Trapping and Tracking Hackers: Collective Security for Survival in the Internet Age

Douglas B. Moran

Vice President, R&D

Recourse Technologies

www.recourse.com

Our Philosophy

- Pure defensive strategy doomed
- Defenses subverted: “bit-rot” and legit user
- Respond to attackers when still detectable
  - Assess and prioritize
  - Defenses change in response to changes in threat
  - If wait for undetectable: response = recovery
- Some attacks will succeed: ameliorate

Collective Security

- **Multilevel**
  - Subnet/Cluster
  - Enterprise/Organization/Site
  - Coalitions
  - Internet
- **Collective security of defensive systems**
  - Detect attacks/evasion against others
  - Simplify design of tools
  - Increase complexity of attackers choices

Better Reporting

Needed:

- More detections
- More reports
- More complete
- More consistent
- Sooner
- Attacks, not exploits
- Chains of hosts

Impediments

- Expertise needed
- Labor intensive
- Confidential info
- Loss of confidence

Honeypots

Deception Servers

- Network services
- Shallow deception
- Detect scanning
- New network exploits

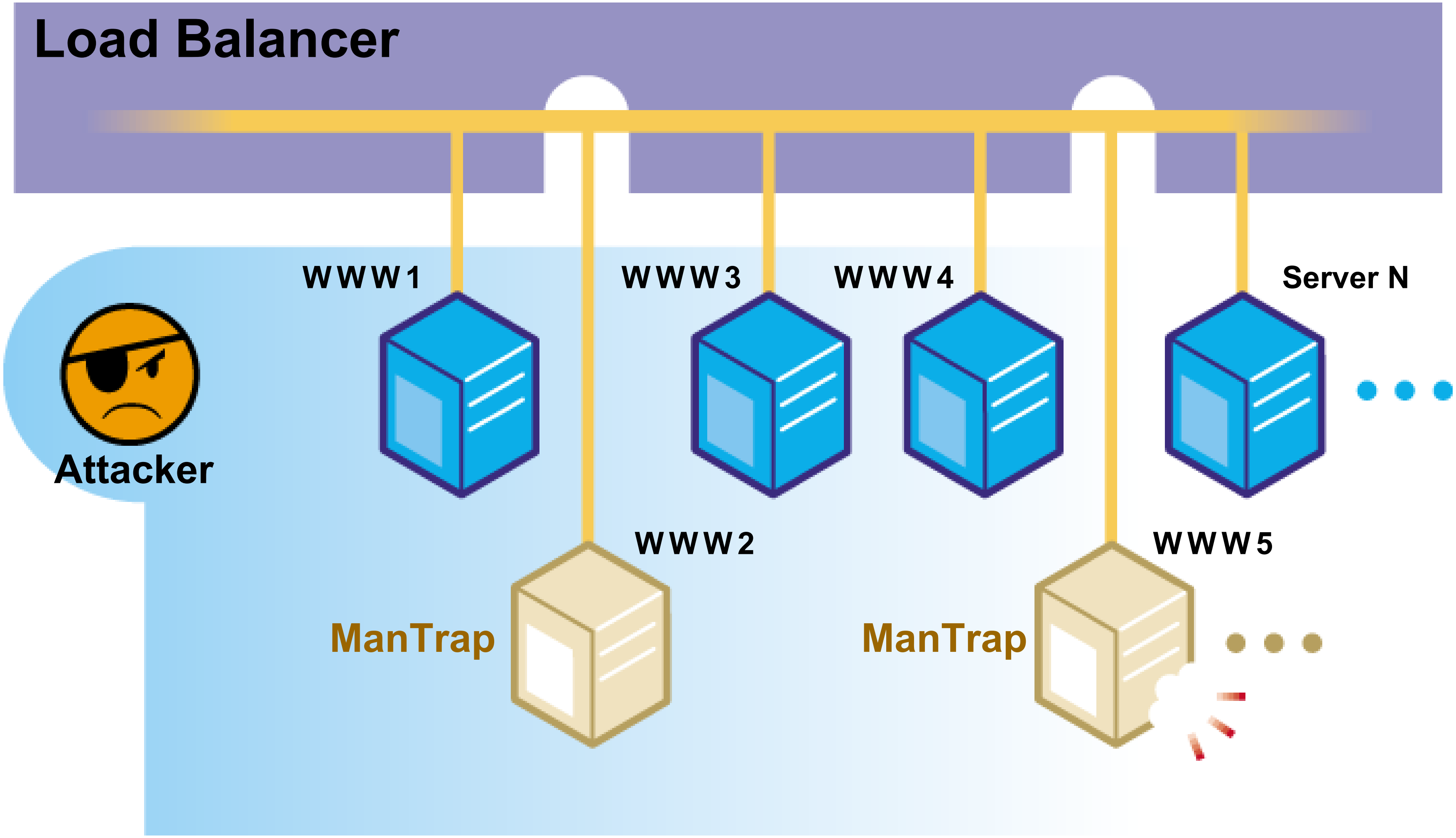
Deception Hosts

- Full environment
- Capabilities&Intentions
- Insider abuse
- Delay
  - For trackback
  - Improve defenses
  - Attacker wastes time

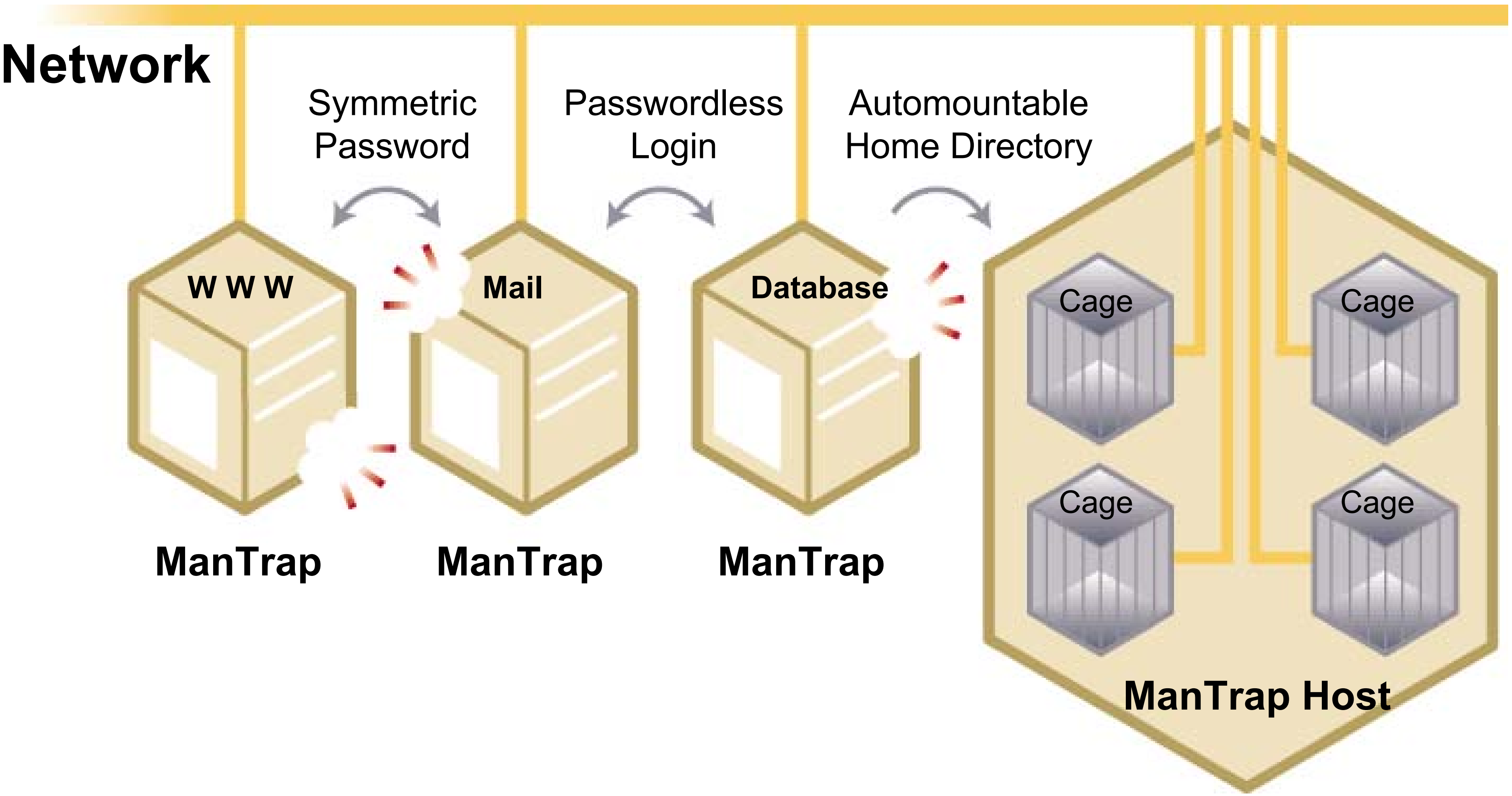
Deception Host: ManTrap™

- Monitoring
- Setup and resetting
- Containment: host
- Quality of the deception
  - Faithful representation of platform
  - Concealment of monitoring and management
  - Convincing content: escalating requirements

