MUNI
C4E

SoK: Contemporary Issues and Challenges to Enable Cyber Situational Awareness for Network Security

Martin Husák[1], Tomáš Jirsík[1], Shanchieh Jay Yang[2]

husakm@ics.muni.cz, jirsik@ics.muni.cz, jay.yang@rit.edu

[1] Institute of Computer Science, Masaryk University

[2] Department of Computer Engineering, Rochester Institute of Technology

August 6, 2020

Part I

Introduction

Motivation & Goals

Motivation

- Investigation of the current status and challenges of research on CSA.

Goals of the Work

- Discussion of SA and CSA definitions
- Brief literature review and identification of influential researchers
- Revision an existing taxonomy of CSA and related tools
- Identification of the contemporary challenges of CSA research and development

Part II

From SA to CSA

Situational Awareness

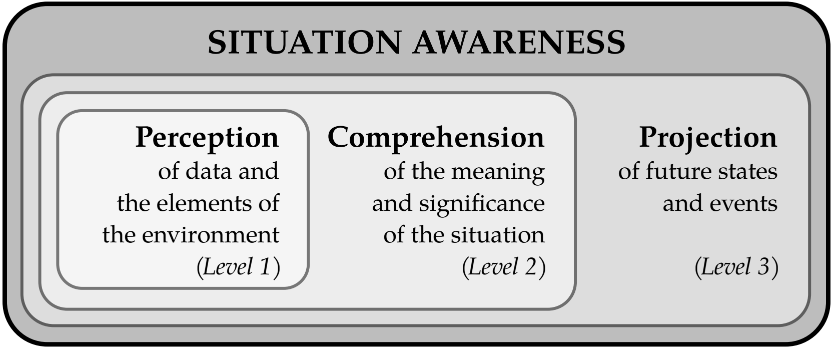
Situational Awareness

- Present in everyday life
- First recognized during WWI, studied in military and aviation from 1980'
- Three major definitions – preceptual cycle, interactive subsystem, three-level model

Cyber Situational Awareness

Cyber Situational Awareness (CSA) is an application of *Situational Awareness* (SA) into the cyber domain

Three-level model of Situational Awareness



SITUATION AWARENESS

Perception of data and the elements of the environment (*Level* 1)

Comprehension of the meaning and significance of the situation (*Level* 2)

Projection of future states and events (*Level* 3)

Mica R. Endsley. Toward a theory of situation awareness in dynamic systems. In: Human Factors. 1995. 37(1).

Cyber Situational Awareness

Specifics of CSA

- Cyber environment – no borders, scale-free, everything/everywhere
- Perception – only sensors, no physical observations
- Performance – unbalanced needs of resources, high speed of events
- Attacker takes the advantage – in contrary to traditional military doctrine

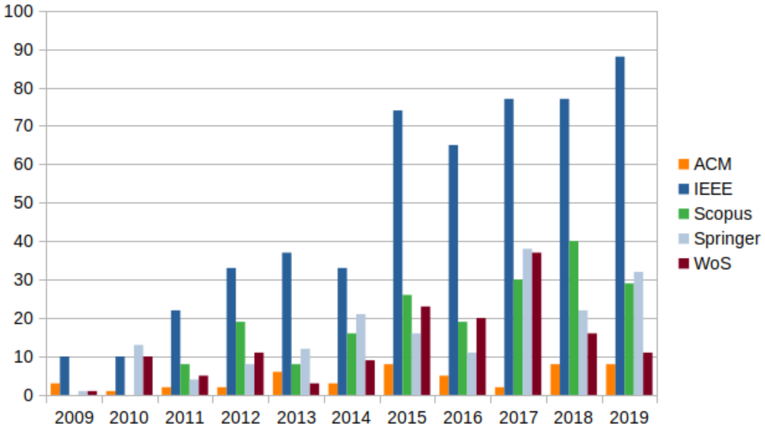
Entities in CSA

- Physical entities – devices, may be characterized by roles
- Immaterial entities – programs and services, loosened connection to devices
- Human entities – characterized by roles

Part III

Review of Research on CSA

Publications on CSA



Major Publications on CSA

Collections

- S. Jajodia, P.Liu, V. Swarup, and C. Wang. Cyber situational awareness: Issues and Research. 2010, Springer.
- A. Kott, C. Wang, and R. F. Erbacher. Cyber defense and situational awareness. 2014, Springer.
- P. Liu, S. Jajodia, and C. Wang. Theory and Models for Cyber Situation Awareness. 2017, Springer.

Surveys

- U. Franke and J. Brynielsson. Cyber situational awareness – A systematic review of the literature. Computers & Security 46 (2014).

Research Groups

- prof. Sushil Jajodia at George Mason University, USA
  http://csis.gmu.edu/
- Alexander Kott at the U.S. Army Research Laboratory
  https://www.arl.army.mil/
- prof. Shanchieh Jay Yang at Rochester Institute of Technology, USA
  https://www.rit.edu/cybersecurity/
- Swedish Defense Research Agency https://www.foi.se/fusion/
  and RISE SICS https://www.sics.se/
- dr. Florian Skopik at Austrian Institute of Technology
  https://www.ait.ac.at/en/research-topics/cyber-security/
- CSIRT-MU at Masaryk University, Czech Republic
  https://csirt.muni.cz/

Research Data

- DARPA datasets – well-known but obsolete, not recommended
  https://www.ll.mit.edu/r-d/datasets
- UNB datasets – large collection of datasets
  https://www.unb.ca/cic/datasets/index.html
- CTU-13 datasets – botnet traffic samples
  https://www.stratosphereips.org/datasets-ctu13
- CAIDA Network Telescope – live data for global situational awareness
  https://www.caida.org/data/
- SABU dataset – live data sample for collaborative alert correlation
  https://data.mendeley.com/datasets/p6tym3fghz/1
- MM-TBM dataset – including network topology and background noise https://ieee-dataport.org/documents/mm-tbm-evaluation-datasets

