Moving-Target Defense With Configuration-Space Randomization

Dr. Sanjai Narain, Telcordia Technologies, Inc.

In Collaboration With

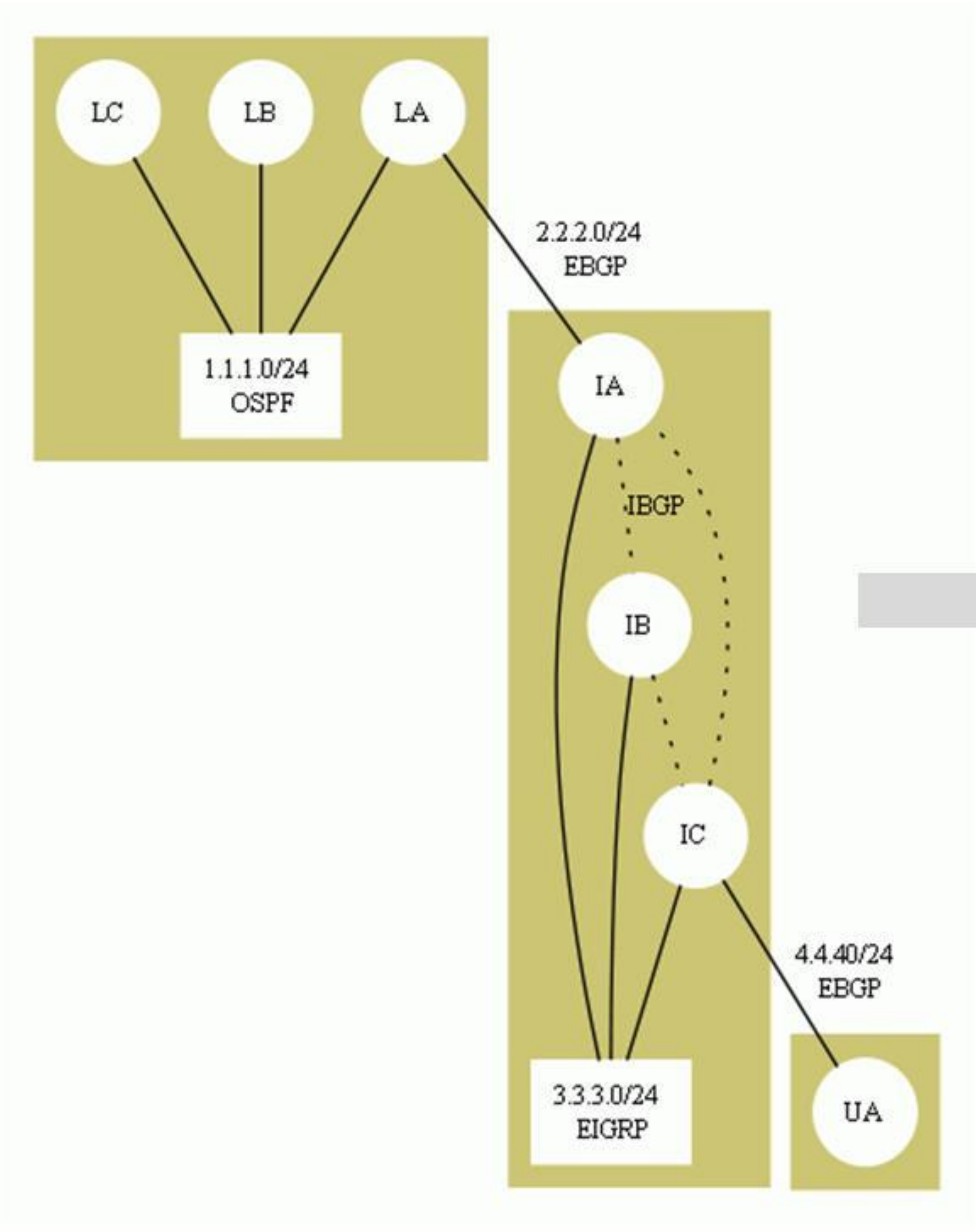
Professor Sharad Malik, Princeton
Professor Daniel Jackson, MIT
Professor Trent Jaeger, Penn State
Professor Ehab Al-Shaer, UNCC

Email: narain@research.telcordia.com
Tel: 908 337 3636

Overview

- Configuration is the glue for logically integrating cyber infrastructure components.
- Configuration errors cause 50%-80% of cyber attacks and downtime in cyber infrastructure.
- ConfigAssure defines a science of configuration
- It contains fundamental tools for eliminating configuration errors
- It is being deployed in a collaboration network at DISA
- It was trialed with High Assurance Platform that integrates VMWare with SELinux for MLS
- It is used to build the ADC system for randomly changing configurations to other correct ones

