

Organizing Large Scale Hacking Competitions

Nicholas Childers

Giovanni Vigna

Ludovico Cavedon

Manuel Egele

Lorenzo Cavallaro

Bryce Boe

Marco Cova



Outline

UC Santa Barbara

- Hacking Competitions Overview
- UCSB's iCTF
 - History
 - 2003-2007 Competitions
 - 2008 Competition
 - 2009 Competition
 - Lessons Learned
- Final Remarks

HACKING COMPETITIONS OVERVIEW

Why a hacking competition?

UC Santa Barbara

- Time constrained
- Provides hands-on security experience
- Mimics real-world scenarios
- It's fun
 - Engaging
 - Motivates students to go beyond the call of duty
 - Promotes participation

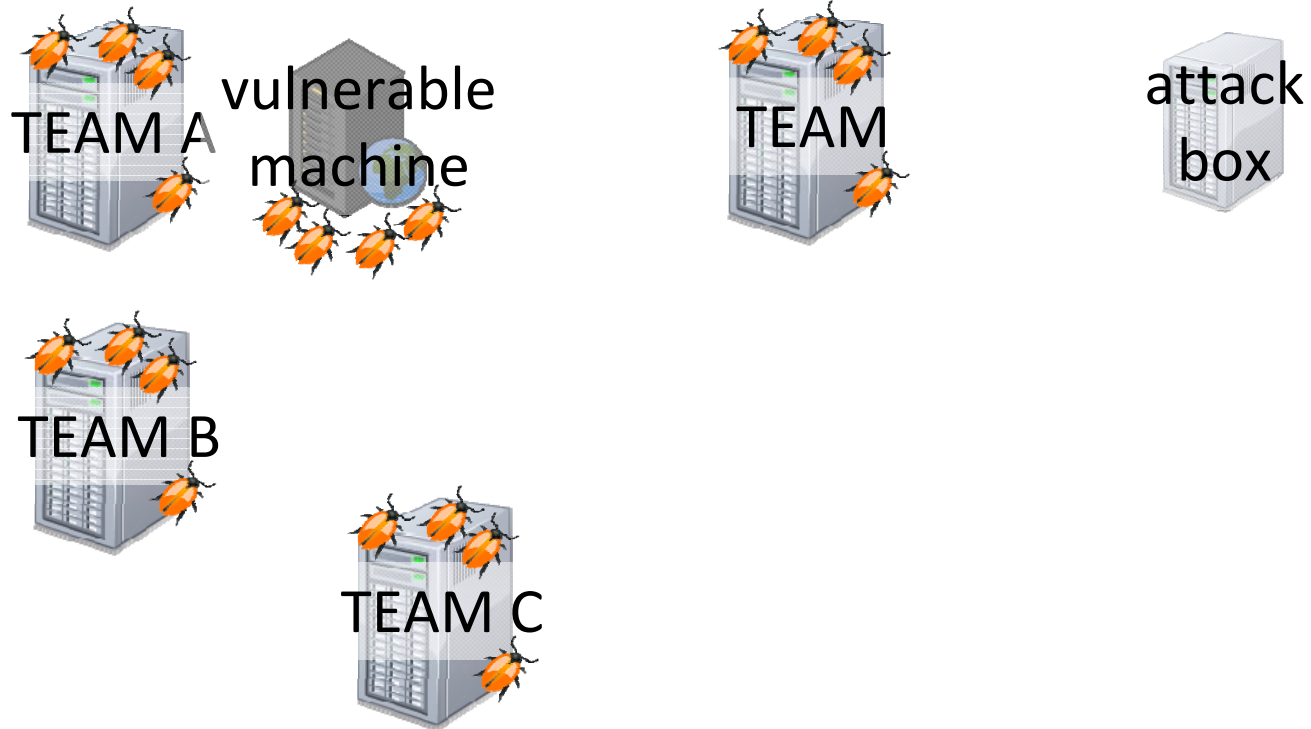
Types of hacking competitions

UC Santa Barbara

- Challenge based
 - DEFCON Quals, Codegate
- Capture the flag
 - DEFCON, **iCTF 2003-2007**, CIPHER, RuCTF

