New Approach to Recognition of VoIP Attacks from Honeypots

Miroslav Voznak, Jakub Safarik
voznak@ieee.org

Campus network monitoring and security workshop
Prague, April 24-25, 2014

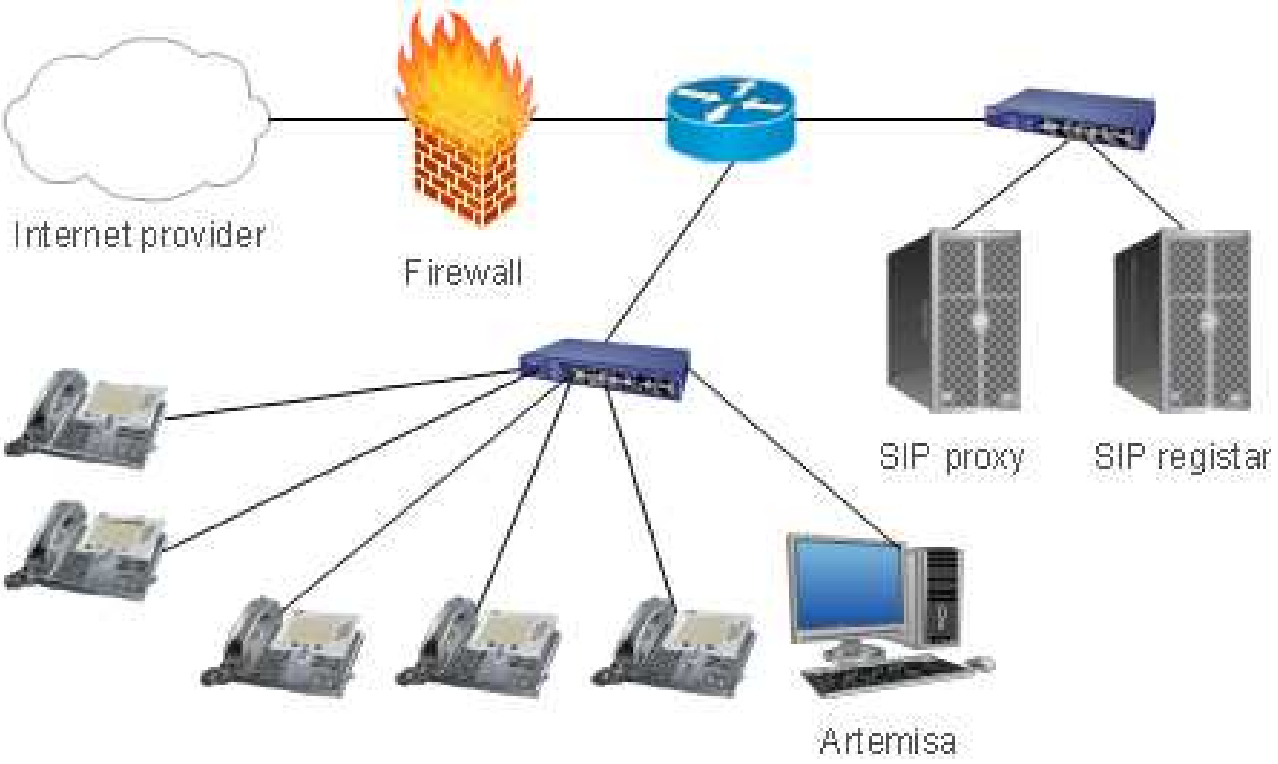
Introduction

- honeypots and usability tests
- DoS attacks and anomalies detection in SIP infrastructure
- Honeypot network concept
- MLP Neural network
- Practical Implementation
- Conclusion

Artemisa

- Artemisa plays a role of a regular SIP phone

•The programme connects to SIP proxy with the extensions defined in a configuration file.



CESNET

Artemisa

- Once the call is established on one of Artemisa extensions, the honeypot simply answers the call.

- At the same time, it starts to examine the incoming SIP messages. Artemisa then classifies the call and saves the result for a further review by the security administrator

- Artemisa looks for fingerprints of well-known attack tools

Artemisa

- Then it checks domain names and SIP ports on the attacker side.
- There is also a similar check for media ports.
- Requested URI are also checked.
- Finally, Artemisa checks the received RTP stream – (audio can be stored in a WAV format).

