What Next in Intrusion Tolerance

29 June 2009

Partha Pal
Rick Schantz ,Joe Loyall, FranklinWebber, Michael Atighechi

3rd Workshop on Recent Advances in Intrusion Tolerant Systems
DSN 2009

Outline

- Intrusion Tolerance and Survivability
- Achievements so far
- Emerging software technologies
- New challenges and issues
- Potential way forward
- A concrete example: electric grids
- Conclusion

Generations of Security Research

BBN TECHNOLOGIES

No system is perfectly secure– only adequately secured with respect to the perceived threat.

Prevent Intrusions
(Access Controls, Cryptography, Trusted Computing Base)


Trusted Computing Base


Access Control & Physical Security


Cryptography

But intrusions will occur

1st Generation: Protection

Detect Intrusions, Limit Damage
(Firewalls, Intrusion Detection Systems, Virtual Private Networks, PKI)


Firewalls


Boundary Controllers


Intrusion Detection Systems


VPNs


PKI

But some attacks will succeed

2nd Generation: Detection

Tolerate Attacks
(Redundancy, Diversity, Deception, Wrappers, Proof-Carrying Code, Proactive Secret Sharing)


Intrusion Tolerance


Big Board View of Attacks
Real-Time Situation Awareness & Response


Graceful Degradation


Hardened Operating System

3rd Generation: Tolerance and Survivability

Survivability and Intrusion Tolerance

BBN TECHNOLOGIES

Premise

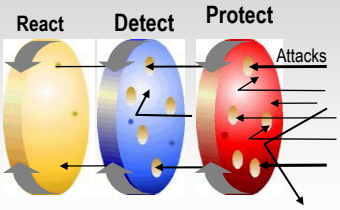
- The number & sophistication of cyber attacks is increasing – some of these attacks will succeed

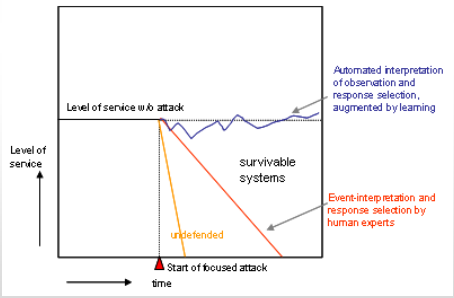
Philosophy

- *Operate through attacks* by using a layered defense-in-depth concept
  - Accept some degradation
  - Protect (C,I, A) of most valuable assets (information, services, …)
  - Move faster than the intruder

Approach

- "Defense Enabling" Distributed Applications
- Survivability architecture

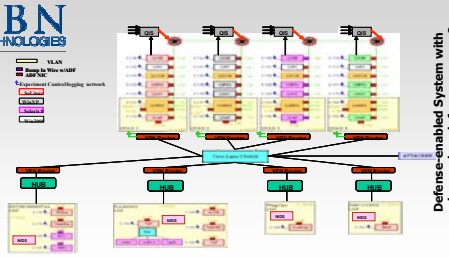


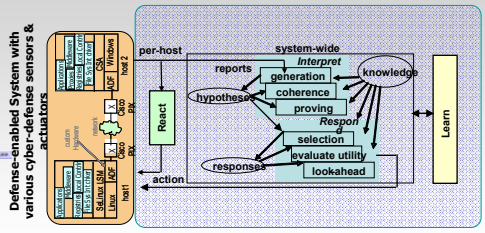


- Exploring beyond degradation-- regain, recoup, regroup and even improve
- Semi-automated: Survivability architecture captures a lot of low level (and sometimes uncertain and incomplete) information – utilizes advanced reasoning and machine learning

Achievements So Far

BBN TECHNOLOGIES





Military (USAF) Joint Battlespace Infosphere (JBI) information management system exemplar made survivable and subjected to sustained attacks over several weeks by multiple independent red teams

Results

- The system survived 75% of attacks
- Of those that succeeded,
  - Average time to failure was 45 minutes
  - Vs. immediately in the unprotected system
  - Minimum of 10 minutes to failure
  - Required combinations of attacks
- Adaptive defenses added 5-20% overhead to call latency

Challenge: Develop automated mechanism that would interpret the reports and decide the effective course of action

CSISM Approach: 3 level decision making- reactive, deliberate and learned; use theorem proving and coherence to reason about accusatory and evidentiary information contained in reported events

Results

- Possible to minimize expert involvement
- Reasoning about accusatory and evidentiary information wrt encoded knowledge
  - Made correct decision in ~75% cases in red team exercises
  - Compute intensive
- Integrating learned responses online needs additional research

