Auto-ISAC

Monthly Community Call

February 2020

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why we're here ➢ Expectations for this community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC overview ➢ Heard around the community ➢ What's Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speakers** ➢ *Junaid Farooq, PhD Candidate, Tandon School of Engineering at New York University*
11:45	**Around the Room** ➢ Sharing around the virtual room
11:55	**Closing Remarks**

Welcome - Auto-ISAC Community Call!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem partners, to:

- ✓ Stay informed of Auto-ISAC activities
- ✓ Share information on key vehicle cybersecurity topics
- ✓ Learn about exciting initiatives within the automotive community from our featured speakers

Participants: Auto-ISAC Members, Potential Members, Partners, Academia, Industry Stakeholders, and Government Agencies

Classification Level: **TLP GREEN:** may be shared within the Auto-ISAC Community, and "off the record"

How to Connect: For further info, questions, or to add other POCs to the invite, please contact Auto-ISAC Staff (staff@automotiveisac.com)

Engaging in the Auto-ISAC Community

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC membership
- ❖ If you aren't eligible for membership, connect with us as a partner
- ❖ Get engaged – *"Cybersecurity is everyone's responsibility!"*

19 *Navigator Partners*

12 *Innovator Partners*

❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, connect with Auto-ISAC Staff– staff@automotiveisac.com
- ❖ Engage & ask questions!

20 *OEM Members*

❖ Share – *"If you see something, say something!"*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

38 *Supplier & Commercial Vehicle Members*

Membership represents **99%** *of cars on the road in North America*

Coordination with **23** *critical infrastructure ISACs through the National ISAC Council*

Auto-ISAC Mission

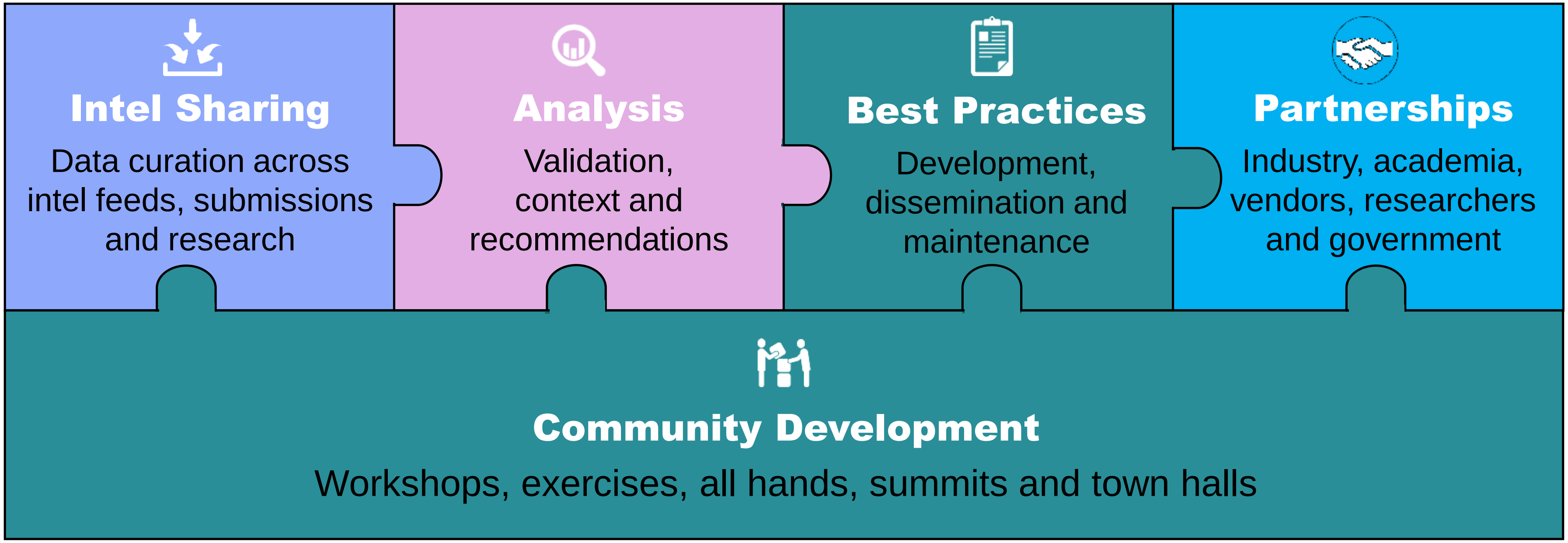
Mission

Serve as an unbiased information broker to provide a **central point of coordination and communication** for the global automotive industry through the analysis and sharing of trusted and timely cyber threat information.

Scope

Light- and heavy-duty vehicles, suppliers, commercial vehicle fleets and carriers. Currently, we **are focused on *vehicle* cyber security**, and anticipate expanding into IT/OT security related to the vehicle.

What We Do



Intel Sharing

Data curation across intel feeds, submissions and research

Analysis

Validation, context and recommendations

Best Practices

Development, dissemination and maintenance

Partnerships

Industry, academia, vendors, researchers and government

Community Development

Workshops, exercises, all hands, summits and town halls

2020 Board of Directors

Executive Committee (ExCom)

Kevin Tierney
Chair of the Board of the Directors
GM

Josh Davis
Vice Chair of the Board of the Directors
Toyota

Jenny Gilger
Secretary of the Board of the Directors
Honda

Tim Geiger
Treasurer of the Board of the Directors
Ford

Todd Lawless
Chair of the Advisory Board
Continental

2020 Advisory Board (AB) Leadership

Todd Lawless
Chair of the Advisory Board
Continental

Brian Murray
Vice Chair of the Advisory Board
ZF

Kevin Walker
Chair of the SAG
Aptiv

Larry Hilkene
Chair of the CAG
Cummins

2020 Auto-ISAC Staff

Faye Francy
Executive Director
fayefrancy@
automotiveisac.com

Josh Poster
Program Operations Manager
joshposter@
automotiveisac.com

Jessica Etts
Senior Intel Coordinator
jessicaetts@
automotiveisac.com

Kim Engles
Membership Engagement Lead
kimengles@
automotiveisac.com

Jake Walker
Cyber Intel Analyst
jacobwalker@
automotiveisac.com

Michelle Menner
Organization Coordinator
michellemenner@
automotiveisac.com

Lisa D. Scheffenacker
Business Administrator
lisascheffenacker@
automotiveisac.com

Julie Kirk
Finance
juliekirk@
automotiveisac.com

Linda Rhodes
Legal Counsel,
Mayer Brown
lrhodes@mayerbrown.com

Recent Activities

Highlights of Key Activities in January

- **Auto-ISAC attended**
  - **CES 2020 in Las Vegas, NV**
  - **SANS Cyber Threat Intelligence Summit & Training in Arlington, VA**
  - **SAE Government Industry Meeting in Washington, DC**

Looking Ahead to February

- **Auto-ISAC will be attending**
  - **Embry–Riddle Aeronautical University Distinguished Cyber Speaker Series in Prescott, AZ**
  - **Auto-ISAC Executive Committee Workshop in Detroit, MI**
- **Auto-ISAC will be releasing 7th Best Practice Guide: Security Development Lifecycle on the website later this week**

Advanced threat actors are actively targeting the automotive and manufacturing industries

-Sodinokibi Ransomware Threatens to Publish Data of Automotive Group: The attackers behind the Sodinokibi Ransomware are now threatening to publish data stolen from another victim after they failed to get in touch and pay the ransom to have the data decrypted. Sodinokibi claims that this data was stolen from GEDIA Automotive Group, a German automotive supplier with production plants in Germany, China, Hungary, India, Mexico, Poland, Hungary, Spain, and the USA. (Link)

-Trend Micro Antivirus Zero-Day Used in Mitsubishi Electric Hack: Chinese hackers have used a zero-day in the Trend Micro OfficeScan antivirus during their attacks on Mitsubishi Electric, ZDNet has learned from sources close to the investigation. Trend Micro has now patched the vulnerability, but the company did not comment if the zero-day was used in other attacks beyond Mitsubishi Electric. Japanese media claimed that the intrusion was the work of a Chinese state-sponsored cyber-espionage group known as Tick. The Tick hacking group is known for carrying out a large number of hacking campaigns aimed at targets all over the world over the past few years. Currently, it is unclear if the group also used the OfficeScan zero-day against other targets. (Link)

-Mitsubishi Electric Data May Have Been Compromised in Cyberattack: Mitsubishi Electric Corp. said Monday it has been targeted in a massive cyberattack, and that information regarding government agencies and other business partners may have been compromised. A key player in Japan's defense and infrastructure industries, the electronics giant said that among the potentially leaked information are email exchanges with the Defense Ministry and the Nuclear Regulation Authority as well as documents related to projects with private firms, including utilities, railway operators, communications and automakers. (Link)

