Interface to Network Service Functions (I2NSF) Working Group

IETF-95, Buenos Aires
Thursday April 7, 2016
17.30 - 19.30 (two hours)
Room: Quebracho B

Chairs:
Linda Dunbar linda.dunbar@huawei.com
Adrian Farrel adrian@olddog.co.uk
AD:
Kathleen Moriarty kathleen.moriarty.ietf@gmail.com
Acting AD:
Alia Atlas akatlas@juniper.net

=======

Introduction from the Chairs:

Provided a summary of where the WG standards with respect to our immediate milestones. A little concerned about being late, and keeping up (or increasing) our momentum.

Good step: Even though a month late, the Problem statement and use cases have been adopted. Gap analysis has been adopted.

Milestone is overdue for Framework. We must concentrate on getting the framework and terminology statement ready for adoption by the WG; this is overdue. Worried about four upcoming milestones (extensions to protocols, existing secure communication mechanisms, and info model in June, and data models in July).

We want to do milestones IN ORDER (with the exception of the info model). Must contribute to previous milestones BEFORE we work on new ones.

--- Working Group Drafts ---

Problem Statement and Use Cases: Sue Hares: draft-ietf-i2nsf-problem-and-use-cases-00

Sue recommends the draft is ready for WGLC, because no comments have been received. Wants people to say ON THE MAILING LIST they have read and understood it.

Adrian asked about the Management Considerations section. Dan Romascanu said that he thought that this is OK.

John Strassner offered to do a thorough review and send to the mailing list. Sue promised to initiate a sector review for the draft.

Chairs: suggest comments on mailing list.

Gap Analysis: Sue Hares, draft-ietf-i2nsf-gap-analysis-00

Thanks to Myo Zarny's comments. Helped getting the terminology document going. The framework draft is now aligned to the terminology document, but wants WG to agree with this.

Dan Romascanu would like data modeling and data models to be added to this draft. Sue said OK. However, she is concerned about the current turmoil in opstate.

John Messenger asked why IEEE802.1 Security (802.1ax and 802.1ar) were not covered; this will be added in. Bob, John, and Dan will review for Sue.

Robert Moskowitz: IEEE802.1AR may have a role in I2NSF.

Sue asked: Who can review the document? LuYuan, John Messanger, John Strassner and Dan R , also Frank Xia raised hands.

--- Drafts for Immediate Milestones ---

Terminology: John Strasner - draft-hares-i2nsf-terminology-00

Purpose is to enable precise and consistent terminology to be used, and that I2NSF terminology does not clash with accepted applicable terminology from relevant domains. The document was created by scanning existing WG documents looking for key terms.

Status: security and policy terminology are reasonably complete for I2NSF purposes. Included terms to facilitate implementation; Sue met with SACM terminology editor (Henk) and they came up with a preliminary list of terms that need alignment. John gave some examples, but the conclusion is that both SACM and I2NSF could benefit from such co-working and alignment.

While related, two separate documents (one from SACM and one from I2NSF) will continue to exist. We will work together to ensure that they do not conflict

Jabber: can you discuss the similarity and differences between SACM and I2NSF terminologies, instead of copy and paste?

Adrian: While we developed the terms, it is good to have it in one place. However, we should publish it in only one place. Duplicate definitions are not good.

Bob: It will not be one line of differences.

John: we will align to SACM terminology draft. WE will make good progress,

Adrian: How many terms are different?

Henk: We have identical terms (~10), and then we have logical terms.

Adrian: We have a document with 2 terms.

Henk: The terms that are defined from RFC4949. We should make sure our differences are very specifically defined. I am on the side of separate documents.

John Strassner: I happy to work with what ever the working group states. Authentication and Authenticate were differentiated. In RFC4949 you said that authenticate, [John Strassner please edit this statement]

IN RFC3539, if an entity reported who the reports state.

Bob: RFC4949 says the same thing as well. "Attribute" is a general attribute in RFC4949.

SACM is working the definition is applying the definition.

Adrian: This tells me separate document.

