CERT

Network Flow Analysis in Information Security Strategy

Timothy J. Shimeall, Ph.D.

Situational Awareness Team

January, 2015

This material is based upon work funded and supported by FloCon cost recovery Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL 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.

DM-0001942

Outline

Security strategies against malefactors

Analytics supporting

- Deception
- Frustration
- Resistance
- Recognition/Recovery

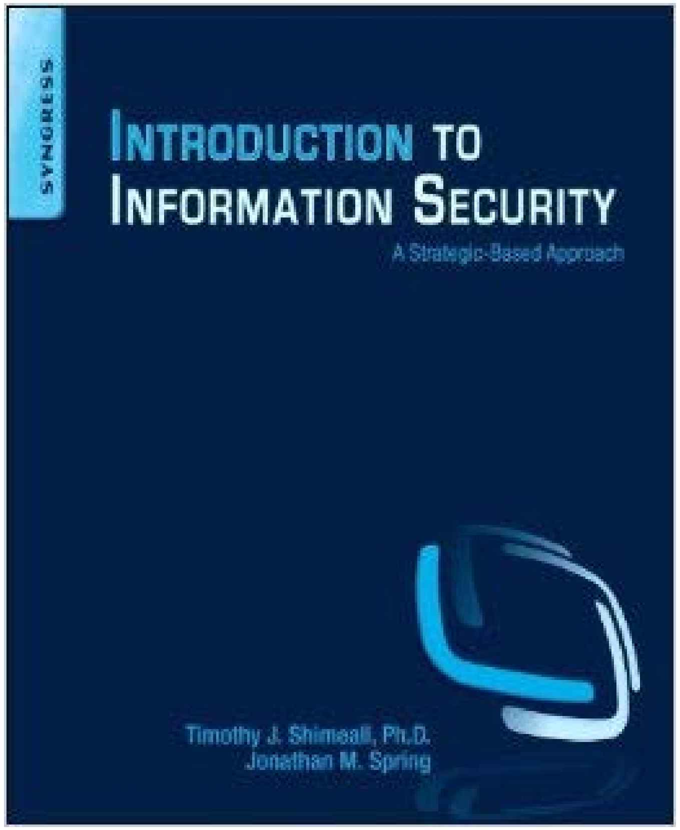
Recapitulation

Security Strategies

Author (with J. Spring) of a Information Security textbook built around security strategies

- Deception
- Frustration
- Resistance
- Recognition/Recovery

This book is the primary reference for this presentation, although flow analysis is profiled only in the recognition/recovery section


SYNGRESS
INTRODUCTION TO INFORMATION SECURITY
A Strategic-Based Approach
Timothy J. Shimeall, Ph.D.
Jonathan M. Spring

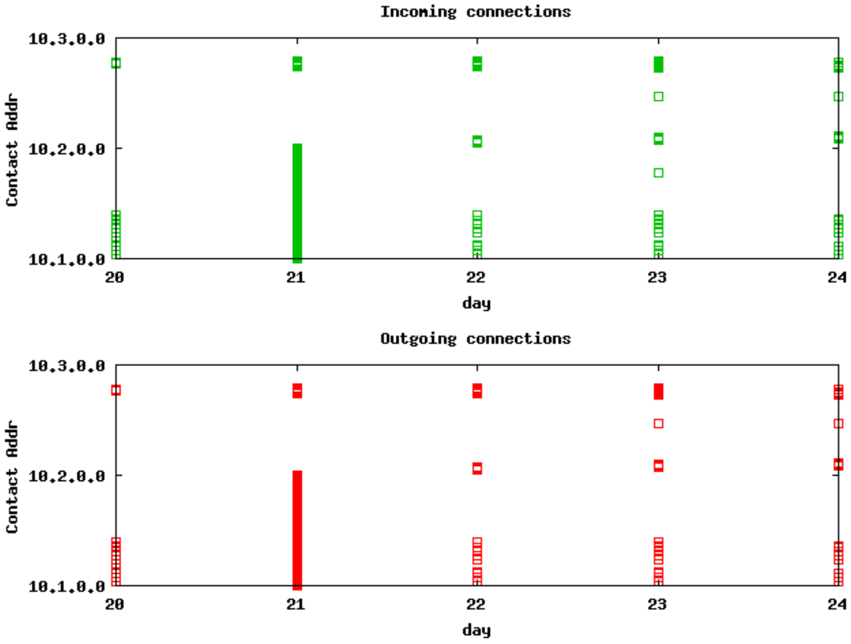
Analytics Supporting Deception

Make deceptive hosts act like production hosts

Traffic baselines
(Jones/Whisnant 2012 tutorial)