-Vietnam-linked Ocean Lotus hacked BMW and Hyundai networks : According to German media, hackers suspected to be members of the Vietnam-linked APT Ocean Lotus (APT32) group breached the networks of the car manufacturers BMW and Hyundai. The intrusion aimed at stealing automotive trade secrets. APT32 used both Windows and Mac malware in its campaigns delivered to the victims via watering hole attacks and leveraged sophisticated techniques to evade detection. In the recent attacks against the car manufacturers, the attackers managed to deploy in the target network the Cobalt Strike hacking tool "Cobalt Strike". (Link)

For more information or questions please contact analyst@automotiveisac.com

SAE and ISO Announce Their First Joint Standard

Builds on SAE J3061^{TM} *"Cybersecurity Guidebook For Cyber-Physical Vehicle Systems"*; provides more detailed expectations and direction

Takes a **Risk-based, Process-driven Approach** to cybersecurity throughout the product development lifecycle

Paves the path to more **Consistent Cybersecurity Practices** and design forethought into the automotive industry

ISO/SAE 21434: Road Vehicles - Cybersecurity Engineering

SURFACE VEHICLE STANDARD

ISO/SAE DIS 21434

Road Vehicles - Cybersecurity Engineering

FOREWORD

[illegible]

DRAFT

Download the standard on February 12
https://www.sae.org/standards/content/ISO/SAE21434.D1

Register for the free February 13 webinar
https://event.webcasts.com/starthere.jsp?ei=1283065&tp_key=95fd2af881

DHS Cybersecurity and Infrastructure Security Agency (CISA)

What's Trending?

For more information about DHS CISA please visit https://www.cisa.gov/

CISA RESOURCE HIGHLIGHTS

Citrix ADC & Gateway Vulnerability Tracked by CISA at TLP: WHITE

- 31JAN2020 – AA 20-031A - Detecting Citrix CVE-2019-19781
  - https://www[.]us-cert[.]gov/ncas/alerts/aa20-031a
- 23JAN2020 - Citrix Releases Security Updates for SD-WAN WANOP:
  - https://www[.]us-cert[.]gov/ncas/current-activity/2020/01/23/citrix-releases-security-updates-sd-wan-wanop

Citrix ADC & Gateway Vulnerability Tracked by CISA at TLP: WHITE (continued)

- 17JAN2020 - Citrix Adds SD-WAN WANOP, Updated Mitigations to CVE-2019-19781 Advisory
  - https://www[.]us-cert[.]gov/ncas/current-activity/2020/01/17/citrix-adds-sd-wan-wanop-updated-mitigations-cve-2019-19781

- 13JAN2020 - CISA Releases Test for Citrix ADC and Gateway Vulnerability
  - https://www[.]us-cert[.]gov/ncas/current-activity/2020/01/13/cisa-releases-test-citrix-adc-and-gateway-vulnerability

Citrix ADC & Gateway Vulnerability Tracked by CISA at TLP: WHITE (continued)

- 22JAN2020 – “FireEye and Citrix Tool Scans for Indicators of Compromise Related to CVE-2019-19781”
  - https://www[.]fireeye[.]com/blog/products-and-services/2020/01/fireeye-and-citrix-tool-scans-for-iocs-related-to-vulnerability[.]html
  - https://www[.]citrix[.]com/news/announcements/jan-2020/citrix-and-fireeye-mandiant-launch-indicator-of-compromise-scann[.]html
  - https://github[.]com/fireeye/ioc-scanner-CVE-2019-19781/
  - https://github[.]com/citrix/ioc-scanner-CVE-2019-19781

Microsoft Vulnerabilities Tracked by CISA - TLP: WHITE

- CISA Current Activities (CA) on Microsoft Vulnerabilities
  - 14JAN2020 - Microsoft Releases January 2020 Security Updates
    - https://www[.]us-cert[.]gov/ncas/current-activity/2020/01/14/microsoft-releases-january-2020-security-updates
  - 14JAN2020 - CISA Releases Emergency Directive and Activity Alert on Critical Microsoft Vulnerabilities
    - https://www[.]us-cert[.]gov/ncas/current-activity/2020/01/14/cisa-releases-emergency-directive-and-activity-alert-critical

Microsoft Vulnerabilities Tracked by CISA - TLP: WHITE (continued)

- Associated items pointed out under the 14JAN2020 CA on the ED and AA:
  - Activity Alert AA20-014A - https://www[.]us-cert[.]gov/ncas/alerts/aa20-014a
  - Emergency Directive 20-02 - https://cyber[.]dhs[.]gov/ed/20-02/
  - CISA Blog: - https://www[.]cisa[.]gov/blog/2020/01/14/windows-vulnerabilities-require-immediate-attention
  - CERT/CC Vulnerability Note VU#491944 - https://www[.]kb[.]cert[.]org/vuls/id/491944/
  - CERT/CC Vulnerability Note VU#849224 - https://www[.]kb[.]cert[.]org/vuls/id/849224/
  - National Security Agency Cybersecurity Advisory - https://media[.]defense[.]gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114[.]PDF

For more information:

cisa.gov

Questions?

CISAServiceDesk@cisa.dhs.gov:

1-888-282-0870:

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA

CYBER+INFRASTRUCTURE

Community Speaker Series

Why Do We Feature Speakers?

- These calls are an opportunity for information exchange & learning
- Goal is to educate & provide awareness around cybersecurity for the connected vehicle

What Does it Mean to Be Featured?

- Perspectives across our ecosystem are shared from members, government, academia, researchers, industry, associations and others.
- Goal is to showcase a rich & balanced variety of topics and viewpoints
- Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC

6 *Best Practice Guides available on website*

How Can I Be Featured?

- If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact our Auto-ISAC (staff@automotiveisac.com)

