Session 1: Setting the Stage — Understanding Attacker Behavior and Current Practice

Report by
David Powell
LAAS-CNRS

Observations (Jay Lala)

- Spectrum of threats: from script kiddies to nation-states, terrorists and multinationals
  - ≠ motivations
  - ≠ means: innovation, planning, stealth, coordination
    - Need to evaluate according to threat environment
- Exponentially growing number of incidents & vulnerabilities
    - Can do better prevention, but perfection is impossible
    - So need to *quantify* degree of (im)perfection

IAM taxonomies (Dennis Hollingworth)

- Top-down conceptual terminologies
  - Not amenable to measurement
  - Terminology does not help for defining measures
  - Inconsistent — different viewpoints
  - Natural language — not machine-processable
  - Not amenable to definition of causality relationships
- Taxonomies amenable to measures need to be discovered from bottom up
- Need to invest in getting the dirty real low-level engineering work done

Defense-centric taxonomy (Roy Maxion)

- Attack-centric taxonomies are useful to the attacker, not the defender
- Examples of x-taxonomies
  - flaw classifications (Landwehr)
  - classifications of attacks by symptoms (Puketsa, Kumar)
  - classifications of attacks by intent (Lindqvist+, Lippmann+)
- Tested suitability hypothesis of one: Lippmann+
- Attacks that manifest in the same way come from many attack-centric classes
- Full defense-centric attack taxonomy tested against Stide IDS

Formal (verif.) methods (George Dinolt)

- Required features
  - Describe desired system properties
  - Describe desired functionality
  - Provide assurance that it makes sense (functionality consistent with desired properties)
  - Provide assurance that it is correctly implemented (implementation is an instance of the functionality)
- Measuring assurance?
  - Depth of formalization process (like "test coverage criteria")
- CISR microkernel project
  - CC EAL7 evaluatable micro kernel

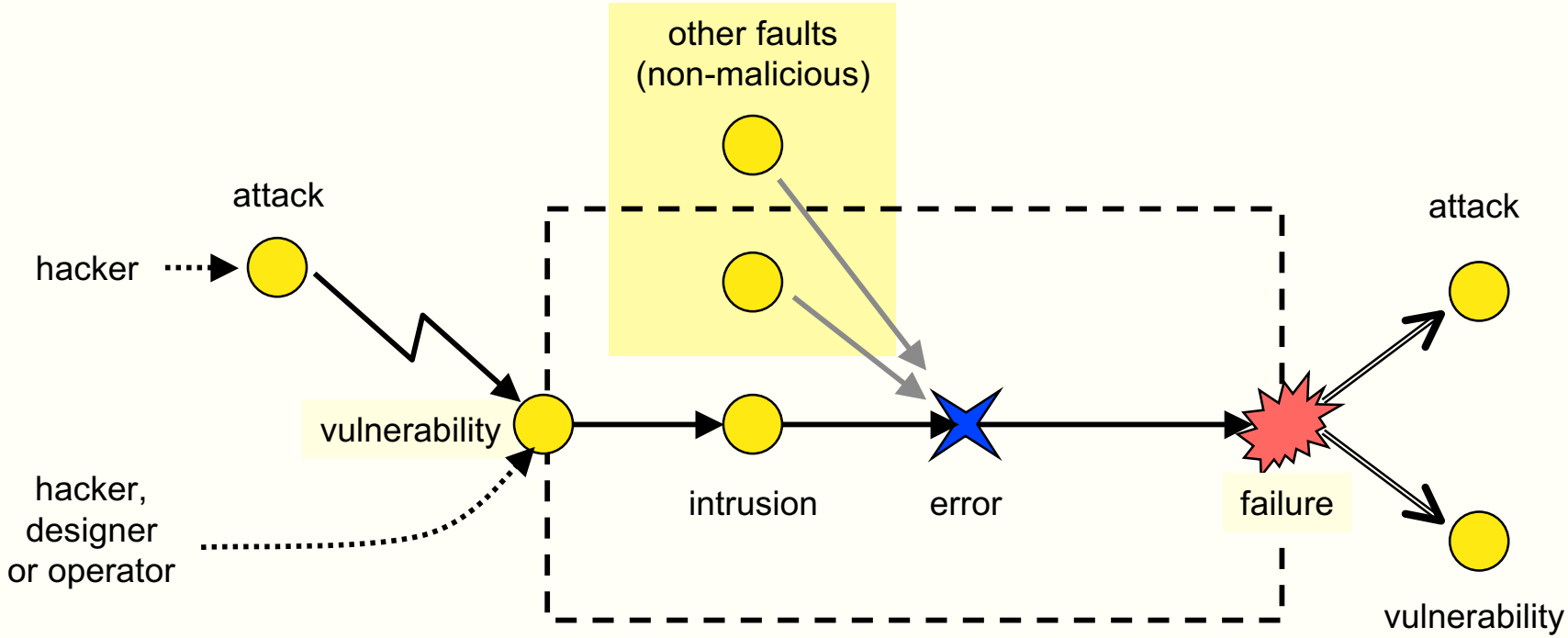
Evaluation via red teams (Bradley Wood)

- Effort needed as a measure of survivability?
  - Some successes, but expensive and too aggressive
- An alternative: Critical Security Rating (CSR)
  - Consequences X: bad things to avoid + impact (pie chart)
  - Risks: Y: causes + degree of worry (pie chart)
  - Mitigation matrix : consequence X mitigated by risk Y?
  - CSR: sum of "mitigation values"
- Process tested at an R&D lab
  - Highly subjective (but burden on operator)
  - Cheap, yet large potential positive impact
  - Mitigation matrix requires some work

Focus areas (Bill Sanders)

- Basic concepts & terminologies for IA domain issues
- Security and survivability requirement specs
- Threat, attack and vulnerability taxonomies
- Models of attacker intent, objectives and strategies
- Measures: work factor, survivability, operational security, crypto protocol... metrics
- Methods for validating protection & tolerance mechanisms

Attack, vulnerability, intrusion



Security methods

Fault	Attack (human sense)	Attack (technical sense)	Vulnerability	Intrusion
Prevention (how to prevent occurrence or introduction of…)	deterrence, laws, social pressure, secret service…	firewalls, authentication, authorization…	semi-formal and formal specification, rigorous design and management…	= attack & vulnerability prevention & removal
Tolerance (how to deliver correct service in the presence of…)	= vulnerability prevention & removal, intrusion tolerance		= attack prevention & removal, intrusion tolerance	error detection & recovery, fault masking, intrusion detection and response, fault handling
Removal (how to reduce number or severity of…)	physical countermeasures, capture of attacker	preventive & corrective maintenance aimed at removal of attack agents	1. formal proof, model-checking, inspection, test… 2. preventive & corrective maintenance, including security patches	⊆ attack & vulnerability removal, i.e., preventive & corrective maintenance
Forecasting (how to estimate present number, future incidence, likely consequences of…)	intelligence gathering, threat assessment…	assessment of presence of latent attack agents, potential consequences of their activation…	assessment of: presence of vulnerabilities, exploitation difficulty, potential consequences…	= vulnerability & attack forecasting

Security Assessment Methods

Fault	Attack (human sense)	Attack (technical sense)	Vulnerability	Intrusion
Forecasting (how to estimate present number, future incidence, likely consequences of…)	intelligence gathering, threat assessment…	assessment of presence of latent attack agents, potential consequences of their activation…	assessment of: presence of vulnerabilities, exploitation difficulty, potential consequences…	= vulnerability & attack forecasting