Workshop on Security Assessment: Metrics and Methods

January 24-25, 2014

Sorrento, Italy

Co-chairs:

Zbigniew Kalbarczyk (U. Illinois)

John Meyer (U. Michigan)

Bill Sanders (U. Illinois)

Security assessment: Why?

- The need for secure information systems is universally recognized as being essential for most all IT applications.
- But does system security need to be assessed?
- Yes! Because system manufacturers/owners/ leasers/managers/users want to know whether a system
  - satisfies prescribed security requirements (e.g., specified threshold values for various metrics)
  - is more secure this year than last year (e.g., after implementing revisions with this intent)
  - has better security than an alternative system
  - etc.

Security metrics

- Why the term metric as opposed to measure?
  - Measure is a precise mathematical notion and is well-suited to the quantification of system security.
  - On the other hand, the term metric appears to have more widespread use in a security context.
  - Certain security docs published by USA's NIST go both ways:
    - SP 800-55: *Security metrics guide for IT systems*
    - SP 800-55 Rev 1: "metric" is replaced by "measure"
- Basic security concerns (CIA triad):
  - Confidentiality
  - Integrity
  - Availability

Security metrics (cont'd)

- Metrics quantifying I and A are well understood by the dependability community and have been for half a century.
- However, metrics for C and related security-unique properties are more elusive with regard to their definition and formulation.
- More generally, there has yet to emerge a set of well-defined and widely-accepted metrics by which the security of information systems can be evaluated for specific purposes such as
  - prediction
  - comparison
  - verification
  - validation

Assessment methods

- In turn, there's a need for effective methods of determining the values of such metrics.
- Although metrics for I and A are old friends to dependability evaluation, methods of assessing them in a security context pose new challenges.
- This is due, in no small part, to more complex fault classes such as attacks that can cause corruption of data (loss of I), denial-of-service (loss of A), etc.
- Methods of security assessment are likewise more difficult with respect to metrics that quantify security-unique properties such as confidentiality, authenticity, and non-repudiation.

Workshop objectives

- Discuss current practices in security assessment.
- Identify challenges that accompany the assessment needs noted earlier.
- Propose metrics and methods that respond to these challenges.

Workshop program - Friday

- 09:00 Session 1
  - Moderator: Jay Lala - Raytheon
    - Andrea Guarino - Acea SpA
    - Zbigniew Kalbarczyk - University of Illinois
- 11:15 Session 2
  - Moderator: Lisa Spainhower - IBM (retired)
    - Mustaque Ahamad - Georgia Institute of Technology
    - Salvatore Stolfo - Columbia University
- 16:00 Session 3
  - Moderator: Tom Anderson - University of Newcastle
    - Richard Lippmann - MIT Lincoln Laboratories
    - Steve Noel - Mitre Corporation

Workshop program - Saturday

- 08:30 Session 4
  - Moderator: Karama Kanoun - LAAS-CNRS
    - Robin Bloomfield - City University of London
    - Laurie Williams - North Carolina State University
- 10:45 Session 5
  - Moderator: Mootaz Elnozahy - King Abdulla University
    - DongSeong (Dan) Kim - University of Canterbury
    - Andrea Cecarrelli - University of Florence
- 16:00 Wrap-up session
  - Moderator: Zbigniew Kalbarczyk - University of Illinois

Wrap-up Session

- Led by the session moderators.
- Each moderator will have10 minutes to
  - summarize (in at most 5 minutes) what was said/questioned during their session, with the option of including a personal take on what transpired,
  - in the 5+ minutes that remain, moderate any final questions/comments addressed to the speakers in their session.
- So if you didn't have a chance to squeeze in a choice comment or question during one or more of the regular sessions, save them for the wrap-up session.

Reminders for the speakers

- During the 45-minute period allotted for your presentation, please leave sufficient time (15 minutes or so) to field questions both during and after your talk.
- If comments/questions during your talk become excessive, suggest that they be deferred to the 15-minute discussion period that follows your session.
- The session moderator will help you keep track of time and, if needed, help control the amount of questioning.
- **We are looking forward to lively and informative contributions from all of you!**