Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

Automotive Security Analyzer for Exploitability Risks

An Automated and Attack Graph-Based Evaluation of On-Board Networks

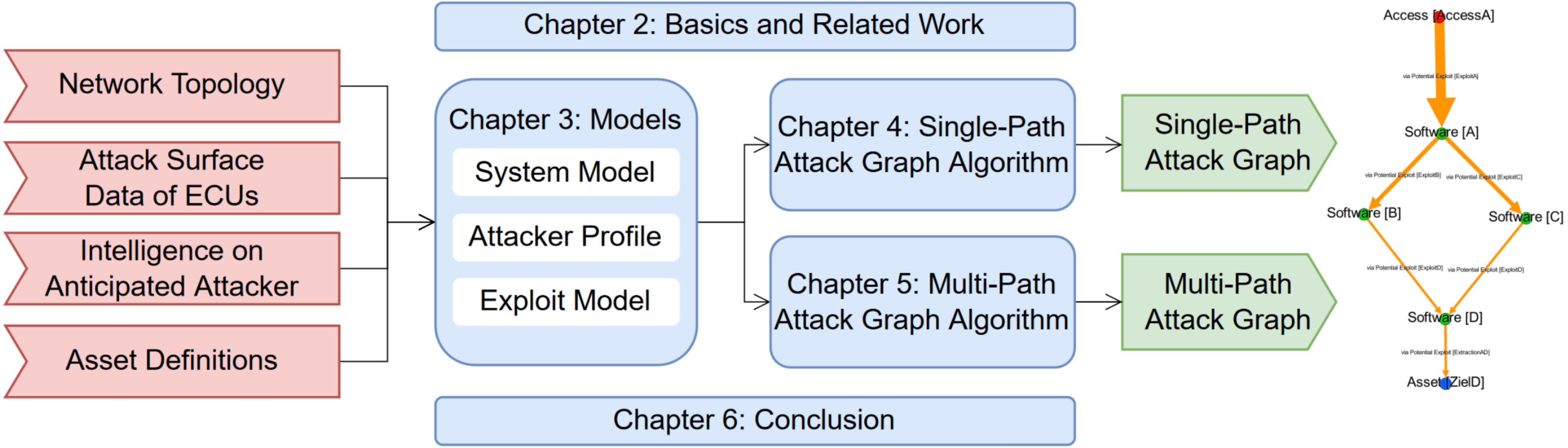


Image Sources: Salfer

Questions and Disclaimer

Feel free to ask questions at any time, even during the talk. I will repeat them for the recording.

- Short questions during the talk.
- Normal questions during the Q&A, or afterwards.

Disclaimer

- Personal opinions only - not employers' views.
- Automotive Security Analyzer for Exploitability Risks Proof of Concept approved, but surrounding tools/processes NOT.
- Informational purposes only - no liability.
- Third-party IP remains with owners.

> whoami

Academia:

- TUM: PhD in “**Automotive Security Analyzer for Exploitability Risks**: An Automated and Attack Graph-Based Evaluation of On-Board Networks”.
- National Institute of Informatics in Tokio, Japan on content security.

Industry:

- Research and Development for **On-Board Networks 2008-2015**.
- In IT Security full time for 14 years.

Study:

- TUM/LMU/UniA: M. Sc. with honours in Software Engineering.
- HM/KPU: B.Sc. in Computer Science.

Military: Electronic Warfare Battalion 932 in Frankenberg/Eder.

Image Sources: TUM, BMW, NII, LMU, UniA, Bw, HM, KPU

Agenda

1. **Motivation**
   - Problem: Larger Attack Surface and More Attacks
   - Vision: Attack Graphs with Risk Annotations
   - C1 Survey
2. **Data and Models**
   - C2 System Model, Attacker Profile, a. Exploit M.
   - C3 Attack Surface Exploitability Quantification
   - C4 Implementation and Evaluation of Models
3. **Practical Demo**
4. **Algorithms for Attack Graphs**
   - C5 Single-Path Attack Graph Algorithm (PI+PII)
   - C6 Implementation and Evaluation of PI+PII
5. **Algorithms for Total Risk**
   - C7 Probabilistic Model
   - C8 Multi-Path Attack Graph Algorithm (P3Salfer)
   - C9 Bayes Network Unsuitability Finding
   - C10 Design and Implementation of an Alternative Algorithm with Bayesian Networks (P3Bayes)
   - C11 Implementation and Evaluation of the Multi-Path Attack Graph Algorithm (P3Salfer)
6. **Future Work**
7. **Further Material Overview**

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

Larger Attack Surface and Assets Raise the Protection Level

Vehicles connect to the whole world.
Vehicles carry our credentials and our lives.

Image Sources: Lehmann, Leoni and Intel

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

C1: Survey: Tools and Standards Boost Hacking

Some hacking examples:

- **Chevrolet Impalla**: Koscher et al. @ S&P 2010 and Checkoway et al. @ Usenix Security 2011;
- **Keyless Entry**: Rouf et al. @ Usenix Sec. 2010 and Verdult/Garcia/Balsch @ Usenix Sec. 2012;
- **Jeep**: Miller/Valasek @ BlackHat 2015.
- **Tesla Model S**: Rogers/Mahaffey @ Def Con 23 and Keen Labs in 2016 and @ Blackhat ‘17;
- **Public Charging**: see Dalheimer @ 34C3.
- **Tesla’s Passive Entry system**: See Herfurt @ Troopers22

Image Sources: Checkoway et al., Koscher et al., Rouf et al., Greenberg, Francillon et al., Keen Labs.

Stakeholder to Support on Potential Security Risks

Architects: „How bad would this affect security?“

Penetration Tester: “Where to look at first?”

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

Vision: Attack Graphs with Risk Annotations

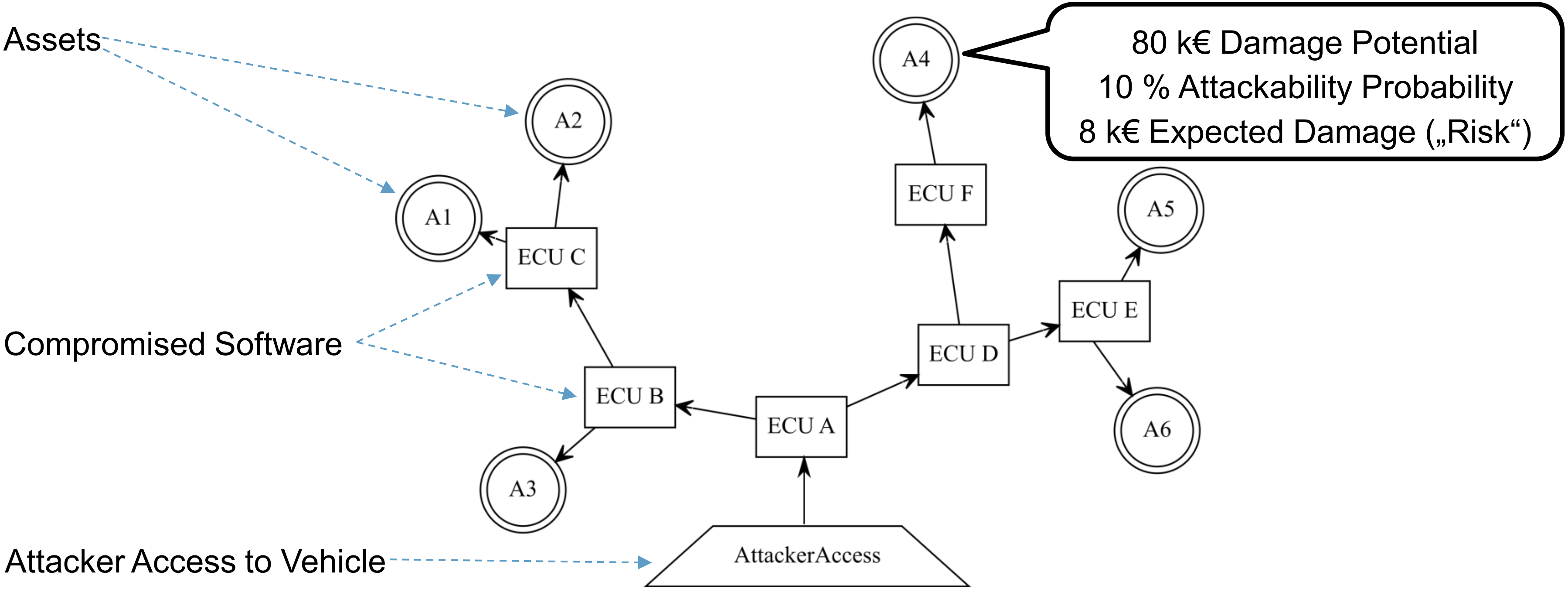


Image Sources: Salfer

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

C1: Survey: From Safety Analysis to Security Automation

<u>1980s: Safety Precursors</u>
FTA (Fault Tree Analysis), FMEA (Failure Modes and Effects Analysis).

<u>1990s: Attack Trees</u>
E. Amoroso(Bell Labs), Salter (NSA), Schneier.

<u>2000s: Automated Construction</u>
Sheyner et al. und Ou et al.

<u>2010s: Automated Sourcing and Effects</u>
Roschke et al. (HPI-VDB and IDS).