Artemisa

- The result is then shown in a console and can be saved into a pre-defined folder or sent by e-mail.

- Once the call has been examined, a series of bash scripts is executed (with pre-defined arguments.

- Artemisa can launch some countermeasures against the incoming attacks.

```
... output ommitted ...

| | Category: Interactive attack

+ Checking if media port is opened...
|
| No RTP info delivered.
|
| Category: Spoofed message

... output ommitted ...

+ The message is classified as:
| Attack tool
| Spoofed message
| Interactive attack
| Dial plan fault
| Scanning
| Ringing

************************************ Correlation **************

Artemisa concludes that the arrived message is likely to be:

* The attack was created employing the tool SIPVicious.
* A flooding attack.

... output ommitted ...
```

Dianoea

• Dionaea belongs to a multi-service oriented honeypot which can simulate many services at a time

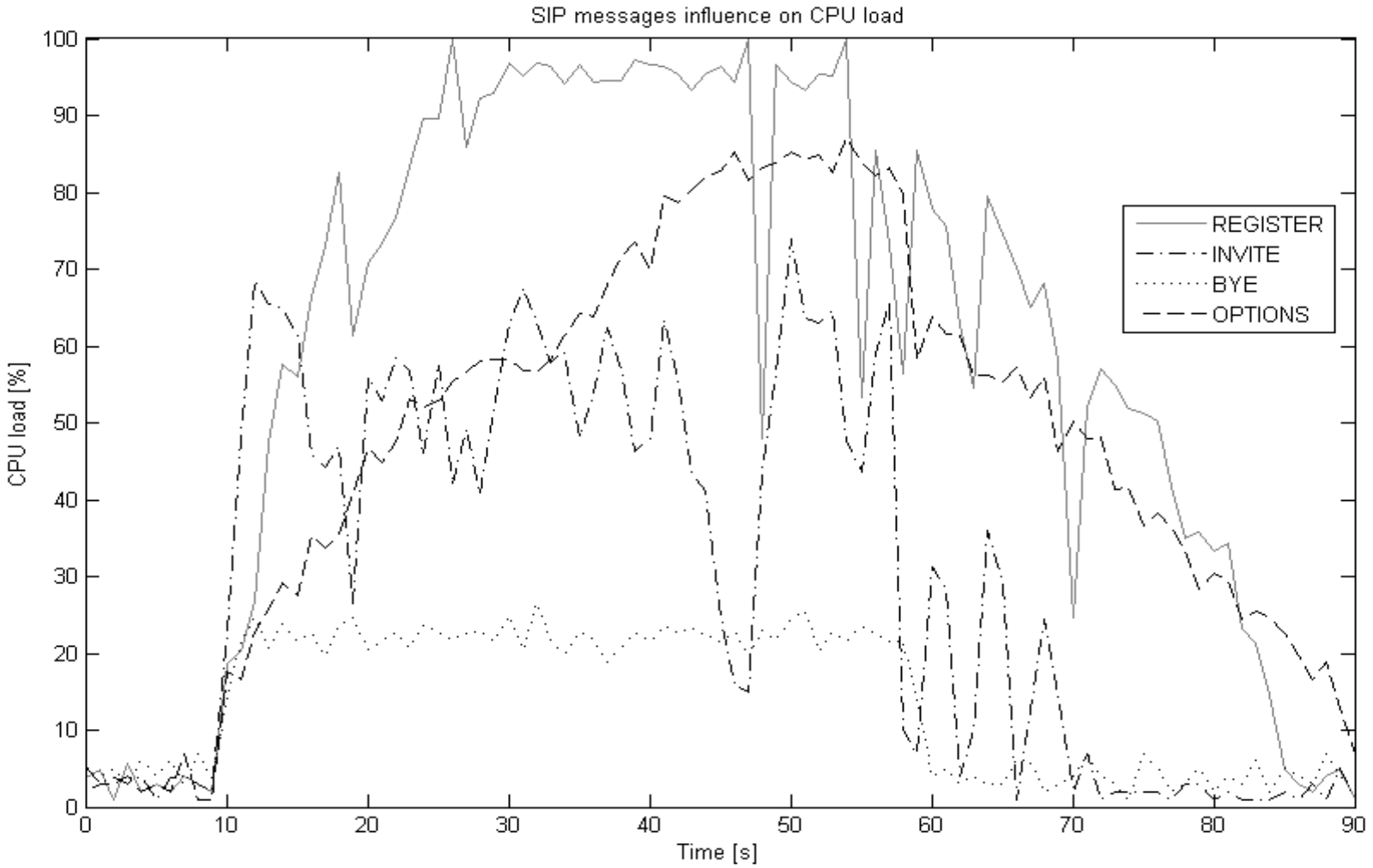
• simply waits for any SIP message and tries to answer it.