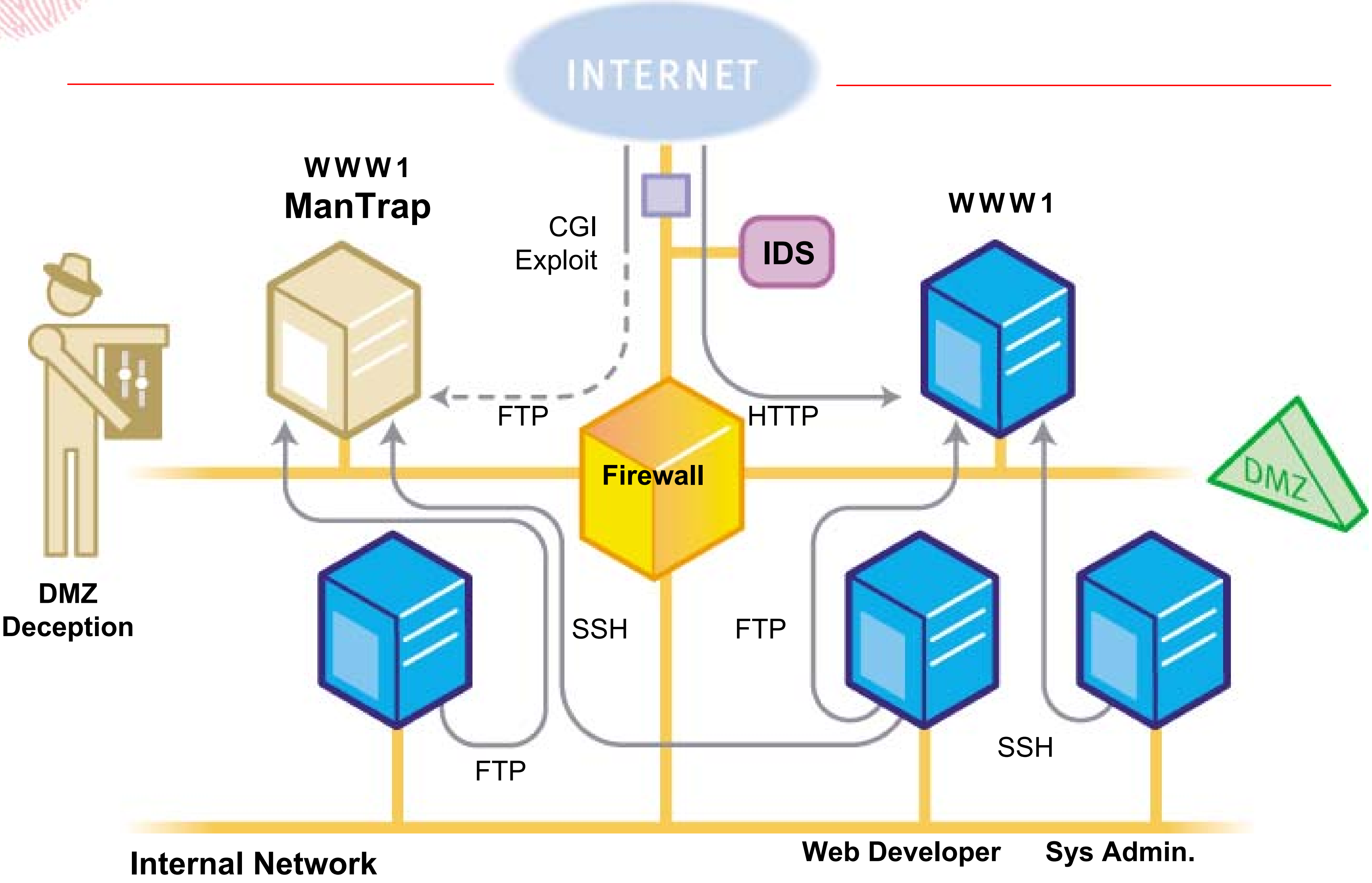
Deployment: “Minefield”



