# Impact Analysis

# Impact Analysis

- For each attack it determines the loss if it is successful
- Depends upon
  - The resources the attacker can control
  - The processes using these resources
- It depends upon the attribute(s) that the attacker controls (confidentiality, ….)
- Some loss
  - Cannot be quantified (eg human lifes)
  - Are very difficult to estimate (image and so on)

# Impact Analysis

- It requires information about the processes of the organization that are using the data
- Information may be collected by interviews
- The impact
  - also depends upon the time to discover and remediate the attack
  - is a function of which attacker controls some resources (eg organized crime vs terrorism)

# Impact Analysis

- Proper questions to ask an organization
  - How long could the business continue to operate while that system is down?
  - What would be the opportunity cost of that downtime?
  - What would be the real costs associated with bringing that system back?
- The answers depend upon the role of the ICT system in an organization, the more critical the system, the larger the impact

# Probability Distribution

- An exact, numerical extimate of the impact is rather difficult
- The impact is modelled as a random variable with a probability distribution and the impact is the average of the distribution
- A very popular distribution is the normal one

$$f(y) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(y-\mu)^2}{2\sigma^2}}$$

Probability of an impact =y

The impact is centered around the average $\mu$

# Normal distribution

- Several nice mathematical properties
- Central limit theorem:
  - The impact is the sum of several contributions, each with its own probability distribution
  - The limit of the sum of several distributions is a normal distribution
- Even the error in the analysis may be normally distributed

# Normal distribution

- Thin tail = an exponential decrease in the value of the impact
- Values at a distance larger than 3 / 4 standard deviations from the average value have a very low probability
- Centered around the average
- Sometime it is too optimistic

# Normal Distribution

- “mild” randomness (Mandelbrot) or Mediocristan (Taleb)
- Mild randomness is denoted by the thin tails
- Models a process that is the sum of several other processes and where each process may compensate the other ones (sum of distances from the average is zero, proper of physics)

# Heavy tailed

- A rather distinct case arise if the impact X satisfies

  i) $\lim_{\delta \to \infty} \text{Prob}(X>\delta+h) / \text{Prob}(X>\delta) = 1 \ \forall \ h$

  Or

  ii) $\forall \ h \ \ \exists \ w \mid v> w$ then $\text{Prob}(X> h*v)/\text{Prob}(X>v)$ does not depends upon h

- These two conditions states that there is a value of the impact such that if the threat can achieve that impact, then she will achieve any impact

# Heavy tailed

- The threat can achieve any impact if she fully control the system and the owner cannot regain control of the system
- In these cases, the impact cannot be model by a normal distribution

# Power-law & Heavy Tails

- Any probability distribution prob(imp) that satisfies

  $prob(imp) \propto imp^{-\lambda}$ for $imp > imp_0$,

  $\lambda>1$ is the "exponent" of the power law.

