Collaborative Red Teaming for Anonymity System Evaluation

Sandy Clark (Penn)
Chris Wacek (Georgetown)
Matt Blaze (Penn)
Boon Thau Loo (Penn)
Micah Sherr (Co-PI, Georgetown)
Clay Shields (Co-PI, Georgetown)
Jonathan Smith (Penn)

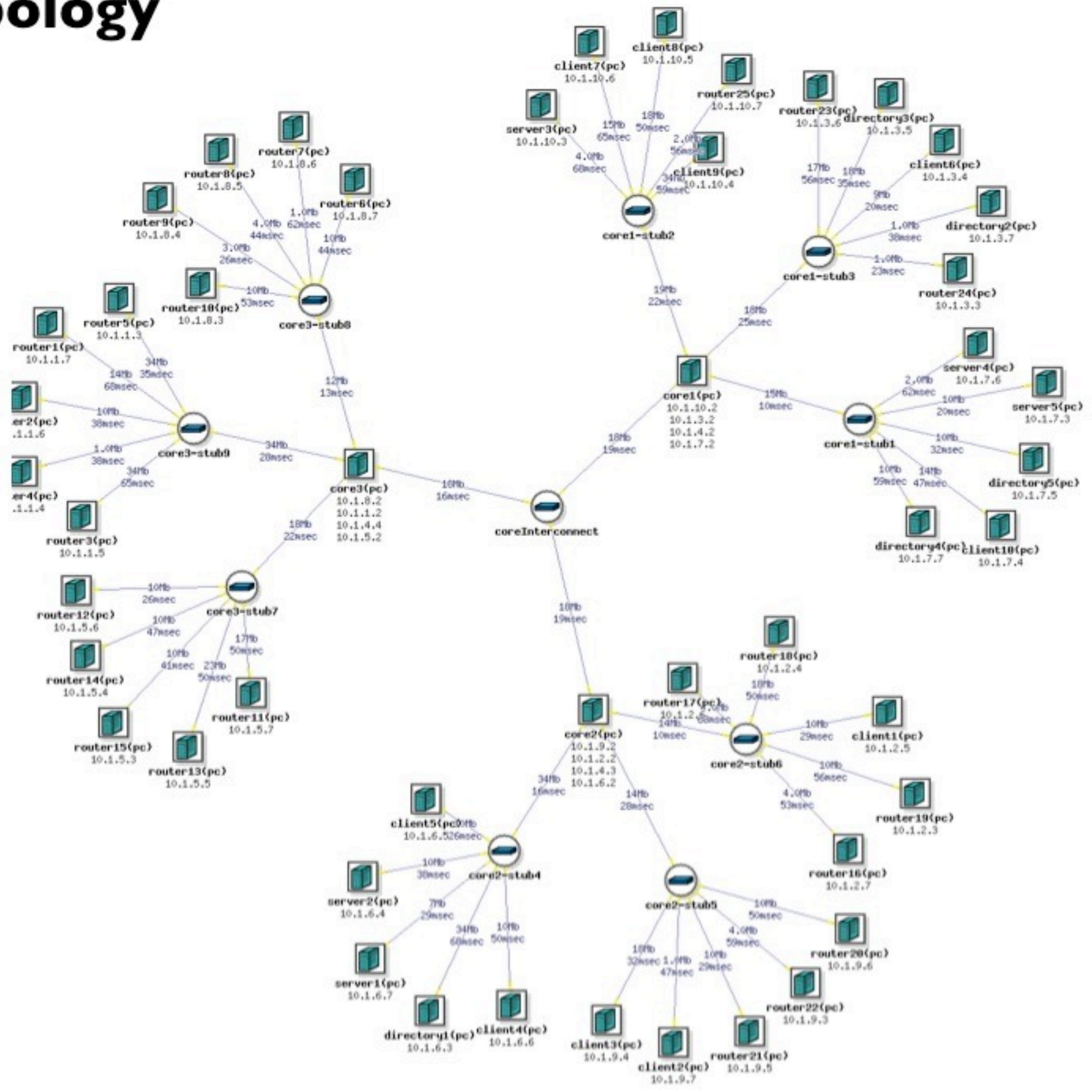




Outline

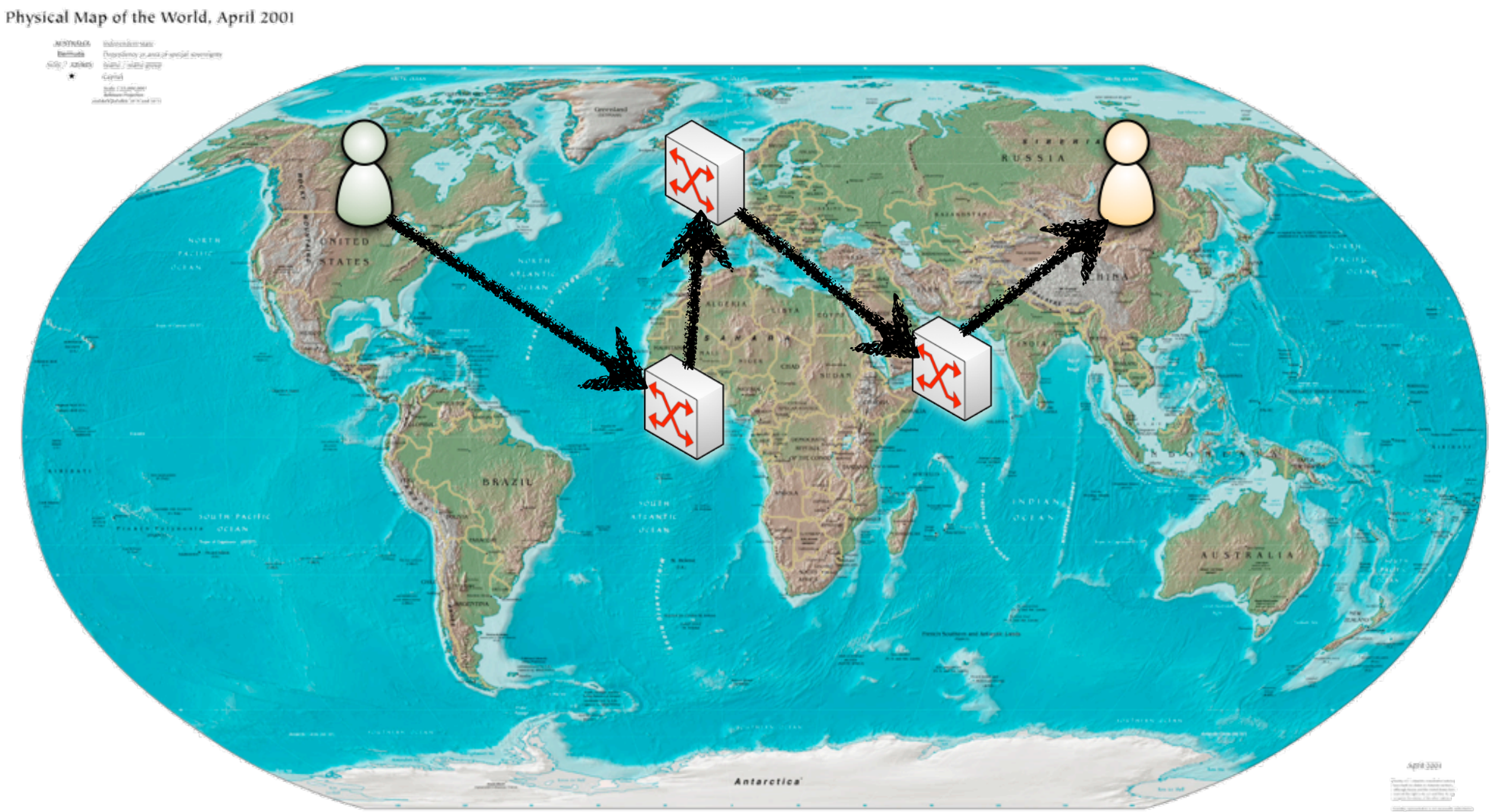
- Introduction
- Overview of SAFEST Evaluation Framework
- Penetration Testing
- School of Fish

