Using Crowdsourcing to Protect Web Privacy

Dr Vasileios Vlachos CTI

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)

Possible threats

Third party tracker or advertising company

Cookies

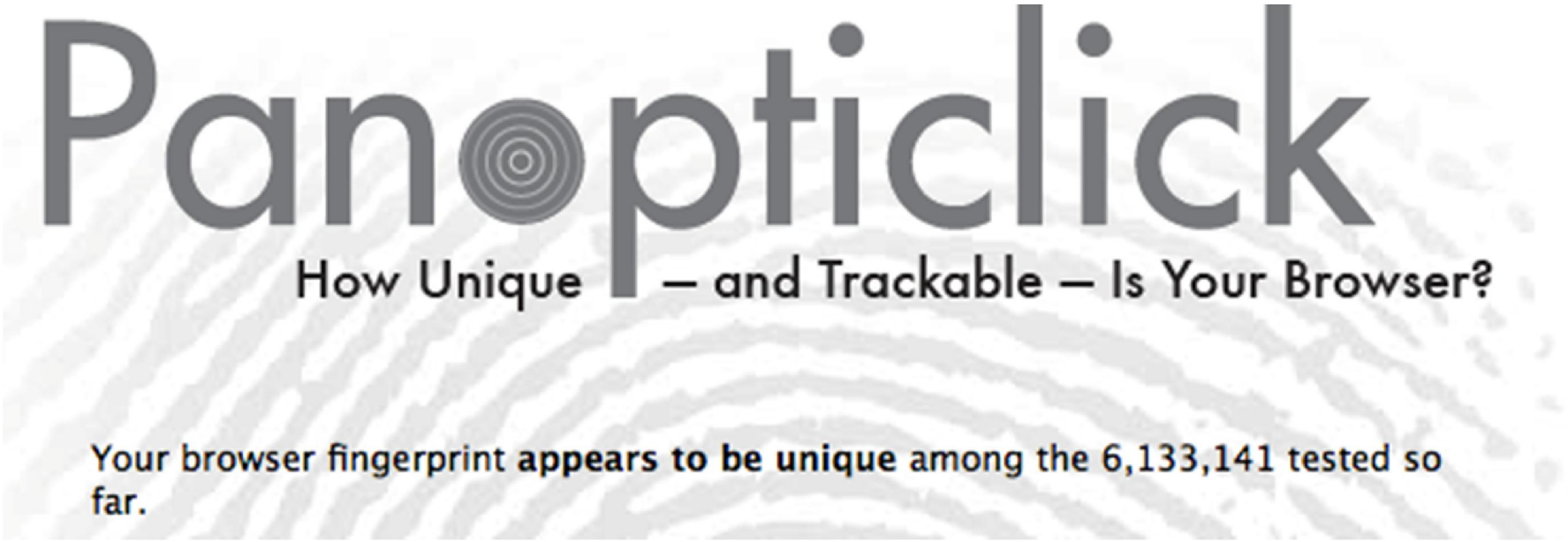
Fingerprinting

Traffic analysis

PrivacyFlag AddOn User

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:



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					✓				✓	

Smartphone Privacy Invasion in action

- Apps were infected after developers used a malicious version of the **Xcode** — Apple's developer toolkit used to develop iOS and Mac OS X apps.
- Xcode is downloaded directly from Apple for free as well as from other sources such as developer forums. Chinese file-sharing service **Baidu Yunpan** offers some versions of Xcode that contains extra lines of code.
- Once installed, the malicious app contains dangerous XcodeGhost code prompt fake alerts to:
  - Phish user credentials
  - Hijack URLs
  - Read and Write data, such as victims' iCloud passwords
  - Infect other apps using iOS

Smartphone Privacy Invasion in action

- A total of 39 apps, including the popular instant messaging app **WeChat**, Chinese Uber-like cab service , music streaming service **NetEase**, photo editor **Perfect365** and card scanning tool **CamCard**, were found to be infected by the malicious Xcode

- Apple users outside China are also affected by the malware. The mainstay **WinZip** decompression app, **Musical.ly**, and the **Mercury** Browser are also among the affected apps