• all SIP requests from RFC 3261 (REGISTER, INVITE, ACK, CANCEL, BYE, OPTIONS), multiple SIP sessions and RTP audio streams (data from stream can be recorded).

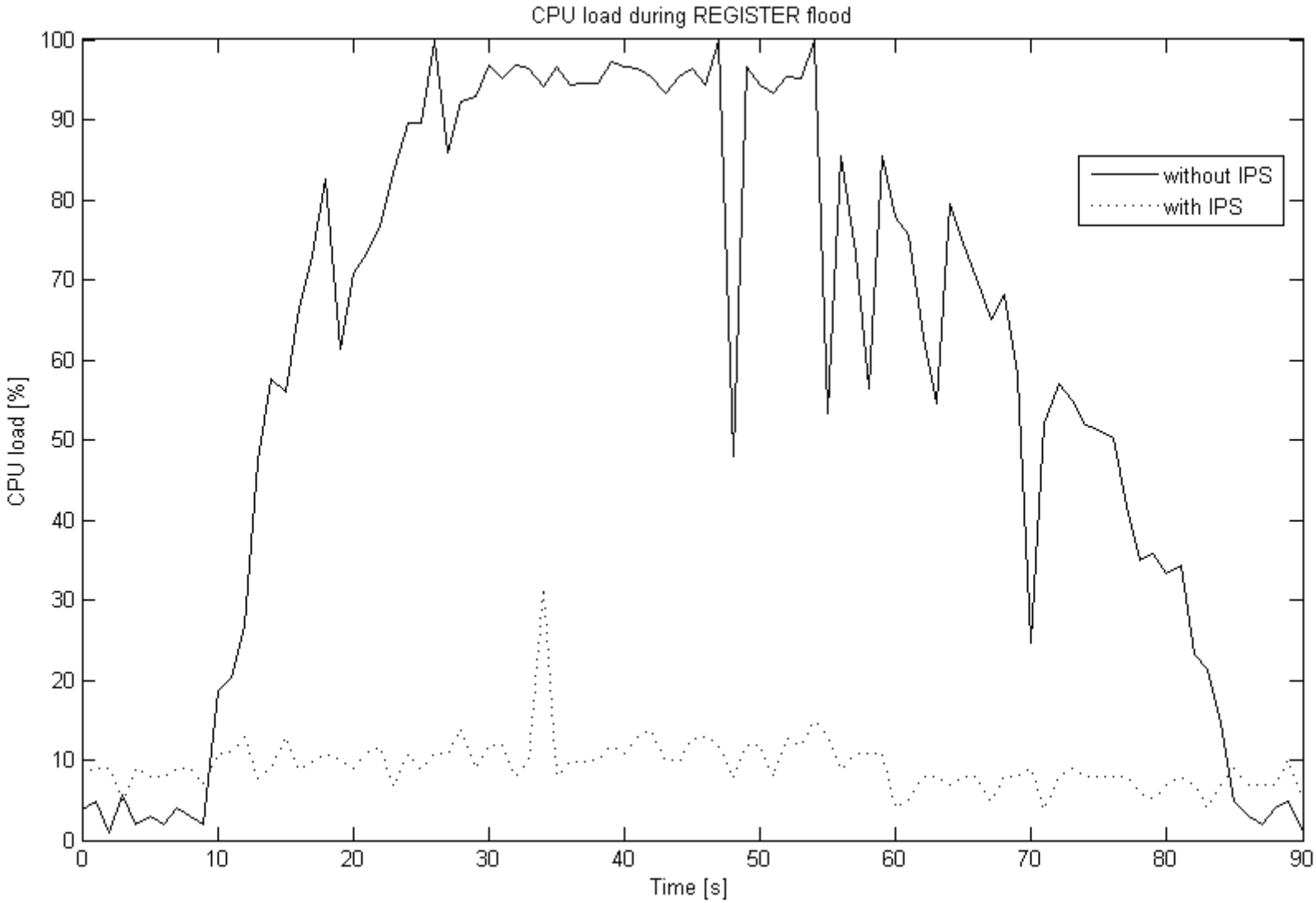
• logs are saved in plain-text files and in sqlite database.