SAFEST Experimental Topology

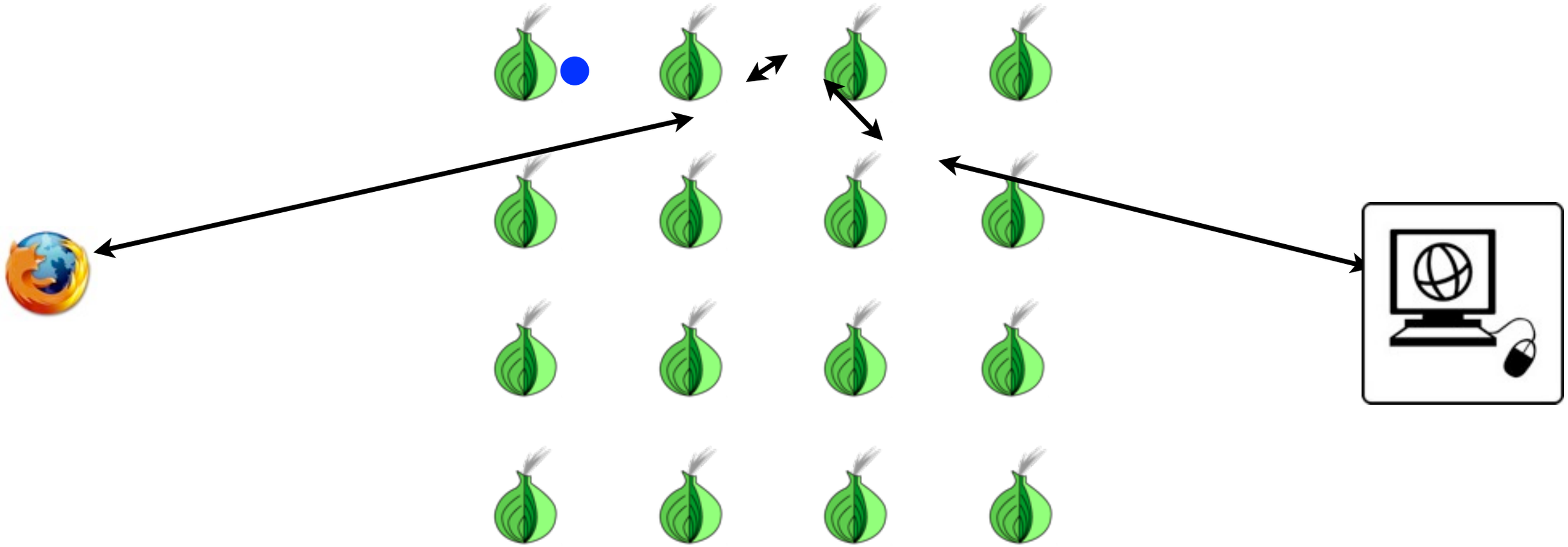


Birds Eye View: SAFEST Approach

1. Intelligently select anonymizing routers to increase performance



SAFEST Coordinate System



Penetration Testing Methodology



Overt :

Initial Brain storming Session with Designers

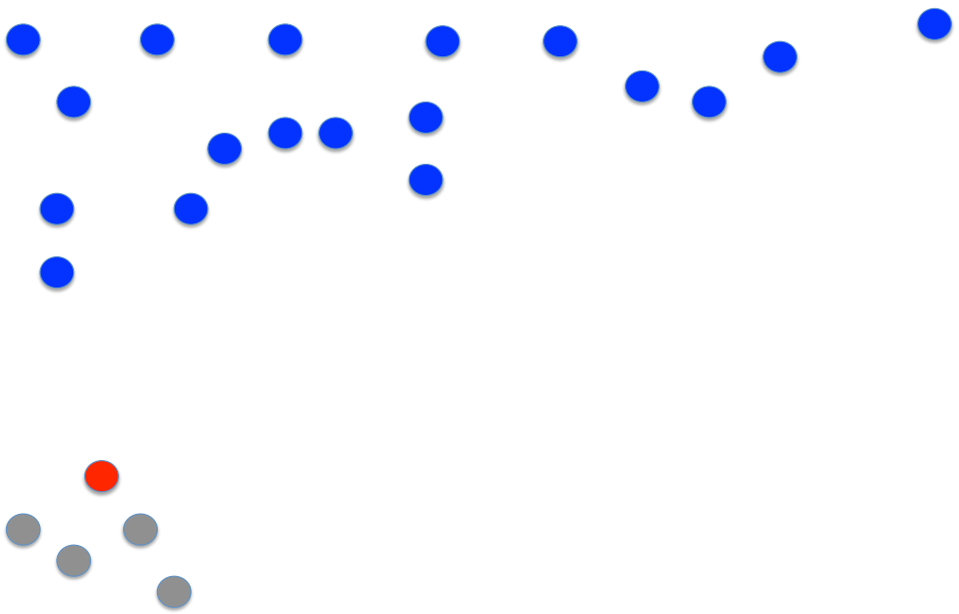
Covert:

