

Next-Generation Information Attack Strategies

Dan Ellis

703-983-5807 • ellisd@mitre.org

MITRE Sponsored Research



MITRE
Technology
Program

Problem

- How do you describe the potency of worms?
- How potent are *contemporary worms*?
- What are next-generation worms like?
- How potent can *smart worms* be?
- What defenses are possible?

Background



How bad can worms possibly be?



A worm strikes...



All right. How can I defend myself?

Objective

- **To understand the threat that contemporary and next-generation worms pose**
- **To identify defensive tactics, strategies, and postures that are possible against these threats**

Activities

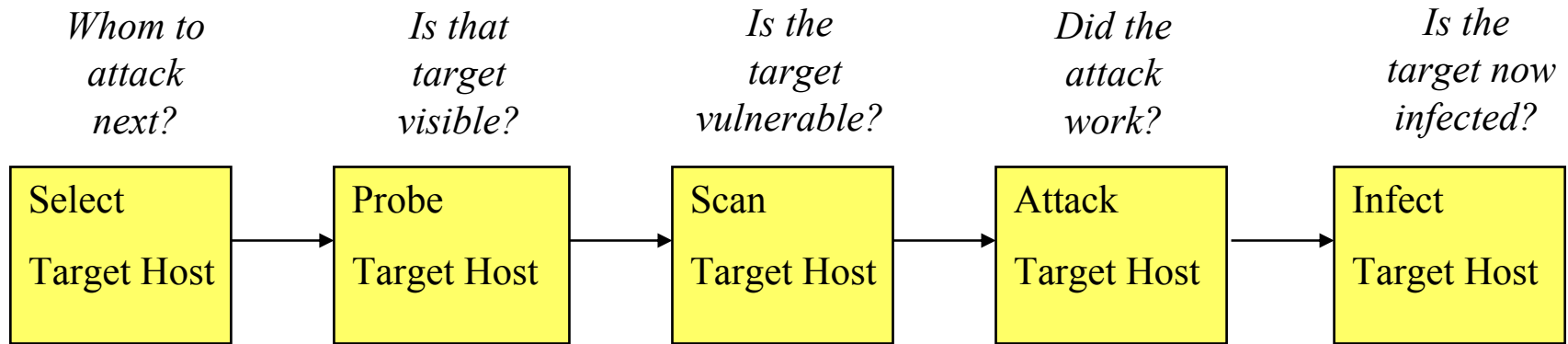
■ Analysis of Worms

- design model of contemporary worms and smart worms
- derive potency relation over attributes and environment
- identify defenses

■ Implement Prototype

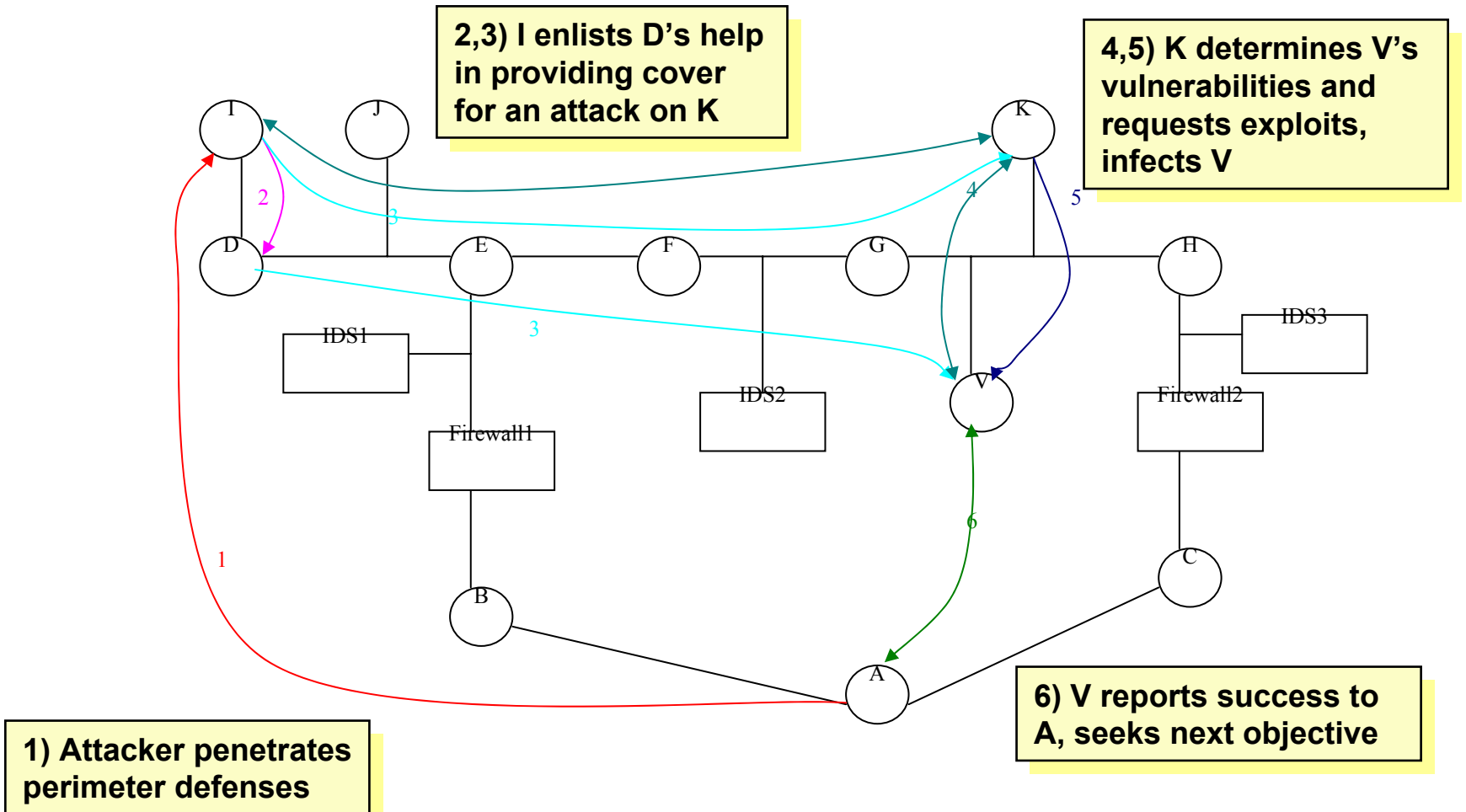
- prototype smart worm
- prototype defenses

Highlight



Procedural Model of Contemporary Worms

Demonstration



**A Coordinated Network Attack on V
by a Smart Worm**

Impacts

■ Design better defenses

- describe potency of inbound attacks
 - help defenders allocate resources during an attack
- guide development of defenses

■ Build and validate better defenses

- validate prognostic use of R
- validate defenses developed

Future Plans



- Identify and validate anti-worm defenses