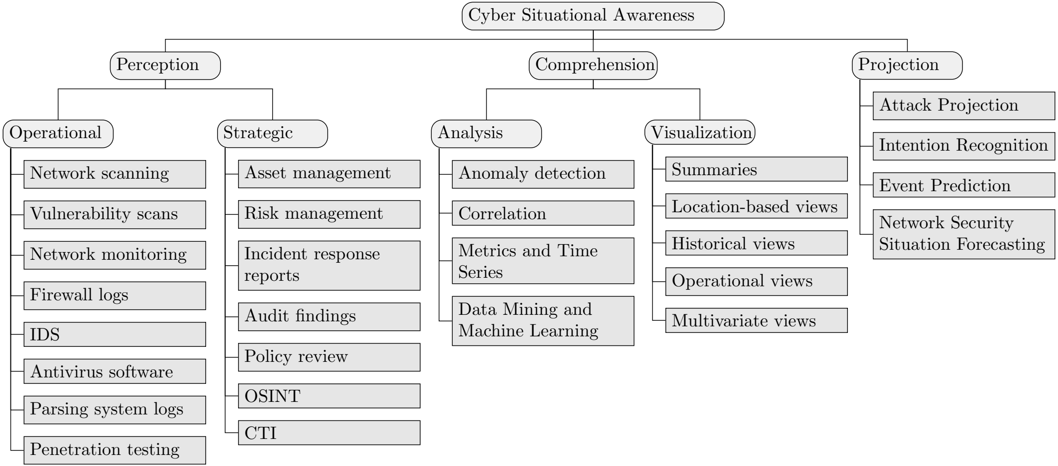
National Policies

- The Australian Cyber Security Operations Centre *provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to cybersecurity events of national importance.*
- USA define their role in cyberspace's future defense as *steady progress towards shared situational awareness of network vulnerabilities and risks among public and private sector networks.*
- The German national cybersecurity strategy establishes National Cyber Response Center to *directly inform the crisis management staff headed by the responsible State Secretary at the Federal Ministry of the Interior if the cybersecurity situation reaches the level of an imminent or already occurred crisis.*
- The UK aims to *enhance cyber threat awareness, detection, and reaction functions, through the development of a Cyber Security Operations Centre that uses state-of-the-art defensive cyber capabilities to protect the cyberspace and deal with threats.*

Part IV

Taxonomy and Components of CSA

Taxonomy and Components of CSA



Based on the taxonomy proposed in Antti Evesti et al.: Cybersecurity Situational Awareness Taxonomy.
In 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)

List of Changes

New categories inspired by three-level model of SA

- Perception – renamed Data Gathering
- Comprehension – fusion of Analysis and Visualization
- Projection – new category, inspired by survey [1]

New or modified items

- CTI, OSINT – emerging sources of information for Perception phase
- System log parsing – moved from Analysis to Comprehension to Perception
- Data mining was generalized from clustering and merged with Machine learning
- Metrics – added changes of observed values in time
- Anomaly detection – may appear in both Perception and Comprehension

M. Husák, et al. Survey of attack projection, prediction, and forecasting in cyber security. IEEE Communications Surveys & Tutorials.

Part V

Contemporary Challenges for CSA

Data and Toolset Perspectives

Data Perspective

- CSA exhibits unique characteristics in *volume*, *velocity*, *veracity*, *variety*, and *volatility*
  - *volume* and *velocity* of global network traffic is rising
  - *variety* of the network traffic increases with new applications
- Big Data characteristics of CSA data opens new challenges for CSA

Toolset Perspective

- A toolset used by an operator significantly influences his/her level of CSA
  - monitoring and data analysis tools,
  - standardized threat models,
  - visualization tools
- Many tools are under rapid development

Data Perspective

Volume with Velocity and Veracity

- Sensors produce massive amount of raw data that bring little understanding

  Data overload – Meaning underload
- Demand for real-time analysis and results delivery
- Emphasis on correct time ordering where causality is of interest

Variety and Volatility

- Homogenizing data from different source and of different types

  Central processing in desired, requires proper metrics and thresholds
- Heterogeneous attack behaviors and network environments

  Often not dependent on what has been observed in the past

Toolset Perspective

Variety with Veracity and Volatility

- A special tool is needed to process data from each different source
- Tension between specialized tools and integrated and unified platforms
- Existing standards and taxonomies differ across organizations and countries
- Shared threat intelligence is vital, yet of low fidelity

Value through Visualization

- High noise-to-signal ratio, low value of information in CSA data
- Major issue is visualization of large-scale, dynamically changing networks
- Anticipatory CSA lacks visualization completely – uncharted scientific challenge

Performance amid Volume, Velocity, Veracity, and Volatility

- Closely related to data challenges
- Scalability can be met by parallelization and cloud computing
- Stream processing reduce delays and incident response times

Part VI

Conclusion

Conclusion

- Discussion of the way from SA to CSA and unique features of CSA
- Brief overview of research on CSA
  - Impactful researchers and fundamental works
  - Number of new publications on CSA per year is still rising
  - More and more applied research and reports from operational environment
  - Interest from governments and national strategies
- Updated taxonomy of CSA tools and components

Challenges for Future Work

- Coping with rising volume, variety, and velocity of the data (Big Data)
- Supporting the CSA operators with the right data at the right time
- Visualizing the data in a meaningful manner
- Maintaining sufficient performance

MUNI
C4E

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

C4E.CZ