Network Situational Awareness for Municipal Government

Timothy J. Shimeall, Ph.D.

(With thanks to Sid Faber, Alex Musicante)

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

Overview

The City: Pittsburgh PA

The Network

Flow Collection for Situational Awareness

Results

Conclusions

The City: Pittsburgh PA

Historical:

- George Washington
- John Chapman
- Louis & Clark
- Mike Fink
- Stephen Foster
- Andrew Carnegie
- Richard Mellon
- Jonas Salk
- Andy Warhol
- Fred Rogers
- Herbert Simon
- And many more…

3 major universities
Major medical system
Pittsburgh Steelers, Penguins, Pirates

Vibrant multigenerational social structure

Diverse population:
- 1.2 Million (2010, Allegheny County)

Modern budget issues

The City: Information Systems

City CIO (currently acting CIO)

2 full-time network security staff (others as-needed)

"City Information Systems plans, acquires, installs, and supports the City's proprietary and open computing environments, including personal and mobile computers. CIS also develops software programs for Public Safety, Finance and other departmental initiatives, provides network services, develops and maintains the official City website, and trains City employees in Microsoft Office applications."

The Network

city.pittsburgh.pa.us

205.141.128.0/18

Diverse mission space:

- Operations (Governance, HR, Payroll, Purchasing, …)
- Police, Fire, Ambulance, Courts
- Tax collection, Property assessment, Building inspection
- Park & recreation, Event planning
- Housing, Water & Sewer, Public Works
- City planning, Urban redevelopment

Network Situation Awareness

"Telling the CIO what is needed to know"

Pre-existing

- Firewalls
- Network IDS
- Host-based controls

Motivation

- G20 summit (& protests)
- Legal requirements
- University of Pittsburgh bomb threats
- Proactive security

Flow Collection for Network Situational Awareness

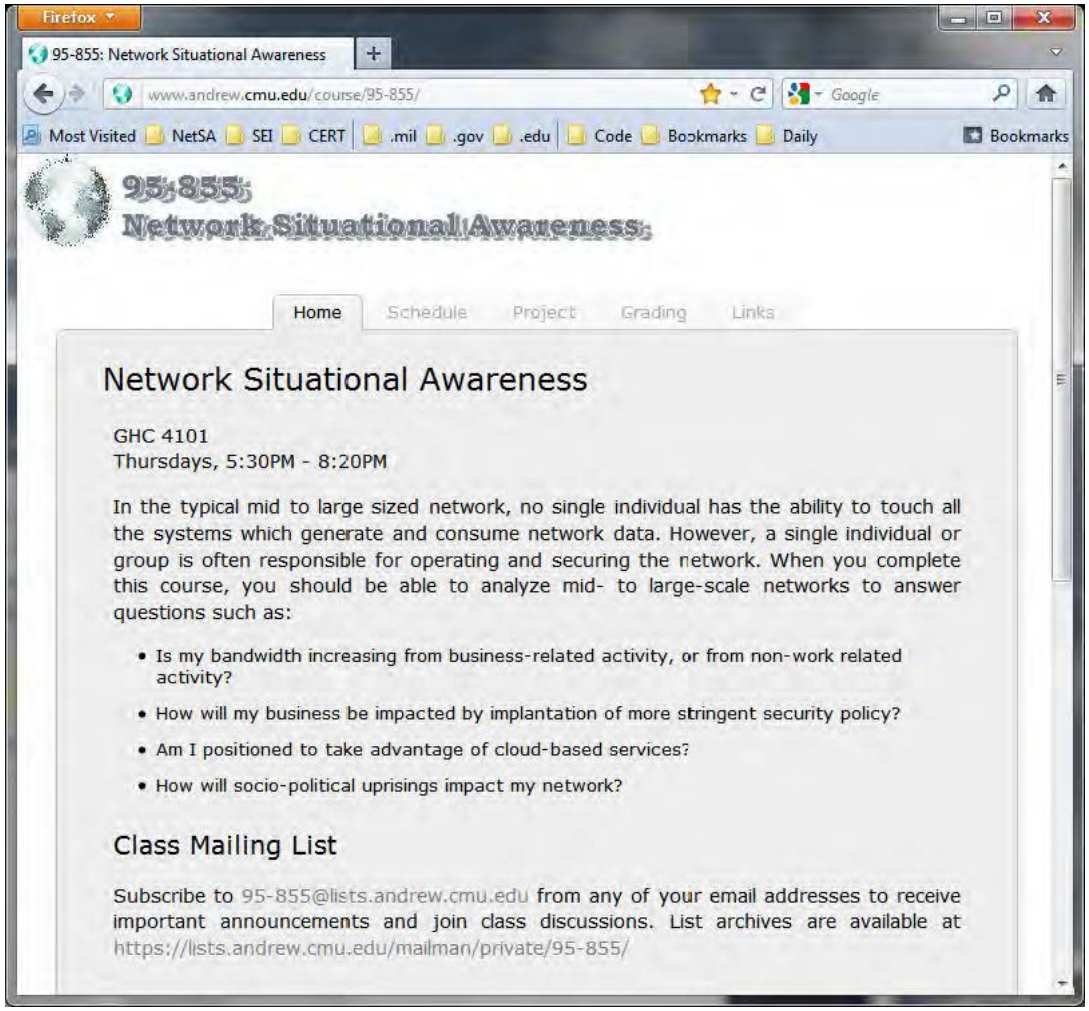
http://www.andrew.cmu.edu/course/95-855/

