Federated Autonomic Network Access Control

Simon N. Foley, William M. Fitzgerald and Wayne Mac Adams

Department of Computer Science, University College Cork, Ireland
email: s.foley@cs.ucc.ie, wfitzgerald@4c.ucc.ie, w.macadams@4c.ucc.ie

Ontologies for NAC Configuration

OWL-DL ontologies are developed for iptables, TCP-Wrapper and XMPP application-level firewalls.

Linux iptables Firewall Ontology Excerpt

The *IPTRule* concept defines an iptables rule as being composed of a rule index, exactly one chain, one or more filter conditions and a single permission action.

$$\begin{aligned} \mathit{IPTRule} \equiv\ & \exists_{=1} \mathit{hasIndex}.\mathit{Integer} \sqcap \\ & \exists_{=1} \mathit{hasChain}.\mathit{ChainType} \sqcap \\ & \exists_{\geq 1} \mathit{hasGenericFilter}.\mathit{Condition} \sqcap \\ & \exists_{=1} \mathit{hasAction}.\mathit{Action} \end{aligned}$$

Example Invalid TCP Packet Filtering

The following iptables rule, drops packets identified as part of the XMAS TCP port scan where TCP flags `FIN`, `PSH` and `URG` are simultaneously set.

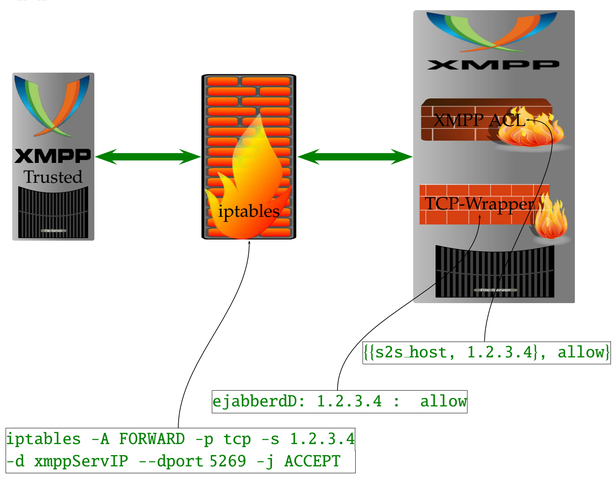
```
iptables -A FORWARD -p tcp --tcp-flags
    FIN,PSH,URG FIN,PSH,URG -j DROP
```

This firewall rule is represented as:

$$\begin{aligned} & \mathit{IPTRule}(\mathtt{iptr}_{\mathtt{DropXMAS}}) \\ \leftarrow\ & \mathit{hasChain}(\mathtt{iptr}_{\mathtt{DropXMAS}}, \mathtt{forward}) \sqcap \\ & \mathit{hasProtocol}(\mathtt{iptr}_{\mathtt{DropXMAS}}, \mathtt{tcp}) \sqcap \\ & \mathit{hasTCPFlagCheck}(\mathtt{iptr}_{\mathtt{DropXMAS}}, \mathtt{fin\_psh\_urg}) \sqcap \\ & \mathit{hasTCPFlagSet}(\mathtt{iptr}_{\mathtt{DropXMAS}}, \mathtt{on}) \sqcap \\ & \mathit{hasAction}(\mathtt{iptr}_{\mathtt{DropXMAS}}, \mathtt{drop}) \end{aligned}$$

Sample Configuration

Server-to-Server federation is permitted with XMPP server (IP address 1.2.3.4). The XMPP server is protected by a gateway firewall, a locally hosted firewall and XMPP's own application-level ACL firewall.



Ontology for NAC Configuration

The security mechanism topology is represented as:

$$\begin{aligned} & \mathit{Service}(\mathtt{ejabberd}) \\ \leftarrow\ & \mathit{protectedBy}(\mathtt{ejabberd}, \mathtt{xmppACL}) \sqcap \\ & \mathit{protectedBy}(\mathtt{ejabberd}, \mathtt{tcpwrapper}) \sqcap \\ & \mathit{protectedBy}(\mathtt{ejabberd}, \mathtt{iptables}) \end{aligned}$$

