Introduction

• Bejtlich ("bate-lik") biography
  – General Electric, (07-present)
    • TaoSecurity (05-07)
    • ManTech (04-05)
    • Foundstone (02-04)
    • Ball Aerospace (01-02)
    • Captain at US Air Force CERT (98-01)
    • Lt at Air Intelligence Agency (97-98)
  – Author
    • Tao of Network Security Monitoring: Beyond Intrusion Detection (solo, Addison-Wesley, Jul 04)
    • Extrusion Detection: Security Monitoring for Internal Intrusions (solo, Addison-Wesley, Nov 05)
    • Real Digital Forensics (co-author, Addison-Wesley, Sep 05)
    • Contributed to Incident Response, 2nd Ed and Hacking Exposed, 4th Ed
Overview

- What do I do?
- What can we do to improve security?
- Definitions and measurement
- Evidence-based policy via trials
- How to obtain visibility?
- Soccer goal security
- Where to obtain visibility?
- Challenges to visibility
- Potential approaches
- Questions
What do I do?

- Director of incident response = as close to problem as could be
- Deal with failure, where theory meets reality
- Risk equations not needed; facts and evidence everywhere
- Worst possible place to perform “security” (or is it?)
- I would rather not work here -- “prevention is preferred”
What can we do to improve security?

• What is “security”?
• Consider “what is healthy?”
  – Blood pressure below 120/80
  – Cholesterol below 200
  – Body mass index below (some value)
  – Imagine other measurements... but you might still have cancer
• Lesson is you need to define *something*, and then measure it *somehow*
Definitions and measurement

- **Input metrics:**
  - AV running and current?
  - Patches applied?
  - Configured properly?
- **Output metrics**
  - Botnet participant
  - Disclosed earnings report earlier via exposed share
  - Unavailable due to ongoing DDoS attack
- Output metrics are often ignored, but they are crucial: What's the score of the game?
- **What to measure?**
  - Outputs: incidents (as identified in many different forms)
  - Inputs: controls whose application affects the outputs
Evidence-based policy via trials

- *Economist*, 14 June 2008 article on random trials to guide developmental aid policy in Africa
- Process as applied to digital security
  - Determine desired outcome and ways to measure it
  - Identify control group(s) and trial group(s)
  - Apply changes to trial group(s)
  - Compare results
- In most enterprises, defenses are unevenly applied, or deployed in stages, so control and trial groups can be identified
- Process encourages *management by fact, not by belief*
- Measurement requires visibility
How to obtain visibility?

• Visibility means being able to see what is happening inside the enterprise
• Visibility enables digital situational awareness
• Obtaining situational awareness is the first requirement for completing (and tightening) your OODA loop
• OODA loop
  – Observe
  – Orient
  – Decide
  – Act
• If you don't OO, any DA that results in improvement only occurs through luck
• Risk management without evidence is probably miseducated guesswork
Soccer goal security

- Is this your enterprise?
- How would you know?
Where to obtain visibility?

- Visibility should be obtained at trust boundaries, according to enterprise risk tolerance
- Here we come to Network Security Monitoring, which involves collecting, analyzing, and escalating traffic
- General process
  - Identify trust boundaries
  - Apply instrumentation
  - Develop collection, analysis, and escalation strategies
- Enterprise Visibility Architect works with Enterprise Security Architect
- “Building security in” is nice, but “building visibility in” should be more important
- Schneier said in 2001: “Monitor first”
- Usually feature -> management -> security -> visibility (backwards)
Challenges to visibility

• Cloud
• Virtualization
• Nontraditional platforms
• Privacy concerns and laws
• Lack of skilled resources
• Tools built for performance or development, not security or forensics
Potential approaches

• When you don't own, manage, or work inside the “factory,” but only consume products and services, on what do you rely?
  – Government regulation
  – Industry standards
  – Certifications and licenses
  – Inspections
  – Press and watchdog groups
  – Reputation, brand, and history

• Just beginning to realize that trusting endpoints is a bad idea – might have to be extended everywhere (Amazon S3 example)

• Cost rules all; precludes development of more trustworthy systems

• Need to fund and engage law enforcement and counterintelligence

• Where else do victims investigate their own crime scene?
Questions?

KNOW YOUR NETWORK BEFORE AN INTRUDER DOES

Richard Bejtlich
richard@taosecurity.com
www.taosecurity.com
9532 Liberia Ave Suite 141
Manassas VA 20110
202.409.8045