Instructors:

- Tim Shimeall*
- Sid Faber

Access to city network flow data

- Initiated with CIO
- Reviewed by legal
- Sensor at primary ISP outside firewall
- Volunteers



Flow Analysis

Gain network situational awareness

Provide feedback to city

Done in the blind

Follow-on investigation by CIS staff

Process:

- Find large traffic producers and consumers
- Create profile
- Eliminate bogons
- Monitor over time
- Explore deviations

Discussions

ACL/ Least privilege

DNS

Remote access

Streaming video

Results

Scans

Client web, Served Web

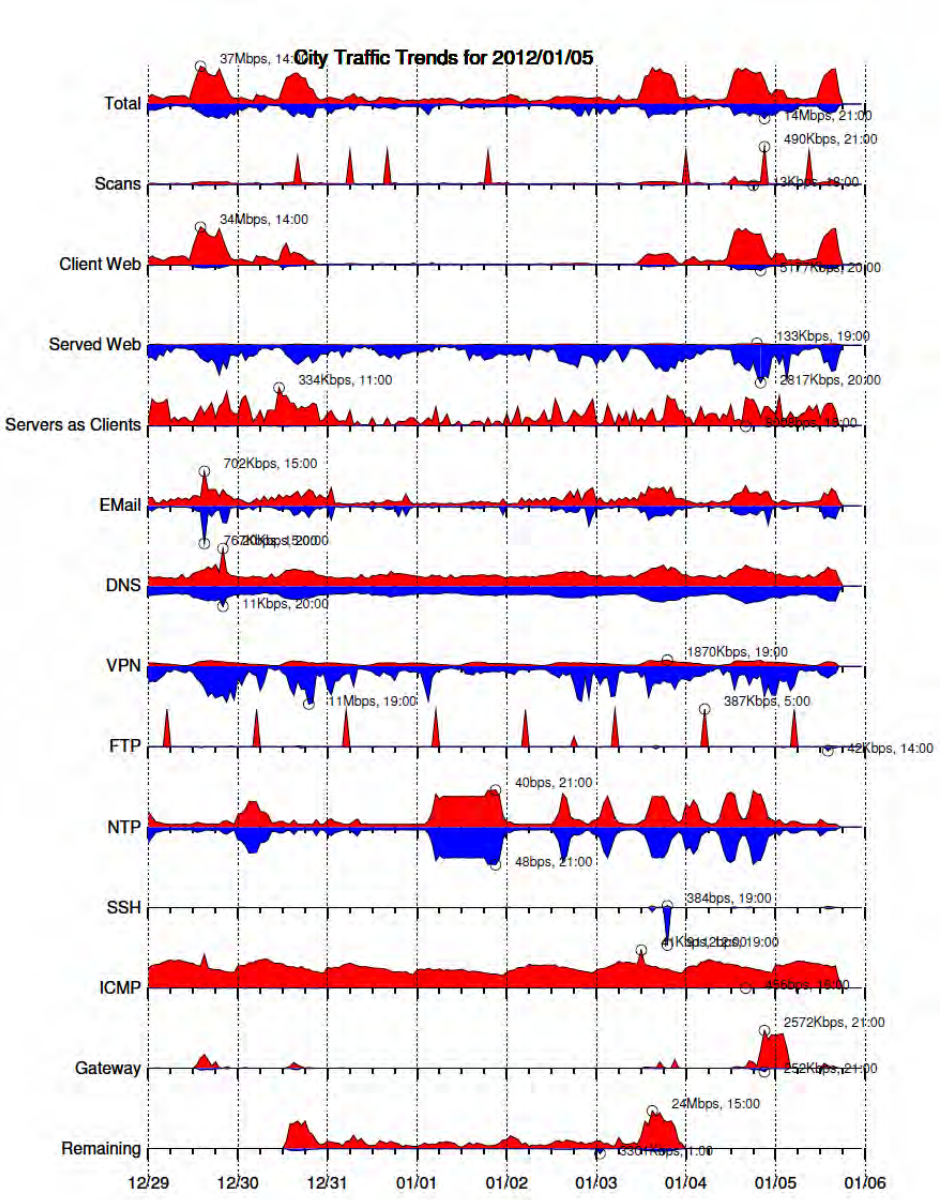
Servers as Clients

Email

DNS

NTP

etc.



