Automatic Detection of Cybersecurity Events from Turkish Twitter Stream and Turkish Newspaper Data

Özgür Ural
1819622
Advisor : Assoc. Prof. Dr. Cengiz Acartürk

Middle East Technical University
Cyber Security

August 7th 2019

Outline

Motive

FIGURE – *Tweets in Turkish After the Turktrust Vulnerability Announcement on 3 January 2013. Retrieved June 28, 2019, from https ://twitter.com.*

Objectives

- Investigate **potential data sources** to determine the most suitable ones to use it for real-time event detection with Turkish text.

Objectives

- Investigate **potential data sources** to determine the most suitable ones to use it for real-time event detection with Turkish text.
- Design and develop a software system for **real-time cyber security event detection using Turkish texts**.

Objectives

- Investigate **potential data sources** to determine the most suitable ones to use it for real-time event detection with Turkish text.
- Design and develop a software system for **real-time cyber security event detection using Turkish texts**.
- Design the system as a **framework** for further research.

Routine Tasks of an Information Security Analyst

- Take **countermeasures** for **protecting organizational-level, mission-critical and sensitive information**, as well as being prepared for **cyber attacks**.

Routine Tasks of an Information Security Analyst

- Take **countermeasures** for **protecting organizational-level, mission-critical and sensitive information**, as well as being prepared for **cyber attacks**.
- **Analyze data** and **recommend changes** to managers.

Challenges of being an Information Security Analyst

FIGURE – *Research results of IBM Security Lab about Cyber Security Analysts*

Challenges of being an Information Security Analyst

FIGURE – *Research results of IBM Security Lab about Cyber Security Analysts*

Challenges of being an Information Security Analyst

Is it really sustainable ?

FIGURE – *Research results of IBM Security Lab about Cyber Security Analysts*

What is Natural Language Processing and Text Mining ?

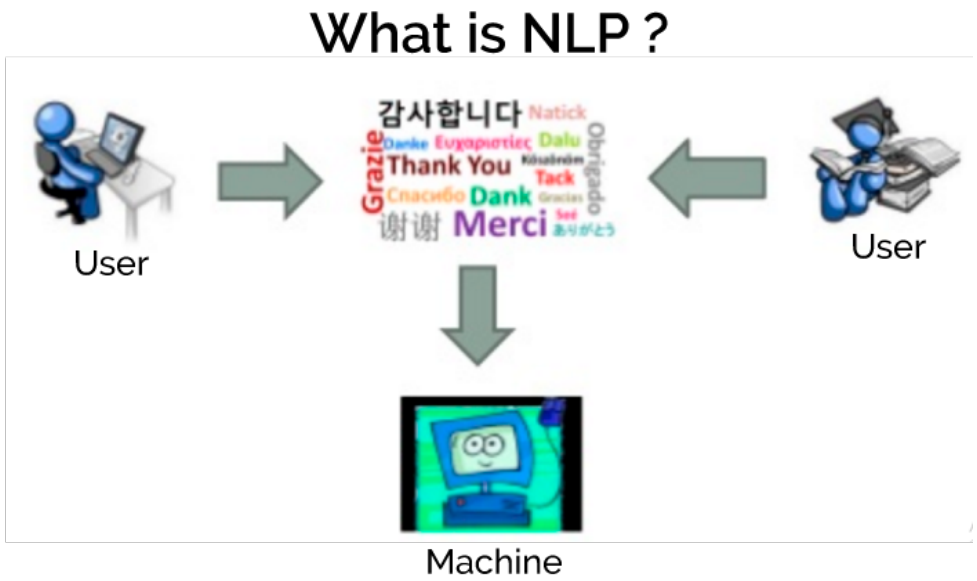


FIGURE – *A Simple diagram to explain what Natural Language Processing does.*

- **Natural Language Processing** is ability of machines to understand and interpret human language the way it is written or spoken.

What is Natural Language Processing and Text Mining ?

