Privacy Flag Observatory

Dr. Vasileios Vlachos
CTI / University of Applied Sciences – TEI of Thessaly

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

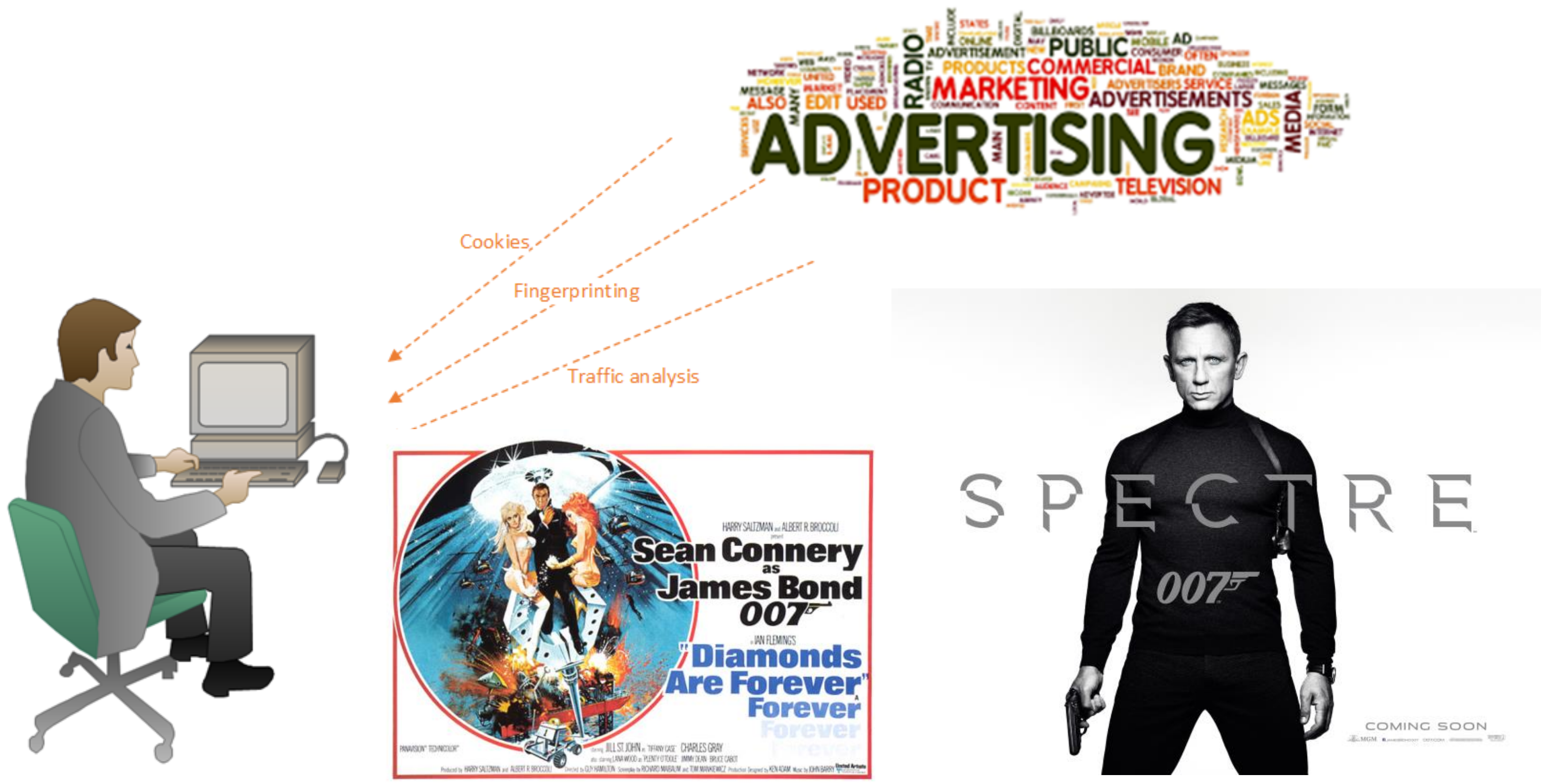
About CTI

- 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 7 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)

Co-funded by the European Union

Co-funded by the Swiss Confederation

~~Future~~ Current threats



Third party tracker or advertising company

Cookies

Fingerprinting

Traffic analysis

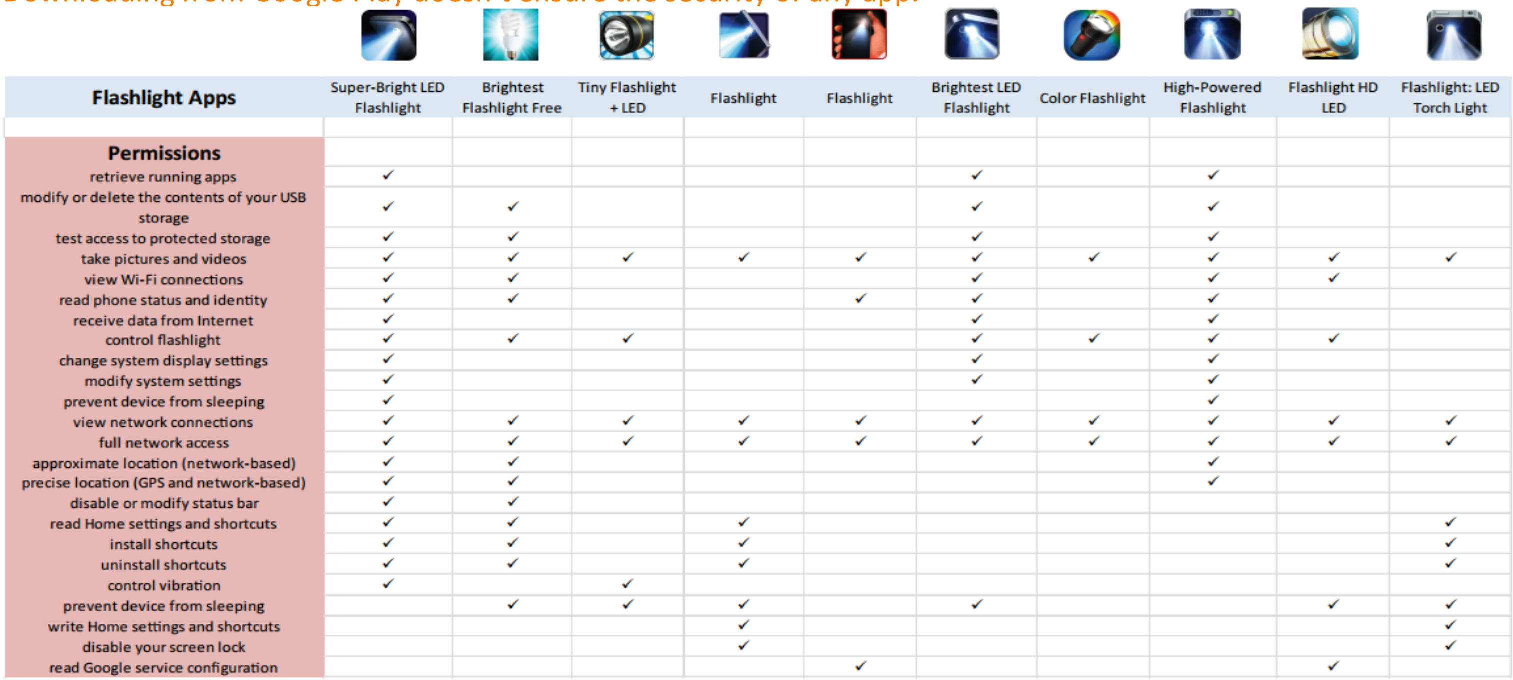
PrivacyFlag AddOn User

Co-funded by the European Union

Co-funded by the Swiss Confederation

Smartphone Privacy Invasion in action

- ☎ It was revealed that the most commonly used flashlight apps are secretively 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.



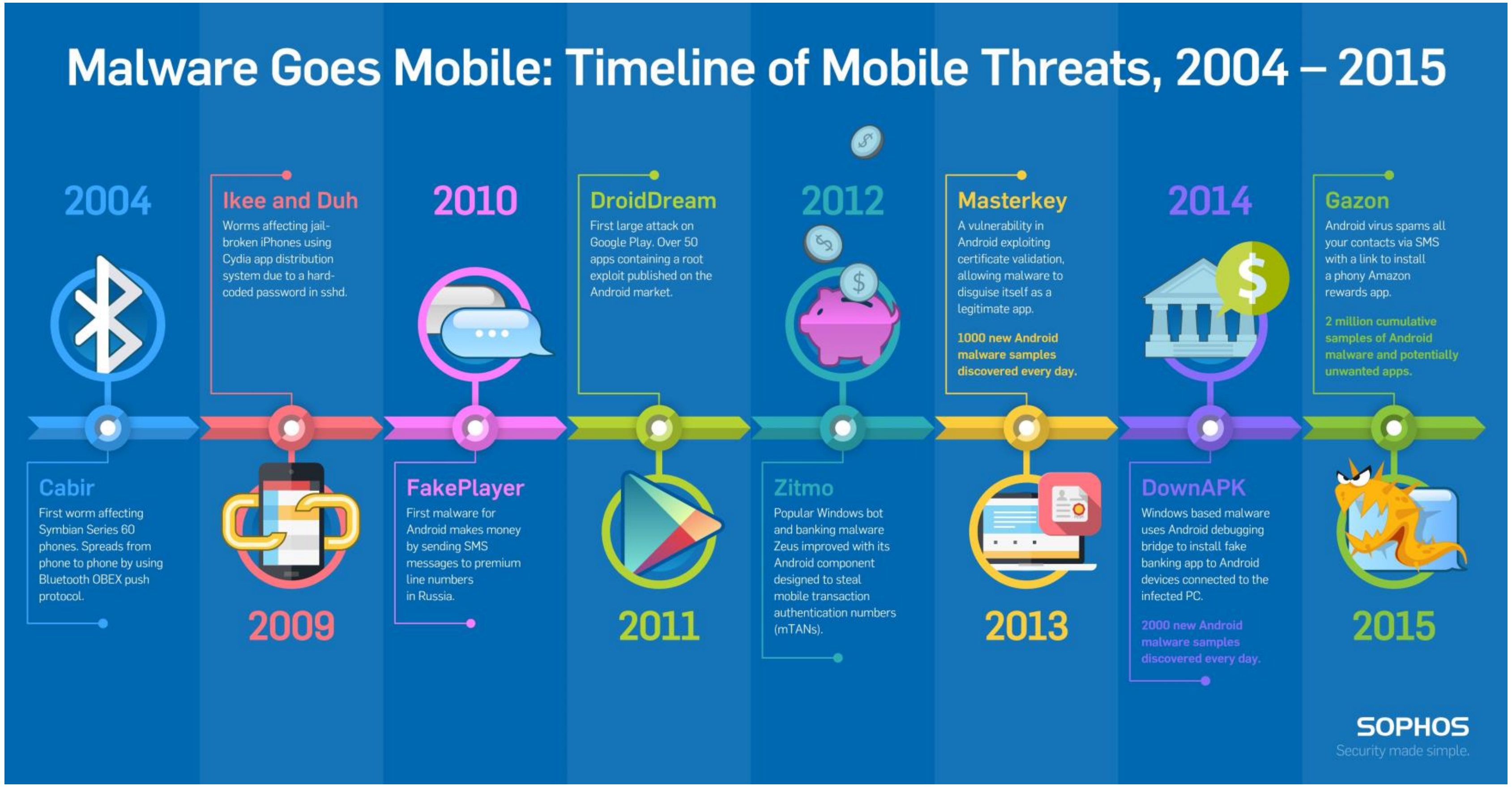
Flashlight Apps	Super-Bright LED Flashlight	Brightest Flashlight Free	Tiny Flashlight + LED	Flashlight	Flashlight	Brightest LED Flashlight	Color Flashlight	High-Powered Flashlight	Flashlight HD LED	Flashlight: LED Torch Light
Permissions										
retrieve running apps	✓					✓		✓		
modify or delete the 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					✓				✓	

Source:TheHackerNews https://thehackernews.com/

Co-funded by the
European Union

Co-funded by the
Swiss Confederation

Smartphone Privacy Invasion in action



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

2004

Cabir
First worm affecting Symbian Series 60 phones. Spreads from phone to phone by using Bluetooth OBEX push protocol.

2009

Ikee and Duh
Worms affecting jail-broken iPhones using Cydia app distribution system due to a hard-coded password in sshd.

2010

FakePlayer
First malware for Android makes money by sending SMS messages to premium line numbers in Russia.

2011

DroidDream
First large attack on Google Play. Over 50 apps containing a root exploit published on the Android market.

2012

Zitmo
Popular Windows bot and banking malware Zeus improved with its Android component designed to steal mobile transaction authentication numbers (mTANs).

2013

Masterkey
A vulnerability in Android exploiting certificate validation, allowing malware to disguise itself as a legitimate app.

1000 new Android malware samples discovered every day.

