ACHIEVING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN VIRTUALIZED ARCHITECTURES

Michael Brady

Jason Stoudt

Andrew Miller

THE PROBLEM

- Industry movement toward third party cloud infrastructures
  - Critical systems are also moving to the cloud (i.e. ground systems)
- Key attributes of the cloud are contrary to the notion of "Trust"
  - Multi-tenancy
  - Loaned resources
- Today's threats are both external and internal

SAFETY-CRITICAL DESIGN

- Safety-Critical Systems
  - Systems that could cause critical harm if they fail (flight, medical, nuclear, construction, defense)
- Design goal is to minimize the probability of failure to an acceptable low level
- Areas of focus
  - Single point failures and common mode failures must be mitigated in Safety-Critical designs
- Failing Safe…
  - When an error occurs, a critical system should fail to a safe state

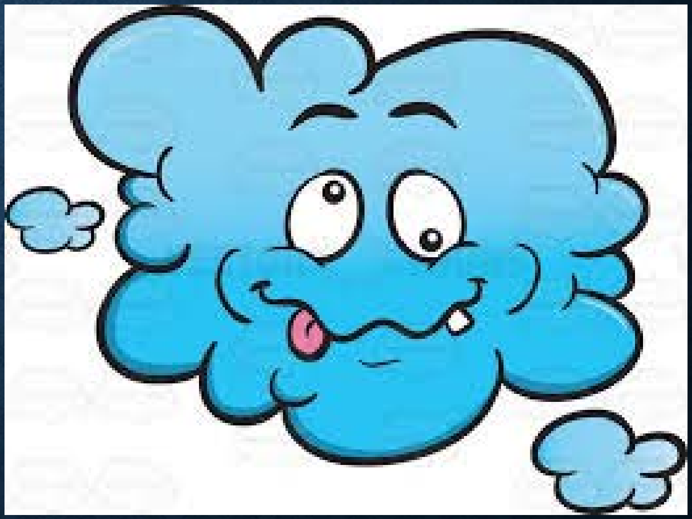
REDUNDANCY FOR FAIL-SAFE

- Redundancy is a way to fail safe
- Homogenous Redundancy
  - Uses exact clones
  - Mitigates random hardware failures
- Heterogeneous Redundancy
  - Uses different hardware/software
  - Mitigates random and systematic failures (More resilient!)
- Controllers
  - Used to check the results outputted by various heterogeneous redundant processes