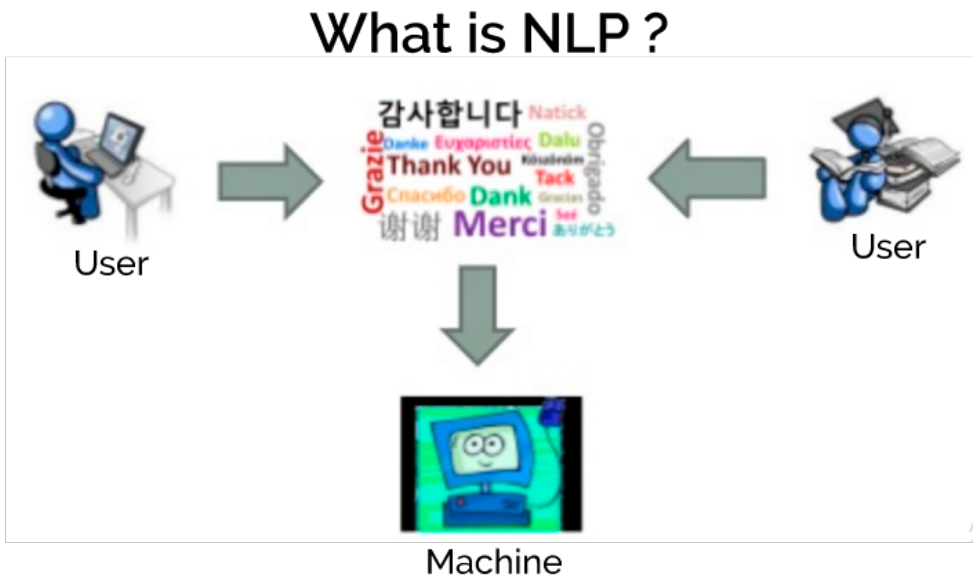


FIGURE – *A Simple diagram to explain what Natural Language Processing does.*

- **Natural Language Processing** is ability of machines to understand and interpret human language the way it is written or spoken.
- **Text mining** is the process or practice of examining large collections of written resources to generate new information. In this thesis, we used **keyword-based analysis** and **statistical techniques**.

Why do we need Natural Language Processing and Text Mining ?

FIGURE – *Research results of IBM Security Lab about Cyber Security Analysts*

Literature Review

- "Weakly Supervised Extraction of Computer Security Events from Twitter". (Ritter, Wright, Casey, & Mitchell, 2016)

Literature Review

- "Weakly Supervised Extraction of Computer Security Events from Twitter". (Ritter, Wright, Casey, & Mitchell, 2016)
- “Automatic Detection of Cyber Security Related Accounts on Online Social Networks : Twitter as an Example”.(Aslan, Sağlam, & Li, 2018)

Literature Review

- "Weakly Supervised Extraction of Computer Security Events from Twitter". (Ritter, Wright, Casey, & Mitchell, 2016)
- “Automatic Detection of Cyber Security Related Accounts on Online Social Networks : Twitter as an Example”.(Aslan, Sağlam, & Li, 2018)
- "DDoS Event Forecasting Using Twitter Data”. (Wang & Zhang, 2017)