DoS attacks on application level

- register and invite flood (silent killers, CPU depletion)



Impact of SSI (Snort, SnortSAM, IPtables)



Detection of SIP infrastructure attack

- some methods rely on IDS systems as SNORT and its features (exceeding **thresholds**), **fingerprints** of attacks

- and statistical methods such as **Hellinger-Distance**

$$H^2(P,Q) = \frac{1}{2}\sum_{i=1}^{n}\left(\sqrt{p_i} - \sqrt{q_i}\right)^2$$

p – distribution of data within training period
q - distribution of data within short period

Test on similarity of both distributions

Anomalies Detection in SIP infrastructure

- or detection of anomaly using predictive model such as **Holt-Winters** model

$$\hat{y}_t = L_{t-1} + P_{t-1} + S_{t-T}$$

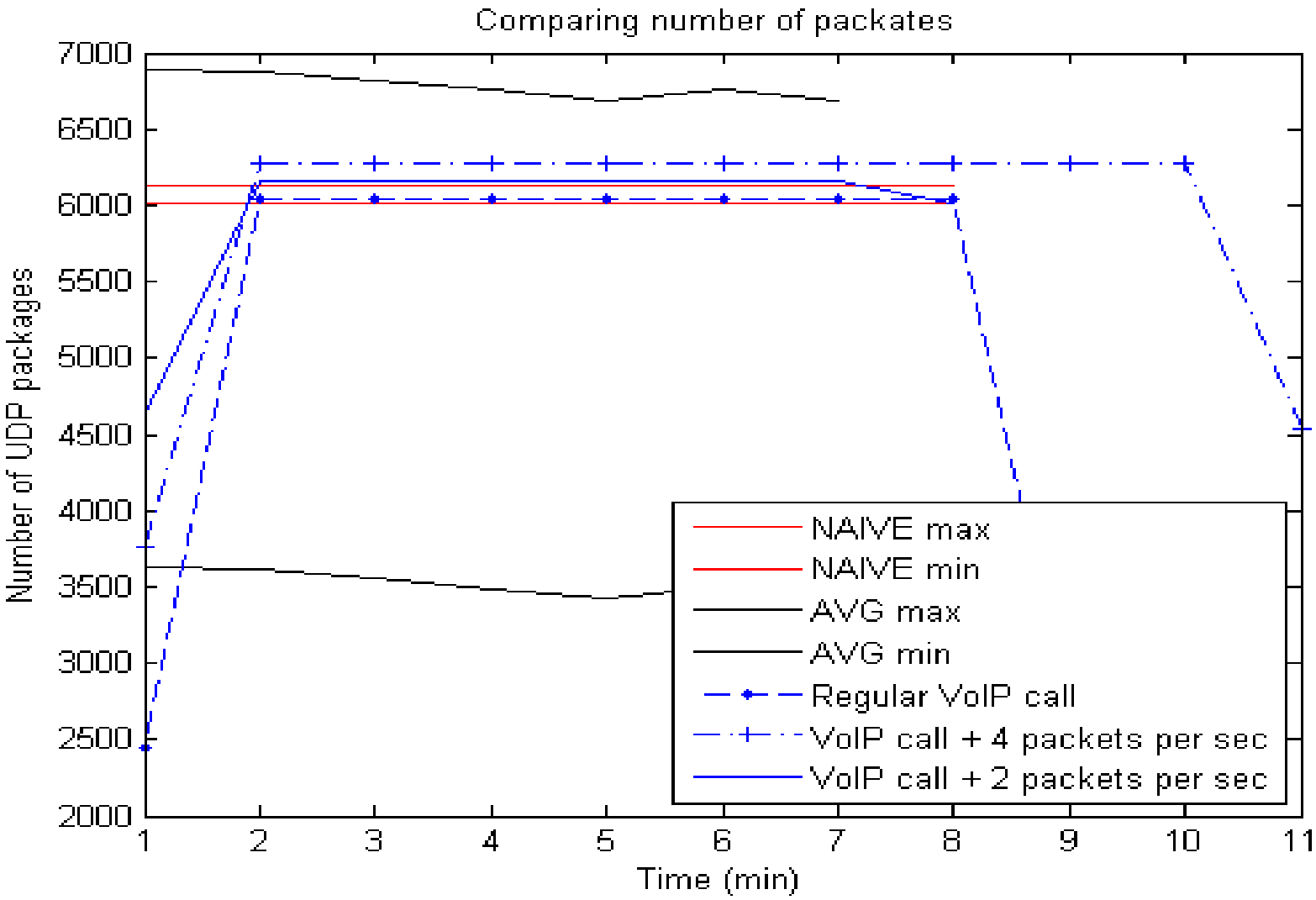
L (level), P (trend) and S (seasonal) components

