From: **Michael Collins** mcollins@isi.edu
Subject: [Mten-workshop-pc] MTEN Workshop Proposal: Improving Network Monitoring Through Contracts
Date: August 22, 2022 at 8:44 AM
To: mten-workshop-pc@iab.org

Improving Network Monitoring Through Contracts

We propose _monitoring contracts_ as a mechanism to describe an asset's (in this context, any device connected to a network whose behavior is observable and controllable across this network) behavior to a network's security control infrastructure (_i.e._, policy enforcement tools such as firewalls, as well as the security operations team). A contract is a description of the expected behavior of an asset under different conditions. The behavior includes phenomena such as the frequency and servers contacted for software updates, open server ports, the expected volume over time, and what monitoring the asset will allow during emergencies.

The Role of Monitoring in Incident Response

The contract concept derived from our experience in managing these alerts by re-engineering networks for _detectability_. Detectability involves redesigning networks to make anomalous our hostile behavior more visible; this was motivated by our experience with the limits of machine-learning based anomaly detection[Gates06], in particular excessively high false positive rates. As an example of designing for detectability, consider the problem of detecting scanning by looking for failed connections to dark networks -- if the attacker assumes that addresses are linearly allocated (as they usually are), then the number of failed connections on a common port may be close to zero. However, if the network is allocated so that all assets in the network are evenly distributed within a much larger IP space, then the defender can identify a scanner quickly enough to automatically constrain them.

The motivation for developing these detection systems is to manage the _economy of attention_ which drives security operators. Operators have a limited focus relative to the number of incidents they must process daily, so operations is a constant triage process. By implementing security controls that mitigate obviously hostile behavior, we can free up analyst attention to focus on more complex and subtle phenomena.

In an economy of attention, the role of formal security controls such as firewall rules is to constrain obvious attacks. By providing a precise definition of an asset's behavior, a monitoring contract provides operators with multiple potential courses of action with the asset: the operator may decide to impose formal constraints on the system (_e.g._, firewall or HIDS rules), create anomaly definitions for monitoring (_e.g._, raise an alert if activity is seen on any port not specified by the contract), or not to allow traffic under the contract.

Specifying a Contract

To be effective, monitoring contracts must both describe traffic and deal with dynamic phenomena. In the interest of brevity, we will focus on the issue of dynamic phenomena. Briefly, we envision traffic descriptions as containing one or more fields from a flow specification, descriptions of allowable ranges of values and a specification for how long the contract is valid.

Dynamism is focused less on time and more on scenarios. Leveson notes that effective monitoring systems must accommodate for both normal operations and crises, such as security incidents [Leveson95]. Monitoring is dynamic; as noted above in our discussion on economy of attention, operator attention is limited and the amount of data collected is often far larger than what the operator can pay attention to. A common reaction during an incident is to reorganize and focus instrumentation in suspicious areas.

Consider two different categories of network data differentiated by risk: _personal_ and _control_. Attacks on personal data are attacks on confidentiality -- the risk is that personal data will spill PII, PHI or other information that damages a person. Attacks on control data are attacks on integrity; the risk is that control data is corrupted or inaccessible.

Safe control data requires multiple redundant monitoring systems in order to provide fallback when individual sensors fail and to monitor integrity if individual sensors are corrupted. In this environment, assuming encryption by default can reduce system safety. For example, consider a smart gas oven which is controllable via IFTTT (https://ifttt.com/hc_oven) -- in this case, control information which may include a substantial physical risk is only accessible by physically watching to the oven.

By making the difference between these two risk categories _explicit_, we can consider the issues of proactive protection and separation of both categories. Control traffic, for example, should be designed to be authenticated, and can be designed with constrained formal structures which limit the amount of information transferred. A monitoring contract may specify that some specific subset of information is control data, and will be sent using specific protocols and to specific sites.

Citations

- [Gates06]. Gates, C. and Taylor, C. Challenging the Anomaly Detection Paradigm A provocative discussion. Proceedings of the 2006 New Security Paradigms Workshop (NSPW). 2006.
- [Leveson95]. Leveson, N. Safeware: System Safety and Computers, 1st Edition. Addison-Wesley Professional, 1995.