



**BULGARIAN ACADEMY OF SCIENCES**  
**INSTITUTE OF INFORMATION AND COMMUNICATION**  
**TECHNOLOGIES**



# **Cyber Threat Modeling** **(existing systems)**

**Assist. Prof. Elena Paunova & Peter Stoyanov**  
**IICT – BAS**

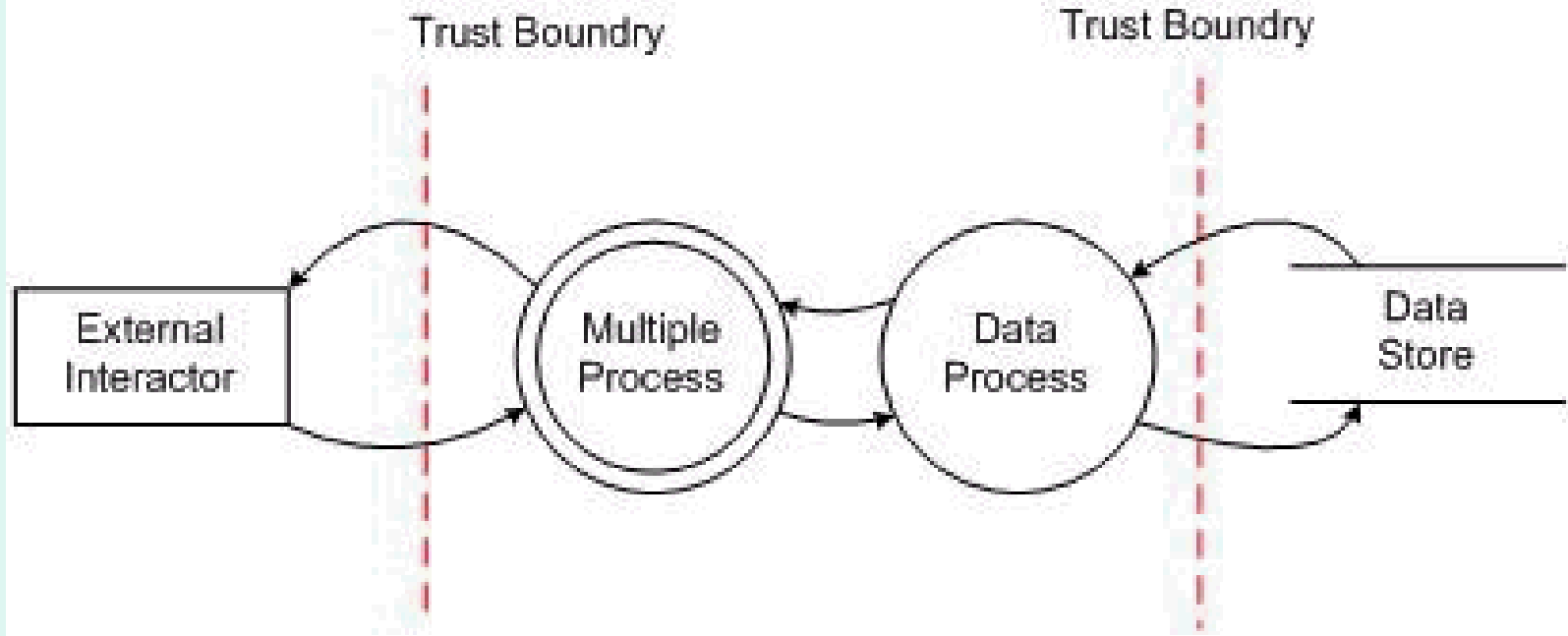


**A Feasibility Study on Cyber Threats Identification and their Relationship with Users' Behavioural Dynamics in Future Smart Homes, Research Grant 'Funding of Fundamental & Applied Scientific Research in Priority Fields', Bulgarian Science Fund, Ministry of Education Youth and Science, 2012-2014, DFNI-T01/4**

