[STIF]

Security Tools
Integration Framework

or

the insights on

automated hacking

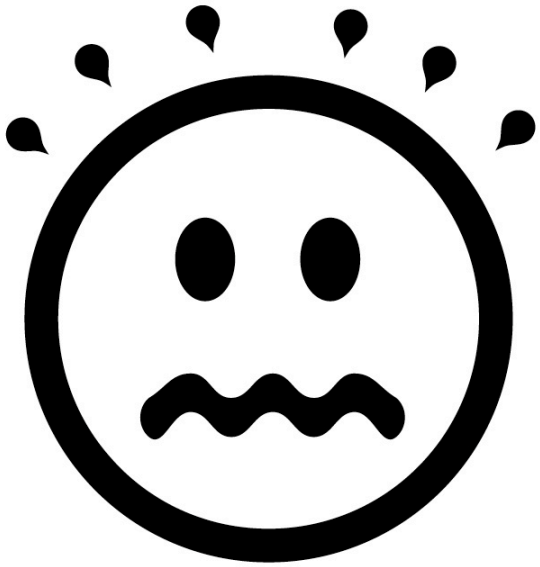
STIF

Security Tools

Integration Framework

“Sick”urity Industry

Dedicated to all victims of the “security” industry



STIF
Security Tools
Integration Framework

Why hacking automation…?

Why automation?

• boring/repetitive actions could be scripted out (intelligent mass hacking)

•Automated “intrusion detection” facilities could be tested using ‘real-life’ tools

•Deployed in intelligent agent based software

•Could be used to mitigate ‘human error’ factor

Other, “INFOSEC-biz” influenced:

• Pen-testing – slavery (can keep your boss happy)

• Saves more time for ‘fun’ stuff

• Your system “hack” while you sleep (or code)..

STIF

Security Tools

Integration Framework

Why integration?

Why integration?

- Numerous security tools available, but no unified framework for data exchange and representation
- No facility for machine data analysis, aggregation and correlation
- Repetitive manual handling for large-scale networks is a nightmare
- Integration into autonomous ‘network-propagating’ agents

STIF

Security Tools

Integration Framework

Example

Example

A **security analyst** runs a set of network discovery tools to map the network

*/usage of word **hacker** is not recommended in this context/*

He reviews the produced log files, based on what he finds out and remembers, he picks up further

“network-discovery” tools to use.. Repeat..

PROBLEMS: boring, tiring, non-productive use of time

STIF

Security Tools

Integration Framework

Why not let machine do the boring work…

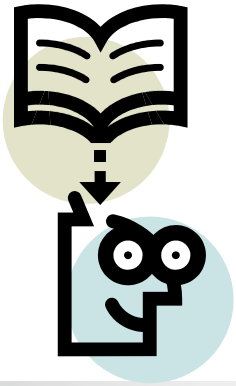
STIF

Security Tools

Integration Framework

Possible solutions

Possible solutions…



- Shell scripts?
- Security Scanners?
- Exploit toolkits??

- …or room of pen-testing “monkeys..?

STIF

Security Tools

Integration Framework

Or.. Please meet STIF!!

Meet STIF

Our ultimate automated

Monkey for your networking

Needs!

Our design goals

- Simplicity of adding and integrating new tools/”w4r3z” (no extra code hacking)
- Ability to script out different scenarios
- Ability to guide and “direct” the execution monkey in the right direction (by providing “knowledge” facts, that monkey may miss)

STIF

Security Tools

Integration Framework

Implementation

Implementation

Data format unification and integration module

encapsulation of data into set of messages, that we will refer as ‘STIF-Message’ throughout this presentation.

Inference engine

Data exchange, aggregation, correlation, rule-based execution scenarios

Unification components

Unified components execution and data import mechanisms

STIF

Security Tools

Integration Framework

What is a STIF message..

What is it?

Encoded fact of knowledge regarding target

System or network…

TARGET (target address=192.168.1.1)

PORT (port 80 state=open address 192.168.1.1)

PLATFORM (platform linux address 192.168.1.1)

APPLICATION …

URL/FILE LOCATION

…(add yours)

STIF
Security Tools
Integration Framework

STIF-Message …

Serialized STIF message in XML format..

