Economics of Security and game theory for security risk management

Patrick Maillé, Peter Reichl Bruno Tuffin

TELECOM Bretagne, FT Wien, INRIA-Rennes Bretagne Atlantique

EconTel WG 4, Vienna, Austria

Context: security and game theory

- Network security mechanisms aim at protecting against "natural" failures and volontary attacks.
- This implies that the actions of the attacker be foreseen and countered:
  - Security mechanisms depend on the defender's knowledge of the possible attacks,
  - and the attacker will take into account the target's defense strategies when determining its own attack type.
  - Non-cooperative game theory is the typical modeling framework.
- Increasing security is often at the expense of performance (bandwidth for instance).
- Similarly, developping an attack can incur a cost.
- Those trade-offs have to be analyzed.

Context: economics of security

- Besides the interactions between malicious attacks and protection strategies, security brings new economic issues to network service providers.
- Game theory again allows to represent the business interactions between
  - a provider and its customers first,
  - but also to represent competition among providers for customers having to choose between different offers.
- The growth of a network such as the Internet has had a positive externality from a business point of view, but has also a negative externality when talking about security.

Outline

Model based on risk percentage

Something we are currently working on.

- A provider has different *initial* security levels (or classes) $\ell \in \{1, \ldots, L\}$, to which an intrusion risk r_ℓ is associated, with

$$r_{\ell_1} < r_{\ell_2} \text{ for } \ell_1 < \ell_2$$

  and a price p_ℓ with

$$p_{\ell_1} > p_{\ell_2} \text{ for } \ell_1 < \ell_2.$$

- Security levels may correspond to various options concerning the availability of hardware or software security.
- A typical situation is virus scan softwares, where different softwares can have different efficiencies but are also sold at different prices.
- The larger number of customers on a class, the more likely new attacks will happen (according to Metcalfe's or a power law for instance)
- Indeed attacks basically concentrate on larger populations.
- Demand splits among the different classes, but the larger the number in a class the smaller the *actual* security level.

Two contexts for modeling

- Assuming non-atomic users, demand can then be characterized by a so-called Wardrop equilibrium, i.e. a combination of price and actual security risk which is the same for all classes having positive demand.
- Providers can then determine their security levels and prices.
- Two situations can be considered:
  - all the levels are managed by a single provider (a monopoly) which then tries to maximize its revenue by paying with prices,
  - or each security level is handled by an independent provider, and providers compete for customers at a higher level by playing on prices (an oligopoly).
- We expect to determine the resulting equilibria.

A related work

Marc Lelarge. Economics of Malware: Epidemic Risks Model, Network Externalities and Incentives (2008).

Framework:

- network of interconnected agents, subject to epidemic risks;
- each agent can decide to invest to self-protect, decreasing the probability of contagion;
- SImple model:
  - Two states by agent: S (Safe) or N (Not safe), with respective loss probability p^S and p^N ($p^S < p^N$).
  - Investing in security induces a cost c. If w initial wealth and ℓ the loss when infected:
  - In N, expected wealth is $p^N(w-\ell)+(1-p^N)w$, and $p^S(w-\ell-c)+(1-p^S)(w-c)$ in S.
  - Interest in investing if $c < (p^N - p^S)\ell$.
  - When several levels of security, invest in level j if $c_j < (p^N - p^j)\ell$.

Case of a graph

- Direct probability of infection p_j when security level j, and p^+ when N.
- Neighbors contaminated with probability q_j if the neighbor is in level j and q^+ if in N.
- each agent has his own c and ℓ, as private information.
- γ vector providing the fraction of population in each security level. The p^j and p^N depends on γ.
- There is then a fixed point equation to determine the equilibrium.
- Externalities determined using results on random graph theory.

Coalitions when competing security service providers

- Cooperation becomes an issue.
- Indeed, a low security provided by a competitor induces a risk for its own customers, and therefore a lower security level.
- Coalition formation can thus become efficient for providers, in terms of reputation and revenue.
- Goal: designing suchs models to investigate the incentive for forming such coalitions, and whether or not a full cooperation is the best solution for all providers.

