

# Modeling the economic incentives of DDoS Attacks: femtocell case study<sup>1</sup>

Vicente Segura ([vsg@tid.es](mailto:vsg@tid.es))

WEIS Conference  
**25th of June, 2009**

1. This material is based upon work supported by the SEGUR@ Project funded by the Centre for the Development of Industrial Technology (CDTI) of the Spanish Ministry of Science and Innovation



# Index

- 01 Introduction**
  - Risk analysis methodologies
  - Applying economic models
- 02 Use case presentation**
  - Case of study
  - Supply chain of DDoS attacks
- 03 Economic model**
  - The model
  - Application of the model
- 04 Conclusion**

# 01 Introduction

## Risk analysis methodologies

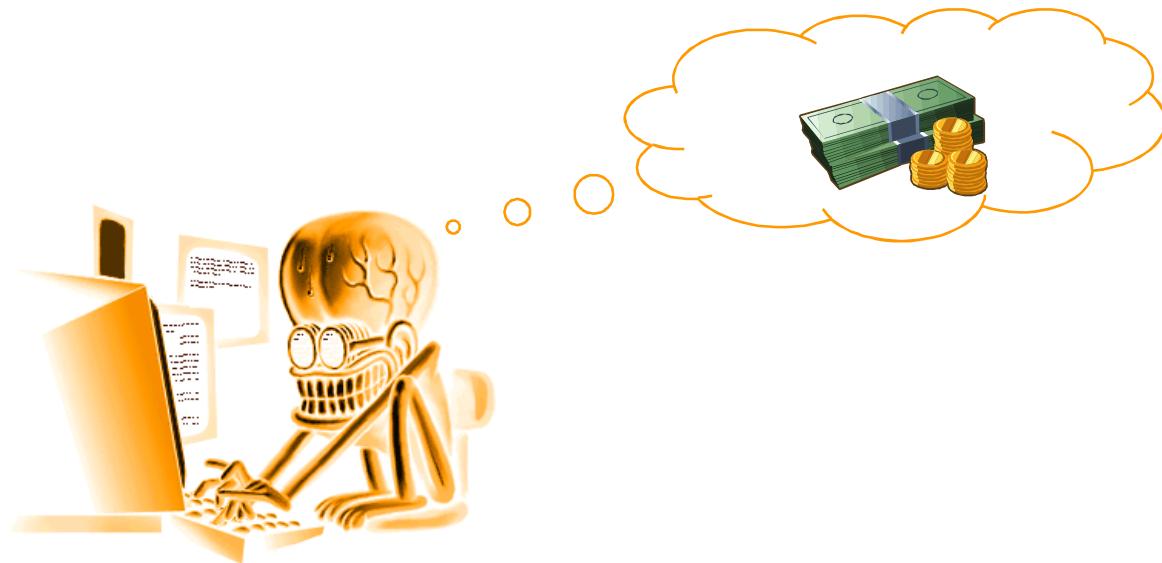


- They all offer procedures for identifying and calculating risks
- But they require to estimate some factors (such as frequency of occurrence, impact ...) whose knowledge is not evident

