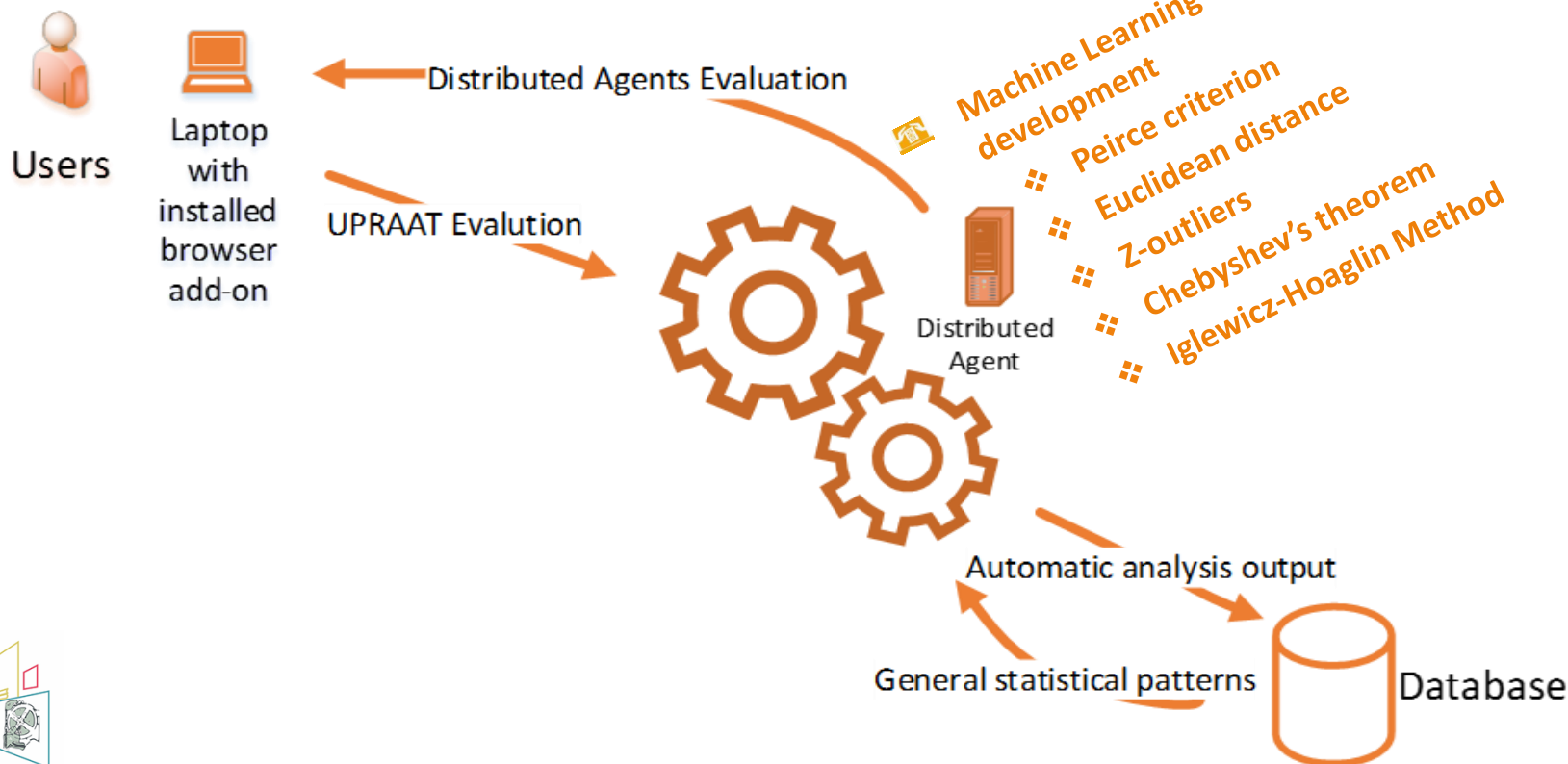
- 📞 Collect and process few bits of information from a large number of systems (crowdsourcing) rather than a vast amount of data from a limited number of systems (traditional approach)
- 📞 The sum of the PrivacyFlag manual and automatic analysis is the crowdsourced decision
- 📞 The more users , the better the accuracy