- The power-law behavior occurs for

  $$imp > imp_0$$

  that is the tail of the distribution that is called an heavy tail,

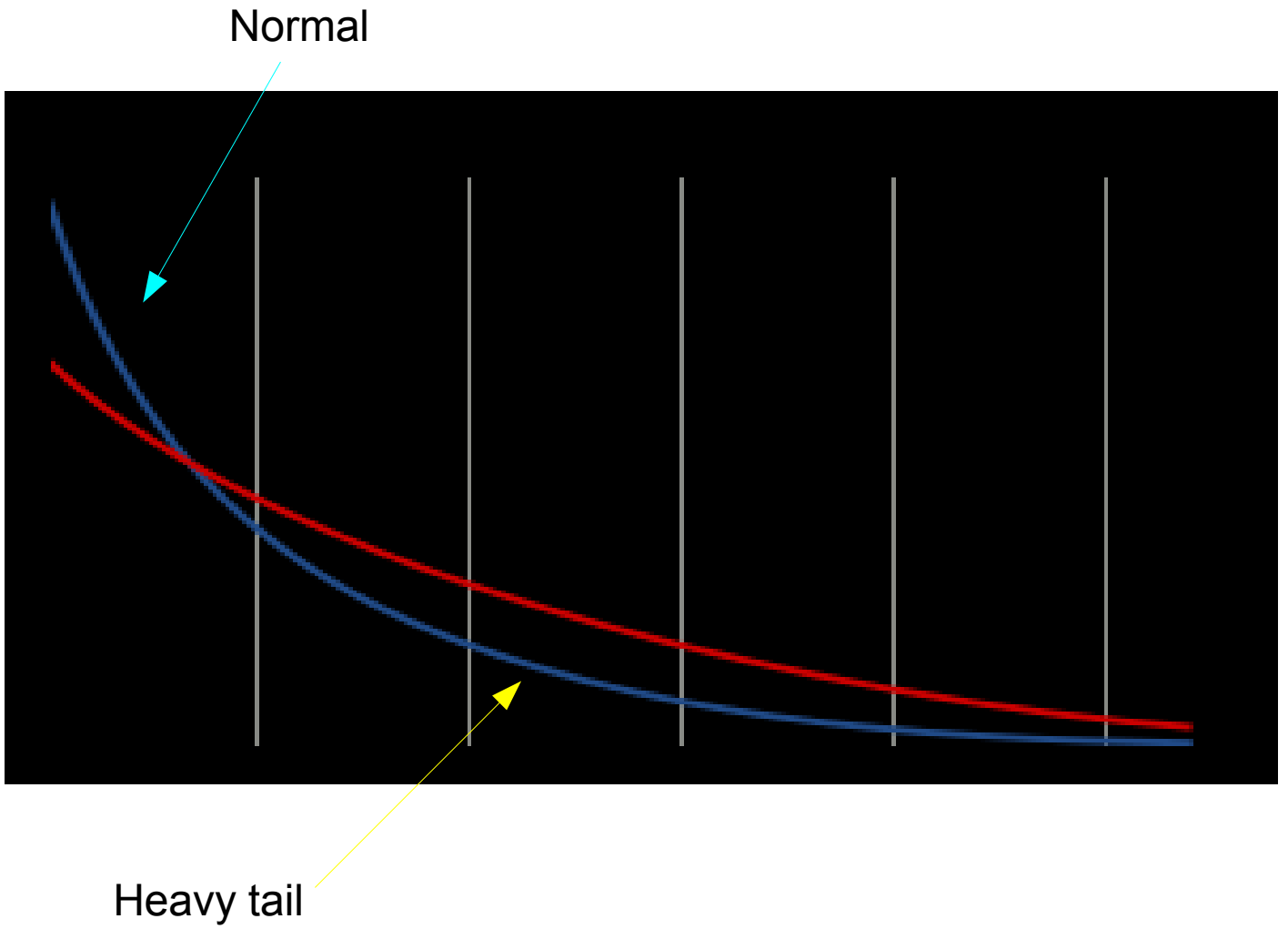
- Extreme impacts are far more likely than they would be in a Gaussian distribution.

# Heavy tailed

The power law is an heavy tailed law

- Probability distribution = $g(x)(1/x^{\alpha})$ $\alpha>1$
- If $\alpha<2$ all the moments (average, standard deviation, .. .) are unbounded
- If $2<\alpha<3$ only the average exists

# Heavy Tail



# Heavy tailed

- The impact of an attack that results in the knowledge of some credit card numbers.
  - Can be modelled through a normal law
  - We can introduce mechanisms to bound the impact
- The impact of an attack against the server that stores all the credit card numbers
  - Cannot be bounded
  - Cannot be modelled through a normal law