- or **Brutlag method** (predicted deviation) $\hat{y}_{\max_t}$ and $\hat{y}_{\min_t}$
- or **Moving avarage**, where k is number of measurements in time series

$$\hat{y}_t = \frac{\sum_{i=t-k}^{t-1} y_i}{k}$$

Anomalies Detection in SIP traffic

- Snort.AD, preprocessor http://www.anomalydetection.info

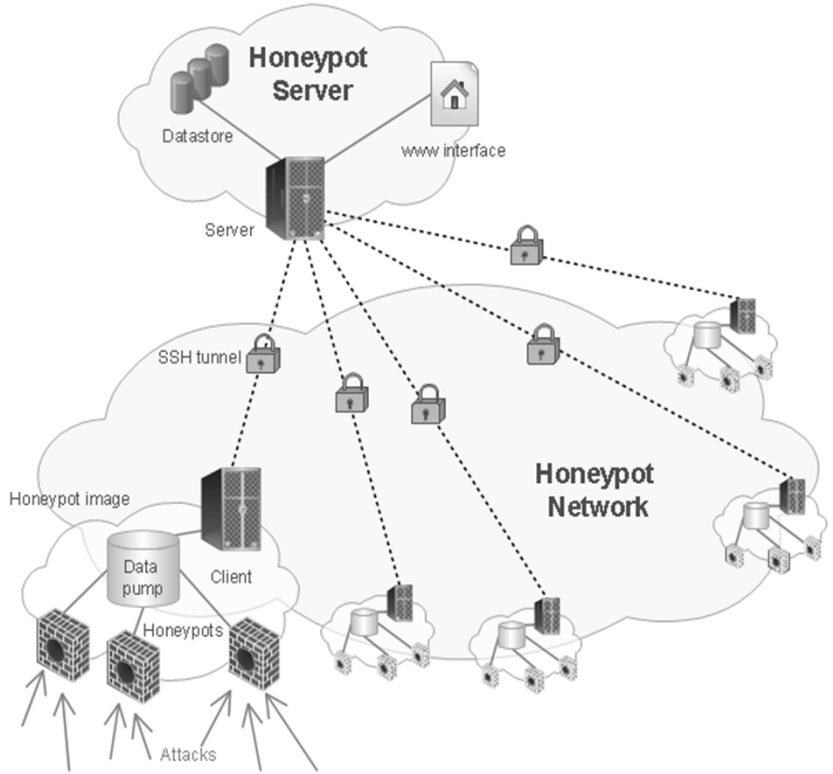


Honeypot Network Concept

The proposed design of a **distributed honeypot network**

centralized server for data gathering, analysis and honeypot monitoring

the main part of distributed network concept is honeypot image

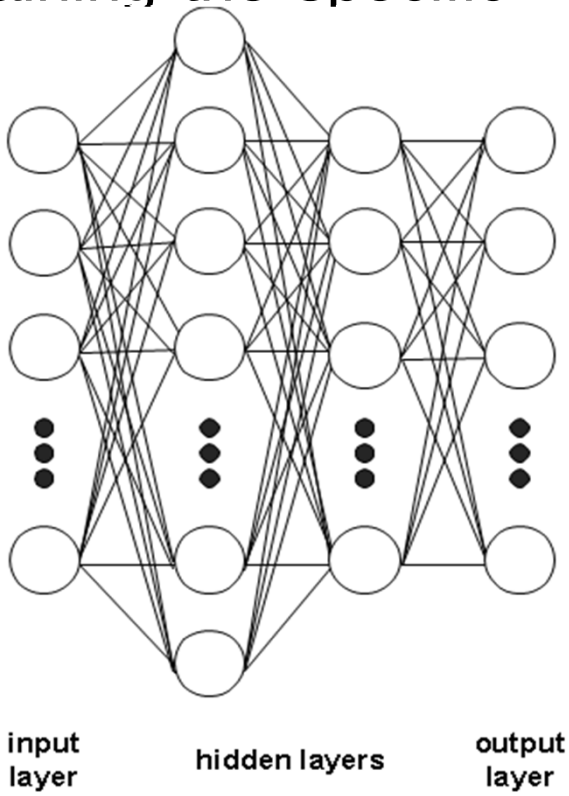


MLP Neural Network

- MLP neural network was used for VoIP attack classifications.

- It consists of several layers, each containing the specific number of neurons called perceptron.

- perceptrons in one layer are Interconnected to each other in the following layer (synapse)



MLP Neural Network

- each neuron in the input layer has a value based on input parameters, the same number of neurons as there are parameters in the input set.
- output layer has the same number of neurons as the number of attack classes, so each neuron is then a single class of learned attack
- Number of neurons inside hidden layers depends on neural network configuration (typically higher than the number of neurons in input or output layers).

MLP Neural Network

- output of neuron *0* means inhibition and *1* excitation
- activation function (sigmoid)
- z : output from previous layer

$$y = \frac{1}{1 + e^{-cz}}$$

neuron x and multiplies by corresponding connection weight w

$$z = \sum_{i=1}^{n} w_i x_i$$

c represents a skewness of the function, higher values bring the skewness of a sigmoid closer to a step function

memory of neural network is saved in connection weights. learning mechanism – **backpropagation** is used to acquire these values.

Practical Implementation

- 10 input layer neurons, two hidden layers contain 30 and 24 neurons, the last and output layer **8 neurons**