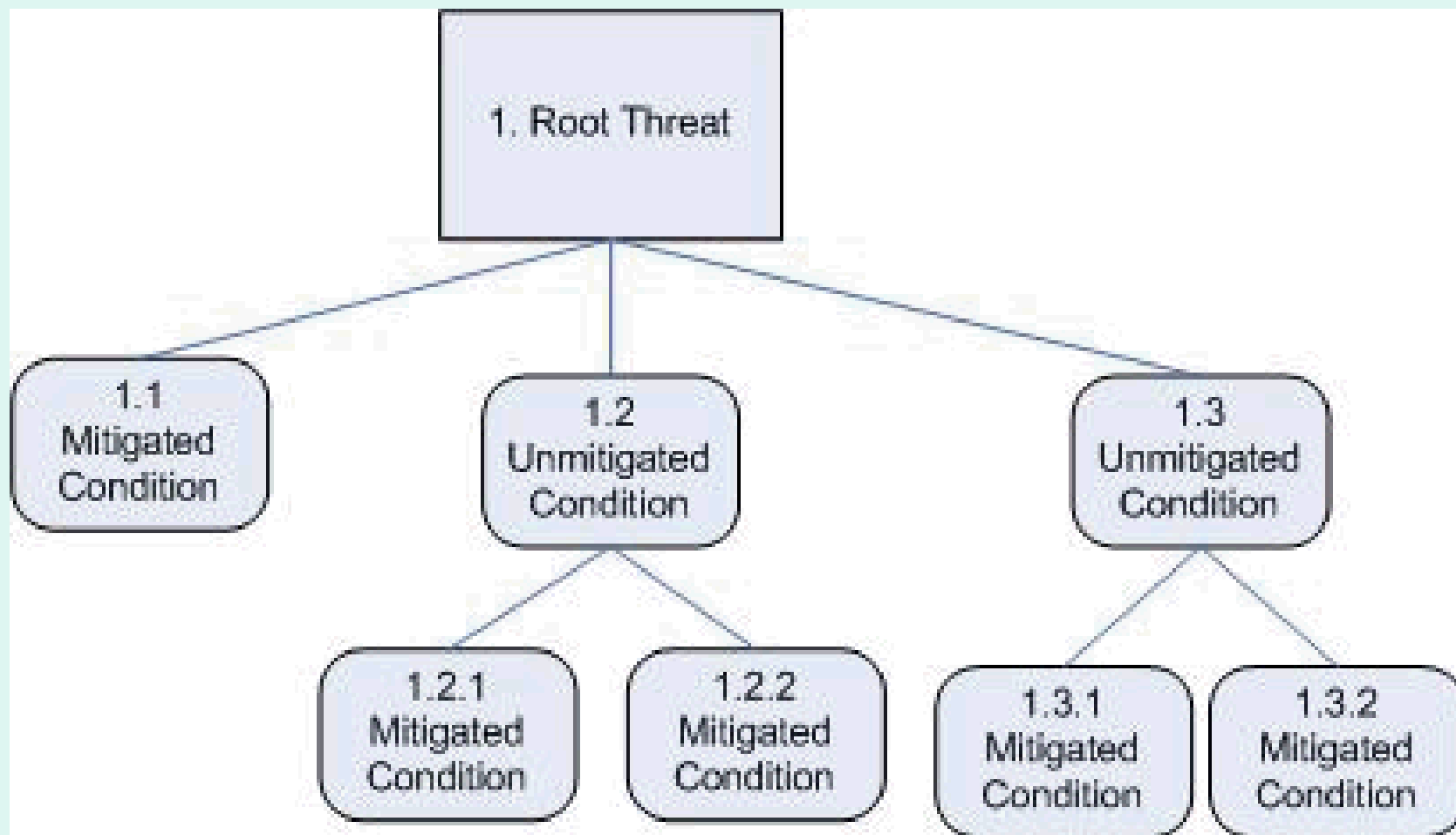
# Threat Modeling

- Threat modeling is a systematic way to find design-level security and privacy weaknesses in a system. It also helps guide a designer or architect to determine the correct mitigation(s) to use to reduce the overall risk to a system and the data. [8]
- STRIDE (**S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**levation of Privilege)