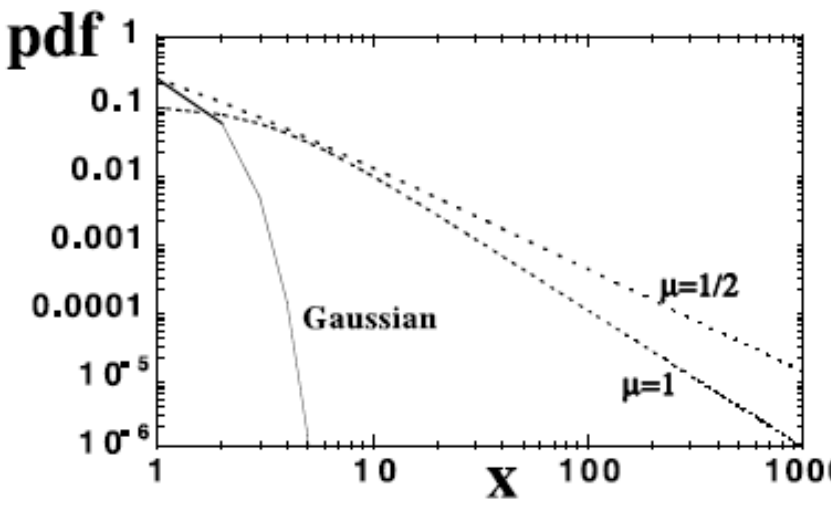
# Examples

- Assume that, on the average, the loss of the number of a credit card is 1.000 euros
- If we lose 100 credit card number we can expect an impact that is distributed as a normal distribution with an average equal to 1.000 x 100
- But if we lose a database with 1.000.000 credit card numbers, the impact has to be evaluated in a different way and we have an head tail

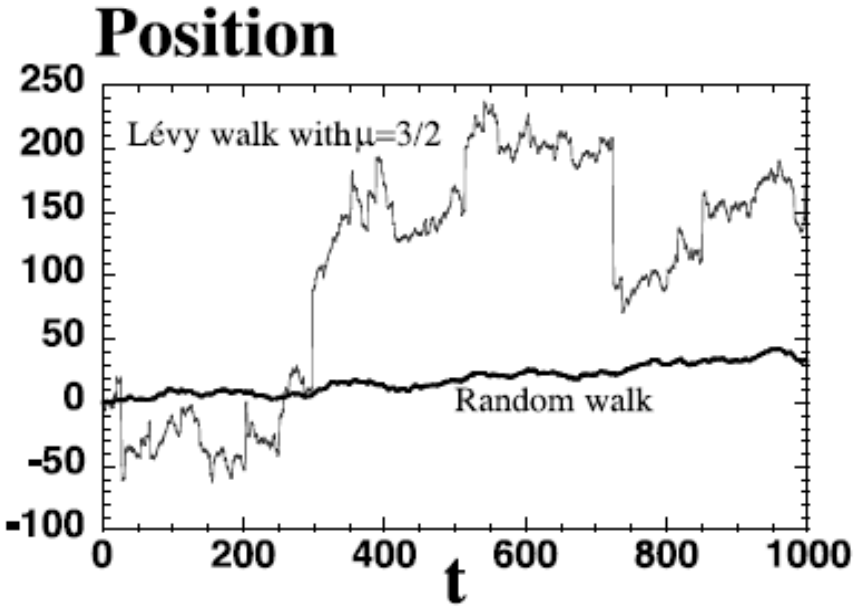
# Other cases with power law

- To minimize the cost of an infrastructure, the designer may adopt strategies such preferential attachment or “the rich will become richer”
- This results in a interconnection structure described by a scale free graph where the number of connection of each node decreases with a power law
- The impact of an intelligent attack against such an infrastructure is modelled as
  - a power law
  - all the moments are unbounded

