LABORATORY FOR COMMUNICATIONS AND APPLICATIONS LCA

PRIVACY AND SECURITY OF ONLINE ADVERTISING

Internet economy relies on online advertising as the main business model for monetizing online content. Over the last decade, online advertising has become a major component of the Web, leading to large annual revenues (e.g., $31.7 billion in US in 2011). Given the ad revenue at stake and the lack of legislation against ad fraud in many countries, fraudsters have economic incentive to engage in fraudulent activities and exploit online advertising systems. In our work, we evaluate the threat to online advertising systems, identify vulnerabilities and exploits of the system, propose countermeasures and evaluate economic incentives of the stakeholders to deploy secure solutions.

A general introduction to online advertising system models, an overview of the known system vulnerabilities, classification of the identified attacks and countermeasures can be found **here.**

Inflight Modification of Ad Traffic

Our work focuses on a novel type of ad fraud that consists in inflight modification of ad traffic (e.g., by ISPs, hotspots or botnets of compromised access points). We identify possible exploits of the advertising systems and propose secure solutions to thwart such attacks. We also evaluate economic incentives of involved stakeholders, notably ad networks, to invest in secure solutions in order to protect their revenue.

- N. Vratonjic, J.-P. Hubaux, M. Raya and D. C. Parkes.**Security Games in Online Advertising: Can Ads Help Secure the Web?** In *Workshop on Economics of Information Security (WEIS) 2010*, Cambridge, MA, USA, June 7-8,

2010.

- N. Vratonjic, J. Freudiger, and J.-P. Hubaux.**Integrity of the Web Content: The Case of Online Advertising.** In *Usenix Collaborative Methods for Security and Privacy (CollSec) 2010*, Washington, DC, USA, August 10, 2010.
- N. Vratonjic, M. Manshaei, M. Raya, and J.-P. Hubaux.**ISPs and Ad Networks Against Botnet Ad Fraud**. In *Conference on Decision and Game Theory for Security (GameSec) 2010*, Berlin, Germany, November 22-23, 2010.

Towards Privacy-Friendly Online Advertising

Internet advertising is a very successful form of advertising as it provides an easy and effective way for advertisements to be targeted to individual users' interests. Obviously, learning users' private information is of tremendous importance for the success of targeted advertising and its business model. This leads the stakeholders (e.g., the ad networks) to deploy mechanisms to profile users. Currently, the most widely deployed techniques to track users' activities online are mostly based on exploiting client-side browser state (e.g., third-party cookies). Unfortunately, these techniques can allow access to users' browsing information and lead to the identification of users. Users are thus in need of a way to control the sharing of their browsing information with advertisers in order to protect their privacy. We propose a privacy-preserving cookie-management mechanism that enables advertisements to have discrimination capabilities without allowing for excessive tracking of users.

- J. Freudiger, N. Vratonjic, and J.-P. Hubaux. **Towards Privacy-Friendly Online Advertising**. In *IEEE Web 2.0 Security and Privacy (W2SP) 2009*, Oakland, California, May 21, 2009.

The Inconvenient Truth about Web Certificates

Authentication of publishers' Web servers and ad networks' ad servers is a necessary part of the proposed solutions to secure online advertising systems. The de facto solution for authentication on the Internet is based on digital certificates. Yet, the provided security is dubious, notably because of the obscure management of digital certificates. We investigate this problem and provide a large-scale empirical analysis of the current deployment of certificate-based authentication.

- N. Vratonjic, J. Freudiger, V. Bindschaedler and J.-P. Hubaux. **The Inconvenient Truth about Web Certificates**. *Workshop on Economics of Information Security (WEIS) 2011*, Fairfax, Virginia, USA, June 14-15, 2011.

Ad-blocking Games: Monetizing Online Content Under the Threat of Ad Avoidance

Much of the Internet economy relies on online advertising for monetizing digital content: Users are expected to accept the presence of online advertisements in exchange for content being free. However, online advertisements have become a serious problem for many Internet users: while some are merely annoyed by the incessant display of distracting ads cluttering Web pages; others are highly concerned about the privacy implications - as ad providers typically track users' behavior for ad targeting purposes. Similarly, security problems related to technologies and practices employed for online advertisement have frustrated many users. Consequently, a number of software solutions have emerged that block online ads from being downloaded and displayed on users' screens as they browse the Web. We focus on these advertisement avoidance technologies for online content and their economic ramifications for the monetization of websites. More specifically, our work addresses the interplay between users' attempts to avoid commercial messages and content providers' design of countermeasures. Our investigation is substantiated by the development of a game-theoretic model that serves as a framework usable by content providers to ponder their options to mitigate the consequences of ad avoidance techniques. We complement our analytic approach with simulation results, addressing different assumptions

about user heterogeneity. Our findings show that publishers who treat each user individually, and strategically deploy fee-financed or ad-financed monetization strategy, obtain higher revenues, compared to deploying one monetization strategy across all users. In addition, our analysis shows that understanding the distribution of users' aversion to ads and valuation of the content is essential for publishers to make a well-informed decision.

- N. Vratonjic, H. Manshaei, J. Grossklags and J.-P. Hubaux. **Ad-blocking Games: Monetizing Online Content Under the Threat of Ad Avoidance**. *Workshop on Economics of Information Security (WEIS) 2012*, Berlin, Germany, June 25-26, 2012.

Hyper Geolocalization for Location-targeted Advertising

Location privacy has been extensively studied over the last few years, especially in the context of location-based services where users purposely disclose their location to benefit from convenient context-aware services. To date, however, little attention has been devoted to the case of users' location being unintentionally compromised by others. We study a concrete and widespread example of such situations, specifically the location-privacy threat created by access points (e.g., public hotspots) using network address translation (NAT). Indeed, because users connected to the same hotspot share a unique public IP, a single user making a location-based request is enough to enable a service provider to map the IP of the hotspot to its geographic coordinates, thus compromising the location privacy of all the other connected users. When successful, the service provider can locate users within a few hundreds of meters, thus improving over existing IP-location databases. Even in the case where IPs change periodically (e.g., by using DHCP), the service provider is still able to update a previous (IP, Location) mapping by inferring IP changes from authenticated communications (e.g., cookies). Our contribution is three-fold: (i) We identify a novel threat to users' location privacy caused by the use of shared public IPs. (ii) We formalize and analyze theoretically the threat. The resulting framework can be applied to any access-point to quantify the privacy threat. (iii) We experimentally assess the state in practice by using real traces of users accessing Google services, collected from deployed hotspots. Also, we discuss how existing countermeasures can thwart the threat.

- N. Vratonjic, K. Huguenin, V. Bindschaedler and J.-P. Hubaux. **How Others Compromise Your Location Privacy: The Case of Shared Public IPs at Hotspots**. *Privacy Enhancing Technologies Symposium (PETS), 2013* Bloomington, Indiana, USA, July 10-12, 2013.

EVENTS

WEIS
GameSec
Usenix Security
W2SP

PEOPLE

Prof. Jean-Pierre Hubaux
Dr. Nevena Vratonjic
Dr. Julien Freudiger
Dr. Mohammad Hossein Manshaei
Dr. Maxim Raya

Collaborators

Prof. David C. Parkes,
Harvard University
Prof. Márk Félegyházi
BME, Hungary
Prof. Jens Grossklags,
Pennsylvania State
University