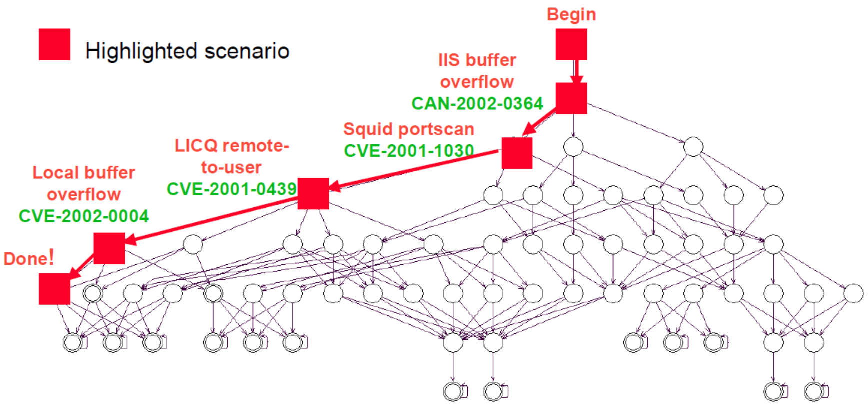
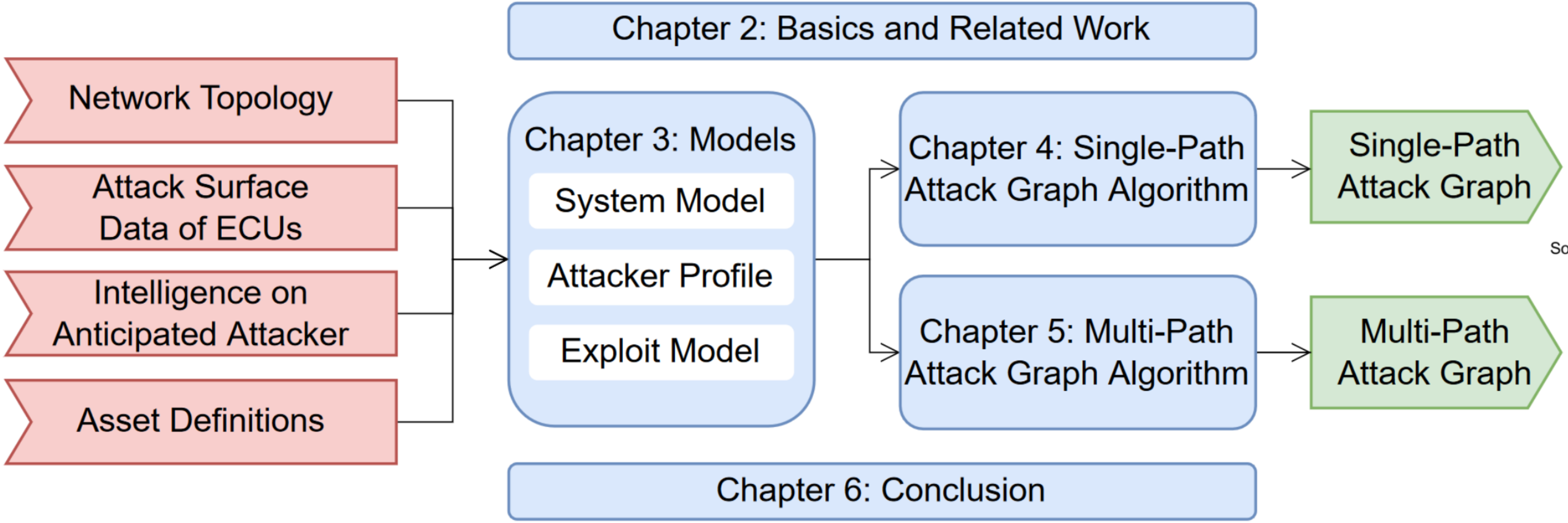


Image Sources: Sheyner

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

Automotive Security Analyzer for Exploitability Risks (AutoSAlfER)

An Automated and Attack Graph-Based Evaluation of On-Board Networks



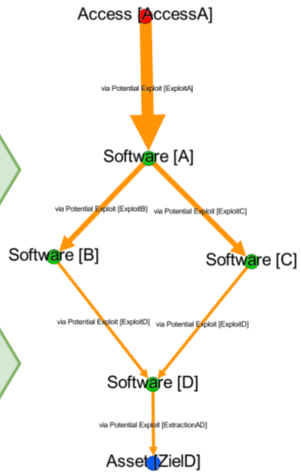
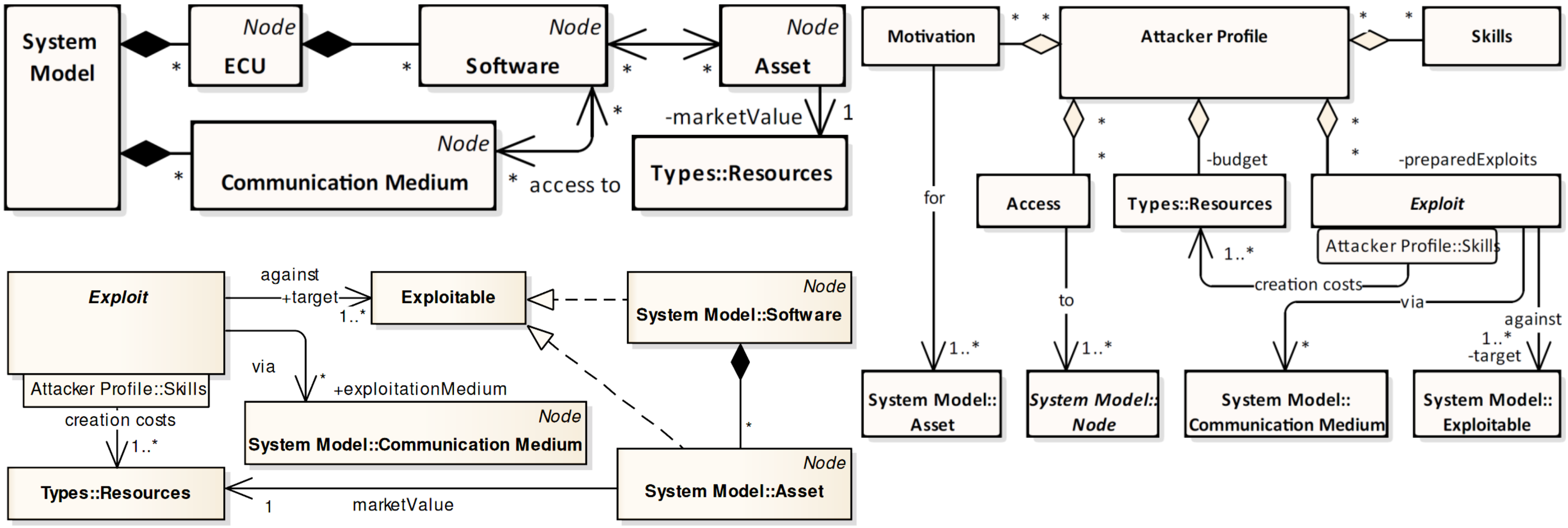


Image Sources: Salfer

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

C2: System Model, Attacker Profile, and Exploit Model



C3: Attack Surface Exploitability Quantification

Possibility for a vulnerability:

$$P_B(X > 0) = 1 - P_B(X = 0) = 1 - q^i = 1 - (1 - v)^i$$

Total effort estimation:

$$\bar{\mathscr{C}}_E = s_{sf0} + s_{\bar{s}fi} \left(s_{sv} \sum_{i=1}^{i=k} \left(i\,(1 - s_{sv})^{i-1} \right) + k\,(1 - s_{sv})^{k} \right) + s_{\bar{s}a} + s_{\bar{s}b} + s_{\bar{s}c}$$

