Modeling the economic incentives of DDoS Attacks: femtocell case study[1]

Vicente Segura (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

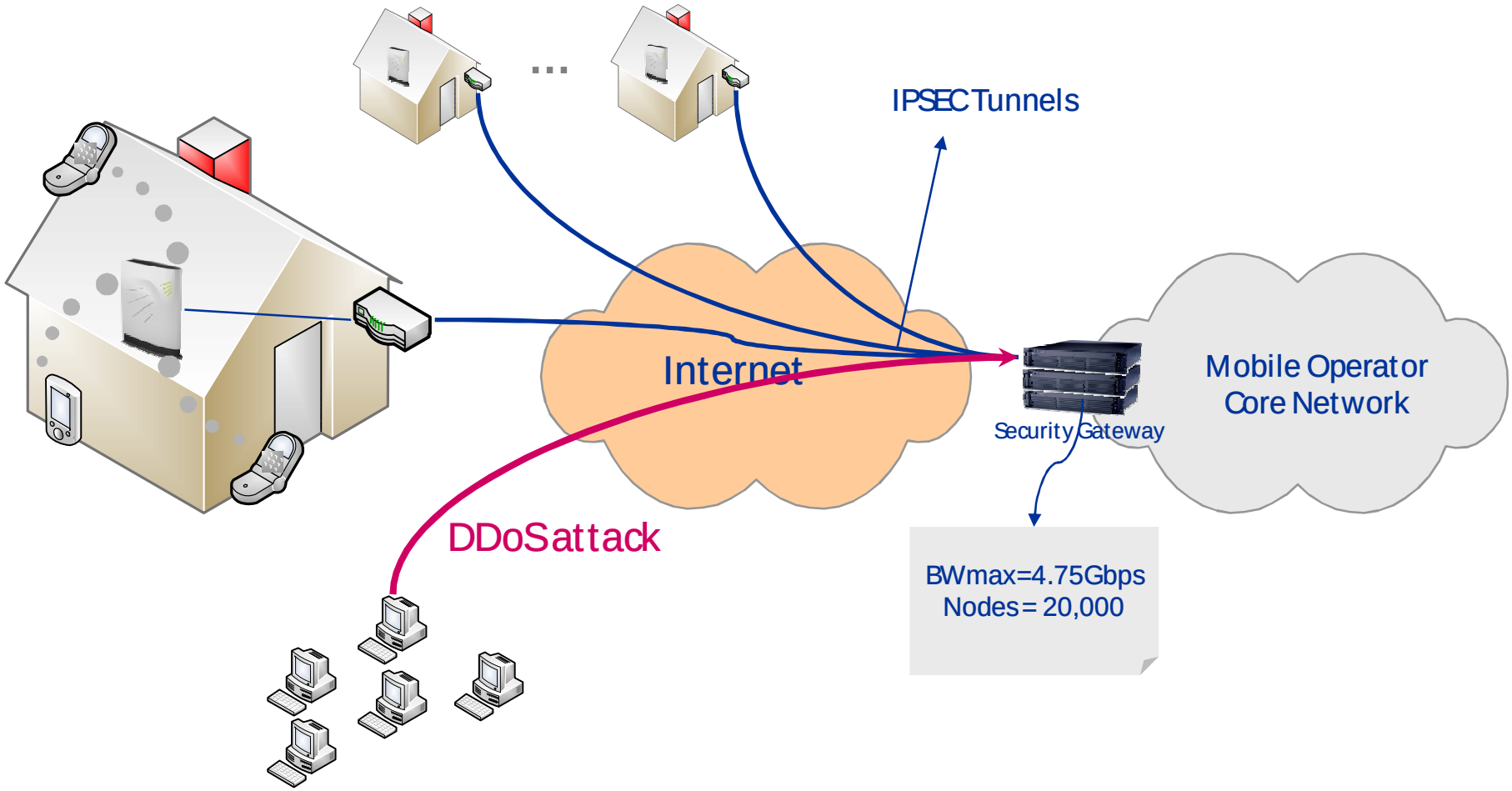
- They all offer procedures for identifying and calculating risks
- But they require to estimate some factors (such as frequence of occurrence, impact …) whose knowledge is not evident