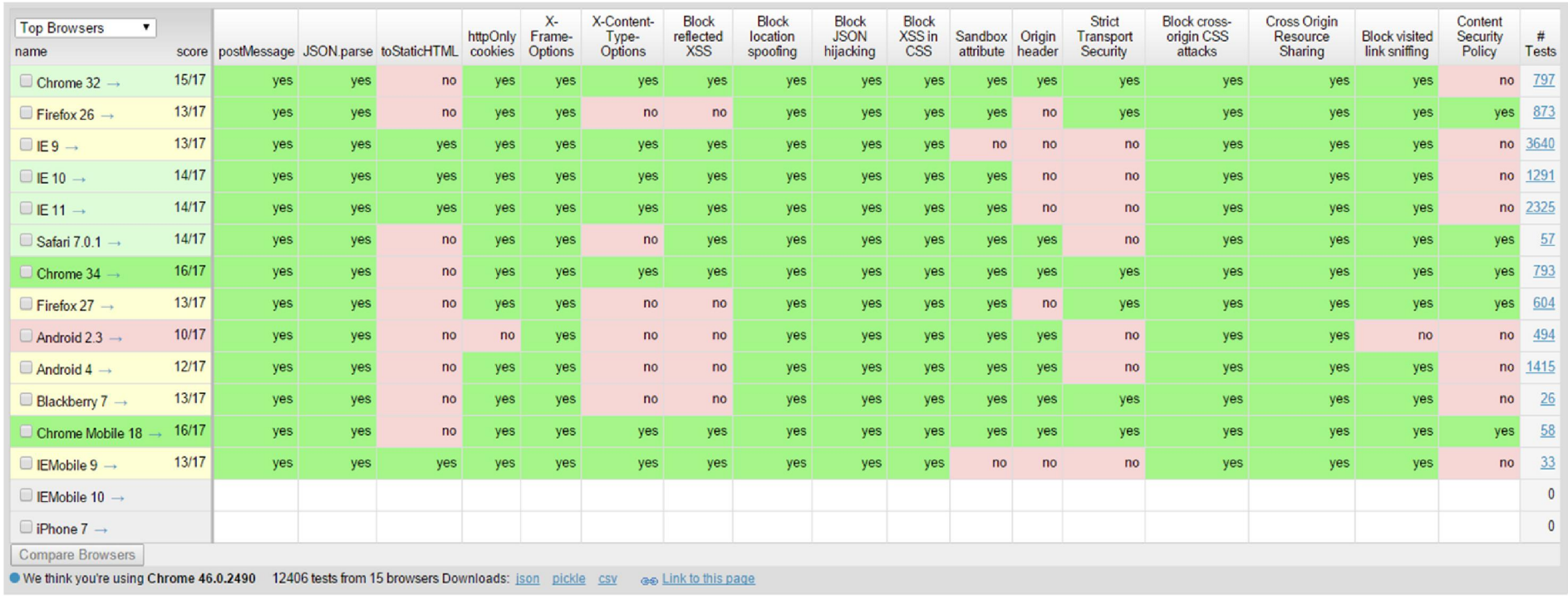
- Apple has ***removed more than 300 malware-infected apps*** from its App Store after a counterfeit version of its developer tool kit allowed many Chinese apps to leak users' personal data to hackers

IoT Privacy?

- “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

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.



