LABORATORY FOR COMMUNICATIONS AND APPLICATIONS LCA

Privacy and Security Games

Printer-friendly concise version of this page

Security and privacy are often studied by focusing on how (rather than why) attacks are perpetrated. However, in practice, the attacker is motivated by various incentives and his success often depends on his (limited) capabilities, and on users' defensive strategies. Moreover, due to their inherent interconnected nature, users often face mutual security and privacy risks. In many cases, the selfish behavior of users with misaligned incentives results in inefficient outcomes for all stakeholders. Game theory has demonstrated to be very powerful for modeling and analyzing the interplay between rational agents with (possibly) conflicting interests. Consequently, it is a key tool for studying attacker-defender interactions in security and privacy environments. It is also very relevant for analyzing the strategic behaviors of interconnected agents in networked systems.

At the Laboratory for Communications and Applications 1 (EPFL), we have applied game theory in order to analyze several privacy and security problems. We have analyzed individuals' decisions about how to manage and secure their genomic data. In the context of location privacy, we have modeled and analyzed the best strategies of mobile users against a strategic adversary, the outcomes resulting from non-cooperative behavior, and incentives to foster collaboration in location privacy-preserving mechanisms. In addition, we have studied the interactions between various stakeholders in online advertising and we have designed optimal protocols for revoking users in ephemeral networks.

LCA Contributions

Location Privacy

In mobile networks, authentication is a required primitive of the majority of security protocols. However, an adversary can track the location of mobile nodes by monitoring pseudonyms used for authentication. A frequently proposed solution to protect location privacy suggests that mobile nodes collectively change their pseudonyms in regions called mix zones. Because this approach is costly, self-interested mobile nodes might decide not to cooperate and could thus jeopardize the achievable location privacy. In this work, we analyze the non-cooperative behavior of mobile nodes with a game-theoretic model, where each player aims at maximizing its location privacy at a minimum cost. We first analyze the Nash equilibria in -player complete information games. Because mobile nodes in a privacy-sensitive system do not know their opponents' payoffs, we then consider incomplete information games. We establish that symmetric Bayesian-Nash equilibria exist with simple threshold strategies in -player games and derive the equilibrium strategies. By means of numerical results, we show that mobile nodes become selfish when the cost of changing pseudonym is small, whereas they cooperate more

when the cost of changing pseudonym increases. Finally, we design a protocol - the PseudoGame protocol - based on the results of our analysis.

- R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, J.-Y. Le Boudec, “Protecting location privacy: Optimal Strategy Against Localization Attacks,” In ACM Conference on Computer and Communications Security (CCS), 2012.
- F. Santos, M. Humbert, R. Shokri, and J.-P. Hubaux, “Collaborative Location Privacy with Rational Users,” In GameSec 2011.
- M. Humbert, M.H. Manshaei, J. Freudiger, and J.-P. Hubaux, “Tracking Games in Mobile Networks,” In GameSec 2010.
- J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, “On Non-cooperative Location Privacy: A Game-theoretic Analysis,” In ACM Conference on Computer and Communications Security (CCS), 2009.

Survey of Applications of Game Theory to Communication Networks

- M.H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux, "Game Theory Meets Network Security and Privacy", in ACM Computing Surveys, June 2013

Genomic Privacy

Over the last few years, the vast progress in genome sequencing has highly increased the availability of genomic data. Today, individuals can obtain their digital genomic sequences at reasonable prices from many online service providers. Individuals can store their data on personal devices, reveal it on public online databases, or share it with third parties. Yet, it has been shown that genomic data is very privacy-sensitive and highly correlated between relatives. Therefore, individuals' decisions about how to manage and secure their genomic data are crucial. People of the same family might have very different opinions about (i) how to protect and (ii) whether or not to reveal their genome. We study this tension by using a game-theoretic approach. First, we model the interplay between two purely-selfish family members. We also analyze how the game evolves when relatives behave altruistically. We define closed-form Nash equilibria in different settings. We then extend the game to N players by means of multi-agent influence diagrams that enable us to efficiently compute Nash equilibria. Our results notably demonstrate that altruism does not always lead to a more efficient outcome in genomic-privacy games. They also show that, if the discrepancy between the genome-sharing benefits that players perceive is too high, they will follow opposite sharing strategies, which has a negative impact on the familial utility.

- M. Humbert, E. Ayday, J.-P. Hubaux, and A. Telenti, “On Non-cooperative Genomic Privacy,” In Conference on Financial Cryptography and Data Security (FC), 2015.