2014

DownAPK
Windows based malware uses Android debugging bridge to install fake banking app to Android devices connected to the infected PC.

2000 new Android malware samples discovered every day.

2015

Gazon
Android virus spams all your contacts via SMS with a link to install a phony Amazon rewards app.

2 million cumulative samples of Android malware and potentially unwanted apps.

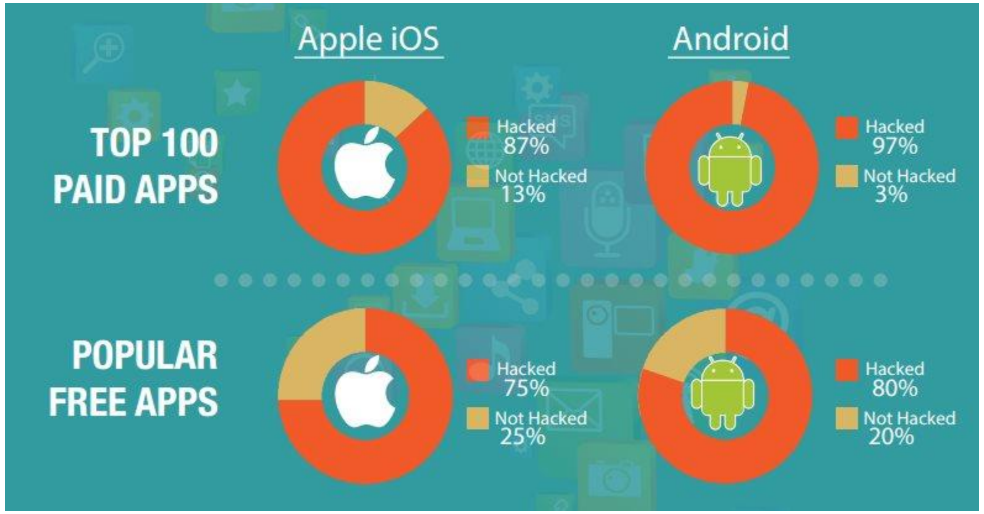
SOPHOS
Security made simple.

SOPHOS

Co-funded by the
European Union

Co-funded by the
Swiss Confederation

Smartphone Privacy Invasion in action



ARXAN

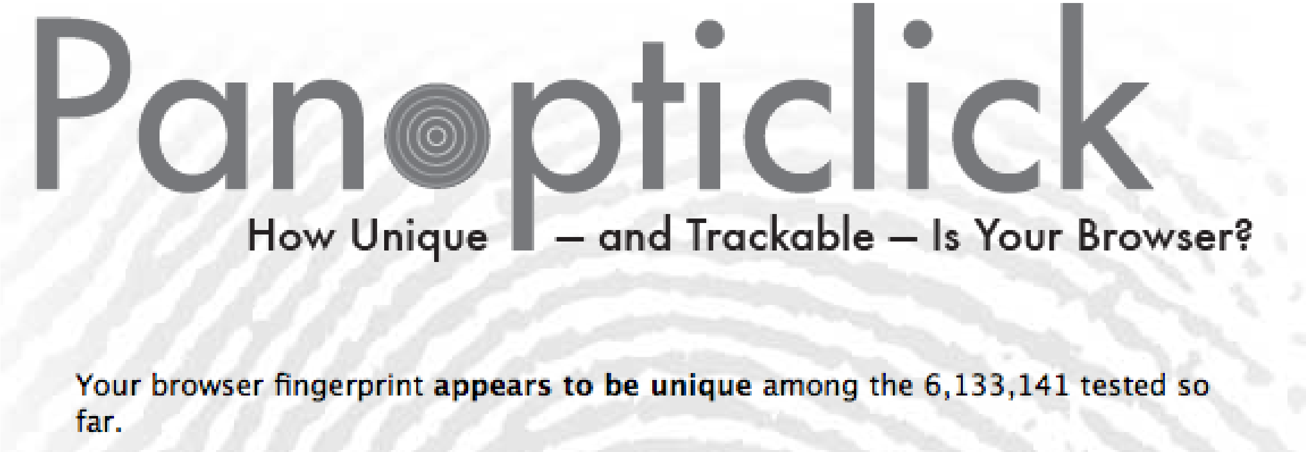
2014 results

Co-funded by the European Union

Co-funded by the Swiss Confederation

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:



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

Co-funded by the European Union

Co-funded by the Swiss Confederation

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

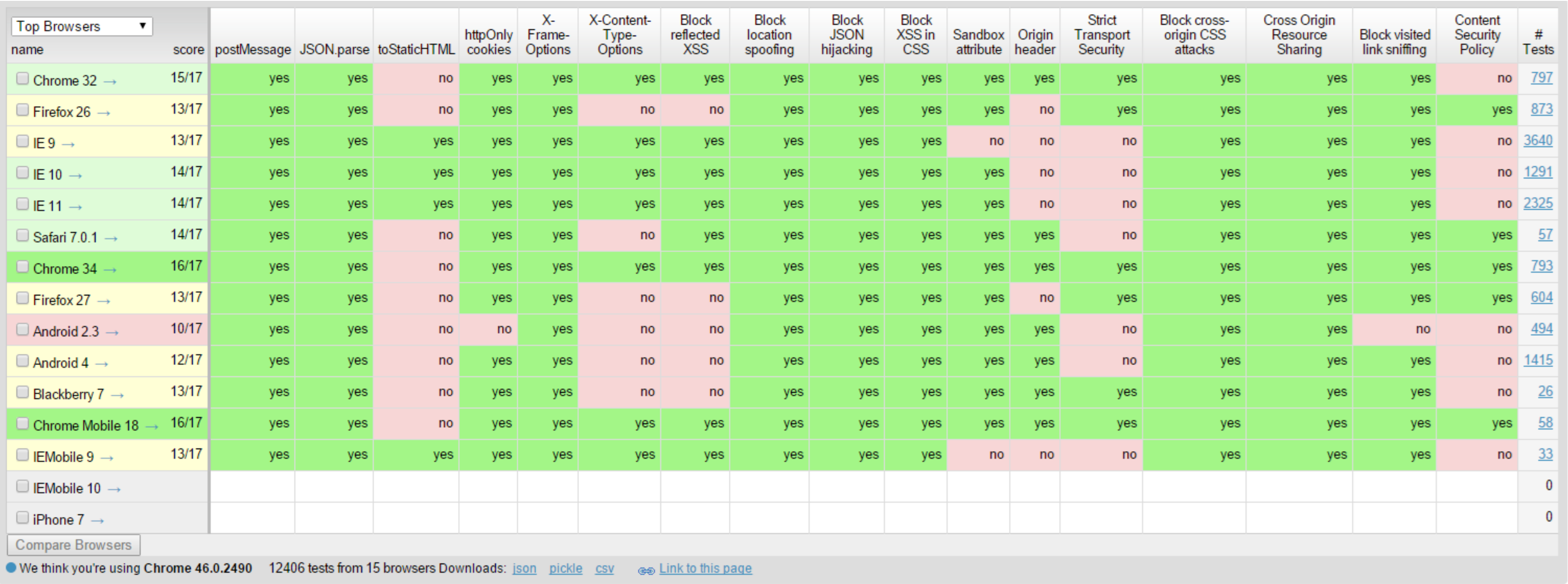
CTI "DIOPHANTUS" computer technology institute & press

Co-funded by the European Union

Co-funded by the Swiss Confederation

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
☐ Chrome 32 →	15/17	yes	yes	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	797
☐ Firefox 26 →	13/17	yes	yes	no	yes	yes	no	no	yes	yes	yes	yes	no	yes	yes	yes	yes	yes	873
☐ IE 9 →	13/17	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	no	no	yes	yes	yes	no	3640
☐ IE 10 →	14/17	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	no	yes	yes	yes	no	1291
☐ IE 11 →	14/17	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	no	yes	yes	yes	no	2325
☐ Safari 7.0.1 →	14/17	yes	yes	no	yes	yes	no	yes	yes	yes	yes	yes	yes	no	yes	yes	yes	yes	57
☐ Chrome 34 →	16/17	yes	yes	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	793
☐ Firefox 27 →	13/17	yes	yes	no	yes	yes	no	no	yes	yes	yes	yes	no	yes	yes	yes	yes	yes	604
☐ Android 2.3 →	10/17	yes	yes	no	no	yes	no	no	yes	yes	yes	yes	yes	no	yes	yes	no	no	494
☐ Android 4 →	12/17	yes	yes	no	yes	yes	no	no	yes	yes	yes	yes	yes	no	yes	yes	yes	no	1415
☐ Blackberry 7 →	13/17	yes	yes	no	yes	yes	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	26
☐ Chrome Mobile 18 →	16/17	yes	yes	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	58
☐ IEMobile 9 →	13/17	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	no	no	yes	yes	yes	no	33
☐ IEMobile 10 →																			0
☐ iPhone 7 →																			0

● 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

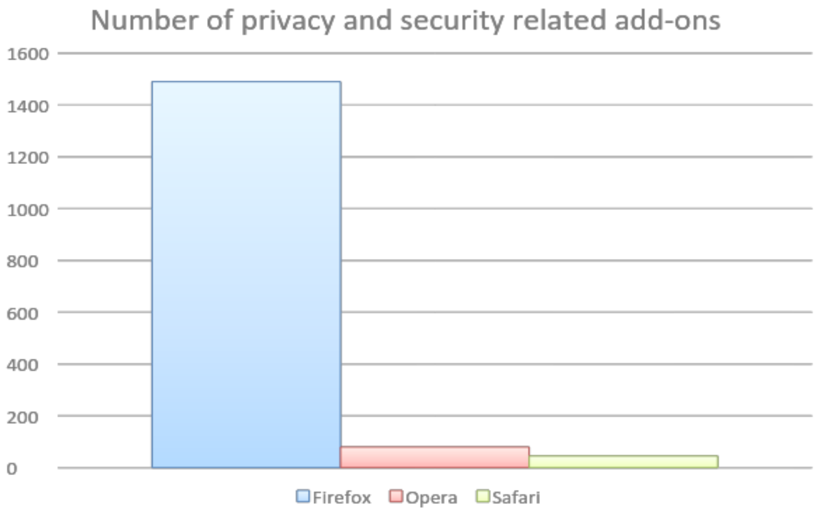
Bottomline: Firefox is the most privacy enabled browser, with a clear privacy policy. But, in essence all browsers are similar regarding privacy issues.

