AN ADVERSARIAL RISK-BASED APPROACH FOR NETWORK ARCHITECTURE SECURITY MODELING AND DESIGN

CS Conference
June 2018

Paul A. Wortman[1], Fatemeh Tehranipoor[2], & John A. Chandy[1]
University of Connecticut[1], San Francisco State University[2]

UCONN

How do we measure security?

- Building of trust model
- Identify key characteristics
  - How to present risk factors
- Applications of safety and security assessment
  - Risk assessment techniques
- Arbitrary metric comparison
  - Difficult to compare quickly

Why center around risk?

- Probabilities of events
  - Adversary prospective
  - Potential attack vectors
    - Possible exploits
  - Single vs Combination of events

UCONN

Building an equation

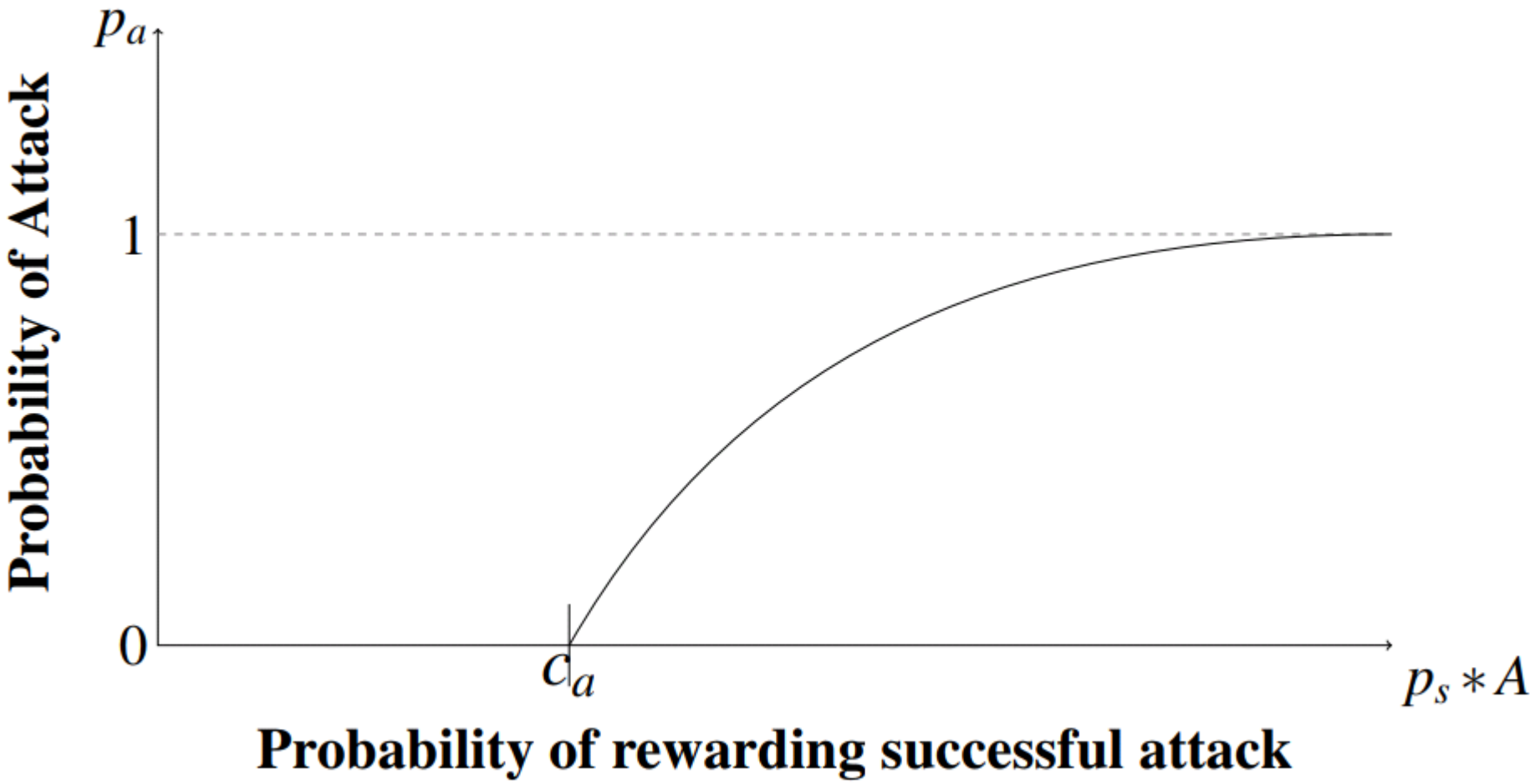
- **Replacing traditional risk**

$$SecurityRisk = p_a * p_s * Impact$$

- **Create ranking of 'Probability of Success' (p_s)**
  - **0 to 1 ranking of known solutions [single element]**
  - **Use attack tree calculation [multi-element]**
- **p_a related to p_s as well as the cost to an attacker**
  - **Influence by cost to attacker**

