Copenhagen
Business School
HANDELSHØJSKOLEN

Business and social evaluation of denial of service attacks in view of scaling economic counter-measures

L-F Pau, Prof. Mobile business, Copenhagen business school, and Rotterdam school of management lfp.inf@cbs.dk

Copenhagen Business School
HANDELSHØJSKOLEN

SCOPE

- To take a total economic and social view in the assessment of damages from cyber-warfare attacks on a society or business target;
- Consider that the target has a diversity of assets included in a portfolio, each with varying life-cycles, and that any attack affects the overall value and sustainability of the portfolio;
- Analyzing over time the economic, business, and social implications of denial of service and distributed DoS attacks, aiming at asset preservation;
- Providing an analytical basis for legal or policy driven dissuasive, retaliation or compensation/ restoration actions, using common law "tort" principles.

Copenhagen Business School
HANDELSHØJSKOLEN

APPLICABILITY OF THE METHOD

- The DoS/DDoS attack affects a *finite* number of supply or service chains, where consequences can be identified and sized; thus attacks at a national level normally are out of scope
- Retaliation assumes the existence of formal agreements or contracts reaching to parties in the jurisdiction or economlc sphere of the attacker

Copenhagen Business School
HANDELSHØJSKOLEN

APPROACH (1) : DYNAMICS

- Argument : Traditionally the damage assessment has been considered "binary" and limited in time, in that the target was considered to be rendered totally dysfunctional until full restoration of its information and communication capabilities. Vice-versa, sometimes, the replacements made to infrastructure damaged by the attack will be less obsolete leading to better future robustness.

- Approach : Use time preference dynamics applied together to the incremental monetary flows and time dependent capability levels, needed for:
- short term partial restoration of capabilities,
- long term investments to rebuild capabilities,
- the usability of the capabilities of the target and the linked parties after an attack.

NB: In economics, time preference (or "discounting") pertains to how large a premium a user will place on usage nearer in time over more remote usage.

Copenhagen Business School
HANDELSHØJSKOLEN

APPROACH (2) : TANGIBLE AND INTANGIBLES

Argument : Lessons learnt tell us that other organizational, physical, human and social capabilities are to be counted as representing often larger collateral damage of the attacks; their restoration eventually takes quite some time, especially if the surrounding society does not have enough technology and civil defence means/ skills in place.

Approach : Cost-benefit analysis allows to bundle into the internal rate of return both tangible and some intangible effects.The internal rate of return expresses the time preference on tangible and intangible assets , old and new, which gives a break even net present value over the long term.

Copenhagen Business School
HANDELSHØJSKOLEN

APPROACH (3) : MODELING THE DoS / DDoS ATTACK

Argument : Obviously only the exact attack method and protocol(s) allow for modeling; however, in terms of impact, macro-level approximations by known or tailored distributions already provide a good basis

Approach :Brownian shock diffusion models with catalogued parameters, linked to an attack affecting the command and control node of the society or business target, which have their normal long term equilibrium return rates.

Copenhagen Business School
HANDELSHØJSKOLEN

KEY PARAMETERS

- *Mission critical aspects*: time increment for the attack, and capabilities adjustment periods
- *Business or process dependencies*: explicit dependency levels, with lags, between the target and downstream users of its' capabilities
- *Emergency management*: time horizon to rebuild and possibly improve on the asset's capabilities
- *Economic / Business / Social* :Equilibrium time preference for the tangible and intangible assets
- *Policy making*: intensity of the feedback force towards the equilibrium time preference
- *Investment willingness*: Capital for rebuilding and improving capabilities
- *Risk tolerance* : volatility of the time preference fluctuations on capabilities and their restoration (Brownian)
- *Finance*: maturity dependent interest rate curve

Copenhagen
Business School
HANDELSHØJSKOLEN

ILLUSTRATIVE CASE

Illustrative case: a data centre in a company supporting all divisions and some customers

- IT and COMs scrap value of 10 MEuros
- company turnover of 500 MEuros/year; dependent client capabilities of 500 MEuros /year (contingent liabilities)
- equilibrium time preference is equivalent to the company's net operational profit margin from operations of 50 %/year
- attack at t=0 for 1 hour; the target wants perceptually all measures to be taken for immediate recovery of the data centre
- minimum nominal restoration time of TK= 3 months

Analysis results (for chosen parameters, with possible sensitivity analysis):

- the initial long term investments needed to recoup supplies and capabilities can be estimated at about 235 M Euros
- half of the overall capability is only restored at time 0,5/ (1,2-VA/3) which can be longer than 3 months for some values of tolerated usage risk volatility VA

Copenhagen
Business School
HANDELSHØJSKOLEN

APPLICATIONS

- Public services

  Case : minimal public transport service under employee strikes; use for negotiations

- Company products and services

  Case: corporate DoS/DDoS liability insurance estimate for CRM provider

- Loss of shared infrastructure

  Case : attack on 3G operator BSC with partial recovery via other operator(s); use of intercarrier settlement contracts

- Technology providers

  Case : discussion on sharing attack profiles between a technology provider and its customers, to determine investments in protection against DoS

Copenhagen
Business School
HANDELSHØJSKOLEN

DENIAL OF SERVICE IMPACT ANALYSIS USAGE PROCESS

- ** Dissuasive process: preemptively to a denial of service, by policy makers or companies, to announce that these claims would be raised if an attack occurs. The policy makers or companies may not have evidence yet or from past cases to identify the attackers, but may communicate to make such a categorization of attackers credible and visible to attackers .

- *** Retaliation process: if the attackers are traced and identified by technical and/or judicial means, or if strong assumptions and partial evidence exist (e.g. from IP addresses, software code structure, software forensics, etc…), legal or forceful retaliation would be done for the same size of claims against direct or indirect interests of the attackers.

- * Compensation / Recovery process: if the attackers are traced and identified by judicial means, and can be put on trial, this process would use the contradictory damage assessments as normally done in a judicial court procedure.

- There is of course a fourth process, which is to ignore attacks, keep silent, not exchange data , and not to sue, often for “image» and brand impact reasons.

Copenhagen Business School
HANDELSHØJSKOLEN

CONCLUSION

- Just as technical vulnerability reduction demands collaborative efforts between users, technology providers and operators, the business and social impact assessments also demand such collaboration and information exchange, besides internal due diligence.
- This work has direct policy making implications, with emphasis on accounting, auditing, insurance policies and contractual processes
- The issue is: which governments, players and sectors, like the communications industry, will take concrete steps in this direction ?