STIF-Message

```
<STIF-Message created="2004-09-02T15:03:01+6">
  <Port number="80" state="open" protocol="tcp">
    <Address type="ipv4-addr">192.168.1.1</Address>
    <Protocol>
      HTTPS
      <Application>
          Apache/1.3.27 (Unix) PHP/4.3.1
      </Application>
    </Protocol>
  </Port>
</STIF-Message>
```

Implementation (cont)

Inference engine

assists the data exchange process between the tools

provides data aggregation and correlation facilities (including regular expressions based matching to the knowledge base facts)

Knowledge base maintenance

Maintains execution flow using rule-based scenarios

STIF

Security Tools

Integration Framework

Implementation

(cont)

Implementation

Unification components

Provides unified methods for execution of integrated tools and
Inference engine knowledge base system data import

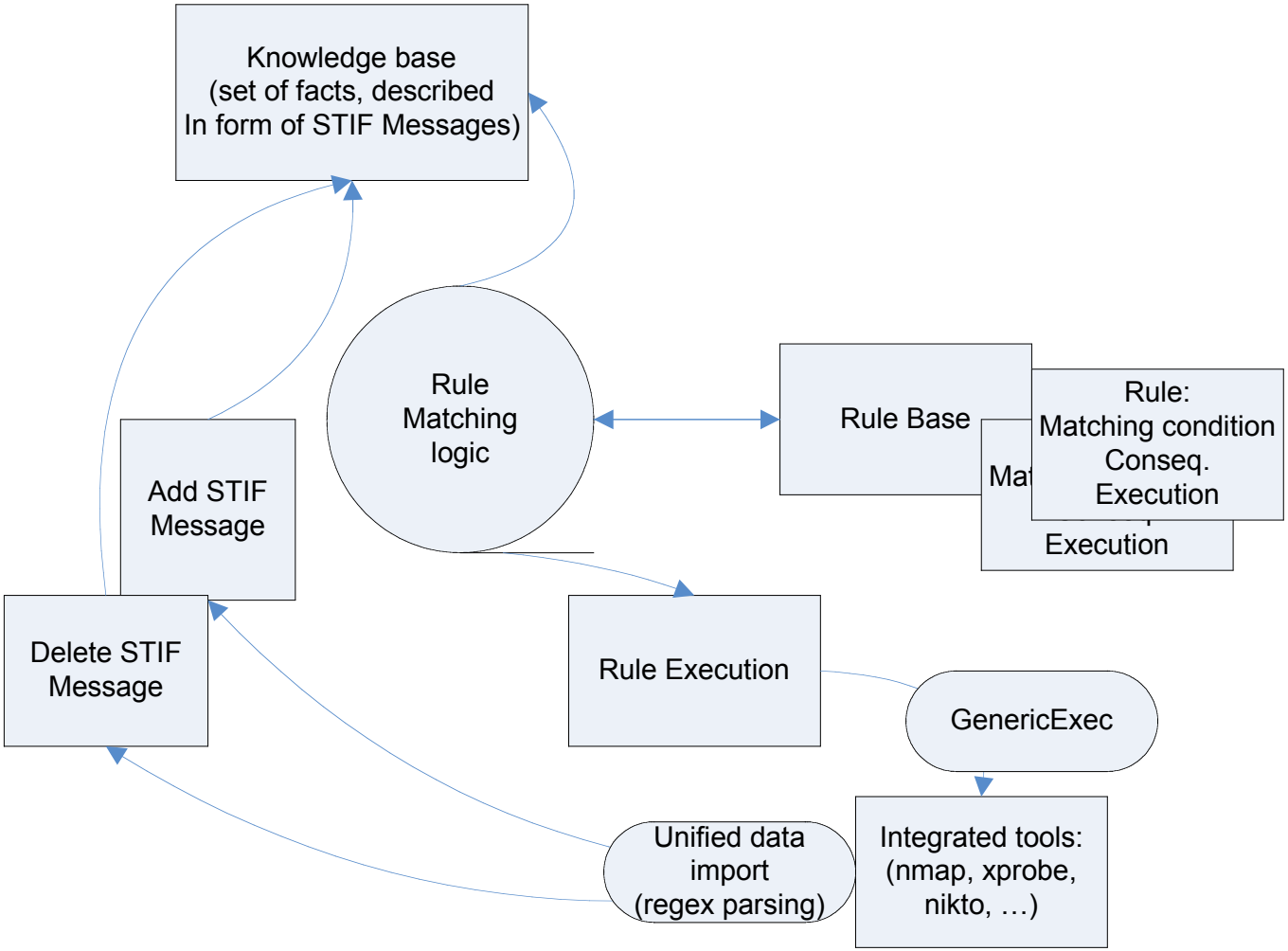
STIF

Security Tools

Integration Framework

How it glues

How it glues together



STIF

Security Tools

Integration Framework

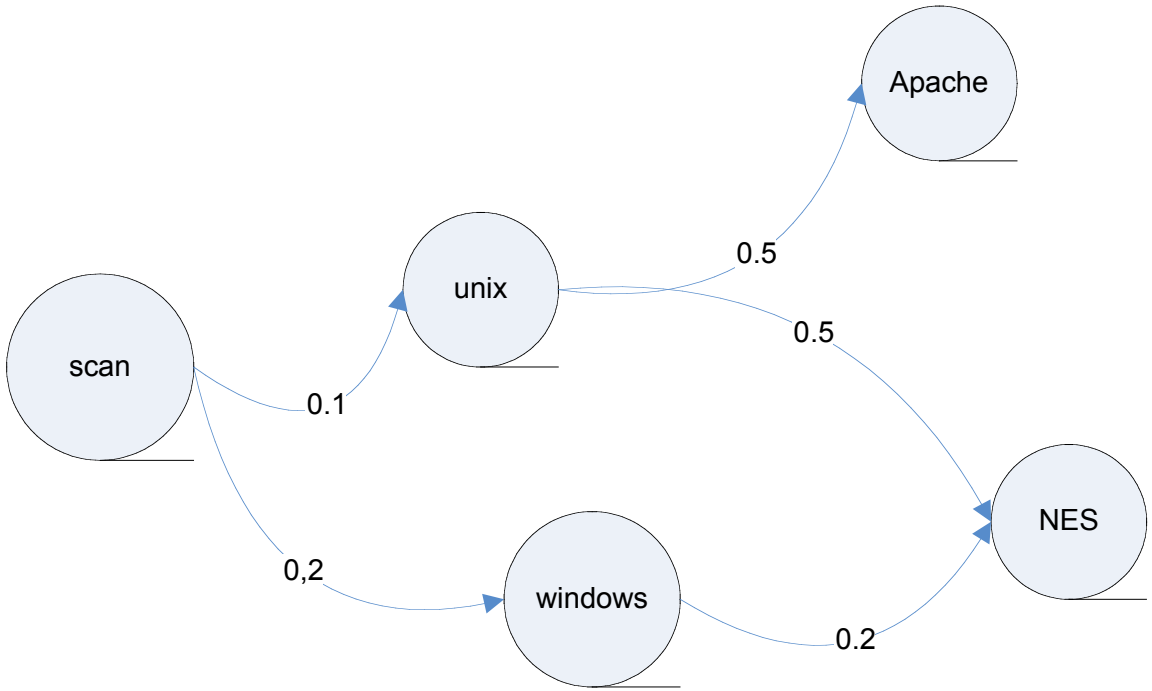
demonstration

demo

Other thoughts

Weight-based rule based systems

(implementation of Markov chains of probabilistic execution flows)



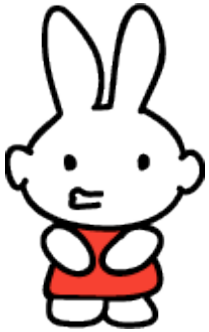
STIF

Security Tools

Integration Framework

Feedback

Questions and comments…



fygrave@o0o.nu

meder@o0o.nu

http://o0o.nu

STIF

Security Tools

Integration Framework

The End

Thanks!