UCONN

Modeling the Attacker



UCONN

Building a Model

- Aggregate risk:

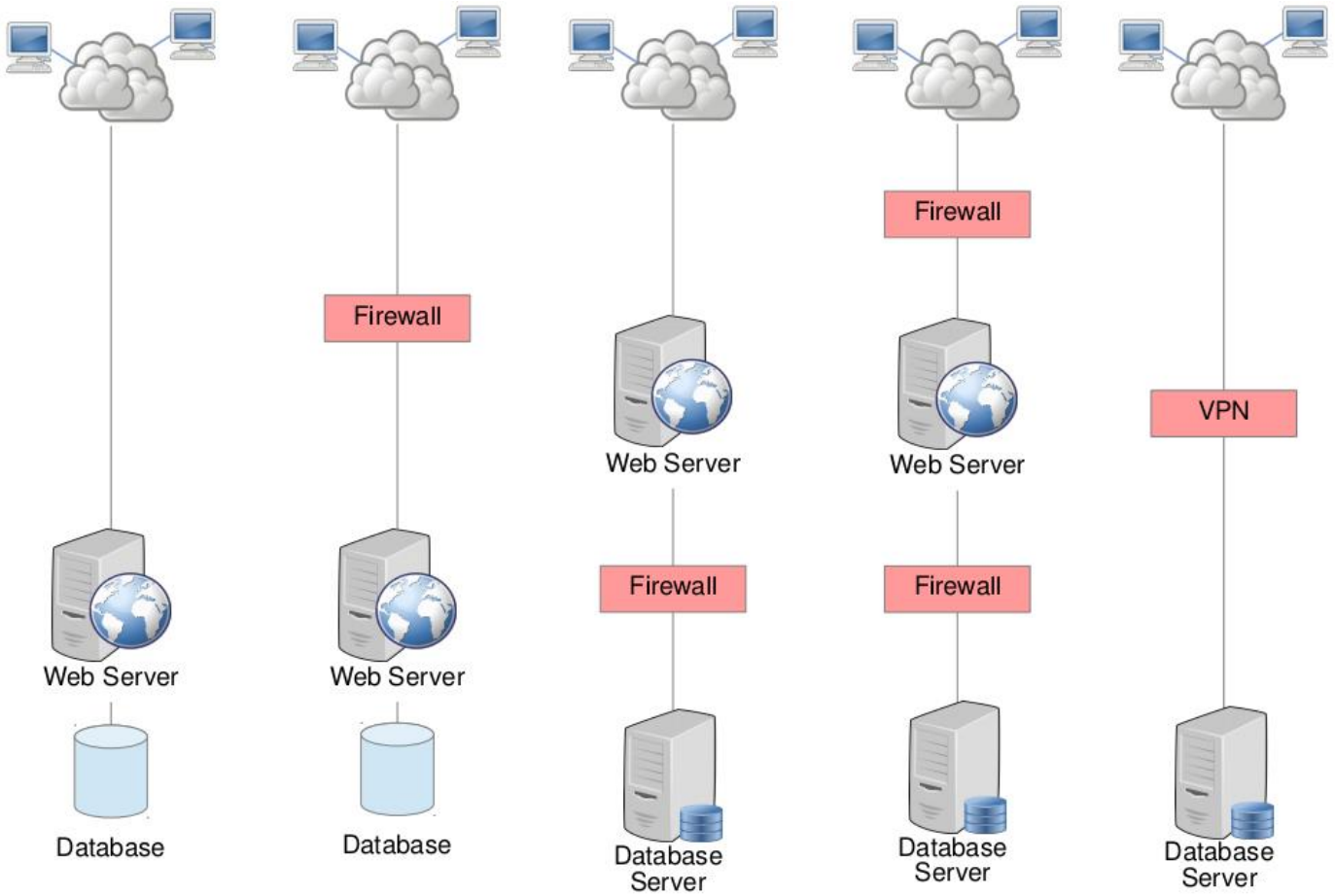
$$SR_{ia} = \sum_{j=1}^{J} \begin{cases} \left(1 - e^{-\alpha(p_{s_{ij}} * A_i - c_a)}\right) * p_{s_{ij}} * I_i, & if\ p_{s_{ij}} * A_i \geq c_a \\ 0, otherwise \end{cases}$$

