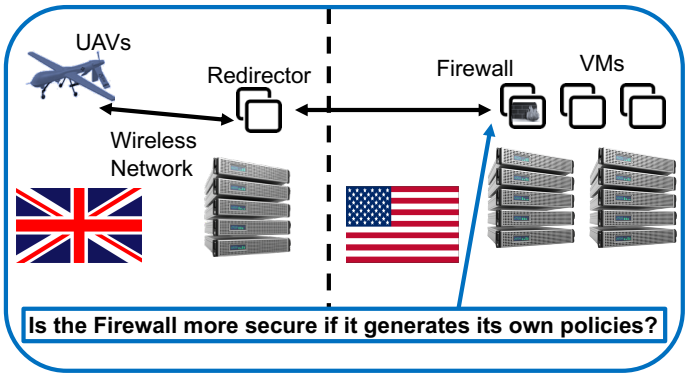
On the Impact of Generative Policies on Security Metrics

Dinesh Verma (IBM US), **Elisa Bertino** (Purdue), **Geeth de Mel** (IBM UK), **John Melrose** (Dstl)

Objectives

- Understand Security Metrics
- Impact of generating policies on security metrics

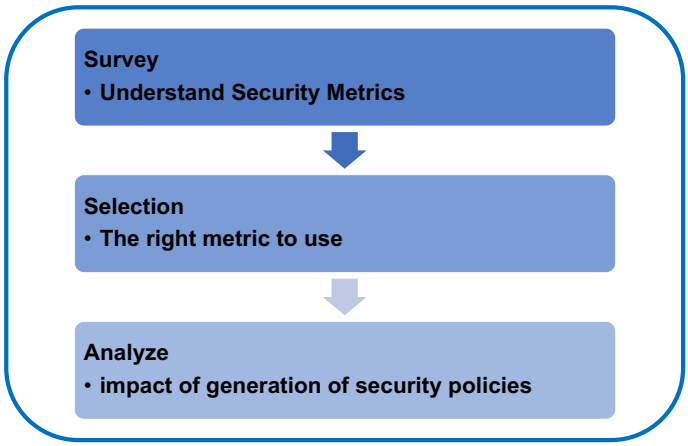


Technical Challenges

- Security Metrics are ill-defined
- Impact of dynamicity unclear

Approaches

- Survey Security Metrics in Literature
- Select more suitable Metric for Policy Assessment
- Determine equivalence to systems with static policies

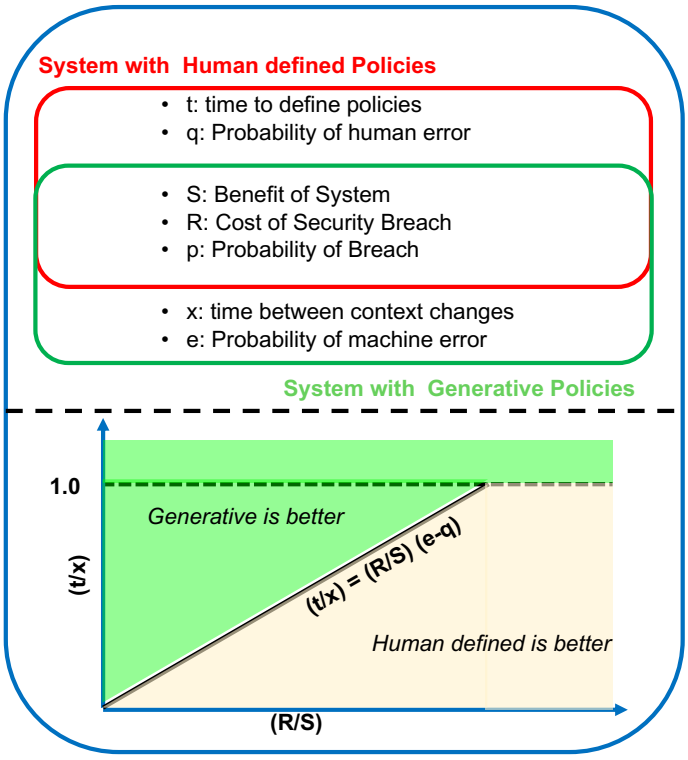


Military & Coalition Relevance

- Understanding Security Metrics important for V&V
- Required for transition of research activity

Results

- Surveyed state of research in security metrics
- Two Broad sets of efforts
  - (1) Classes of Metrics
  - (2) Measuring Security Metrics
- Adopted Cost-benefit approach of Security Metrics
- Identified conditions when generating policies is better
  - (1) When human errors are more likely
  - (2) When humans policy definition time is high
  - (3) When system context is highly dynamic



- Determined way to map security metrics of a system using generative policies to a system with human defined policies
  – Generative policies reduce breach probability by a factor of [(t/x)(S/R)/p – e]

Summary & Future Work

- Compare human definition with policy generation
- Approaches to simplify human policy definition
- Understand effectiveness of different AI approaches on security policy metrics

Publication(s) & Impact

- Appeared at IEEE SmartComp 2019 in Alexandria, VA