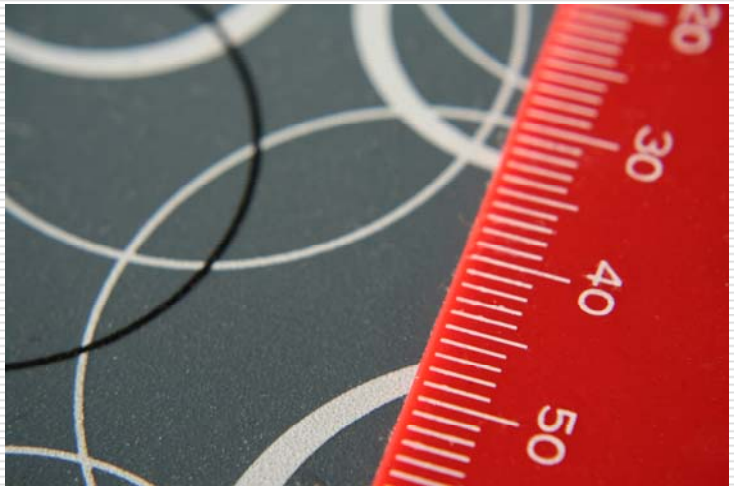
Security Metrics
What Can We Measure?

Zed Abbadi

The Public Company Accounting Oversight Board

What is a “Metric”

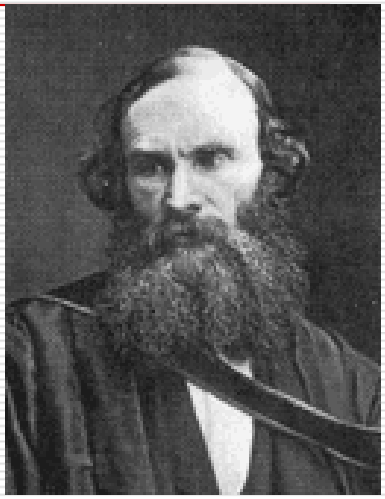


- A metric is a system of related measures enabling quantification of some characteristic. A measure is a dimension compared against a standard.*
- Security metric is a system of related dimensions (compared against a standard) enabling quantification of the degree of freedom from possibility of suffering damage or loss from malicious attack.*

**QoP’ 06, Oct. 2006*

Do We Really Need Metrics?

"If you cannot measure it, you cannot improve it."



Lord Kelvin

"In physical science the first essential step in the direction of learning any subject is to find principles of numerical reckoning and practicable methods for measuring some quality connected with it. I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of Science, whatever the matter may be." [PLA, vol. 1, "Electrical Units of Measurement", 1883-05-03]

“You cannot manage what you cannot measure"

Drivers For Metrics

- Money matters
  - Asset vs. liability
- Governance
- You claim it is a science?
  - Do as good as math, physics and astrology
- Decision aid
- How are we doing with security

Good Metrics. vs. Metrics

- Quantitative
- Objective
- Based on a formal model
- Has a time dimension
- Universally acceptable
- Has ground truth
- Inexpensive
- Obtainable
- Repeatable

Data Collection

- Vulnerabilities, exploits and attacks
- Organization vs. industry vs. everyone else
- Disclosure Policies
- Accuracy
- Statistical Significance

Attempts at Measuring Security

- TCSEC (Orange book)
- ITSEC (Europe's Orange book)
- CTCPEC (Canada's Orange book)
- Common Criteria (everyone's Orange book)
  - Framework rather than a list of requirements
- SSE-CMM
- NIST FIPS-140 series
- NIST SP 800-55

Security Metrics Types

- Process Security Metrics
- Network Security Metrics
- Software Security Metrics
- People Security Metrics
- Other