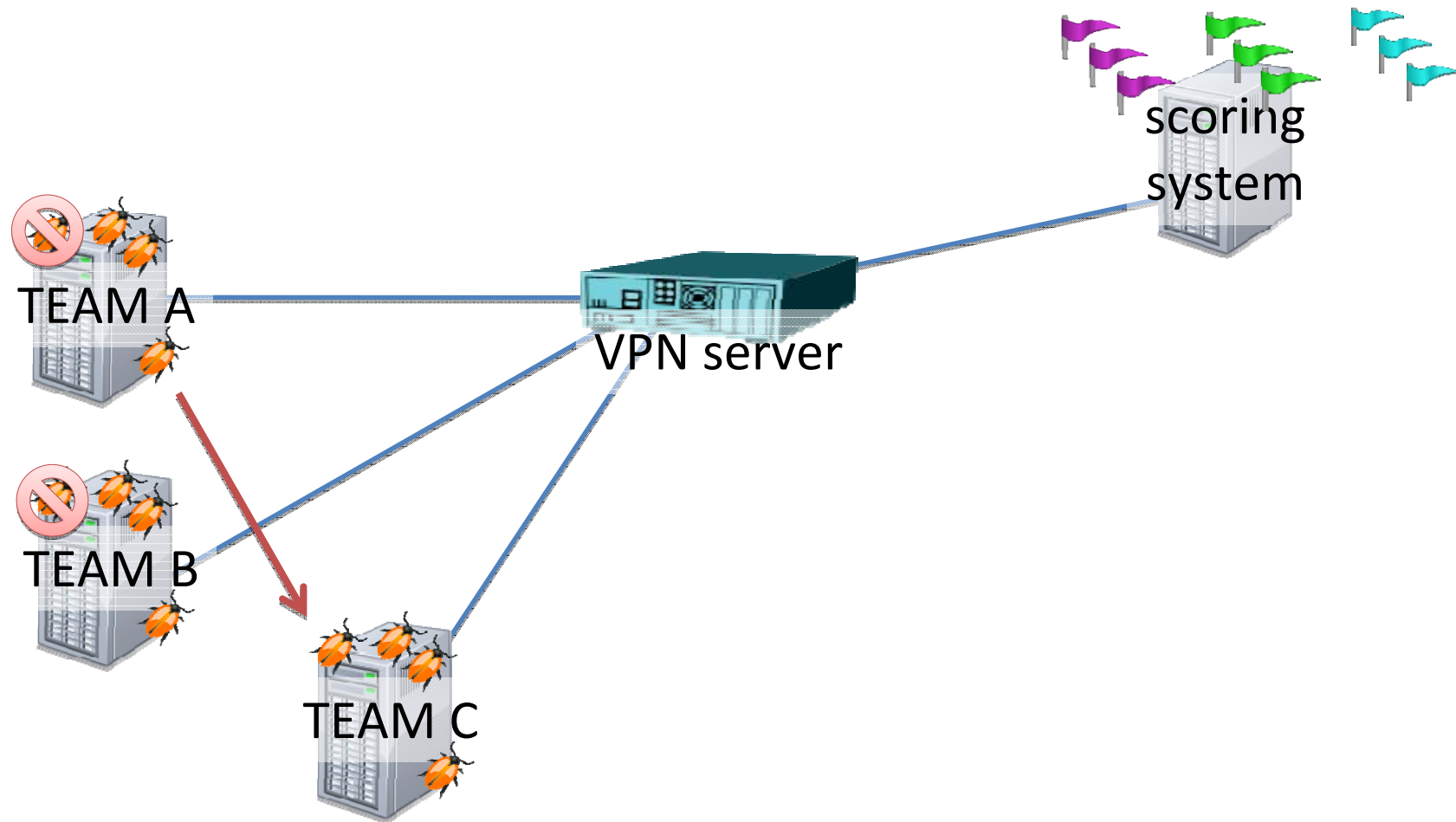
2003-2007 iCTF example

UC Santa Barbara



2003-2007 iCTF example

UC Santa Barbara



Types of hacking competitions

UC Santa Barbara

- Challenge based
 - DEFCON Quals, Codegate
- Capture the flag
 - DEFCON, **iCTF 2003-2007**, CIPHER, RuCTF
- Attack based
 - Pwn2Own, **iCTF 2008-2009**
- Defense based
 - Cyber Defense Exercise (CDX)
 - NSF Security Grand Challenge