Contact sets

- Build IP sets incoming/outgoing over time per interesting host
- Profile / graph



Contact patterns

- Identify interesting contact sequences
- Count over time per interesting host

Contact Set Generation

```
rwfilter Selection --type=in,inweb \
   --dipset=my-net.set \
   --not-sipset=ignore.set --pass=stdout \
  | rwstats --fields=dip --values=records \
    --count=threshold --top \
  | tail -n +4 | cut -f1 -d\| \
  | rwsetbuild - active.set

for day in list; do
  rwfilter selection($day) --type=out,outweb \
     --sipset=active.set \
     --not-dipset=ignore.set \
     --pass=stdout \
  | rwset dip=stdout \
  | rwsetcat - --integer-ips >contact-$day.txt
done
```

Analytics Supporting Frustration

Block initial intrusion into network

Attack surface estimation

- Extract common services accessed externally and provisioned internally by the network
- Identify rate of service and commonly-accessing hosts
- Identify network blocks serving as communication partners
- Profile time-based patterns of activity

Vulnerability estimation

- Extract common services accessed externally and provisioned internally
- Identify traffic signatures for relevant vulnerabilities on these services
- Profile activity for hosts involved in traffic matching these signatures

Attack surface: http://www.cs.cmu.edu/~pratyus/as.html

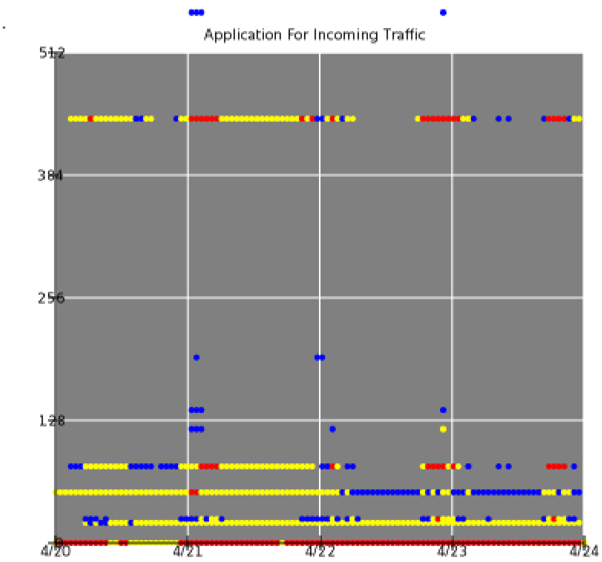
Vulnerability estimation:Igor Kotenko and Mikhail Stepashkin. “Attack Graph Based Evaluation of Network Security”. 10th IFIP TC-6,TC-11 International Conference, CMS 2006. Heraklion, Crete, Greece. October 2006. pp. 216-227.

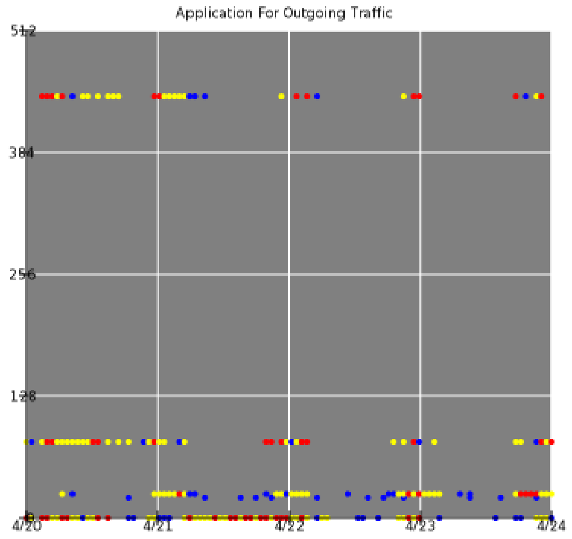
Attack Surface Estimation

```
rwfilter Selection  --type=in,inweb\
   Partition --pass=stdout \
  | rwfilter stdin \
   --python-exp="rec.sport>rec.dport" \
   --pass=stdout \
  | rwstats --fields=dport,protocol \
   --values=records --top --count=Threshold1 \
  | tail -n +3 | cut -f1,2 -d\| >tmp-itpl.txt

rwfilter --type=in,inweb Selection \
   Partition --tuple-file=tmp-itpl.txt \
   --pass=stdout \
  | rwbag --dip-flows=tm-in.bag

rwbagtool --mincount=Threshold2 tmp-in.bag \
--coverset --out=surf-in.set
```