Co-funded by the European Union

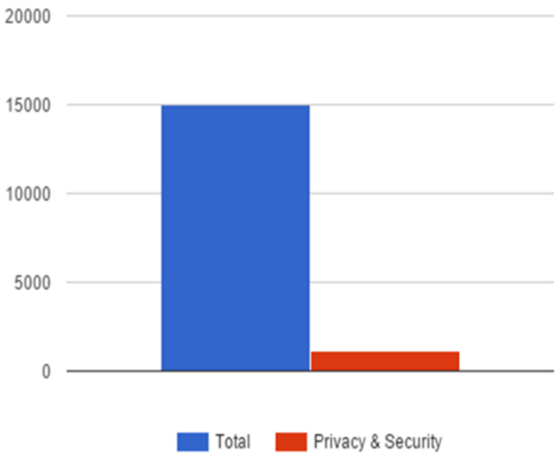
Co-funded by the Swiss Confederation

PRIVACY FLAG

Browsers: The weak link in Web Privacy



Browser overall AddOns



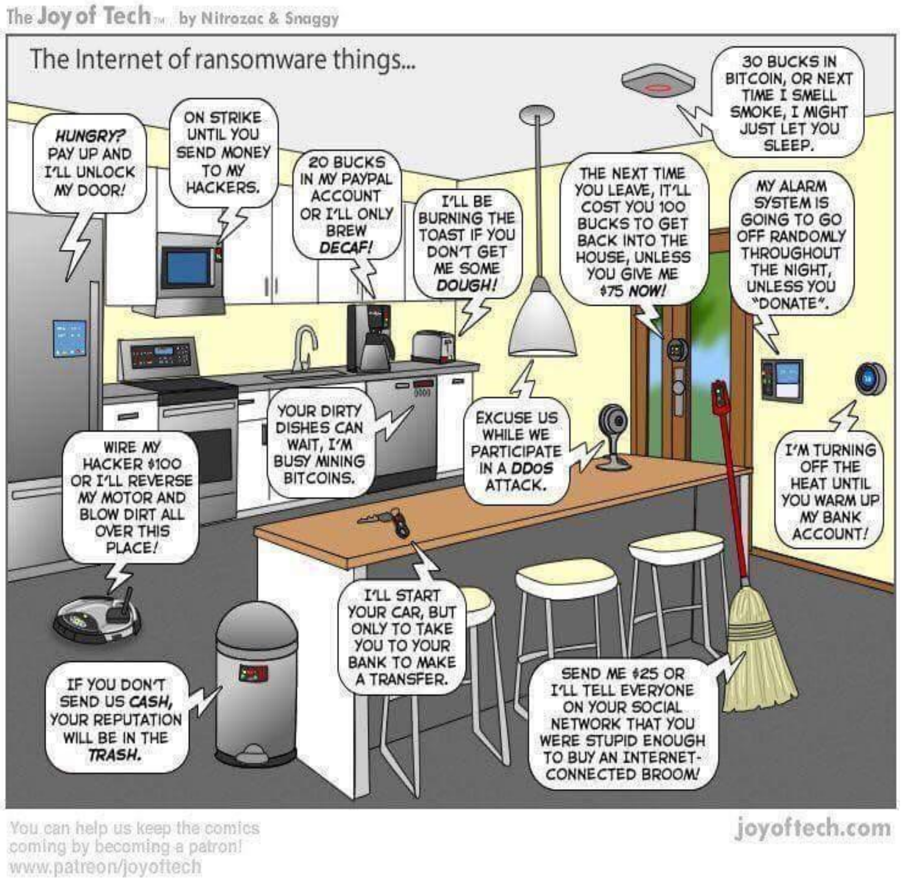
Mozilla Firefox AddOns

Co-funded by the European Union

Co-funded by the Swiss Confederation

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

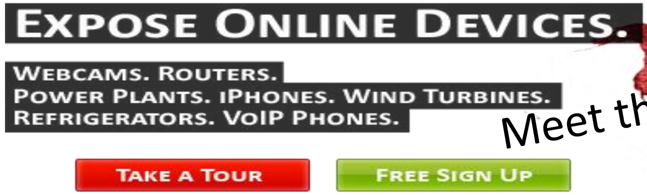

The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

Co-funded by the European Union

Co-funded by the Swiss Confederation

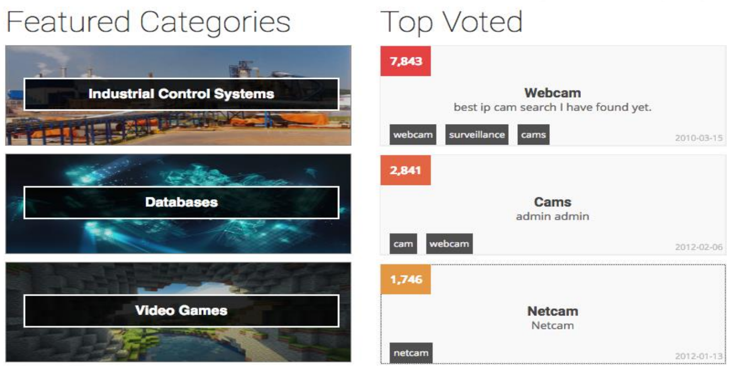
lessons NOT learned: IoT (in)security

SHODAN



EXPOSE ONLINE DEVICES.

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



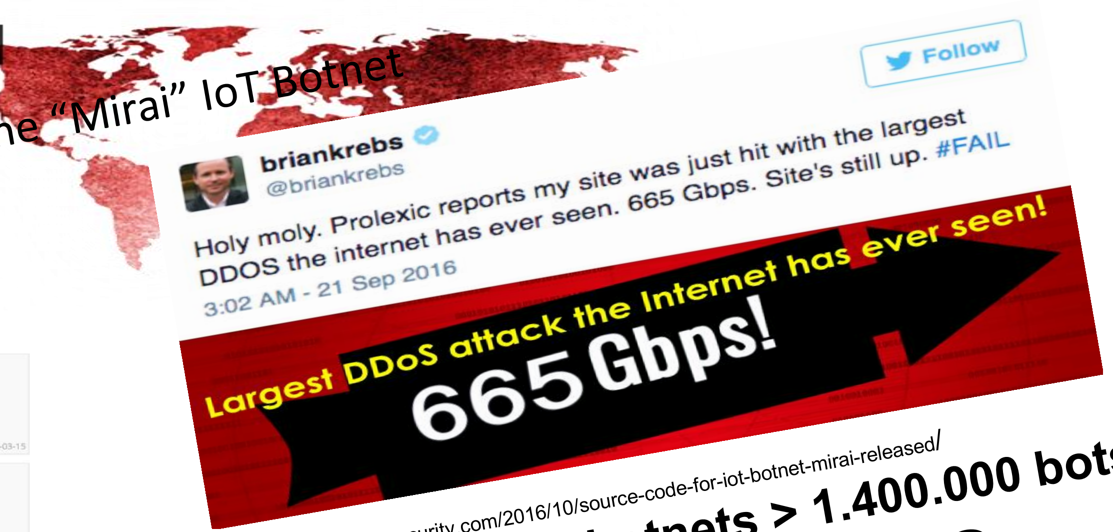
Featured Categories

- Industrial Control Systems
- Databases
- Video Games

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

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

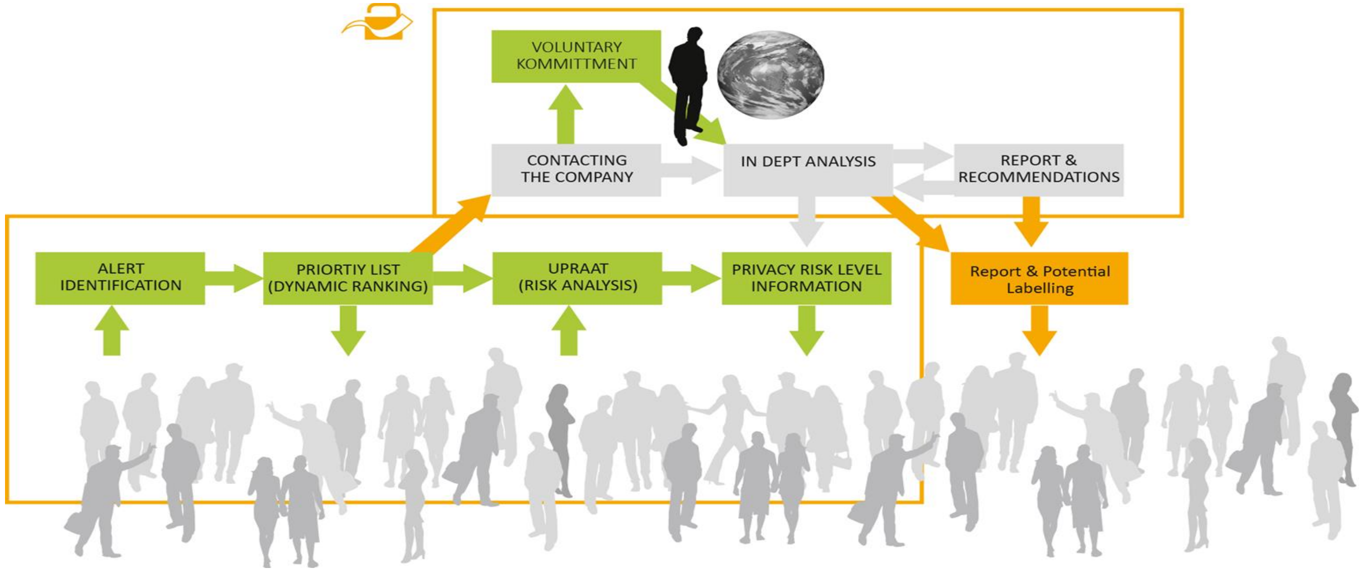
Source: *http://www.shodanhq.com/*

Co-funded by the European Union

Co-funded by the Swiss Confederation

Privacy Challenges

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



Co-funded by the European Union

Co-funded by the Swiss Confederation

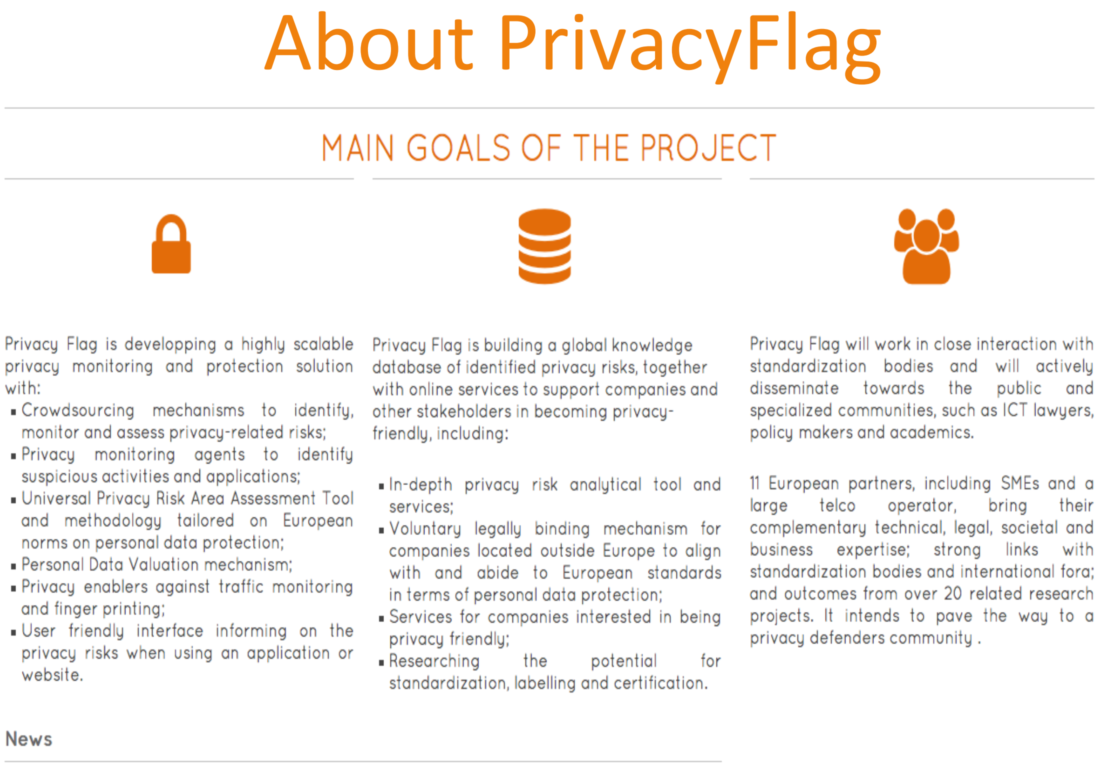
MY DATA
PRIVACY FLAG

OTE

CTI "DIOPHANTUS" computer technology institute & press

velti

uni.lu
UNIVERSITÉ DU LUXEMBOURG



About PrivacyFlag

MAIN GOALS OF THE PROJECT

Privacy Flag is developping 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 finger printing;
- 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

DUNAV NET

University of BRISTOL

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

LULEÅ UNIVERSITY OF TECHNOLOGY

National and Kapodistrian University of Athens

HWCommunications
Cyber Security and Resilience

MANDAT INTERNATIONAL

Archimede Solutions SARL

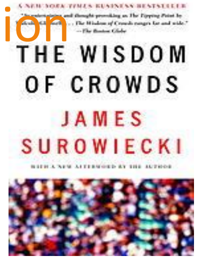
Co-funded by the European Union

Co-funded by the Swiss Confederation

PRIVACY FLAG

Crowdsourcing

- **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.



Co-funded by the European Union

Co-funded by the Swiss Confederation

Crowdsourcing - How can help PrivacyFlag

- 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

Co-funded by the
European Union

Co-funded by the
Swiss Confederation

Based on the Task 4.2
CROWDSOURCING MONITORING OF PRIVACY RISKS WITH DISTRIBUTED AGENTS

Co-funded by the European Union

Co-funded by the Swiss Confederation

PF Threat Observatory

Co-funded by the
European Union

Co-funded by the
Swiss Confederation

PRIVACY FLAG

Top20 become more generic to be more effective

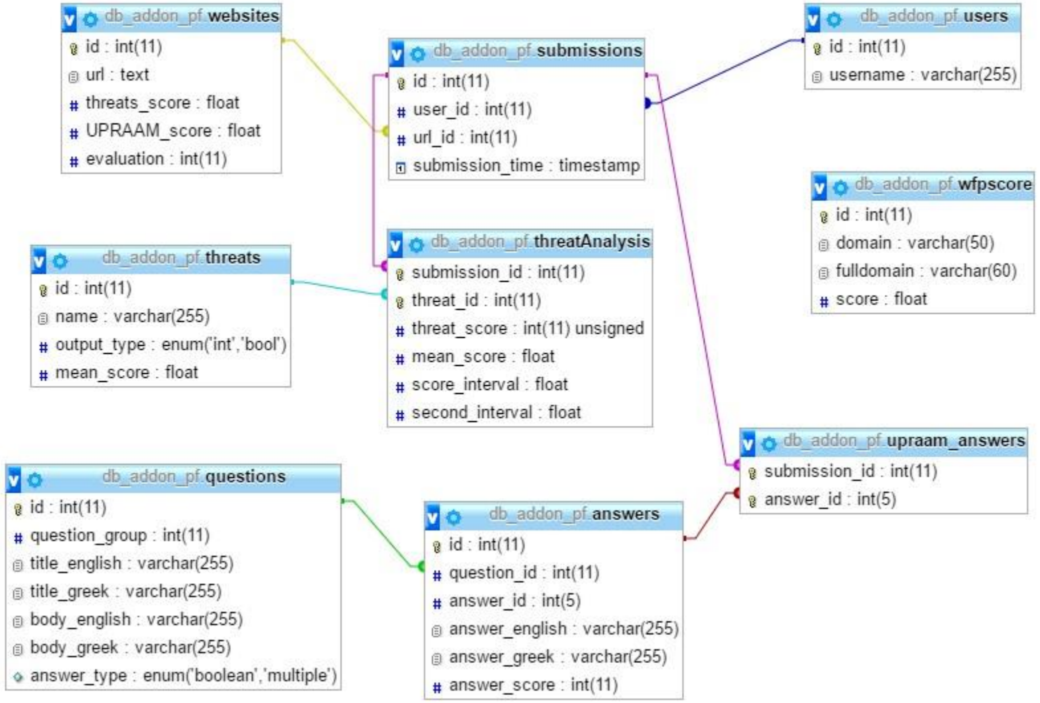
The Top20 Web Privacy Threat Matrix has been completed