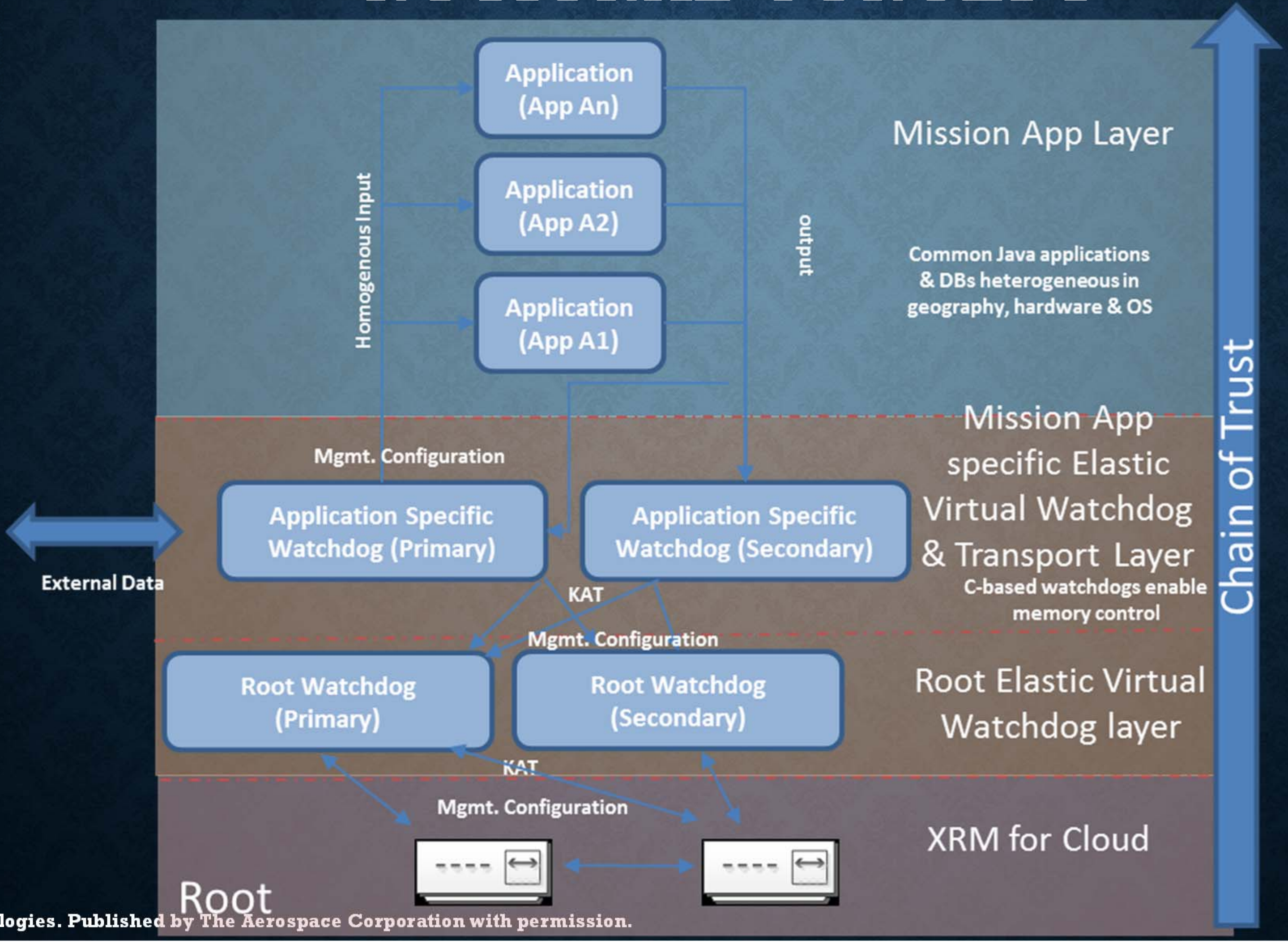
FAIL-SAFE ALERT!
MISSILES LAUNCHING
COUNTDOWN
Missile launch: 60 s.
Global nuclear war: 90 s.
To cancel, enter your security code and give the counter-order within 60 seconds.
CLICK CLICK CLICK CLICK
Sorry, this page requires a newer version of Adobe Flash. Click here to update your Adobe Flash plugin.
Fail-Safe.
icanbarelydraw.com CC BY-NC-ND 3.0

CAN THESE CONCEPTS BE APPLIED TO THE CLOUD?

- Redundancy costs money!
  - But cloud processing is relatively cheap
- Application boot?
- Communication security?
- Who watches the Watchdog?



NOTIONAL CONCEPT



Mission App Layer

Application (App An)

Application (App A2)

Application (App A1)

Homogenous Input

output

Common Java applications & DBs heterogeneous in geography, hardware & OS

Mission App specific Elastic Virtual Watchdog & Transport Layer

C-based watchdogs enable memory control

Mgmt. Configuration

Application Specific Watchdog (Primary)

Application Specific Watchdog (Secondary)

External Data

KAT

Mgmt. Configuration

Root Watchdog (Primary)

Root Watchdog (Secondary)

