Using Systems Engineering to add to the APT Mitigation Strategy

What is Advanced Persistent Threat?

- Organized Entity – nation state, Terrorist Organizations (getting better at it), hacktivists - such as Anonymous
- Full Spectrum Capability – Information Operations, Computer Network Exploitation, Vulnerability Research, Software and Instrumentation Engineering, Social Engineering, Clandestine Operations Support
- Well Funded
- Highly Trained
- Goal Oriented - Defined Target Profile with objectives and priorities
- Effective – near 100% success rate
  - Experts in LPD/LPI
  - Slow Roll/Slow Bleed
  - Deep penetration
  - Pervasive across the target boundary

The attack plane grows bigger and bigger

- Moving towards cloud based computing
  - Information boundary, not network boundary
- It's a mobile world so it demands a mobile workforce
  - Increase in end-point access -Cell phone, Smartphone, PDA
- Computing Architectures are more sophisticated (not necessarily better) and often divergent
  - Trusted Computing for PC vs Ipad vs smartphone…

CIO's want it all – Confidentiality, Integrity, Assurance

Consumers want it all – Scalability, Portability, Mobility

What is the APT Operation looking for?

- National Secrets
  - National/Foreign Policy/Strategy, Weapons Design (Kinetic and non-kinetic)
- Intellectual Property
  - China is the leader in IP theft of US based companies
- Highlight a Social Cause by
  - Causing financial disruption – SONY, PAYPAL, AMAZON, etc…

What might an APT operation be looking to get from your organization?

Typical Response methods to an APT

- Security Training - Mitigation
- Information/Data classification/tagging - Mitigation
- Information Flows tied to business operations - Mitigation
- System Updates/Patching - Mitigation/Remediation
- HIDS/NIDS - Mitigation/Remediation
- Anti-virus/Anti-spyware - Remediation
- Incident Response Methods - Remediation
- Logging/Auditing - Remediation
- Deniability - shhh…don't let anyone one know we've been attacked

More than half of the 600 IT managers operating critical infrastructure in 14 countries reported being recently hit by "high-level" adversaries such as organized crime, terrorists or nation states.*

Re-cap

- APT is bad an its likely you've been hit, are hit, or will be hit.
- Typical Responses – remediation based (after the fact)
  - Perimeter defense – Firewalls, HIDS/NIDS, VPNs
  - Logging/Auditing
  - Security Training
  - Data Tagging/Classification
  - Deny or downplay publicly (gotta protect stock price), then work like mad to fix, realize you cant do it alone, then come clean publicly and get a black eye for not coming clean to begin with…or something like that.

Adding Systems Engineering to your APT Mitigation Strategy

Current State: APT mitigation is not a design requirement

- Many organizations do not consider APT threats as a security requirement
  - Not included during design or build time
  - After thought – Bolted on rather than built in
  - Fractured and often incomplete
  - Easy to miss vulnerabilities – security gaps
  - Some of the parts does not equal the whole