- All attack information is gathered through multi-service oriented honeypot application Dionaea

- events are stored in sqlite internal database (SIP message, IP addresses, ports or specific SIP header values)

- All data for final classification are aggregated from selected tables to an array with 10 attributes.

Practical Implementation

- 10 attributes serve as an attack vector (NN input).
- aggregation depends on attack origin and also time of last message occurrence (there is 5 minute sliding window after last message detection): **attack time duration; connection count; REGISTER message count; INVITE msg. count; ACK msg. count; BYE msg. count; CANCEL msg. count; OPTIONS msg. count; SUBSCRIBE msg. count; connection rate.**
- The connection count attribute holds the number of connection from a single source on honeypot. The connection rate is the ratio of all received SIP messages to connection count.

Practical Implementation

- SIP attack classification MLP network is evaluated as learned, if there correctly identify more than 95% of items in the training set
- After specific number of iteration cycles (100) is automatically checked successfulness of classification.
- restart after 2 500 000 backpropagation cycles.

- Result of analyses with MLP networks has following successfulness: **94.94%; 79.85% and 97.54%.**

- The lowest classification precision 79.85% was caused by new call attack, which was not included in the training set.

Conclusion

• The proposal distributed honeypot network in combination with neural network classifiers serves as another security level.

• With the possibility to change firewall rules or network routing., whole system can prepare precaution mechanisms against attacks.

• Classification by human is very precise, but time consuming and expensive. Automatic classification mechanism brings a solution for VoIP classification and simplifies the analysis of attacks.

Thank you for your attention

Q&A