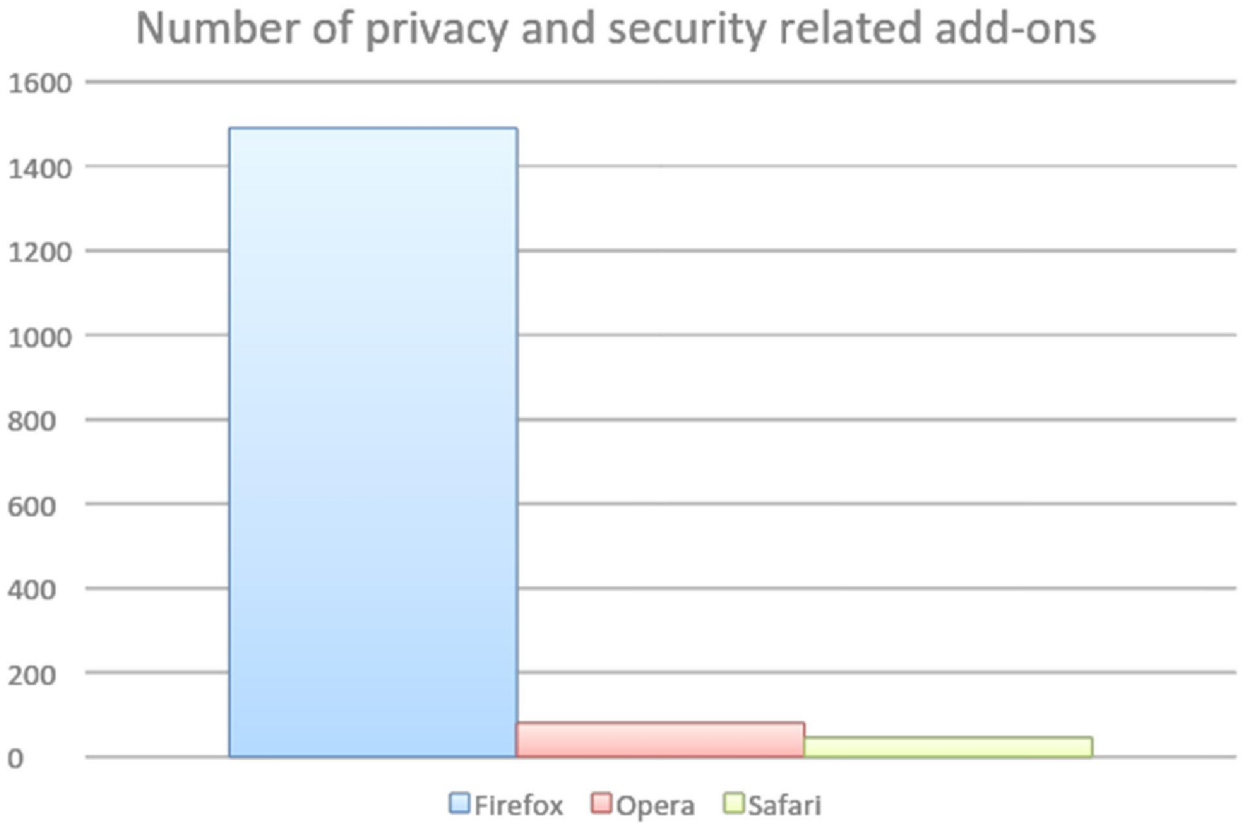
Top Browsers

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

Compare Browsers

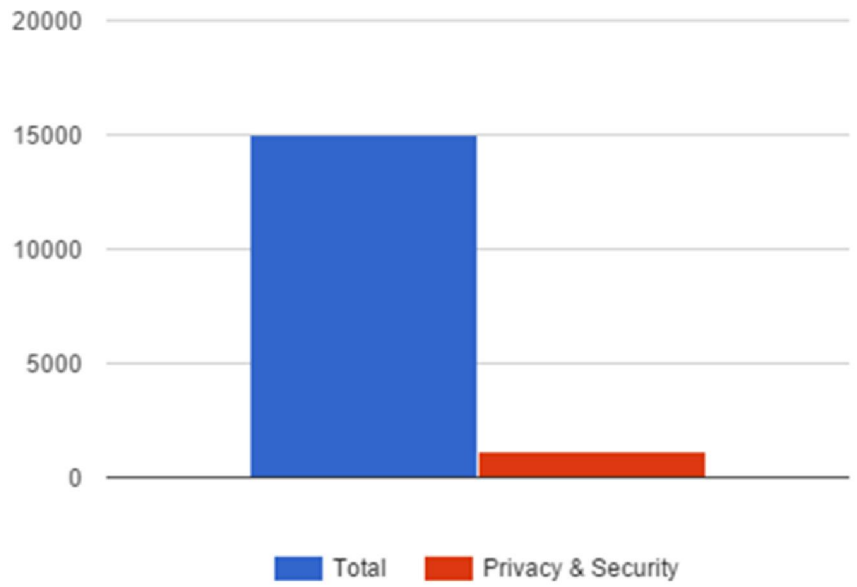
We think you're using Chrome 46.0.2490 12406 tests from 15 browsers Downloads: json pickle csv Link to this page

Browsers: The weak link in Web Privacy



There are no available data for Google's Chrome browser, but the number of add-ons is comparable to that of Mozilla's Firefox.

Browsers: The weak link in Web Privacy



Number of Privacy and security enabled addons compared to the total number of addons available for Mozilla Firefox

Browsers: The weak link in Web Privacy

Several add-ons are available for modern browsers such as:

Privacy Badger: Stops advertisers and other third-party trackers from secretly tracking users without their permission. Privacy Badger automatically blocks such advertisers from loading content on the user's browser.

Adblock Plus: It allows users to prevent page elements, such as advertisements, from being downloaded and displayed. Can block tracking, malware domains, banners, pop-ups and video ads. Unobtrusive ads aren't being blocked in order to support websites

Click&Clean: Can protect user privacy by cleaning up all traces of their internet activity by erasing temporary files, cookies, emptying cache, removing Flash Cookies (LSOs) and more.

Browsers: The weak link in Web 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.