01 Introduction
Applying economic models

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

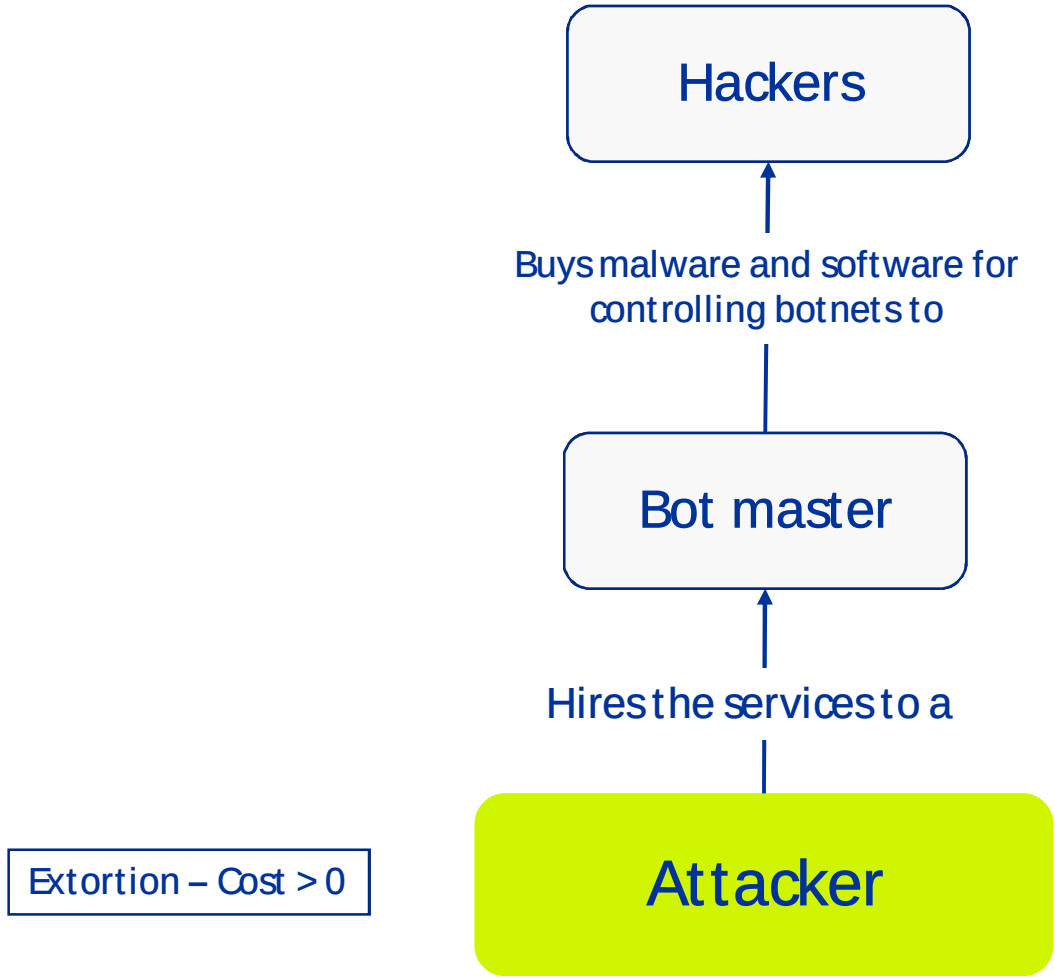
02 Use case presentation

Case of study



02 Use case presentation

DDoS attack supply chain



03 Economic model

The model

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

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

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

- 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

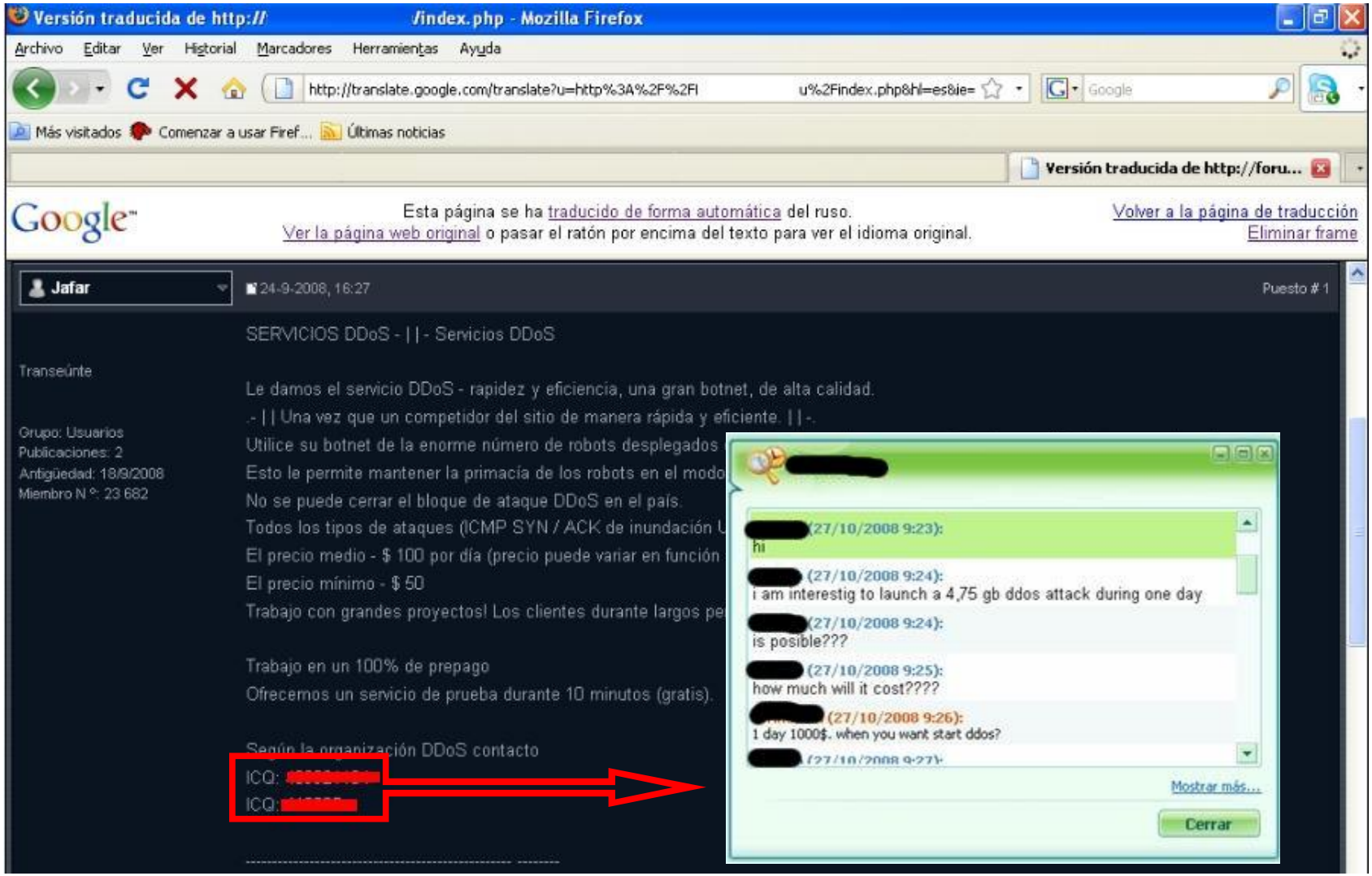
- Average revenue per SeGW:
  - Femtocells per SeGW: 20,000[1]
  - Monthly average revenue per femtocell: 28$[2]
- Relation between revenues and extorted amount (k): 0.001[3]

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

1 Alcatel-Lucent VPN Firewall Brick 1200 HS (Femto Access Gateway)
2 Femtocells in the consumer market: business case and marketing plan. Analysis Research
3 Obtained by comparing 2004 figures of online betting sites with extortion demands

03 Economic model

Cost – renting cost collection (1/2)