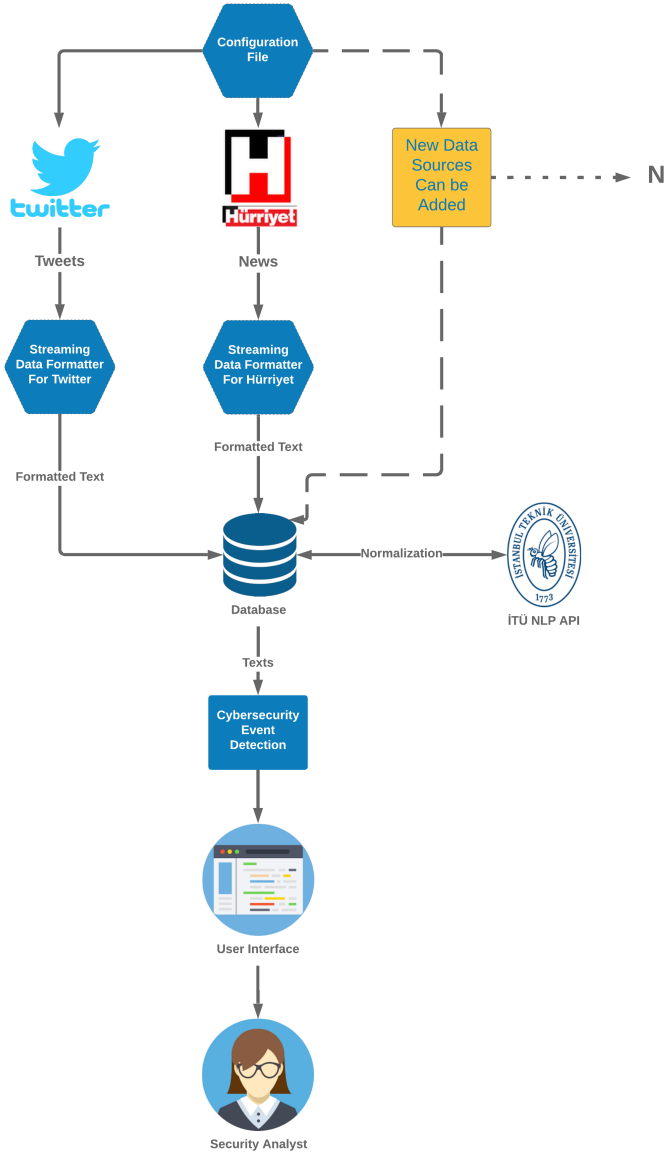
Literature Review

- "Weakly Supervised Extraction of Computer Security Events from Twitter". (Ritter, Wright, Casey, & Mitchell, 2016)
- “Automatic Detection of Cyber Security Related Accounts on Online Social Networks : Twitter as an Example”.(Aslan, Sağlam, & Li, 2018)
- "DDoS Event Forecasting Using Twitter Data”. (Wang & Zhang, 2017)
- “Prediction of Drive-by Download Attacks on Twitter”. (Javed, Burnap, & Rana, 2019)

Literature Review

- "Weakly Supervised Extraction of Computer Security Events from Twitter". (Ritter, Wright, Casey, & Mitchell, 2016)
- “Automatic Detection of Cyber Security Related Accounts on Online Social Networks : Twitter as an Example”.(Aslan, Sağlam, & Li, 2018)
- "DDoS Event Forecasting Using Twitter Data”. (Wang & Zhang, 2017)
- “Prediction of Drive-by Download Attacks on Twitter”. (Javed, Burnap, & Rana, 2019)
- “Crowdsourcing Cybersecurity : Cyber Attack Detection using Social Media”. (Khandpur et al., 2017)

Pipeline


Configuration File
twitter
Hürriyet
New Data Sources Can be Added
N
Tweets
News
Streaming Data Formatter For Twitter
Streaming Data Formatter For Hürriyet
Formatted Text
Formatted Text
Normalization
İSTANBUL TEKNİK ÜNİVERSİTESİ 1773
Database
İTÜ NLP API
Texts
Cybersecurity Event Detection
User Interface
Security Analyst

Data Collection and Data Processing

Data Collection

- **Hürriyet API** and **Twitter API**
- We can get up to **%1 of the Twitter stream**, which is approximately one million Tweets per day due to Twitter API limitation, which is **limited by Twitter**.
- We can get up to **12,000 request per day** in Hürriyet newspaper API, which is **limited by Hürriyet**.

Data Collection and Data Processing

Data Collection

- **Hürriyet API** and **Twitter API**
- We can get up to **%1 of the Twitter stream**, which is approximately one million Tweets per day due to Twitter API limitation, which is **limited by Twitter**.
- We can get up to **12,000 request per day** in Hürriyet newspaper API, which is **limited by Hürriyet**.

Data Processing

- Filter selected keys from JSON streams of Twitter API and Hürriyet API.
- Filter consecutive non-ASCII characters from the fetched data.
- Sent the raw data to ITU NLP API to **normalize** them.

Multi-Process and Microservice Architecture

The Processes Developed as a Framework in This Thesis :

- Twitter API Stream to Database
- Hurriyet API Stream to Database
- ITU NLP API Normalization
- Security Events Web Portal

Multi-Process and Microservice Architecture

The Processes Developed as a Framework in This Thesis :

- Twitter API Stream to Database
- Hurriyet API Stream to Database
- ITU NLP API Normalization
- Security Events Web Portal

Microservices :

- **Resilient :** Failure in one service does not impact the other services of our project.
- **Scalable :** if our database technology becomes insufficient for our software, we can easily change the database technology with a more suitable one.
- **Less dependency** and **easy to modify** its code and test them.