The iptables access-control rule is represented as:

$$\begin{aligned} & \mathit{IPTRule}(\mathtt{iptr}_{\mathtt{AllowIP1.2.3.4XMPPPkt}}) \\ \leftarrow\ & \mathit{hasChain}(\mathtt{iptr}_{\mathtt{AllowIP1.2.3.4XMPPPkt}}, \mathtt{forward}) \sqcap \\ & \mathit{hasProtocol}(\mathtt{iptr}_{\mathtt{AllowIP1.2.3.4XMPPPkt}}, \mathtt{tcp}) \sqcap \\ & \mathit{hasSrcIP}(\mathtt{iptr}_{\mathtt{AllowIP1.2.3.4XMPPPkt}}, \mathtt{ip1.2.3.4}) \sqcap \\ & \mathit{hasDstIP}(\mathtt{iptr}_{\mathtt{AllowIP1.2.3.4XMPPPkt}}, \mathtt{xmppServIP}) \sqcap \\ & \mathit{hasDstPort}(\mathtt{iptr}_{\mathtt{AllowIP1.2.3.4XMPPPkt}}, 5269) \sqcap \\ & \mathit{hasTarget}(\mathtt{iptr}_{\mathtt{AllowIP1.2.3.4XMPPPkt}}, \mathtt{accept}) \end{aligned}$$

The TCP-Wrapper access-control is represented as:

$$\begin{aligned} & \mathit{TCPWrapperRule}(\mathtt{twr}_{\mathtt{Allow1.2.3.4XMPPPkt}}) \\ \leftarrow\ & \mathit{hasDaemon}(\mathtt{twr}_{\mathtt{Allow1.2.3.4XMPPPkt}}, \mathtt{ejabberdD}) \sqcap \\ & \mathit{hasClient}(\mathtt{twr}_{\mathtt{Allow1.2.3.4XMPPPkt}}, \mathtt{ip1.2.3.4}) \sqcap \\ & \mathit{hasAction}(\mathtt{twr}_{\mathtt{Allow1.2.3.4XMPPPkt}}, \mathtt{allow}) \end{aligned}$$

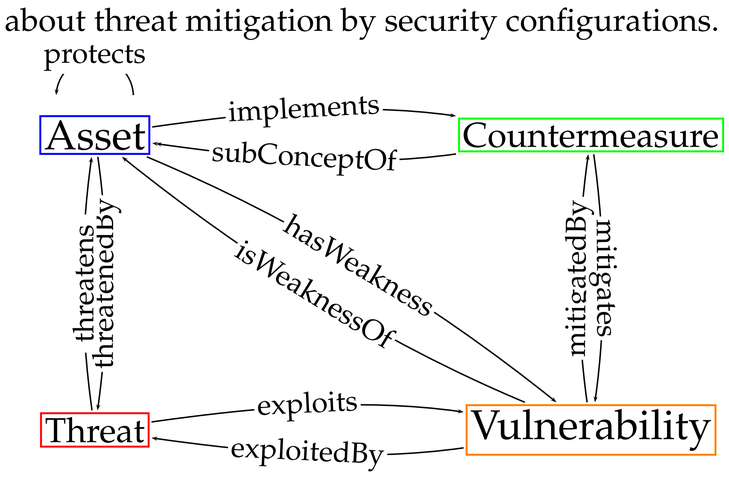
The XMPP access-control rule is represented as:

$$\begin{aligned} & \mathit{ACLRule}(\mathtt{xmppr}_{\mathtt{Allow1.2.3.4XMPPPkt}}) \\ \leftarrow\ & \mathit{federateWith}(\mathtt{xmppr}_{\mathtt{Allow1.2.3.4XMPPPkt}}, \mathtt{ip1.2.3.4}) \sqcap \\ & \mathit{hasPermission}.(\mathtt{xmppr}_{\mathtt{Allow1.2.3.4XMPPPkt}}, \mathtt{allow}) \end{aligned}$$