Process Security Metrics

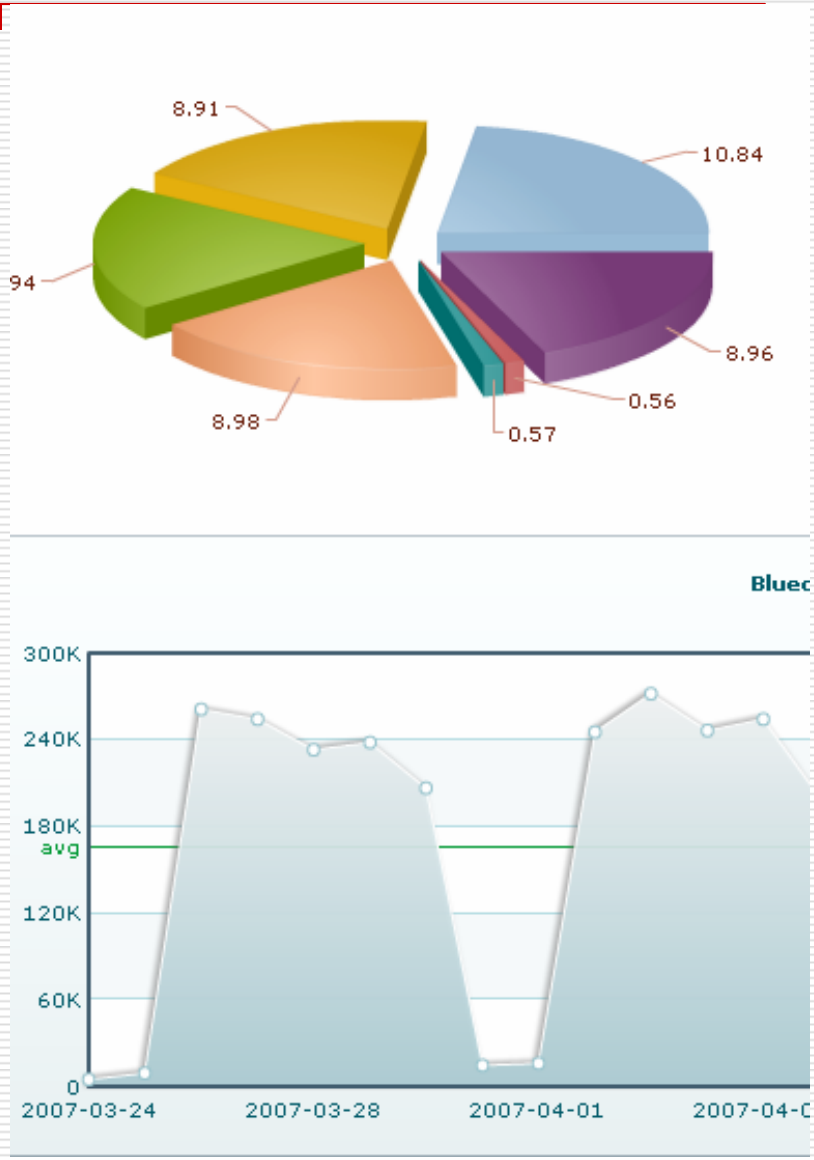
- Measure processes and procedures
- Imply high utility of security policies and processes
- Relationship between metrics and level of security not clearly defined
- Compliance/Governance driven
- Generally support better security
- Actual impact hard to define

Examples

- No. of Policy Violations
- % of systems with formal risk assessments
- % of system with tested security controls
- % of weak passwords (non-compliant)
- No. of identified risks and their severity
- % of systems with contingency plans

