



AbOSE Report

(**A**bilene **O**perational **S**ecurity **E**xercise)

T. Charles Yun, Internet2

Presentation Overview



- A bit of scene setting and background
- Background, Goals
- Methodology
- Findings
- Lessons Learned
- Follow up
- Invitation to International Security Exercise
- Contact Info

Background Information

Abilene Network Backbone



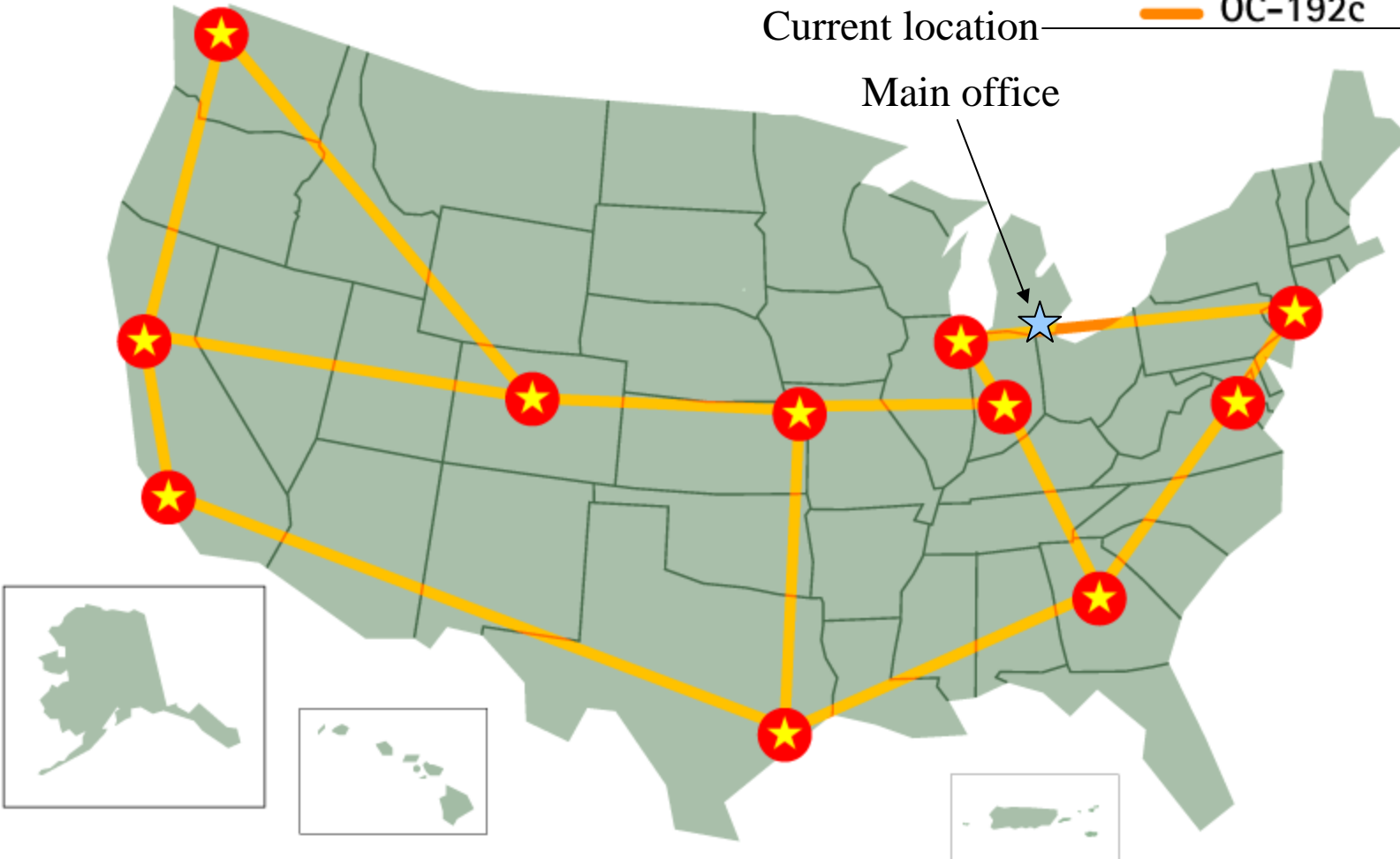
Logo

-  Core Node
-  OC-192c

2006 January

Current location

Main office



TF-CSIRT, Amsterdam, the Netherlands

Slide 3

Salsa (1 of 2)



2006 January

- Advisory and coordination group for security activities for Internet2
 - Security at Line Speed workshop (S@LS), the “fruitcake” document, annual meetings
- Working Groups and meetings
 - Network Authorization (NetAuth), Federated Wireless Network Authentication (FWNA), Computer Security Incident (CSI2)
 - Reconnections “Managing Academic Networks With New Requirements”, NetGurus

TF-CSIRT, Amsterdam, the Netherlands

Salsa (2 of 2)

- Address security in various ways:
 - Time frames: short, medium, long
 - Process, procedure, policy (think ISO-9000, legal requirements, etc.)
 - Groups: community, Community, COMMUNITY
 - Operational, exploratory, R&D

AbOSE

- One day long event, held November 2005 in Indianapolis, Indiana, USA
- Designed to initiate conversations on the Network Operation Center's (NOC) activities in their support of Abilene
- This was not an audit
 - Information gathering, **gap analysis**, baseline, document
- Report is currently in draft and has been released to participants, public version soon.

Methodology

- Two scenarios, invented, refined, executed
- “Table top” exercise (talking, no flows initiated)
- DDoS attack
 - Backbone link is inconsistently saturated between two core router nodes
 - Targeting an important demo
- Router compromise with press/reporter investigation
 - Router provides indication of problem and reporter has been contacted by “bad guy” to advertise the compromise

Findings

- Report identifies ~40 observations with suggested responses
- Patterns of activity emerged in the two scenarios, some expected and others not.
- Some processes were in place and followed, others need to be developed, noting that the any new process is hinged on the NOC's return on investment
- Some observations revealed policy questions that should be answered by Internet2, or, the NOC's response is based on other people's decisions.

Lessons Learned (some of them)

- Well designed, **detailed** scenarios are important to respond to unexpected questions.
- Engineers (plural) need to be involved in the design ***and*** execution of the scenario. (Obviously, these engineers will not participate in the exercise.)
- Make sure that every external “event” or “character” is represented by a real person. If someone is supposedly upset and sending email, have a real person start sending email... and then call a person’s cell phone.
- Test processes, not the cleverness of engineers.

Follow Up

- Initiate regularly occurring Abilene exercise
 - Planning to hold annually, during the summer holidays
 - Potentially run a table-top **and *live*** exercise
- “Regular” exercises with international partners
 - What is the proper format of an international exercise? Process analysis or “real problems”
 - Start off with a similar baseline exercise and evolve into more complicated activities

Invitation to Intl Security Exercise



- Which entities should participate (regional, national, backbone, or collaborative organizations)?
- Who should organize?
- When: I suggest late summer 2006
- Format: Baseline assessment, similar to the AbOSE reported here. Probably a distributed event, via video+voice+IM (or in Hawaii/Sicily/Provence)
- Goals: Some are obvious, additional thoughts?

2006 January

TF-CSIRT, Amsterdam, the Netherlands

Slide 11

Contact Info

- T. Charles Yun
Internet2
charles @ internet2 . edu
734.352.4960 (desk)
Ann Arbor, Michigan, USA
- <http://security.internet2.edu/>