# 01 Introduction

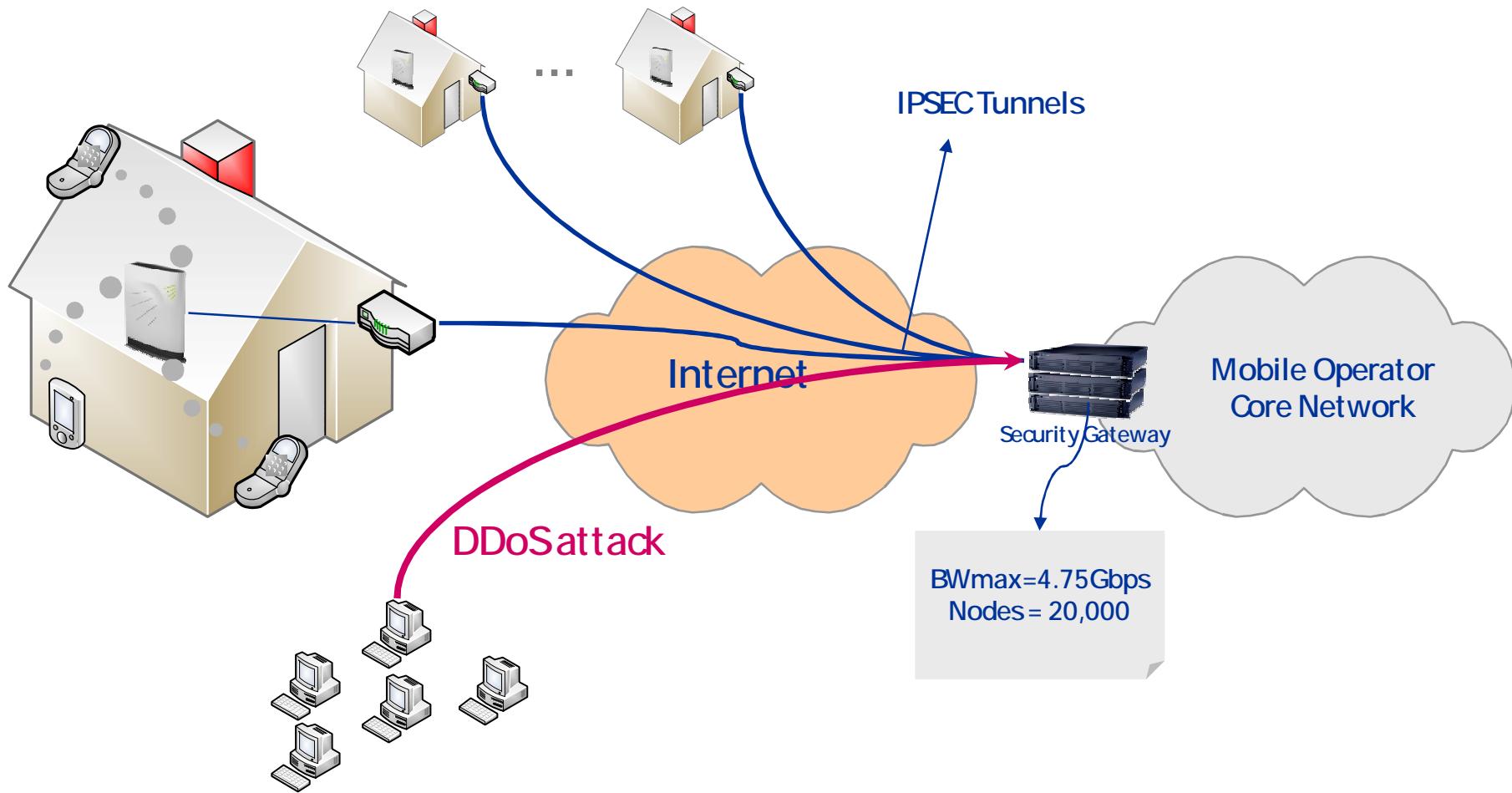
## Applying economic models

- n **Assuming that:**
  - Attackers are rational and
  - they act moved by money ...
- n **Applying economic models can help to estimate some of those factors**



