Cyberdefense and the Kobayashi Maru

Yiorgos Adamopoulos
Friend of OWASP
Technical Chamber of Greece
adamo@ieee.org

OWASP

Greek Chapter Meeting
2011-03-16

The OWASP Foundation
http://www.owasp.org

This is not your normal .ppt

- My grunts and bitterness about the sad state of cybersecurity thinking, cooperation and blindness in Greece
- Changing (almost) daily, like my mood
- With a little help from my friends

Has Greece been under a large scale DoS?

- TWICE!
  - Algeria Earthquake (2003)
    - Two ISPs with minimum connectivity
    - One more with “unauthorized” proxy access

2007 fires

Smaller scale incidents

- Ad-hoc group formation by sysadmins:
  - Bypassing business hierarchy
  - Bypassing business policies
  - Personal relationships save the day
- Systems must at least deliver:
  - DNS resolving
  - Mail
- Main incident response objective:
  - Stop the attack; continue service
  - Forensics later

Lessons learned

(none)

And what about other cyber attacks?

(again nothing)

A need emerges…

The critical infrastructure slowly awakes…

"Hey! Let's do a cyber exercise!"

"I want in!"

"Me too!"

2 NATO and 1 Greek Cyberdefense exercises after

Did we win?

The problem of the medium

- Cyberdefense exercises suffer from the reliance on the fact that the network players communicate on operates normally
- Complaints about communication:
  - VPN connectivity and speed
  - Forum / IR software and usability

Parkinson's Law of Triviality

"You can get approval for building a multi-millon dollar atomic power plant, but if you want to build a bike-shed, you will be tangled up in endless discussions"

This presentation suffers from Parkinson's Law too

Understand this

Communication problems during the exercise are a **blessing** in disguise.

- Extra pressure
- Thinking out of the box
- Improvise
- Innovate

The message must be delivered

"Neither snow nor rain nor heat nor gloom of night stays these couriers from their swift completion of their appointed rounds"

- We do not give up!
  - The incident must be dealt with

"*You are setting the bar too high!"*

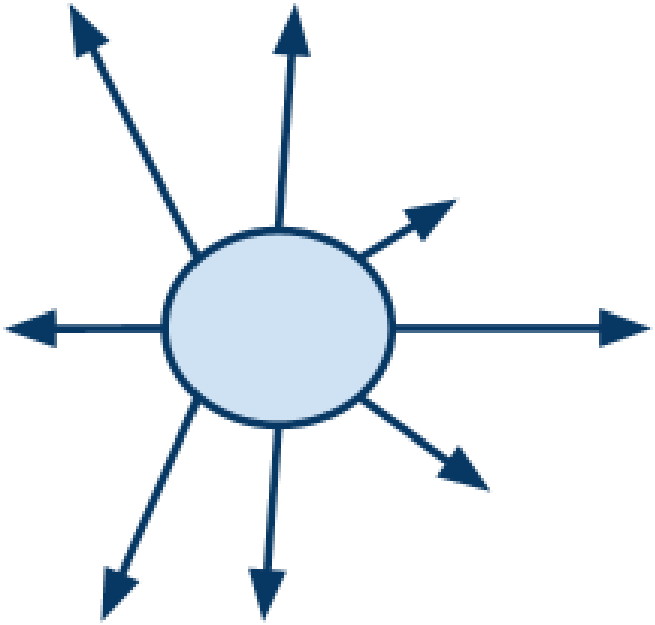
NO!

You are setting it too low

The real problem

- Team Formation (Tuckman)
  - Forming
  - Storming
    - Objection to team formation
  - Norming
    - Working together
  - Performing
    - Project delivery

The real problem #2



Everybody claims space, role and audience

Is there any hope?

- The question is wrong!
- Trusted group formation is the key
- Groups are formed by people
  - Organizations rarely understand this

Organizing Cyber-defense (and –offense)

Form of Organization	Mutual Association	Mutual Participation	Division of Labor	Extended Organization
Loners	No	No	No	No
Colleagues	Yes	No	No	No
Peers	Yes	Yes	No	No
Mobs	Yes	Yes	Yes	No
Formal Organizations	Yes	Yes	Yes	Yes

Source: Organizing Deviance, Best & Luckenbill

Thank you!

- Yiorgos Adamopoulos
- adamo@ieee.org
- @hakmem
- http://blog.postmaster.gr
- http://gr.linkedin.com/in/yiorgos