The Gap Between Requirement and Configuration

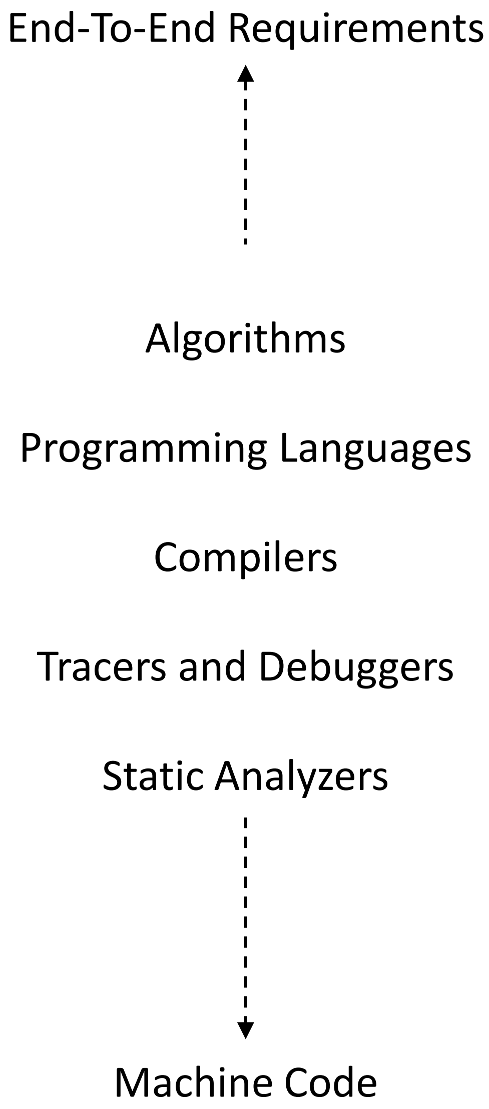


Conceptualization At High-Level

```
interface eth0
   ip address 1.1.1.1 255.255.255.0
   access-group FILTER-I-A in
   access-group FILTER-O-A out

router eigrp 25
    network 10.10.10.1 0.0.0.0
    no auto-summary

router bgp 5803
    neighbor 214.13.128.2 remote-as 5803

...
and hundreds more commands like these
```

Implementation with Low-Level commands

For Software Development, Many Tools Bridge Gap Between Requirements and Machine Code



End-To-End Requirements

Algorithms

Programming Languages

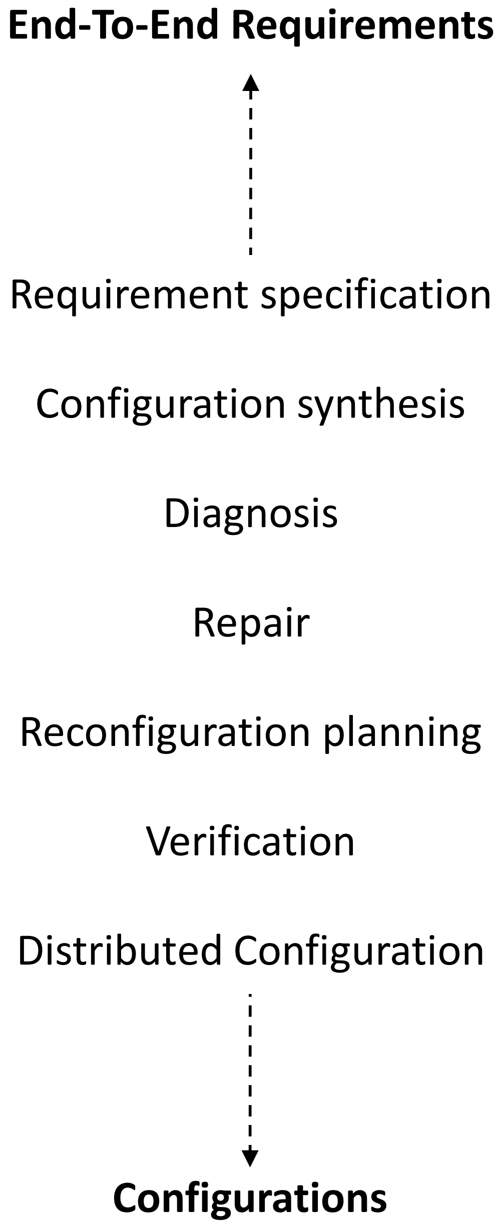
Compilers

Tracers and Debuggers

Static Analyzers

Machine Code

But For Infrastructure We Have Almost Nothing



End-To-End Requirements

Requirement specification

Configuration synthesis

Diagnosis

Repair

Reconfiguration planning

Verification

Distributed Configuration

Configurations

Why Are These Problems Hard?