1800+ *Community Participants*

25 *Featured Speakers to date*

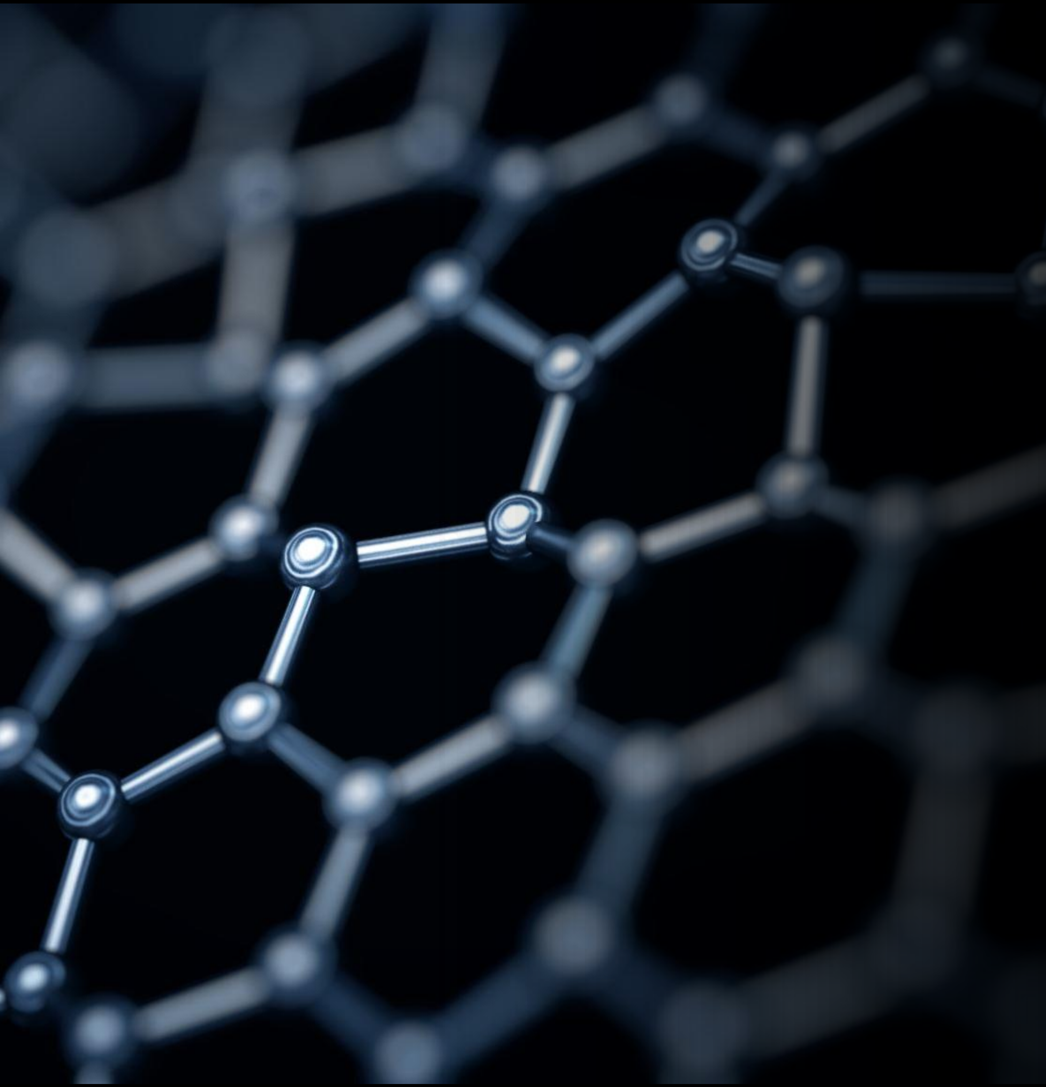
EXAMPLE OF PREVIOUS COMMUNITY SPEAKERS

- **Urban Jonson, NMFTA, Heavy Vehicle Cybersecurity Working Group (April 2018)**
- **Ross Froat, American Trucking Association, ATA Cyberwatch Program (Oct 2018)**
- **Katherine Hartman, Chief – Research, Evaluation and Program Management, ITS Joint Program Office, US DOT (August 2019)**
- **Joe Fabbre, Global Technology Director, Green Hills Software (October 2019)**
- **Oscar Marcia, CISSP, Eonti, Device Authentication in Auto-ISAC as a Foundation to Secure Communications (November 2019)**
- **Amy Smith, the Manager of Pre-College Educational Programming at SAE International (January 2020)**

Community Call Slides are located at: www.automotiveisac.com/communitycalls/

Welcome to Today's Speaker

Junaid Farooq is a PhD Candidate at the Tandon School of Engineering at New York University (NYU). He received a BS degree in Electrical Engineering from the National University of Sciences & Technology (NUST) and the MS degree in Electrical Engineering from the King Abdullah University of Science & Technology (KAUST) in 2013 and 2015 respectively. He was then a researcher at the Qatar Mobility Innovations Center (QMIC) in Doha, Qatar. His current work is focused on improving the efficiency, security and economics of IoT-enabled smart systems, networks, and infrastructure. He is a recipient of several awards including the President's Gold Medal from NUST, the KAUST Fellowship award from KAUST, the Ernst Weber Fellowship award from NYU, and the Athanasios Papoulis award from NYU.



Cyber-Physical Supply Chain Risk Analysis and Mitigation for Internet of Things Networks

Feb 05, 2020

Junaid Farooq

Center for Cyber Security

New York University

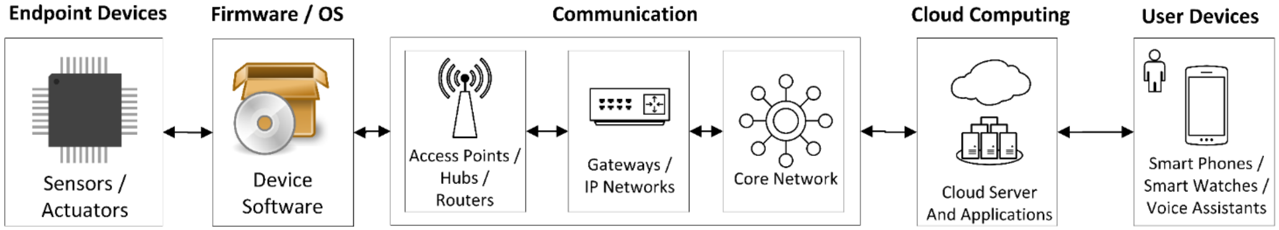
Email: junaid.farooq@nyu.edu

Overview

- IoT becoming ubiquitous in critical infrastructure (CI) systems
- **Cyber-physical integration** creates opportunity for **malicious cyber activity** to undermine performance and/or operation
- IoT ecosystem becoming new **attack surface** for IoT-enabled CI
- Security and resilience of the IoT ecosystem becoming critical

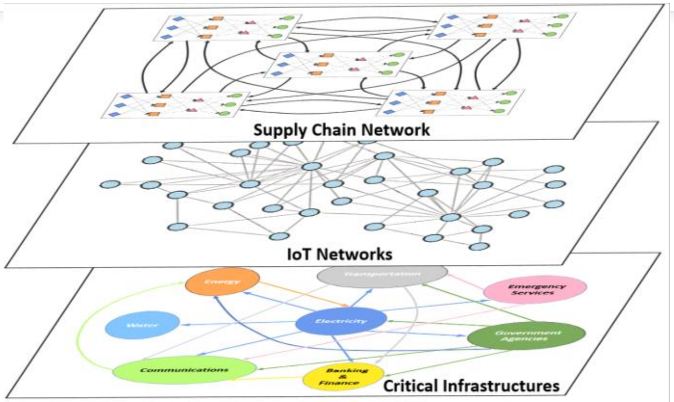
Hypothesis

- IoT is diverse ecosystem: multiple components from multiple suppliers
- Many critical components produced by vendors outside the US
- Integration of multiple components increases vulnerability of IoT-enabled svstems to malicious activitv



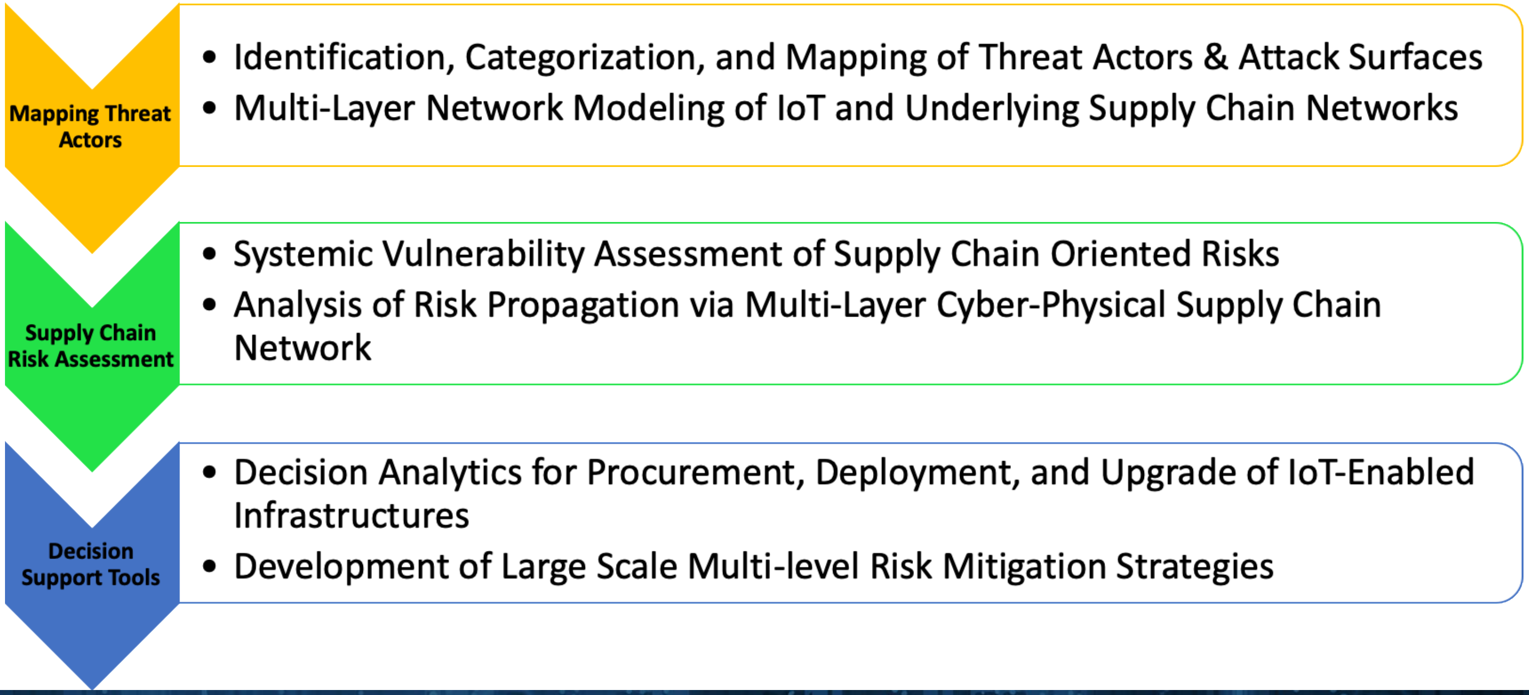
[Farooq and Zhu 2019] IoT Supply Chain Security: Overview, Challenges, and the Road Ahead

