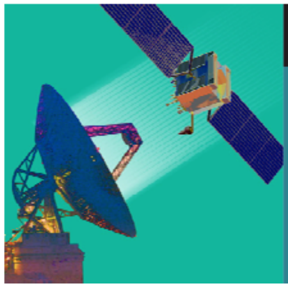
Ground System Architectures Workshop



Session 11B

Cyber Defense in Practice

DJ Byrne and Bryan Johnson

NASA/Jet Propulsion Laboratory

California Institute of Technology

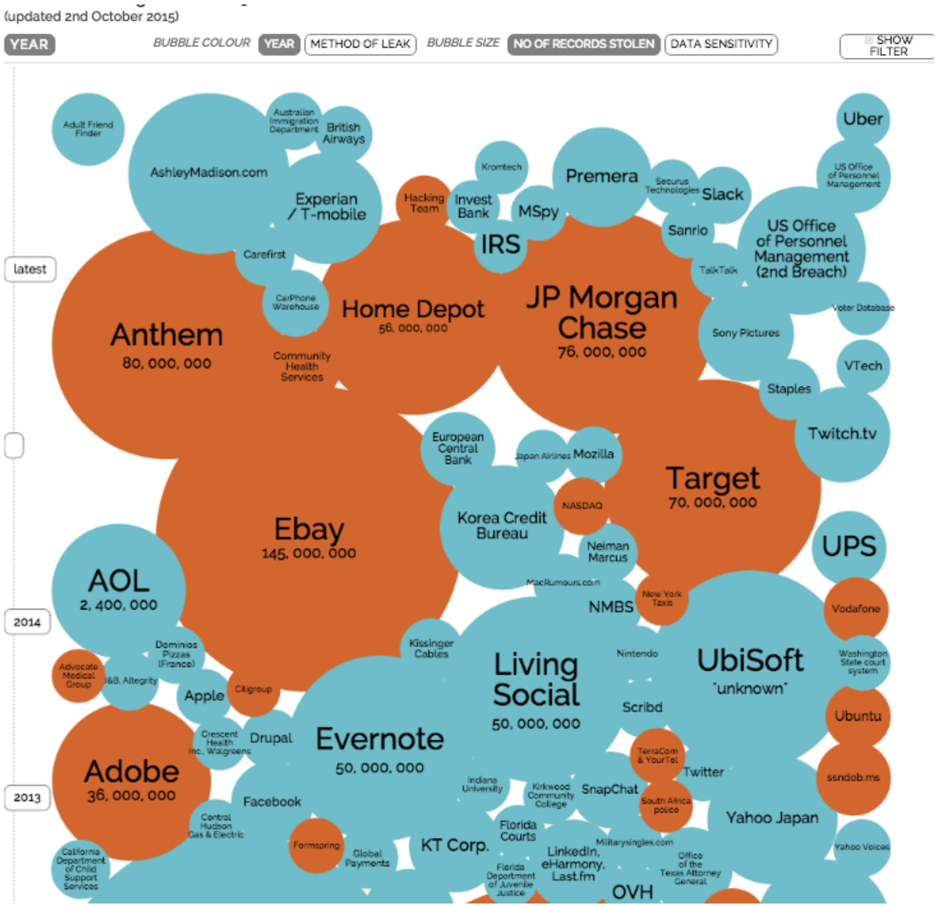
djbyrne@jpl.nasa.gov, bryan@nasa.gov

AEROSPACE

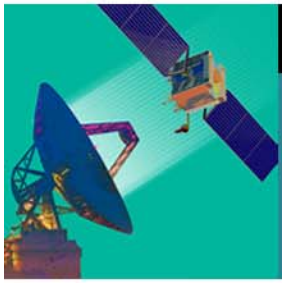
Published by The Aerospace Corporation with permission.

The Problem, Writ Large

- http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/


(updated 2nd October 2015)

Published by The Aerospace Corporation with permission.