- Tension between security and functionality
- Synthesis, reconfiguration planning and verification: Require searching very large spaces
- Diagnosis: Components work in isolation but not together
- Repair: Removing one error can cause another
- Information fragmentation: Across host, network, administrative and geographical boundaries
- Need to enforce end-to-end connectivity, security, application, performance and reliability requirements
- Hard to formalize configuration language grammar documented in 100s of English pages

Consequences of Configuration Errors

- .. the military is betting our lives on architectures with no overall plan nor overriding purpose. In fact, the biggest threat to the network may be a nonintrusive assault that simply causes the network to collapse of its own weight...
  - Col. Kevin B. Jordan who directed planning for C4 networks supporting 95,000 Marine and Allied troops for Operation Iraqi Freedom. Quote in “Coalition Operations Demand Technology Solutions, January 2005”. http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=618&zoneid=8

- We don’t need hackers to break the systems because they’re falling apart by themselves.
  - Peter G. Neumann, SRI. “Who Needs Hackers”, NY Times, September 7, 2007. http://www.nytimes.com/2007/09/12/technology/techspecial/12threat.html

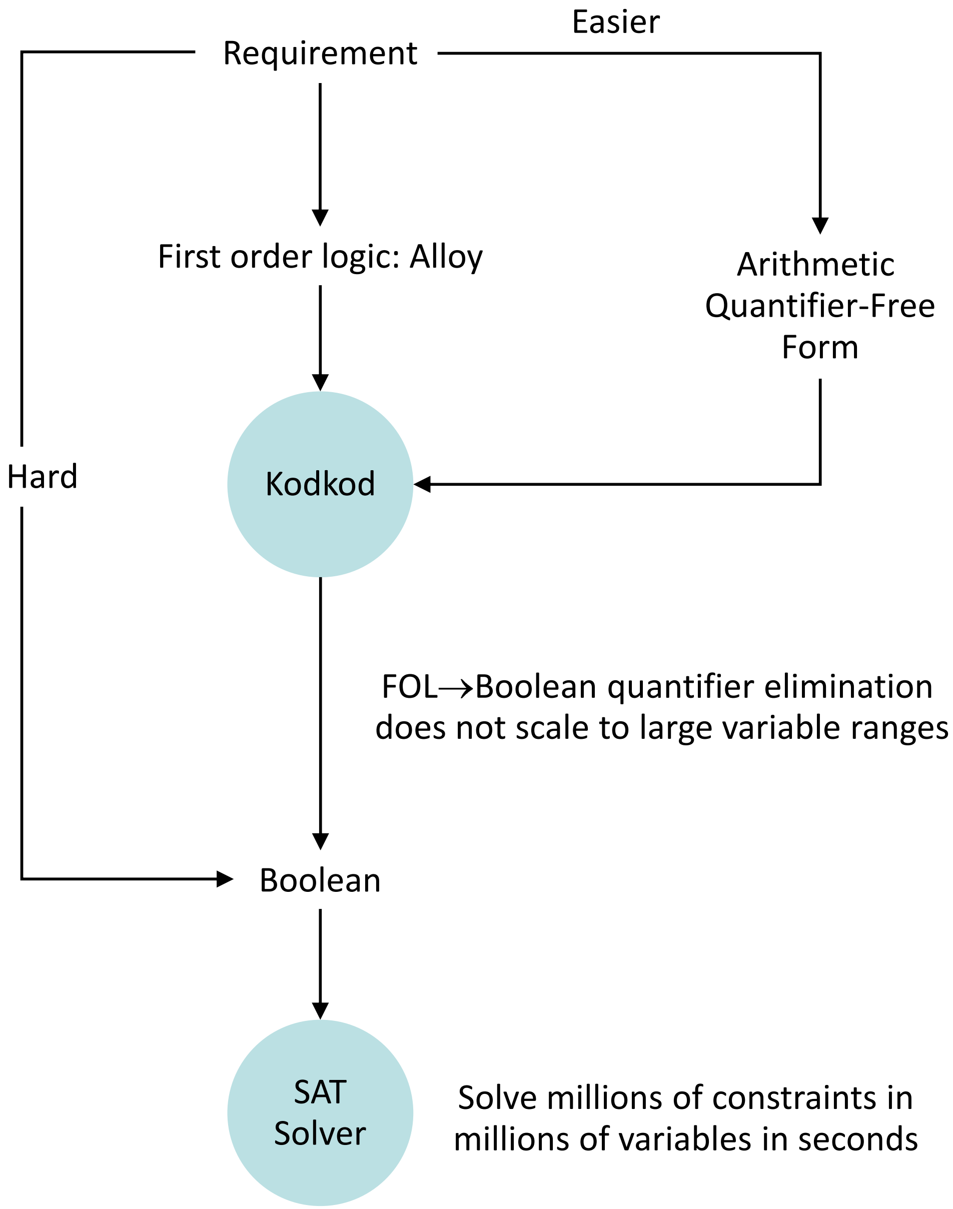
- Things break. Complex systems break in complex ways.
  - Steve Bellovin, Columbia University. “Who Needs Hackers”, NY Times, September 7, 2007. http://www.nytimes.com/2007/09/12/technology/techspecial/12threat.html

