WG10.4 – Session 1 Presentations

- Cyber Security of Medical Data
  - Luigi Romano
- Asymetric Security
  - Nick Multari
- Reliability of Stochastic Models
  - Thomas Gross

KONFID– a European Union Project for Cyber Security of Medical Data

- Goal: Trust and Security Enhancement of Interoperable eHealth Services
- Major Constraints
  - Independence of individual health systems
  - Compatibility with existing standards
- Approach
  - Each country has its own federated architecture
    - No standard solutions at the national level
    - KONFID interfaces multiple National Control Points using Intel Software Guard Extensions

KONFID (Continued)

- Technology Pillars
  - Photonic encryption key generation
  - Homomorphic encryption
  - Custom SEIM (Security Information and Event Management) for real-time security monitoring
  - Logging and audit mechanisms
  - HER (Electronic Health Record) standards
  - STORK electronic identification and trust services

KONFID – Rapporteur Comments

- Multiple Significant Challenges
  - Securely identify patients and users across borders
    - STORK may help here
  - Accurately translate documents across borders
  - Manage encryption among multiple users
    - Major challenge for both encryption and key mgmt
  - Efficiently monitoring overall security status

- Solutions to any of the above will be major technical accomplishment

Asymmetric Cyber Resiliency and its Validation

- ARC (Asymmetric Resilient Cybersecurity) Initiative at US Pacific Northwest National Laboratory
- Asymmetry
  - Disproportionate and exploitable imbalance between competing parties
    - Threats
    - Defense – goal is low-cost defense for high-cost offense
- Resilience
  - Multi-constraint optimization state machine problem

Asymmetric Resiliency (Continued)

- Asymmetric Cost

$$\frac{C_a \text{ (attack cost)}}{C_d \text{ (defense cost)}}$$

- Asymmetric Efficiency

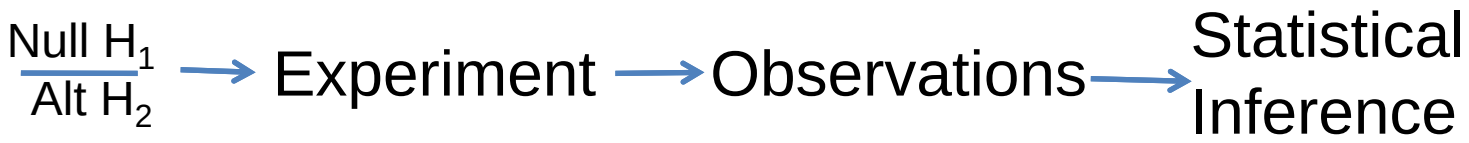
$$\frac{\left(\frac{V_a}{C_a}\right) \quad \text{(attacker efficiency)}}{\left(\frac{V_d}{C_d}\right) \quad \text{(defender efficiency)}}$$

Asymmetric Resiliency – Rapporteur Comments

- Asymmetry Often Credited to Attacker
  - Has choice of penetration point on attack surface
- But Asymentry is Valuable to Defender
  - Defender can manipulate attack surface by modifying application behavior
  - Can minimize attacker efficiency

Human Dimensions of Cyber Security – Statistical Hypothesis Testing

- Research Question:



- Biased Studies
  - The more biased the study, the less likely findings are true

    Ref: Ionnidis: “Why Most Published Research Findings are False”

Human Dimensions of Cyber Security – Statistical Hypothesis Testing – (Cont'd)

- Goal: Maximize PPV (Positive Predictive Value)
  - High PPV
    - Adequate power (sample size for effect size)
    - Few relationships investigated
    - Low bias in experiment design and execution

Human Dimensions of Cyber Security – Rapporteur Comments

- Careful Experiment Design and Execution is Important, but Difficult
  - Hypothesis selection
  - Sampling plan
  - Bias control