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

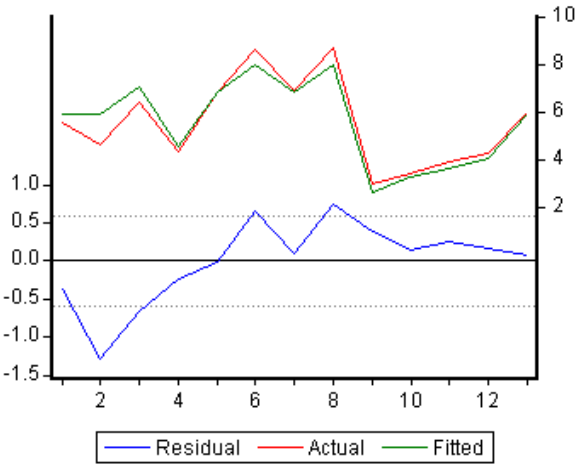
- Regression function of cost

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

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

$R^2 = 0.898$
$K = 0.9640$
$\alpha = 0.5903$
$\beta = 0.5869$



03 Economic model

Profit function

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

$$Profit = f(\alpha, t, A)$$

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

03 Economic model

Application of the model (1/3)

- 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)

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

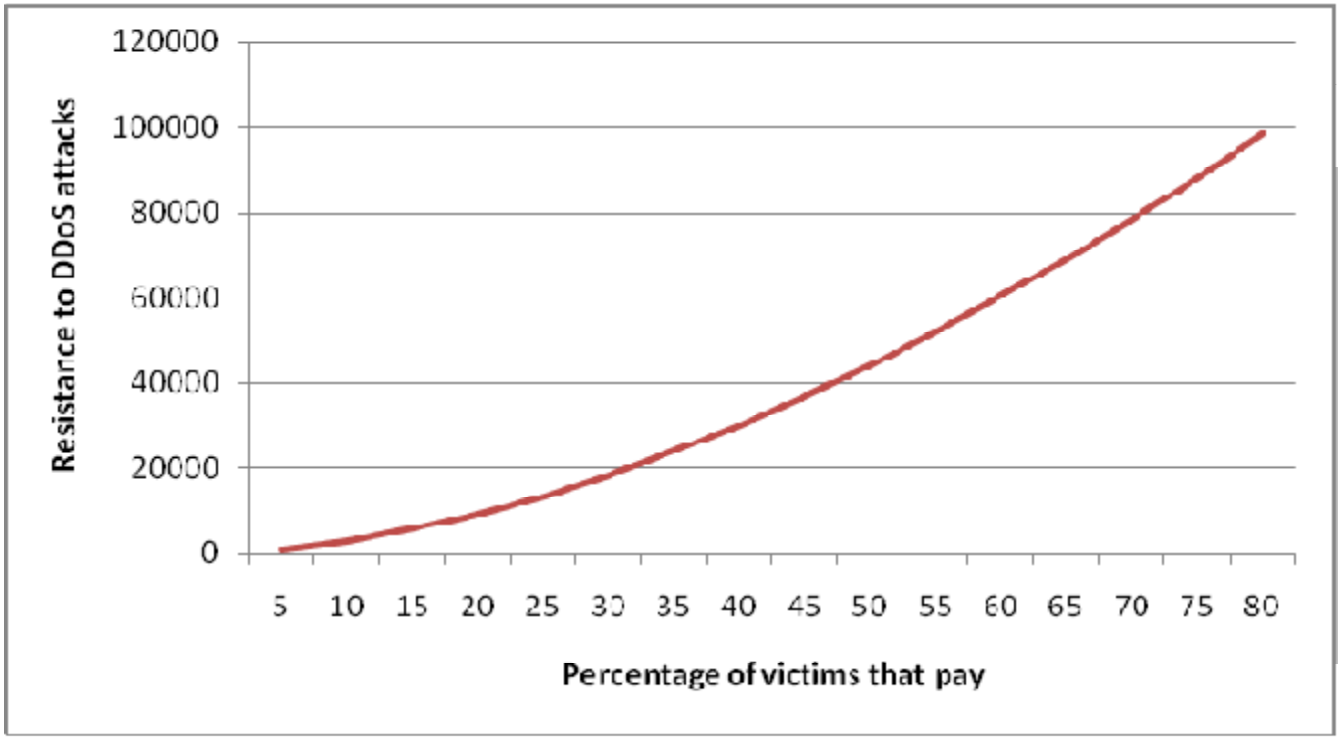
$$\alpha_{MAX} = 0.1347$$

03 Economic model

Application of the model (2/3)