Demonstrative Video

User Interface of The System

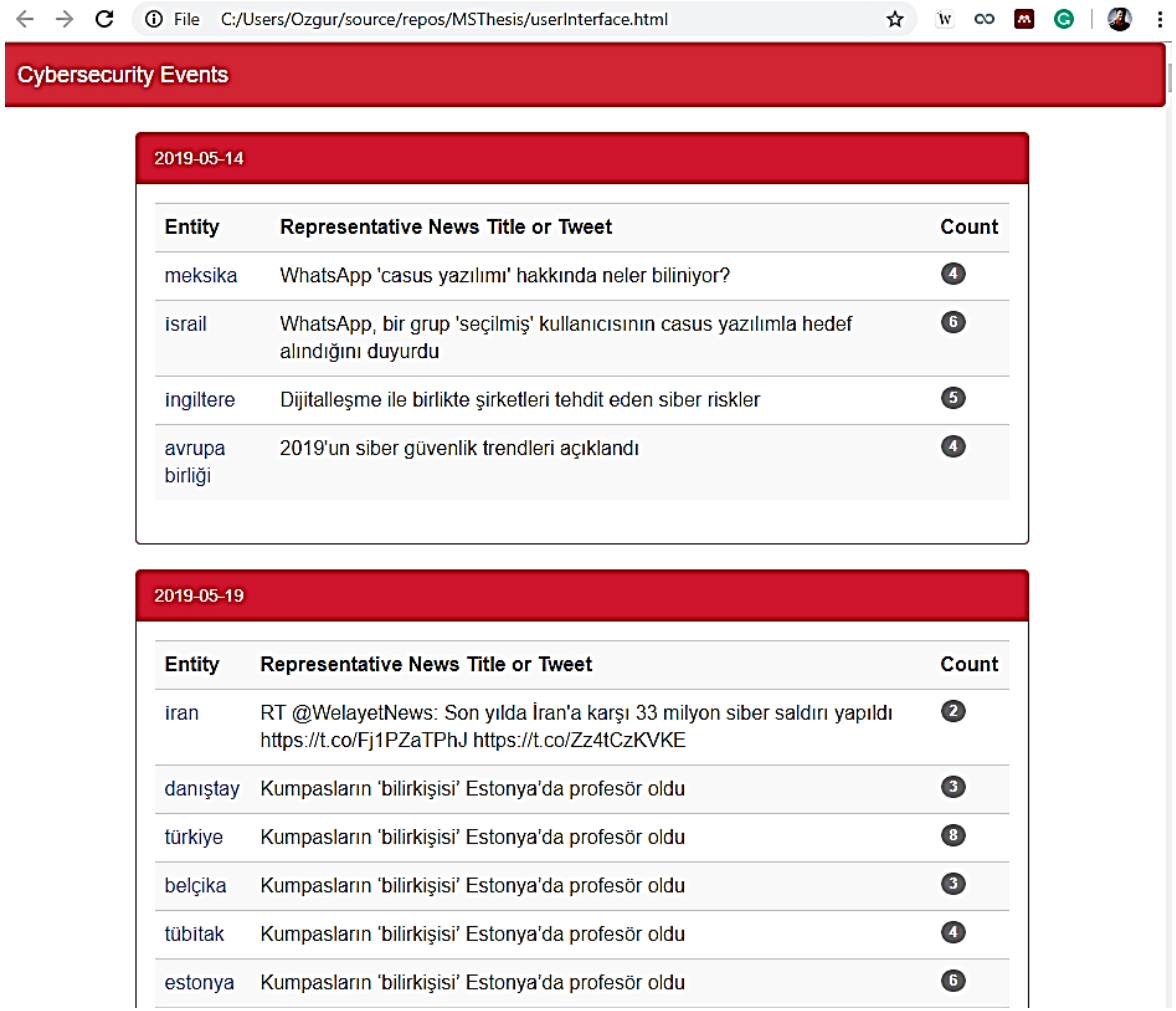


FIGURE – *User Interface of the Cybersecurity Detection Software*

Successful Cybersecurity Event Detection Samples

2019-05-14

Entity	Representative News Title or Tweet	Count
meksika	WhatsApp 'casus yazılımı' hakkında neler biliniyor?	4
israil	WhatsApp, bir grup 'seçilmiş' kullanıcısının casus yazılımla hedef alındığını duyurdu	6