	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 backward compatibility with insecure SSL or TLS versions disabled?	True / False
4	Does the website use a trustworthy certification chain?	True / False
5	Does the website use Certificate pinning?	True / False
6	Does the website use HTTP cookies?	[0…n]
7	Does the website use Third party cookies?	[0…n]
8	Does the site exploit users Web history?	True / False
9	Does the website use HTML5 Web SQL database?	True / False
10	Does the website use LSOs?	[0…n]
11	Does the website use Supercookies?	[0…n]
12	Does the website use technologies with known security issues - PDF?	True / False
13	Does the encrypted user traffic is prone to fingerprinting when accessing this website?	True / False
14	Does the website use technologies with known security issues - Flash?	True / False
15	Does the website contain links to malicious sites (Google's Safe browsing API)?	[0…n]
16	Does the website use potentially dangerous advanced HTML5 APIs: Web Audio API?	True / False
17	Does the website use potentially dangerous advanced HTML5 APIs: WebRTC?	True / False
18	Does the website use potentially dangerous advanced HTML5 APIs: Geolocation (GPS)?	True / False
19	Does the website use technologies with known security issues - ActiveX?	True / False
20	Does the website use technologies with known security issues - Java?	True / False
21	Does the website use technologies with known security issues - Silverlight?	True / False
22	Does the website use HTML5 Local Storage?	True / False
23	Does the website comply with any known privacy policy eTrust, P3P, published privacy policy?	True / False
24	Is SDNS enabled?	True / False

Co-funded by the
European Union

Co-funded by the
Swiss Confederation

The Top20Threat Matrix has been schematized to provide input to the Evaluation Component regarding the Web Privacy Threats



db_addon_pf.websites
- id : int(11)
- url : text
- threats_score : float
- UPRAAM_score : float
- evaluation : int(11)

db_addon_pf.submissions
- id : int(11)
- user_id : int(11)
- url_id : int(11)
- submission_time : timestamp

db_addon_pf.users
- id : int(11)
- username : varchar(255)

db_addon_pf.wfpscore
- id : int(11)
- domain : varchar(50)
- fulldomain : varchar(60)
- score : float

db_addon_pf.threats
- id : int(11)
- name : varchar(255)
- output_type : enum('int','bool')
- mean_score : float

db_addon_pf.threatAnalysis
- submission_id : int(11)
- threat_id : int(11)
- threat_score : int(11) unsigned
- mean_score : float
- score_interval : float
- second_interval : float

db_addon_pf.upraam_answers
- submission_id : int(11)
- answer_id : int(5)

db_addon_pf.questions
- id : int(11)
- question_group : int(11)
- title_english : varchar(255)
- title_greek : varchar(255)
- body_english : varchar(255)
- body_greek : varchar(255)
- answer_type : enum('boolean','multiple')

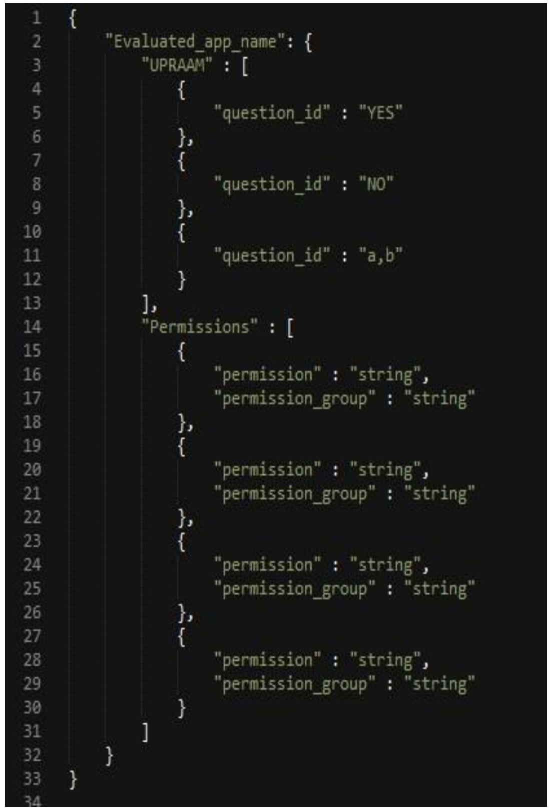
db_addon_pf.answers
- id : int(11)
- question_id : int(11)
- answer_id : int(5)
- answer_english : varchar(255)
- answer_greek : varchar(255)
- answer_score : int(11)

Co-funded by the European Union

Co-funded by the Swiss Confederation

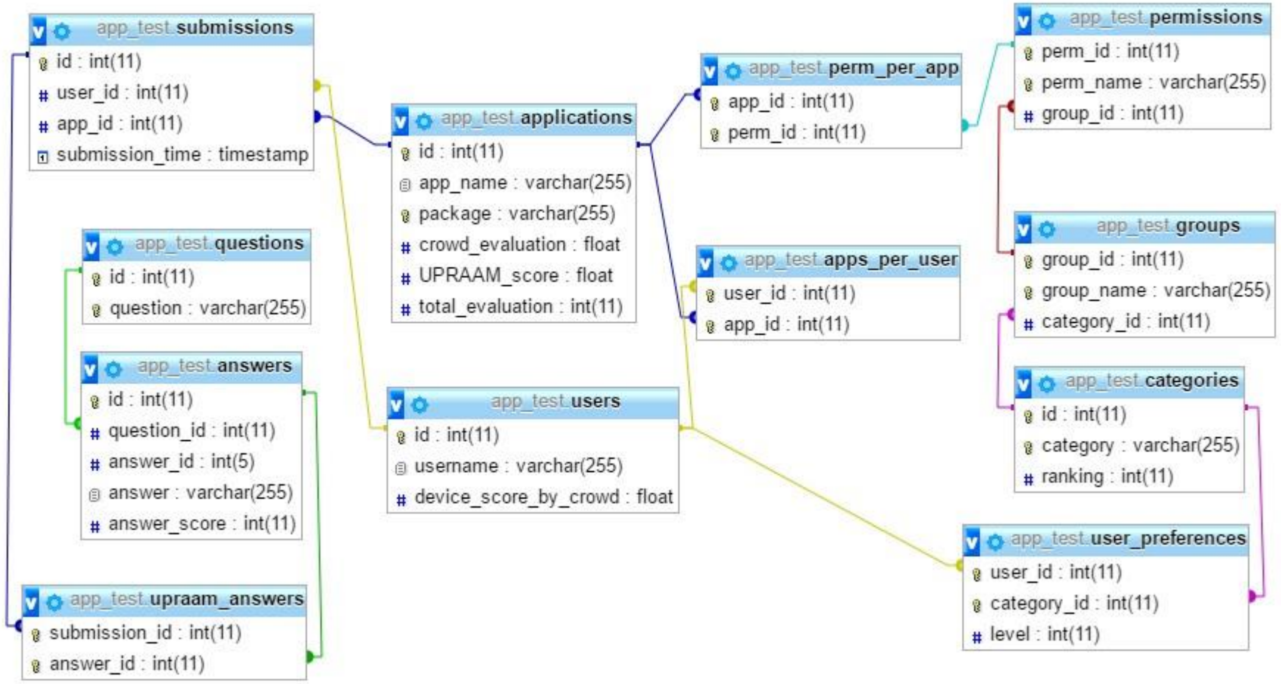
The JSON Quest!

Has been translated to the required JSON files



```
{
    "Evaluated_app_name": {
        "UPRAAM" : [
            {
                "question_id" : "YES"
            },
            {
                "question_id" : "NO"
            },
            {
                "question_id" : "a,b"
            }
        ],
        "Permissions" : [
            {
                "permission" : "string",
                "permission_group" : "string"
            },
            {
                "permission" : "string",
                "permission_group" : "string"
            },
            {
                "permission" : "string",
                "permission_group" : "string"
            },
            {
                "permission" : "string",
                "permission_group" : "string"
            }
        ]
    }
}
```

An example of the internal representation of the PF System



app_test.submissions
id : int(11)
user_id : int(11)
app_id : int(11)
submission_time : timestamp

app_test.questions
id : int(11)
question : varchar(255)

app_test.answers
id : int(11)
question_id : int(11)
answer_id : int(5)
answer : varchar(255)
answer_score : int(11)

app_test.upraam_answers
submission_id : int(11)
answer_id : int(11)

app_test.applications
id : int(11)
app_name : varchar(255)
package : varchar(255)
crowd_evaluation : float
UPRAAM_score : float
total_evaluation : int(11)

app_test.users
id : int(11)
username : varchar(255)
device_score_by_crowd : float

app_test.perm_per_app
app_id : int(11)
perm_id : int(11)

app_test.apps_per_user
user_id : int(11)
app_id : int(11)

app_test.permissions
perm_id : int(11)
perm_name : varchar(255)
group_id : int(11)

app_test.groups
group_id : int(11)
group_name : varchar(255)
category_id : int(11)

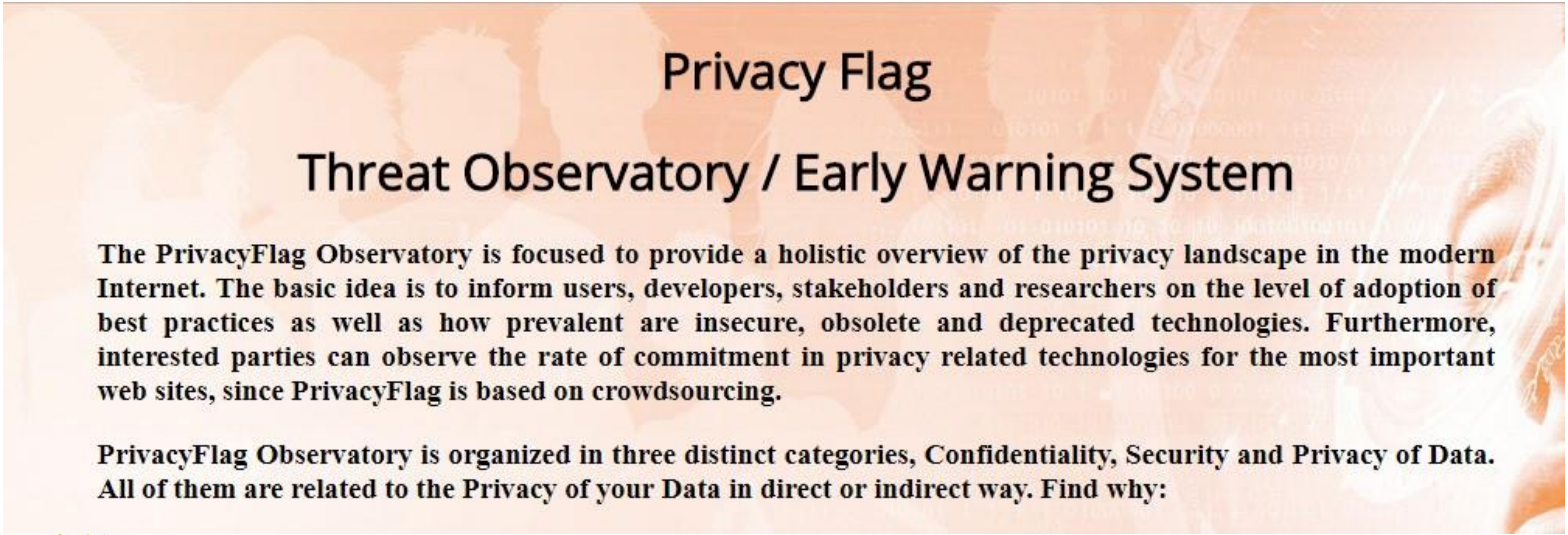
app_test.categories
id : int(11)
category : varchar(255)
ranking : int(11)

app_test.user_preferences
user_id : int(11)
category_id : int(11)
level : int(11)

Co-funded by the
European Union

Co-funded by the
Swiss Confederation

PF Threat Observatory



Privacy Flag

Threat Observatory / Early Warning System

The PrivacyFlag Observatory is focused to provide a holistic overview of the privacy landscape in the modern Internet. The basic idea is to inform users, developers, stakeholders and researchers on the level of adoption of best practices as well as how prevalent are insecure, obsolete and deprecated technologies. Furthermore, interested parties can observe the rate of commitment in privacy related technologies for the most important web sites, since PrivacyFlag is based on crowdsourcing.