Managing Security Configuration

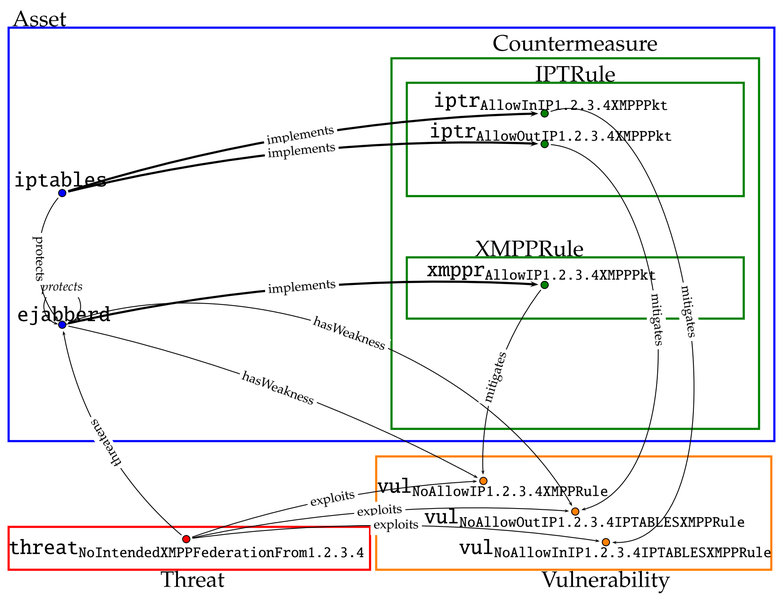
Semantic Threat Graphs

Semantic Threat Graphs are used to model knowledge about threat mitigation by security configurations.



Example Semantic Threat Graphs

XMMP Federation Whitelist Recommendations



Catalogues of Best Practice

Built ontologies for NIST-800-41, NIST-800-41rev1, NIST-800-45v2, NIST-800-44v2, RFC1918, RFC3330, XEP-0205.

Sample Ontology Excerpt for NIST-800-41

iptables Firewall Example

ID	Recommendation Description		
FBP-1	Deny *"Inbound or Outbound traffic from a system using a source address that falls within the address ranges set aside in RFC1918 as being reserved for private networks"*[NIST-800-41].		
	Threat	**Vulnerability**	**Countermeasure**
	$\mathtt{threat}_{\mathtt{Inbound192.168.0.0/16SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenInbound192.168.0.0/16PktToFW}}$	$\mathtt{iptr}_{\mathtt{DropIn192.168.0.0/16SrcIPPktInputChain}}$
	$\mathtt{threat}_{\mathtt{Outbound192.168.0.0/16SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenOutbound192.168.0.0/16PktFromFW}}$	$\mathtt{iptr}_{\mathtt{DropOut192.168.0.0/16SrcIPPktOutputChain}}$
	$\mathtt{threat}_{\mathtt{Inbound192.168.0.0/16SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenInbound192.168.0.0/16PktToHost}}$	$\mathtt{iptr}_{\mathtt{DropIn192.168.0.0/16SrcIPPktForwardChain}}$
	$\mathtt{threat}_{\mathtt{Outbound192.168.0.0/16SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenOutbound192.168.0.0/16PktFromHost}}$	$\mathtt{iptr}_{\mathtt{DropOut192.168.0.0/16SrcIPPktForwardChain}}$
	$\mathtt{threat}_{\mathtt{Inbound10.0.0.0/8SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenInbound10.0.0.0/8PktToFW}}$	$\mathtt{iptr}_{\mathtt{DropIn10.0.0.0/8SrcIPPktInputChain}}$
	$\mathtt{threat}_{\mathtt{Outbound10.0.0.0/8SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenOutbound10.0.0.0/8PktFromFW}}$	$\mathtt{iptr}_{\mathtt{DropOut10.0.0.0/8SrcIPPktOutputChain}}$
	$\mathtt{threat}_{\mathtt{Inbound10.0.0.0/8SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenInbound10.0.0.0/8PktToHost}}$	$\mathtt{iptr}_{\mathtt{DropIn10.0.0.0/8SrcIPPktForwardChain}}$
	$\mathtt{threat}_{\mathtt{Outbound10.0.0.0/8SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenOutbound10.0.0.0/8PktFromHost}}$	$\mathtt{iptr}_{\mathtt{DropOut10.0.0.0/8SrcIPPktForwardChain}}$
	$\mathtt{threat}_{\mathtt{Inbound172.16.0.0/12SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenInbound172.16.0.0/12PktToFW}}$	$\mathtt{iptr}_{\mathtt{DropIn172.16.0.0/12SrcIPPktInputChain}}$
	$\mathtt{threat}_{\mathtt{Outbound172.16.0.0/12SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenOutbound172.16.0.0/12PktFromFW}}$	$\mathtt{iptr}_{\mathtt{DropOut172.16.0.0/12SrcIPPktOutputChain}}$
	$\mathtt{threat}_{\mathtt{Inbound172.16.0.0/12SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenInbound172.16.0.0/12PktToHost}}$	$\mathtt{iptr}_{\mathtt{DropIn172.16.0.0/12SrcIPPktForwardChain}}$
	$\mathtt{threat}_{\mathtt{Outbound172.16.0.0/12SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenOutbound172.16.0.0/12PktFromHost}}$	$\mathtt{iptr}_{\mathtt{DropOut172.16.0.0/12SrcIPPktForwardChain}}$
ID	**Recommendation Description**		
FBP-2	Deny *"Inbound traffic containing ICMP (Internet Control Message Protocol) traffic"*[NIST-800-41].		
	Threat	**Vulnerability**	**Countermeasure**
	$\mathtt{threat}_{\mathtt{ICMPNetworkScan}}$	$\mathtt{Vul}_{\mathtt{InfoDisclosureICMPReplyPktFromFW}}$	$\mathtt{iptr}_{\mathtt{DropInICMPPktInputChain}}$
	$\mathtt{threat}_{\mathtt{ICMPNetworkScan}}$	$\mathtt{Vul}_{\mathtt{InfoDisclosureICMPReplyPktFromHost}}$	$\mathtt{iptr}_{\mathtt{DropInICMPPktForwardChain}}$

