Security Metrics

Computer System Security & Privacy
Advisory Board
June 13-14, 2000

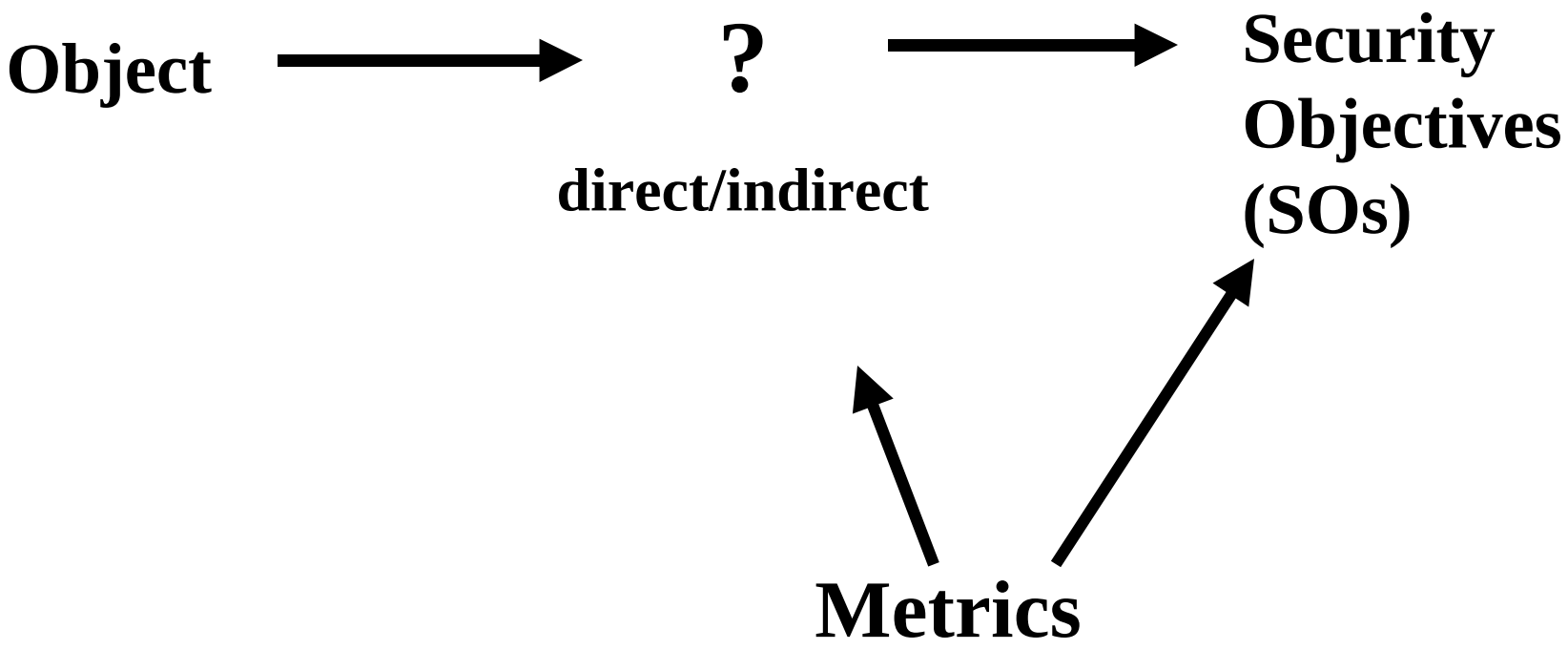
Dr. Stuart Katzke
Chief Scientist, Information Assurance Solutions Group
National Security Agency
(410) 854-7308
swkatzk@missi.ncsc.mil

Security Metrics: Examples

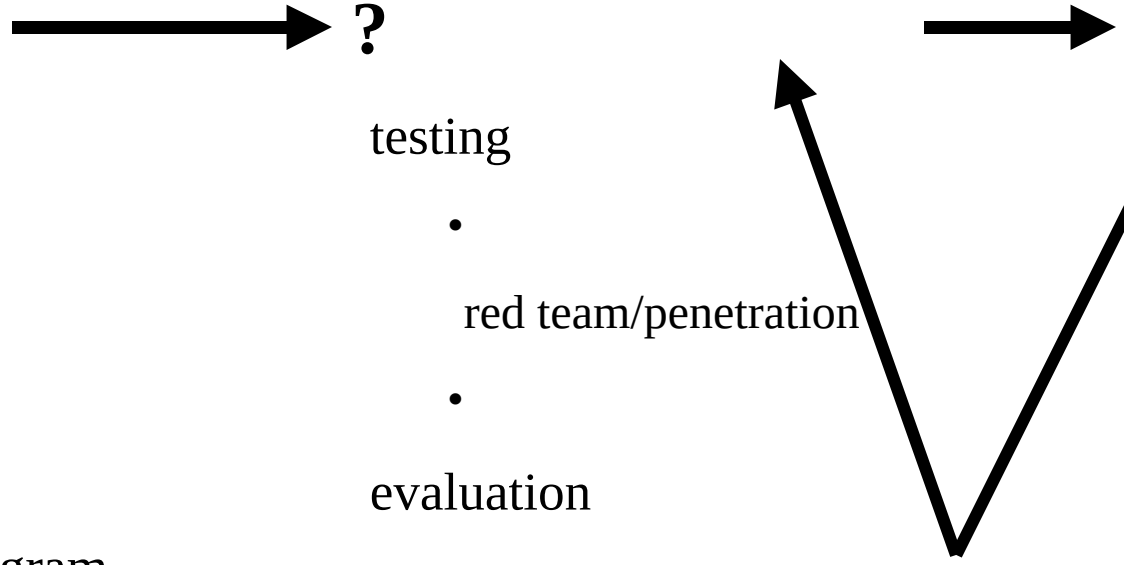
- Measuring the effectiveness of a security program
- Measuring an organizations/individuals ability to do security engineering & security assessment
- Measuring how secure a system/product is
- Measuring how good a security method/approach is
- Measuring risk

Security Metrics

- Ambiguous
- Immature Discipline
- Uncertainty
- Lack Precision
- Good Examples Exist
  - FIPS 140
  - TCSEC (Orange Book)
- Sometimes Use ***Indirect*** Measurement Methods (e.g., process as indicator)


Object
?
direct/indirect
Security Objectives (SOs)
Metrics

Security Metrics: Model



Object

-
- system
  -
  - intranet
- security program
  - individual

?

- testing
  -
  - red team/penetration
  -
- evaluation
-
- risk/vulnerability
-
- accreditation
-
- observation of performance (e.g., intrusion detection)

SOs

- CC
- specs/
- control objectives
- baseline
- maturity models
- IA-CMM

Security Metrics (Who: Object; Description)

- CSSPAB: CS Program; Effectiveness Assessment
- CIO Council: CS Program; Maturity Framework
- Private Sector: Organization; SSE-Capability Maturity Model
- NIAP: Organization; Infosec Assessment-Capability Maturity Model
- NIAP: Individual; Infosec Assessment Methodology (Ability/Capability)

Security Metrics: Activities (cont.)
(Who: Object; Description)

- NSA: Individual; Infosec System Security Engineering
- Many Sources: Products; Protection Profiles (Smartcard, Firewalls, VPNs, OS)
- BITS: Products; PP-like functional specification
- CIO Council: Organization; IT Privacy Impact Assessment (Draft: IRS Model)
- DoD: Organization; Infosec Assurance Readiness Metrics (Draft: self assessment/check list)