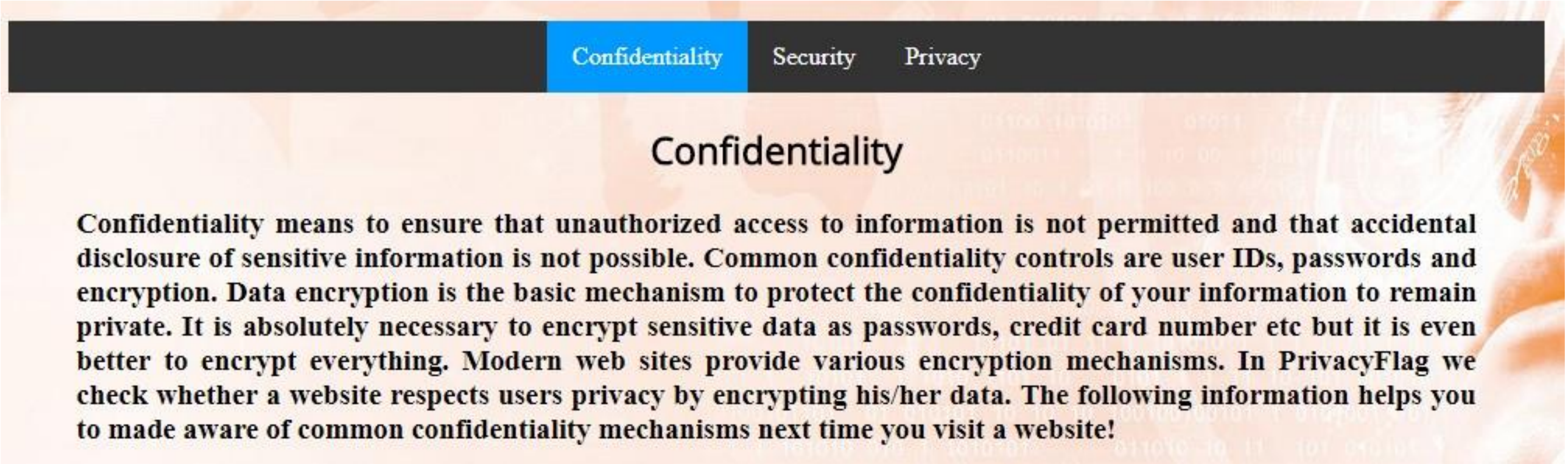
PrivacyFlag Observatory is organized in three distinct categories, Confidentiality, Security and Privacy of Data. All of them are related to the Privacy of your Data in direct or indirect way. Find why:

CTI "DIOPHANTUS" computer technology institute & press

Co-funded by the European Union

Co-funded by the Swiss Confederation

PF Threat Observatory



Confidentiality

Confidentiality means to ensure that unauthorized access to information is not permitted and that accidental disclosure of sensitive information is not possible. Common confidentiality controls are user IDs, passwords and encryption. Data encryption is the basic mechanism to protect the confidentiality of your information to remain private. It is absolutely necessary to encrypt sensitive data as passwords, credit card number etc but it is even better to encrypt everything. Modern web sites provide various encryption mechanisms. In PrivacyFlag we check whether a website respects users privacy by encrypting his/her data. The following information helps you to made aware of common confidentiality mechanisms next time you visit a website!

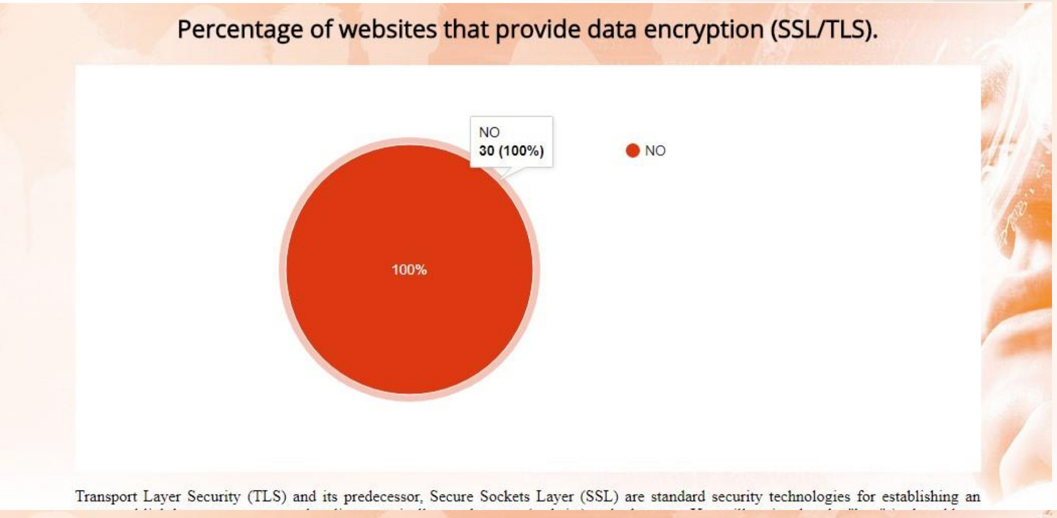
CTI "DIOPHANTUS" computer technology institute & press

Co-funded by the European Union

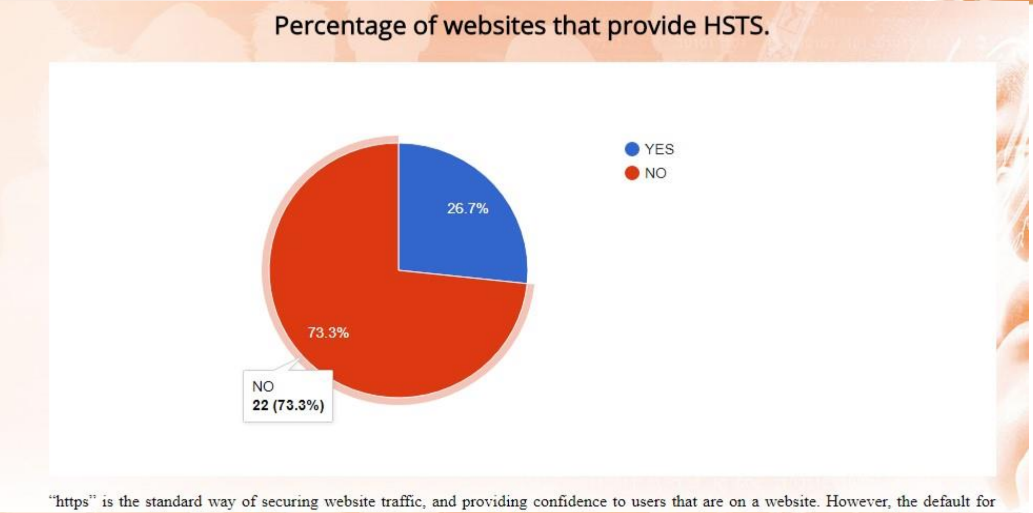
Co-funded by the Swiss Confederation

PRIVACY FLAG

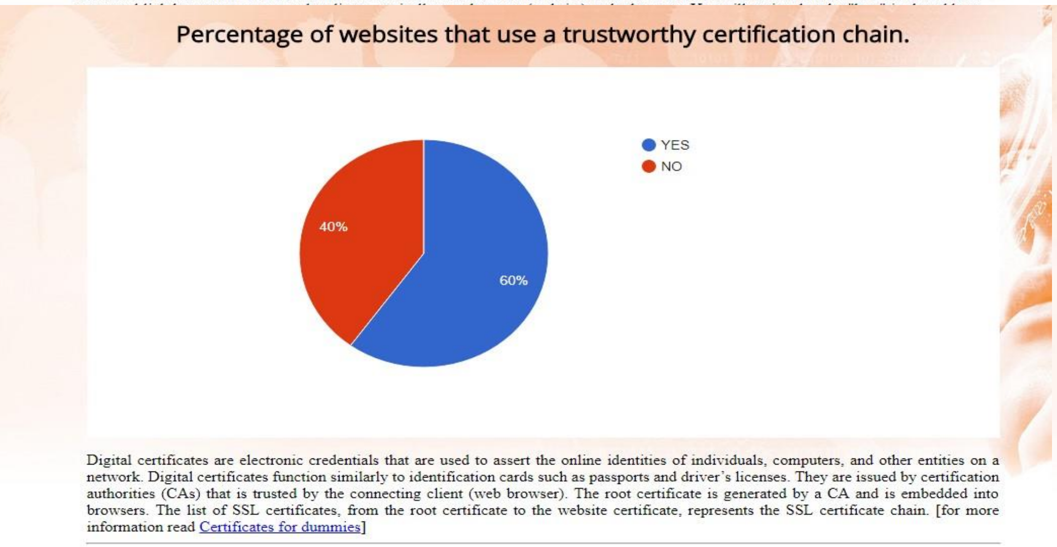
PF Threat Observatory


Percentage of websites that provide data encryption (SSL/TLS).

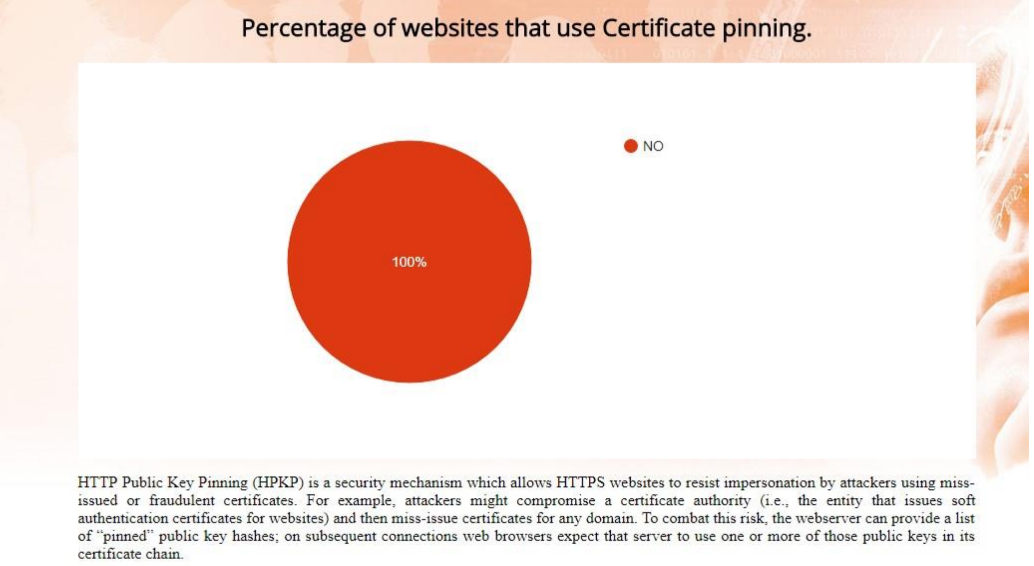
Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL) are standard security technologies for establishing an


Percentage of websites that provide HSTS.

“https” is the standard way of securing website traffic, and providing confidence to users that are on a website. However, the default for


Percentage of websites that use a trustworthy certification chain.

Digital certificates are electronic credentials that are used to assert the online identities of individuals, computers, and other entities on a network. Digital certificates function similarly to identification cards such as passports and driver’s licenses. They are issued by certification authorities (CAs) that is trusted by the connecting client (web browser). The root certificate is generated by a CA and is embedded into browsers. The list of SSL certificates, from the root certificate to the website certificate, represents the SSL certificate chain. [for more information read Certificates for dummies]


Percentage of websites that use Certificate pinning.