Hypothesis



- The interconnection of IoT systems and infrastructure leads to a **complex web of suppliers, manufacturers, and service providers**.
- Multi-layer cyber-physical risk analysis will uncover the underlying web of suppliers and help measure the **intensity of threats** and their **impact on CI**
- By analyzing supply chain oriented risks in IoT systems, we anticipate the ability to make **risk informed decisions** during procurement, deployment, and upgrade of IoT systems

Approach



Mapping Threat Actors

- Identification, Categorization, and Mapping of Threat Actors & Attack Surfaces
- Multi-Layer Network Modeling of IoT and Underlying Supply Chain Networks

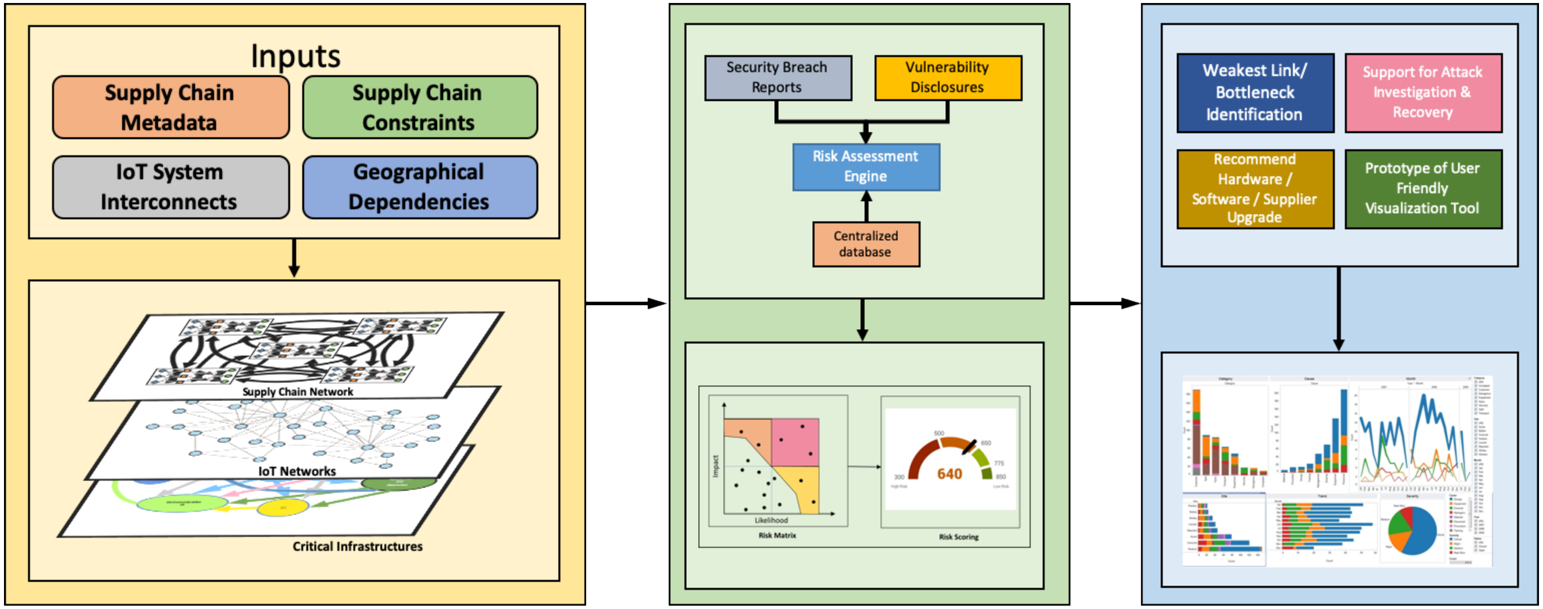
Supply Chain Risk Assessment

- Systemic Vulnerability Assessment of Supply Chain Oriented Risks
- Analysis of Risk Propagation via Multi-Layer Cyber-Physical Supply Chain Network

Decision Support Tools

- Decision Analytics for Procurement, Deployment, and Upgrade of IoT-Enabled Infrastructures
- Development of Large Scale Multi-level Risk Mitigation Strategies

Approach



Inputs

Supply Chain Metadata

Supply Chain Constraints

IoT System Interconnects

Geographical Dependencies

Security Breach Reports

Vulnerability Disclosures

Risk Assessment Engine

Centralized database

Weakest Link/ Bottleneck Identification

Support for Attack Investigation & Recovery

Recommend Hardware / Software / Supplier Upgrade

Prototype of User Friendly Visualization Tool

Multi-Layer Network Mapping of Supply Chain Threat Actors

Risk Scoring and Propagation Analysis

Decision Support and Visualization Tools

Outline

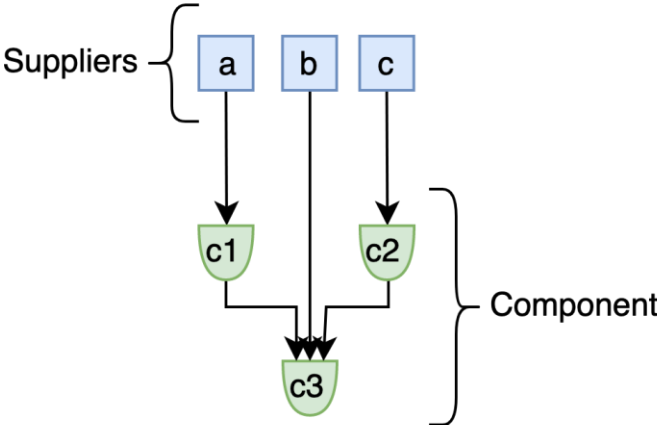
- Tiered Supply Chain Model
- Risk Analysis
- Mitigation Decisions: Supplier Choice Problem
- Case Study & Results

Supply Chain Risk

- How can suppliers be integrated into security risk analysis in a consistent way?
- Attack trees could be designed with nodes for suppliers
  - But given that a supplier could modify the system in very unexpected ways, how could this attack graph be meaningful?
- How can this undefined risk be quantified, and what assumptions are needed?

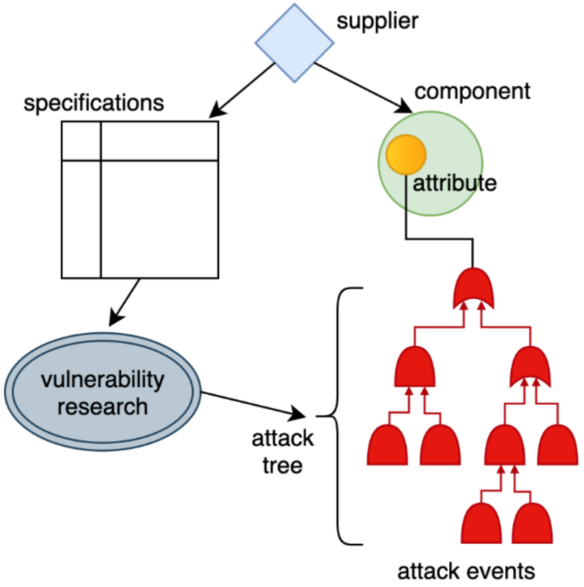
System Model Introduction

- Directed Graph
  - Nodes: Components and Suppliers
  - Edges: Security Dependencies
  - Components have AND/OR logic (as in attack graphs)
  - Security of a node r_i fails in three ways:
    - on its own
      - probability
    - if its supplier's security *j* fails
      - probability 1- t_j
      - or if its dependencies fail
        - AND/OR({dependencies})
- System state is secure if a designated set of nodes are secure



Supplier Involvement

- Suppliers play an essential role in providing information about the nature of a system.
- Assume this information is the basis of a security risk value
- Supplier trust therefore limits the accuracy of risk values.