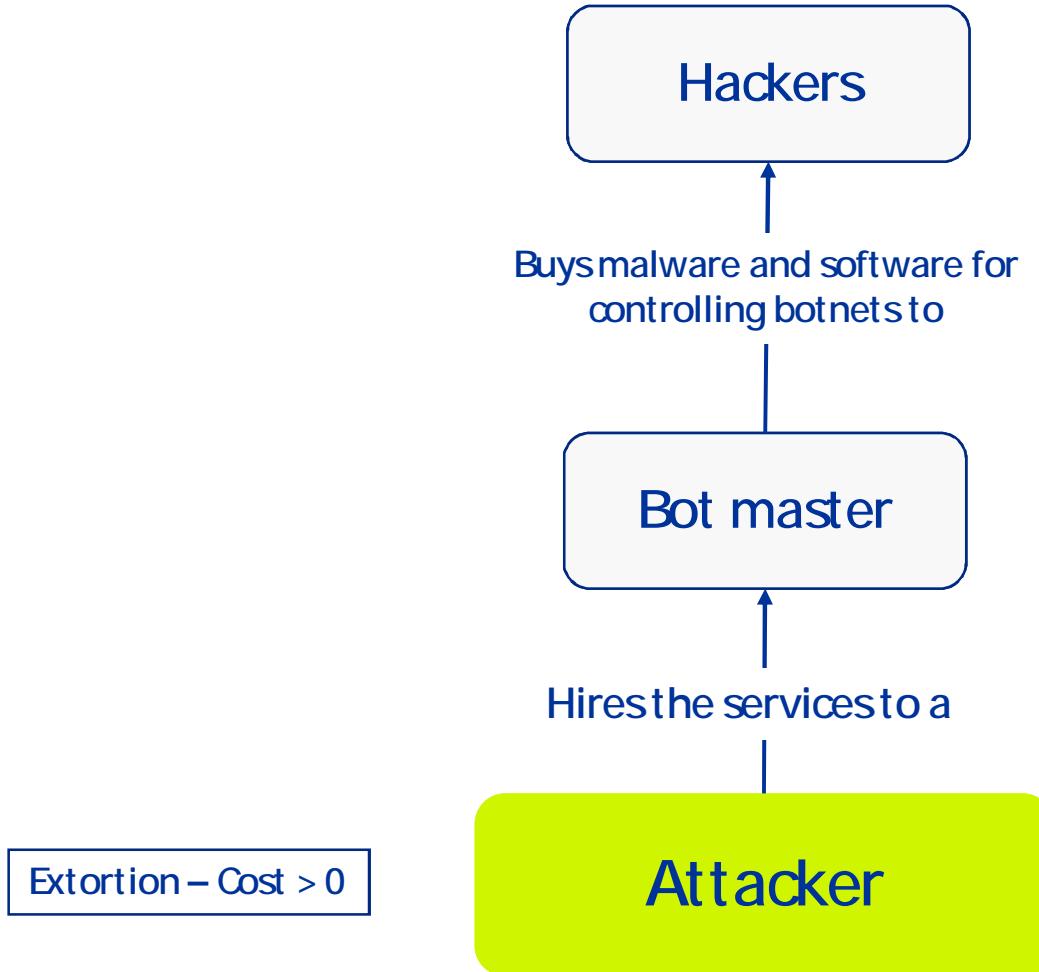
## 02 Use case presentation

### Case of study



## 02 Use case presentation

### DDoS attack supply chain



# 03 Economic model

## The model

$$\text{Profit} = \text{Extortion} - \text{Cost} > 0$$

### n Extortion:

- Assumptions:
  - Depend on victim revenues (revenues per SeGW):  $f(R)$
  - Just a percentage of the victim will give in to blackmail ( $\alpha$ )

$$\text{Extortion} = \alpha \cdot f(R) \approx \alpha \cdot k \cdot R$$

### n Cost of renting the botnet:

- Depends on:
  - Bandwidth of the attack ( $A$ )
  - Duration of the attack ( $t$ )

$$\text{Cost} = g(A, t)$$

## 03 Economic model

### Extortion

- n **Average revenue per SeGW:**
  - Femtocells per SeGW: 20,000<sup>1</sup>
  - Monthly average revenue per femtocell: 28\$<sup>2</sup>
- n **Relation between revenues and extorted amount (k): 0.001<sup>3</sup>**

$$\text{Extortion} = \alpha \cdot f(R) \approx \alpha \cdot k \cdot R = \alpha \cdot (0.001) \cdot (6,720,000) = \alpha \cdot 6,720 \text{ \$}$$

<sup>1</sup> Alcatel-Lucent VPN Firewall Brick 1200 HS (Femto Access Gateway)

<sup>2</sup> Femtocells in the consumer market: business case and marketing plan. Analysis Research

<sup>3</sup> Obtained by comparing 2004 figures of online betting sites with extortion demands

# 03 Economic model

## Cost – renting cost collection (1/2)

The screenshot shows a Firefox browser window with the following details:

- Title Bar:** Versión traducida de http:// /index.php - Mozilla Firefox
- Address Bar:** http://translate.google.com/translate?u=http%3A%2F%2F...&hl=es&ie=UTF-8
- Toolbar:** Archivo, Editar, Ver, Historial, Marcadores, Herramientas, Ayuda
- Menu Bar:** Más visitados, Comenzar a usar Fire..., Últimas noticias
- Content Area:**
  - Google Search Result:** SERVICIOS DDoS - || - Servicios DDoS
  - User Profile:** Jafar (24-9-2008, 16:27)
  - Text Content:** Esta página se ha traducido de forma automática del ruso. Ver la página web original o pasar el ratón por encima del texto para ver el idioma original.
  - Right Side Buttons:** Volver a la página de traducción, Eliminar frame
  - Bottom Left:** Traselurte, Grupo: Usuarios, Publicaciones: 2, Antigüedad: 18/9/2008, Miembro N°: 23 682
  - Bottom Right:** Puesto #1
- IM Conversation Window:** A separate window titled 'Versión traducida de http://forum...' shows a chat between two users. One user asks about launching a 4.75 GB DDoS attack and its cost, to which the other replies with a price of \$1000 per day.

## 03 Economic model

### Cost – renting cost collection (2/2)

- Cost of renting for one day a botnet for launching a successful attack: 900-1000 \$

| Cost of hiring DDoS service |              |           |
|-----------------------------|--------------|-----------|
| Bandwidth (Mbps)            | Duration (h) | Cost (\$) |
| 45                          | 2            | 20        |
| 45                          | 6            | 30        |
| 45                          | 12           | 50        |
| 45                          | 24           | 70        |
| 100                         | 24           | 75        |
| 1000                        | 24           | 250       |
| 1000                        | 24           | 100       |
| 1000                        | 168          | 600       |
| 4750                        | 24           | 900       |
| 4750                        | 168          | 5500      |
| 4750                        | 24           | 1000      |
| 4750                        | 168          | 6000      |
| 5000                        | 5            | 400       |

Source: Internet hacking forums, contact with bot masters

# 03 Economic model

## Cost-regression analysis

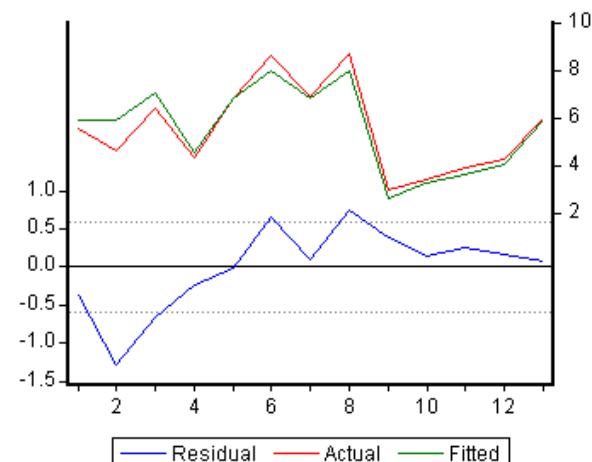
### n Regression function of cost

$$\text{Cost} = g(A,t) \approx K \cdot t^\alpha \cdot A^\beta = 0,964 \cdot t^{0.5903} \cdot A^{0.5869}$$

| Cost of hiring DDoS service |              |           |
|-----------------------------|--------------|-----------|
| Bandwidth (Mbps)            | Duration (h) | Cost (\$) |
| 45                          | 2            | 20        |
| 45                          | 6            | 30        |
| 45                          | 12           | 50        |
| 45                          | 24           | 70        |
| 100                         | 24           | 75        |
| 1000                        | 24           | 250       |
| 1000                        | 24           | 100       |
| 1000                        | 168          | 600       |
| 4750                        | 24           | 900       |
| 4750                        | 168          | 5500      |
| 4750                        | 24           | 1000      |
| 4750                        | 168          | 6000      |
| 5000                        | 5            | 400       |

### Results

$$\begin{aligned} R^2 &= 0.898 \\ K &= 0.9640 \\ \alpha &= 0.5903 \\ \beta &= 0.5869 \end{aligned}$$



# 03 Economic model

## Profit function

$$\text{Profit} = \text{Extortion-Cost} \approx \alpha \cdot k \cdot R - K \cdot t^\alpha \cdot A^\beta$$

$$\text{Profit} = f(\alpha, t, A)$$

$$\text{Profit} = \alpha \cdot 6720 - 0.964 \cdot t^{0.5903} \cdot A^{0.5869}$$

## 03 Economic model

### Application of the model (1/3)

#### n Maximum percentage of victims that pay to nullify incentives

##### — Assumptions:

- **t=24h** (Botnets must be rented for 24 h to be successful)
- **A=4750 Mbps** (The Security Gateway resists attacks of up to 4750 Mbps)