# Power law vs normal



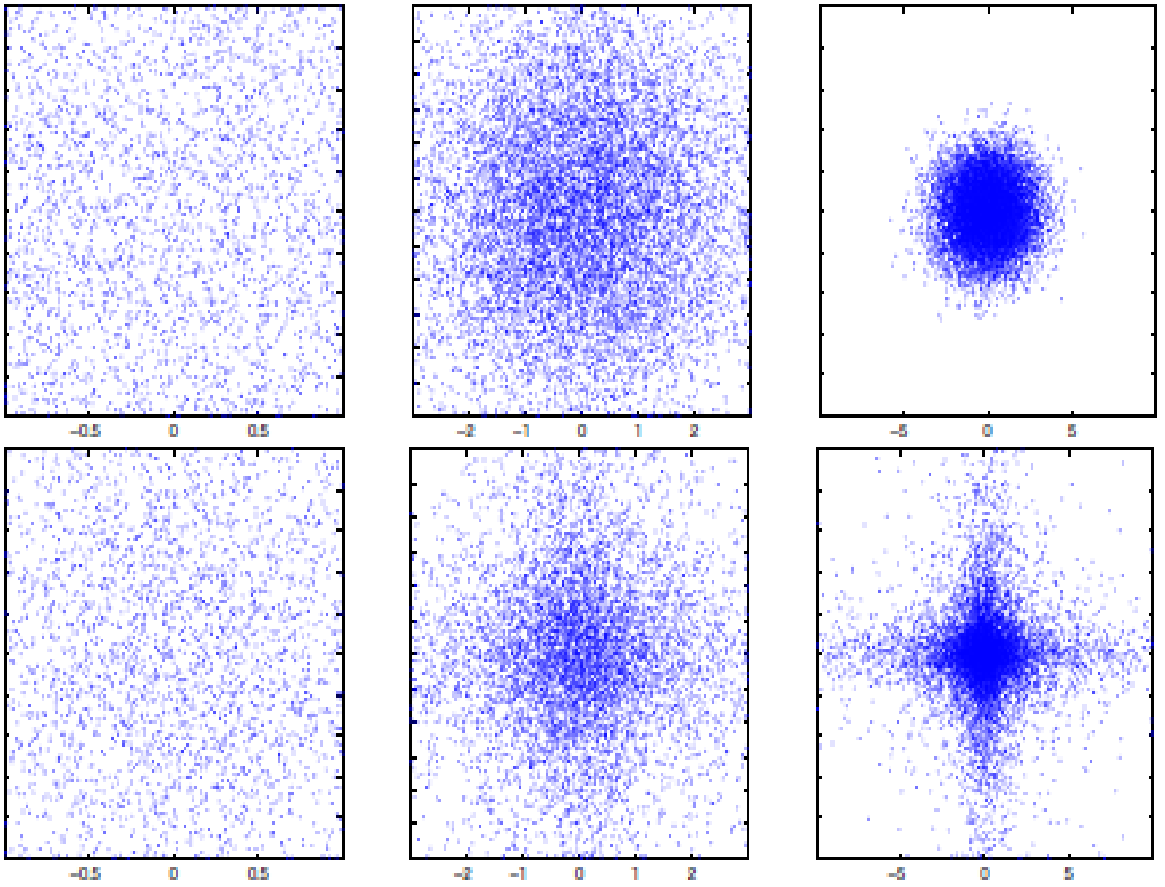

Curve in log-space




Random walks with a normal generation and a power law generation

Sornette, D. - Critical phenomena in natural sciences. Chaos, fractals, self-organization and disorder. Concepts and tools