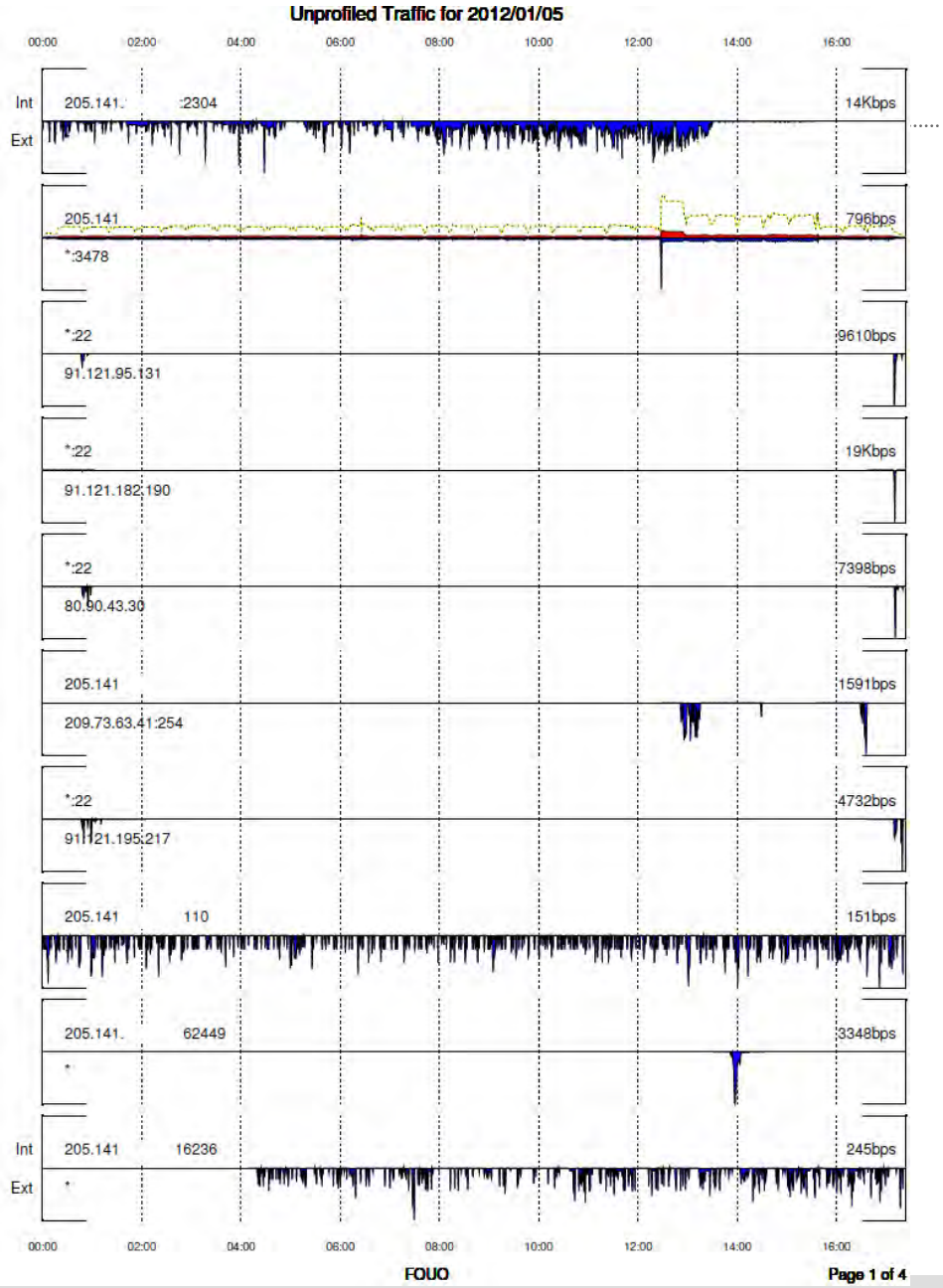
Follow-on

Monitoring

Detection/follow-up

Context for security planning

Further collaboration



Conclusions

Low investment / High value add

Not high-expertise analysis

Controlled additional exposure

Significant risks addressed