Root Elastic Virtual Watchdog layer

KAT

Mgmt. Configuration

XRM for Cloud

Root

Chain of Trust

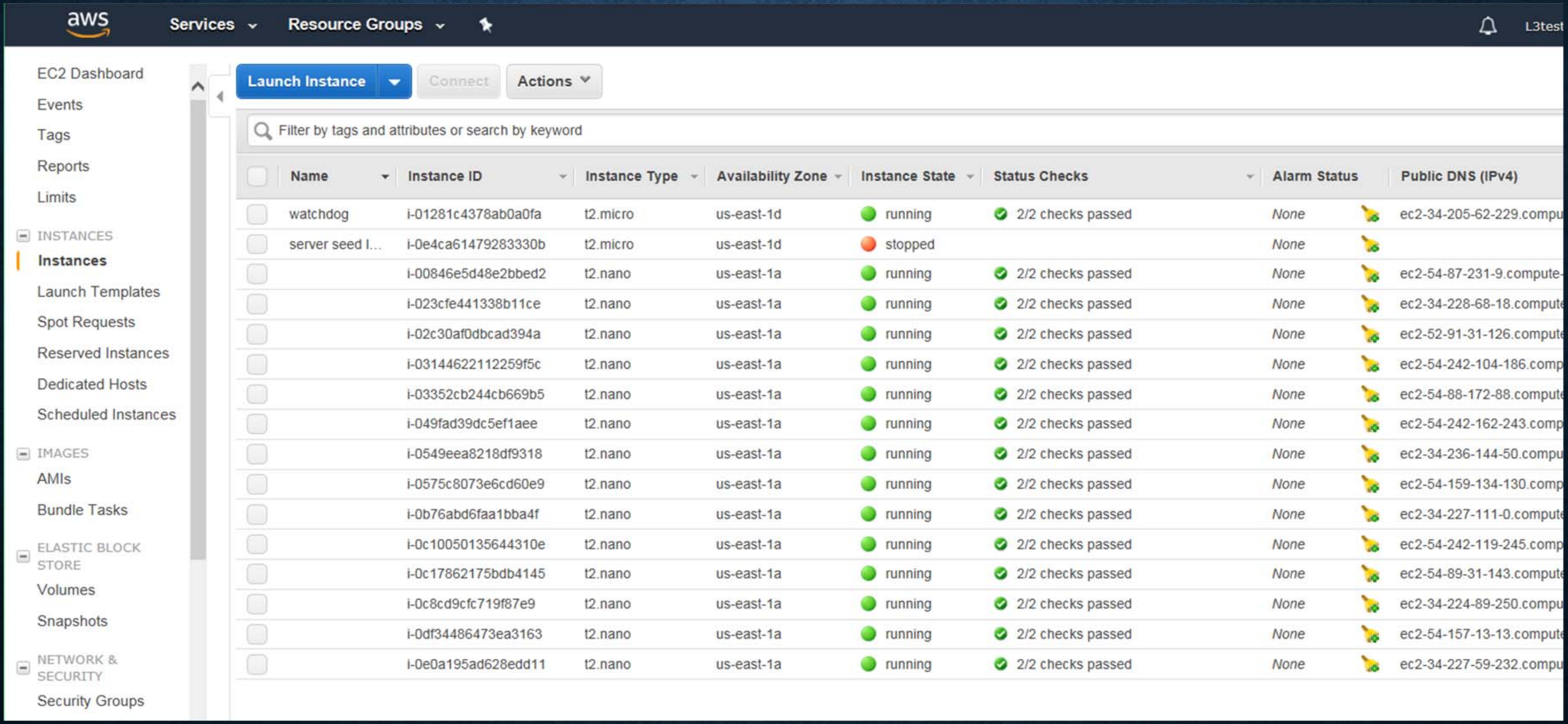
AWS PROOF OF CONCEPT

- Theory
  - Must be deterministic
  - Voting System across instances of an application
    - For this exercise, simple majority wins
  - Two types of voting
    - In-band
      - Wait for majority answer
    - Out-of-band
      - First response wins
      - May send bad answer one time

