SEMESTER PROJECT

ATTACK CRAWLER FOR MODERN NETWORKED SYSTEMS

Supervisors:

Yves Roudier
Ludovic Apvrille

Students:

Vo Huynh Dan
Truong Quang Huy

AGENDA

- Introduction

- Stuxnet Model

- Client-Server Protocol

- External Search Module on TTool

- Demo

- Conclusion

INTRODUCTION

- **Goal**
  - Extract relevant information of threads from Internet sources.
  - Develop a crawler for collecting data of vulnerabilities
  - Integrate the data into Ttool.

- **Time**
  - 1st Semester : Modeled operation of Stuxnet.
  - 2nd Semester :Designed and implemented a protocol for TTool and the Crawler.

STUXNET MODEL

Model con Stuxnet 6 slides 7 phut

Cach lam sao ?

+ mo ta tong quan ve mo hinh: mo hinh gom nhung gi, root attack …..

+

Lay cai hinh ra noi ket qua

Noi 4 cai hinh

STUXNET MODEL

STUXNET MODEL
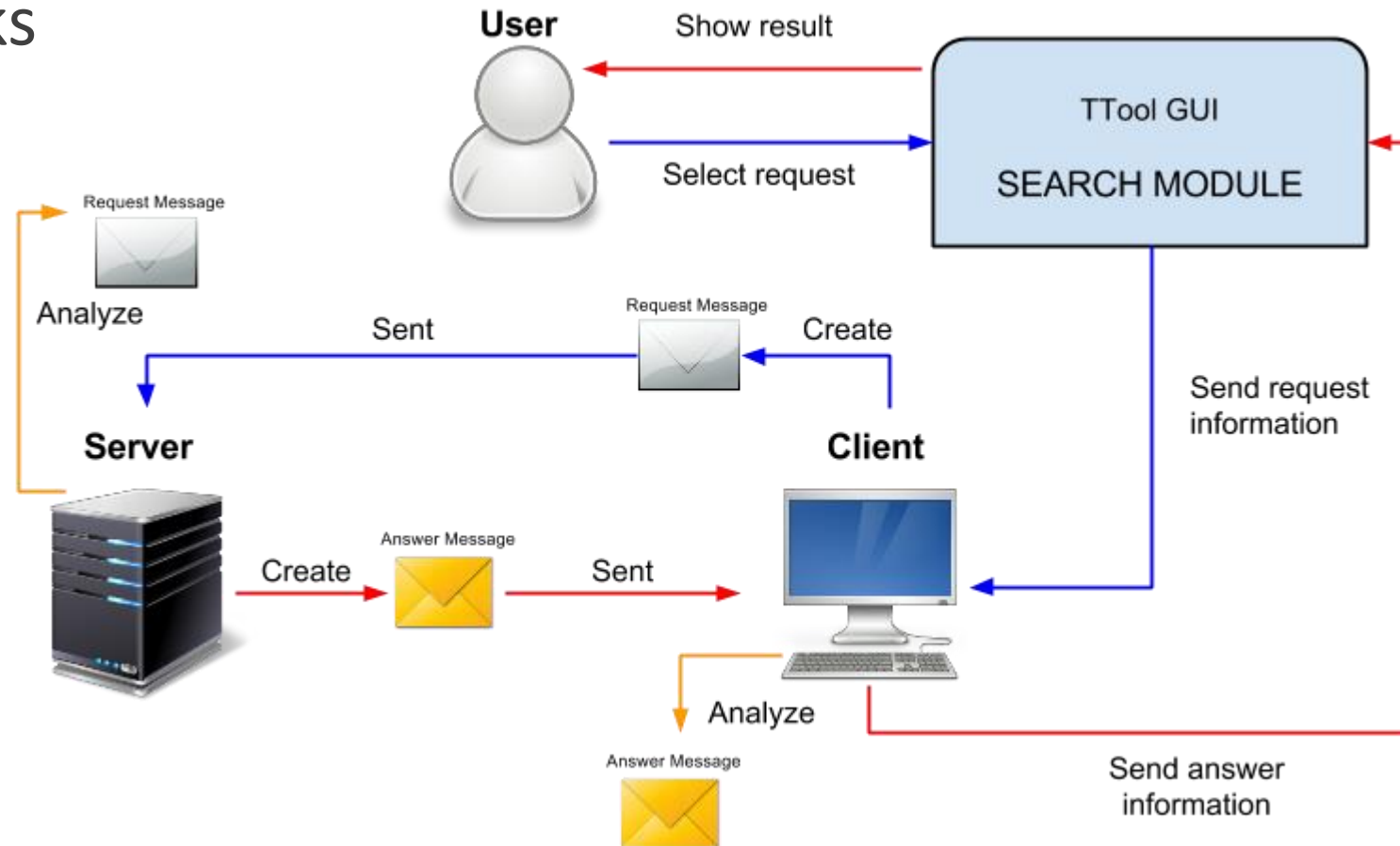
STUXNET MODEL

STUXNET MODEL

STUXNET MODEL

CLIENT-SERVER PROTOCOL

- Objective
  - Connect TTool and Web Crawler database.
  - Exchange information.
  - Secure the information.

- Design
  - Clients – Server
    - Client code is integrated in Ttool.
    - Multithread server.
    - SSL Socket.
  - Message

CLIENT-SERVER PROTOCOL

■ How it works

CLIENT-SERVER PROTOCOL

Structure of a message

Request Message

CLIENT					
cmd	Search				
content					
options	Keyword	Year	System	Score	NoR
values	Stuxnet	This year	Linux	7-8	10

Answer Message

	SERVER
cmd	SearchResult
content	Result from the server in XML format

EXTERNAL SEARCH MODULE

Objective
- Provide an interface allowing users interact with database server and search engine.
- Integrated in TTool source code.
- Design
- A JDialog named External Search.
- Support interaction with components in a diagram.
- Interact with Google Search engines.
- Take advantage of Ttool existing functions.

EXTERNAL SEARCH MODULE

Google Search features

◦ Use Jsoup library

Database Search features

EXTERNAL SEARCH MODULE

Database Search features

DEMO

Show interface

Chay client server

Chay chuc nang search hien hinh anh

SSL

CONCLUSION

Conclusion 1 slide 1p

Finish

knowledge

Future