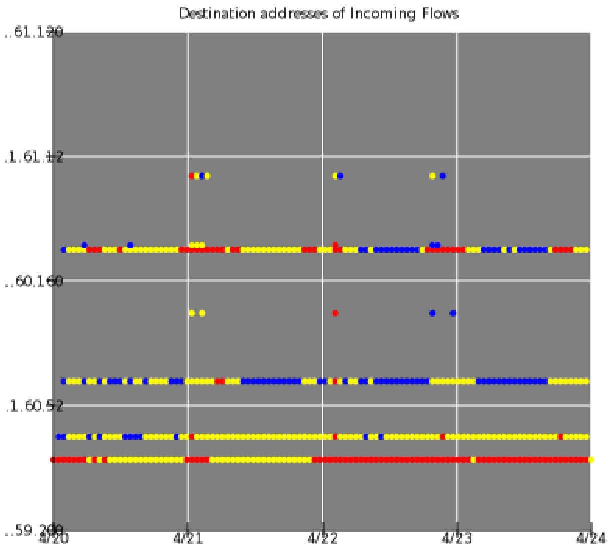
Attack Surface: Existence Plots

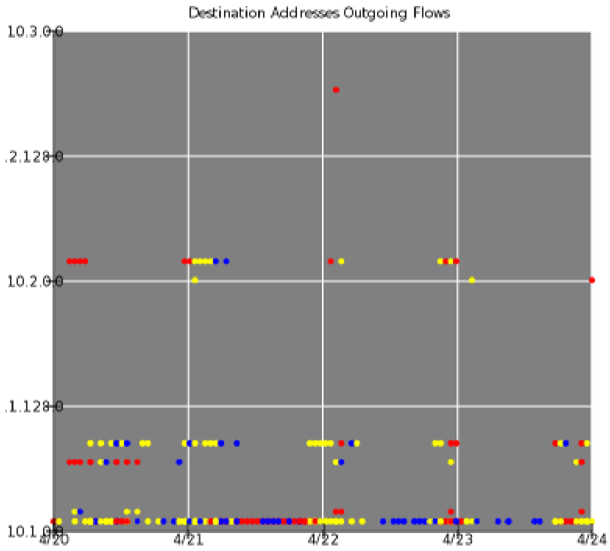
Applications: Incoming and Outgoing





External Addresses: Incoming and Outgoing





Analytics Supporting Resistance

Support controls to prevent or slow propagation or escalation

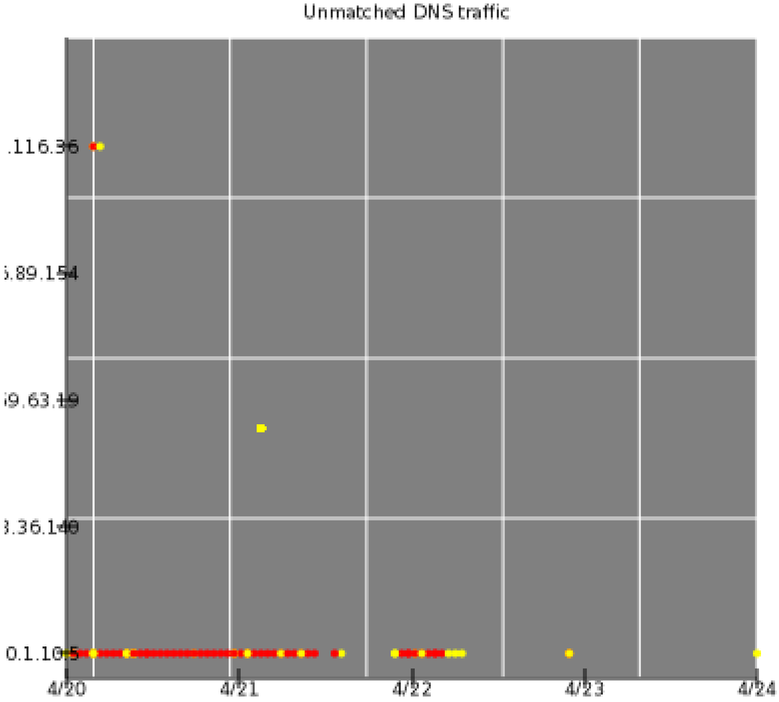
Flow signatures (Jones/Shimeall, FloCon 2014)

- DNS responses without prior requests
- DNS responses from non-authoritative source
- Email or Web contacts to addresses associated with DNS source

Anomaly analysis

- Residuals on stripplot graphics
- Departures from normal volumes on known services

Beacon detection



DNS responses without requests plotted by source

Analytics Supporting Recognition/Recovery

Find malicious activity quickly, prioritize recovery efforts

(Covered well by many previous FloCon presentations)