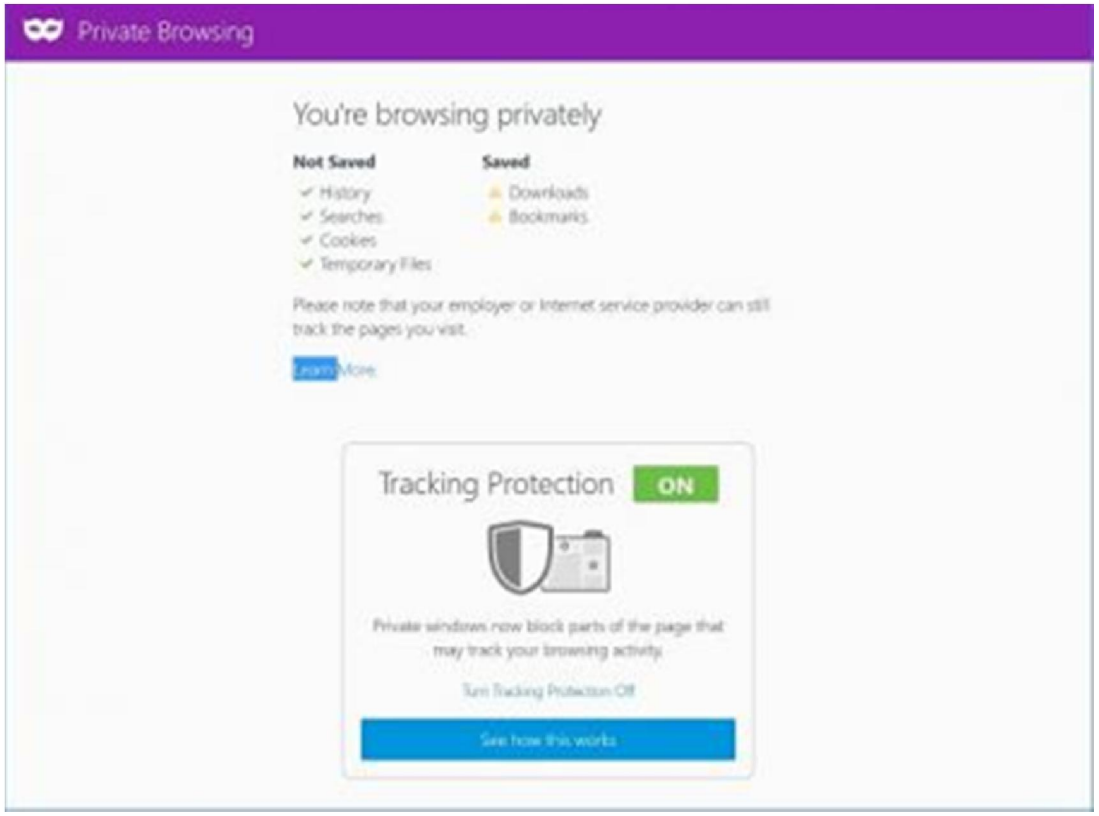
- **Other browsers:**

  - 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.

Browsers: The weak link in Web Privacy

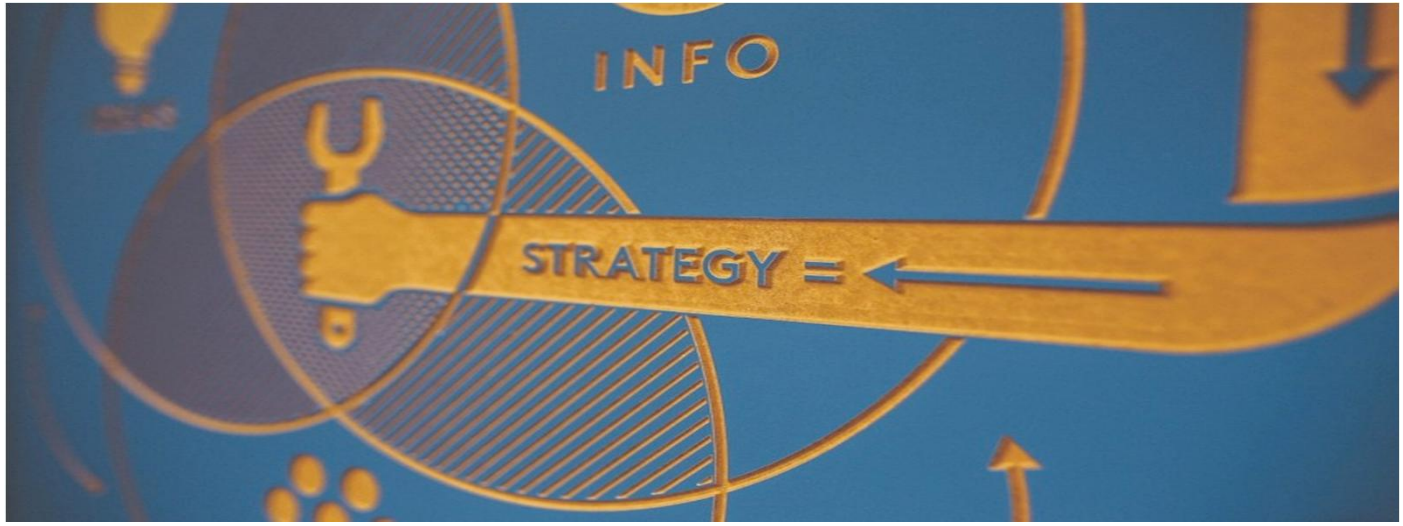
- Dubbed Tracking Protection is part of the browser's existing Private Browsing mode, and gives users control over the data that third-parties receive from them.
- This feature does not appear in similar private browsers offered by Chrome, Safari, Edge or Internet Explorer.
- Mozilla has also launched a Control Center in its browser that places site security and privacy controls in a single place - the browser address bar.