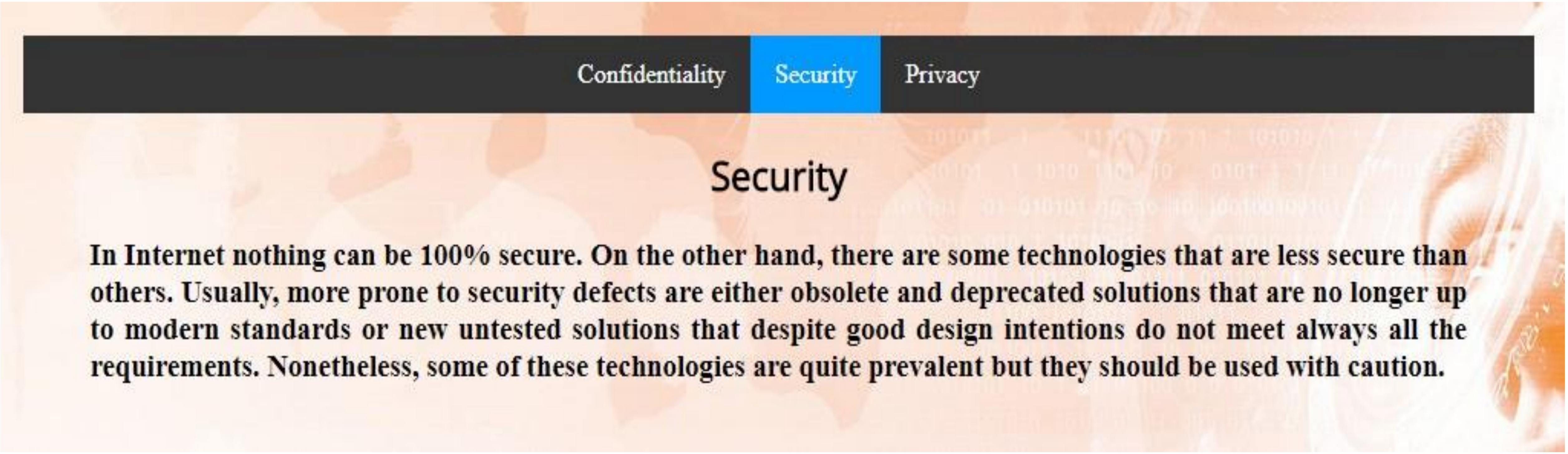
HTTP Public Key Pinning (HPKP) is a security mechanism which allows HTTPS websites to resist impersonation by attackers using miss-issued or fraudulent certificates. For example, attackers might compromise a certificate authority (i.e., the entity that issues soft authentication certificates for websites) and then miss-issue certificates for any domain. To combat this risk, the webserver can provide a list of “pinned” public key hashes; on subsequent connections web browsers expect that server to use one or more of those public keys in its certificate chain.

CTI "DIOPHANTUS" computer technology institute & press

Co-funded by the European Union

Co-funded by the Swiss Confederation

PF Threat Observatory



Security

In Internet nothing can be 100% secure. On the other hand, there are some technologies that are less secure than others. Usually, more prone to security defects are either obsolete and deprecated solutions that are no longer up to modern standards or new untested solutions that despite good design intentions do not meet always all the requirements. Nonetheless, some of these technologies are quite prevalent but they should be used with caution.

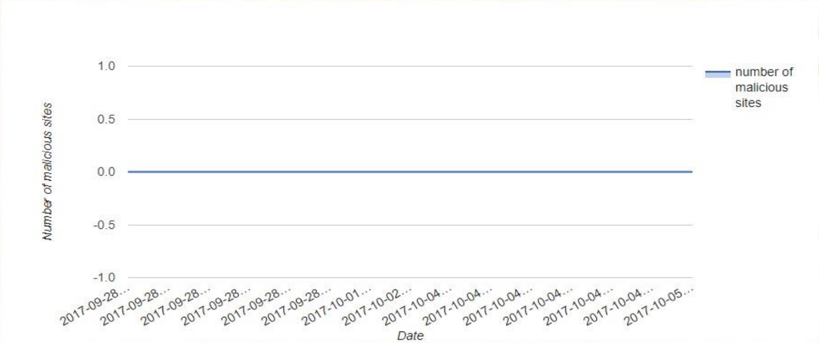
CTI "DIOPHANTUS" computer technology institute & press

Co-funded by the European Union

Co-funded by the Swiss Confederation

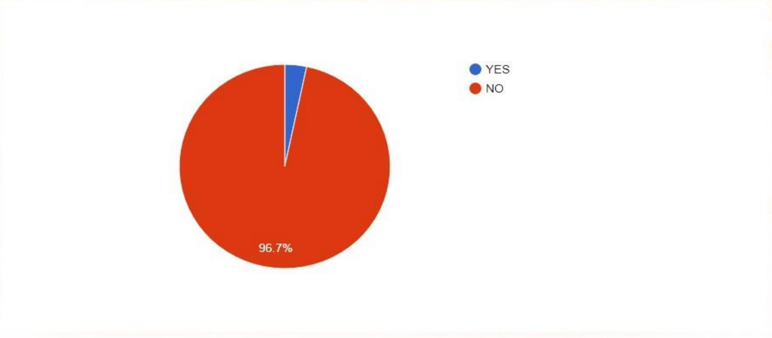
PF Threat Observatory

Average number of embedded links that direct to malicious websites.



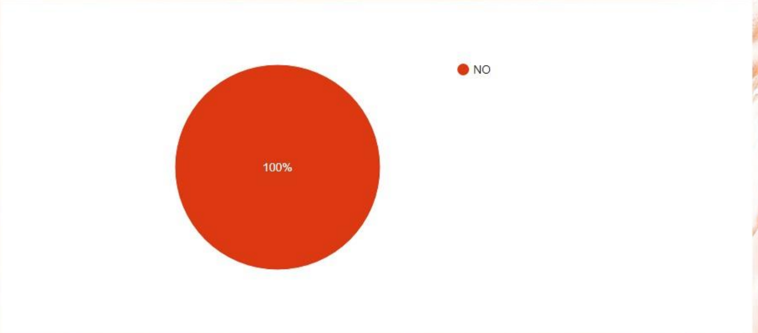
PrivacyFlag scans every website for links which direct users to malware infected web sites. During a malware epidemic it is possible many innocent sites to became infected and unknowingly to their owners to host malware. Generally, the average number of infected sites should be minimal, close to zero in comparison to the vast amount of web sites.

Percentage of websites that use technologies with known security issues - Flash.



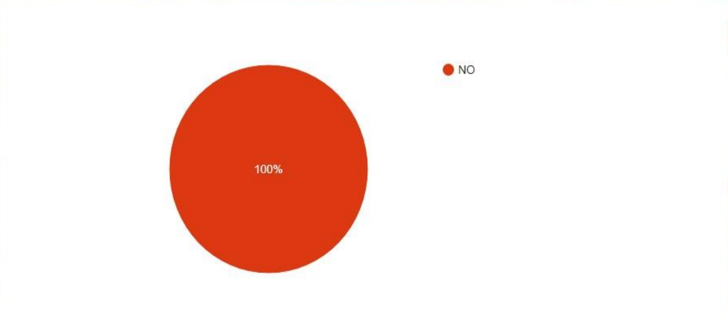
Flash was once the king of multimedia content and was used thoroughly in the Web. Most web sites delivered multimedia video almost exclusively in Flash. Unfortunately, Flash protocol was also ranked high as the major source of vulnerabilities and other security risks. Therefore, most modern web sites tend to abandon the Flash protocol in favor of a new multimedia codecs. So, though not always possible to avoid Flash at all, try to use web sites with HTML5 video native players to enjoy your web video experience safely.

Percentage of websites that use potentially dangerous advanced HTML5 APIs - Web Audio API.



HTML5 Web Audio is a very useful technology to capture and store sound streams form various audio input sources as well as the microphone. Naturally, a great deal of care must be taken to protect users from unauthorized recordings, thus this specific functionality should be used with caution.

Percentage of websites that use potentially dangerous advanced HTML5 APIs - WebRTC.



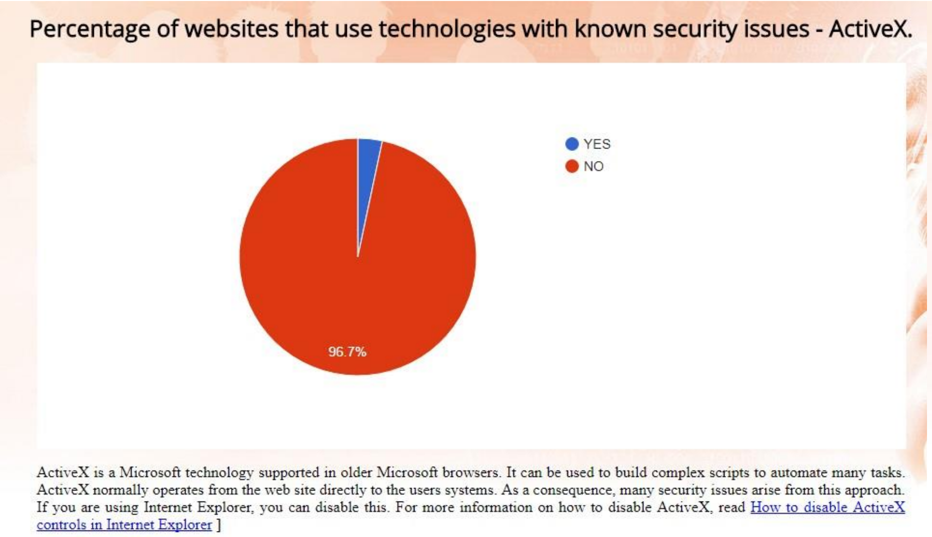
HTML5-WebRTC is a very effective mechanism for providing real time communication but is also used by hackers to leak sensitive information or deanonymize users. This is a promising and useful technology, but whenever privacy is absolute necessary, WebRTC should be avoided.

Co-funded by the European Union

Co-funded by the Swiss Confederation

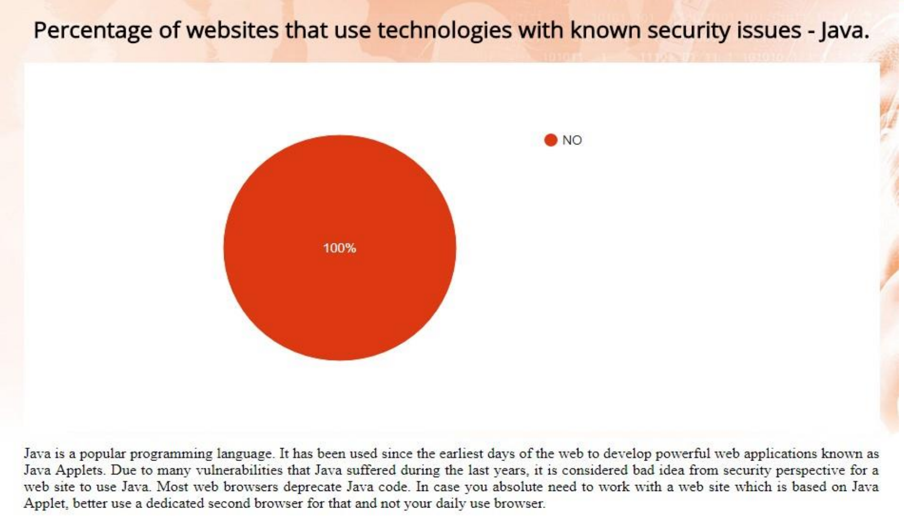
MY DATA
PRIVACY FLAG

PF Threat Observatory



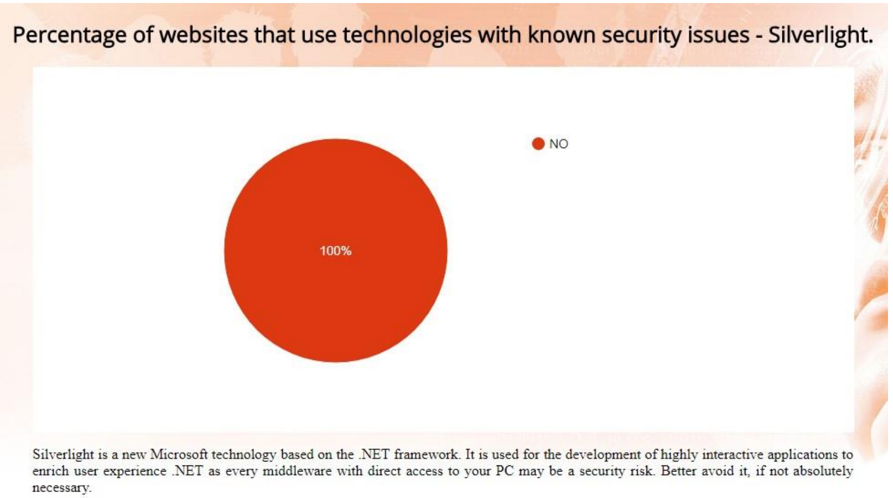
Percentage of websites that use technologies with known security issues - ActiveX.

ActiveX is a Microsoft technology supported in older Microsoft browsers. It can be used to build complex scripts to automate many tasks. ActiveX normally operates from the web site directly to the users systems. As a consequence, many security issues arise from this approach. If you are using Internet Explorer, you can disable this. For more information on how to disable ActiveX, read How to disable ActiveX controls in Internet Explorer]



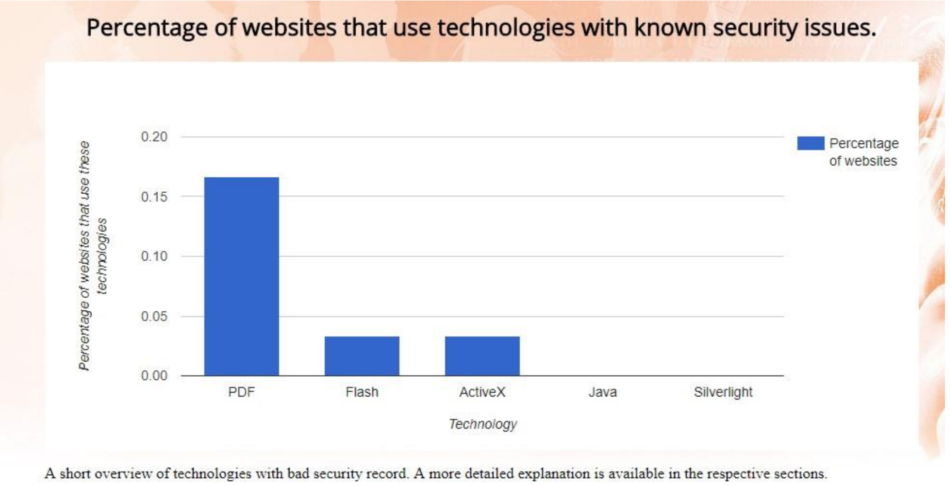
Percentage of websites that use technologies with known security issues - Java.