… see the paper on SECRYPT 2015

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

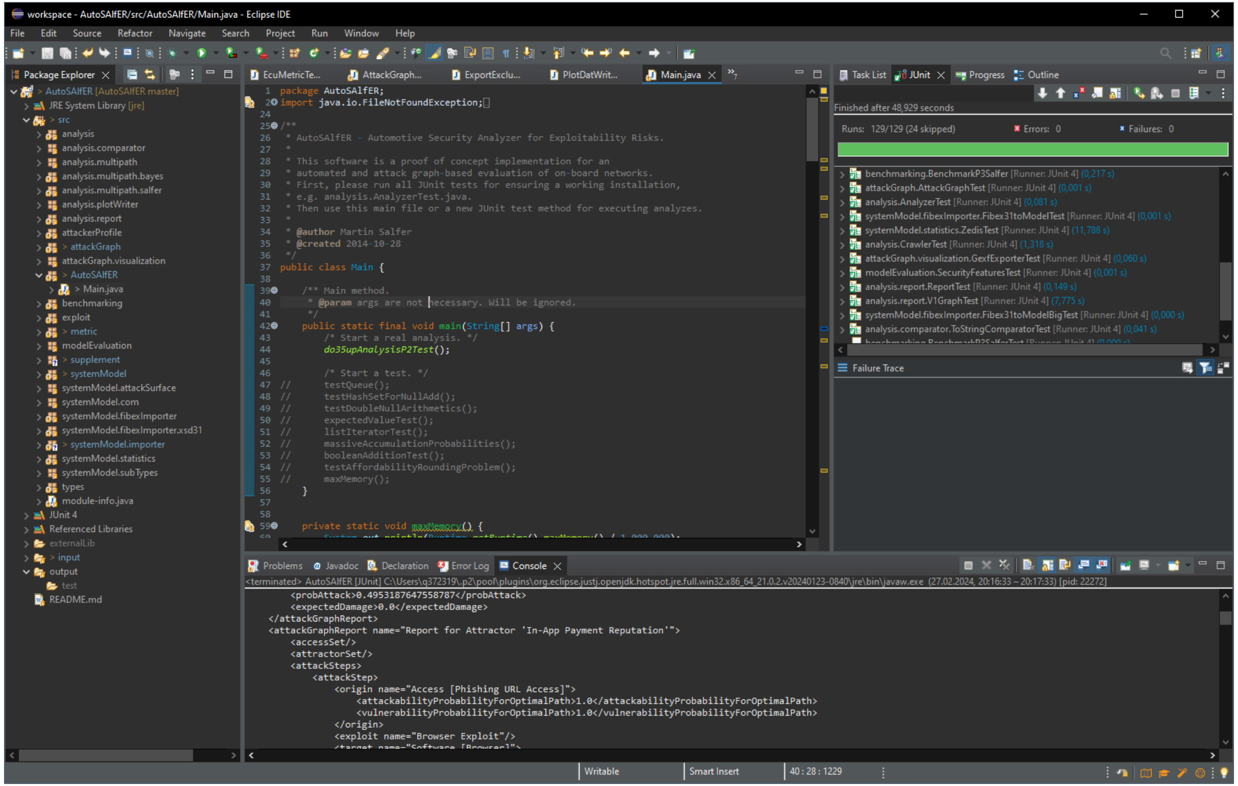
C4: Implementation and Evaluation of the Models and the Attack Surface Exploitability Quantification


```
        REF="_93bda6eb477b49a48417cb897d075c41_25_64ca21c7bf884ed1948ed94cadb4ce33_13"/>
      </fx:SIGNAL-TRIGGER>
    </fx:SEND-CONDITION>
    <ho:DESC xml:lang="de" TYPE="Standard">Die Nachricht wird - ab Klemme 15 EIN - bei jeder Änderung eines
      versandt.</ho:DESC>
  - <fx:MANUFACTURER-EXTENSION xsi:type="[redacted]MANUFACTURER-EVENT-CONTROLLED-TIMING-EXTENSION">
    - <[redacted]N-SEND-CONDITION>
      - <[redacted]SIGNAL-TRIGGER-ON-VALUE-CHANGED>
          <[redacted]IGNAL-INSTANCE-REF ID-
            REF="_93bda6eb477b49a48417cb897d075c41_25_65578f269cce4492bdf2a550e3eecd13_5"/
          <[redacted]IGNAL-INSTANCE-REF ID-
            REF="_93bda6eb477b49a48417cb897d075c41_25_64ca21c7bf884ed1948ed94cadb4ce33_13
        <[redacted]SIGNAL-TRIGGER-ON-VALUE-CHANGED>
      <[redacted]N-SEND-CONDITION>
    </fx:MANUFACTURER-EXTENSION>
  </fx:EVENT-CONTROLLED-TIMING>
</fx:TIMINGS>
<fx:PDU-REF ID-REF="_93bda6eb477b49a48417cb897d075c41_25"/>
```


- Tech Stack: Java with xmlbeans, poi, poi-ooxml, gexf4j, StAX, and JUnit
- Ingest File Types:
  – FIBEX,
  – OfficeOpenXML, and
  – XLS
- Output File types:
  – GraphViz DOT
  – GEXF

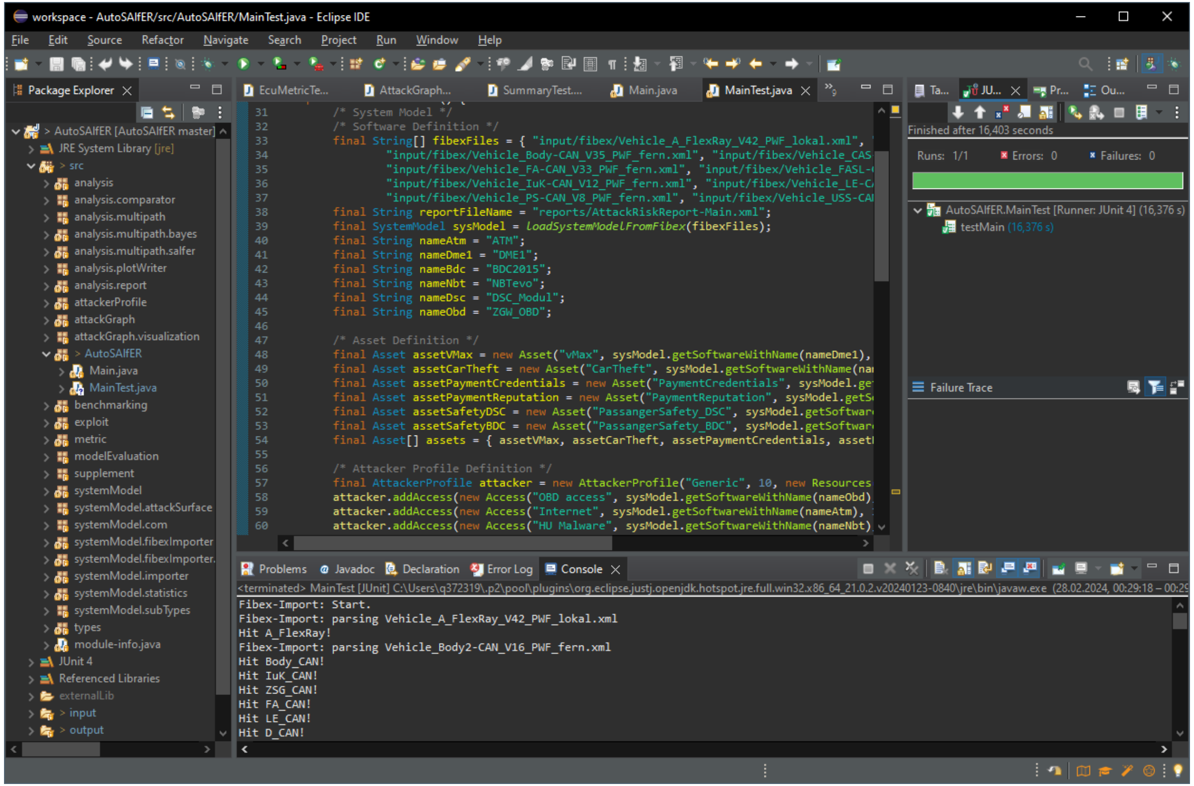
Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