- ..human factors, is the biggest contributor—responsible for 50 to 80 percent of network device outages.
  - What’s Behind Network Downtime? Proactive Steps to Reduce Human Error and Improve Availability of Networks. http://www.juniper.net/solutions/literature/white_papers/200249.pdf

Classes of Configuration Errors In Enterprise Networks

- Connectivity
  - Incorrect addressing or IP, GRE, MPLS, IPSec links
- Security
  - Incorrect firewall policies
- Performance
  - Inconsistent QoS policies
- Reliability
  - Single points of failure due to misconfigured routing protocols, in spite of diversity
  - Single points of failure across layers
- Interaction between security and performance
  - Packet dropping due to mismatched MTU and ICMP blocking
- Interaction between security and reliability
  - IPSec tunnels not replicated in HSRP cluster
- Interaction between security and connectivity
  - Static routes not directing packets into IPSec tunnels
- Lack of centralized configuration authority
  - Static routes accumulated due to inefficient collaboration between network administrators

ConfigAssure Evolution



Requirement

Easier

First order logic: Alloy

Arithmetic Quantifier-Free Form

Hard

Kodkod

FOL→Boolean quantifier elimination does not scale to large variable ranges

Boolean

SAT Solver

Solve millions of constraints in millions of variables in seconds

Now EUF

Now SMT Solver

Overview of ConfigAssure

- Visualization of logical structures latent in configuration

- Specification language allows specifying sets of acceptable values of configuration variables, i.e., constraints
  - High-level language compiled into EUF = Boolean logic with data structures

- Traditional languages force one to specify concrete values

- Configuration synthesis: Set intersection, i.e., constraint solving. Use SMT solvers

- Diagnosis: Find x=c in proof of unsolvability, x a configuration variable

- Repair: Remove x=c and solve again

- Verification: Showing absence of counterexample. To show for all x. p(x) show there is no solution to some x. not(p(x))

- Reconfiguration planning: Convert a safety invariant into constraint on times of variable change, then solve it to obtain schedule of change