Privacy Flag

Privacy Challenges

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



About PrivacyFlag

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.

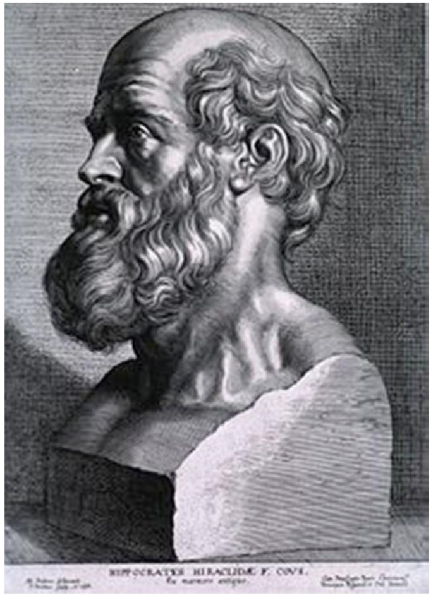
11 European partners, including SMEs and a large telco operator, bring their complementary technical, legal, societal and business expertise; strong links with standardization bodies and international fora; and outcomes from over 20 related research projects. It intends to pave the way to a privacy defenders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

News

Privacy in modern times

Desperate times require desperate measures

- Crowdsourcing intelligence
- Aggregated information
- Autonomous Systems
- Biodiversity



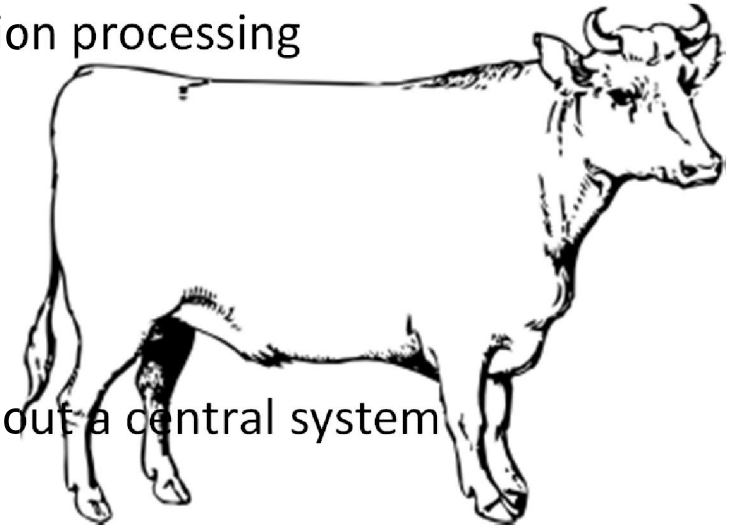
Crowdsourcing intelligence

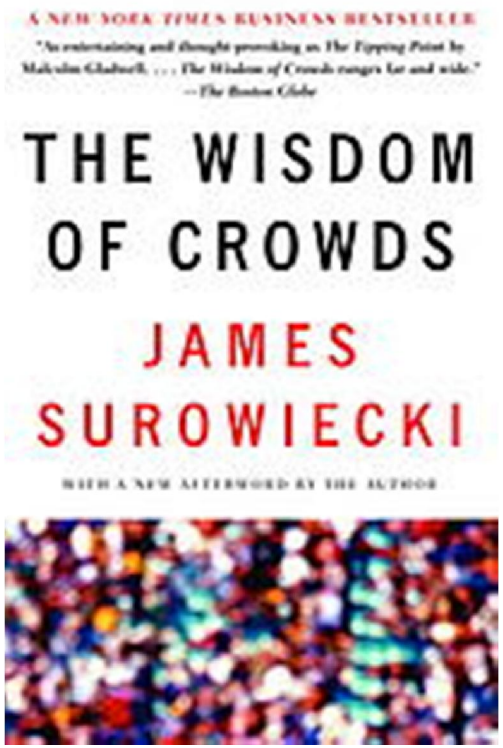
Surowiecki's seminal work on crowds

Cognition
Thinking and information processing

Coordination
Accurate judgments

Cooperation
Networks of trust without a central system





Can provide accurate intelligence through "wisdom of the crowd"

Example: 800 people estimated the weight of a slaughtered and dressed ox, with 1% accuracy of the true weight.