Hosting a hacking competition

UC Santa Barbara

- Design
 - Challenging but not frustrating
 - Cater to various abilities
 - Be objectively scored
- Development
 - Allocate ample time
- Execution
 - Maintain and monitor network
 - Support remote teams
 - Limited timeframe

UCSB'S INTERNATIONAL CAPTURE THE FLAG COMPETITION

iCTF History

UC Santa Barbara

- 2003: 14 US university teams
- 2004: Addition of European teams
- 2005: Addition of more international teams
- 2006: 25 teams
- 2007: 36 teams
- 2008: 39 teams
- 2009: 56 teams

2003-2007 Competitions

UC Santa Barbara

- Traditional CTF format with side challenges
- Limited to universities
- Addition of remote teams
- Introduced traffic blending technique

Limitations

- Favored experienced teams
- No longer unique

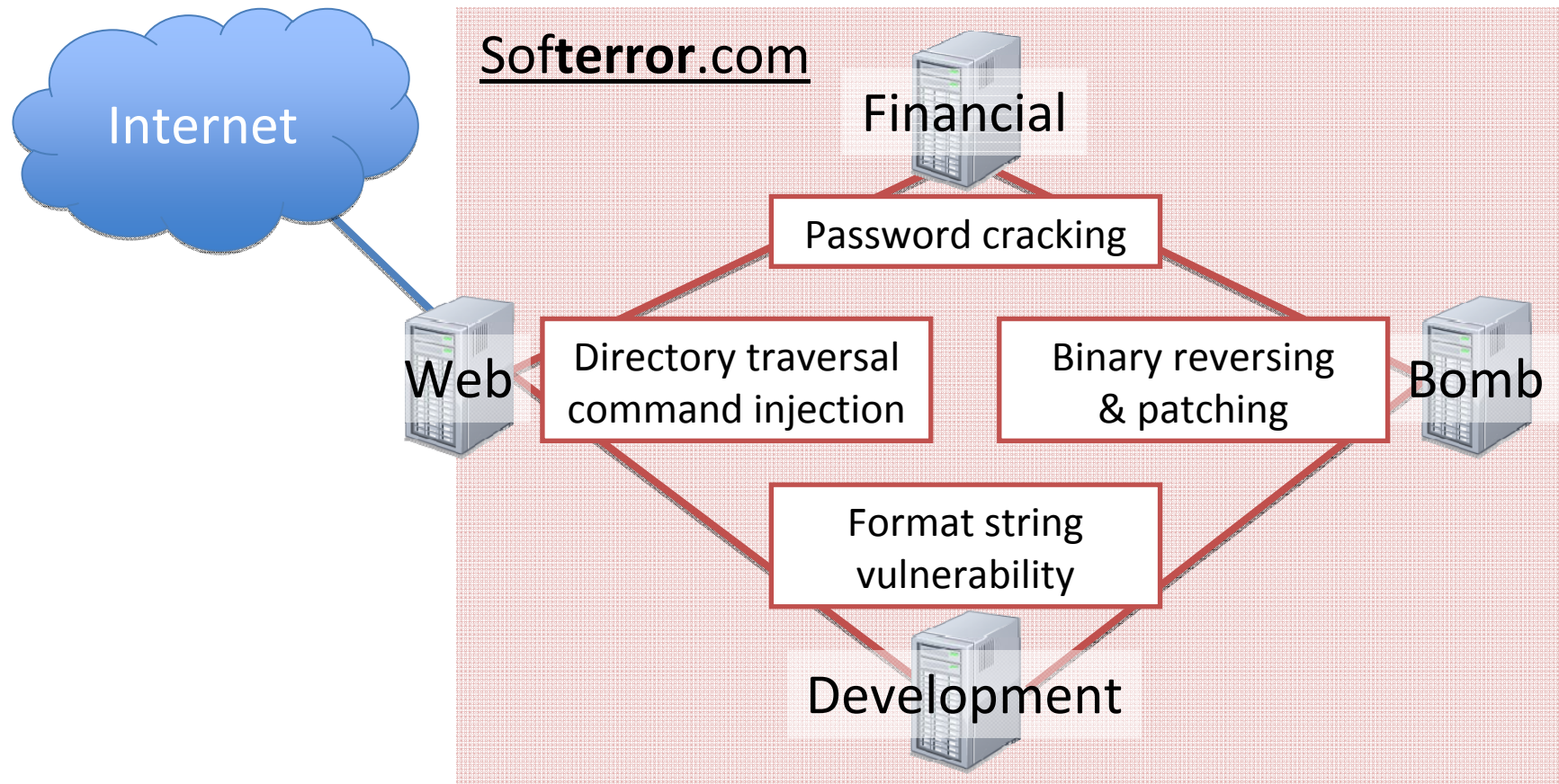
2008 iCTF

UC Santa Barbara

- Attack-based with side challenges
- Mimics a “save the world” scenario
- Goal: Defuse bomb by breaking into the **softerror.com** network