Demo
main

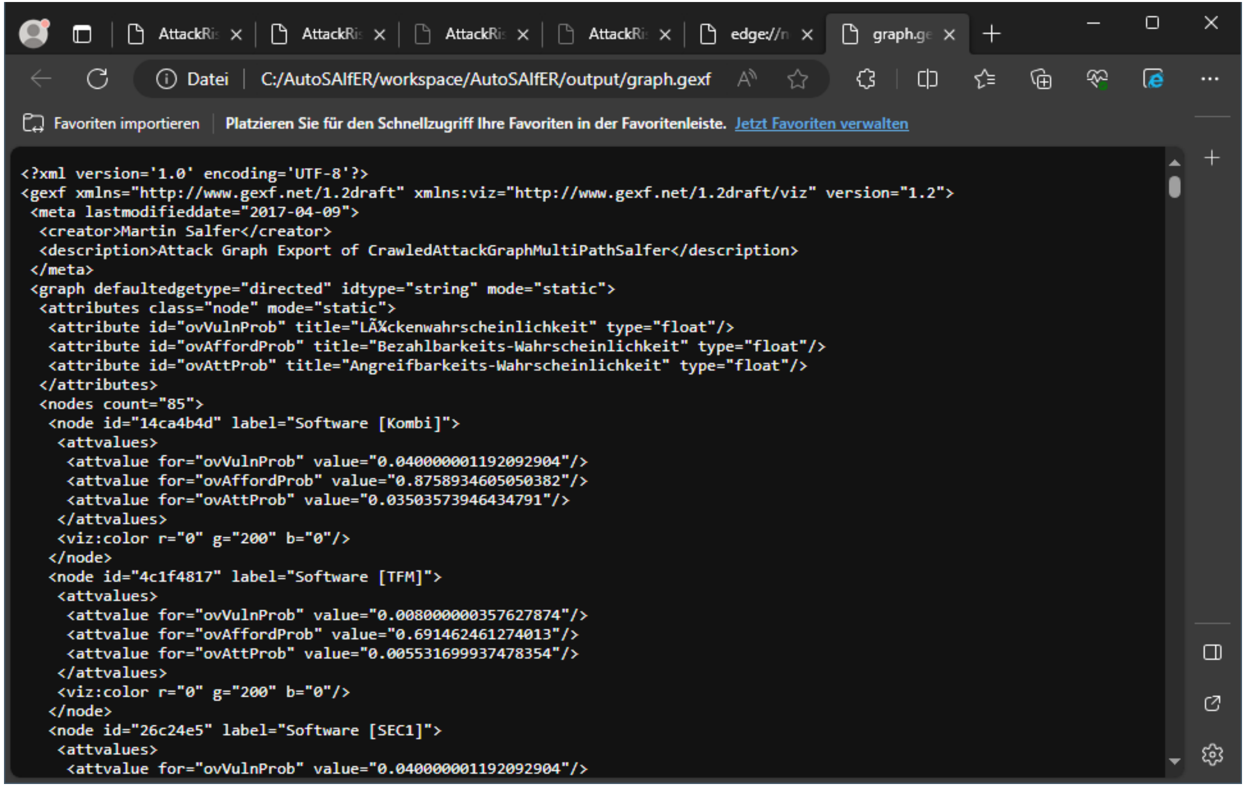


Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

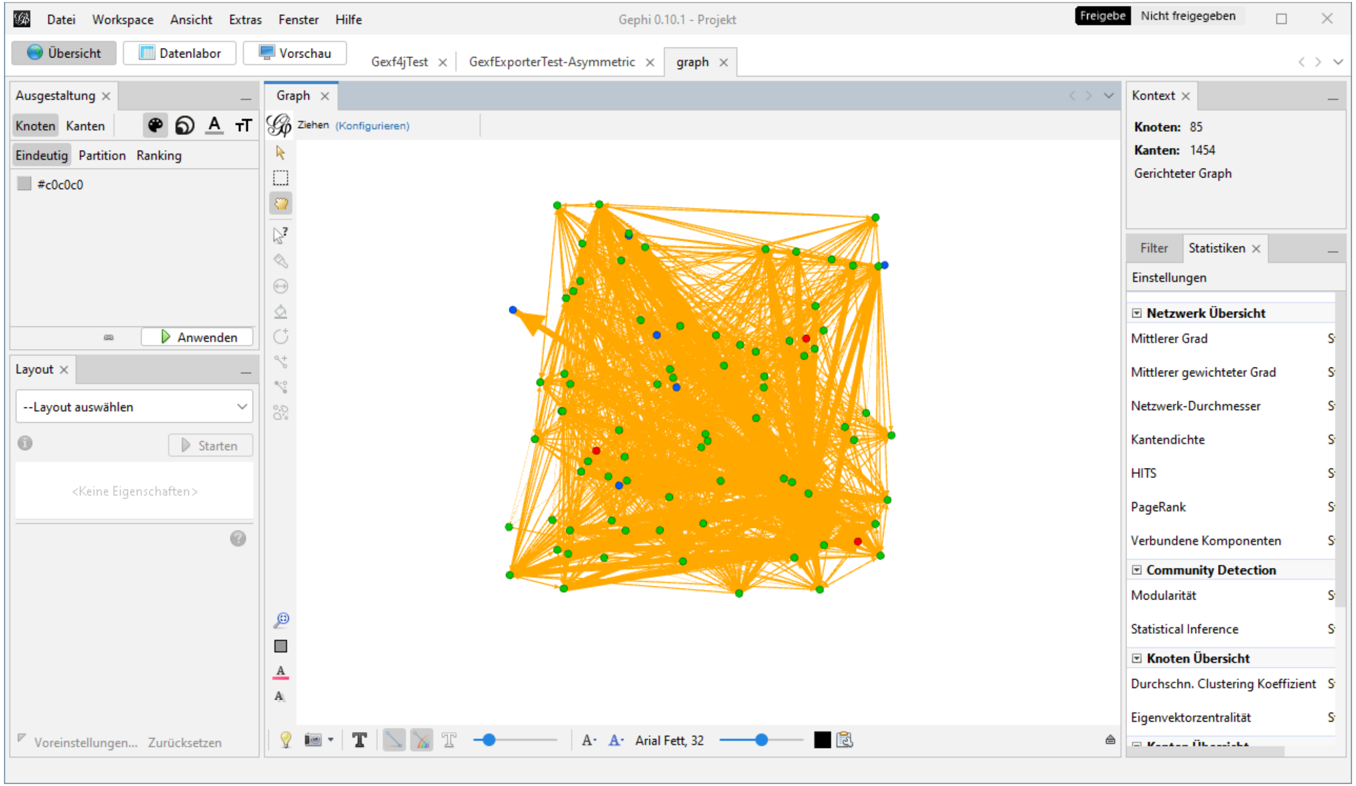
Demo
Input



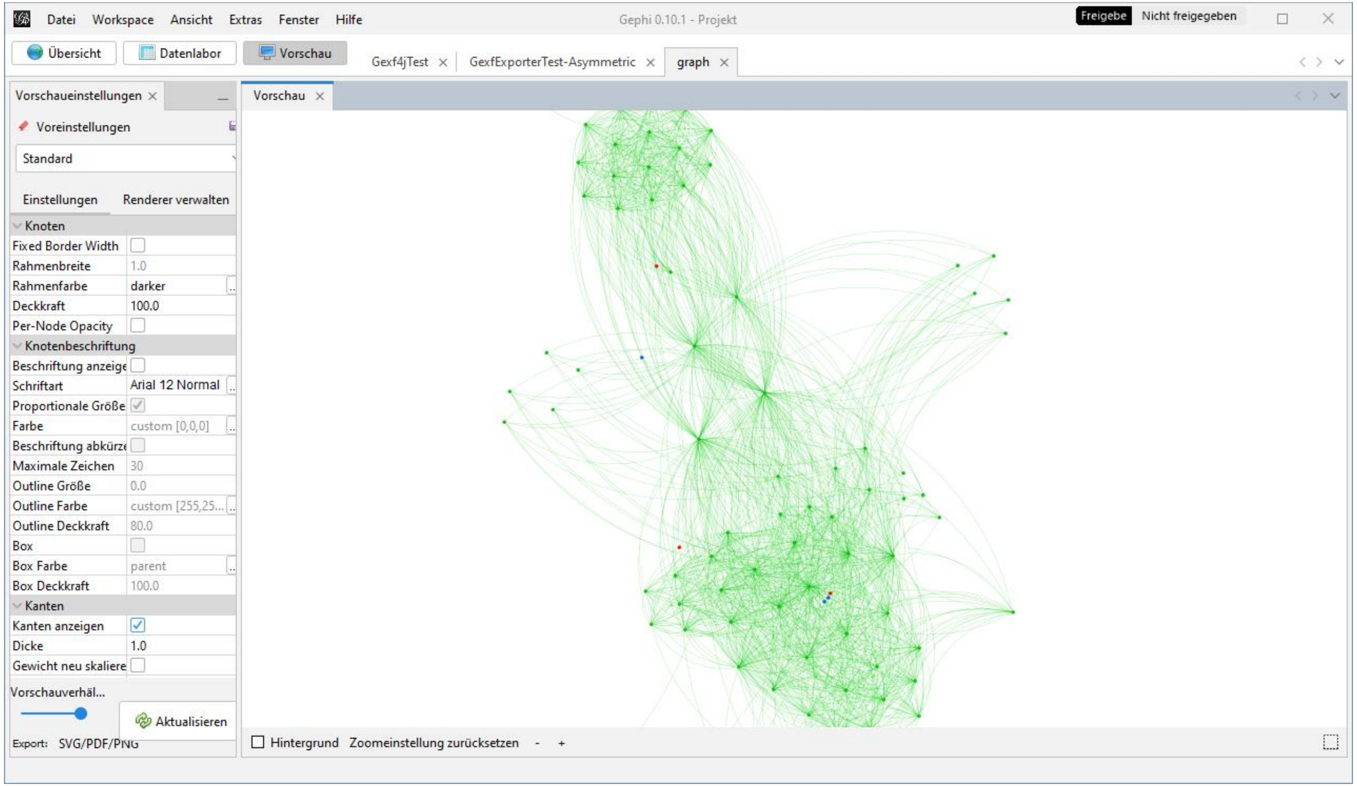
Demo Output Graph (1/3)



Demo Output Graph (2/3)

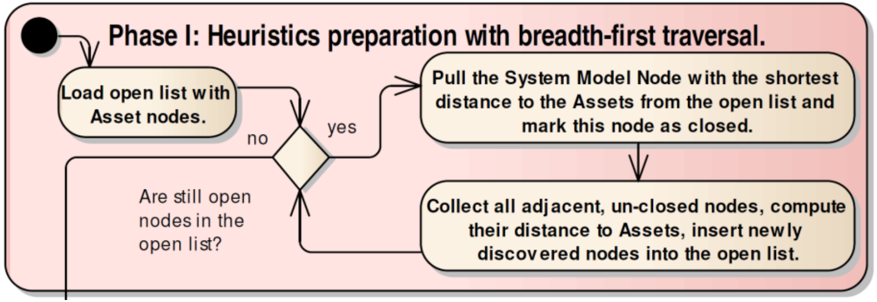


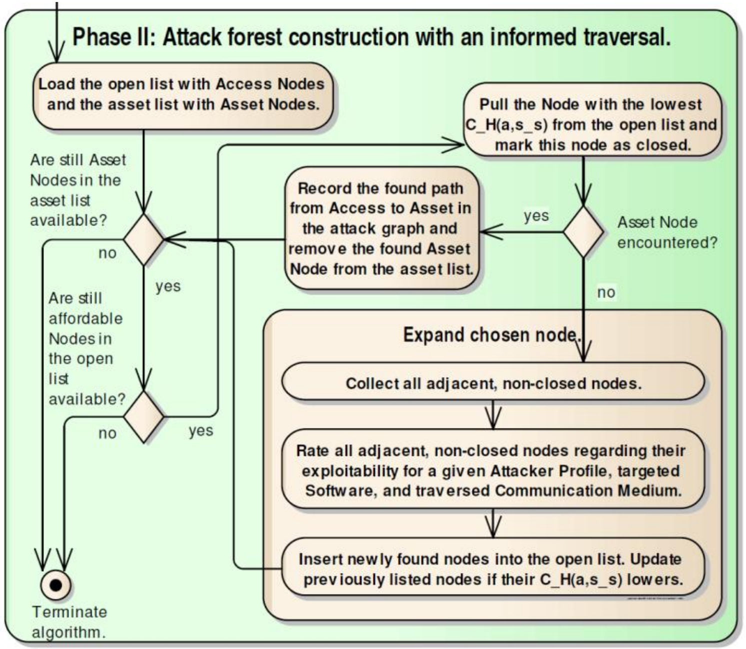
Demo Output Graph (3/3)



Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

C5: Design of the Single-Path Attack Graph Algorithm (1/2)





C5: Design of the Single-Path Attack Graph Algorithm (2/2)

- Sheyner (2004): **$O(c^n)$**:
  with NuSMV and Model Checking takes
  - 5 minutes for a network of 2 hosts and
  - 30 minutes for a network of 4 hosts.

