# Some examples of security games

Patrick Maillé, Peter Reichl, Bruno Tuffin

Telecom Bretagne, FTW, INRIA-Centre Bretagne Atlantique

COST IS0605 (Econ@tel) WG4 meeting, Vienna, Apr 2009



# Outline

1. To insist on the attack or to stop?
   - Model
   - Attacker's point of view
   - The information game for targets: claim to be secure!
2. Routing ("cat-and-mouse") games
   - Malicious packet hiding within normal flow: attacker as the mouse
   - Malicious packet scanning: attacker as the cat
3. Conclusion

# Outline

# Model

*Cremonini, M, Nizovtsev, D. Understanding and influencing attackers? decisions : implications for security investment strategies In: Proc. of 5h Workshop on the Economics of Information Security (WEIS 2006), Cambridge (UK), 2006*

- $N$ potential targets, and some attackers
- An attacker can attack one target at a time, and put *progressively* a certain amount of effort $x$ into the attack, with increasing and convex cost $C(x)$
- Probability of success of the attack: $\pi(x)$
- If the attack succeeds, the attacker gets reward $G$.

# Attacker's point of view

- Objective=maximum benefit (as usual...)
- Strategy: **when to stop the attack?** $\Rightarrow$ optimal stopping rule

The attacker computes the *expected gain of carrying on with the attack* until $\hat{x}$ if there has been no success until $x$ (thus $C(x)$ has already been spent):

$$\int_x^{\hat{x}} \underbrace{\rho(\tau)}_{\substack{\text{Cond distrib}| \\ \text{no success at x}}} \underbrace{(G - C(\tau) + C(x))}_{\text{gain}} d\tau - \underbrace{\left(1 - \int_{\hat{x}}^{+\infty} \rho(\tau))d\tau\right)}_{\mathbb{P}(\text{failure})} (C(\hat{x}) - C(x))$$

# Attacker's point of view

- Objective=maximum benefit (as usual...)
- Strategy: **when to stop the attack?** $\Rightarrow$ optimal stopping rule

The attacker computes the *expected gain of carrying on with the attack* until $\hat{x}$ if there has been no success until $x$ (thus $C(x)$ has already been spent):

$$\int_x^{\hat{x}} \underbrace{\rho(\tau)}_{\substack{\text{Cond distrib}| \\ \text{no success at x}}} \underbrace{(G - C(\tau) + C(x))}_{\text{gain}} d\tau - \underbrace{\left(1 - \int_{\hat{x}}^{+\infty} \rho(\tau))d\tau\right)}_{\mathbb{P}(\text{failure})} (C(\hat{x}) - C(x))$$

**Application**: if $C'(x) = \alpha_0 + \alpha_1 x$ and $\pi(x) = 1 - e^{-x/\mu}$ (i.e. $\mu \approx$security level), then *Best strategy:*

$$\textit{stop at } x = \frac{G}{\mu} - \frac{\alpha_0}{\alpha_1}$$

# Switching targets

- Assume there is a switching cost $C_S$ for the attacker to change targets
- The attacker changes targets if the expected benefit of going on with the current target gets below the difference (exp. benef. with new target - switching cost)