Emerging Trends

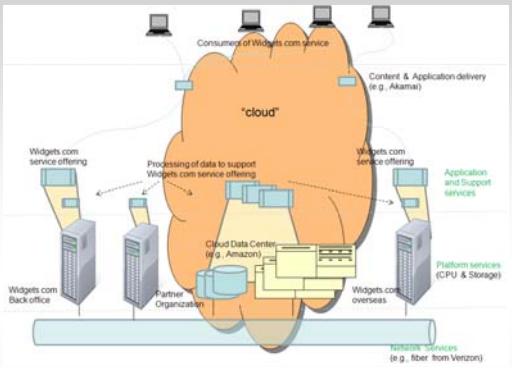
BBN TECHNOLOGIES

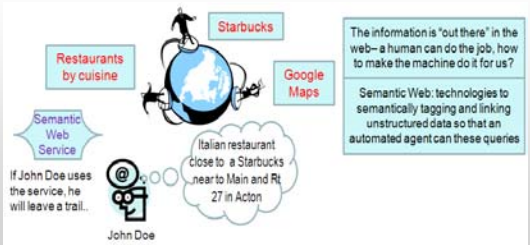
CLOUD: Somebody else's data center

Compute, storage, communication
Scale, Provisioning
Dynamism

SOA: Think information systems in terms of services: as opposed to algorithms, protocols, data structures, objects… is it really a new think?

Loose coupling
Externalization
Reuse and dynamism





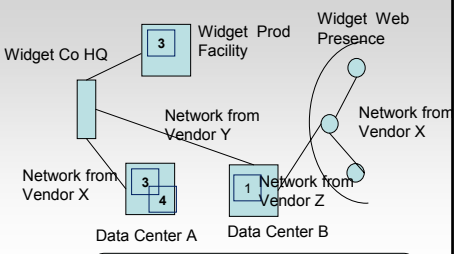
Semantic Web: Automate associating or relationship discovery in available data based on semantics

Semantic tags, Linking and Link Chasing
Mash ups

Things that will improve

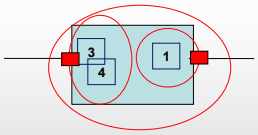
BBN TECHNOLOGIES

- Defense in depth
  - Buy protected, guaranteed connectivity from Verizon
  - Buy storage and servers from Amazon
  - Diversity (different cloud vendors), Dynamic, Cheap(er)



1. Svc for sales force management
2. Svc for supply chain
3. Svc for pay roll management
4. Svc for HRM

- Access control to networks, CPU, storage
  - Cloud owner's revenue depends on it



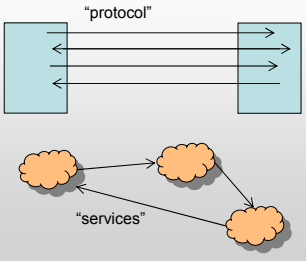
- Situation Assessment Reasoning
  - Semantic correlations and patterns

Things that will remain challenging…

BBN TECHNOLOGIES

- Validation and trust
  - How to validate security and intrusion tolerance of a service offering?
  - How to judge trustworthiness of cloud?

- Accountability
  - Tasks that used to be "internal" to an organization, will now span multiple organization boundaries
    - Organizations will log and audit
    - But may be mismatched



New Challenges

- Data protection
  - Social networking model
  - Encrypt before storing
  - Data gleaned while your process executes?
  - Leakage through semantic linking?
  - What about metadata?
- Service Management
  - End to end security:
    - Orchestration, (re)provisioning of cloud resources
    - What happens when failures cannot be masked within?
    - Externalization may not always be good!
- Regulatory Issues
  - Privacy
  - Detecting, deterring bad guys while facilitating legitimate use
    - Cloud offering encrypted storage
    - Communication vendor offering encrypted guaranteed bandwidth

Potential Way Forward

- Service-oriented Security
  - What does crumple zones mean for services?
  - Service-layer VPGs
  - Service conglomerates
- MILS
  - Inside a cloud
  - VM techniques
- Online Continued Indicator of Assurance
  - Quality of assurance
- Securing Digital Objects
  - Encode access control and authentication policies as metadata
  - Leverage Service Orientation and fast networks
- Practical Privacy Preserving Schemes
  - Crowds
  - One time codes

A Concrete Case

BBN TECHNOLOGIES

- Grid modernization
- Role of information systems
- Emerging software technologies
- But what about Intrusion Tolerance?

Conclusion

BBN TECHNOLOGIES

- Intrusion Tolerance
  - Still important, probably more so now…
  - Going mainstream (plug for the panel)
    - Has it? Going to?
    - Impediments? Accelerators?
  - Bottom-line: need to constantly update itself
    - Arms race against the adversary
    - Advanced technology helps the attacker as well
    - Beware of bandwagons!