Host monitoring

Service monitoring

Attack profiling

Beacon detection

Data exfiltration

Combined Analytics

Analytics may be shared across strategies

- Network profiling supports both deception and recognition/recovery
- Many recognition/recovery analytics may support frustration and resistance
- Some analytics may support frustration (focused externally, configuration) and resistance (focused internally, active hardening)

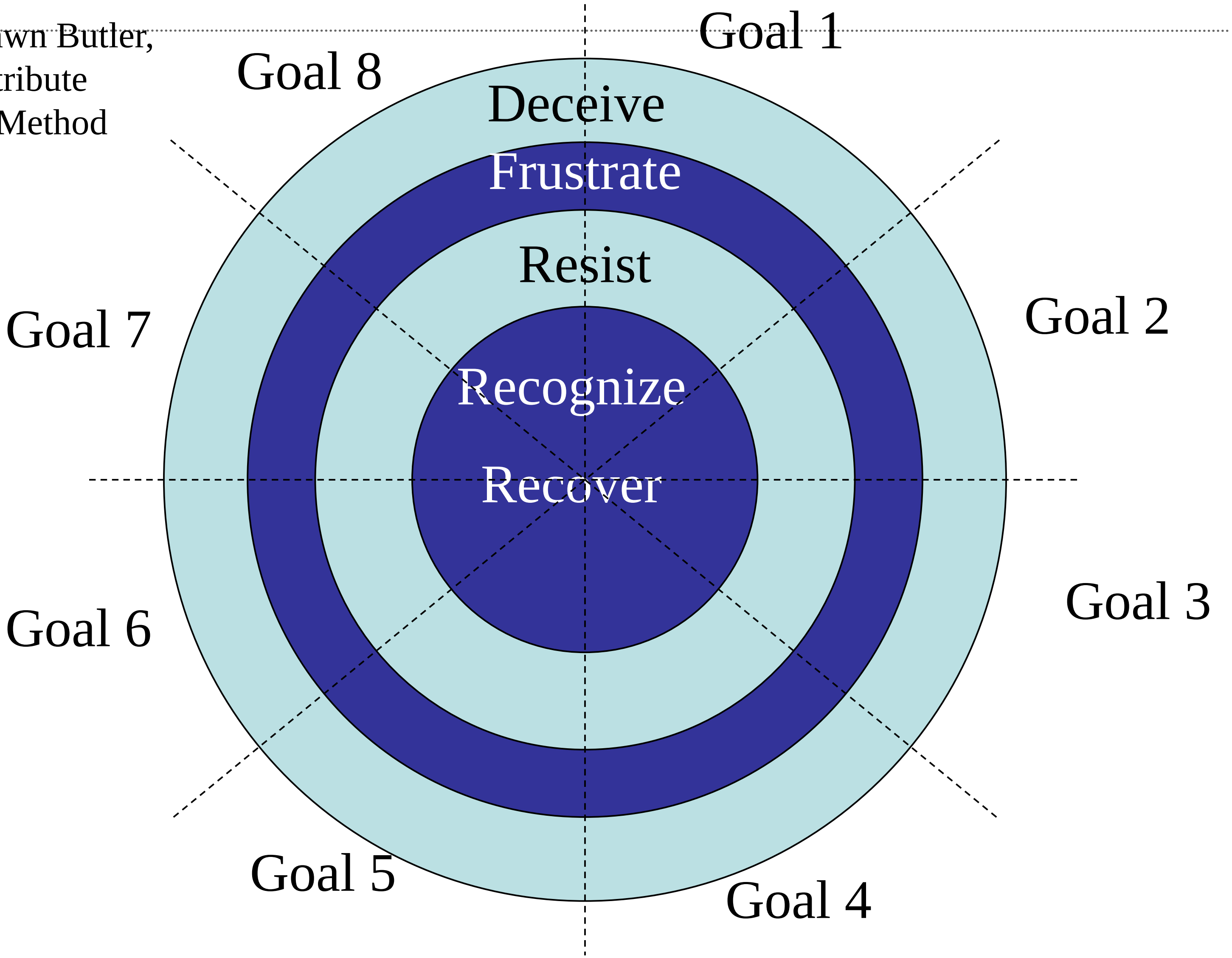
Analytics may support other analytics

- Network profiling supports attack surface estimation
- Attack surface estimation support vulnerability estimation
- Service monitoring supports beacon and exfiltration recognition

Well-planned defense uses multiple strategies

Layered Defenses

Source: Shawn Butler, Security Attribute Evaluation Method



Recapitulation

Network Flow Analysis has historically been associated with either network engineering or incident response

Many other applications are productive

Analytics are not difficult, but need to be focused and tuned

New analytics are being formulated

Questions?

Tim Shimeall, Ph.D.

Netsa-contact@cert.org

4500 Fifth Ave

Pittsburgh PA 15213