$\Rightarrow$the attack effort before switching increases with $C_S$

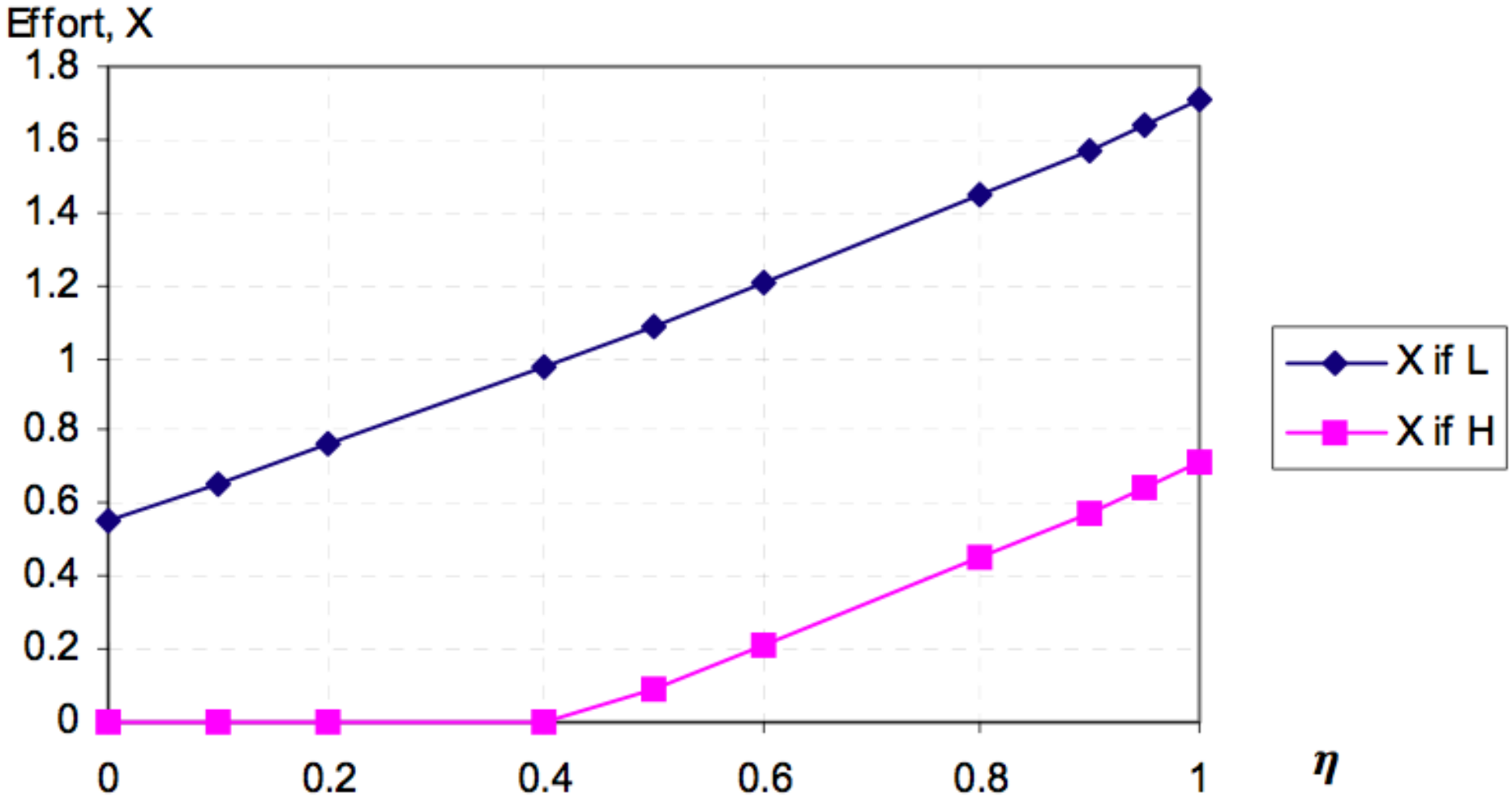
With heterogeneous targets (High or Low security protection), assuming the attacker realizes the target security level after switching to it