Even if all these issues were considered, you'd still get attacked

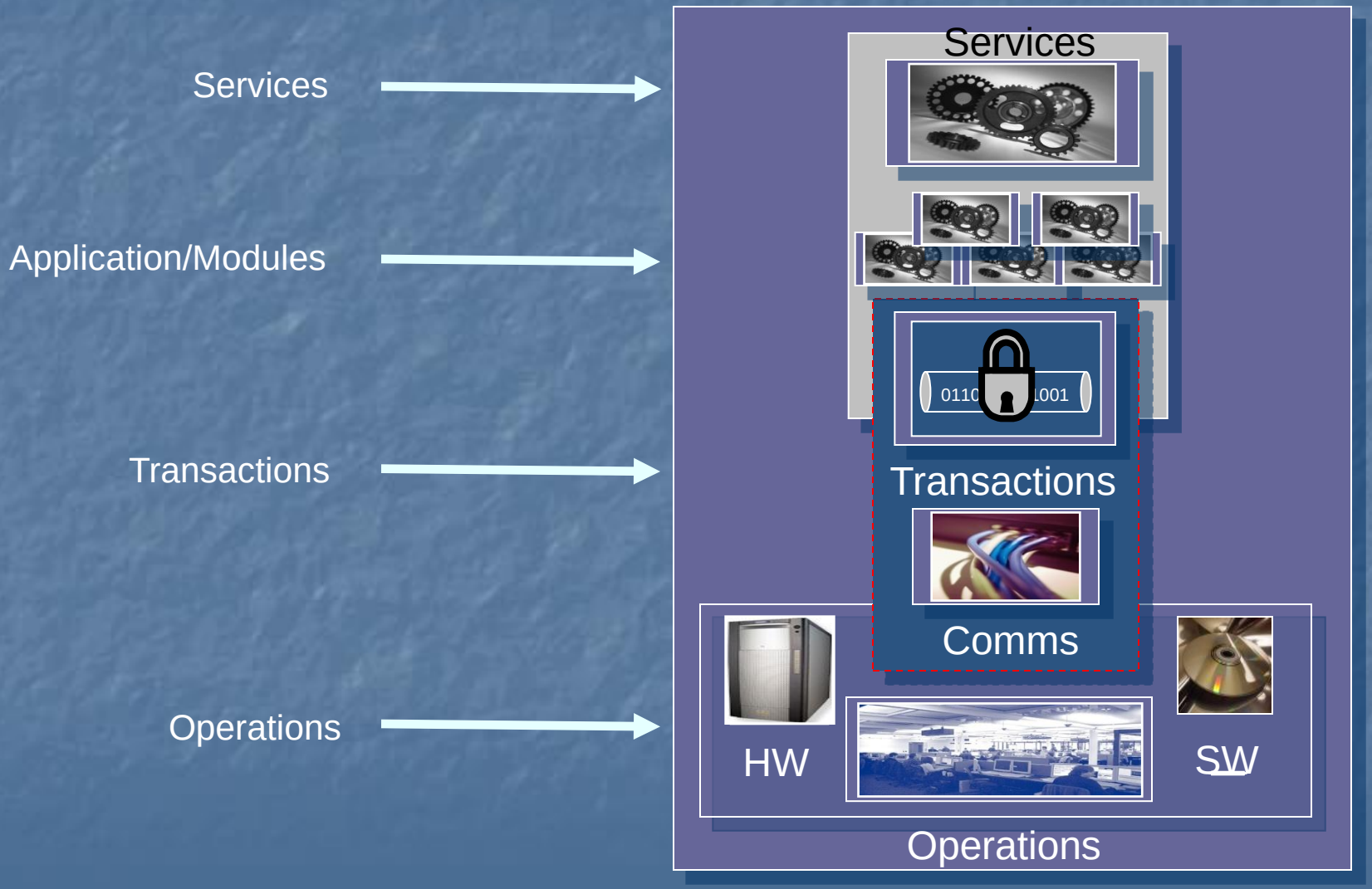
Attributes of the Assured Design Process