[Kieras, Farooq, and Zhu 2019] RIoTS: Risk Analysis of IoT Supply Chain Threats

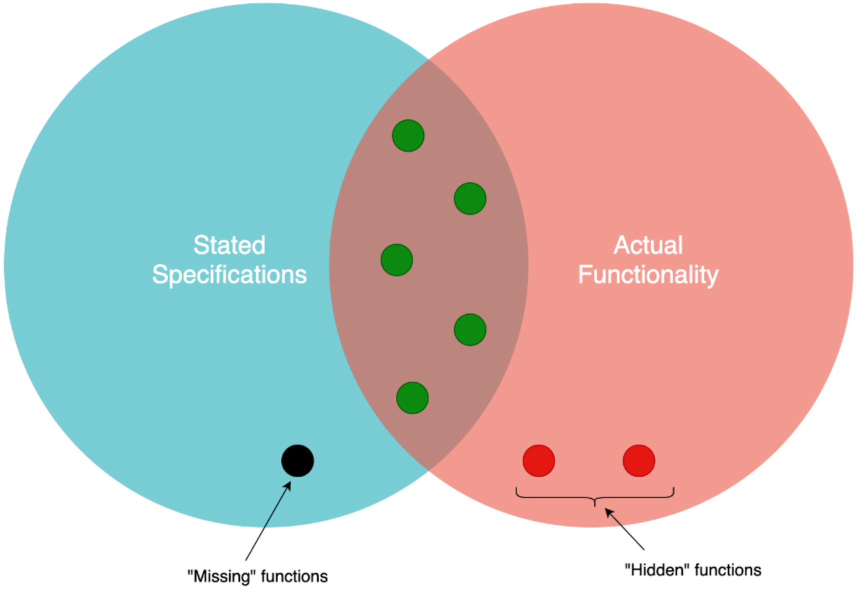
Supplier Trust as Probability

- A component is characterized by the functions it implements.
- Functions can be actual/real or only alleged/putative.
- Where

  P = Putative Functions

  A = Actual Functions

- Trust = $\dfrac{|P \cap A|}{|P \cup A|}$

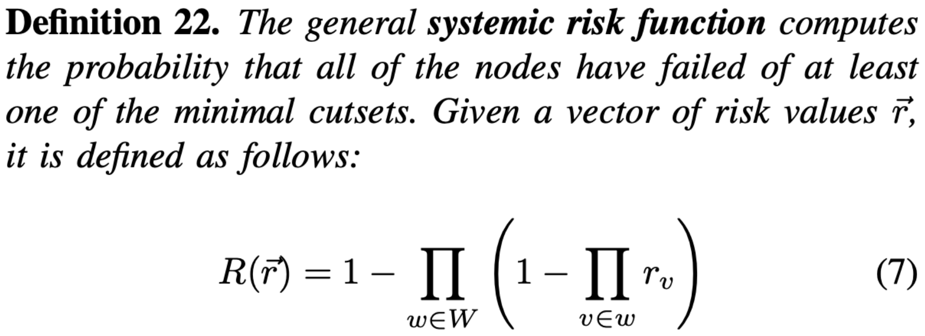


System Model Attributes

- System model can be analyzed in two ways:
  - Component nodes have AND/OR logic representing different relationships to dependencies.
  - Suppliers may belong to groups or be dependent on other suppliers.

Risk Function

- Analogous to system reliability, conditions of a security failure are captured by the minimal cutsets (W). Risk is the probability that at least one of the cutsets has been fully attacked.



Definition 22. *The general* ***systemic risk function*** *computes the probability that all of the nodes have failed of at least one of the minimal cutsets. Given a vector of risk values $\vec{r}$, it is defined as follows:*

$$R(\vec{r}) = 1 - \prod_{w \in W} \left(1 - \prod_{v \in w} r_v \right) \qquad (7)$$

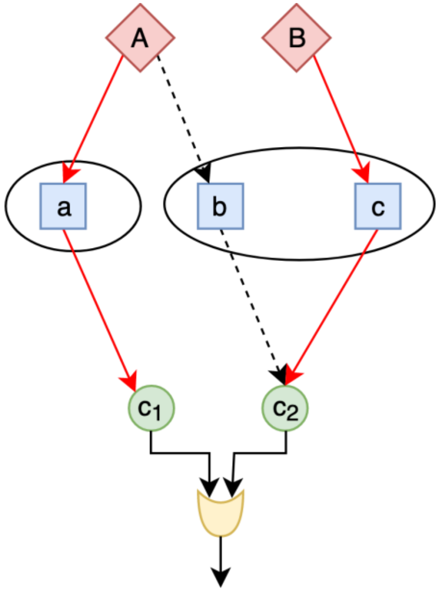
Importance Measures

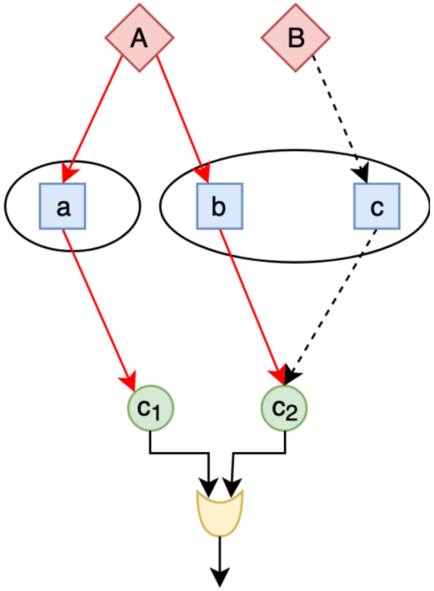
- Also from system reliability analysis, nodes can be ranked by importance using different measures, such as:
  - Improvement Potential
  - Birnbaum Importance (Sensitivity)
    - Used in mitigation decisions

$$BI_i = \frac{\partial R(r)}{\partial r_i}$$

Mitigation: Supplier Choice Problem

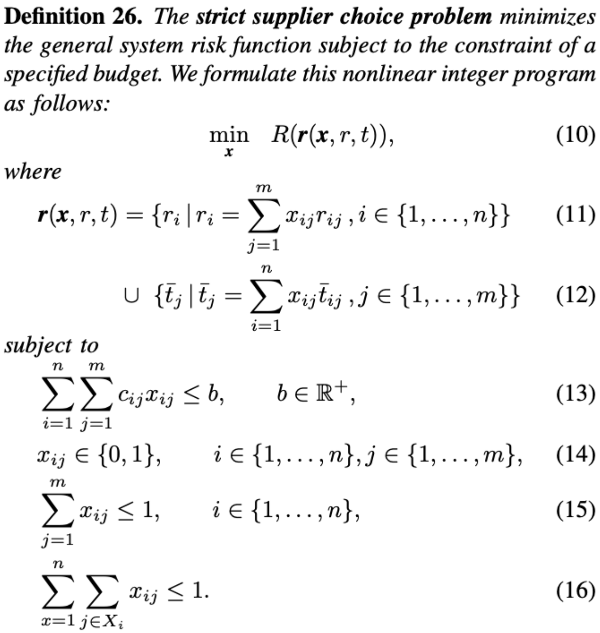
Two Possible Solutions





Mitigation: Supplier Choice Problem

Basic Formulation:



Definition 26. *The **strict supplier choice problem** minimizes the general system risk function subject to the constraint of a specified budget. We formulate this nonlinear integer program as follows:*

$$\min_{\boldsymbol{x}} \quad R(\boldsymbol{r}(\boldsymbol{x}, r, t)), \tag{10}$$

where

$$\boldsymbol{r}(\boldsymbol{x}, r, t) = \{r_i \,|\, r_i = \sum_{j=1}^{m} x_{ij} r_{ij} \,, i \in \{1, \dots, n\}\} \tag{11}$$

$$\cup \;\; \{\bar{t}_j \,|\, \bar{t}_j = \sum_{i=1}^{n} x_{ij} \bar{t}_{ij} \,, j \in \{1, \dots, m\}\} \tag{12}$$

subject to

$$\sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij} x_{ij} \leq b, \qquad b \in \mathbb{R}^{+}, \tag{13}$$

$$x_{ij} \in \{0, 1\}, \qquad i \in \{1, \dots, n\}, j \in \{1, \dots, m\}, \tag{14}$$

$$\sum_{j=1}^{m} x_{ij} \leq 1, \qquad i \in \{1, \dots, n\}, \tag{15}$$

$$\sum_{x=1}^{n} \sum_{j \in X_i} x_{ij} \leq 1. \tag{16}$$

Chief Problem:

(1) The risk function requires minimal cutsets (NP-Hard). This is arguably necessary for risk analysis as a one-time cost, but it is infeasible to use the risk function as the objective, when each possible solution requires this operation to evaluate.

Mitigation: Using Approximations

Birnbaum Importance
(Risk Importance)

$$\min_{\boldsymbol{x}} \sum_{j=1}^{m} \sum_{i=1}^{n} x_{ij} r_{ij} I_i$$

We find that using the Birnbaum Importance to weight component risks functions as a useful approximation when optimizing for minimal risk.