Java is a popular programming language. It has been used since the earliest days of the web to develop powerful web applications known as Java Applets. Due to many vulnerabilities that Java suffered during the last years, it is considered bad idea from security perspective for a web site to use Java. Most web browsers deprecate Java code. In case you absolute need to work with a web site which is based on Java Applet, better use a dedicated second browser for that and not your daily use browser.



Percentage of websites that use technologies with known security issues - Silverlight.

Silverlight is a new Microsoft technology based on the .NET framework. It is used for the development of highly interactive applications to enrich user experience .NET as every middleware with direct access to your PC may be a security risk. Better avoid it, if not absolutely necessary.



Percentage of websites that use technologies with known security issues.

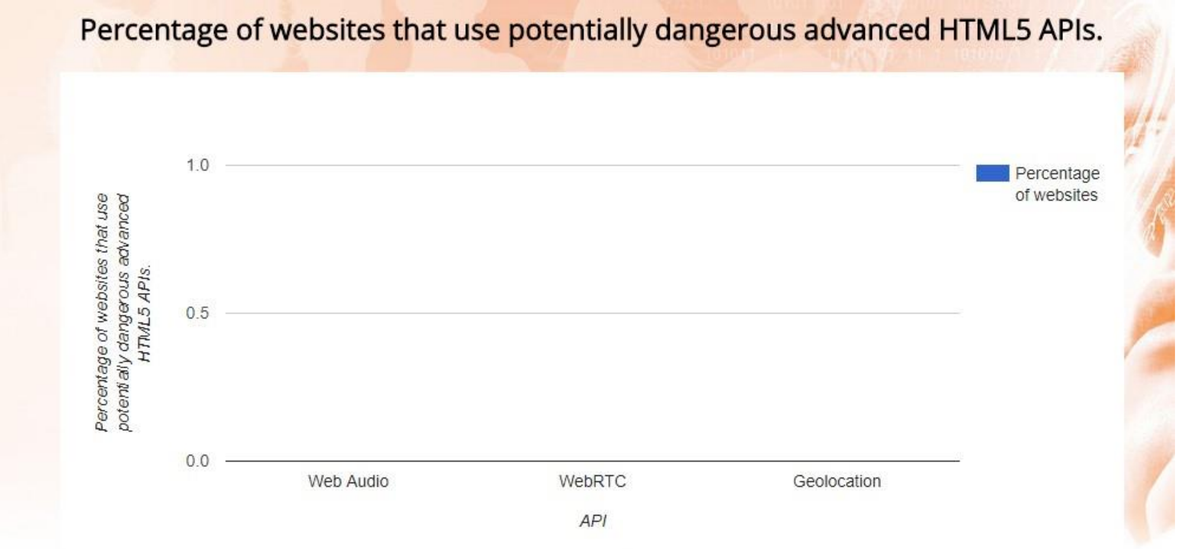
A short overview of technologies with bad security record. A more detailed explanation is available in the respective sections.

CTI "DIOPHANTUS"
computer technology institute & press

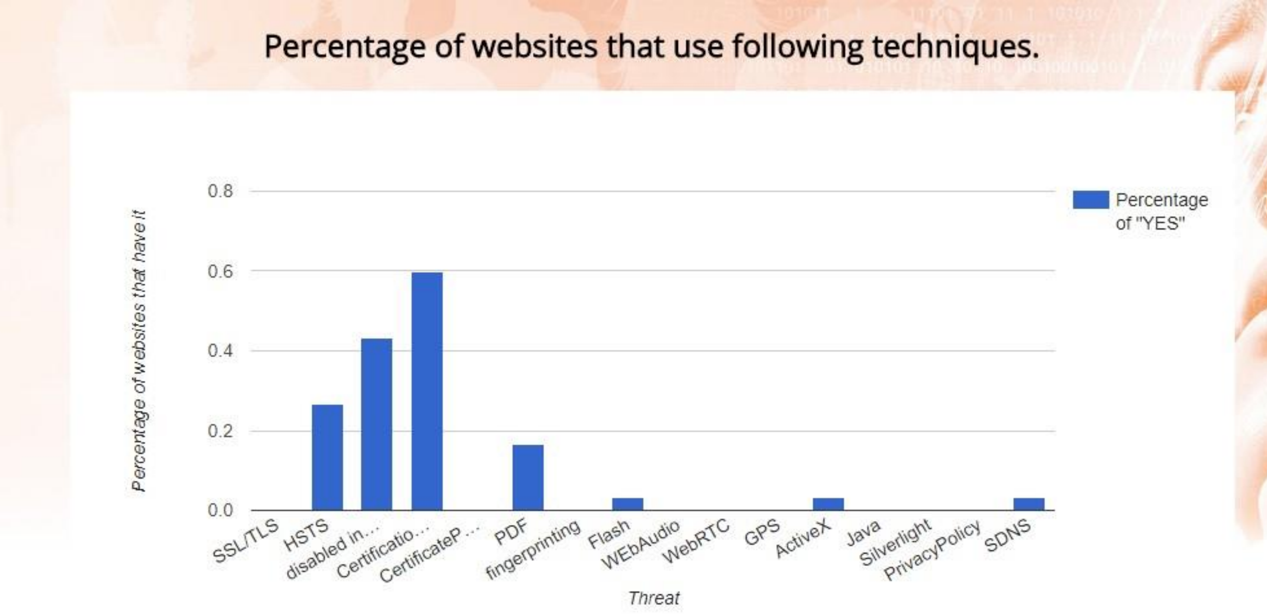
Co-funded by the European Union

Co-funded by the Swiss Confederation

PF Threat Observatory


Percentage of websites that use potentially dangerous advanced HTML5 APIs.

HTML5 is the newest Web standard, it is definitely the future of the WWW and is here to stay. As it happens with any new powerful technology it provides a set of new impressive features. On the other hand, some of them might have some security and privacy issues. PrivacyFlag have identified some potential problematic, from privacy perspective, technologies. Unless there is a good reason for a web site to use this functionality it is better not enable them yet.

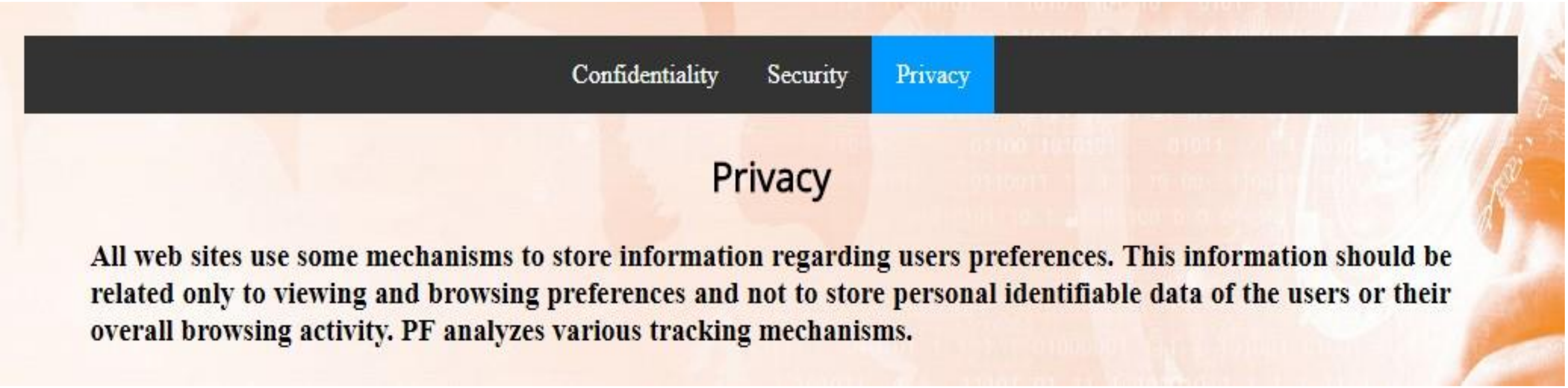

Percentage of websites that use following techniques.

A summary of the powerful technologies used in websites.

Co-funded by the European Union

Co-funded by the Swiss Confederation

PF Threat Observatory

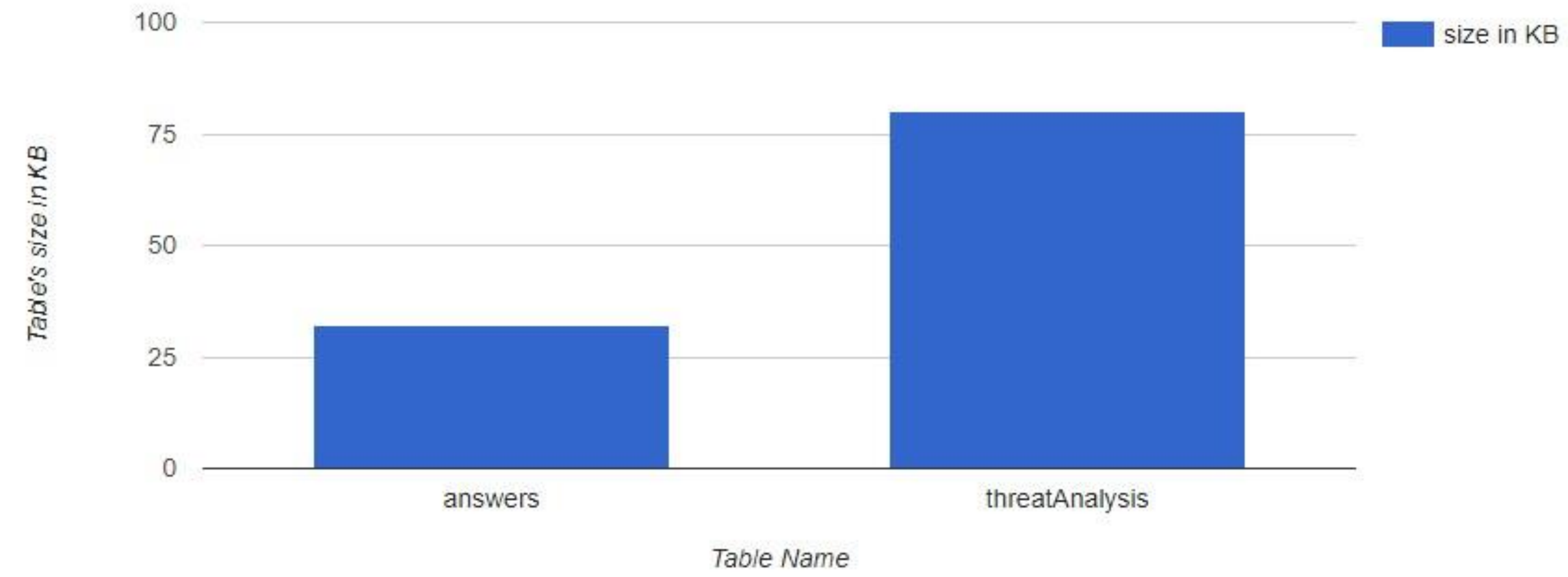


Privacy

All web sites use some mechanisms to store information regarding users preferences. This information should be related only to viewing and browsing preferences and not to store personal identifiable data of the users or their overall browsing activity. PF analyzes various tracking mechanisms.

PF Threat Observatory

PrivacyFlag DB size.



The size of the PrivacyFlag DataBase indicates the total amount of information that we have processed so far. The more websites and application our users visit and evaluate, the larger our DataBase gets and more accurate are our predictions. A large PrivacyFlag DataBase help us to provide you with the best privacy recommendations.