$$\text{Profit} = \alpha \cdot 6720 - 0.964 \cdot t^{0.5903} \cdot A^{0.5869} = 0$$

$$\alpha_{\text{MAX}} = 0.1347$$

## 03 Economic model

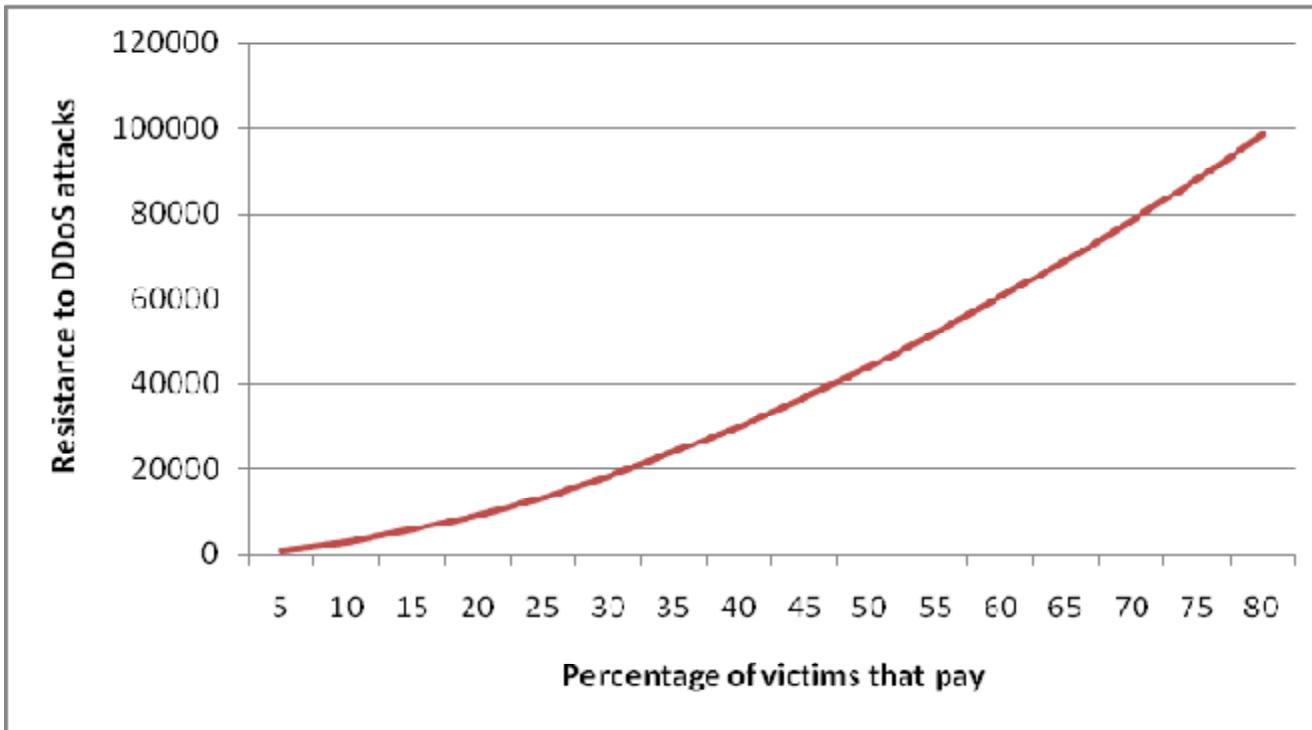
### Application of the model (2/3)

- n Required attack resistance of the security gateway to nullify profits as a function of the percentage of victims that pay

- Assumptions:

- t=24h (Botnets must be rented for 24 h to be successful)