Illustration of a game between attackers and defenders

Alpcan, T., Basar, T. A game theoretic approach to decision and analysis in network intrusion detection. In: *Proceedings of the 42nd Conference on Decision and Control*. Maui, HI (2003)

- The attacker can launch an attack or do nothing,
- The defender can trigger or not its (costly) detection scheme.
- Game with no pure Nash equilibrium for reasonable payoffs

	Attack	No attack
Trigger detection	$(a, -\alpha)$	$(-b, 0)$
No detection	$(-c, \gamma)$	$(0, 0)$

- Usually $c \gg b$.

Equilibrium in mixed strategies

Unique equilibrium in mixed strategies if $c > 2b$

- If π_{def} the probability of the defender triggering the detection scheme, and by π_{att} the probability of the attacker launching the attack
- utilities

$$\begin{aligned} u_{def}(\pi_{def}, \pi_{att}) &= a\pi_{def}\pi_{att} - b\pi_{def}(1-\pi_{att}) - c\pi_{att}(1-\pi_{def}) \\ u_{att}(\pi_{def}, \pi_{att}) &= -\alpha\pi_{def}\pi_{att} + \gamma\pi_{att}(1-\pi_{def}). \end{aligned}$$

- By derivation, we obtain $\pi_{att} = \frac{b}{a+b+c}$ and $\pi_{def} = \frac{\gamma}{\alpha+\gamma}$.
- Can be easily extended to a set of attacks and a set of defense.
- Real challenge in the area: determining utility functions

Other kinds of useful games

- Repeated games to include the time aspect into game theory.This also allows to build mechanisms that sanction non-contributing (to security) actors, in order to create the proper incentives.
- Stochastic games, which also have memory and are played over time, but memory is represented by a state (ex: not compromised, compromised, stolen, the type of application used, the ongoing attacks and activated countermeasures, etc).
  - There is a *transition probability* for each state, that depends on the actions taken by the players at the current period.
- Bayesian games characterized by an *incomplete* information about the opponents (e.g. their payoff functions).
  - In a security context. Ex: the difference between malicious attackers and non-malicious ordinary users who are accessing the system regularly.
  - The system only has a belief, e.g. a probability distribution between malicious/non-malicious users.
  - Belief probability distributions updated in the course of the game according to Bayes' rule.

Worm propagation games

A. Ganesh, et al.: Efficient quarantining of scanning worms: Optimal detection and co-ordination. In: IEEE INFOCOM. Barcelona, Spain (2006)

- Worm propagation characterized by fluid models, which can represent a large population of vulnerable hosts.
- For total population N, I_t number of infected ndes at time t.
- Simplest evolution

$$\frac{dI_t}{dt} = \beta I_t (N - I_t)$$

with β rate of infection. Here speed of infection depends on the number of nodes infected, but also the remaining ones.

- In the slow start phase $\frac{dI_t}{dt} = \beta N I_t$, whose solution is $I_t = I_0 e^{-\beta N t}$.
- Countermeasures affect the rate at which nodes are infected, with reduction θ_t so that

$$\frac{dI_t}{dt} = \beta N \left[I_0 \theta_0 + \int_0^t I_s \theta_{t-s} ds \right],$$

whose solution is $I_t = I_0 + \int_0^t I_{t-s} \beta N \theta_s ds$.

Description of the game

- Stackelberg game with
  - the leader, the worm, playing first its strategy,
  - to which the detection and containment technique responds (the follower)
  - Example: quarantining strategy for time τ, $\theta_t = P[\tau \geq t]$.
  - Pay-off is the speed of spread
  - Detection is performed through a CUSUM (cumulative sum) test.

Conclusions

- Game theory a relevant tool for describing both
  - interactions between attackers and defenders
  - interactions between cuctomers and security providers as well as competition among security providers.
- Current common activity between GET, INRIA and FTW.
- STSM of Patrick last December on this issue, as well as mine this week