# SANS Institute [6]



# SANS Institute [6]

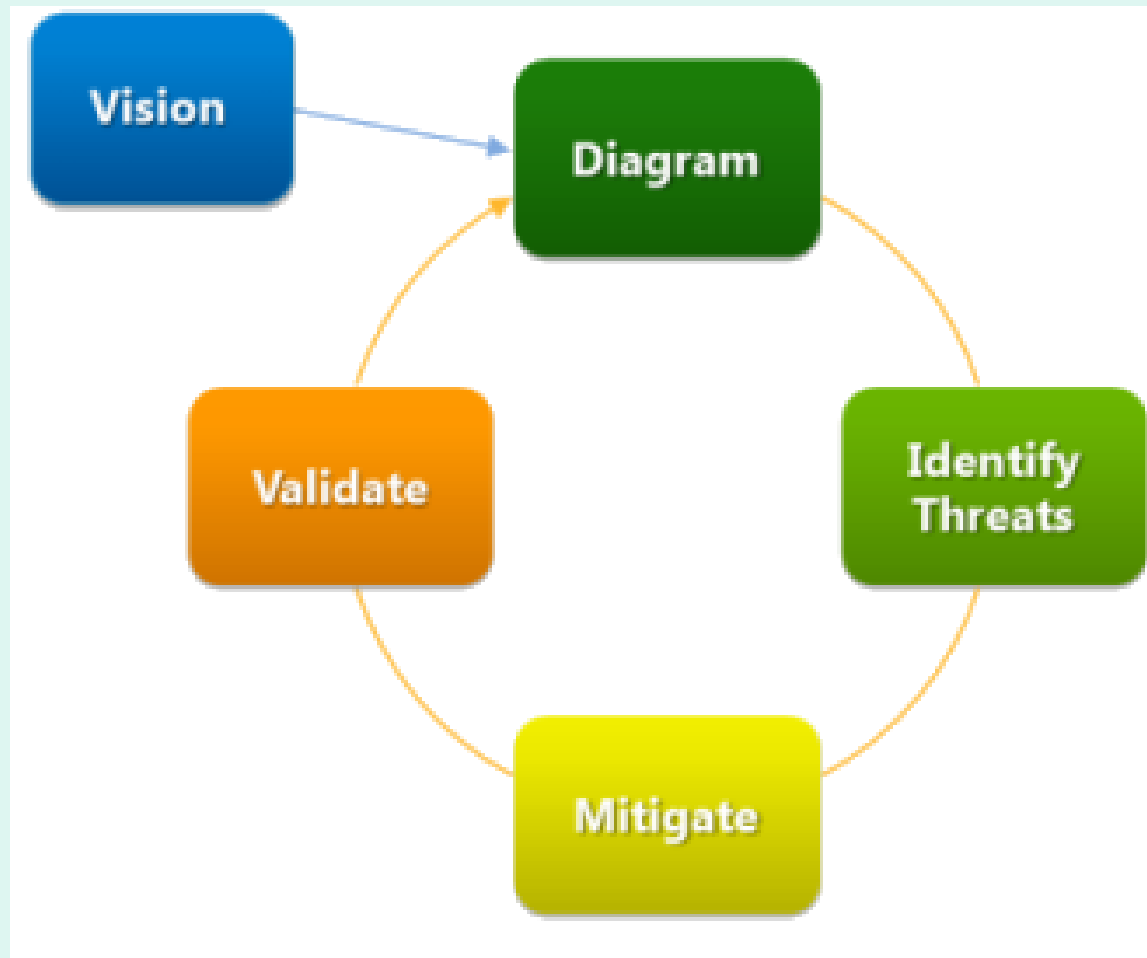


# Trike [3] [4] [5]

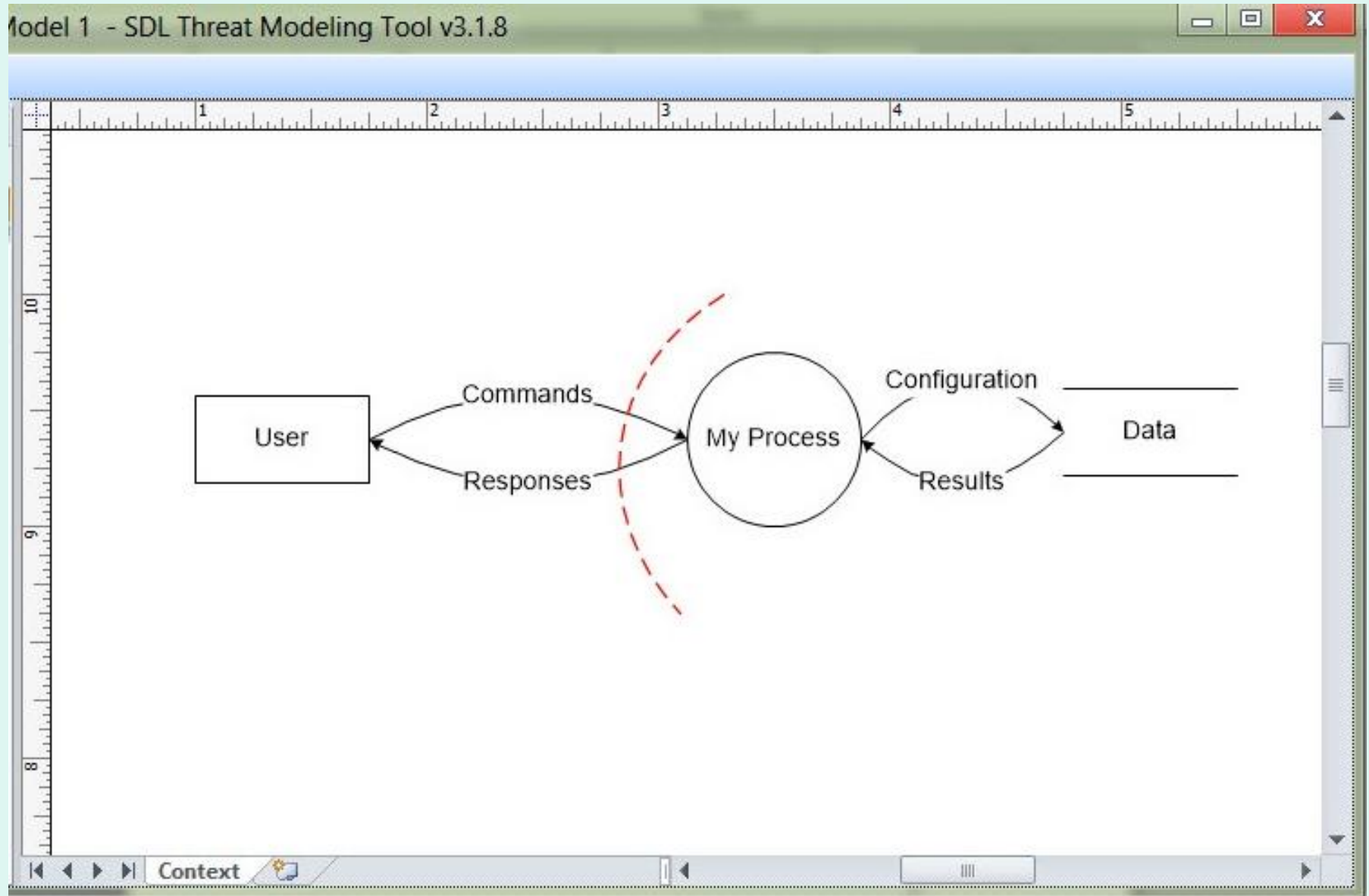
## Threat Model

- Threat Generation
- Attacks, Attack Trees, and the Attack Graph
- Weaknesses
- Vulnerabilities
- Mitigations
- Attack Libraries

# MicroSoft – SDL [1][2]



# MicroSoft – SDL



# MicroSoft – SDL

| New Model 1 - SDL Threat Modeling Tool v3.1.8 |    |                              |              |                            |                       |        |            |
|-----------------------------------------------|----|------------------------------|--------------|----------------------------|-----------------------|--------|------------|
|                                               | ID | Element Name                 | Element Type | Element Diagram References | Threat Type           | Bug ID | Completion |
| ▶                                             | 3  | Commands (User to My P...    | DataFlow     | Context                    | Tampering             |        |            |
|                                               | 4  | Commands (User to My P...    | DataFlow     | Context                    | InformationDisclosure |        |            |
|                                               | 5  | Commands (User to My P...    | DataFlow     | Context                    | DenialOfService       |        |            |
|                                               | 9  | Configuration (My Proces...  | DataFlow     | Context                    | Tampering             |        |            |
|                                               | 10 | Configuration (My Proces...  | DataFlow     | Context                    | InformationDisclosure |        |            |
|                                               | 11 | Configuration (My Proces...  | DataFlow     | Context                    | DenialOfService       |        |            |
|                                               | 6  | Responses (My Process to ... | DataFlow     | Context                    | Tampering             |        |            |
|                                               | 7  | Responses (My Process to ... | DataFlow     | Context                    | InformationDisclosure |        |            |
|                                               | 8  | Responses (My Process to ... | DataFlow     | Context                    | DenialOfService       |        |            |
|                                               | 12 | Results (Data to My Proce... | DataFlow     | Context                    | Tampering             |        |            |