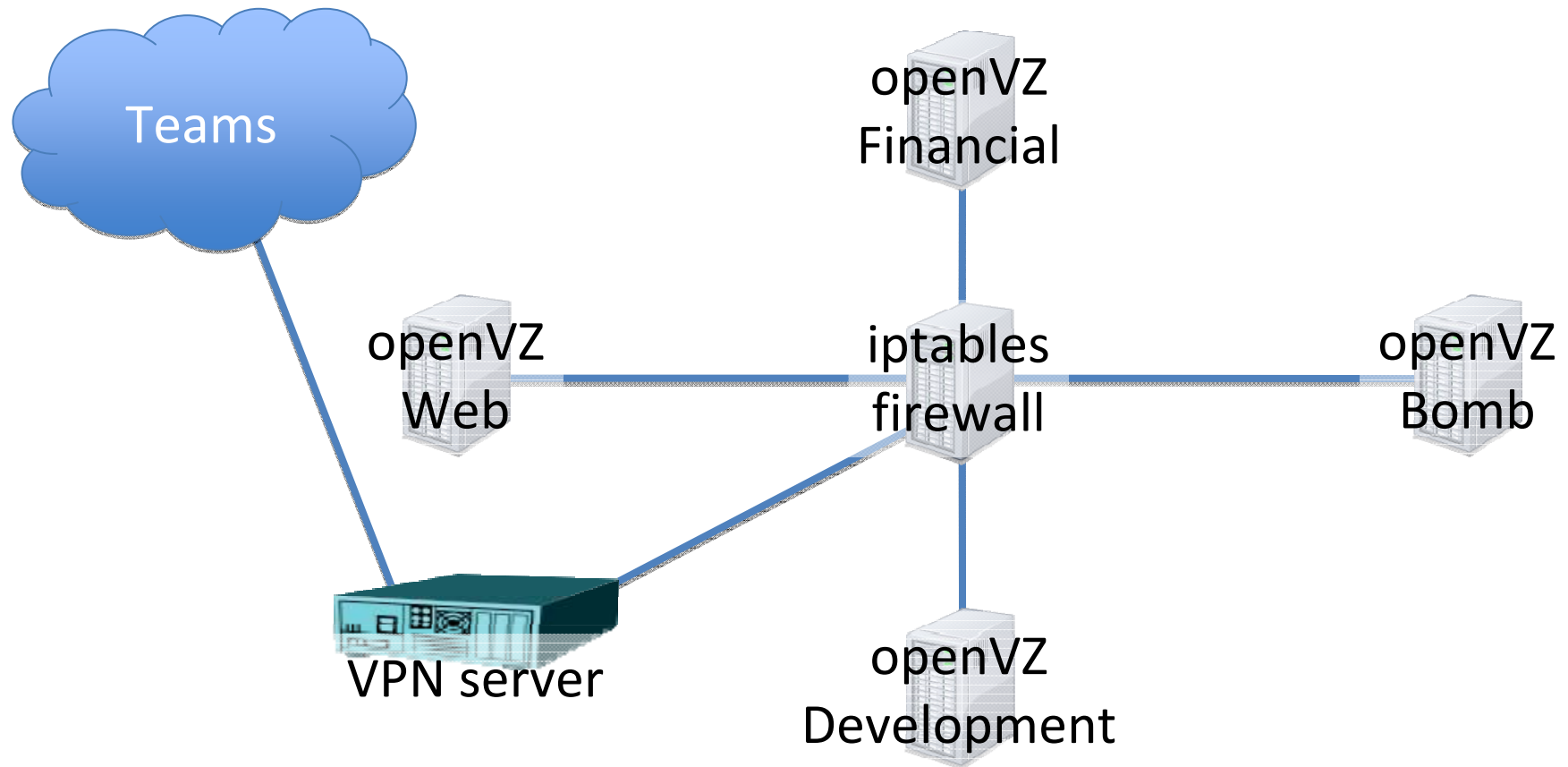
2008 Simulated Network

UC Santa Barbara



2008 Physical Network

UC Santa Barbara



2008 Dataset

UC Santa Barbara

- Snort Alerts (by team)
 - Mean: 8482
 - Max: 43254
- Pcap files
 - 5.5 GB data (3 GB compressed)
 - 34 million packets
- Useful for attack correlation research

2009 iCTF

UC Santa Barbara

- Also attack based with side challenges
- Mimics a “botnet creation” scenario
- Goal: Deliver *profitable* drive-by-downloads to simulated web users

