Why to adopt a security metric? a brief survey

Andrea Atzeni, Antonio Lioy

(shocked, lioy @ polito.it)

Politecnico di Torino
Dip. di Automatica e Informatica
TORSEC security group

QoP'05 - Milano 05/09/15

Pervasive influence

Computers are portable

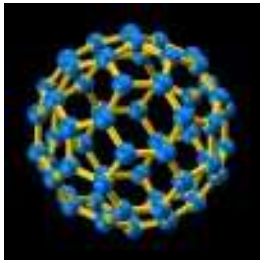
Computers are versatile

Computers are powerful

Computers are everywhere

Security: from empiricism to science

- from an empirical and subjective approach
  - lack of formal definitions
  - lack of objective goals
  - lack of comparable results
  - “expert’s” knowledge
  - ...
- to accurate science
  - measurable quantification of security component
  - estimable interaction with the system
  - evaluation of different security configurations
  - ...



What's a measure?

A measure is the result of a measurement, i.e. a process aiming to acquire quantitative or qualitative values of real world attributes

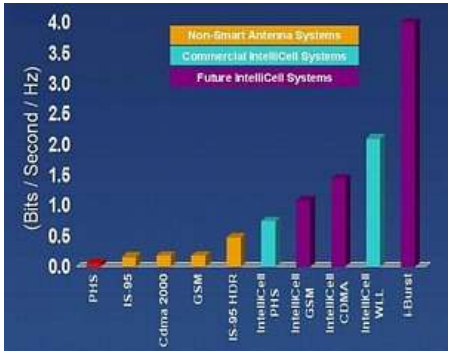
Metric “good properties”

- clarity
  - easy to interpret
- objectiveness
  - not influenced by the measurer
- repeatability
  - should return the same result if repeated in the same context
- easiness
  - simple to be performed
- succinctness
  - consider only the important aspects

Why to adopt a security metric? Efficiency

- working without a measure is inefficient

- acquisition of knowledge improves the system
  - knowledge efficiency
- "The better one understands a phenomenon, the more concisely the phenomenon can be described"
  - description efficiency
- "When performance is measured, it improves"
  - control efficiency



Why to adopt a security metric? Economical evaluation

- in its early days, Internet concerned “good guys”
  - restricted environment (university, military)
  - efficiency and availability were the main topics
  - no economical concern

- now, Internet is of large economical concern
  - B2C - B2B - Supply chain - ...
  - many “bad guys” come into play
  - big economic loss for internet companies

Risks, security, countermeasures

<table>
<tr><td rowspan="2">unknown risks</td><td colspan="2">known risks</td></tr>
<tr><td>accepted</td><td>avoided by countermeasures</td></tr>
</table>

monitoring

+

insurance

cost – benefits analysis

Why to adopt a security metric?
Crime prevention

- Internet is currently the most powerful tool for information exchange
  - terrorist information exchange
  - intelligence information exchange
  - computer crime and sensitive information loss

- metrics to understand the actual state of national security

Possible approaches

- technical analysis
  - modelization of the system
    - reliability block diagram, fault tree, attack tree, Markov chain, simulation, ...
- evaluation by standards
  - standardization of procedure
  - best practices
  - questionnaires
  - international standards of evaluation
- economical evaluation of effects
  - security expressed in monetary terms

Possible approaches - examples

- attack trees
  - + clarity, easiness, repeatability
  - - objectiveness, succinctness
- international standards
  - +/- repeatability, objectiveness
  - - clarity, easiness, succinctness

Conclusions and future work

- security metric is an immature field:
  - no widely-accepted measure of security
  - no widely-accepted “monetization” of security
- suggested developments in this field:
  - (formal) description of the system
  - ... for automatic reasoning on the system
  - ... for economical evaluation of attacks and countermeasures