Summary of Session 5

Mootaz Elnozahy

Scalable Security Models (Dan Kim)

- Security modeling for scalable cloud systems
- Scalability:
  - Number of vulnerabilities
  - Number of vulnerability type
  - Number of system components (e.g. hosts, networks, etc.)
- Approach: 3M
  - Security Measures
  - Security Metrics
  - Security Model (attack model)

Approach to Scalability

- Attack Representation Model (ARM):
  - Pre-processing of vulnerability, reachability analysis, etc.
  - Build an attack graph
  - Representation in visual or textual form
  - Security analysis using security metrics, then apply best practices in security
- A hierarchical approach: Hierarchical Attack Representation Model (HARM)
  - Upper level (host-to-host)
  - Lower level (within host)
- Further pruning:
  - Security based on important components

Results

- Simulation study showing different network types (ring, star), and different parameters (number of vulnerabilities, number of hosts)
- Shows that HARM is more scalable than AG (Attack Graph)
- Discussion
  - How to determine important components and effect on accuracy
  - Relationship to high-level, user-observable measures?
  - How do the results relate to risk?
  - Why not exploit the uniformity of a cluster to reduce overhead further (similar to BDD)

Design and Security Assessment of a Protocol for Continuous User Identity Verification (Andrea Ceccarelli)

- Design of an authentication protocol
- Model-based security analysis
- Context:
  - Secure user authentication for Web applications
  - Biometric data
  - Assessing trust
- Probability of a match error
- CASHMA (Context-Aware Security by Hierarchical Multilevel Architecture):
  - N sensors
  - Probability of Match error
  - Subsystem trust level: Probability of correctness
  - Problem: Global trust level, that is, belief at time t that the user is authentic

A Model of Trust Related To Authentication

- Mathematical model showing how trust decays over time
- Establishes a higher level of trust at the beginning proportional to the number of biometrics used
- Time decays more slowly with a higher initial level of trust (larger timeout on trust)
- Assessment: Using the model and a threat agent library from Intel (access limits, resources, skills, …)
- Biometrics: Voice, face, fingerprint
- Attackers: Generic with different capabilities (voice recording, picture,. …)
- ADVISE attack execution graph used to produce the results

Discussion

- Usability concern: Impact on the user
- Linking trust to the initial level of trust based on biometrics was a fodder for discussion
  - Trust decays exponentially linked to an attack not initial trust?
- One scenario was presented in the evaluation