Computing the Birnbaum Importance
for each component requires the minimal cutsets
of the component graph.
This is a one-time cost.

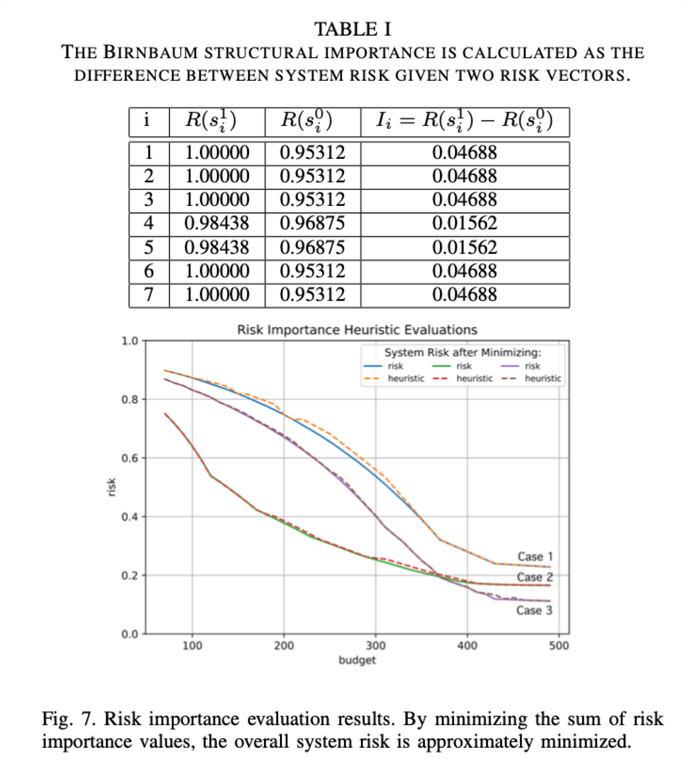


TABLE I
THE BIRNBAUM STRUCTURAL IMPORTANCE IS CALCULATED AS THE DIFFERENCE BETWEEN SYSTEM RISK GIVEN TWO RISK VECTORS.

i	$R(s_i^1)$	$R(s_i^0)$	$I_i = R(s_i^1) - R(s_i^0)$
1	1.00000	0.95312	0.04688
2	1.00000	0.95312	0.04688
3	1.00000	0.95312	0.04688
4	0.98438	0.96875	0.01562
5	0.98438	0.96875	0.01562
6	1.00000	0.95312	0.04688
7	1.00000	0.95312	0.04688

Fig. 7. Risk importance evaluation results. By minimizing the sum of risk importance values, the overall system risk is approximately minimized.

Mitigation: Using Approximations

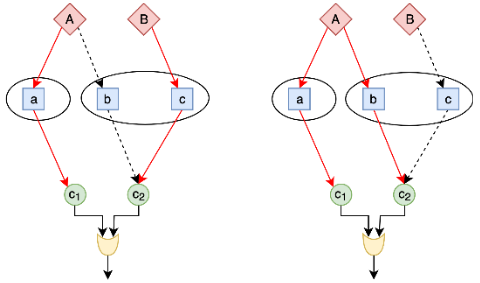
Supplier Involvement

Intuition: The risk posed by a supplier is a non-linear function of the number of components it supplies.

We improve the accuracy of this by weighting the value of a supplier by the Birnbaum Importance of the component(s) it supplies, and the risk/trust of the supplier.

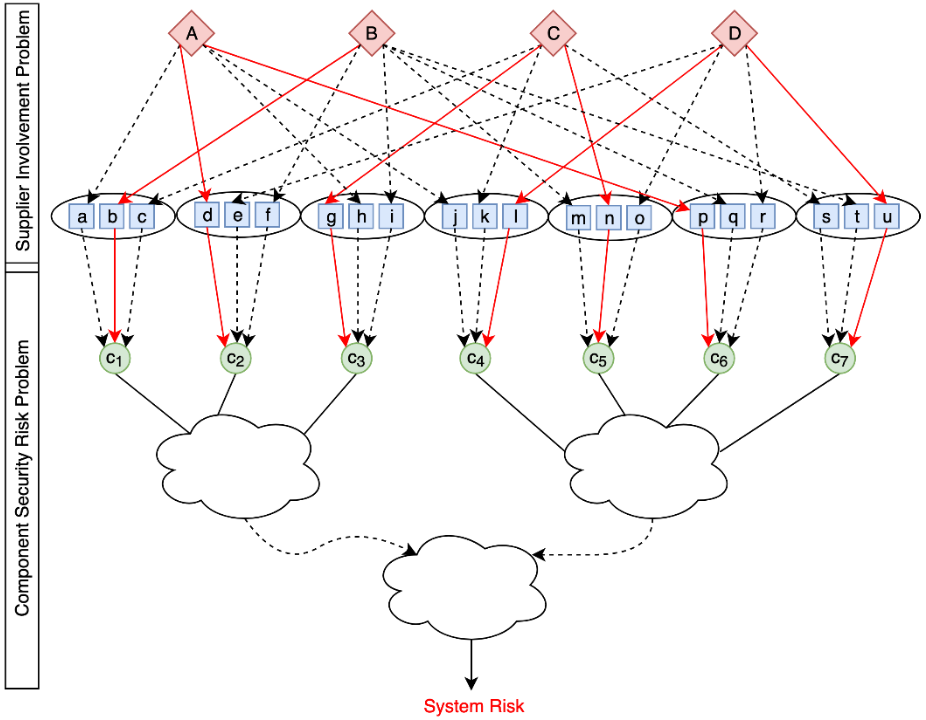
$$\min_{x} \sum_{k=1}^{K} \Big(\sum_{j \in G_k} \sum_{i=1}^{n} x_{ij} I_i \Big)^2 \bar{t}_k$$

Two Solutions

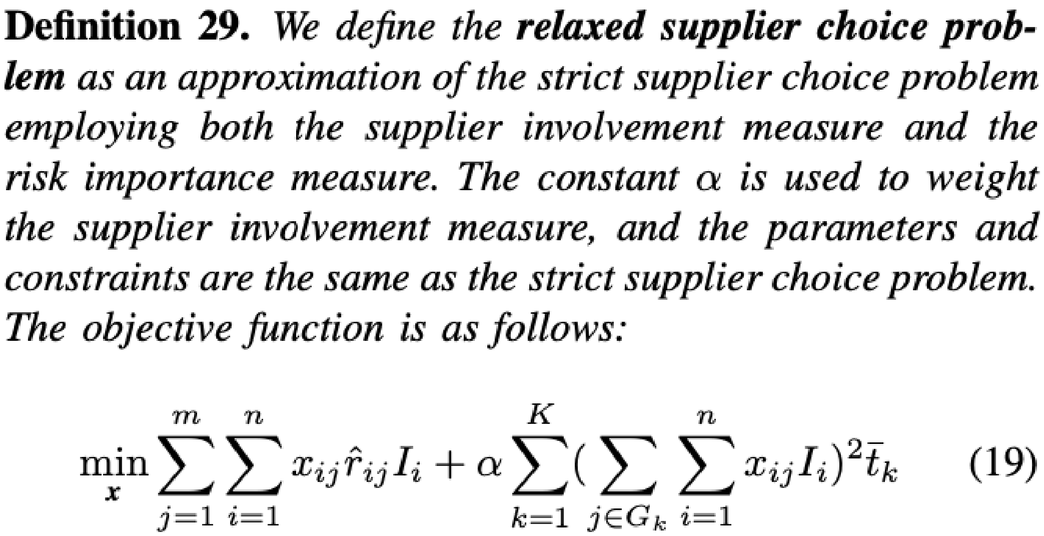


In Solution 1 (left), controllers A and B have same involvement.
In Solution 2 (right), controller A has more involvement than B.
Generally, Solution 1 should be preferred to Solution 2, if all other variables are equal.

