SRN: Secure and Resilient Networking

Sponsored by NSF CNS 1528099, CNS 1523994, and CNS 1526299

ASU: Dijiang Huang (PI), Ankur Chowdhary, Chun-Jen (James) Chung, Sandeep Pisharody; UMKC: Deep Medhi (PI), Sheyda Kiani, Mirza Maswood; Duke: Kishor Trivedi (PI), Xiaodan Li.

Problem Statement

- Establishing an orchestrated and resilient defense mechanism in an enterprise environment based on quantifiable metrics, models and evaluation methods. Moving target defense (MTD) by attack prevention and mitigation in timely and intelligent fashion
- Network security measurement and attack analytic model for virtual networking system using Attack Graph.
- A comprehensive network evaluation model based on attack, vulnerabilities, network and system resources to improve attack resilience.
- Exploiting SDN to use different anomaly detection systems and analyzing software bugs due to security and non security vulnerabilities.

Thrust 1: Attack Graph based Security Analysis

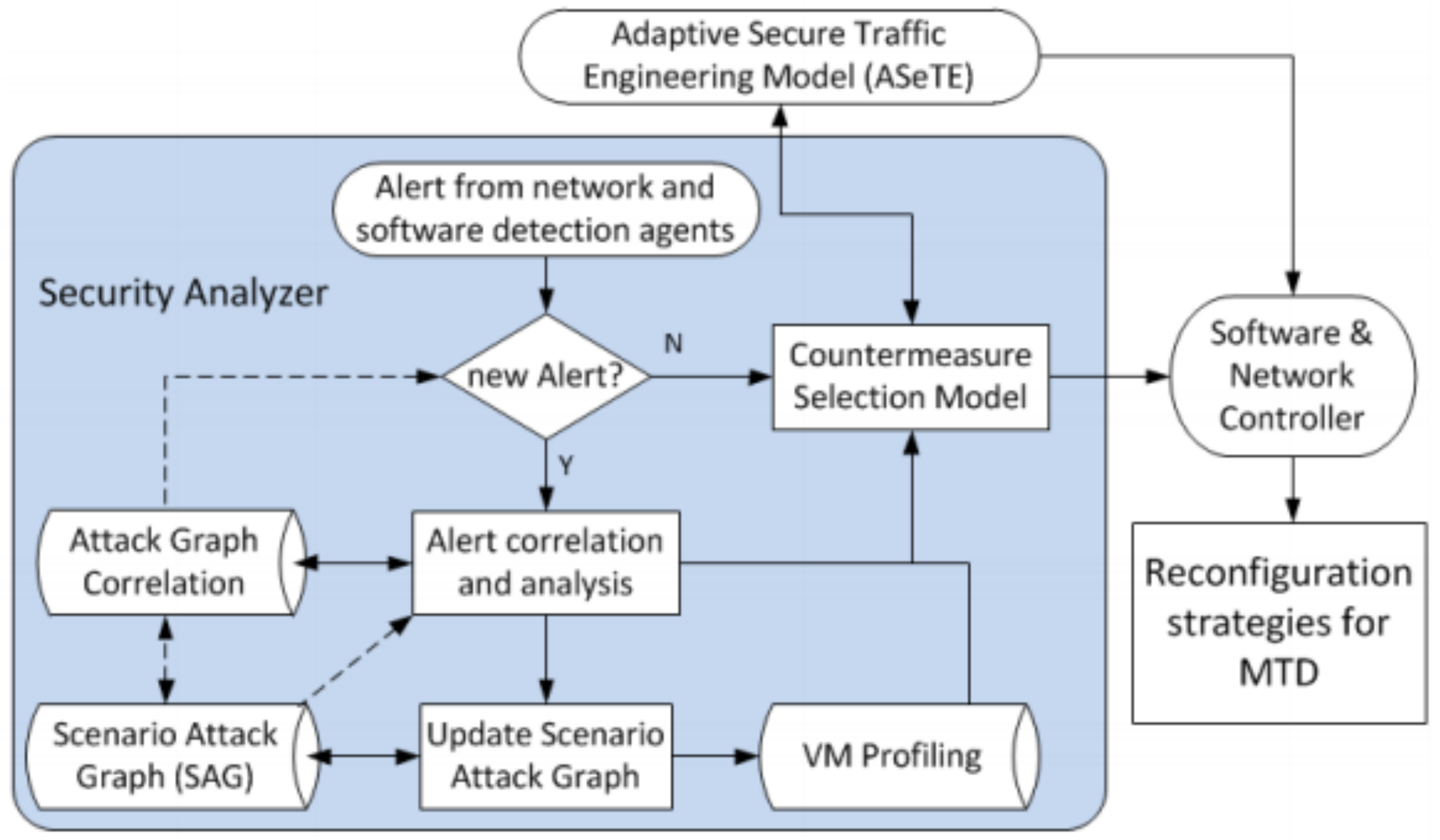
Adaptive Secure Traffic Engineering Model (ASeTE)
Security Analyzer
Alert from network and software detection agents
new Alert?
N
Y
Countermeasure Selection Model
Software & Network Controller
Reconfiguration strategies for MTD
Attack Graph Correlation
Alert correlation and analysis
Scenario Attack Graph (SAG)
Update Scenario Attack Graph
VM Profiling