Framework: Diego Lopez - draft-merged-i2nsf-framework-05

Reviewed high-level architecture. Diego prefers to use "developer" instead of "vendor" for the registration

Major changes:

- Clarified packet- and flow-based processing
- Changes Subject-Object-Action-Function to ECA
- defined policy rule, event, condition, action, and how each of these are used in I2NSF
- Removed references to PCIM (doubts about flaws associated with PCIM)
- clarified that we want to standardize the form and function of profiles and signature files while concurrently enabling vendor-specific elaborations of each
- added capability layer interface details
- added vendor-facing interface details
- Updated to use terms in Terminology Draft
- added security requirements

Additional discussion:

- There are three types of interfaces: configuration, signaling, and rule provisioning
- Diego showed a nice mapping of how different functions (e.g., how context and constraints) are mapped to ECA

- Brief discussion about the "v" in vNSF. Starting to lean towards NOT explicitly separating vNSF from pNSF (physical NSF).

However, it was noted that some problems that are unique to vNSFs (e.g., restart, having policies follow an NSF, having multiple vNSFs collectively enforce policies)

- We have covered controller-NSF; should we consider client-controller as well? Should we elaborate on differences between rules for the capability vs. service layers? What about capability negotiation?

- Question about security controller. Diego clarified that this was NOT the typical "reactive" controller. It needs to be smarter, to translate capabilities and constraints to NSFs. Question from someone about "is this a controller" or not. John replied that it MAY be more instructive to think of this as a continuum - it is called "controller" because of the real-time nature of the decision, but it could be constructed as management.

- Open discussion

Still need to determine if it is "Flow-based NSF" or "packet-based NSF".
mohamed.boucadair@orange.com: Just defining, a policy does not work. We should stick to network data structure.
Diego: I am glad you say so. I think are converging.
Bob Moskowitz: How are the security issues that impact the virtual NSF versus the physial NSF.
Diego: The protection of the secrets is good.
....
Diego: Should we consider the connection.
Sumandra Megee (F5): I like what you put up on the framework.
Diego: This is for the controller to feed the function. The controller gets to this type of capabilities to the general capabilities to handle.
Sumndra Megee (F5): [missed] what are the events? which makes me a little nervous
Diego: The events are defined by you. The security controller is not reactive controller.

Sumandra : when software who write controller, they have specific feature in mind.

John Strassner: this is a classical terminology debate: real time matter qualifies the entity to be "controller" instead of "management".

Sue: I2RS WG also uses the "ECA" model.

Preliminary poll for adoption

draft-hares-i2nsf-terminology-00
draft-merged-i2nsf-framework-05

Adrian: is there anyone object adopting those two drafts to WG drafts? No one object.
No one disagrees; therefore, the poll will go to the list.

--- Interfaces and Information Models ---

Capability Interface Information Model: Frank Xia - draft-xia-i2nsf-capability-interface-im-04

This draft is about how to monitor what is going on in the I2NSF architecture, and is more about designing the information model for the capability interface for NSF. It will realize the security policy provisioning rules that govern how packets are treated by the I2NSF framework. This decouples the network security controller from vendor-specific NSFs, and avoids unnecessary constraints on using the functionality of NSFs.

There are three categories of security functions:
- Network security control (inspecting and processing packets and flows using ECA)
- Content security control (e.g., detect and remediate against malicious contents); needs standardized input/output parameters
- attack mitigation control (detect and remediate against different types of network attacks); needs a standardized interface

Showed a functional logic diagram of how ECA works. Basically, when an event fires, this triggers the evaluation of the condition. If the condition is then true, then the action MAY be executed. Note that each clause may in general be a complex Boolean expression.

Discussed the various tables and grammar.

Next Step: solicit comments, and add more detail on capabilities, constraints, and how to extend the associated information model.

Sumandra Megee stood at the microphone to ask question

Adrian: Due to we are running out of time. Please discuss after the session or on the mailing list

User-group-based Security Policy for Service Layer: John Strassner - draft-you-i2nsf-user-group-based-policy-01

Key point: this is an extensible identifier to identify user groups. It will be generated by policies under operator control, and takes the form of roles plus additional criteria. This provides operators flexibility in making policy decisions by decoupling what identifies a user from a static representation of a user in the network.

Dan Romascanu: There was no time to ask this question in the room, but I asked side-wise John: Why not use roles? the concept of superposing domains becomes trivial if multiple roles are used.
John replied that it is roles plus some other information, with the collection of information being controlled by policies.

Information Model for Security Policy Exchange: Luyuan Fang (Microsoft): draft-fang-i2nsf-inter-cloud-ddos-mitigation-api

We currently lack an efficient, automated, standard way to exchange security information between providers. The problem is at the boundary between providers. If this point is compromised, then both providers, and especially inter-cloud operations, are also compromised.