- Ou et al. (2006): **$O(n^2)$**: with Prolog and Logic Programming

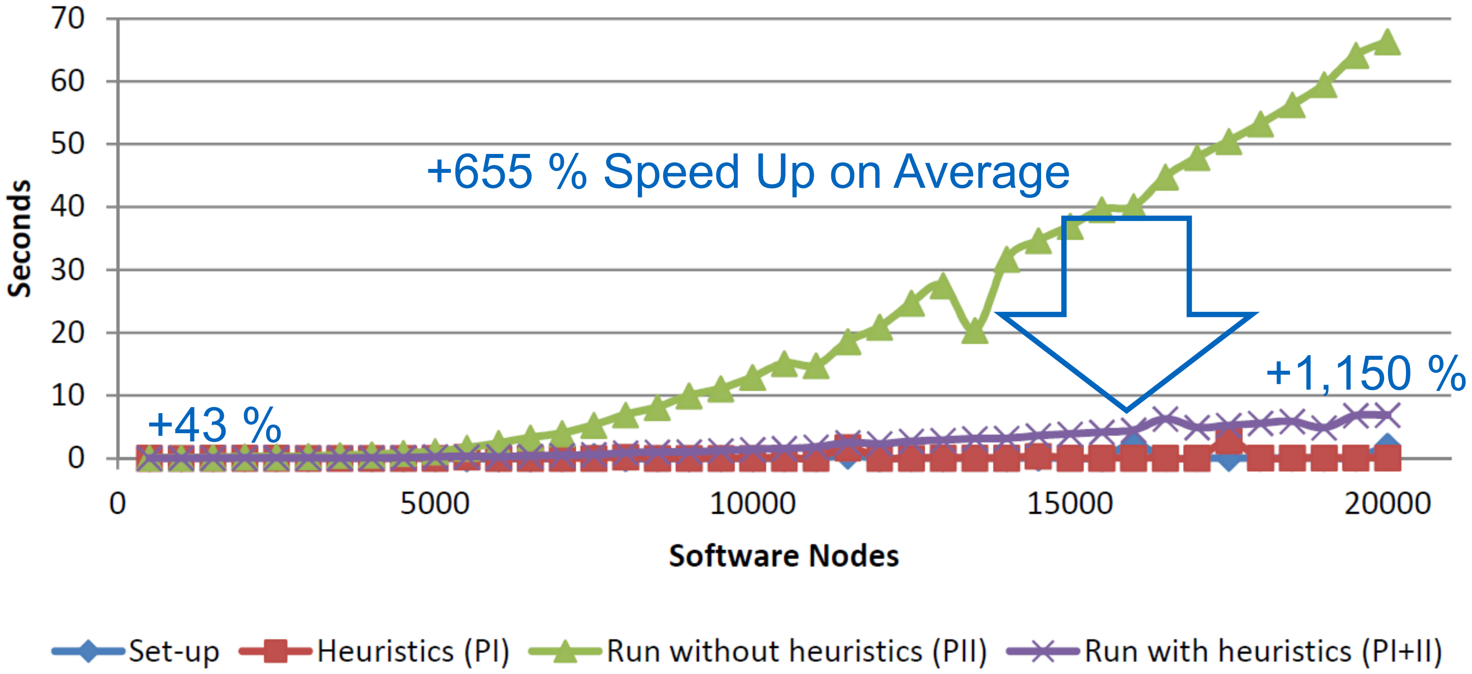
- Salfer et al. (2014): **O(n*log(n))** and **Ω(n+m)** with Java and Imperative Programming with n hosts and m exploits

```
/**
* Run the second phase of the system model crawl.
* This phase finds the shortest path and acts depth-first.
* The heuristic must be consistent, as nodes are expanded
* only once.
* Complexity: O(S*(log(S)+E).
*/
private void runPhase2Crawl() {
 clearLists(); // Complexity: O(1)
 loadAccessNodesIntoOpenList(); // Complexity O(1) as of
     assumption 5.
 loadOpenAttractors(); // Complexity O(1) as of assumption 5.
 while (openAttractors.size() > 0 && openList.size() > 0) {
     // Complexity: O(S) as a software node is closed each
     round.
  Crawlable c = openList.poll(); // Complexity: O(log(S)).
  c.close(); // Complexity: O(1).
  expand(c); // Complexity: O(log(S)+E) as of *
 }
 clearLists();  // Complexity: O(1)
}
```

… see paper at ISC 2014

Image Sources: Salfer

C6: Implem. and Eval. of the Single-Path Attack Graph Algor.



… see paper at ISC 2014

Image Sources: Salfer

3. What Other Attack Paths Exist and What is the Total Risk for an Asset?

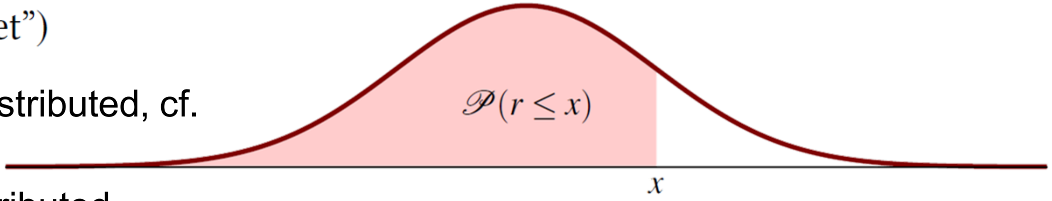
C7: Probabilistic Model
C8: Multi-Path Attack Graph Algorithm (P3Salfer)
C9: Bayes Network Unsuitability Finding
C10: Design and Implementation of an Alternative Algorithm with Bayesian Networks (P3Bayes)
C11: Implementation and Evaluation of the Multi-Path Attack Graph Algorithm (P3Salfer)

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

C7: Probabilistic Model for Overall Risk Computation (1/2)

Budget

$\mathcal{P}_B(a, p) = \Phi(\text{“cost}\leq\text{budget”})$



1. **Cost Value**: Approximated Gaussian distributed, cf. Central Limit Theorem.
2. **Budget Value**: Assumed Gaussian distributed

The accumulated probability $\mathscr{P}(r \leq x) = \Phi\left(\frac{x-\mu_r}{\sigma_r}\right)$

Budget Cost

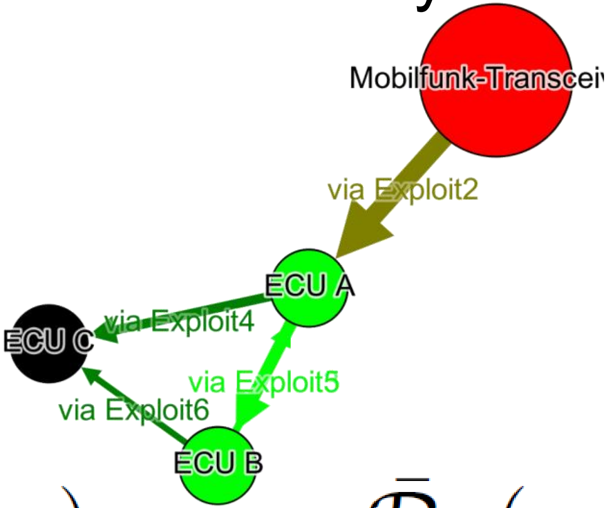
$$= \Phi\left(\frac{a_{b\mu} - C(a,p)_\mu}{\sqrt{a_{b\sigma}^2 + C(a,p)_\sigma^2}}\right)$$

Carl F. Gauß 1777-1855

Image Sources: Salfer, Public Domain

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

C7: Probabilistic Model for Overall Risk Computation (2/2)
Vuln. and Attackability



Vulnerability Probability

$$\mathcal{P}_V(p) := \prod_{i=1}^{n} \mathcal{P}_V(s_{si})$$

Attackability Probability

$$\mathcal{P}_A(p) = \mathcal{P}_V(p) * \mathcal{P}_B(p)$$

Risk

$$\mathcal{R}(a, s_a) := s_{av}\bar{\mathcal{P}}_A(a, s_a) = s_{av}\frac{\sum_{i=1}^{n} \mathcal{P}_A(a, p_1)}{n}$$