$$A = \left( \frac{6720}{0.96 \cdot 24^{0.59}} \right)^{1.70} a^{1.70}$$



# 03 Economic model

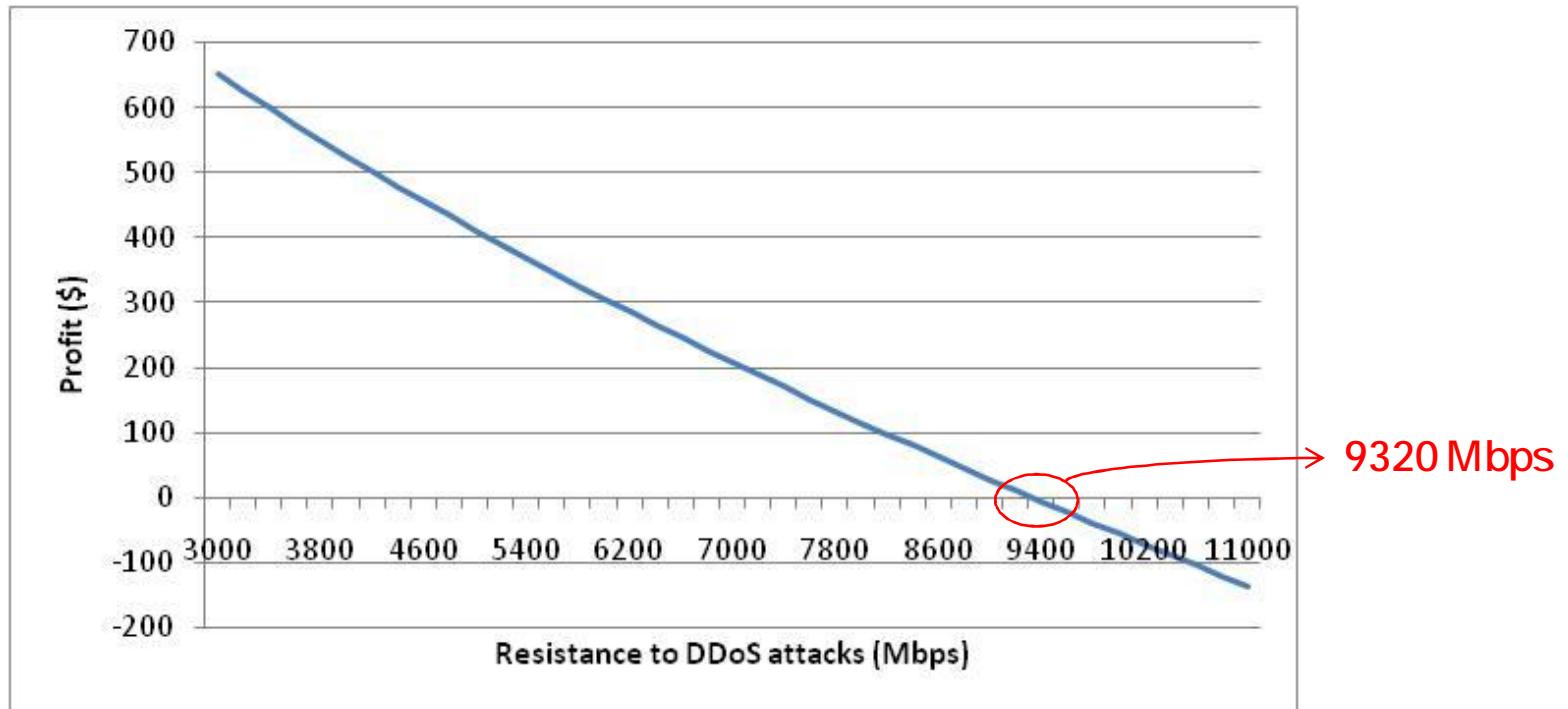
## Application of the model (3/ 3)

### n Required attack resistance of the security gateway to nullify profits

#### — Assumptions:

- $\alpha = 20\%$  (Attackers hope that 20% of victims give in to extortion)
- $t=24\text{h}$  (Botnets must be rented for 24 h to be successful)
- $A=4750 \text{ Mbps}$  (The Security Gateway resists attacks of up to 4750 Mbps)