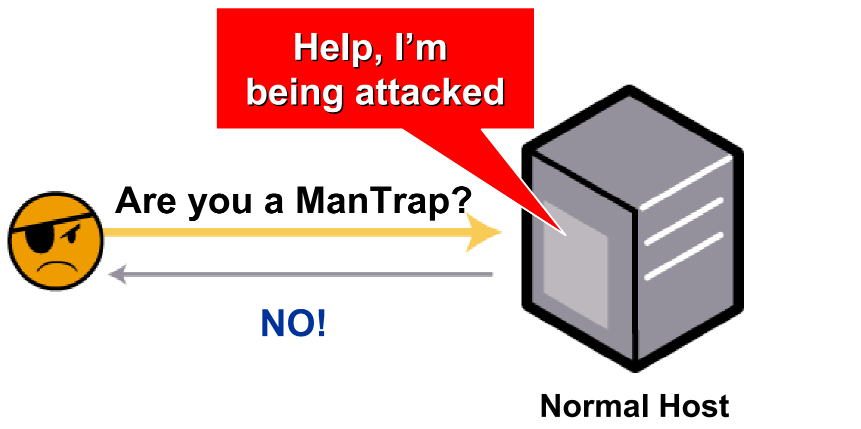
Deployment: "Zoo"



Deployment: “Shield”



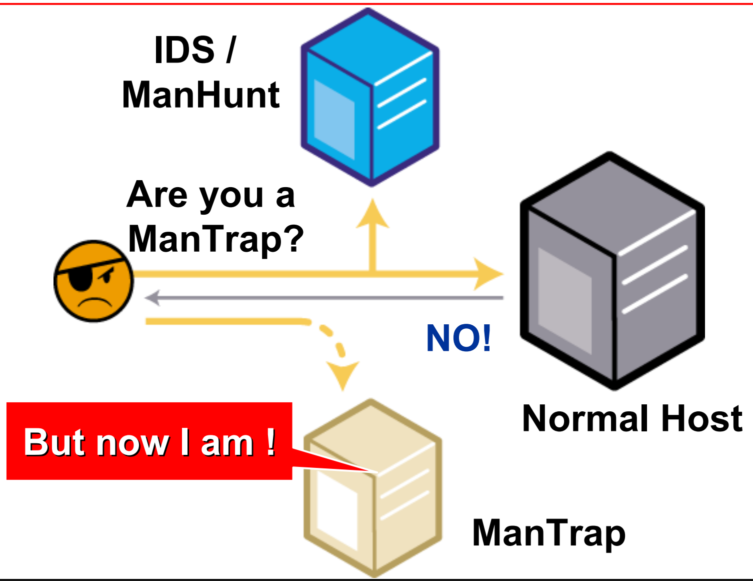
Collective Security


Help, I'm being attacked

Are you a ManTrap?

NO!

Normal Host


IDS / ManHunt

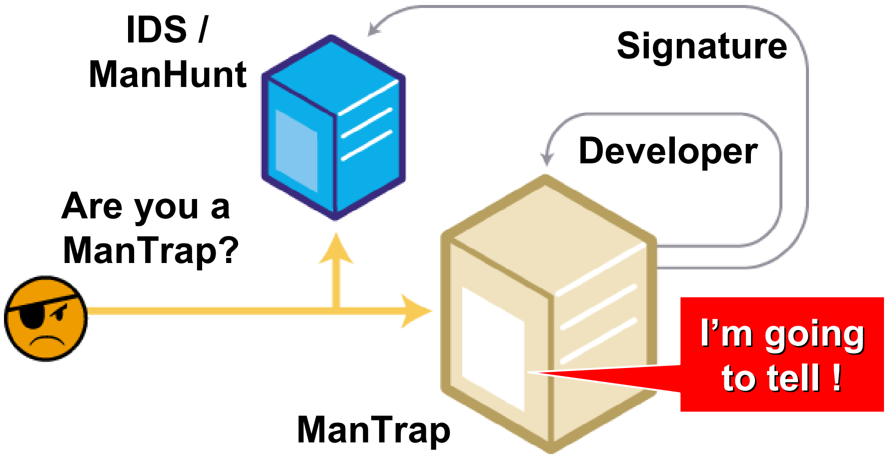
Are you a ManTrap?