CTI "DIOPHANTUS" computer technology institute & press

Co-funded by the European Union

Co-funded by the Swiss Confederation

CTI’s Threats Detection: **Web Scraper**

http://150.140.193.133:5000/CTI_demo/threats/

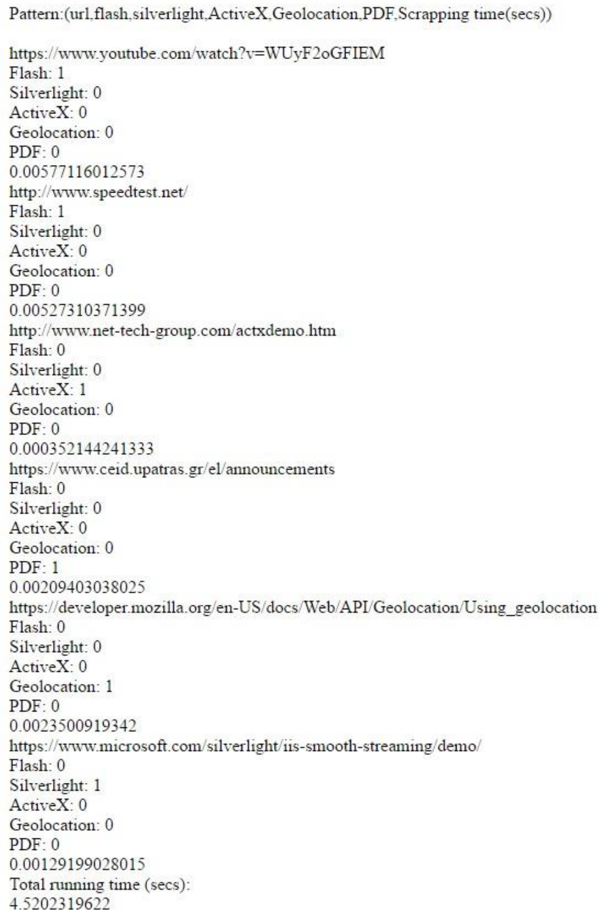
A **web service** is developed to detect the following threats by scrapping the websites (text pattern matching, html parsing).

We check if the html code of the website includes specific object or file extension patterns for the following threats:

- Flash player
- Silverlight
- ActiveX
- Geolocation
- PDF

The web service output is:

- Threat output
  - 1 (true) or 0 (false)
- The time needed for each website to check for the threats.
- **Finally, the total elapsed time is reported**.



```
Pattern:(url,flash,silverlight,ActiveX,Geolocation,PDF,Scrapping time(secs))

https://www.youtube.com/watch?v=WUyF2oGFIEM
Flash: 1
Silverlight: 0
ActiveX: 0
Geolocation: 0
PDF: 0
0.00577116012573
http://www.speedtest.net/
Flash: 1
Silverlight: 0
ActiveX: 0
Geolocation: 0
PDF: 0
0.00527310371399
http://www.net-tech-group.com/actxdemo.htm
Flash: 0
Silverlight: 0
ActiveX: 1
Geolocation: 0
PDF: 0
0.000352144241333
https://www.ceid.upatras.gr/el/announcements
Flash: 0
Silverlight: 0
ActiveX: 0
Geolocation: 0
PDF: 1
0.00209403038025
https://developer.mozilla.org/en-US/docs/Web/API/Geolocation/Using_geolocation
Flash: 0
Silverlight: 0
ActiveX: 0
Geolocation: 1
PDF: 0
0.0023500919342
https://www.microsoft.com/silverlight/iis-smooth-streaming/demo/
Flash: 0
Silverlight: 1
ActiveX: 0
Geolocation: 0
PDF: 0
0.00129199028015
Total running time (secs):
4.5202319622
```

Co-funded by the European Union

Co-funded by the Swiss Confederation

A historical perspective of PrivacyFlag evaluation:

- **PF Observatory version 1**:
  - link: http://app.privacyflag.eu:2080/privacy/addon/metrics.php
  - a small list of graphs is included (only 5 graphs)
  - graph library: JpGraph (http://jpgraph.net/)
- **PF Observatory version 2:**
  - link:http://app.privacyflag.eu:2080/privacy/addon/new_metrics.php
  - 17 new graphs were implemented.
  - new graph library: Google Charts (https://developers.google.com/chart/)

Final Version:

PF Observatory version 3 (current version):

- link: http://app.privacyflag.eu:2080/privacy/addon/observatory.php
- According to the report from pilots that took place, there were the three following recommendations, regarding to Privacy Flag Observatory:
  - A more detailed information about each chart.
  - Having some guidelines about what each risk entails
  - Splitting the charts into categories

All of them have been addressed.

Co-funded by the European Union

Co-funded by the Swiss Confederation

PF Early Warning System:

Outlier Detection and Epidemic modeling:

- ~~Peirce criterion and Euclidean distance → to detect outliers~~
- ~~Epidemic Curves → for malware links and possible for other high risk threats~~
- ~~Some simple outlier detection methods are researched~~
- New more effective outlier detection mechanisms have been employed {**z-score**, Chebyshev’s theorem, Iglewicz-Hoaglin Method)

T4.5
DATABASE AND SERVER IMPLEMENTATION

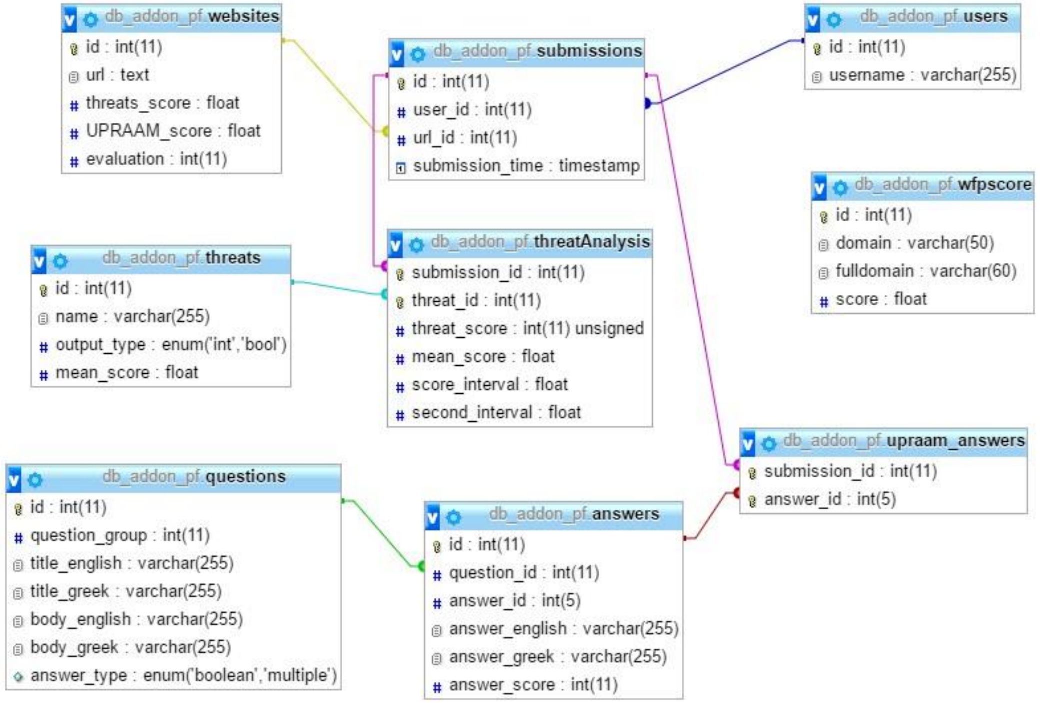
Co-funded by the
European Union

Co-funded by the
Swiss Confederation

PRIVACY FLAG

T4.5 Database and server implementation

More efficient PF DataBase Schema both for the PF AddOn and thr PF SmartPhoneApp



db_addon_pf.websites
- id : int(11)
- url : text
- threats_score : float
- UPRAAM_score : float
- evaluation : int(11)

db_addon_pf.submissions
- id : int(11)
- user_id : int(11)
- url_id : int(11)
- submission_time : timestamp

db_addon_pf.users
- id : int(11)
- username : varchar(255)

db_addon_pf.wfpscore
- id : int(11)
- domain : varchar(50)
- fulldomain : varchar(60)
- score : float

db_addon_pf.threats
- id : int(11)
- name : varchar(255)
- output_type : enum('int','bool')
- mean_score : float

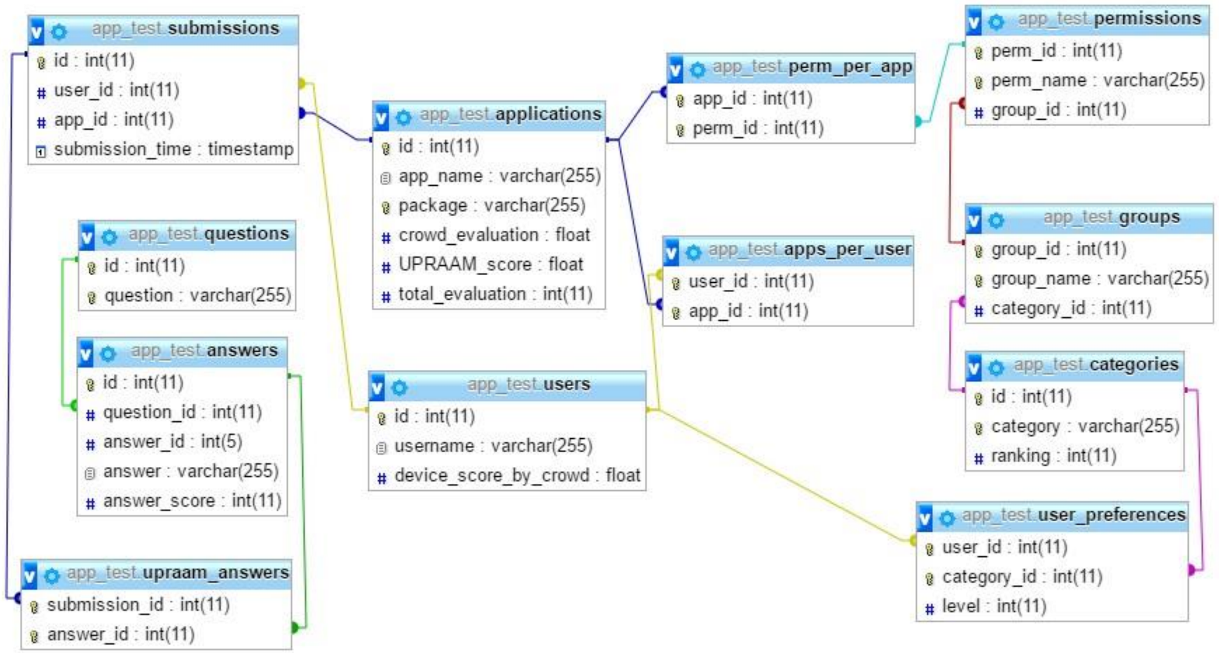
db_addon_pf.threatAnalysis
- submission_id : int(11)
- threat_id : int(11)
- threat_score : int(11) unsigned
- mean_score : float
- score_interval : float
- second_interval : float

db_addon_pf.upraam_answers
- submission_id : int(11)
- answer_id : int(5)

db_addon_pf.questions
- id : int(11)
- question_group : int(11)
- title_english : varchar(255)
- title_greek : varchar(255)
- body_english : varchar(255)
- body_greek : varchar(255)
- answer_type : enum('boolean','multiple')

db_addon_pf.answers
- id : int(11)
- question_id : int(11)
- answer_id : int(5)
- answer_english : varchar(255)
- answer_greek : varchar(255)
- answer_score : int(11)

PF WebAddOn



app_test.submissions
- id : int(11)
- user_id : int(11)
- app_id : int(11)
- submission_time : timestamp

app_test.questions
- id : int(11)
- question : varchar(255)

app_test.answers
- id : int(11)
- question_id : int(11)
- answer_id : int(5)
- answer : varchar(255)
- answer_score : int(11)

app_test.upraam_answers
- submission_id : int(11)
- answer_id : int(11)

app_test.applications
- id : int(11)
- app_name : varchar(255)
- package : varchar(255)
- crowd_evaluation : float
- UPRAAM_score : float
- total_evaluation : int(11)

app_test.users
- id : int(11)
- username : varchar(255)
- device_score_by_crowd : float

app_test.perm_per_app
- app_id : int(11)
- perm_id : int(11)

app_test.apps_per_user
- user_id : int(11)
- app_id : int(11)

app_test.permissions
- perm_id : int(11)
- perm_name : varchar(255)
- group_id : int(11)

app_test.groups
- group_id : int(11)
- group_name : varchar(255)
- category_id : int(11)

app_test.categories
- id : int(11)
- category : varchar(255)
- ranking : int(11)

app_test.user_preferences
- user_id : int(11)
- category_id : int(11)
- level : int(11)

PF SmartPhoneApp

Co-funded by the European Union

Co-funded by the Swiss Confederation

PF Infrastructure

- Server Information
  - **OS:** Ubuntu 14.04 LTS
  - **Database:** MySQL
  - **HTTP Server:** Apache2
- API implementation
  - **Javascript with Node.js:** v6.2.1 (https://nodejs.org/)
  - **PHP** v5.5.9
  - **HTML5** and **CSS3**
- API documentation and demonstration
  - **Swagger** Framework (http://swagger.io/)

Co-funded by the
European Union

Co-funded by the
Swiss Confederation

PRIVACY FLAG

Thank You!
Q&A

CTI
"DIOPHANTUS"
computer
technology
institute & press

Co-funded by the
European Union

Co-funded by the
Swiss Confederation