Figure 3: Work flow of security analyzer.

- Attack Graph generation algorithms face state space explosion as the size of the network increases . Countermeasure selection based on effectiveness and deployment cost is a challenging task [1].
- Attack Graph generation based on reachability and vulnerability information using advanced clustering algorithms. An attack countermeasure tree from multiple attack graphs [2].
- A parallel computing approach such as Hadoop, Spark and security filtering appliance between virtual network zones to address scalability.
- Countermeasure selection based on cost/intrusiveness recommendations from ASeTE taking the network traffic QoS into consideration.

System Architecture

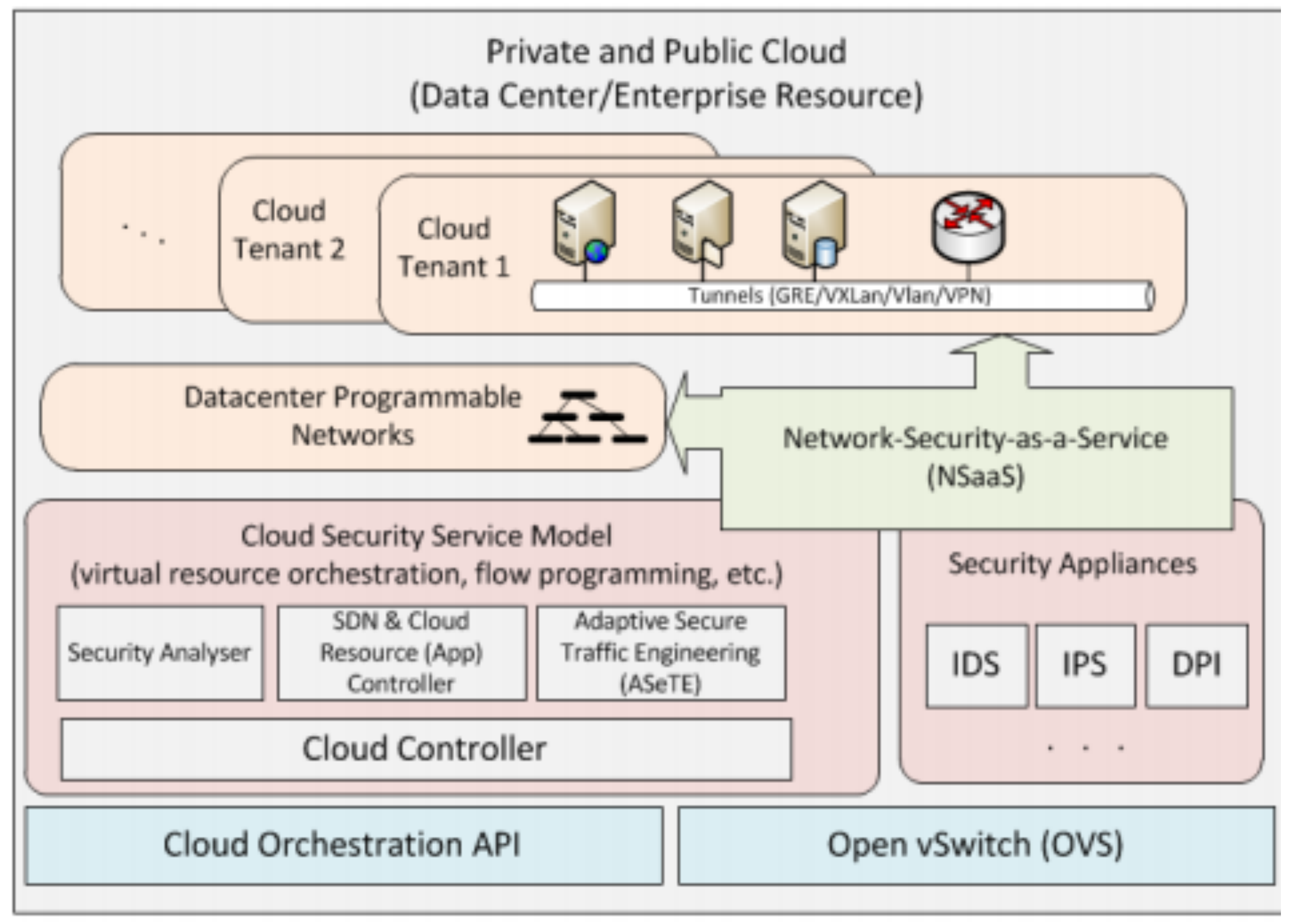
Private and Public Cloud
(Data Center/Enterprise Resource)
. . .
Cloud Tenant 2
Cloud Tenant 1
Tunnels (GRE/VXLan/Vlan/VPN)
Datacenter Programmable Networks
Network-Security-as-a-Service (NSaaS)
Cloud Security Service Model
(virtual resource orchestration, flow programming, etc.)
Security Analyser
SDN & Cloud Resource (App) Controller
Adaptive Secure Traffic Engineering (ASeTE)
Cloud Controller
Security Appliances
IDS
IPS
DPI
. . .
Cloud Orchestration API
Open vSwitch (OVS)

Figure 1: SRN system setup within one datacenter cluster.

Thrust 2: Security Enabled Traffic Engineering

- Virtual Network (VN) provisioning problem based on the attack graph deployment and scope of SRN, e.g., one scenario may require a new VM for tenants for Intrusion Prevention System(IPS). Another scenario may require new paths.
- Regularly scheduled virtual network provisioning based on review points and on demand provisioning to address attack countermeasures and vulnerabilities.
- Virtual Network provisioning based on factors such as system variation [3], cost based objective function variation.
- Traffic engineering to address network load balancing, VM load balancing, and availability.

Thrust 3: Software Vulnerability for MTD

- Detection and removal of software bugs and vulnerabilities is a vexing and difficult task. Software aging and environment dependent bugs –Mandelbugs [4] are difficult to reproduce.
- Analysis of environmental factors causing Mandelbugs and aging related vulnerabilities.
- Vulnerability classification into Bohr, Mandel, and aging related vulnerabilities, based on earlier NASA satellite bug classification.
- Incorporation of stochastic analysis and optimization techniques to study nature of vulnerability and security violation triggers.