Supplier Choice Scenario



Mitigation: Using Approximations

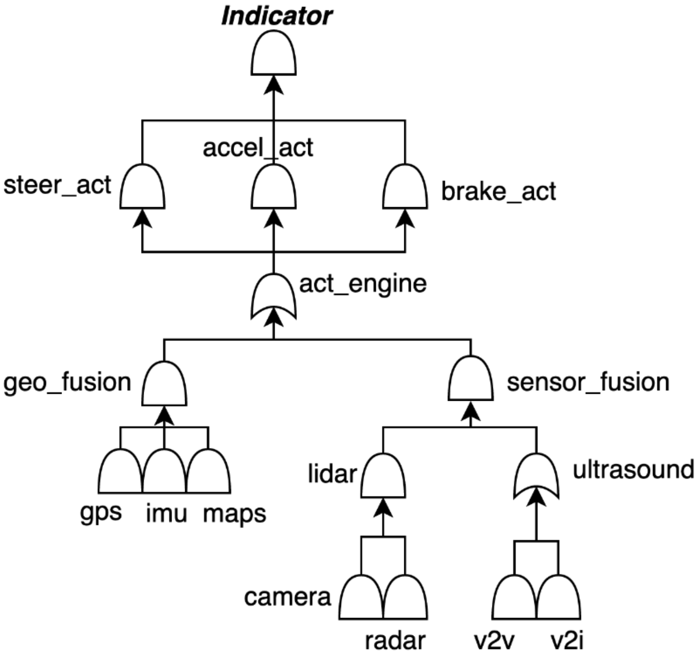


Definition 29. *We define the* ***relaxed supplier choice problem*** *as an approximation of the strict supplier choice problem employing both the supplier involvement measure and the risk importance measure. The constant* α *is used to weight the supplier involvement measure, and the parameters and constraints are the same as the strict supplier choice problem. The objective function is as follows:*

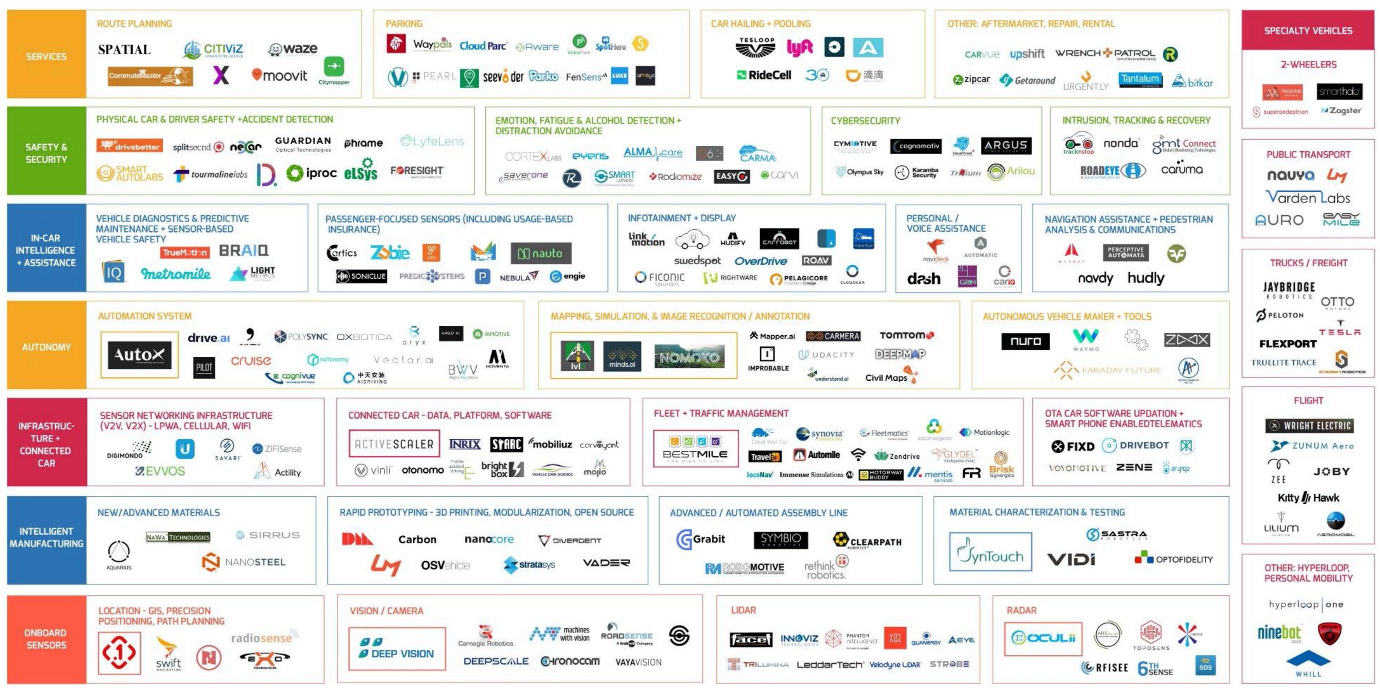
$$\min_{\boldsymbol{x}} \sum_{j=1}^{m}\sum_{i=1}^{n} x_{ij}\hat{r}_{ij}I_i + \alpha\sum_{k=1}^{K}\Big(\sum_{j\in G_k}\sum_{i=1}^{n} x_{ij}I_i\Big)^2\bar{t}_k \tag{19}$$

With a case study and simulation, we study the results of optimizing with this objective function.

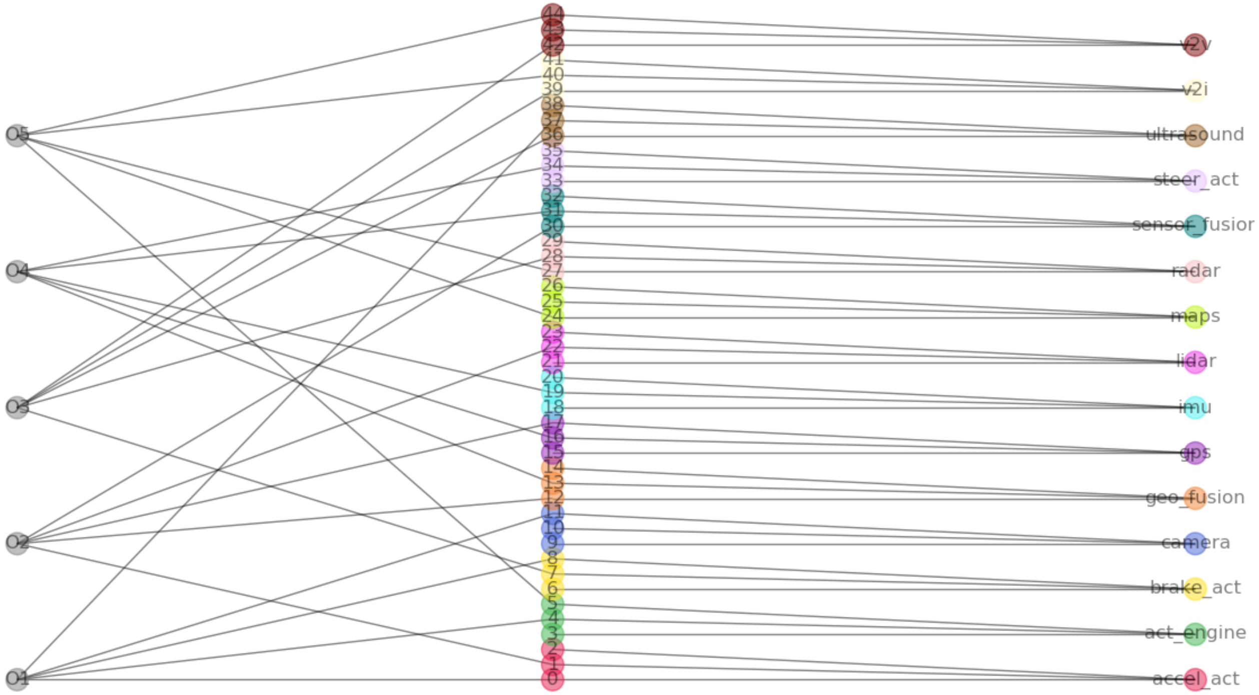
Case Study: Autonomous Car



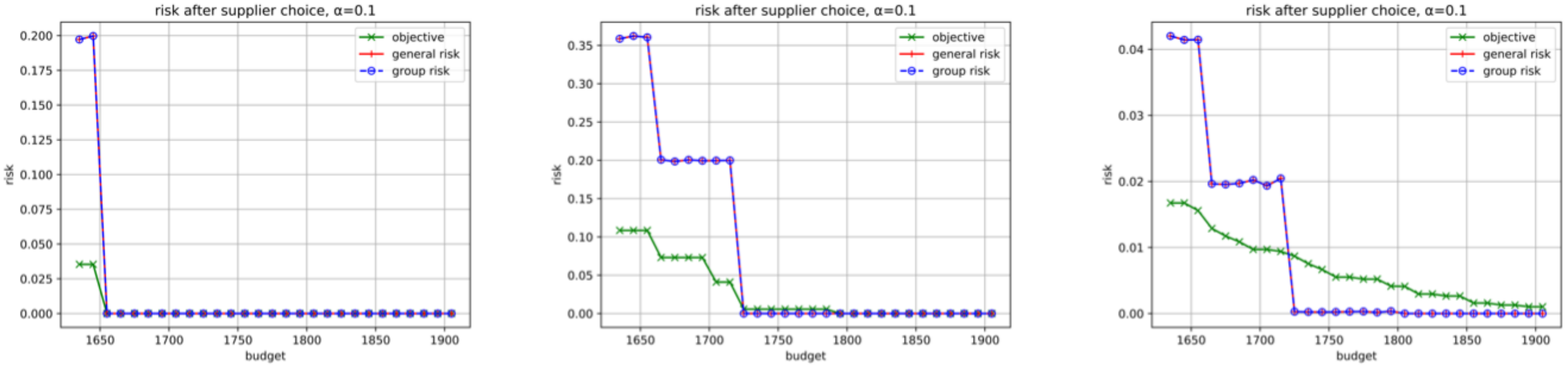
Supplier Footprint in Autonomous Vehicles