PRIVACY FLAG

The Privacy Flag Crowdsourcing model

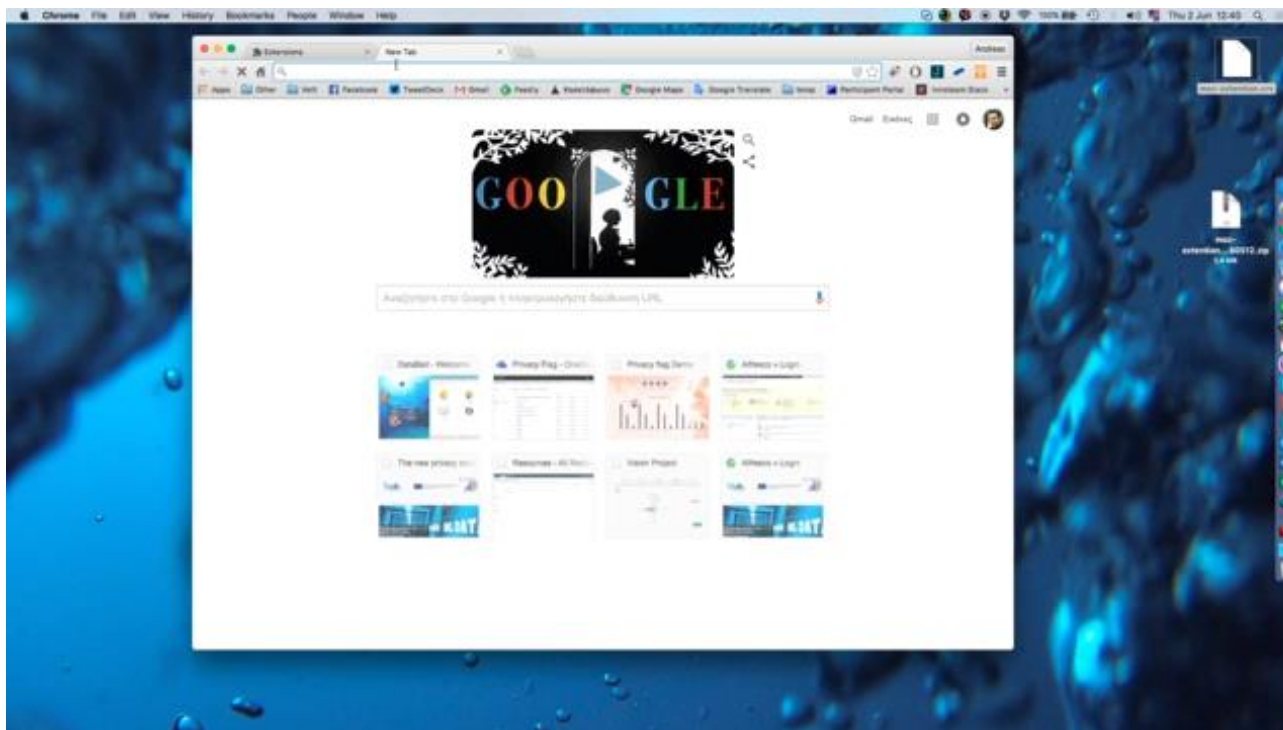




PRIVACY FLAG

Crowdsourcing monitoring of privacy risks with distributed agents and humans

The Top25Threat Matrix is analyzed automatically as well as manually





PRIVACY FLAG

Crowdsourcing monitoring of privacy risks with distributed agents - SmartPhones

 Crowdsourcing: Let the users choose what is (privacy-related) important: Borda count

 Different privacy perspective of a businessman (my contacts) than of a teenager (my photos and sms)