… see paper at ARES 2018

Image Sources: Salfer

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

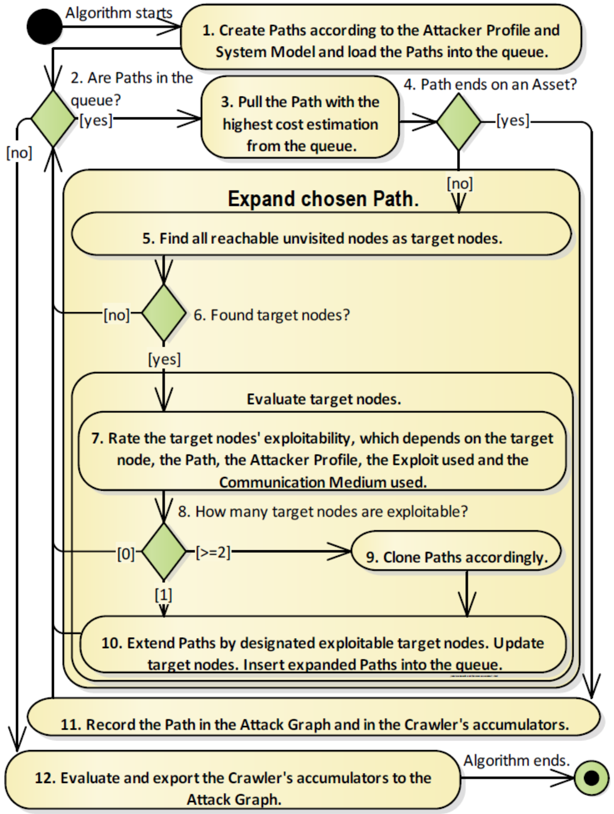
C8: Design of the Multi-Path Attack Graph Algorithm (P3Salfer)

Performance Considerations:

- Early Path Drops, still >95% coverage @ 2σ.
- Fast Gauß Computation Instead of Sampling
- “MapReduce-able”: > 94% computational time is independent.

Termination Guarantee

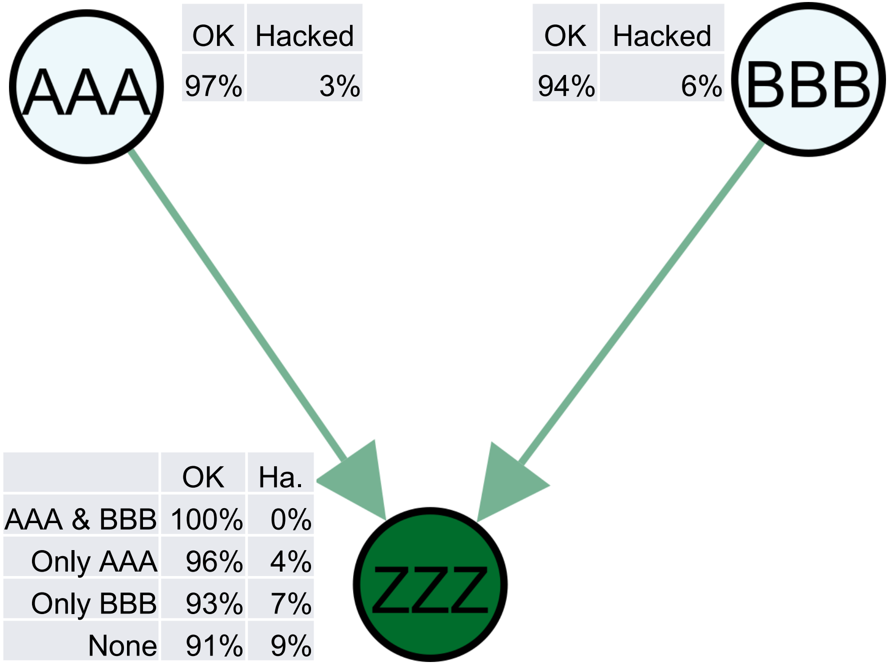
- Budget Overrun
- Probability Insignificance
- Reaching all Assets
- Expansion Exhaust



… see paper at ARES 2018

Image Sources: Salfer

C9: Bayes Network Unsuitability Finding



	OK	Hacked
AAA	97%	3%

	OK	Hacked
BBB	94%	6%

	OK	Ha.
AAA & BBB	100%	0%
Only AAA	96%	4%
Only BBB	93%	7%
None	91%	9%

Stochastic, graphical models

Thomas Bayes 1701-1761

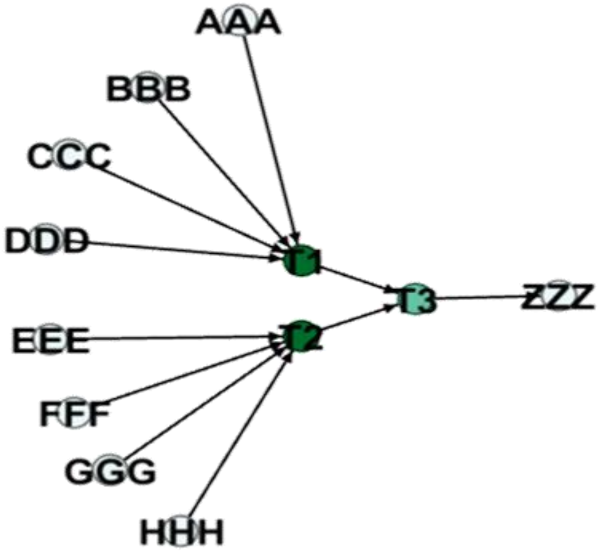
But:

1. **Distribution Table Explosion (or node growth)**, Space complexity: $2^{(n+4)}$B; n=30 inputs ➔ ~17 GB.
2. **Cycle Inability**
3. **Probabilities are static / history-agnostic**

… see paper at ARES 2018

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

C10: Design and Implem. of an Altern. Algorithm with Bayesian Networks (P3Bayes)



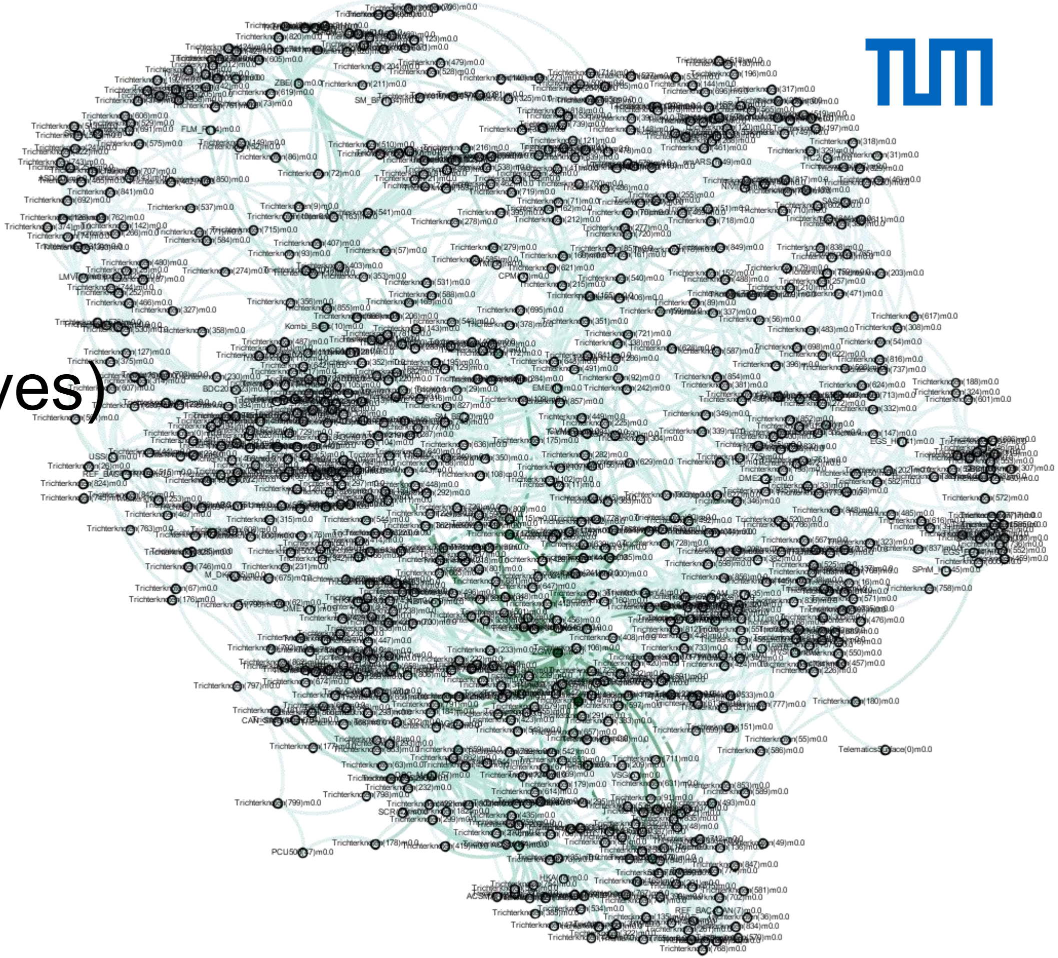
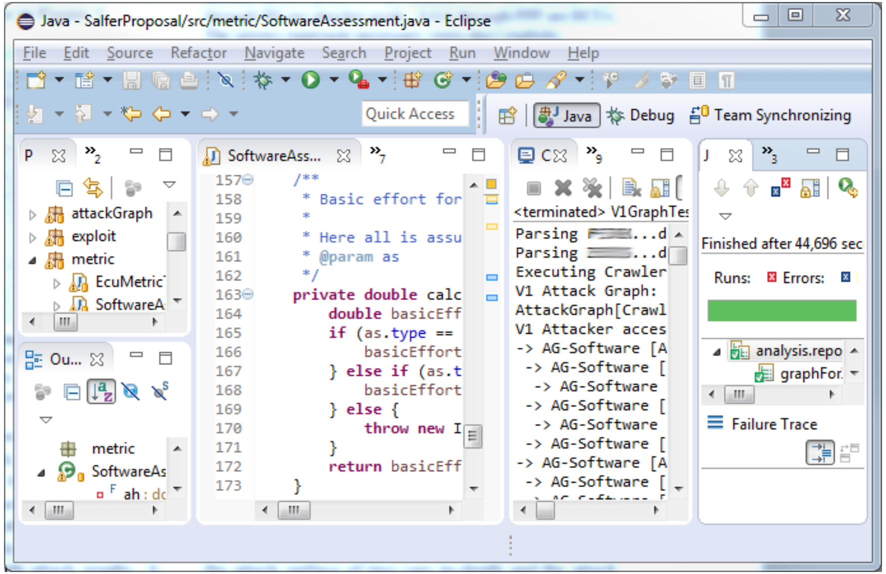


