“Hacker-Web - Securing Cyber Space”

Faculty- Salim Hariri, Youssif Al-Nashif

Collab. Faculty - Hsinchun Chen, Ronald Breige, Tom Holt - Michigan State University

Graduate Student – Karan Chadha

Project URL - http://acl.ece.arizona.edu/projects/current/scs/index.html

Intro/Background

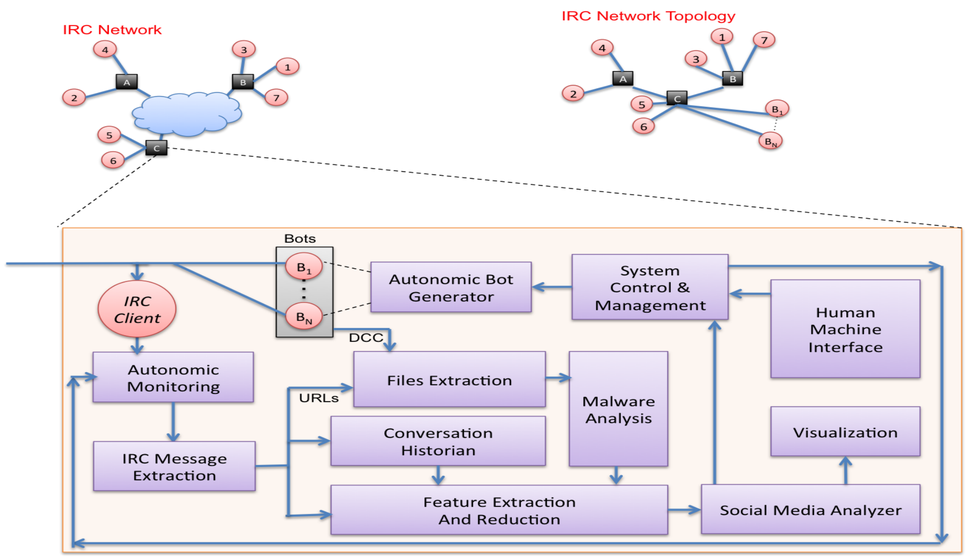
- Detect, classify, measure and track the formation, development and spread of topics, ideas, and concepts in cyber attacker social media communication.
- Identify cyber criminals interests, intent, sentiment, and opinions in online discourses.
- Induce and recognize hacker identities, online profiles/styles, communication genres, and interaction patterns

OBJECTIVES

- Develop autonomic monitoring and analysis of **IRC** hacker messages.
- Build an IRC test bed, to experiment with and evaluate the effectiveness of our tools and algorithms.
- Collect and analyze hacker messages
- Identifying and using IRC based botnet.

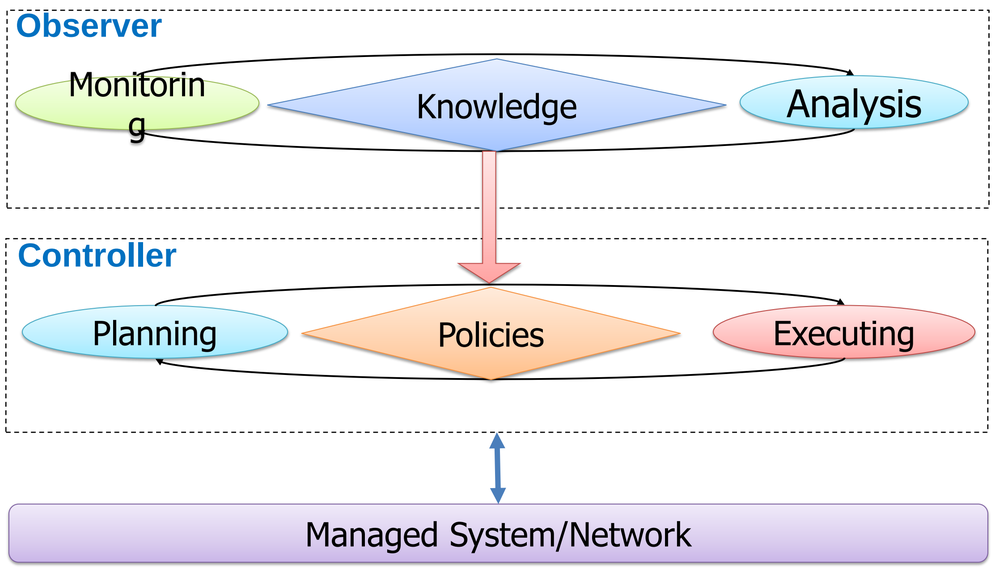
Solution

IRC Client based technique



To autonomize any software module or resource, we add two software modules: **Observer and Controller**

- The Observer is used for sensing and analyzing the current state of managed system and predict its behavior.
- The controller executes recommended actions to keep the managed system operating normally (self-manage).