AWS PROOF OF CONCEPT

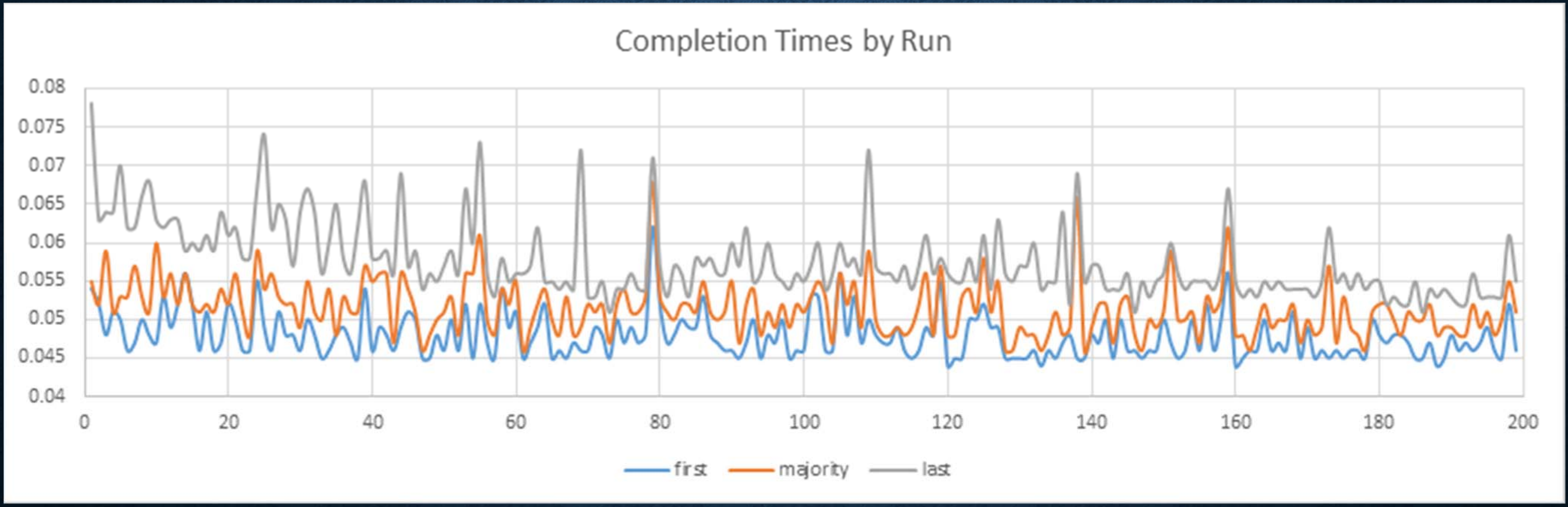
- Applied
  - One Watchdog
    - EC2 AMI instance running Java Watchdog app
    - Responsible for lifecycle of simple app
  - 9 instances of a simple app
    - EC2 AMI instance running simple app that responds to a request from the Watchdog
    - App computes whether a user is located within a satellite spot beam
  - Homogenous environment
    - One AWS Region (N. Virginia)
    - One EC2 AMI seed instance