FIGURE – *WhatsApp Spyware Attack Detection*

2019-04-26

Entity	Representative News Title or Tweet	Count
stm	Uzaktan Hasta Takip Sistemi uygulamalarında tehlike	5

FIGURE – *STM Warns about Remote Patient Tracking System Applications*

Unsuccessful Cybersecurity Event Detection Samples

ant	@omerturantv72 Ömet bey inanamiyorum; gercekten bunlari siz mi yaziyorsunuz yoksa hesabiniz mi hacklendi?	4

FIGURE – *Sample False Positive Cybersecurity Event Detection*

çin	Beni takip eden bütün takipçilerime duyurumdur: Twitter hesabım hacklendiği için abuk sabuk reklam, ilan ve de tele... https://t.co/8njVtCkfNQ	7

FIGURE – *Sample Indirectly Useful Cybersecurity Event Detection*

Evaluation of the Results

On a Sample Test Run :

- The database of the software includes **437** entries. **186** of them are **Twitter Tweets**, and **251** of them are from **Hürriyet Newspaper**.

Evaluation of the Results

On a Sample Test Run :

- The database of the software includes **437** entries. **186** of them are **Twitter Tweets**, and **251** of them are from **Hürriyet Newspaper**.
- The software solution can detect **29 cybersecurity events** from that entries.

Evaluation of the Results

On a Sample Test Run :

- The database of the software includes **437** entries. **186** of them are **Twitter Tweets**, and **251** of them are from **Hürriyet Newspaper**.
- The software solution can detect **29 cybersecurity events** from that entries.
- **22** of them are **positive detection**, and **7** of them are **false positive detection**.

Evaluation of the Results

On a Sample Test Run :

- The database of the software includes **437** entries. **186** of them are **Twitter Tweets**, and **251** of them are from **Hürriyet Newspaper**.
- The software solution can detect **29 cybersecurity events** from that entries.
- **22** of them are **positive detection**, and **7** of them are **false positive detection**.
- Our software solution's **success rate** is approximately **%76**.

Evaluation of the Results

On a Sample Test Run :

- The database of the software includes **437** entries. **186** of them are **Twitter Tweets**, and **251** of them are from **Hürriyet Newspaper**.
- The software solution can detect **29 cybersecurity events** from that entries.
- **22** of them are **positive detection**, and **7** of them are **false positive detection**.
- Our software solution's **success rate** is approximately **%76**.
- Success rate is **dependent external factors** like selected time frame, selected keyword vector, selected named entity vector, number of data in dataset and so on. The success rate may increase or decrease according to these factors.

Evaluation of the Results

On a Sample Test Run :

- The database of the software includes **437** entries. **186** of them are **Twitter Tweets**, and **251** of them are from **Hürriyet Newspaper**.
- The software solution can detect **29 cybersecurity events** from that entries.
- **22** of them are **positive detection**, and **7** of them are **false positive detection**.
- Our software solution's **success rate** is approximately **%76**.
- Success rate is **dependent external factors** like selected time frame, selected keyword vector, selected named entity vector, number of data in dataset and so on. The success rate may increase or decrease according to these factors.
- These statistics show that this methodology works in the detection of cybersecurity events from Turkish texts with an acceptable success rate.

Conclusion

- Every automation system has unique requirements to achieve its purposes.

Conclusion

- Every automation system has unique requirements to achieve its purposes.
- Social media is one of the fastest ways to detect cybersecurity events because people and bots share such events in there.

Conclusion

- Every automation system has unique requirements to achieve its purposes.
- Social media is one of the fastest ways to detect cybersecurity events because people and bots share such events in there.
- Processing the newspaper data is relatively more straightforward because false-positive cybersecurity events are rarely shared in the newspaper websites.

