Delegating Network Security with More Information

{“Stanford”: [“Jad Naous”, “Ryan Stutsman”,
    “David Mazières”, “Nick McKeown”],
“MIT CSAIL”: [“Nickolai Zeldovich”]}
Context

- Roberto
- Alicia
- Carlito
Context

Alicia
Policies Alicia Wants

• Skype only to Skype
• email clients only to email server
• Only Roberto can use openssh ver < 5.0
• Allow R&D machines to talk anywhere in net, but not Sales
Common Problem

Alicia does not have all information necessary
Simple Solution

Ask!
Who should Alicia ask?

- Ask the whole path between sender and destination.
- Each network along the path might have different information (e.g. authenticated user)
- Augment responses along the path
- Communicate any relevant information
- Let the Alicia decide what to use
What information might Alicia want?

- username and authenticated usernames
- Application name, type, hash, version, ...
- OS information, patches, ...
- Network name, type, location, security, ...
- Application expected behavior, network rules, destination rules, ...
Soliciting Information: ident++

Proposal for requesting information:

1. Ask for more information for every new flow.

2. Arbitrary user/admin-definable key-value pairs

3. Networks along the path augment responses
Example: e-mail

👩‍💻 Mail-server accessed by mail clients only
👩‍💻 Thunderbird is the only mail client allowed
👩‍💻 Only users authenticated by the network are allowed access.
Example: e-mail

Data Flow
From 192.168.0.1:2358
To 192.168.1.1:25
Payload
Example: e-mail

Query
From 192.168.0.1:2358
To 192.168.1.1:25

Query
From 192.168.0.1:2358
To 192.168.1.1:25
Example: e-mail

Response
From 192.168.0.1:2358
To 192.168.1.1:25
-app-name: thunderbird
-version: 2.0.3
-user: roberto
-type: email-client

Response
From 192.168.0.1:2358
To 192.168.1.1:25
-app-name: cyrus
-user: imap
-type: email-server
Example: e-mail

Response
From 192.168.0.1:2358
To 192.168.1.1:25
-app-name: thunderbird
-version: 2.0.3
-user: roberto
-type: email-client
-authed-user: roberto

Response
From 192.168.0.1:2358
To 192.168.1.1:25
-app-name: cyrus
-user: imap
-type: email-server
Example: e-mail

Data Flow
From 192.168.0.1:2358
To 192.168.1.1:25
Payload
Example: evil e-mail

Response
From 192.168.0.1:2358
To 192.168.1.1:25
-app-name: thunderbird
-version: 2.0.3
-user: roberto
-type: email-client
-authed-user: unknown

Response
From 192.168.0.1:2358
To 192.168.1.1:25
-app-name: cyrus
-user: imap
-type: email-server
Example: evil e-mail
Example: e-mail

Client Configuration File:
@app /usr/bin/thunderbird {
  name    : thunderbird
  version : 2.0.3
  type    : email-client
}

Backbone Firewall Rules:

block all
pass all
  with eq(@src[type],
           email-client)
  with eq(@dst[type],
           email-server)
  with eq(@src[name],
           thunderbird)
  with not eq(@src[auth-user],
               unknown)
Extended PF language

- $PF+=2$ Allows flexible policies based on query results (key-value pairs)

- Extensible via arbitrary functions.
Trust and Delegation

• We delegate every day
• Makes lives easier
• Delegate to trusted people
• Trust levels vary so delegation levels vary
Example: e-mail
Example: e-mail

😊 Mail-server accessed by mail clients only
😭 Thunderbird is the only mail client allowed
_only users authenticated by the network are allowed access._
How it is done today

Alicia, Carlito, and David get together, coordinate, and then change the rules.

An easier way?
Example: e-mail

Data Flow
From 192.168.0.1:2358
To 192.168.1.1:25
Payload
Example: e-mail

Query
From 192.168.0.1:2358
To 192.168.1.1:25

Query
From 192.168.0.1:2358
To 192.168.1.1:25
Example: e-mail

Response
From 192.168.0.1:2358
To 192.168.1.1:25
-app-name: thunderbird
-version: 2.0.3
-user: roberto
-type: email-client

Response
From 192.168.0.1:2358
To 192.168.1.1:25
-app-name: cyrus
-user: imap
-type: email-server
-rule: only from email-client
Example: e-mail

Response
From 192.168.0.1:2358
To 192.168.1.1:25
-app-name: thunderbird
-version: 2.0.3
-user: roberto
-type: email-client
-authed-user: bob

Response
From 192.168.0.1:2358
To 192.168.1.1:25
-app-name: cyrus
-user: imap
-type: email-server
-rule: only from email-client
-rule: thunderbird only
Example: e-mail

Data Flow
From 192.168.0.1:2358
To 192.168.1.1:25
Payload
Example: e-mail

Server Configuration File:
```
@app /usr/bin/cyrus {
    name : cyrus
    type : email-server
    rule :
        block all
        with not eq(@src[type],
                     email-client)
}
```

Backbone Firewall Rules:
```
block all
pass all
    with allowed(@dst[rules])
    with not eq(@src[auth-user],
                 unknown)
```
Third-Party Delegation

• Another Example
  – Allow users to run any application as long as it conforms to rules signed by trusted third-party
  – Rules can be downloaded by user and stored locally.
  – Security devices check signatures before accepting rules.
Summary

• If you don’t know, ask!
• Trust and delegation intertwined (be careful who you delegate to or what information you trust)
• ident++ delegation enabler, says nothing about trust
Questions?

This work was funded partially by an NSF grant.