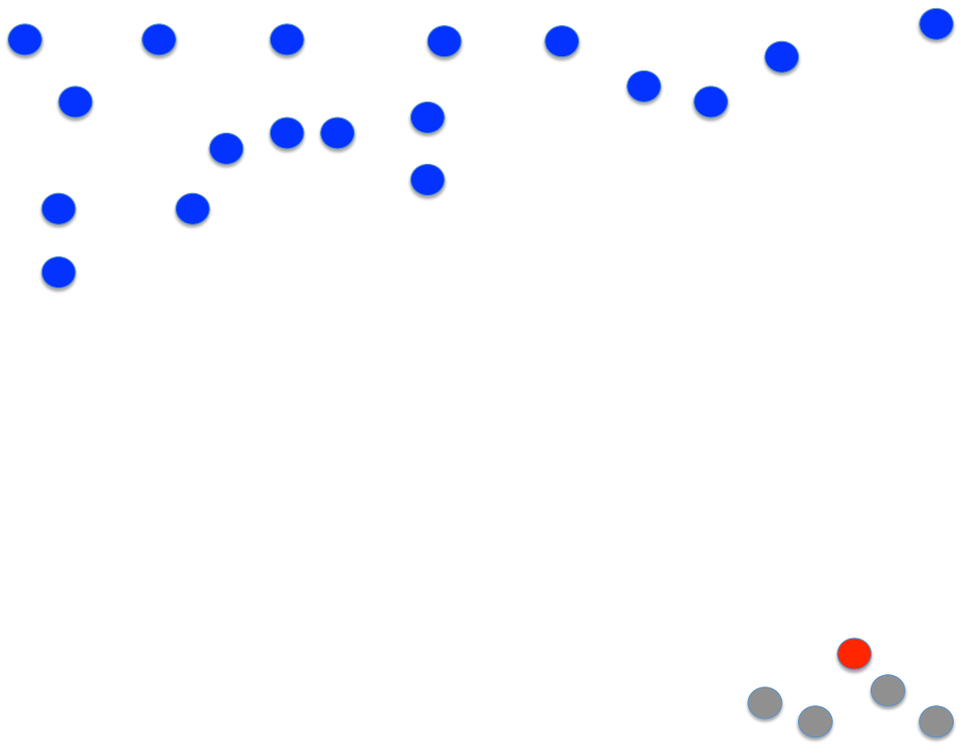
Designers/IT staff unaware of sytem evaluation

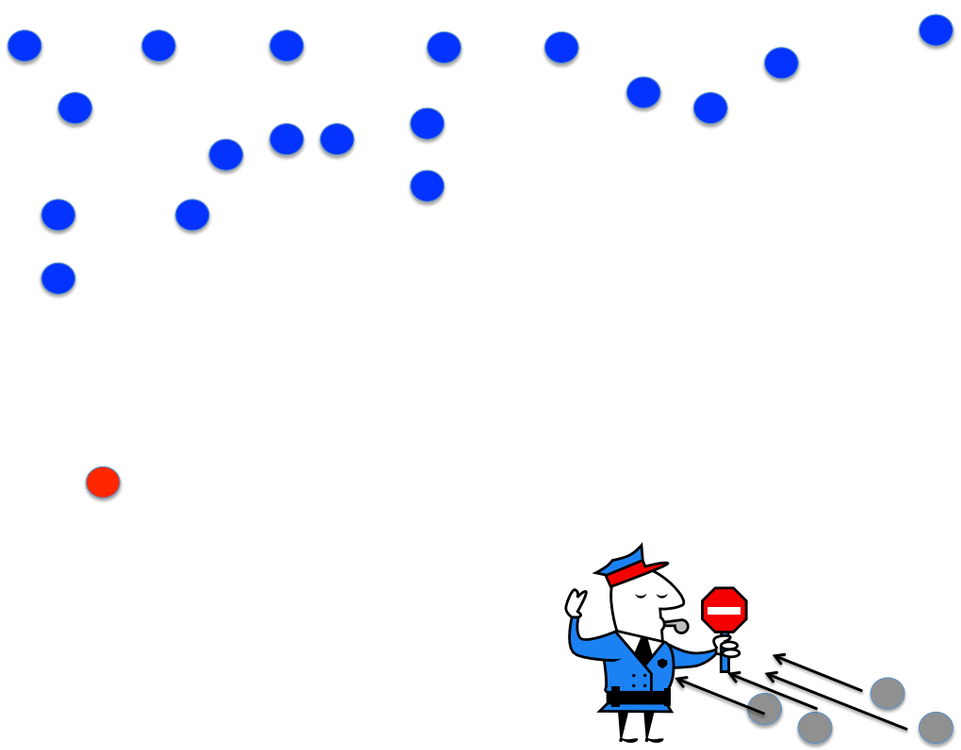
Developers *rarely* participate in the Analysis or Exploitation phases