# Power law vs normal: scale is important




normale

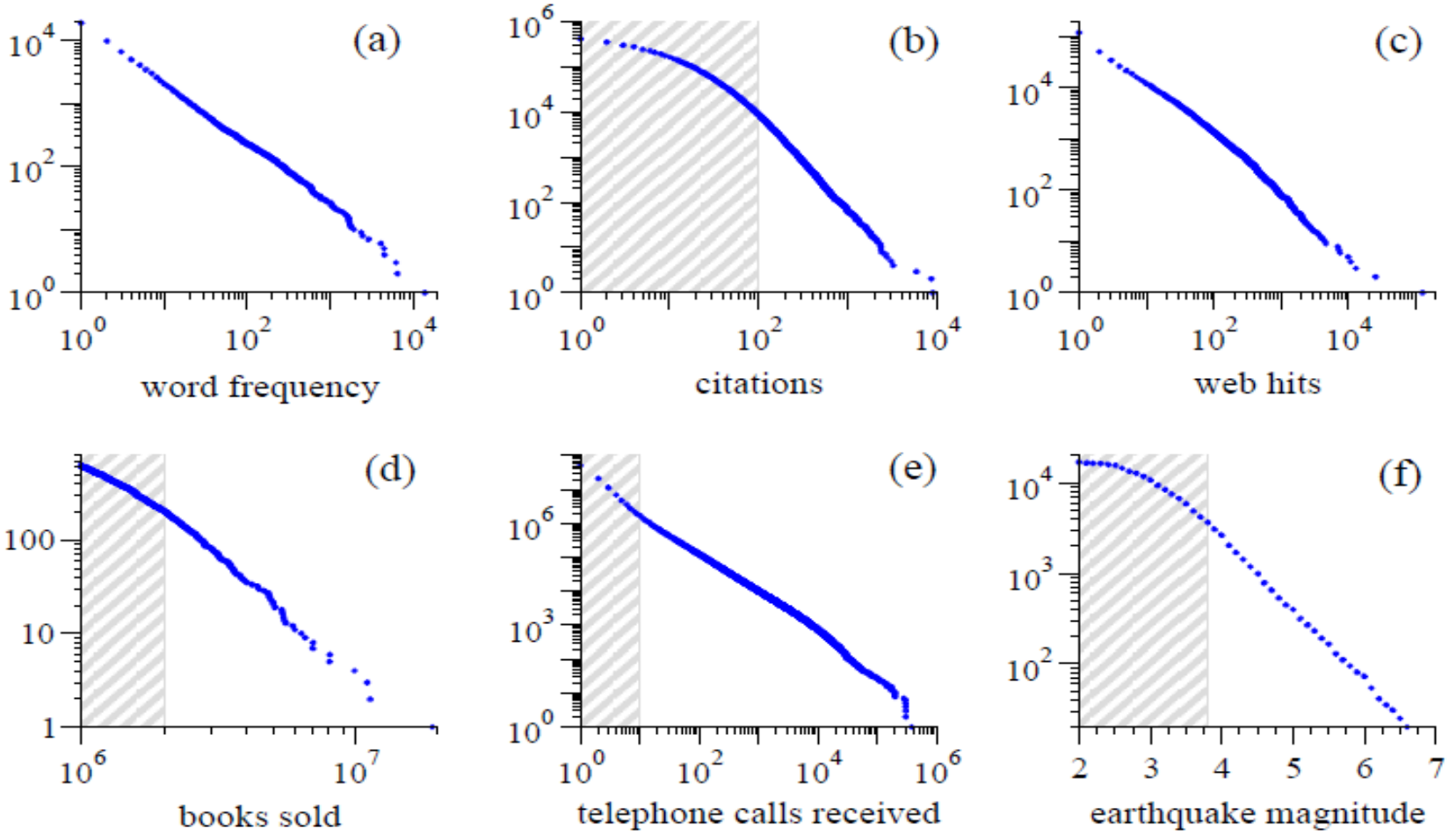
Power law

Random points generation with a normal or a power law
F.Clementi, T.Di Matteo, M.Gallegati “The power law tail exponent of income distribution
Physica, 2006

# Power law vs normal

- The difference cannot be discovered in an experimental way because the number of data available may result in a too little difference
- We have to decide according to the features of the attack of interest