Overview

- This is an open forum to discuss enterprise level experiences with cyber defense
  - Implementations
  - Verifications and Validations
  - Measuring their impacts
  - Adaptations
- Expected Take-aways
  - Benchmark your experiences with others
  - Identify gaps
  - Keeping relevant over time
  - Lessons Learned from others

Topics to start off

- Lay of the Land
- Organizational Politics
- Implementing an Architecture
- Verification and Validation
- Embracing Change During Operations
- Space Peculiarities

Lay of the Land

Resources, Dangers, Constraints

Lay of the Land

- What resources should every cyber professional know about?
  - – NIST standards, at least the titles and thrusts
    - http://csrc.nist.gov/publications/PubsSPs.html
    - http://www.nist.gov/cyberframework/
    - http://scap.nist.gov/specifications/cpe/
  - – CWE (Common Weakness Enumerations)
    - https://cwe.mitre.org/
  - – CVE (Common Vulnerabilities and Exposures)
    - https://cve.mitre.org/
  - – CAPEC (Common Attack Pattern Enumeration and Classification)
    - https://capec.mitre.org/

Lay of the Land (cont)

- ...Resources, cont.
  - SANS Top 20 Security Controls
    - https://www.sans.org/critical-security-controls
  - SANS: Top 25 Most Dangerous Software Errors
    - https://www.sans.org/top25-software-errors/
  - Australian Defence Signals Directorate
    - http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
  - OWASP for web coding
    - https://www.owasp.org/
  - NASA IV&V Secure Coding Portal
    - https://nen.nasa.gov/web/coding/tutorials

Lay of the Land (cont)

- What threat agents are credible (relevant to GSAW)?
  - Supply chain exposure
  - Your competitors
  - Insiders
- What attacks are active in the wild, and how can you be alerted?
  - US CERT (Computer Emergency Response Team)
    - http://www.us-cert.gov/cas/techalerts/
- How can attacks be described for categorization and prioritization?
  - TAXII (Trusted Automated Exchange of Indicator Information)
  - CybOX (Cyber Observable Expression)
  - STIX (Structured Threat Information Expression)
  - MISP (Malware Information Sharing Platform)
    - http://www.misp-project.org/

Lay of the Land (cont)

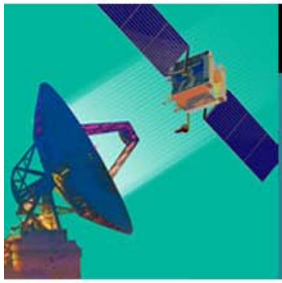
- What laws, regulations, and policies are in effect, or coming down the road?
  - What tools (or additional work) does that generate for us?

Implementing an Architecture

- Is system modeling helpful for risk assessment?
- What architectural choices undermine defenses?
  - Human in the loop? Maybe yes, maybe no.
- What defenses have had the most bang for the buck for your organization?
- Budget and schedule matter; what tasks should be done in what order for best effect?
- What tools are in common use, and what have our experiences been with them?

Verification and Validation

- How effective are compliance-based approaches?
- How to evaluate security of Cloud Computing?
- What test venues?



Organizational Politics

- What institutional barriers have been encountered, and how to overcome them?
- What pain points have manifested during implementation?
  - Information sharing?
- Who is in charge of what during an incident response?
- Who is accountable for breaches?
- Organizational structure for cyber issues?
  - CIO (Chief Information Officer)?
  - CISO (Chief Information Security Officer)?
  - Each project or business unit responsible for itself?
  - What are the reporting chain(s)?

Embracing Change During Operations

- Refreshing the architecture as threats evolve
  - Linear vs circular lifecycles
- "Securing the Human" - how to mitigate against human error and misbehavior?
- How to measure/quantify the effectiveness of defenses?
  - Drives change in cyber-strategy's implementation
- What drives deployment changes?
  - E.g., vendor product end-of-life, new technologies, cost
  - How must defenses change to keep in step?

Space Peculiarities

- How to apply cyber security to space? Consider whether the relative priorities between ***confidentiality*** vs ***availability*** or mission assurance are different than for other types of data systems.
- How are space-ground communications links different from other networks?
- Experience with legacy systems
  - How to mitigate evolving threats
  - ...While maintaining configuration management?