Research Thrusts

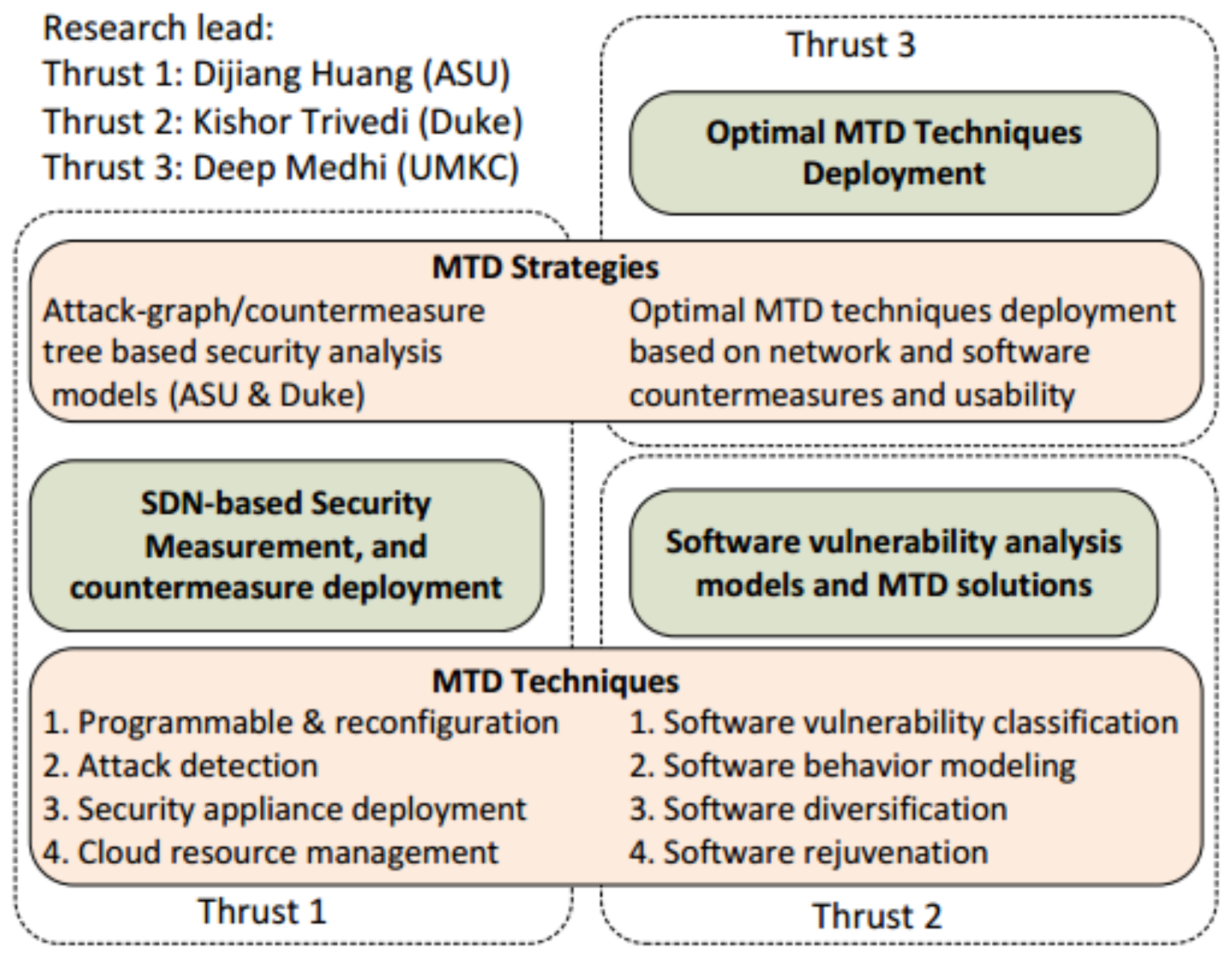
Research lead:
Thrust 1: Dijiang Huang (ASU)
Thrust 2: Kishor Trivedi (Duke)
Thrust 3: Deep Medhi (UMKC)
Thrust 3
Optimal MTD Techniques Deployment
MTD Strategies
Attack-graph/countermeasure tree based security analysis models (ASU & Duke)
Optimal MTD techniques deployment based on network and software countermeasures and usability
SDN-based Security Measurement, and countermeasure deployment
Software vulnerability analysis models and MTD solutions
MTD Techniques
1. Programmable & reconfiguration
2. Attack detection
3. Security appliance deployment
4. Cloud resource management
1. Software vulnerability classification
2. Software behavior modeling
3. Software diversification
4. Software rejuvenation
Thrust 1
Thrust 2

Figure 2: SRN Research Thrusts and relations.