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

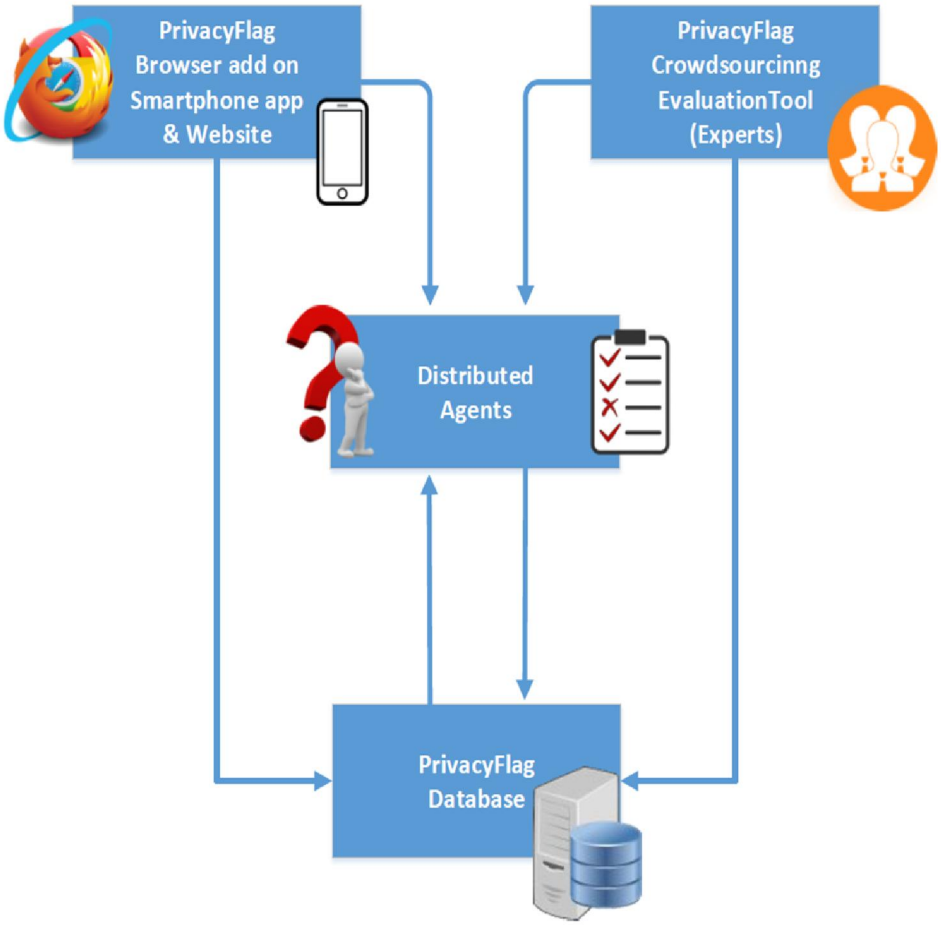
Possible threats

Description	Threat	Level	Metric
HTTP Cookie	Misuse of cookies for authentication or store of sensitive information	Low	Value [0..n]
Third party cookie	Tracking user's browsing history	Medium	Value [0..n]
Zombie Cookie	Persistent tracking -can track users across browsers on the same machine	Medium	Value [0..n]
Evercookie	Persistent tracking	Medium	Value [0..n]
Local Shared Object (LSO) or Flash Cookie	Detailed Tracking, Allows spyware or malware to be installed	High	Value [0..n]
Supercookie	Disrupts or impersonates legitimate user requests to another website that shares the same Top-Level Domain as the malicious website	High	Value [0..n]
Geolocation	Reveal the physical location of the user. After location access is granted, the location data may be used for other purposes.	High	Boolean
Web Bug	A Web bug can gather statistics such as: The IP address, the URL of the page that the Web bug is located on, a previously set cookie value, etc.	Low	Value [0..n]
Scripting Languages	Cross-site scripting, Malicious Code injection, etc.	Low	Value [0..n]

Possible threats

Description	Threat	Level	Metric
Device Fingerprinting	Are used to identify individual users even when cookies are turned off. It makes it possible to uniquely distinguish between all machines on a network.	High	Unable to detect
HTML5 – Canvas Fingerprinting	Extension of device fingerprinting, that uses the <canvas> tag of HTML5	Medium	Boolean
HTML5 – Web Storage	A third-party advertiser could use a unique identifier stored in its local storage area to track a user across multiple sessions.	Medium	Value [0..n]
HTML5 – Web Messaging	Poor origin checking can pose a risk for applications which employ cross-document messaging.	Medium	Value [0..n]
Media Capture and Streams	Without authorization, it offers the ability to tell how many devices there are of each class (audio or video). The number of devices adds to the fingerprint surface.	Medium	Value [0..n]
SSL/TLS Encryption	Easy to intercept users sensitive information at multiple points using a network sniffer. All data are visible to the ISP as well as to the network gateway.	High	Boolean
Privacy Certification (eTrust, W3C)	If a certification is absent there is no way to validate whether a website protects the user's private data.	Low	Boolean
Privacy Policy Agreement	A web site without Privacy Policy in not legally bound to protect or respect users personal data. Therefore it is possible that privacy violations might happen.	Medium	Boolean
Traffic Analysis	Create a detailed profile of the user's personality based on his/her surfing habits	High	Cannot be evaluated

The PrivacyFlag Project



Step 1: Calculates a **Local Threat Level Score** for each threat in the Threat List and submits it to the distributed agents (DA) and the database (DB).