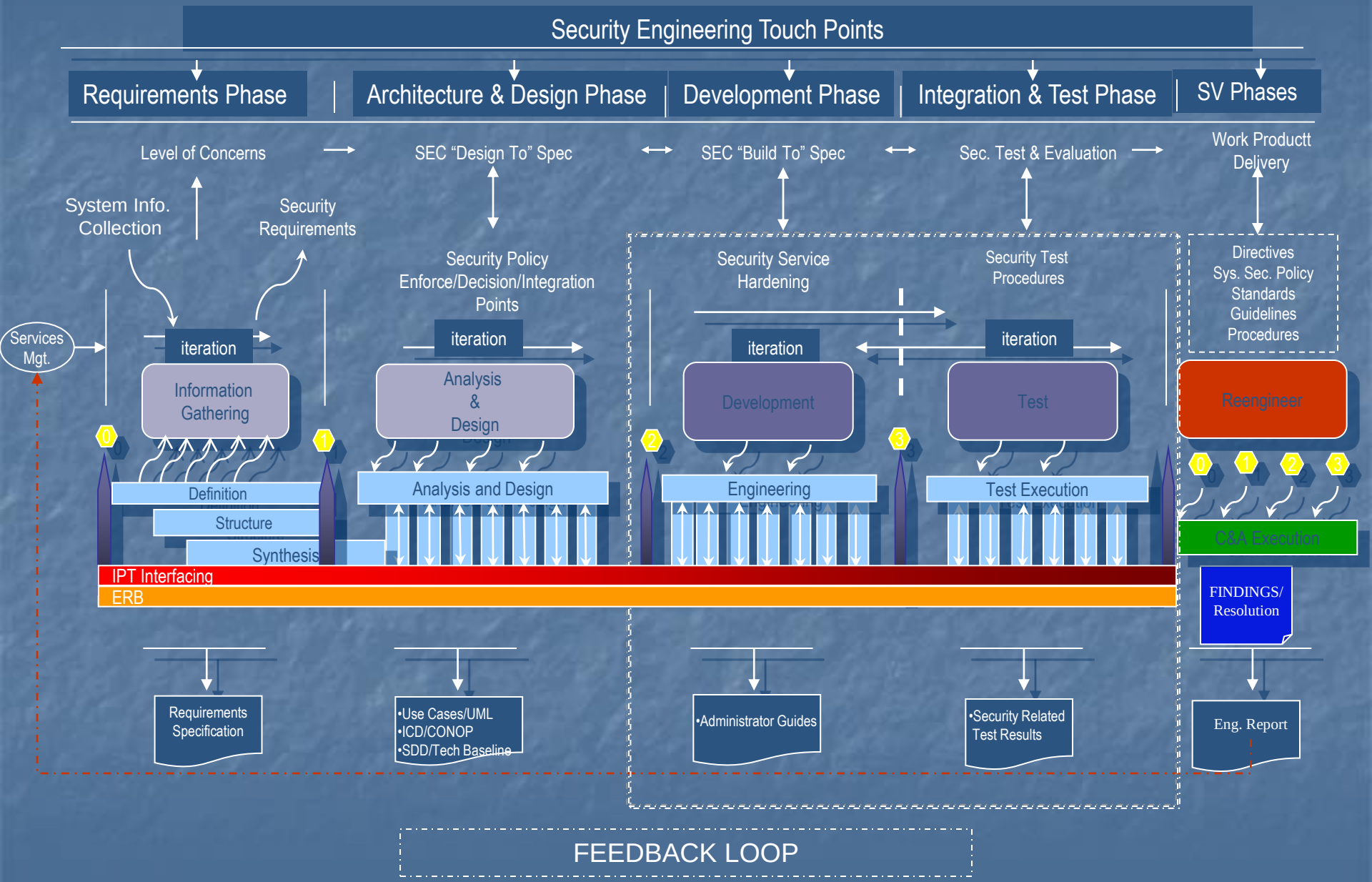
- Is a full-spectrum Security Systems Engineering process
  - Full Spectrum means:
    - Security Designs for Service, Application, Transactional, and Operational Security Features and Processes
- Assured Designed spans all aspects of the design and development life-cycle (Security Design, Engineering, and Development, Maintenance and Operations).
- Includes both Explicit and Implicit Security
  - Explicit Security means:
    - Integrated explicit features such as:
      - Focused Design of Security Process for Applications, Transactions, and Operations.
      - Explicit Enablers like:, TLS, Certificates, Access Control Features, Security Controls, Audits, Security Policies, LDAP, Cryptographic bit splitting for data at rest and data in motion – SecurityFirst Corp's Secure Parser ®
  - Implied Security Means:
    - Non-obvious Security Features such as:
      - Services are orchestrated and configured to preserve the security posture regardless of event.
      - Application/Module Design that does not expose vulnerabilities as part of the design – IE Sound Design
      - Transactions with properly encoded control checks - Transaction Centric Architectures
      - Operations - good SA and NETOPS processes that ensure cradle to grave follow-through, run-books, clearly written start-up, shut-down process, towards establishing and maintaining a protected state.

Assured Design Performance Requirements

- Operationally Relevant
- Provide proof that "as built = as designed"
- Ensure Design Integrity during all Phases
  - IV&V during Architecture and Engineering Phases
  - IV&V results integrate into ERB status to mitigate "under the radar" engineering.
- Start with Expectation Management
  - Security woven in, not bolted on
  - Design for Relevance
- Bound the Problem Space
  - Defining the Operational Context
  - Determining the Transactions
  - Determining the Configuration/Orchestration Options
  - Architect to outcome, Build to Constraint
- Begin Security Engineering at Design Inception
  - Interface with the DAA as early as possible
  - Conduct initial Assessment based on relevant requirements
  - Produce Artifacts that meet development requirements ("Build To" Specification).
- Promote Buy-Off with auditor/verifier
  - DAA Buy-off begins at design inception and ends with DAA Certification
  - Provide DAA with as much Shrink-Wrapping as possible

What do I need to look at for Designing APT Mitigation?




Security Engineering Touch Points
Requirements Phase
Architecture & Design Phase
Development Phase
Integration & Test Phase
SV Phases
Level of Concerns
SEC "Design To" Spec
SEC "Build To" Spec
Sec. Test & Evaluation
Work Productt Delivery
System Info. Collection
Security Requirements
Security Policy Enforce/Decision/Integration Points
Security Service Hardening
Security Test Procedures
Directives
Sys. Sec. Policy
Standards
Guidelines
Procedures
Services Mgt.
iteration
Information Gathering
Analysis & Design
Development
Test
Reengineer
0
1
2
3
Definition
Structure
Synthesis
Analysis and Design
Engineering
Test Execution
C&A Execution
IPT Interfacing
ERB
FINDINGS/ Resolution
Requirements Specification
•Use Cases/UML
•ICD/CONOP
•SDD/Tech Baseline
•Administrator Guides
•Security Related Test Results
Eng. Report
FEEDBACK LOOP

Thank You!