Note that this is much harder to handle. It is very difficult to identify the attacker as well as the status of a provider's partners; there is a distinct lack of automated tools to exchange attack-related data, as well as to support coordinated remediation.

We need a standardized set of inter-provider APIs for network security policy exchange, so that providers can create and deploy their tools on top of this standard framework. This in turn requires an information model. Four types of information: mitigation capabilities, mitigation request and response, monitoring and reporting, and knowledge sharing.
Want to try and define knowledge sharing objects.

John said that an info model is vital, but in order to define semantics,
you MAY need ontologies and/or some formal type of logic (such as the
ISO Common Logic (24707) work).

Doug Montgomery: How does this related to TAXI/STIX.
Adrian: Coordination is required and will happen. It needs to be coordinated.
Tobias: DOTS co-chair. If you have concerns, please send them to the mail list.
Luyuan: We come with a problem, and we need a solution.
Linda: The I2NSF is about the security policy from one entity (domain) to another domain. The DOTS is about the signaling among DDoS mitigation, especially between DDoS client and the DDoS servers.
Kathleen: I can help the coordination with TAXI/STIX. Taxi - is a bunch of transports
STIX - is closer.

--- Monitoring related subjects --

Information Model for Monitoring NSFs: Dacheng Zhang (presented by Frank Xia as DaCheng couldn't make it to Argentina). draft-zhang-i2nsf-info-model-monitoring-00

This draft specifies the information model for the monitoring part of the capability interface. Want to concentrate on alarm and report messages. The model will include common information that should be included in all alarms and reports (e.g., NSF name, vendor name, timestamps, type of NSF, NSF model,...); preliminary definitions of each were shown.

--- Other Work ---

Remote Attestation Procedures for Virtualized NSFs: Diego Lopez - draft-pastor-i2nsf-vnsf-attestation

Showed a diagram explaining what the principles of attestation are. Create a trusted channel, then users and the security controller mutually authenticate to establish a trusted connection with the security controller, which then makes the attestation available to the user.

Next version will include a deeper discussion on procedures,

Dan R: why isn't this merged into the framework?

Diego: it could be; at the least, a reference should be there. However, this draft contains additional information that goes beyond the scope of the framework.

Dan R: why not incorporated this into the framework

Diego: the framework started before this work started. It could be. At the least, a reference should be there. However, this contains additional information that goes beyond the scope of the framework.

SDN-Based Security Functions: Jaehoon (Paul) Jeong - draft-jeong-i2nsf-sdn-security-services-04

The main goal is to show how we use the I2NSF framework to achieve the security services.

Described updates from -03 to -04:

- Added new use case (VoIP/VoLTE) and two new requirements.

Described an OpenFlow-based architecture for a VoIP IPOS based on ODL. The experiment in general follows the layers described in the framework draft. Next steps: provisioining of the service- and capability layers, and provide more details about the prototypes.

I2NSF Data Flow Requirements & Secure Session Layer Services: Sue Hares: draft-hares-i2nsf-mgtflow-reqs

Working on management data flow. Thought about different types of attacks, such as TCP-SYN and ICMPO attacks. What could I2RS do to help, and what could simplify the protocol?

DOTS and Mile have a set of management traffic requirements. These place a set of important requirements on the flow of management data. I2RS has some complementary requirements. A potential solution (in draft-hares-i2nsf-ssls) describes placing a function above the many transports being used so that a management entity can choose the **best** transport to use.

draft-hares-i2nsf-ssls-00

```
Sue: We need input on the security requirements from I2NSF
Adrian: thank you for going quick.
```

Security alerts over the first MILE: Robert Moskowitz: draft-moskowitz-firstmile

No standard mechanism exists to inform NSF about the policies for dealing with security alerts in the monitoring system. Also, no mechanism exists for NSF to report these alerts/events to the

Monitoring system.

Note that this is different than DOTS (DDoS alerting/mitigation) and MILE (inter-admin defense coordination). There are many other attacks (e.g., Ping of death, TCP SYN, port scan, ...). In addition, we need to be able to report events when the network itself is under attack.

We need a pub-sub reporting system and a registration of defense system monitoring entities.

Sue stated that the pub-sub work is being done in I2RS.