SRN Testbed Deployment and Security Assessment

- Cross platform SRN testbed between ASU Mobicloud and NATO (security measurement platform between DUKE and ASU).
- Security Analyzer software package to provide a security analysis of the current security system status and predictions of future security related events.
- Network Controller to provide integrated management of both SDN software switches and software vulnerability evaluation models, and also provides visual aids security operators management and reconfigure network systems,
- ASeTE Manager to provide run-time traffic engineering and management based on a set of system performance measurement metrics while taking into considerations the security situations.

Project Products

Project demonstration site: https://mobsphere.asu.edu

Publications:

- Chun-Jen Chung, Tianyi Xing, Dijiang Huang, Deep Medhi, and Kishor Trivedi, “SeReNe: On Establishing Secure and Resilient Networking Services for an SDN-based Multi-Tenant Datacenter Environment”, *in Proceedings of the IEEE Workshop on Dependability Issues on SDN and NFV (DISN)*, 2015
- Jin B. Hong, Chun-Jen Chung, Dijiang Huang, Dong Seong Kim, “Scalable Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems”, *First International Symposium on Dependability in Sensor, Cloud, and Big Data Systems and Applications, Achieved in Algorithms and Architectures for Parallel Processing, Volume 9532, Lecture Notes in Computer Science, Pages 582-592, December,* 2015.
- Chun-Jen Chung, Tianyi Xing, Dijiang Huang, Deep Medhi, and Kishor Trivedi, “SeReNe: On Establishing Secure and Resilient Networking Services for an SDN-based Multi-Tenant Datacenter Environment”, *in Proceedings of the IEEE Workshop on Dependability Issues on SDN and NFV (DISN)*, 2015
- Ricardo J. Rodriguez, Xiaolin Chang, Xiaodan Li, and Kishor S. Trivedi, “Survivability Analysis of a Computer System under an Advanced Persistent Threat Attack”, in *proceedings of 3rd International Workshop on Graphical Models for Security*, June 2016, Lisbon, Portugal.
- José M. Martínez, Kishor S. Trivedi, and Benny N. Cheng. “Efficient Computation of the Mean Time to Security Failure in Cyber Physical Systems”. In Proceedings of the 10th EAI International Conference on Performance Evaluation Methodologies and Tools (VALUETOOLS 2016), Taormina, Italy, Oct 2016.
- Mirza Mohd Shahriar Maswood, Chris Develder, Edmundo Madeira, Deep Medhi, “Dynamic Virtual Network Traffic Engineering with Energy Efficiency in Multi-Location Data Center Networks,” in Proceedings of 28th International Teletraffic Congress, September 2016, Wurzberg, Germany.
- Duo Lu, Zhichao Li, Dijiang Huang, Xianglong Lu, Yuli Deng, Ankur Chowdhary, and Bing Li, “VC-bots: A Vehicular Cloud *Computing Testbed* with Mobile Robots*”, in Proceedings of ACM MobiHoc Workshop on Internet of Vehicles and Vehicles of Internet (IoV-VoI),* 2016.
- Zhiyuan Ma, Guangchun Luo, Dijiang Huang, “Short Term Traffic Flow Prediction Based on On-line Sequential Extreme Learning Machine”, *in proceedings of International Conference on Advanced Computational Intelligence*, 2016
- Abdullah Alshalan, Sandeep Pisharody, and Dijiang Huang, “MobiVPN: A Mobile VPN Providing Persistency To Applications”, in *Proceedings of 2016 International Conference on Computing, Networking and Communications, Wireless Networks (ICNC),* 2016.
- Xiaodan Li, Xiaolin Chang, Jose M. Martinez, John A. Board, Kishor S.Trivedi, “A Novel Approach for Software Vulnerability Classification”, *in proceedings of 2017 Annual Reliability and Maintainability Symposium (RAMS)*, January 2017, Orlando, Florida.