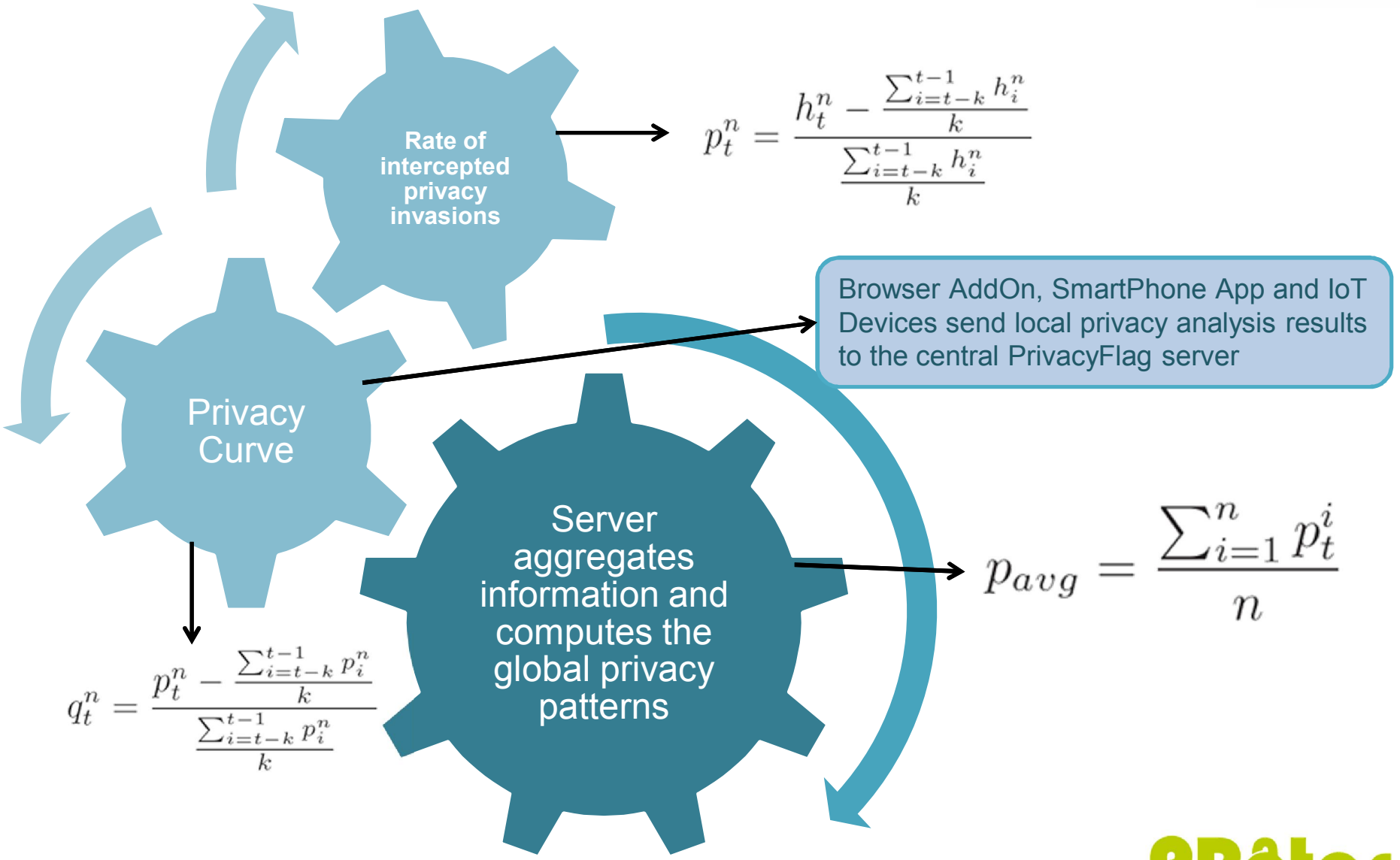
Step 2: The crowdsourced evaluation tool (CET) experts evaluate the web site manually.

Step 3 (independent - out of order): The DB calculates the **Mean Threat Level Score** and the **Mean CET Evaluation Score**

Step 4: The DAs query the DB for CET evaluations of the specific site.