- 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)

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

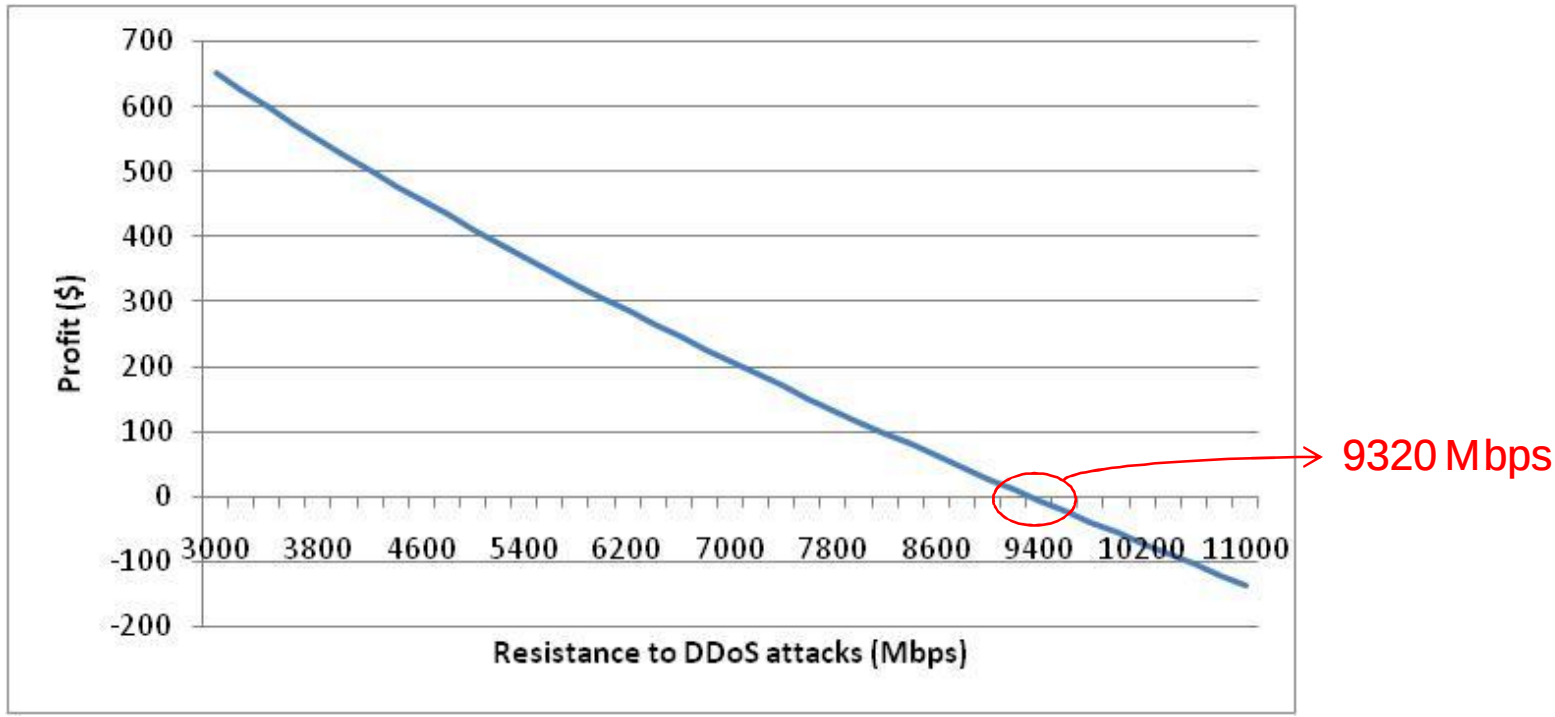


03 Economic model

Application of the model (3/3)

- Required attack resistance of the security gateway to nullify profits
  - Assumptions:
    - $\alpha = 20\%$ (Attackers hope that 20% of victims give in to extortion)
    - $t=24h$ (Botnets must be rented for 24 h to be successful)
    - $A=4750$ Mbps (The Security Gateway resists attacks of up to 4750 Mbps)