- Application to security risk equation:

$$SR = \left(1 - e^{-\alpha(p_s * A - c_a)}\right) * p_s * I$$

- Applies to single instance

Network Security Example



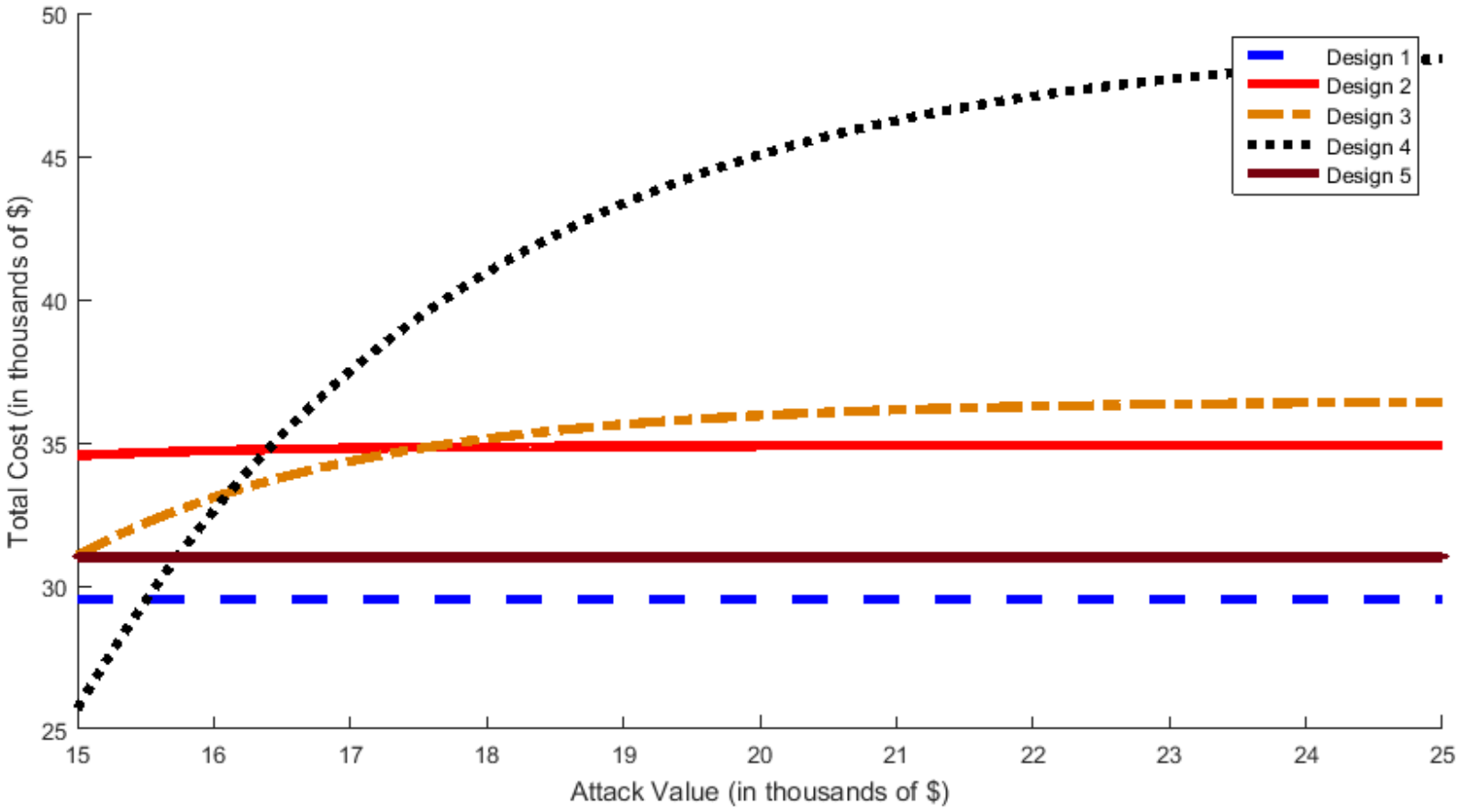
UCONN

Cost and Calculations

Component	Cost
Database	$3,000
Router	$6,000
Web Server	$10,000
Internal Firewall	$12,000
External Firewall	$8,000
VPN Implementation	$22,000