$\Rightarrow$ the attacker insists less on high-security targets

Therefore there is a double protection effect, the indirect one being prominent

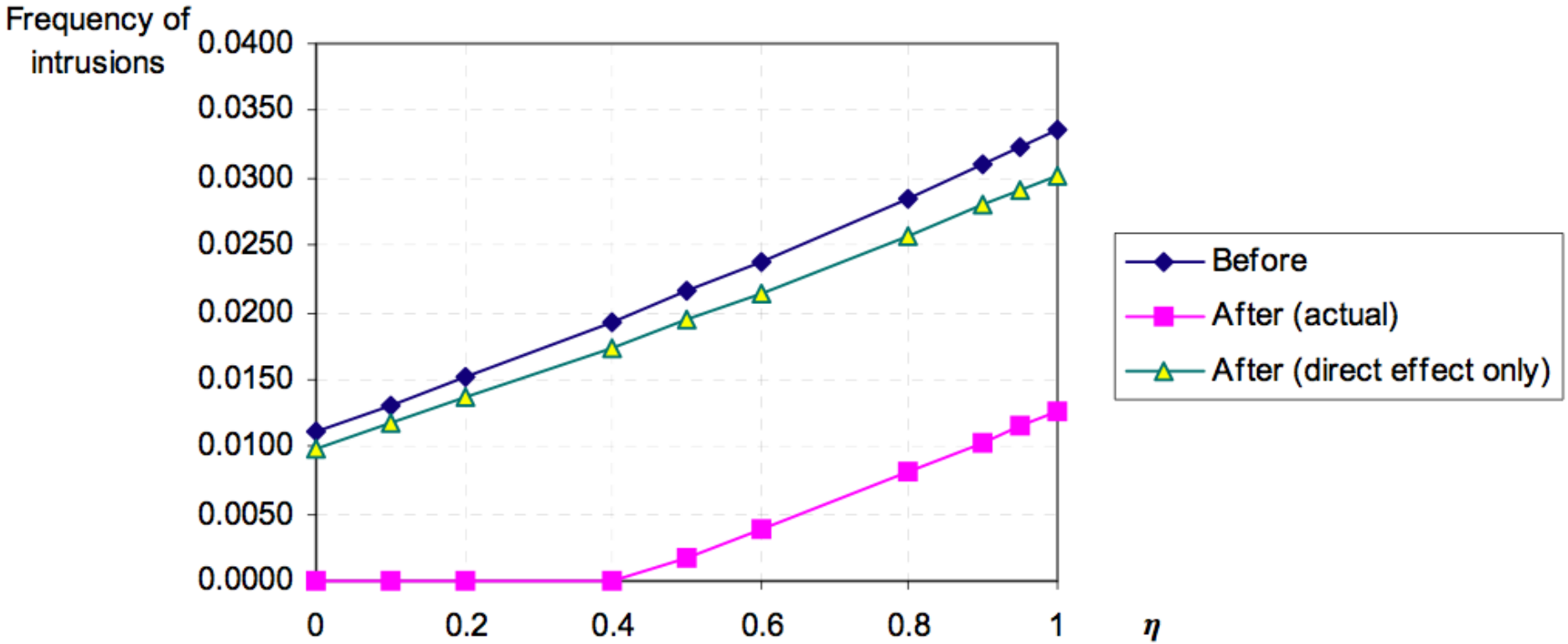
# The indirect or behavioral effect

$\eta$=proportion of H-type targets



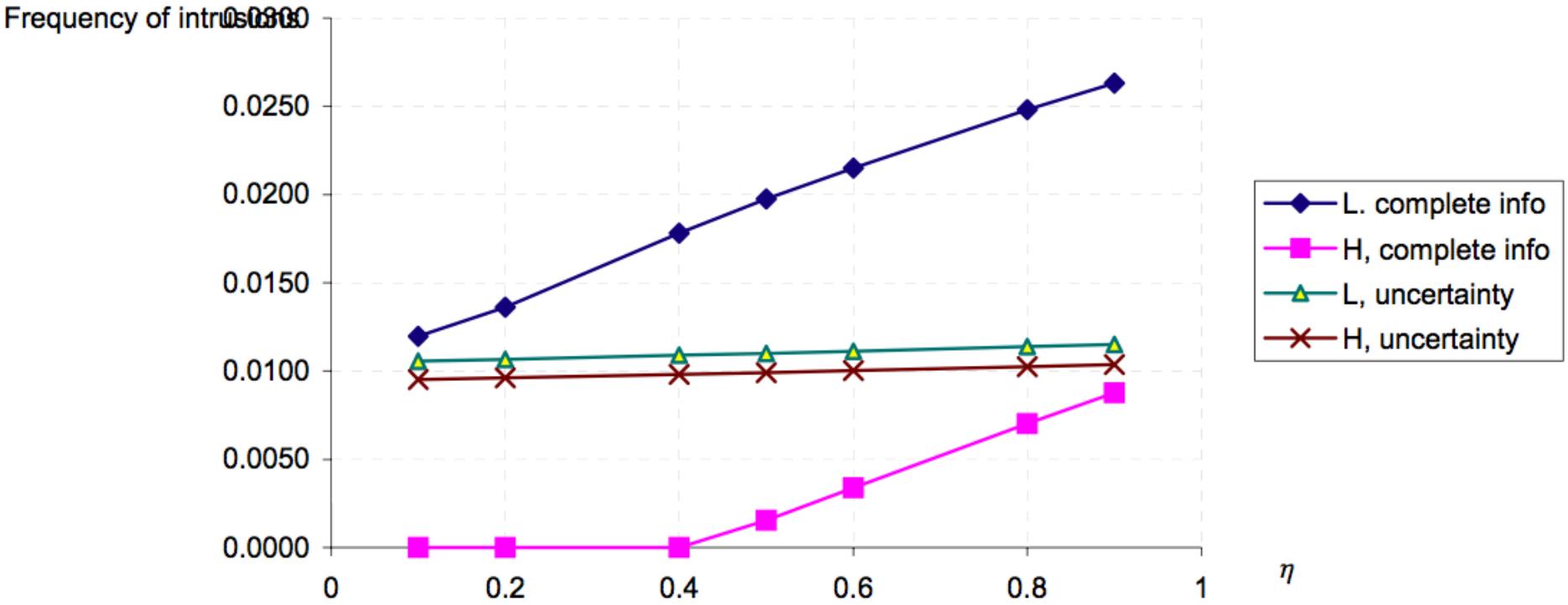
# Defender's point of view: worthiness of security improvement