Demo: https://configassure.research.telcordia.com/csr

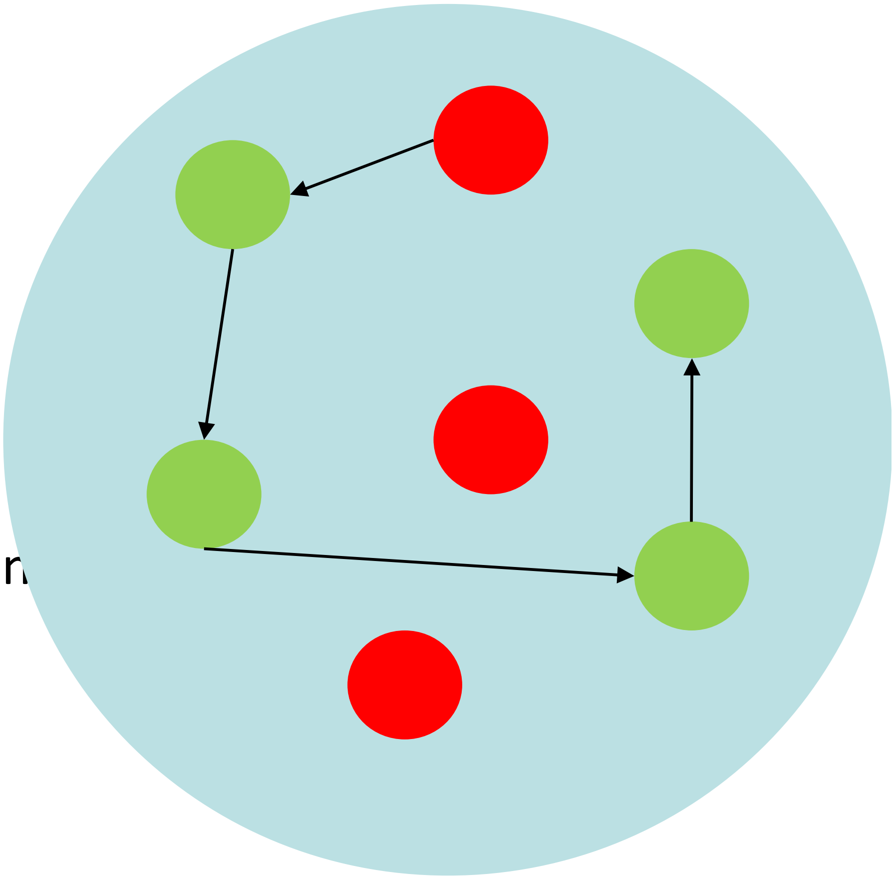
For username and password, please contact narain@research.telcordia.com

Configuration Space-Randomization

- Attack = Adversary gaining knowledge of critical parameters for a duration of time.

- Moving-target defense = changing critical parameters within that duration while maintaining system requirements on security and functionality

- Idea: If system requirement has more than one solution, then:
  - Each provides service to legitimate users
  - But transition from one to other confuses adversary



Configuration Space

References

1. Al-Shaer E, Marrero W, El-Atawy A, ElBadawy K (2009) Towards Global Verification and Analysis of Network Access Control Configuration. International Conference on Network Protocols

2. Anderson P (2006) System Configuration. In Short Topics in System Administration ed. Rick Farrow. USENIX Association

3. Enck W, Moyer T, McDaniel P, Sen S, Sebos P, Spoerel S, Greenberg A, Sung Y-W, Rao S, Aiello W, (2009) Configuration Management at Massive Scale: System Design and Experience. IEEE Journal on Selected Areas in Communications

4. Hamed H, Al-Shaer E and Will Marrero (2005) Modeling and Verification of IPSec and VPN Security Policies, Proceedings of IEEE International Conference on Network Protocols.

5. Homer J, Ou X (2009) SAT-solving approaches to context-aware enterprise network security management. IEEE JSAC Special Issue on Network Infrastructure Configuration

6. Mandelbaum Y, Fisher K, Walker D, Fernandez M, and Gleyzer A (2007) PADS/ML: A functional data description language. ACM Symposium on Principles of Programming Language

7. Narain et al. Formal Methods in Networking. Princeton University, Spring 2010 http://www.cs.princeton.edu/courses/archive/spring10/cos598D/FormalMethodsNetworkingOutline.html

8. Narain S (2005) Network Configuration Management via Model-Finding. Proceedings of USENIX Large Installation System Administration (LISA) Conference

9. Narain S, Levin G, Kaul V, Malik, S (2008) Declarative Infrastructure Configuration Synthesis and Debugging. Journal of Network Systems and Management, Special Issue on Security Configuration, eds. Ehab Al-Shaer, Charles Kalmanek, Felix Wu

10. Narain S, Talpade R, Levin G (2010) Network configuration validation. Chapter in “Guide to reliable Internet Services and Applications” eds Chuck Kalmanek, Richard Yang, Sudip Misra, Springer

11. Voellmy A, Hudak P Nettle (2009) A domain-specific language for routing configuration. Proceedings of ACM SafeConfig Workshop. http://bebop.cs.yale.edu/voellmy/nettle.html

12. Xie G, Zhan J, Maltz D, Zhang H, Greenberg A, Hjalmtysson G, and Rexford J (2005) On Static Reachability Analysis of IP Networks. IEEE INFOCOM

Summary

- ConfigAssure is a suite of fundamental tools for bridging gap between requirements and configuration:
  - Requirement specification
  - Synthesis
  - Diagnosis
  - Repair
  - Verification
  - Reconfiguration planning
  - Visualization

- Being deployed at DISA and trialed with High Assurance Platform

- Being used to build moving-target defense by configuration space randomization