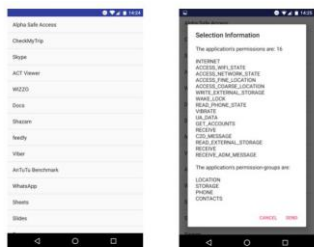


Figure 4.3: First version of the Privacy Flag application



Privacy Flag

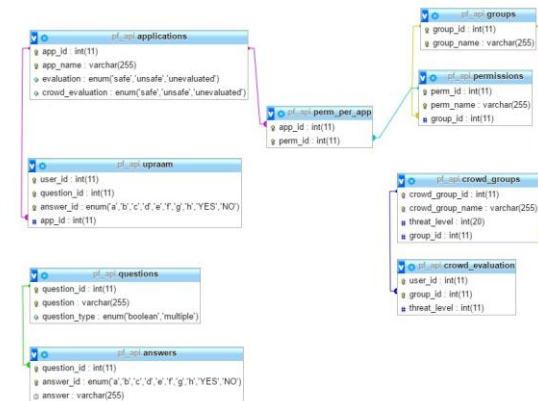
Crowdsourcing the Threat Level of Android Permissions

Please order the Android Permissions Groups listed below from the most dangerous to the least one (i.e. the most dangerous group should be placed in Level 1).

So let us know how privacy threatening do you think a permission access to your calendar / contacts / microphone?

Everything that has to do with calendar	Select level *
Everything that has to do with camera	Select level *
Everything that has to do with contacts	Select level *
Everything that has to do with location	Select level *
Everything that has to do with microphone	Select level *

Select





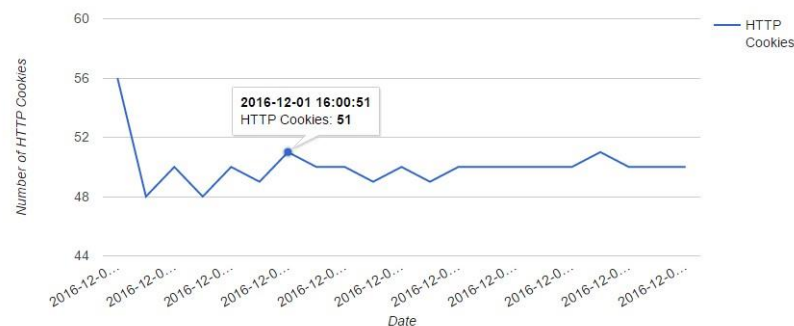
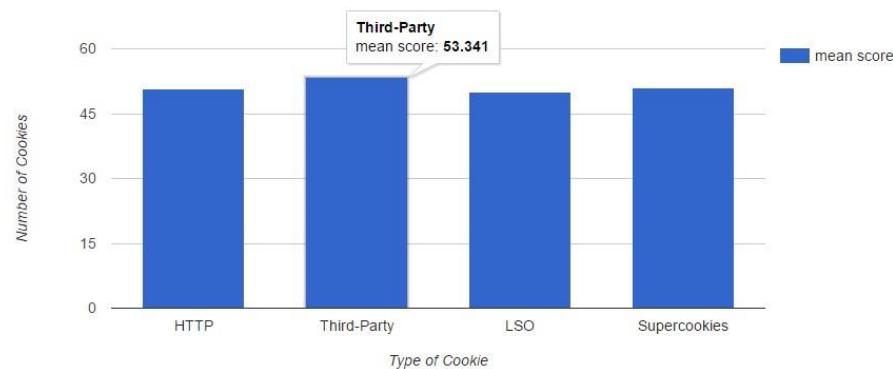
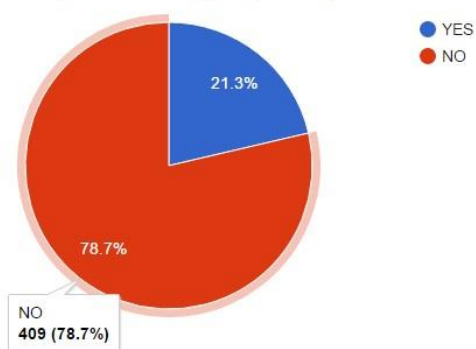
PRIVACY FLAG

PrivacyFlag Threat Observatory

http://150.140.193.133:2080/privacy/addon/new_metrics.php

Various metrics are depicted.

Websites that provide data encryption (SSL/TLS)





PRIVACY FLAG

Last words



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



National and Kapodistrian
University of Athens



**PRIVACY
FLAG**



Co-funded by the
European Union



Co-funded by the
Swiss Confederation