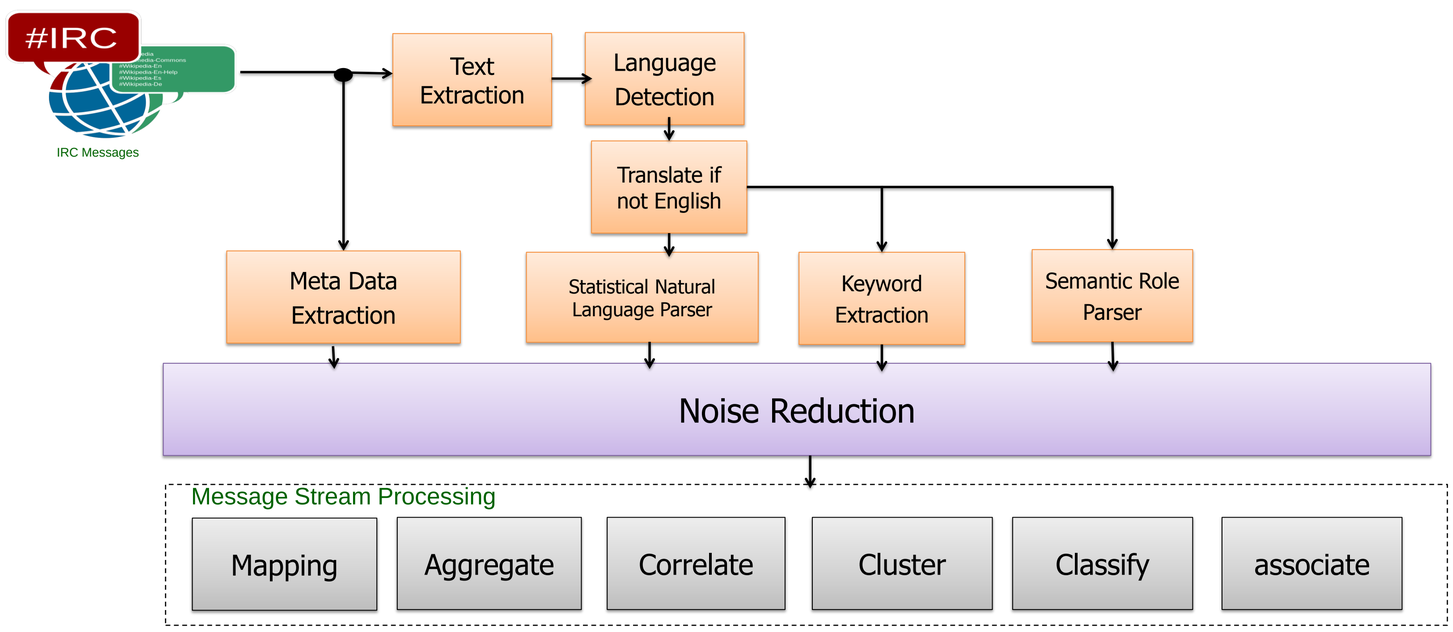
Method/Results

IRC message extraction

- Creating botnet over the network to log and extract the text, files and URL’s from the channel chats.

```
* jabber_420 (jabber_420@Test-D7A3CF8.ece.arizona.edu) Quit (Client exited)
* jabber_420 (jabber_420@Test-D7A3CF8.ece.arizona.edu) has joined #test
<jabber_420> Hey Everyone !!
<@kkkk> good morning ACL lab
<@kkkk> Hello everyone
<@kkkk> Hey Jabber
<@kkkk> hey jabber
<jabber_420> hey
<@kkkk> how are you doing ?
<jabber_420> I am doing good ! how about yourself ?
```

Feature extraction and reduction from IRC messages



- Using the Automatic semantic role labelling which automates the FrameNet approach (a lexical database of English that is both human- and machine-readable, based on annotating examples of how words are used in actual texts)

  Eg [$_{\text{Cook}}$ the boys] ... GRILL [$_{\text{Food}}$ their catches] [$_{\text{Heating\_instrument}}$ on an open fire].

Conclusion

Current work includes extraction of information from the IRC messages which would be stored in a database for later retrieval and analysis.

After completing with the IRC message extraction module, the future tasks will include

Task 1: Deploying open source malware analysis tools.

Task 2: Developing the System Control and Management component.

Task 3: Developing the Autonomic Bot Generator module.

Task 4: Testing and Evaluation of the previous tasks

This work is partially supported by AFOSR DDDAS award # FA9550-12-1-0241, and NSF awards IIP-0758579, DUE-1303362 and SES-1314631.

Cloud and Autonomic Computing Center

THE UNIVERSITY OF ARIZONA