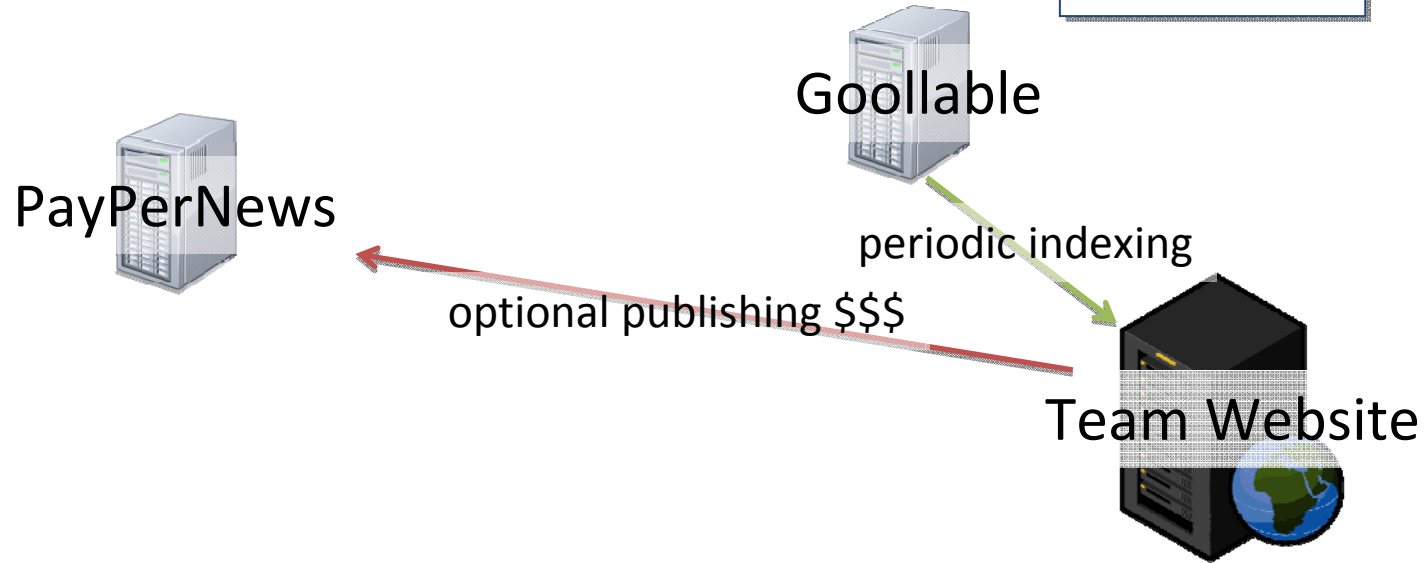
2009 Game Play

UC Santa Barbara



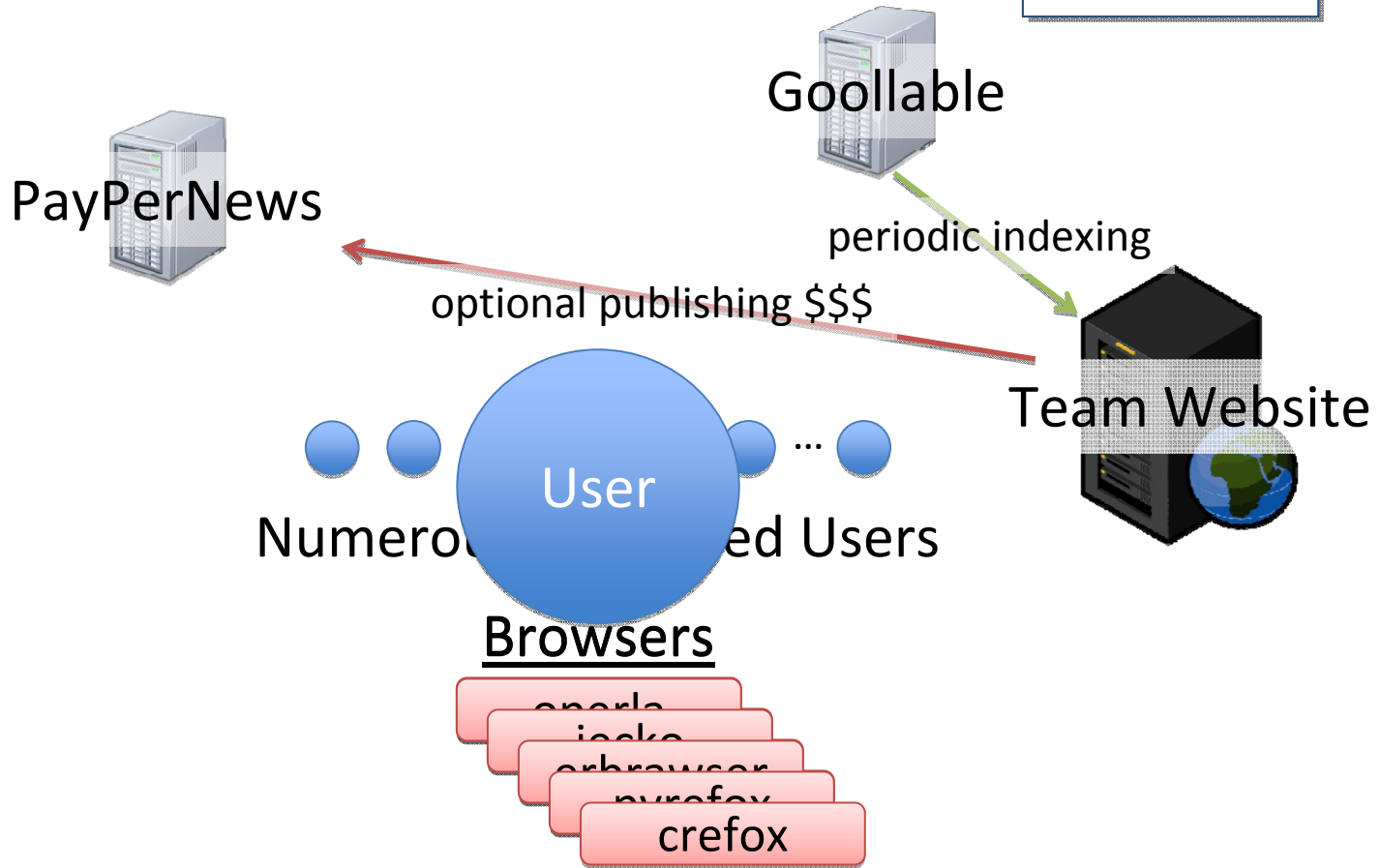
2009 Game Play

UC Santa Barbara



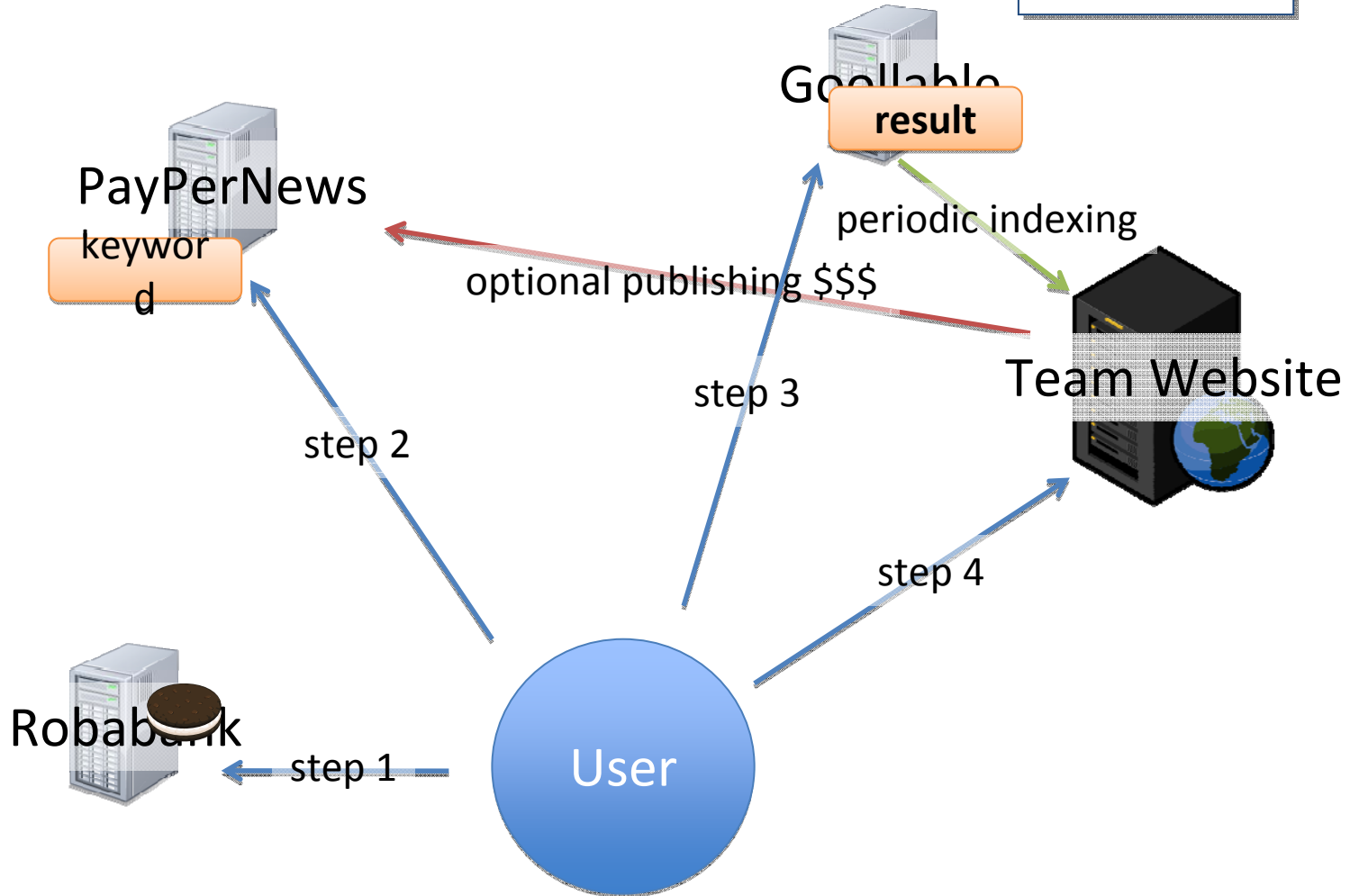
