Name: Mohammed Alsaleh

Hard Problem Area: Resilient Architectures

Overall Research Goal(s):
As cyber complexity and vulnerability increases, cyber-attacks become highly sophisticated and stealthy. This makes attacks and breaches inevitable, and it will require defense mechanisms that are capable of both recovering from deliberate cyber-attacks, and limiting their consequences. Network resiliency is the property of the system to deter, resist, and mitigate attacks, rather than merely preventing them, in order to maintain the mission integrity of cyber systems. Many proactive and reactive resiliency techniques are proposed in the research literature to achieve this goal. However, no sufficient effort has been made to develop formal models and metrics to verify the safety, correctness, and effectiveness of such techniques in specific network environments.

The main goal in this work is to verify the resiliency of network configuration against cyber-attacks. Our proposed framework takes the specification of various types of resiliency techniques along with the complete network configuration, the system mission's requirements, and a set of resiliency metrics and verifies whether the techniques provide the expected resiliency for the system. We consider the network configuration as resilient if it satisfies the system's mission integrity and the resiliency techniques are effective against particular attacks.

Broad Impact:
The recent incidents of data breaches, such as the attacks on Target, SnapChat, and others reported in Verizon 2015 Data Breach Investigations Report, emphasize two important facts. First, cyber threats are becoming more sophisticated and attackers, motivated by money or politics, are always introducing innovations and sophisticated strategies, while defenders are lagging behind. Second, attacks and breaches are inevitable. This requires sophisticated defense mechanisms that are capable of both withstanding and recovering from deliberate cyber attacks by providing the means to manage the consequences of attacks and contain their impacts. Even if the network administrators are aware of the best practices or resiliency policies that should be employed in their networks, the complexity of current systems increases the likelihood of misconfigurations. This might create vulnerabilities that jeopardize the system's mission. In this work, we provide specification languages to describe the expected outcome on organizations as a result of resiliency mechanisms and verify whether they are met in a network configuration.

Specific Research Goals:
Proactive resiliency techniques, such as diversity, isolation, and redundancy, are usually statically integrated in the cyber architecture and configuration to create built-in attack resistance and enhance the system resiliency. Due to the increasing complexity of cyber configuration and inter-dependency between its components, it is hard to ensure that these
techniques are configured correctly and effectively. Our goal in this work is to develop models and properties to verify the effectiveness, integrity and consistency of proactive static resiliency based on access control configurations in traditional or software defined networks. To achieve this goal, we provide a verification framework that analyses the complete network configuration and verifies if given resiliency techniques are deployed correctly in the network and they satisfy certain resiliency properties. We implemented our framework on OpenFlow-based software defined networks.

Specifically, we focus on the static proactive resiliency techniques (i.e., diversity, isolation, and redundancy). Given the complete data plane of an OpenFlow network, a set of mission requirements expressed in a special specification language, and a set of resiliency metrics, we are proposing to verify that:
- Particular diversity and isolation patterns are enforced by the network configuration.
- The network mission is satisfied.
- The network configuration meets the specified resiliency metrics.

**Success Criteria:**
In this work, we believe there are two criteria to determine whether our research goals are satisfied:
- Applicability to practical network administrator's needs. We are proposing a specification language to define network mission's requirements, resiliency techniques and properties. The mission here is restricted to the infrastructure mission that is usually mapped from the network services requirements. This language should be flexible enough to express wide range of administrator's requirements.
- Efficient Verification. If our specification language can specify the network mission and resiliency properties, we need to design a scalable framework that can analyze complex network systems. It is well-known that verification models normally require high computing power. In our work, we need to model quantitative requirements and resiliency properties, which introduce another challenge. We believe our research is successful if we build a scalable framework that can analyze large-scale networks in a timely fashion.

**Anticipated Difficulties, Limitations, and Criticisms:**
In order to complete our research objectives, there are many research challenges that we need to address. The major challenges are as follows:
- Model Checking with Arithmetic Constraints. In order to model and verify requirements derived from the network mission, it is challenging to efficiently model and quantify arithmetic constraints to quantify the system's mission.
- Network devices heterogeneity. Isolation resiliency techniques depend on the deployment of different defense countermeasures in the network. We need to model different types of network devices in order verify isolation requirements.
- Scalability. Networks may consist of thousands of devices. Therefore, it is challenging to model this large number of devices along with their complete
configuration in order to verify the system mission’s requirements. The size of the network is proportional to the complexity of the transitions in our model checker.