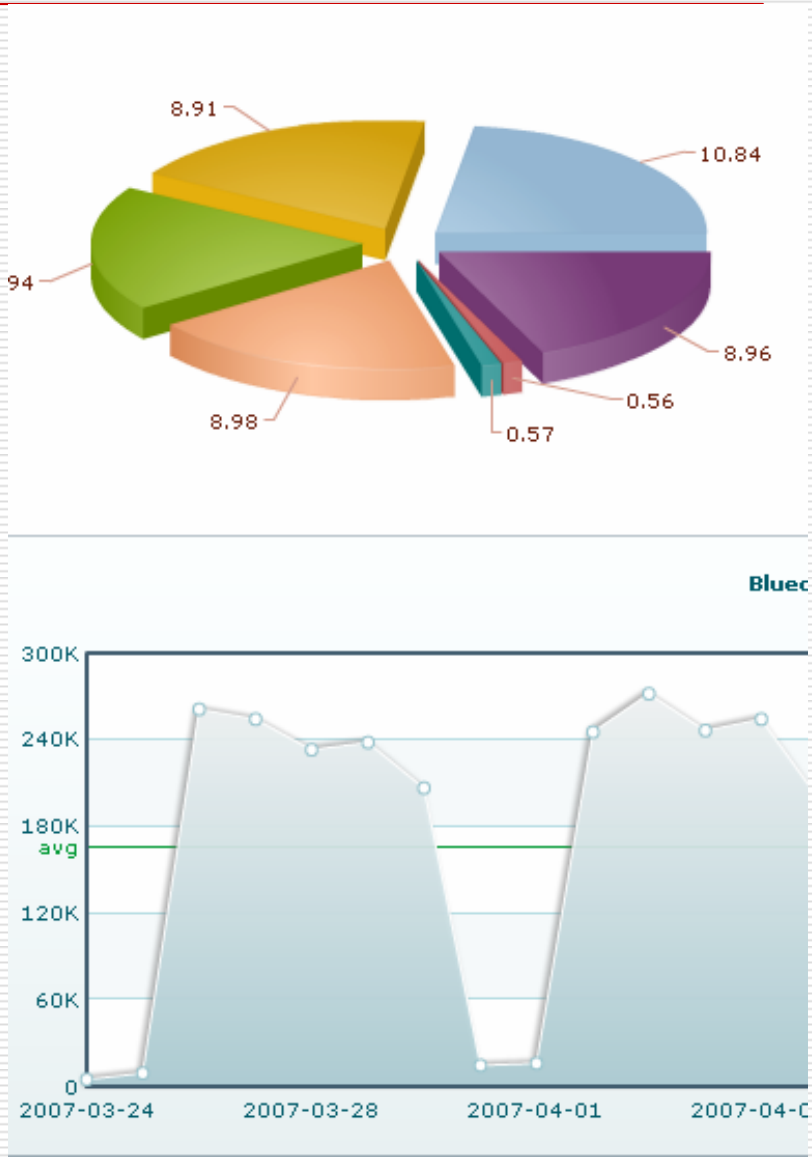
Network Security Metrics

- Driven by products (firewalls, IDS etc)
- Readily available
- Widely used
- Gives sense of control
- Nice charts and interfaces
- Can be misleading



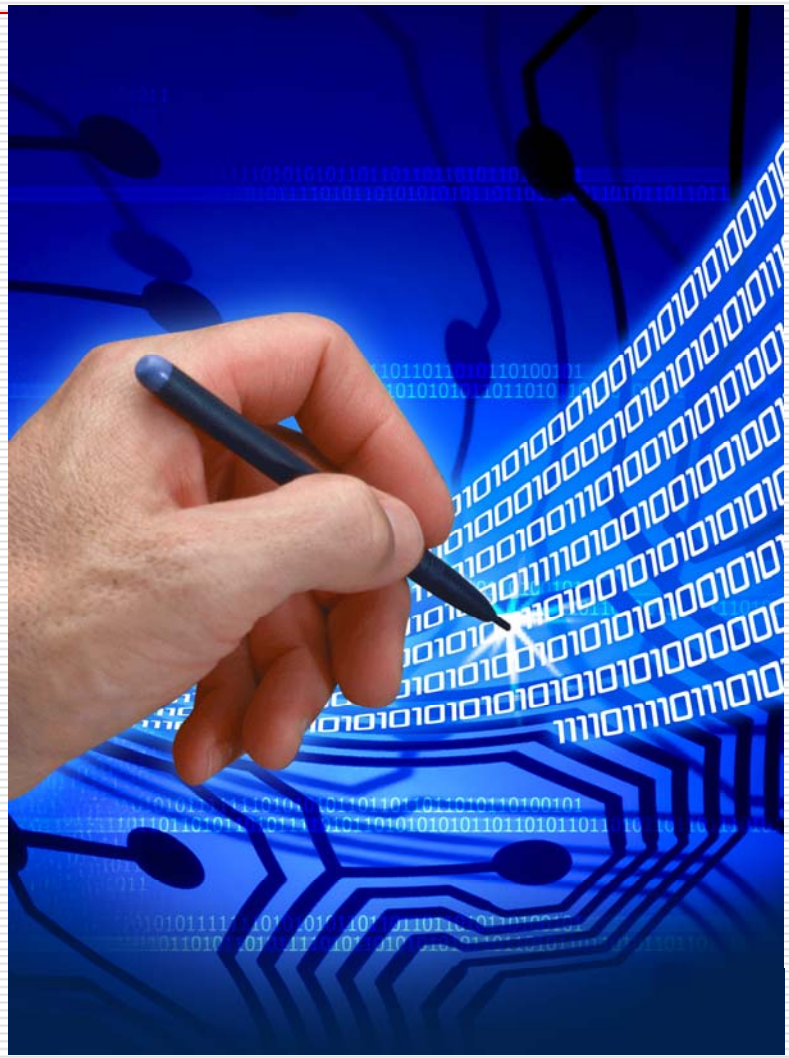
Examples

- Successful/unsuccessful logons
- No. of incidents
- No. of viruses blocked
- No. of patches applied
- No. of spam blocked
- No. of virus infections
- No. of port probes
- Traffic analysis