2009 Game Play

UC Santa Barbara



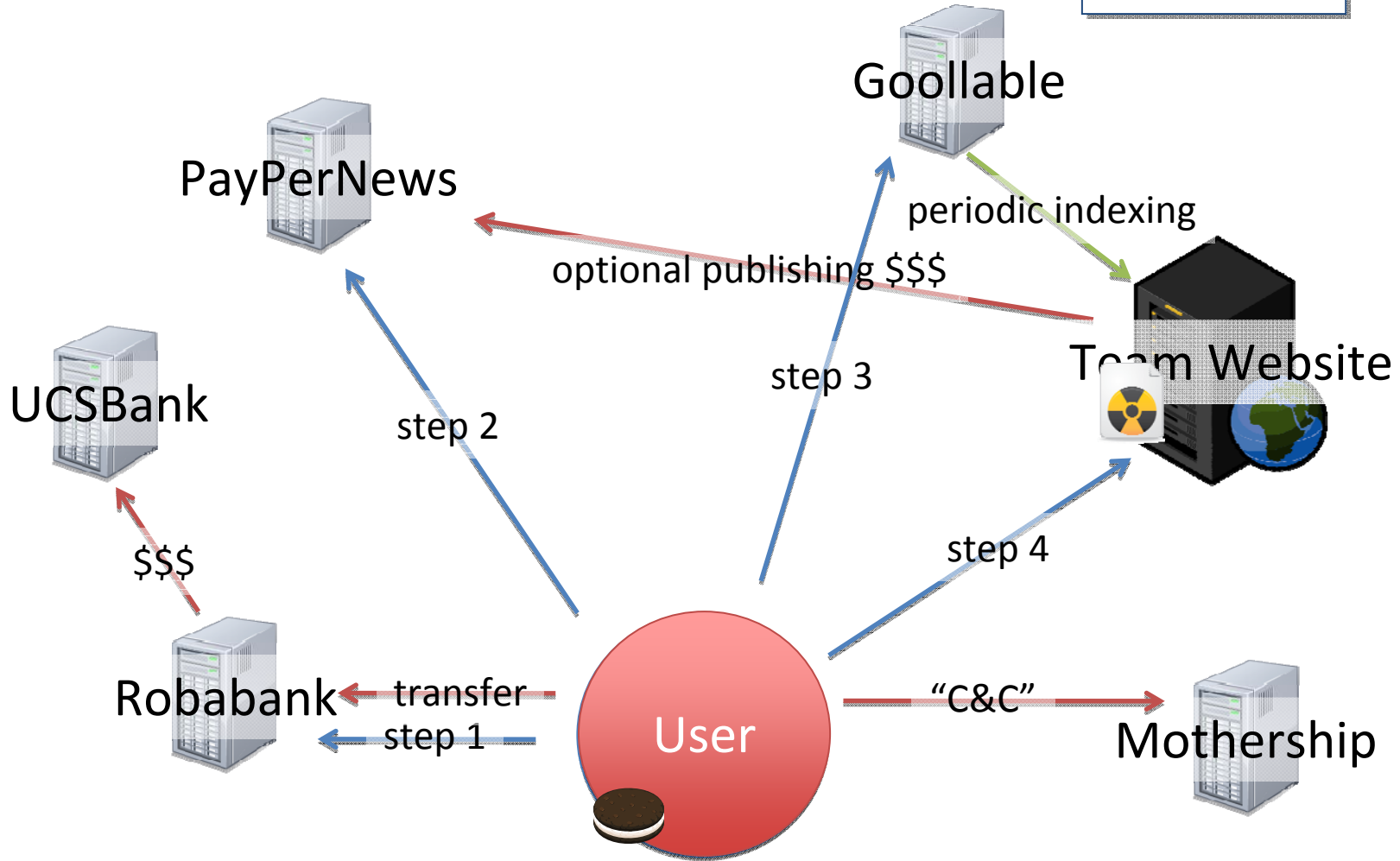
2009 Game Play

UC Santa Barbara



2009 Game Play

UC Santa Barbara



Lessons Learned

UC Santa Barbara

- KISS principle
- Budget sufficient time and resources
- Stress test competition components
- Scoring
 - Fully automated
 - Rollback and repeatable
- Attack only competitions level the playing field

Final Remarks

UC Santa Barbara

- Hacking Competitions
 - Fun and Challenging
 - Engaging
- Datasets and source from UCSB's iCTF available at <http://ictf.cs.ucsb.edu>

Questions?

UC Santa Barbara