AWS PROOF OF CONCEPT

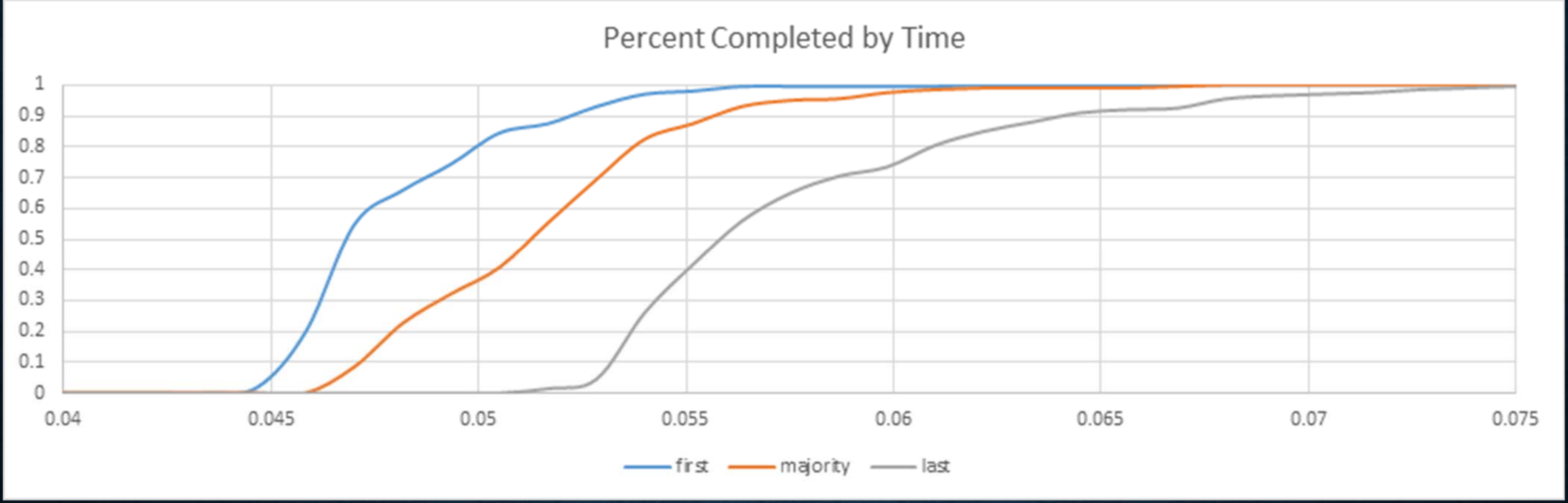


□	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
□	watchdog	i-01281c4378ab0a0fa	t2.micro	us-east-1d	● running	✓ 2/2 checks passed	None	ec2-34-205-62-229.compu
□	server seed l...	i-0e4ca61479283330b	t2.micro	us-east-1d	● stopped		None	
□		i-00846e5d48e2bbed2	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-54-87-231-9.compute-
□		i-023cfe441338b11ce	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-34-228-68-18.compute
□		i-02c30af0dbcad394a	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-52-91-31-126.compute
□		i-03144622112259f5c	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-54-242-104-186.comp
□		i-03352cb244cb669b5	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-54-88-172-88.compute
□		i-049fad39dc5ef1aee	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-54-242-162-243.comp
□		i-0549eea8218df9318	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-34-236-144-50.compu
□		i-0575c8073e6cd60e9	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-54-159-134-130.comp
□		i-0b76abd6faa1bba4f	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-34-227-111-0.compute
□		i-0c10050135644310e	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-54-242-119-245.comp
□		i-0c17862175bdb4145	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-54-89-31-143.compute
□		i-0c8cd9cfc719f87e9	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-34-224-89-250.compu
□		i-0df34486473ea3163	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-54-157-13-13.compute
□		i-0e0a195ad628edd11	t2.nano	us-east-1a	● running	✓ 2/2 checks passed	None	ec2-34-227-59-232.compu

AWS PROOF OF CONCEPT



AWS PROOF OF CONCEPT



SUMMARY

- Safety-Critical designs can support Virtualized Environments
- Concept can bring us a more secure solution on third party infrastructures
- Lots of trades between increased security, processing power, heterogeneity, and latency
- More work to be done on the viability of this design for persistent storage

QUESTIONS?

CONTACT INFORMATION

- Michael Brady
  Solution Architect, Secure Resilient Systems
  L3 Technologies, Communication Systems – East
  (856) 571-3147 michael.brady@L3T.com

- Jason Stoudt
  Software Architect, Secure Resilient Systems
  L3 Technologies, Communication Systems – East
  (856) 338-4411 jason.stoudt@L3T.com

REFERENCE MATERIAL

- Material for this briefing was supported by the following publications:
  - Microsoft Security Intelligence Report, Volume 22 (May 2017)
  - “*Attack on the Cloud Increase 300%*” Infosecurity Magazine, Dan Raywood (21 August 2017)
  - “*Developing a Framework to Improve Critical Infrastructure Cybersecurity*” Forrester Research, Inc. (8 April 2013)
  - “*Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds*” Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage
  - “*Doing Hard Time: Developing Real-Time Systems with UML, Objects, Frameworks, and Patterns*” Bruce Powel Douglass (September 1999)
  - “*A Platform Authentication Model for Network End-Point Integrity based on TPM*” Ned Smith (May 2005)
  - “*TCG Specification Architecture Overview*” Trusted Computing Group, Inc. Revision 1.4 (2 August 2007)
  - “*Achieving Cyber Survivability i9n a Contested Environment Using a Cyber Moving Target*” Dr. Hamed Okhravi, Joshua Haines, Kyle Ingols, High Frontier Journal for Space and Cyberspace Professionals, Volume 7, Number 3 (2011)
  - “*Cloud Ubiquity – it’s coming, but not yet!*” Raj Samani (12 Feb 2017)
  - “Fault Tree Handbook” U.S. Nuclear Regulatory Commission (1981)