UCONN

Comparing Equation Values

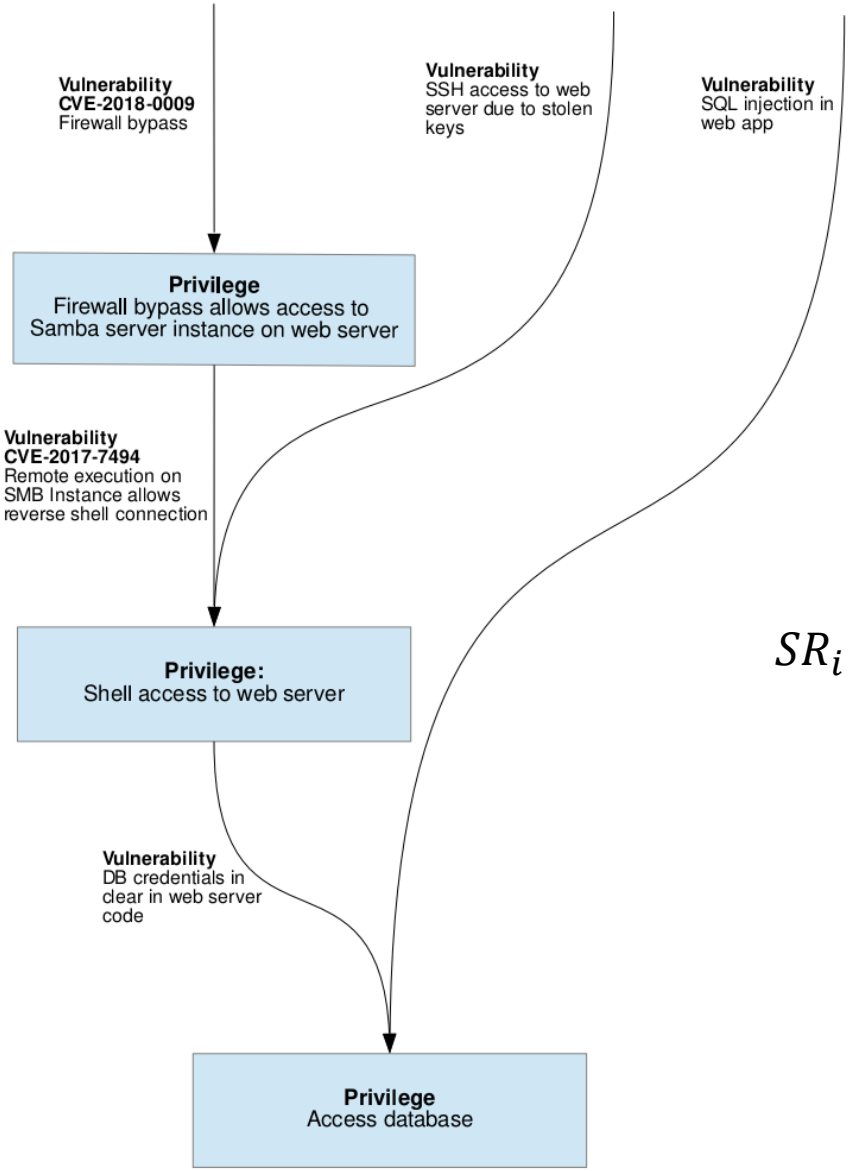


UCONN

Expanding Application

- Walking attack trees for evaluation
  - Walking paths of attack trees
- Users and environment
  - Risk seeking vs risk averse

Attack Tree Evaluation



- Examine each path
  - Risk Probability Product

$$p_s(P) = \prod_{v \in P} p_{ex}(v)$$

- Aggregate paths
  - Sum of combined attack vectors

$$SR_i = \sum_{P \in G_i} \left(1 - e^{-\alpha\left(p_s(P) * A_i - c_{a_i}(P)\right)}\right) * p_s(P) * I_i$$

- Use CVE as approximation of exploit probability
- Repeat process for complete attack graph

UCONN

Conclusions

- Introduced new meaningful security & risk-based metrics
  - Consideration of asset value to attack + defender
- Allow contrast & comparison of gamut of network security designs
  - Monetary cost for easier integration with existing risk-cost models
- Expansion of constraints & considerations
  - Intuitive vs non-intuitive nature
- Incorporation in large design exploration framework

UCONN