TCP-Wrapper Firewall Example

ID	Recommendation Description		
FBP-1	Deny *"Inbound or Outbound traffic from a system using a source address that falls within the address ranges set aside in RFC1918 as being reserved for private networks"*[NIST-800-41].		
	Threat	**Vulnerability**	**Countermeasure**
	$\mathtt{threat}_{\mathtt{Inbound192.168.0.0/16SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenInbound192.168.0.0/16PktToFW}}$	$\mathtt{twr}_{\mathtt{DropIn192.168.0.0/16Pkt}}$
	$\mathtt{threat}_{\mathtt{Inbound10.0.0.0/8SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenInbound10.0.0.0/8PktToFW}}$	$\mathtt{twr}_{\mathtt{DropIn10.0.0.0/8Pkt}}$
	$\mathtt{threat}_{\mathtt{Inbound172.16.0.0/12SrcIPPkt}}$	$\mathtt{Vul}_{\mathtt{UnAuthenInbound172.16.0.0/12PktToFW}}$	$\mathtt{twr}_{\mathtt{DropIn172.16.0.0/12Pkt}}$

Sample real-world anti-bogon iptables firewall rules

Countermeasure	iptables Rule
$\mathtt{iptr}_{\mathtt{DropIn192.168.0.0/16SrcIPPktInputChain}}$	`iptables -A INPUT -i eth0 -s 192.168.0.0/16 -j DROP`
$\mathtt{iptr}_{\mathtt{DropOut192.168.0.0/16SrcIPPktOutputChain}}$	`iptables -A OUTPUT -o eth0 -s 192.168.0.0/16 -j DROP`
$\mathtt{iptr}_{\mathtt{DropIn192.168.0.0/16SrcIPPktForwardChain}}$	`iptables -A FORWARD -i eth0 -s 192.168.0.0/16 -j DROP`
$\mathtt{iptr}_{\mathtt{DropOut192.168.0.0/16SrcIPPktForwardChain}}$	`iptables -A FORWARD -o eth0 -s 192.168.0.0/16 -j DROP`
$\mathtt{iptr}_{\mathtt{DropIn10.0.0.0/8SrcIPPktInputChain}}$	`iptables -A INPUT -i eth0 -s 10.0.0.0/8 -j DROP`
$\mathtt{iptr}_{\mathtt{DropOut10.0.0.0/8SrcIPPktOutputChain}}$	`iptables -A OUTPUT -o eth0 -s 10.0.0.0/8 -j DROP`
$\mathtt{iptr}_{\mathtt{DropIn10.0.0.0/8SrcIPPktForwardChain}}$	`iptables -A FORWARD -i eth0 -s 10.0.0.0/8 -j DROP`
$\mathtt{iptr}_{\mathtt{DropOut10.0.0.0/8SrcIPPktForwardChain}}$	`iptables -A FORWARD -o eth0 -s 10.0.0.0/8 -j DROP`
$\mathtt{iptr}_{\mathtt{DropIn172.16.0.0/12SrcIPPktInputChain}}$	`iptables -A INPUT -i eth0 -s 172.16.0.0/12 -j DROP`
$\mathtt{iptr}_{\mathtt{DropOut172.16.0.0/12SrcIPPktOutputChain}}$	`iptables -A OUTPUT -o eth0 -s 172.16.0.0/12 -j DROP`
$\mathtt{iptr}_{\mathtt{DropIn172.16.0.0/12SrcIPPktForwardChain}}$	`iptables -A FORWARD -i eth0 -s 172.16.0.0/12 -j DROP`
$\mathtt{iptr}_{\mathtt{DropOut172.16.0.0/12SrcIPPktForwardChain}}$	`iptables -A FORWARD -o eth0 -s 172.16.0.0/12 -j DROP`