School of Fish Attack

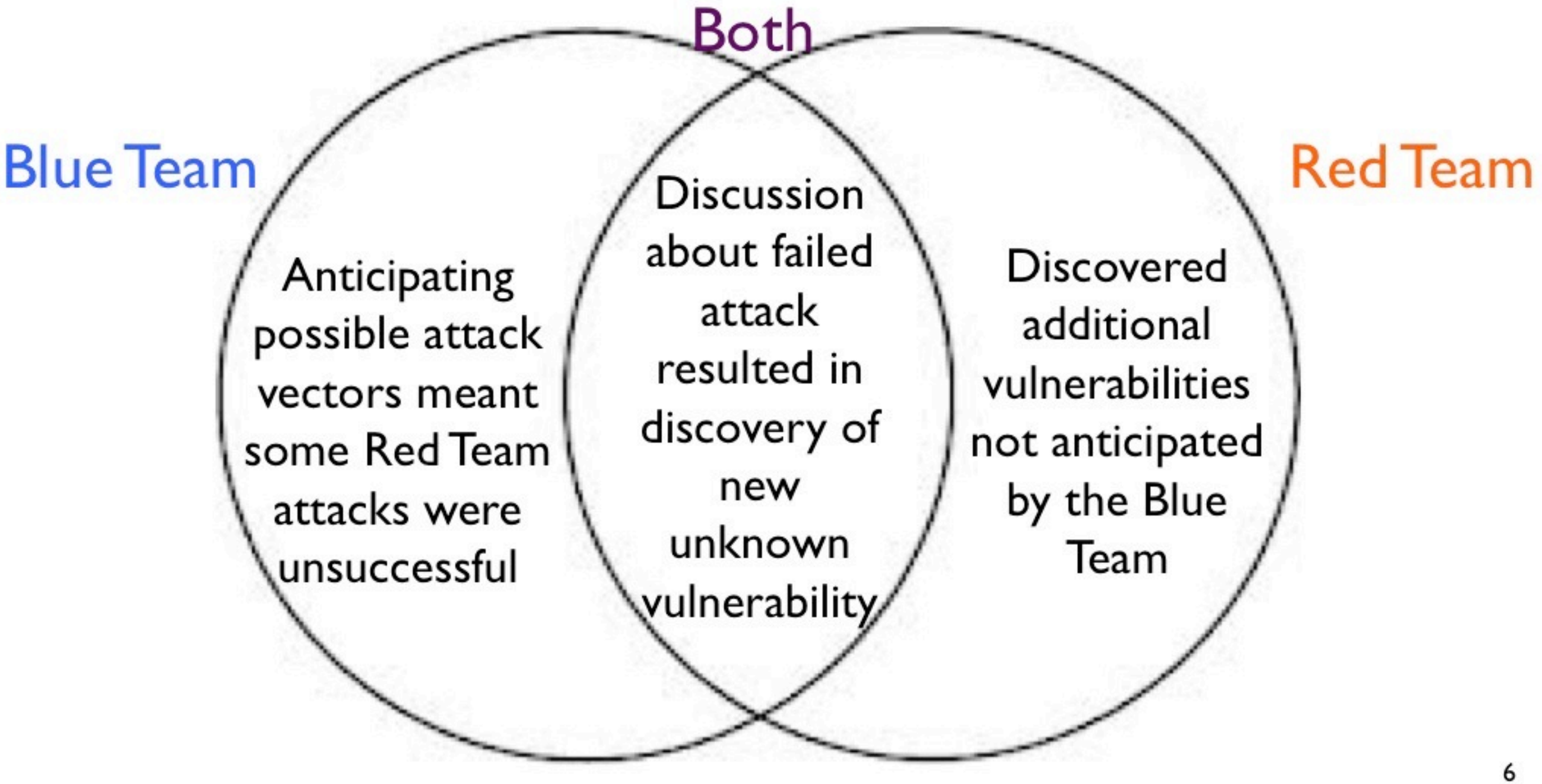








Collaborative Red Teaming



Collaborative Red Teaming Methodology

- Scope Setting
- Information Gathering (with or without Blue team involvement)
- Independent Vulnerability Analysis
- Exploitation Phase
  - **Sandboxing Phase**
- Reporting and Assessment Phase

Lessons Learned

- Red Team would have found this eventually
- So would a motivated Adversary
- Collaborative Red Teaming of SAFEST saved a Discovery-Exploit-Patch iteration (essential for an anonymity system)

Lessons Learned

Blue Team

- Learns new skills and experiences the "Attacker Mindset"

RedTeam

- Gains insight into design assumptions.

Both

Gain from deeper understanding of system, and related, ability to learn interactively.

Gain from diversity of perspectives, and the "many eyes", number of examiners of system.

Questions?