Supplier Choice in Autonomous Car



Optimized choice with simulated risk



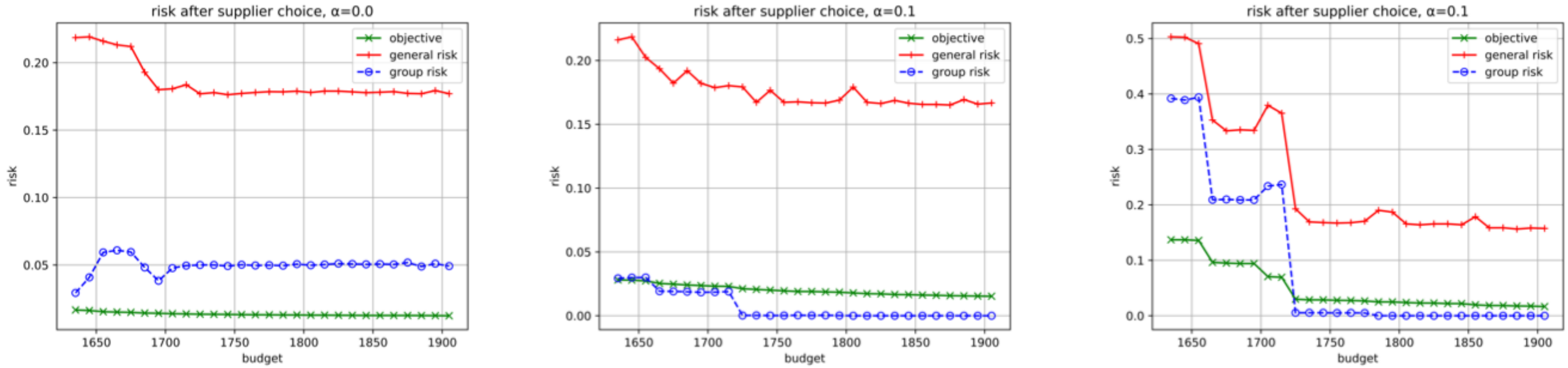
(a) Case 1 Results, $\alpha = 0.1$

(b) Case 2 Results, $\alpha = 0.1$

(c) Case 3 Results, $\alpha = 0.1$

Fig. 9. Results for simple cases. General and group risks overlap and decrease with higher budgets.

- To test the objective function, we developed a set of simple parameters where risk originates only from supplier groups.
- Further cases evaluated the performance with more developed parameters, where risk arises from components, suppliers, and supplier groups.
- In all cases, as the budget increased, minimizing the objective function produced a system with decreasing risk.



(a) Case 5 Results, $\alpha = 0.0$

(b) Case 5 Results, $\alpha = 0.1$

(c) Case 6 Results, $\alpha = 0.1$

Fig. 11. More complex cases confirm the risk minimizing performance along with the effect of prioritizing general and group risk.

- More complex parameters exhibit a trade-off between the two terms in the objective function: either minimizing general risk or minimizing the risk of a supplier-caused incident.

- This trade-off is controlled by the alpha constant that weights the two terms in the objective function.

$$\min_{\boldsymbol{x}} \sum_{j=1}^{m}\sum_{i=1}^{n} x_{ij}\hat{r}_{ij}I_i + \alpha \sum_{k=1}^{K}\Big(\sum_{j\in G_k}\sum_{i=1}^{n} x_{ij}I_i\Big)^2\bar{t}_k \qquad (19)$$

General RIsk

Supplier Caused Risk

Summary

- Supply Chain is a new attack vector in the IoT ecosystem
- Analysis of supplier induced risk in complex networks of networks scenarios is challenging
- Coordinated efforts are required to analyze the risks and take risk mitigation decisions relating to supplier choices

Future Work

- Causal Inference in Multi-Stage problem
    - Given a choice and an incident (component security failures) with an unknown cause, how to assess possible supplier involvement?
        - Updating the choice incorporating changed risk/trust values.
- Dealing with Uncertainties
    - Learning risk/trust values based on choice-result cycles

Questions

Open Discussion

Any questions about the Auto-ISAC or future topics for discussion?

Event Outlook

Connect with us at upcoming events:	
International Conference on Cyber Security and Connected Technologies	Feb. 3-4, Tokyo, Japan
Riscure US Roadshow 2020	Feb. 3, Boston, MA Feb. 4, Baltimore, MD Feb. 6, Detroit, MI Feb. 7, Huntsville, AL
Auto-ISAC Community Call***	Feb. 5, Telecon
Suits and Spooks Taking Ownership of our Security Challenges for the Next 10 Years	Feb. 6-7, Washington, DC
ATA Technology & Maintenance Council (TMC) Annual Meeting & Transportation Technology Exhibition	Feb. 24- 27, Atlanta, GA
Munich Security Conference	Feb. 14-16, Munich, Germany
Cyber Security in Future Mobility	Feb. 17-19, Mountain View, CA
Security BSides San Francisco	Feb. 23-24, San Francisco, CA
AV Silicon Valley 2020	Feb. 24-26, Silicon Valley, CA
RSA Conference 2020	Feb. 24-28, San Francisco, CA

**For full 2019 calendar, visit www.automotiveisac.com

How to Get Involved: Membership

If you are an OEM, supplier or commercial vehicle company, now is a great time to join Auto-ISAC!

- *Real-time Intelligence Sharing*
- *Intelligence Summaries*
- *Regular intelligence meetings*
- *Crisis Notifications*
- *Member Contact Directory*
- *Development of Best Practice Guides*
- *Exchanges and Workshops*
- *Tabletop exercises*
- *Webinars and Presentations*
- *Annual Auto-ISAC Summit Event*

To learn more about Auto-ISAC Membership or Partnership, please contact Auto-ISAC Staff (staff@automotiveisac.com).

Strategic Partnership Programs

Solutions Providers

For-profit companies that sell connected vehicle cybersecurity products & services.

Examples: Hacker ONE, SANS, IOActive

INNOVATOR

Paid Partnership

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed

Associations

Industry associations and others who want to support and invest in the Auto-ISAC activities.

Examples: Auto Alliance, Global Auto, ATA

NAVIGATOR

Support Partnership

- Provides guidance and support
- Annual definition of activity commitments and expected outcomes
- Provides guidance on key topics / activities

Affiliations

Government, academia, research, non-profit orgs with complementary missions to Auto-ISAC.

Examples: NCI, DHS, NHTSA

COLLABORATOR

Coordination Partnership

- "See something, say something"
- May not require a formal agreement
- Information exchanges-coordination activities

Community

Companies interested in engaging the automotive ecosystem and supporting - educating the community.

Examples: Summit sponsorship – key events

BENEFACTOR

Sponsorship Partnership

- Participate in monthly community calls
- Sponsor Summit
- Network with Auto Community
- Webinar / Events

Auto-ISAC Benefits

- ➢Focused Intelligence Information/Briefings
- ➢Cybersecurity intelligence sharing
- ➢Vulnerability resolution
- ➢Member to Member Sharing
- ➢Distribute Information Gathering Costs across the Sector
- ➢Non-attribution and Anonymity of Submissions
- ➢Information source for the entire organization
- ➢Risk mitigation for automotive industry
- ➢Comparative advantage in risk mitigation
- ➢Security and Resiliency

Securing Across the Auto Industry

Our contact info

Faye Francy
Executive Director

20 F Street NW, Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

Josh Poster
Program Operations Manager

20 F Street NW, Suite 700
Washington, DC 20001
joshposter@automotiveisac.com

Michelle Menner
Organization Coordinator

20 F Street NW, Suite 700
Washington, DC 20001
michellemenner@automotiveisac.com