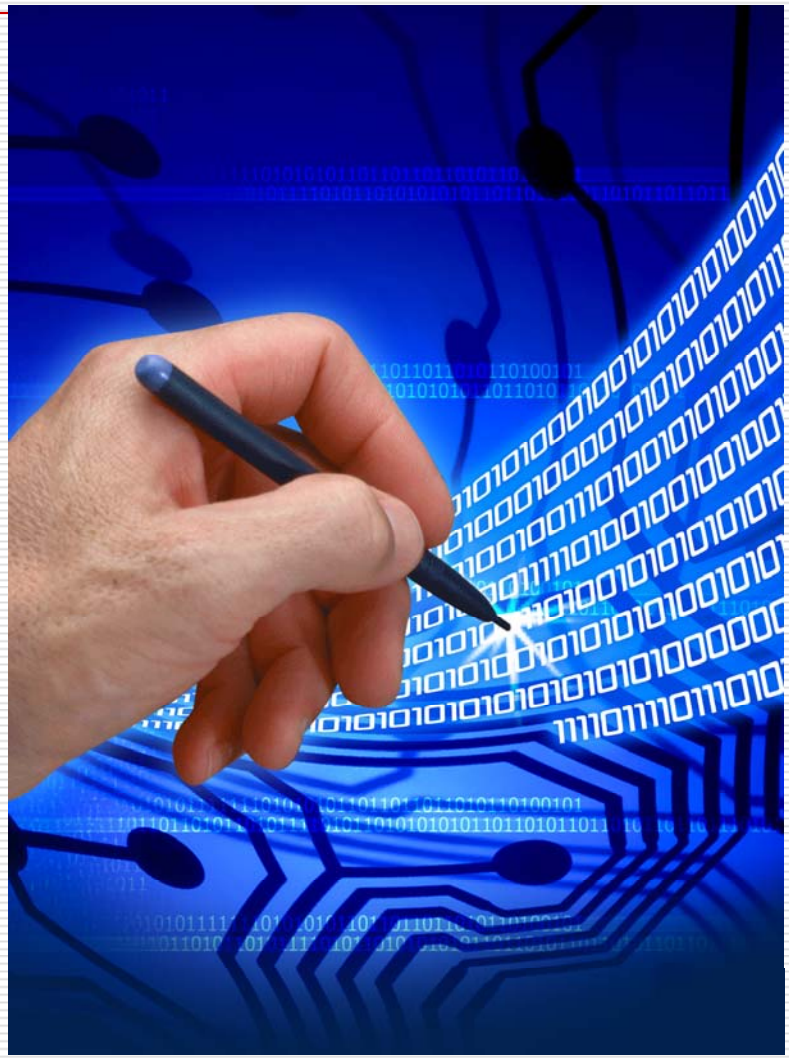
Software Security Metrics

- Software measures are troublesome (LOC, FPs, Complexity etc)
- *"Laws of Physics"* are missing
- Metrics are context sensitive and environment-dependent
- Architecture dependent
- Aggregation may not lead to strength



Examples

- Size and complexity
- Defects/LOC
- Defects (severity, type) over time
- Cost per defect
- Attack surface (# of interfaces)
- Layers of security
- Design Flaws



People Security Metrics

- Relevance
- Unique characteristics
  - Risk perception skewed “optimism Bias”
  - Limited memory and attention span
  - Behavior modeling is difficult
- Awareness training?

Reliability vs. Security

- Similar but different
  - We care more about reliability
  - Different adversary model
- Reliability models exist, but…
- Security is a moving target

Most Common Security Metric

- Risk- *We love this thing!*
  - Source for profit
- Where is the data?
  - Non monetary consequences
  - Adversary behavior models
  - Accuracy against ground truth
  - Mission/system/support models
- Dynamic in nature

Future Of Security Metrics

- Consumers demand better security metrics
- Government involvement is increased
- Science evolves to provide better measures
- Vendors volunteer (forced to) develop universal accurate metrics
- Some vendors cheat, a watchdog is created
- Security problems continue, no change in level of risk

FANTASTIC MEDIA PLAYER

Software Facts

Serving Size 3 Modules on Desktop
Serving Per Package about 17

Amount Per Serving
Usage 3 Hours

	% Daily Value*
Total Bugs 34	
Security Bugs 3	10%
Usability	57%
Reliability	88%
MTTF 1500 Hrs	82%
MTBF 27 Hrs	73%
Complexity	88%
	78%

Microsoft Code 0% • Oracle Code 3%
Open Source 23% • Proprietary 74%

*Numbers are approximate. Vendor not responsible for user errors. No warranty implied. Use at your own risk. User machine must meet software requirements. Software may be unsafe. Not designed for novices. No tech support available