NO!

Normal Host

But now I am !

ManTrap


IDS / ManHunt

Signature

Developer

Are you a ManTrap?

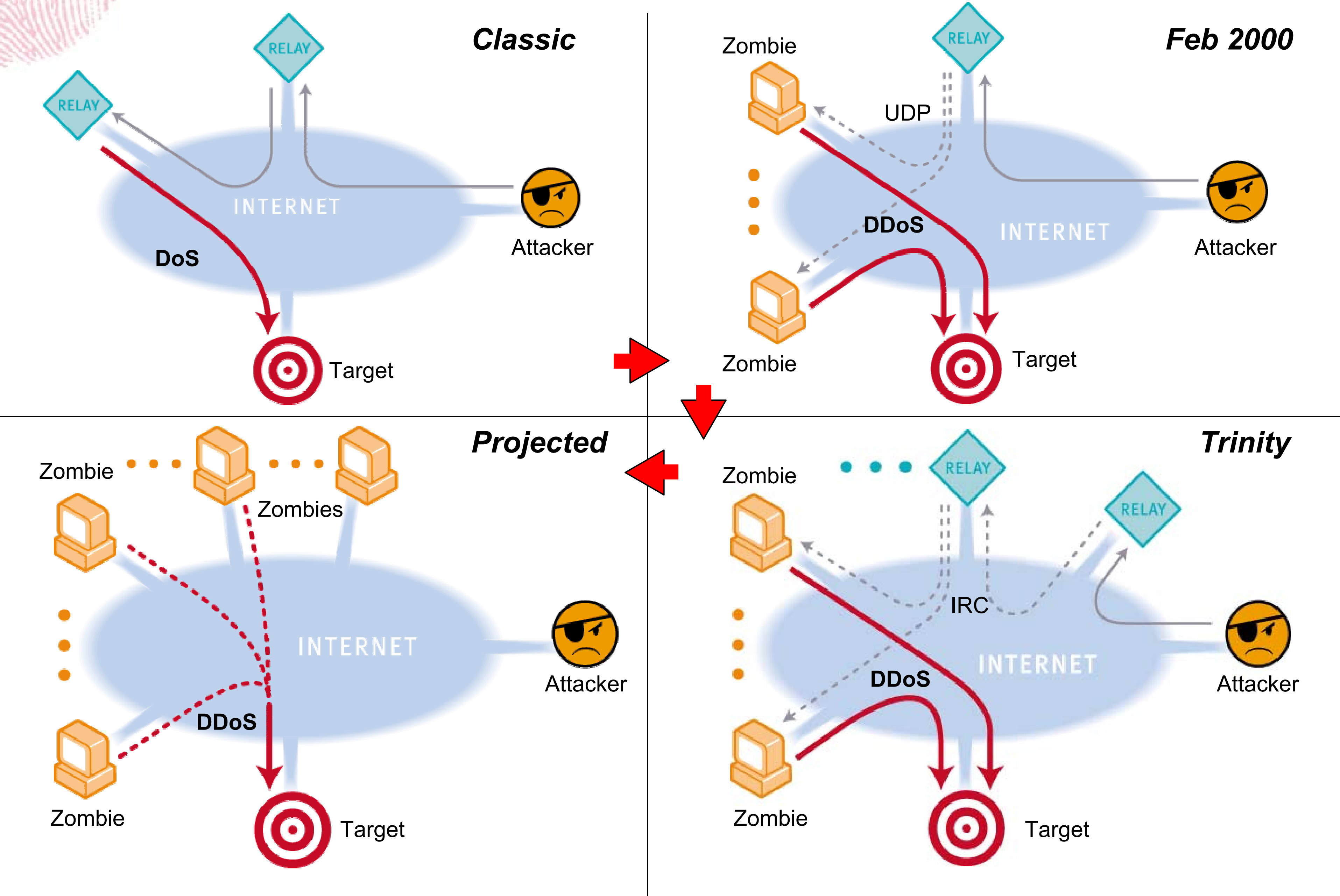
I'm going to tell !