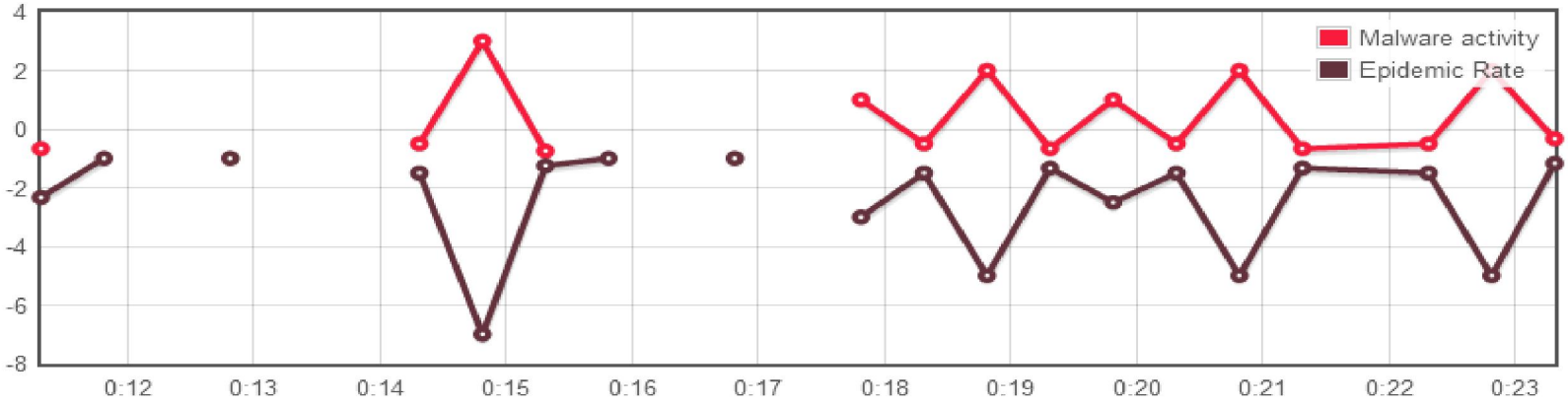
Step 5: The distributed agents decide based on all the above scores if the website is safe or possible data leakage exposure is imminent and informs the user.

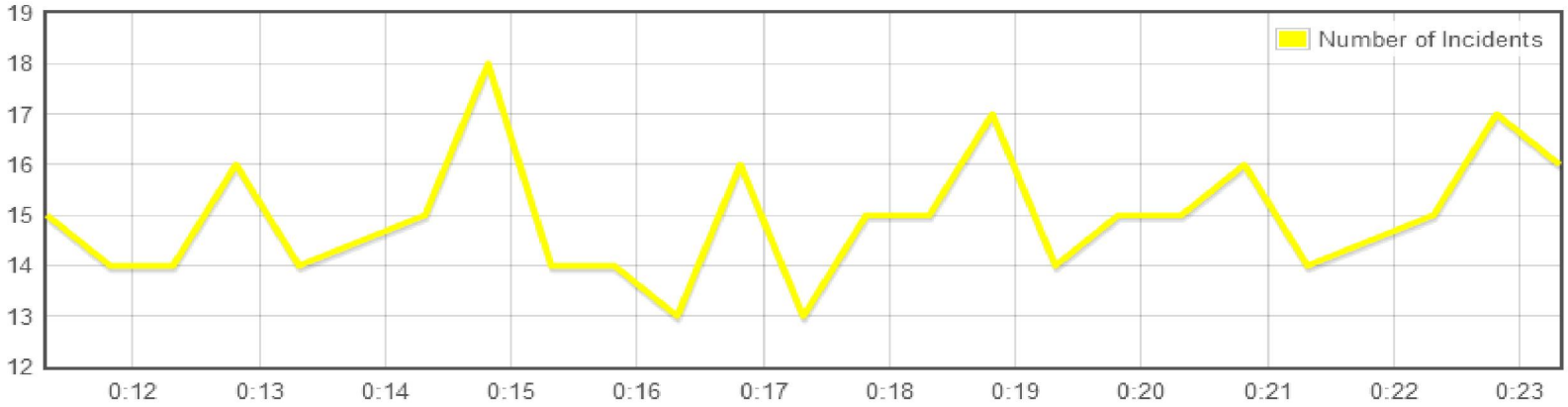
The PrivacyFlag Algorithms



PROactive Threat Observatory System

Time trends of attack incidents





Active Client(s): 15

Max Malware Activity: 3.00 **Min Malware Activity:** -0.75

Max Epidemic Rate: **Min Epidemic Rate:** -7.00

Thank you for your attention!

PRâtos Download: http://protos.cti.gr/ PRâtos

Dr. Vasileios Vlachos
CTI
vsvlachos@gmail.com

Professor of Technological Applications
Department of Computer Science and Engineering
School of Technological Applications
Technological Educational Institute (TEI) of Thessaly