Conclusion

- Every automation system has unique requirements to achieve its purposes.
- Social media is one of the fastest ways to detect cybersecurity events because people and bots share such events in there.
- Processing the newspaper data is relatively more straightforward because false-positive cybersecurity events are rarely shared in the newspaper websites.
- An automated software system for cyberscurity event detection which use various Turkish data sources, named entities, text mining methods is applicable, and security analysts can use our system as a helper tool.

Conclusion

- Every automation system has unique requirements to achieve its purposes.
- Social media is one of the fastest ways to detect cybersecurity events because people and bots share such events in there.
- Processing the newspaper data is relatively more straightforward because false-positive cybersecurity events are rarely shared in the newspaper websites.
- An automated software system for cyberscurity event detection which use various Turkish data sources, named entities, text mining methods is applicable, and security analysts can use our system as a helper tool.
- Even if our software system detects few false positive cybersecurity events, it was often able to detect useful cybersecurity events.

Conclusion

- Every automation system has unique requirements to achieve its purposes.
- Social media is one of the fastest ways to detect cybersecurity events because people and bots share such events in there.
- Processing the newspaper data is relatively more straightforward because false-positive cybersecurity events are rarely shared in the newspaper websites.
- An automated software system for cyberscurity event detection which use various Turkish data sources, named entities, text mining methods is applicable, and security analysts can use our system as a helper tool.
- Even if our software system detects few false positive cybersecurity events, it was often able to detect useful cybersecurity events.
- Our software system can detect cybersecurity events such as WhatsApp Spyware, MuddyWater Attack, the Remote Patient Tracking System Applications vulnerability, Pirate Matryoshka Virus, Zombie Cookies threat.

Future Work

To pave a way for the subsequent studies,

- Move our project to a server, obtain a website.

Future Work

To pave a way for the subsequent studies,

- Move our project to a server, obtain a website.
- Add new Turkish data sources like Eksisozluk, Linkedin, Facebook, and so on to increase success rate and positive detection.

Future Work

To pave a way for the subsequent studies,

- Move our project to a server, obtain a website.
- Add new Turkish data sources like Eksisozluk, Linkedin, Facebook, and so on to increase success rate and positive detection.
- Maintain the framework as an open source project. Our framework can be useful for researchers work on Cybersecurity, Computer Science and Artificial Intelligence fields.

Future Work

To pave a way for the subsequent studies,

- Move our project to a server, obtain a website.
- Add new Turkish data sources like Eksisozluk, Linkedin, Facebook, and so on to increase success rate and positive detection.
- Maintain the framework as an open source project. Our framework can be useful for researchers work on Cybersecurity, Computer Science and Artificial Intelligence fields.
- Detect cybersecurity events that have not yet taken place by processing streaming data using Turkish.

Future Work

To pave a way for the subsequent studies,

- Move our project to a server, obtain a website.
- Add new Turkish data sources like Eksisozluk, Linkedin, Facebook, and so on to increase success rate and positive detection.
- Maintain the framework as an open source project. Our framework can be useful for researchers work on Cybersecurity, Computer Science and Artificial Intelligence fields.
- Detect cybersecurity events that have not yet taken place by processing streaming data using Turkish.
- Add malicious URL detection to our software system.

References

- Eryiğit, G. (2015). ITU Turkish NLP Web Service. 1–4. https ://doi.org/10.3115/v1/e14-2001
- R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. Preventing private information inference attacks on social networks. Knowledge and Data Engineering, IEEE Transactions on, 25(8) :1849–1862, 2013.
- https ://www.ibm.com/security/cognitive
- Petersen, J. (2017). Sonar. Handbook of Surveillance Technologies, Third Edition, (August), 223–291. https ://doi.org/10.1201/b11594-7
- Khandpur, R. P., Ji, T., Jan, S., Wang, G., Lu, C.-T., & Ramakrishnan, N. (2017). Crowdsourcing Cybersecurity : Cyber Attack Detection using Social Media. https ://doi.org/10.1145/3132847.3132866
- What is a Security Analyst ? Responsibilities, Qualifications, and More | Digital Guardian. (n.d.). Retrieved April 29, 2019, from https ://digitalguardian.com/blog/what-security-analyst-responsibilities-qualifications-and-more

Thanks for Listening