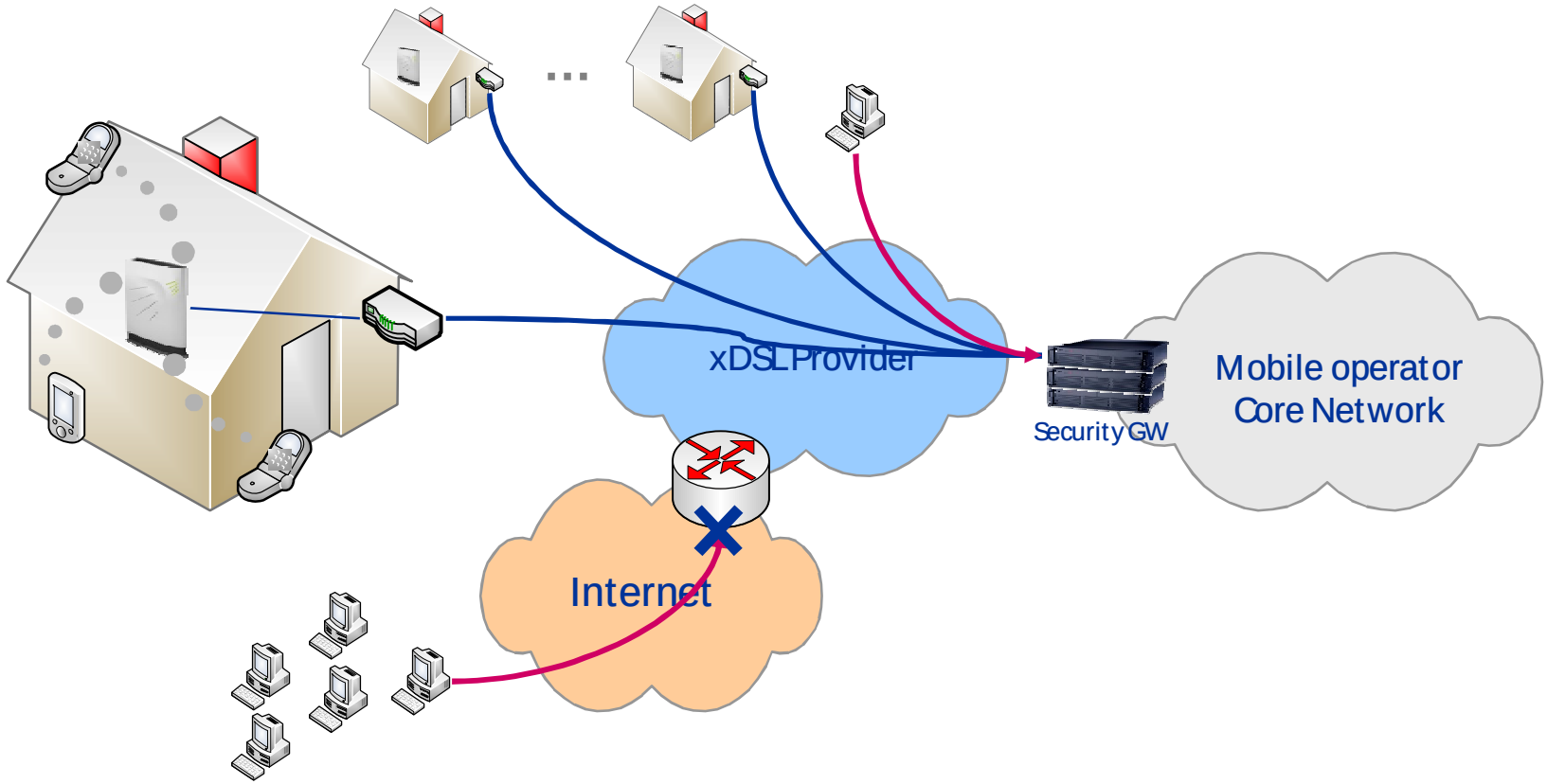
$$Profit = 0.2 \cdot 6720 - 0.964 \cdot 24^{0.5903} \cdot A^{0.5869} = 0$$



03 Economic model

Strategies for mitigating risks

- Strategy 1: we choose a more DDoS attack-resistant security gateway
- 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