Image Sources: Salfer

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

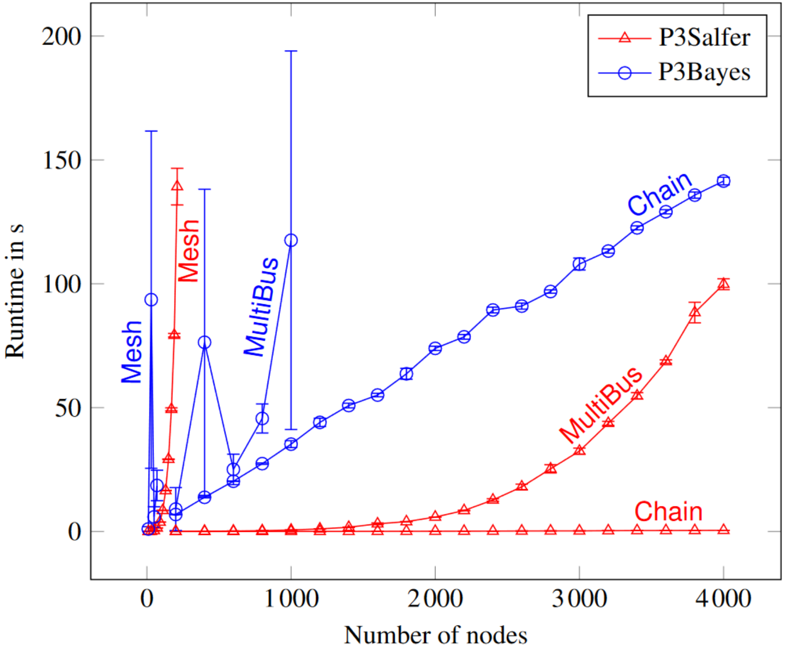
C11: Implementation and Evaluation of the Multi-Path Attack Graph Algorithm (P3Salfer): Feature Comparison



	P3Salfer	P3Bayes
Model	See above	Bayes Network
Inference	See above	Junction Tree
Technology	Standard JDK (Collections, JAXB)	Standard JDK, Unbbayes.jar
Cycles	OK	Not OK
Probabilities	Dynamic	Static
In Parallel	Single-Thread	Multi-Threaded

Image Sources: Salfer

C11: Benchmark Result: 200-5000x faster, 40-200x smaller



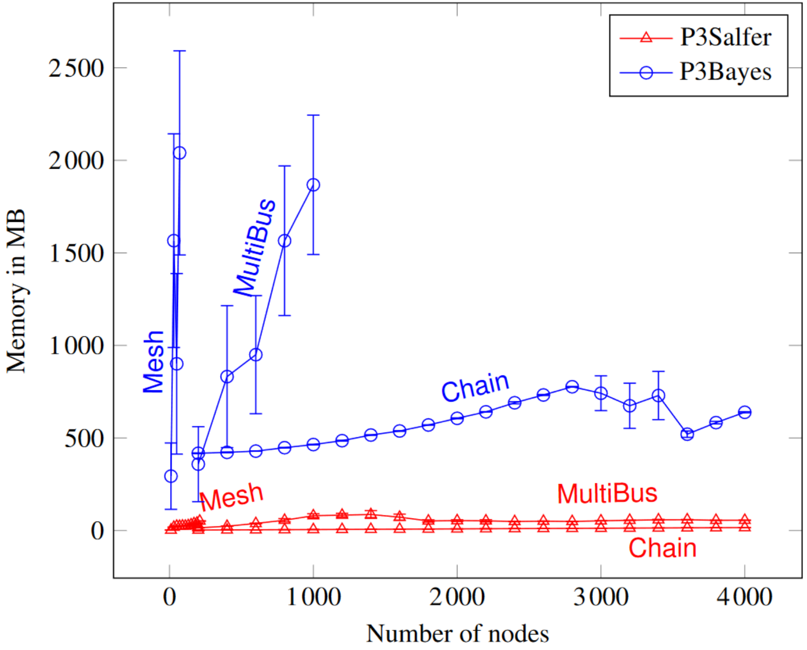


Image Sources: Salfer

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

C11: Benchmarking with Scalable Synthetic Models

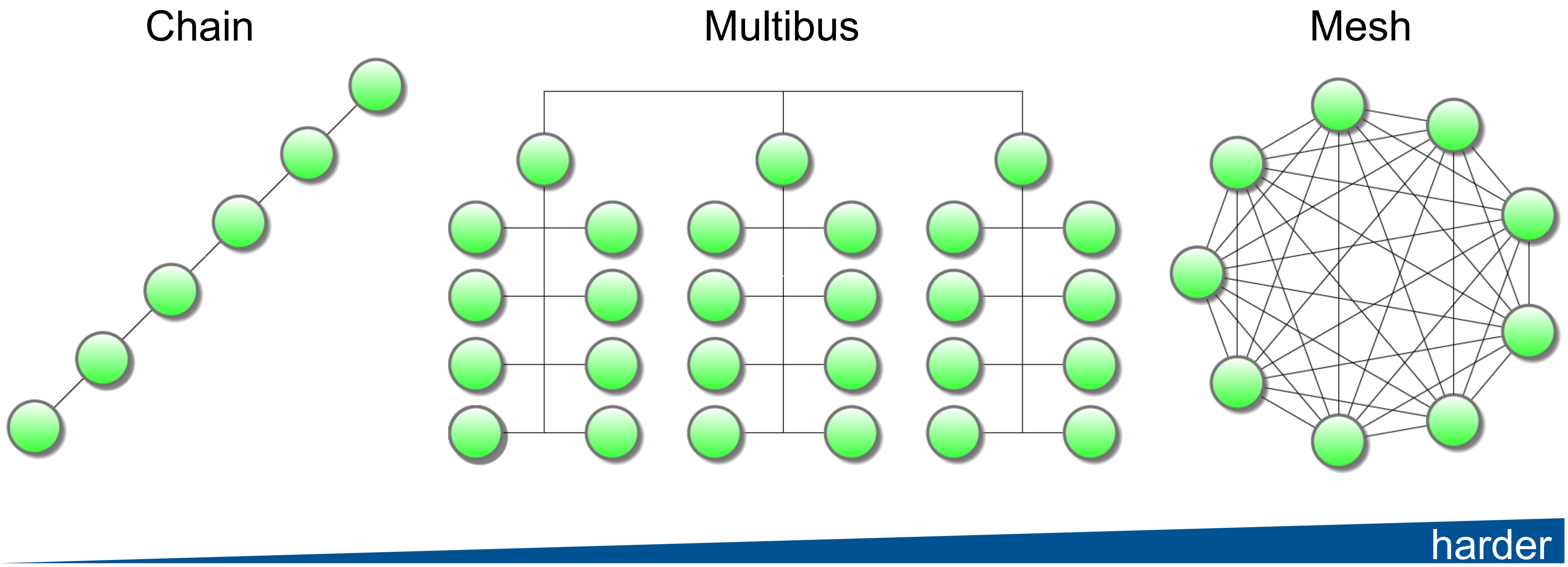


Image Sources: Salfer

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

C11: Application Test with Realistically Sized Graphs

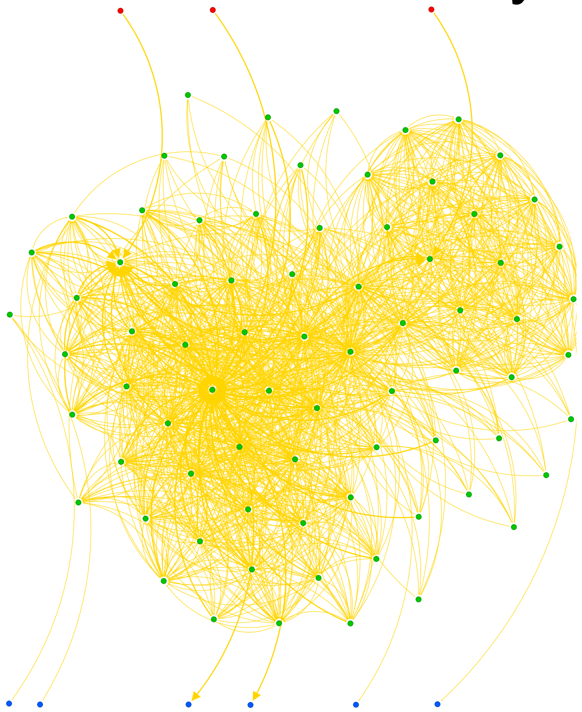


Image Sources: Salfer

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

Future Work

- Graphical user interface
- More input for higher assurance and higher accuracy
  - more development data
  - penetration test tools input for undocumented attack surfaces
- Networks beyond automotive
  - avionics/railway
  - operational technology
  - poorly segmented networks
- Maven packaging
- Documentation