Online Advertising

Some ISPs are trying to become part of the online advertising market. Such ISPs either: (i) cooperate with online advertising entities (e.g., ad networks) by providing users’ private information to achieve better ad targeting in exchange for a share of the revenue, or (ii) modify the ad traffic on-the-fly such that they divert part of the online advertising revenue for themselves. This is a very important issue because online advertising is the core business model on the Internet today and it fuels many free applications and services. We study this behavior using game theory to model the interactions between ISPs and ad networks, and we analyze the effects on the Web caused by ISPs taking part in online advertising. Our results show that if the users’ private information can improve ad targeting significantly or if ad networks do not have to pay a high share of revenue to the ISPs, ad networks and ISPs will cooperate to jointly serve online ads. Otherwise, ISPs will divert part of the online ad revenue for themselves. If the diverted revenue is small, ad networks will not react. However, if their revenue loss is significant, the ad networks will invest into improving the security of the Web and protecting their ad revenue.

- N. Vratonjic, M.H. Manshaei, J. Grossklags, and J.-P. Hubaux, “Ad-blocking Games: Monetizing Online Content Under the Threat of Ad Avoidance”, in WEIS 2012.
- N. Vratonjic, M. Raya, J.-P. Hubaux, D. C. Parkes, “Security Games in Online Advertising: Can Ads Help Secure the Web?,” In WEIS 2010.

ISPs and Ad Networks Against Botnet Ad Fraud

Botnets are a serious threat on the Internet and require huge resources to be thwarted. ISPs are in the best position to fight botnets and there are a number of recently proposed initiatives that focus on how ISPs should detect and remediate bots. However, it is very expensive for ISPs to do it alone and they would probably welcome some external funding.

Among others, botnets severely affect ad networks (ANs), as botnets are increasingly used for ad fraud. Thus, ANs have an economic incentive, but they are not in the best position to fight botnet ad fraud. Consequently, ANs might be willing to subsidize the ISPs to do so. We provide a game-theoretic model to study the strategic behavior of ISPs and ANs and we identify the conditions under which ANs are likely to solve the problem of botnet ad fraud by themselves and those under which the AN will subsidize the ISP to achieve this goal. Our analytical and numerical results show that the optimal strategy depends on the ad revenue loss of the ANs due to ad fraud and the number of bots participating in ad fraud.

- 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.

Trust and Privacy

As privacy moves to the center of attention in networked systems, and the need for trust remains a necessity, an important question arises: How do we reconcile the two seemingly contradicting requirements? In this paper, we show that the notion of data-centric trust can considerably alleviate the tension, although at the cost of pooling contributions from several entities. Hence, assuming an environment of privacy-preserving entities, we provide and analyze a game-theoretic model of the trust-privacy tradeoff. The results prove that the use of incentives allows for building trust while keeping the privacy loss minimal. To illustrate our analysis, we describe how the trust-privacy tradeoff can be optimized for the revocation of misbehaving nodes in an ad hoc network.

- M. Raya, R. Shokri, and J.-P. Hubaux, "On the Tradeoff between Trust and Privacy in Wireless Ad Hoc Networks," In ACM Conference on Wireless Network Security (WiSec), March 2010.

Revocation in Ephemeral Networks

A frequently proposed solution to node misbehavior in mobile ad hoc networks is to use reputation systems. But in ephemeral networks - a new breed of mobile networks where contact times between nodes are short and neighbors change frequently - reputations are hard to build. In this case, local revocation is a faster and more efficient alternative. In these papers, we define several game-theoretic models to analyze the various local revocation strategies. We establish and prove the conditions leading to Nash equilibria. We also derive the optimal parameters for voting-based schemes. Then we design a protocol based on our analysis and the practical aspects that cannot be captured in the model. With realistic simulations on ephemeral networks we compare the performance and economic costs of the different techniques.

- I. Bilogrevic, M. H. Manshaei, M. Raya, and J.-P. Hubaux, "Optimal Revocations in Ephemeral Networks: A Game-Theoretic Framework," In WiOpt, 2010.
- M. Raya, M. H. Manshaei, M. Felegyhazi, and J.-P. Hubaux, "Revocation Games in Ephemeral Networks," In ACM Conference on Computer and Communications Security (CCS), 2008.

EVENTS

GameSec
GameNets

PEOPLE

Prof. Jean-Pierre Hubaux

Alexandra Mihaela Olteanu

Collaborators

Prof. Tansu Alpcan
Prof. Tamer Basar
Prof. Mark Felegyhazi
Dr. Mathias Humbert
Prof. Hossein Manshaei
Prof. David C. Parkes
Dr. Reza Shokri
Quanyan Zhu

CONTACT

Alexandra Mihaela Olteanu
Prof. Jean-Pierre Hubaux

| © 2017 EPFL tous droits réservés