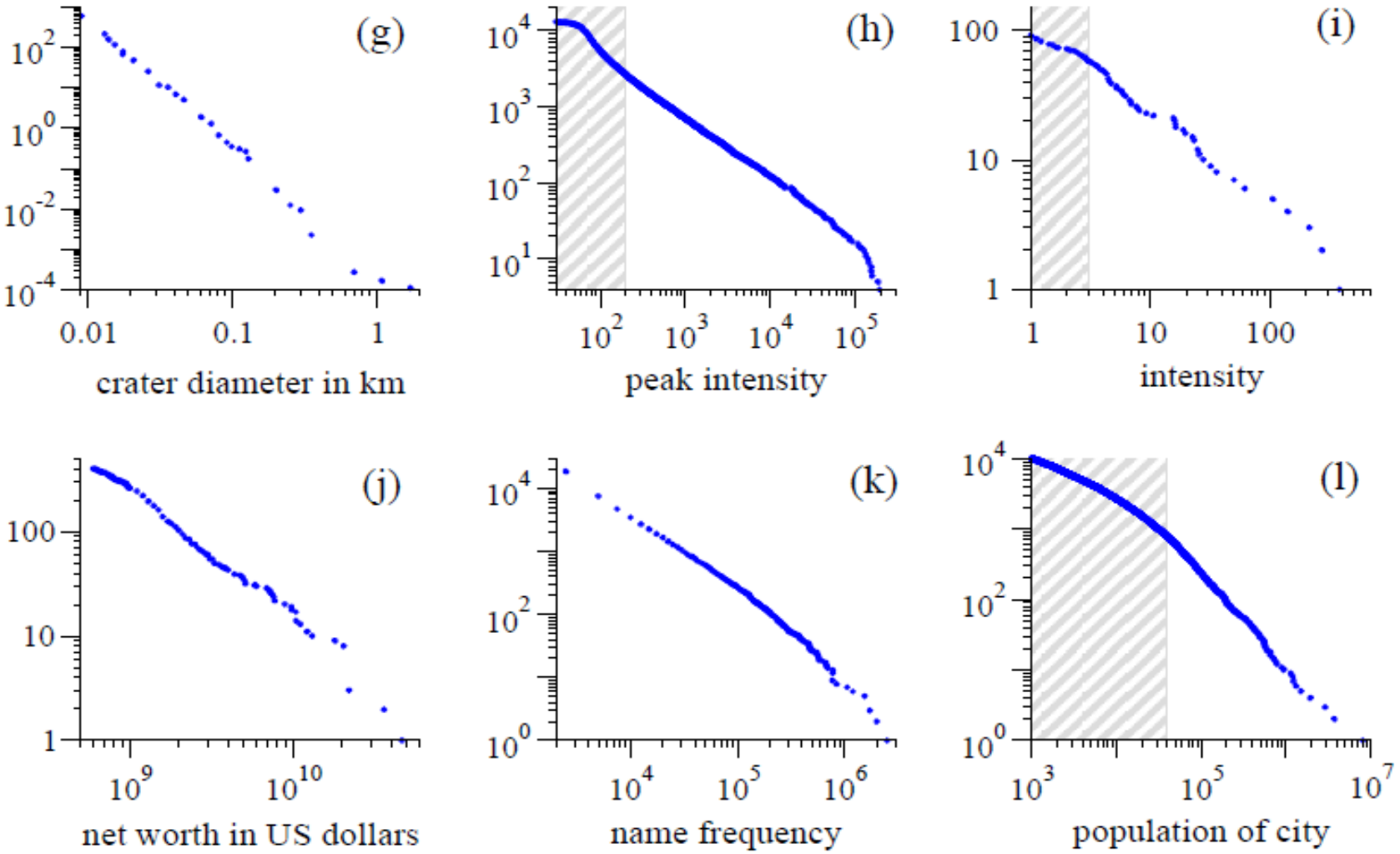
# Some examples of a power law - I




**Power laws, Pareto distributions and Zipf's law**

M. E. J. Newman

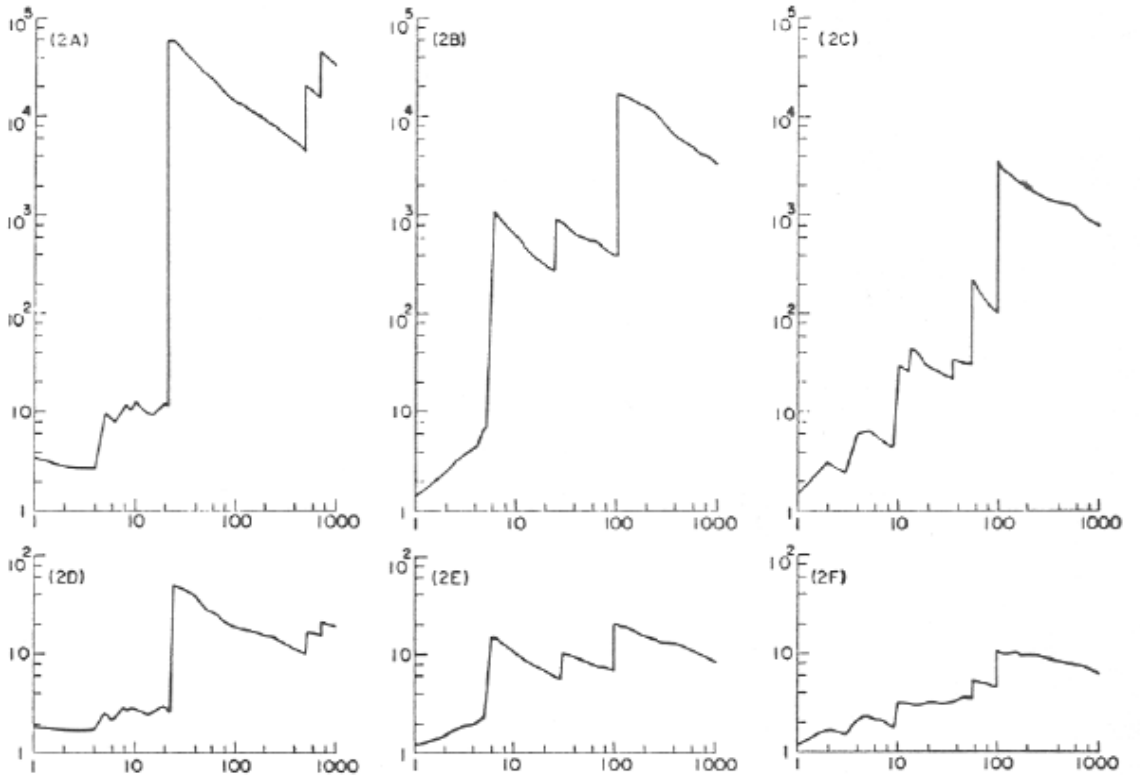
# Other examples - II




**Power laws, Pareto distributions and Zipf's law**

M. E. J. Newman

# Unbounded Moments




Average of a random sample, there is no convergence to a value

# Power Law Vs ROI

- The previous discussion outlines the complexity of defining the ROI in this case because if the impact is unbounded any countermeasure is cost effective
- The definition of a solution is rather complex even if a large amount of data is available

# Risk, Robustness and ROI

… systems designed for high performance naturally organize into highly structured, statistically unlikely states that are robust to perturbations they were designed to handle, yet fragile to rare perturbations and design flaws … high-performance engineering leads to systems that are robust to stresses for which they were designed but fragile to errors or unforeseen events

M.E.J. Newman, M. Girvan, and JD Farmer, “Optimal design, robustness, and risk aversion” Phys. Rev. Lett. 89, 028301 (2002)

# Risk Management vs unbounded impact

- “forget optimization and embrace redundancy”
- Redundancy increase the complexity of attacks (redundancy in controls) and decrease the impact (redundant resources)
- Redundancy is effective only if independence against attacks is guaranteed