Approaches to Security Metrics

Workshop Goals

Fran Nielsen, NIST/ITL

June 13-15, 2000

What’s the problem?

- Metrics are needed to assess, improve and “sell”
- Who’s working on metrics?
  - Lots of players, no rule book, little sharing

What’s the problem?

- What are security metrics?
  - Diversity of opinion on meaning of “metrics”
    - assurance
    - evaluation
    - audit
    - process versus performance measures
    - Webster
      - metric: “a standard of measurement”
      - yardstick: “a standard for making a critical judgment”

Workshop Background

- Kammer Nov ‘98 letter to CSSPAB
- CSSPAB decision to convene a security metrics workshop
- Expected outcomes
  - further the state-of-the-art
  - identify metrics and fill voids
  - recommended actions/activities

Workshop Purpose/Goals

- Focus: security metrics for non-classified cystems
- Goal: assess Current Information Infrastructure Protection Metrics
- Goal: identify security metrics, their uses, and voids

Workshop Agenda

- Day One
  - – Briefings on metric activities
- Day Two
  - – Panels - case studies
    - Government and industry perspective
      - – What is being measured? What can be measured?
      - – How are security features selected?
- Dialogue and interaction (invited participants)

After the Workshop

- Handouts, briefings posted to web-site
  - http://csrc.nist.gov/csspab/
- Workshop summary
  - posted on web-site
  - mailed to attendees
- Follow-on activities
  - **T B D**

Questions/Comments

Fran Nielsen
NIST/ITL/Computer Security Division
301/975-3669
fran.nielsen@nist.gov