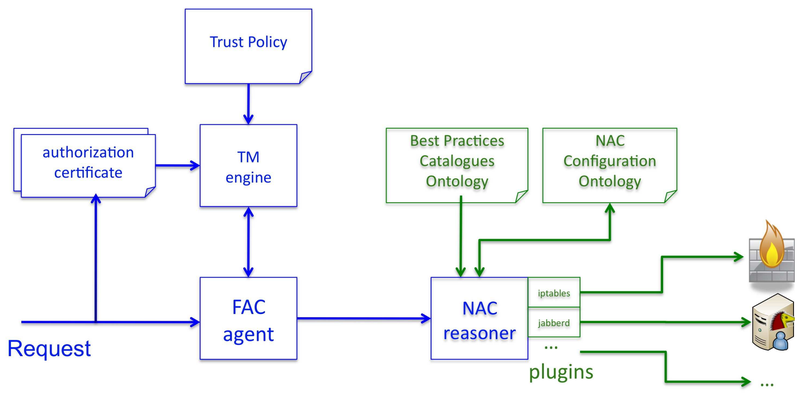
These catalogues are searchable:

- Generate firewall and application-security configurations that mitigate identified threats.
- Analyse a firewall and application-security configuration's effectiveness at mitigating identified threats.

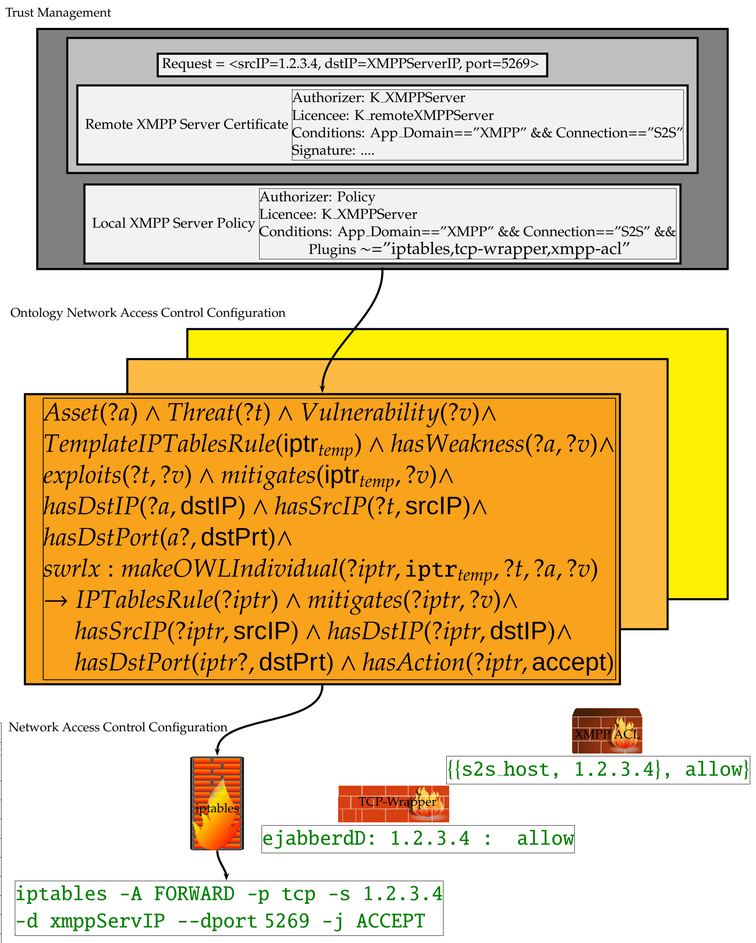
FANAC Prototype

A FANAC Agent is developed to accept remote requests to reconfigure the Network Access Controls. The current prototype focuses on S2S XMPP federaation network access control (re) configuration.

Architecture



Scenario



† This research has been supported by Science Foundation Ireland grant 08/SRC/11403.