Take an L-type target considering the possibility of a security improvement



# The information game for targets: claim to be secure!

- Different model: now the attacker does not know whether the target has high or low security level. Instead, Bayesian inference is performed (calculation of $\mathbb{P}(\text{high security}|\text{no success until } x)$).
- Result: low-security targets are better off and high-security targets are worse off than in the full information case.




$\eta$ =proportion of H-type targets

# The importance of information

- The H-type targets should advertise (if possible, prove) that they are H-type;
- the L-type targets should try to hide the fact that they are L-type.

Therefore the security of the info delivered by targets should be investigated...

**Possible extensions of the model**

- What if the damage is not a boolean, but an increasing function of the effort and decreasing in the security level? (example of denial-of-service attacks)
- What if the security effort is not for once, but has to be maintained (with associated costs)?

# Outline

# Routing games in security

- Games played over the links (or node interfaces) of a network.
- Strategy sets:
  - a link in the network (to carry out an attack, or put an attack detection device),
  - or a whole routing strategy (choice of flow or attack spreading among different available paths).

Model: zero-sum game $U_{\text{attacker}} = -U_{\text{defender}}$.

# Malicious packet hiding within normal flow: attacker as the mouse

*Kodialam, M., Lakshman, T.V.: Detecting network intrusions via sampling: A game theoretic approach. In: Proc. of IEEE INFOCOM. San Francisco, CA, USA (2003)*

Game between an attacker trying not to be detected, and an active defender.

- Attacker should select a path to send his malicious packet so as to minimize the detection probability.
- Malicious packet is less detectable on highly loaded links.
- Defender should select which links to scan so as to maximize the detection probability (with a constraint $B$ in the number of scanned bits per time unit).

# Solution of the game

The Nash equilibrium value of the detection probability is $B/M(f)$, where

- $M(f)$ is the max-flow from the attacker location to the target, assuming each link $e$ has capacity $f_e$,
- with $f_e$ the background traffic on link $e$.

Nash strategies:

- if $m_i$ denotes the flow on the $i$th path for the max-flow mentioned above, attacker chooses that path with probability $m_i/M(f)$.
- Defender selects a *minimum cut* of that maximum flow, and scans each of the links $e$ in the cut with probability $Bf_e/M(f)$.

# Malicious packet scanning: attacker as the cat

*Bohacek, N., Hespanha, J.P., Lee, J., Lim, C., Obraczka, K.: Game theoretic stochastic routing for fault tolerance and security in computer networks. IEEE Transactions on Parallel and Distributed Systems* **18***(9), 1227–1240 (2007)*

Model with roles somehow inverted.
Defender wants to send some flow from one point to another, through a network with vulnerable links: if the attacker attacks a used link $\ell$,then the data is intercepted with probability $p_\ell$.
Player strategies:

- The attacker spreads his (limited) scanning effort among the links.
- The defender chooses routes for his flow.

Existence of a Nash equilibrium, computed through a max-flow problem

# Outline

# Conclusion

- Very different models were the protagonists take the decision of their opponent into account
- Literature on game theory applied to network security is very recent

$\Rightarrow$ A lot to do...