ManTrap

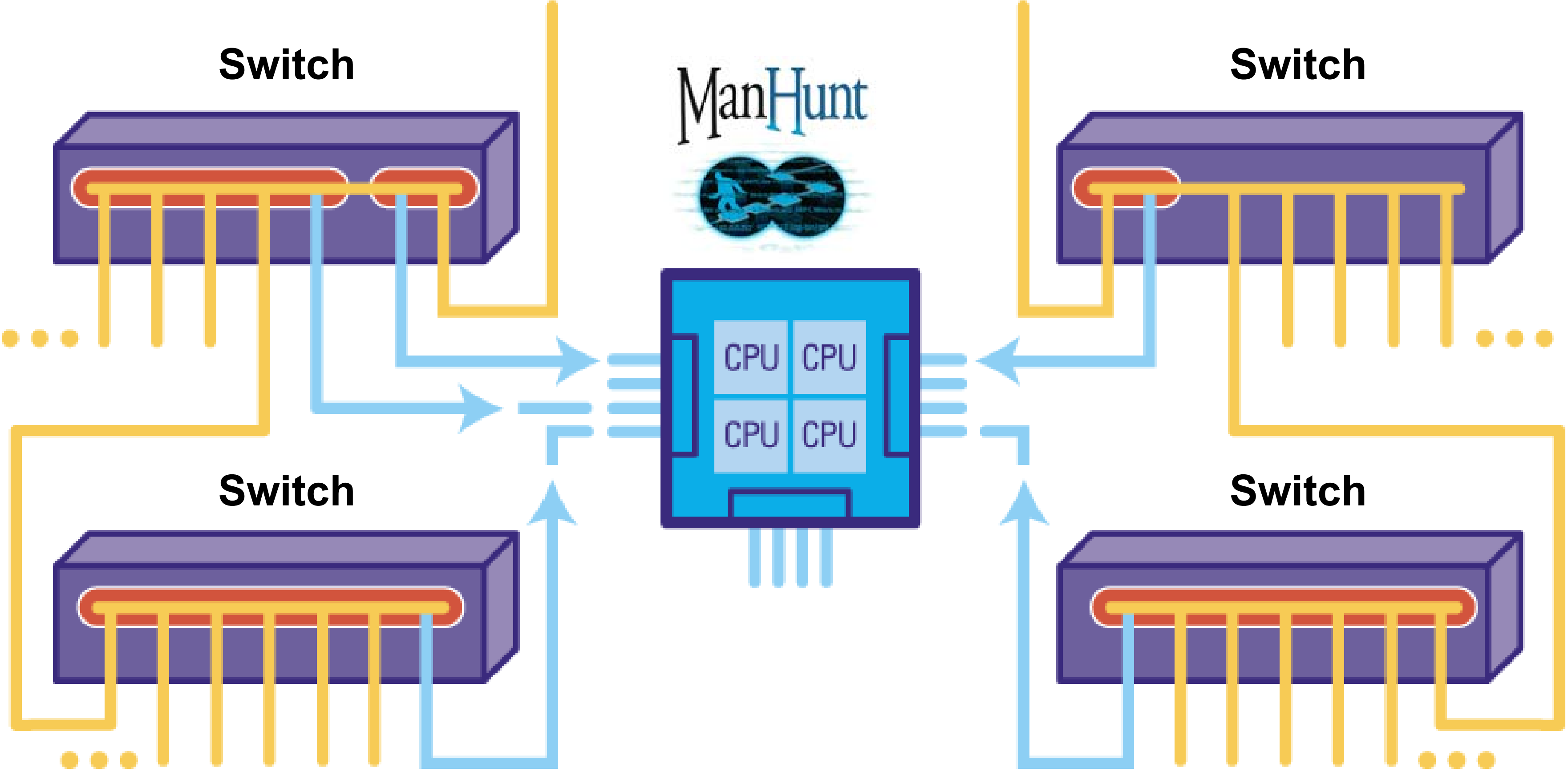
Tradeoffs for Attacker

- To test or not to test
  - detection
  - capability and intentions
- When to test
  - trackback
  - redirection
- When to react to test results

