

# Next-Generation Information Attack Strategies

Dan Ellis

703-983-5807 • [ellisd@mitre.org](mailto:ellisd@mitre.org)

MITRE Sponsored Research

The logo for the MITRE Technology Program, featuring a stylized graphic of stacked blocks in yellow, orange, and blue on the left, and the text "MITRE Technology Program" in yellow and white on the right.

MITRE  
Technology  
Program

# Problem

- How can the potency of worms be characterized?
- How potent are contemporary worms?
- What are next-generation worms like?
- What defenses against worms are possible?

# Background



*How bad can worms possibly be?*

**A worm strikes...**



**...15 seconds later the network is toast**



*How can I defend myself against these worms?*

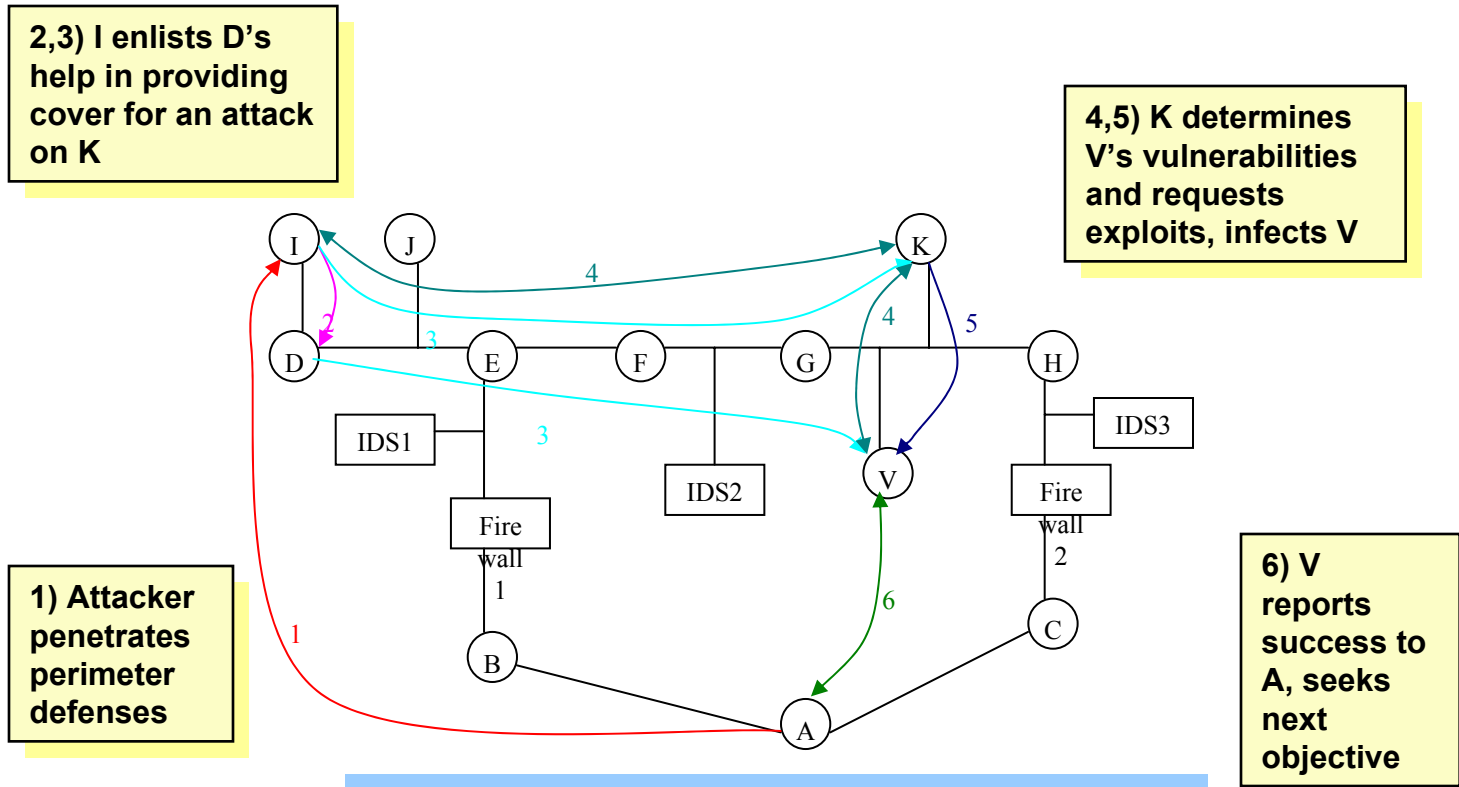
# Objective

- **To understand the threat that worms pose, and be able to quantify that threat**
- **To identify defensive tactics, strategies, and postures that are effective against these threats**

# Activities

- **Analysis of contemporary worms**
- **Model of worm algorithm and potency**
- **Implementation of model in simulation environment**
- **Enumeration of defensive postures and tactics in simulation environment**

# Highlight



**A Coordinated Network Attack on V by a Next-Generation Worm**



# Impacts

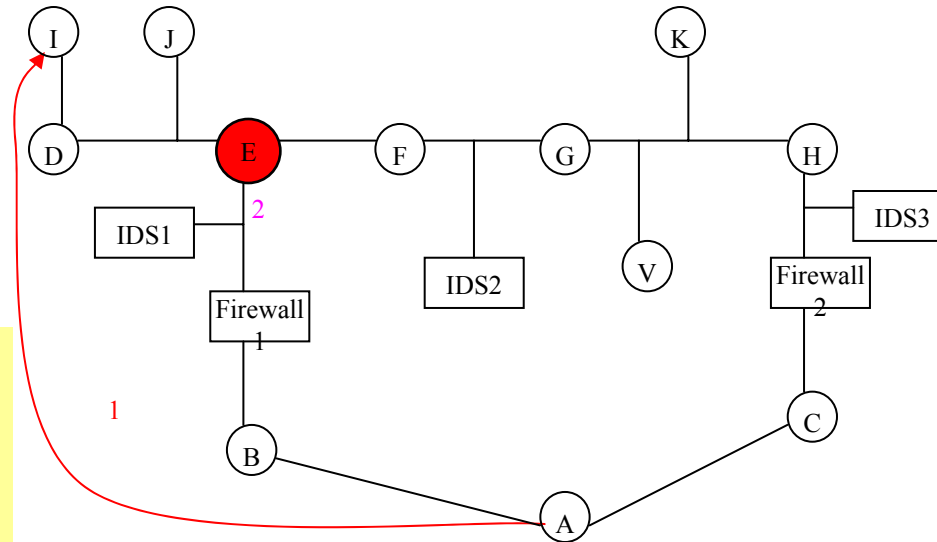
- **Quantitatively reason about hypothetical worm threats**
- **Identify real-time active responses, postures to mitigate the threat**

# Future Plans

2) IDS detects behavior that may be malicious.  
Q: Do you tell E to contain the possibly infected segment? (Balance cost/rewards within capabilities.)

Q1: How do you detect worms?  
Q2: How do you balance the cost of infection with the rewards of the service in real-time?

1) A accesses services on I. If the access is benevolent, there is a reward; if malevolent, a cost.



Open Questions For Countering The Worm Threat