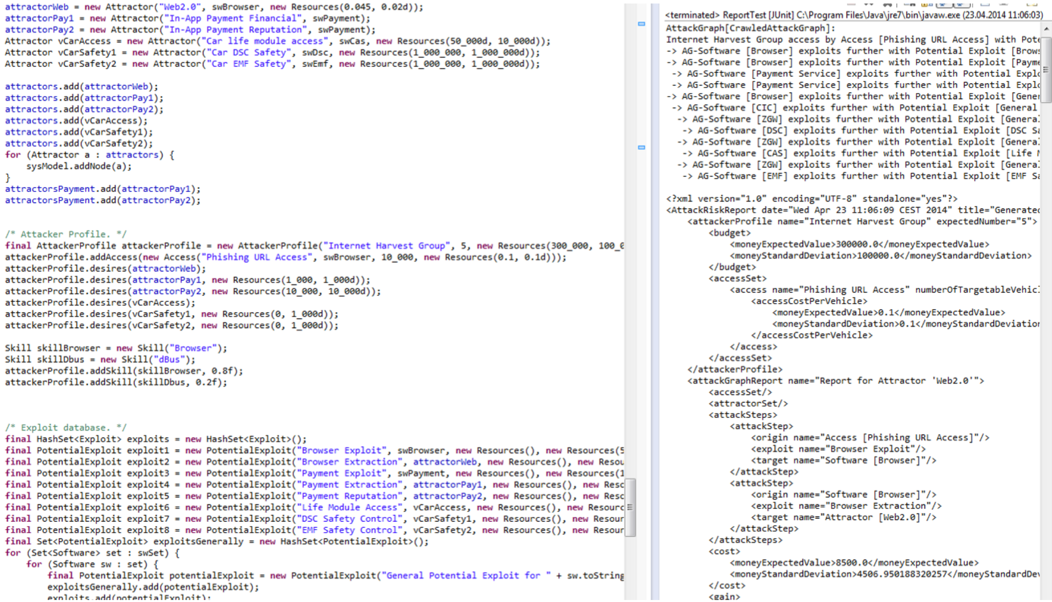


Image Sources: Salfer

Further Material Overview (1/6)

EU Patents

1. M. Salfer, **System and Method for Simulating and Foiling Attacks on a Vehicle On-Board Network**, EP3490223B1, 24.11.2017, https://patents.google.com/patent/EP3490223B1.
2. M. Salfer, Secure and User-Specific Data Use in Motor Vehicles, 15801365.6, EP3235212, 2015-11-18, https://patents.google.com/patent/EP3235212A1/en
3. M. Salfer, Methods and devices for transmitting and identifying radio identifiers, EP3766268, 2022-09-21, https://patents.google.com/patent/EP3766268A1

US-Patent 11,716,165: M. Salfer, Methods and Devices for the Concealment of Radio Identifiers and Transmitter Positions, application: 2019-04-18, patent grant: 2023-08-01, patent expiration: 2040-01-30.

China Patent 111788569: M. Salfer, Method and apparatus for hiding radio identifiers and transmitter locations,, application: 2019-04-18, patent grant: 2023-09-12, patent expiration: 2039-04-18.

Further Material Overview (2/6)

German Patent Filings

1. M. Salfer, Verfahren und Vorrichtungen zur Verschleierung von Funkkennungen und Senderpositionen, 102018206476.8, 26.04.2018,.
2. M. Salfer, Verfahren und Vorrichtungen zum Senden und Identifizieren von Funkkennungen, 102018203949.6, 15.03.2018,.
3. M. Salfer, **Verfahren zur Ermittlung eines Angriffswegs in einem Systemmodell und Computerlesbares Speichermedium**, 102014212419.0 , 27.06.2014
4. M. Salfer, D. Burgkhardt und S. Zimmermann, System und Verfahren für einen beschränkten Zugang zu einem Fahrzeug, 102014219502.0, 26.09.2014
5. M. Salfer, Sichere Datennutzung in Kraftfahrzeugen, 102014226219.4, 17.12.2014
6. M. Salfer, Pseudozufällige Funkkennungen für mobile Funkvorrichtungen, 102015204210.3, 10.03.2015
7. M. Salfer und Z. Ren, Notbelieferung eines Fahrzeugs mit Kraftstoff, 102014213023.9, 04.07.2014
8. M. Salfer, Beschichtung für ein Objekt sowie Fahrzeug umfassend eine Beschichtung., 102014208531.4, 07.05.2014
9. M. Salfer, C. Lottermann und P. Hoffmann, Beobachtung einer Umgebung eines Fahrzeugs, 102014206928.9, 10.04.2014

Further Material Overview (3/6)

Conference Papers

1. M. Salfer und C. Eckert, **"Attack Graph Automation for Assessing Security Risks of Automotive On-Board Networks"** (P3Salfer/P3Bayes), 13th International Conference on Availability, Reliability and Security (ARES 2018), Hamburg, Germany.
2. M. Salfer und C. Eckert, **"Attack Surface and Vulnerability Assessment of Automotive Electronic Control Units"** (Probability Calculations), 12th International Conference on Security and Cryptography (SECRYPT 2015), Colmar, France.
3. M. Salfer, H. Schweppe, und C. Eckert, **„Efficient Attack Forest Construction for Automotive On-board Networks“** (Model + PI/PII), Information Security – 17th Int. Conference (ISC 2014), Hong Kong.
4. N. Broy, S. Goebl, M. Hauder, T. Kothmayr, M. Kugler, F. Reinhart, M. Salfer, K. Schlieper, und E. André, „A cooperative in-car game for heterogeneous players“, in (AutomotiveUI 2011), Salzburg, Austria.
5. M. Salfer, S. Wohlgemuth, S. Schrittwieser, B. Bauer, und I. Echizen, „Data Provenance with Watermarks for Usage Control Monitors at Disaster Recovery“, in (IEEE iThings/CPSCom 2011), China.

Further Material Overview (4/6)

Journal Article

1. Hans-Ulrich Michel, Dirk Kaule, und Martin Salfer, „Virtualisierung: Vision einer intelligenten Vernetzung.“, Elektronik automotive, Nr. 04/2012, S. 28–32, Apr. 2012.

Poster

1. M. Salfer, "IT-Sicherheit im Auto - Graphen-basierte Angriffssicherheitsevaluation von automobilen Bordnetzen.", Poster + Proceedings, BMW ProMotion Dialogtag 2014
2. M. Salfer, "Sicherheitsarchitektur - Quantitative Bewertung von Sicherheitsarchitekturen virtualisierter Mehrkern-Steuergeräte.", Poster + Proceedings, BMW ProMotion Dialogtag 2013
3. M. Salfer, "E/E-Sicherheitsarchitektur - IT-Sicherheit virtualisierter Mehrkern-Systeme im Fahrzeug.", Poster + Proceedings, BMW ProMotion Dialogtag 2012

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

Further Material Overview (5/6)

The software for the contributions

- C4 “Implementation and Evaluation of the Models and the Attack Surface Exploitability Quantification”,
- C6 “Implementation and Evaluation of the Single-Path Attack Graph Algorithm”,
- C10 “Design and Implementation of an Alternative Algorithm with Bayesian Networks (P3Bayes)”, and
- C11 “Implementation and Evaluation of the Multi-Path Attack Graph Algorithm (P3Salfer)”

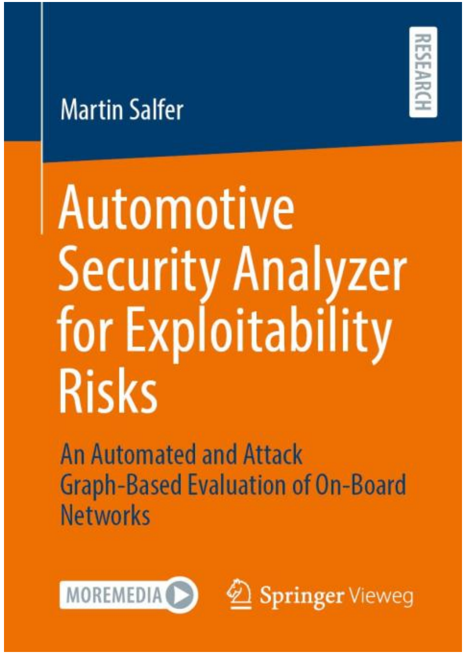
Is published (with the main algorithms in `/src/analysis/Crawler.java`) as

“Automotive Security Analyzer for Exploitability Risks” (AutoSAlfER) on
https://github.com/MarSalfer/AutoSAlfER/
Head start with libraries in https://syncandshare.lrz.de/dl/fiCZTBTseBwuqoJiwqDUvD/externalLib.zip

Chair of IT Security
TUM School of Computation, Information and Technology
Technical University of Munich

Further Material Overview (6/6)

M. Salfer, **Automotive Security Analyzer for Exploitability Risks**: An Automated and Attack Graph-Based Evaluation of On-Board Networks, Springer Vieweg, 2024-03-15, ISBN 978-3-658-43505-9, https://link.springer.com/book/9783658435059



"Smart" features are "not so smart" if these introduce further attack vulnerabilities.

Someone can

- **pay now by investing in proper security** or
- **pay later** by losing lives, assets, or revenue.