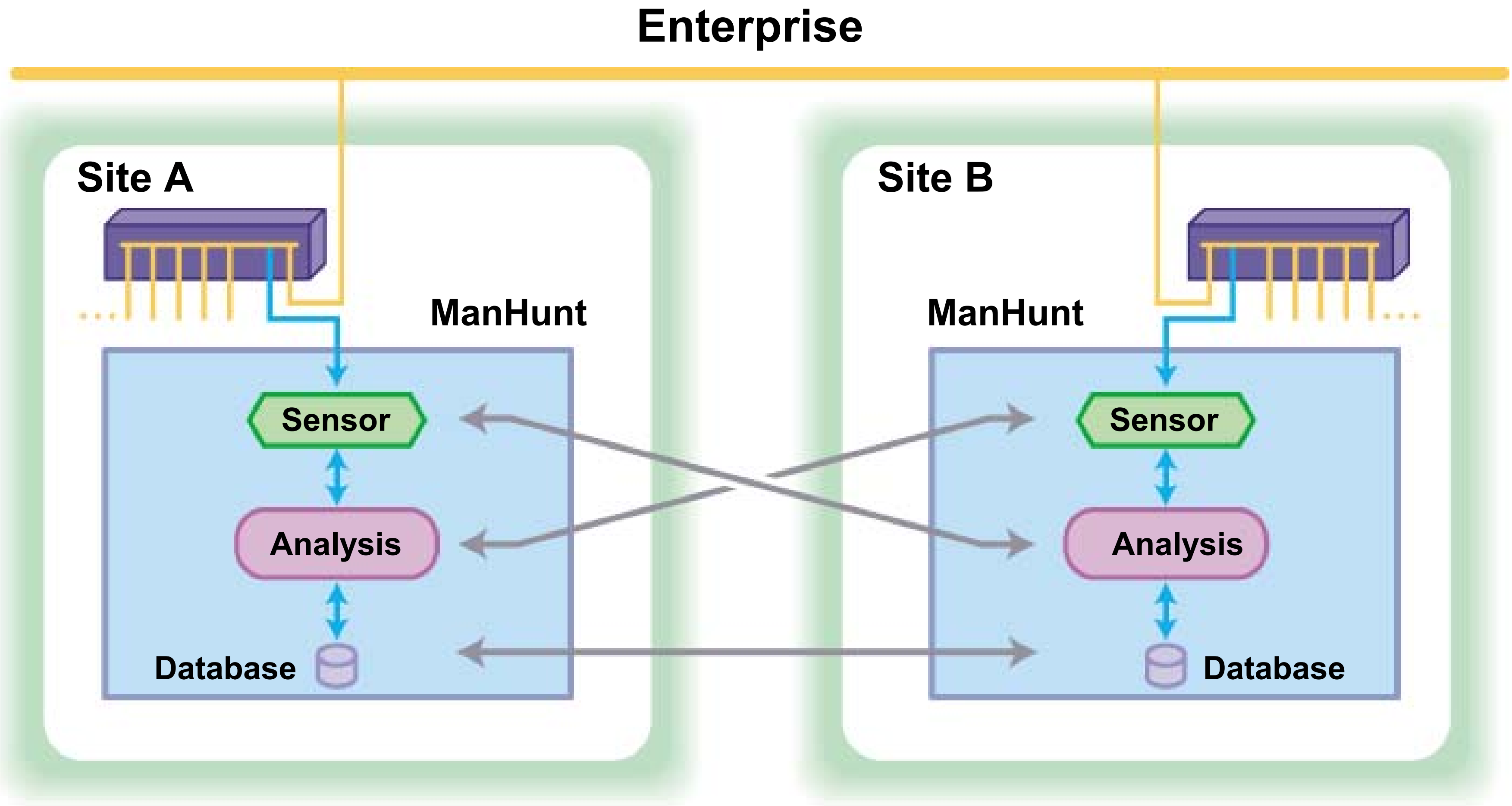
Trajectory of DDoS Technology



ManHunt: Detect and Trackback



ManHunt Cluster



Across Administrative Domains

- No presumption of shared trust
- Decouple trace and construction of chain
- Trace (trackback):
  - Edge flow (minimal info)
  - New info: traffic recognized as attack
  - No automatic backflow (except acknowledge receipt)
- Reconstruction of chain of hosts
  - Various requirements, politics: “trust is not transitive”
  - Automate selectively

Summary

- Attacks will succeed (eventually)
  - Delay onset of damage
  - Collect and disseminate intelligence (quickly)
- Automated trackback
  - Push back battleground: target ⇒ stepping stones
  - Raise chance of catching attacker
- Collective Defense
  - Create unpleasant tradeoffs for attackers
  - Raise complexity of attacks