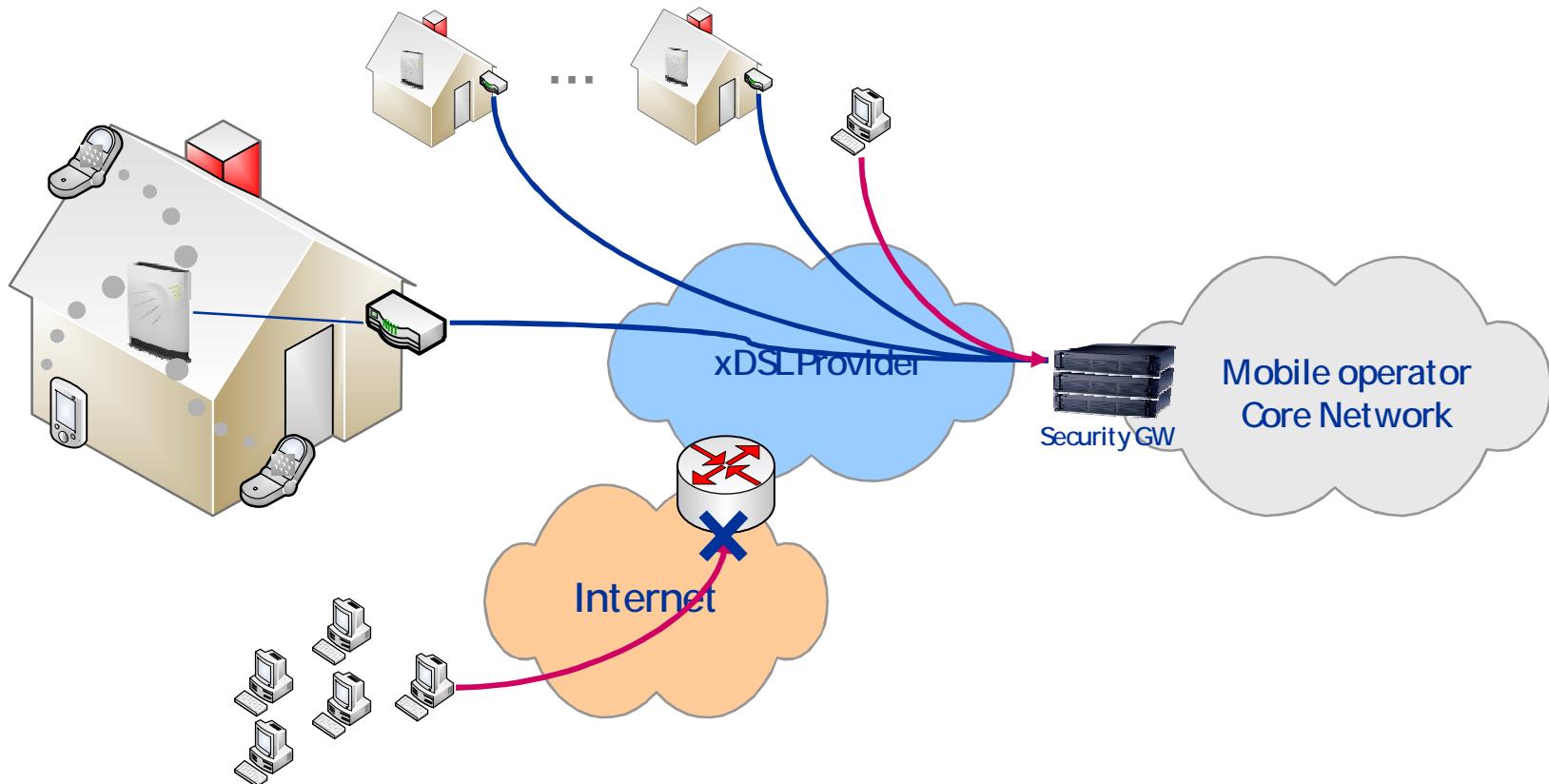
$$\text{Profit} = 0.2 \cdot 6720 - 0.964 \cdot 24^{0.5903} \cdot A^{0.5869} = 0$$



# 03 Economic model

## Strategies for mitigating risks

- n **Strategy 1: we choose a more DDoS attack-resistant security gateway**
- n **Strategy 2: we restrict access to security gateway to xDSL customers**



# 04 Conclusion

- **Things experienced during data collection:**
  - **Cybercriminals are highly specialized:**
    - Some sell the software
    - Others sell botnets or parts of them
    - Others offer DDoS attack services
  - **Cybercriminals are well organized:**
    - There is a fluent communication between them
    - They build botnets on demand
- **Results achieved:**
  - Simple model of attackers' incentives
  - Objective estimations of economic incentives for launching DDoS attacks
- **Limitations:**
  - It is difficult to collect data
  - Attackers are supposed to be rational and to act moved by economic incentives

# Questions



*Telefónica*

---