Using Software Defined Networking to Achieve Network Security

Fred Smith, ANGEL Secure Networks

Outline of the Presentation

- How Auditing a High Performance Network Follows Traditional Concepts of Auditing
- How Auditing a High Performance DOE Network is Different than Traditional Auditing

How Auditing A High Performance Network Follows Traditional Concepts of Auditing

- The auditors determine that various management outputs are correct by examining and comparing the outputs with objective data not under the control of management.
- The fact that the outputs were prepared by duly authorized managers acting within the scope of their management duties is perhaps a necessary, but by no means sufficient, condition to pass an audit.
- Auditors need to examine whether the actions of managers are objectively correct, as determined by comparison with data not under the control of the managers.

How do we know what is “objectively correct” when we are talking about a high performance network?

- For business or university, “objectively correct” means that books presented to the public have to match the underlying reality of the enterprise.
- For a high performance network, “objectively correct” is a murkier concept.

How should we define “objectively correct” for purposes of an Audit of a High Performance DOE Network?

One approach (by no means the only approach)

1. Produce a threat tree.
2. Produce a network design that will deter and detect the threats in the threat tree and take appropriate action in response.
3. Have the design reviewed and approved by multiple parties.

Threat tree for a business or a university

- The enterprise is losing more money than is shown on the books (the books are cooked).
- Somebody is stealing money.
- The enterprise does not have adequate financial controls.

For businesses or universities, everybody knows what the threats are. You don't have to call it a threat tree.

Threat tree for a High Performance Network

- One approach is to say there are no threats.
- Another approach is to say there are no threats except threats that come from outsiders.
- Another approach is that yes, there are threats that come from insiders, but you cannot defend against insiders.
- Another approach is to say well, yes, there are threats, but we don't have any resources to defend against them, so we will wait until something happens.

All of the above are reasonable in some sense.

On the other hand…

- Perhaps it is painful, but it might be useful to at least list what the foreseeable threats are.
- Is it possible to defend against insiders?
- If it is possible, what might it cost, and how hard actually is it?

Threat tree for a DOE High Performance Network

1. Pollute data so an experiment has to be run again.
2. Pollute data so an experiment produces an incorrect although plausible result.
3. Bring down the network, so experimental data cannot be collected and is lost.
4. Ruin an experiment that will be vastly expensive to rerun.

The adversary could be someone who was careless, someone who had a grudge, or someone who wanted to cause harm to the US.

The adversary could be extremely capable. There could be a group of adversaries working together.

Is it possible to audit against insiders?

- A commercial audit is almost entirely an audit against insiders.
- The notion that there is no defense against insiders comes from the computer world and the military world.

How expensive is it to audit a high performance network that would include a defense against insiders?

- The audit would have to be conducted by automated methods.
- It is not necessary to audit everything, just a reasonable sample.
- The most important aspect might be to assure that no single individual had control over the audit.
- An adversary who wanted to cause embarrassment to the US might tend to pick a target perceived to be poorly defended.

These do not appear to be extremely expensive requirements. Assuming the adversary has political motives, appearing to have some defense is much better than appearing to have no defense.

Nuts and bolts of an audit of a high performance network

1. Write a threat tree. Does not have to be elaborate.
2. Write a statement of what the state of the network should be to assure the threats are avoided. Does not have to be complete.
3. Get approval from multiple sources for this statement.
4. The approved statement defines "objectively correct" for a particular high speed network.
5. Find ways to audit automatically to determine whether the network is objectively correct.

Ideally, there would be multiple ways to implement item 5, which could be randomly selected at the time of the audit, so that an adversary would not know exactly what to defend against.

How does SDN fit into the question of auditing a high performance network?

- On the one hand, SDN may increase visibility into the network components that make up a high-speed network, and thereby facilitate automated auditing of a high speed network.

- On other hand, if SDN allows an administrator to configure a network with a single command, an adversary might have the ability to switch rapidly to an unsafe configuration, which might increase the danger of an attack.

What software is needed to conduct an automated audit of a high performance network?

- A highly capable adversary will attempt to distort the results of an audit.
- The auditing software needs, as its first priority, a capability that it cannot easily be reverse engineered by an adversary.
- Our suggestion is that auditors set up a highly secure network of software agents that check on one another.
- Also, that audit be conducted on a “surprise” basis so that the adversary does anticipate when the audit will take place or what data will be examined.

Contact Information

Fred Smith
Director of R&D
ANGEL Secure Networks
20 Godfrey Drive
Orono, Maine 04473
207 866 6537 office
207 992 6289 mobile
fredsmith@angelsecurenetworks.com