|                                               | 13 | Results (Data to My Proce... | DataFlow     | Context                    | InformationDisclosure |        |            |
|                                               | 14 | Results (Data to My Proce... | DataFlow     | Context                    | DenialOfService       |        |            |
|                                               | 21 | Data                         | DataStore    | Context                    | Tampering             |        |            |
|                                               | 22 | Data                         | DataStore    | Context                    | Repudiation           |        |            |
|                                               | 23 | Data                         | DataStore    | Context                    | InformationDisclosure |        |            |
|                                               | 24 | Data                         | DataStore    | Context                    | DenialOfService       |        |            |
|                                               | 1  | User                         | Interactor   | Context                    | Spoofing              |        |            |
|                                               | 2  | User                         | Interactor   | Context                    | Repudiation           |        |            |
|                                               | 15 | My Process                   | Process      | Context                    | Spoofing              |        |            |
|                                               | 16 | My Process                   | Process      | Context                    | Tampering             |        |            |
|                                               | 17 | My Process                   | Process      | Context                    | Repudiation           |        |            |
|                                               | 18 | My Process                   | Process      | Context                    | InformationDisclosure |        |            |
|                                               | 19 | My Process                   | Process      | Context                    | DenialOfService       |        |            |
|                                               | 20 | My Process                   | Process      | Context                    | ElevationOfPrivilege  |        |            |

# References

- [1] <http://blogs.technet.com/b/security/archive/2012/08/23/microsoft-s-free-security-tools-threat-modeling.aspx>
- [2] <http://www.microsoft.com/security/sdl/adopt/threatmodeling.aspx>
- [3] <http://octotrike.org/home.shtml>
- [4] [http://octotrike.org/papers/Trike\\_v1\\_Methodology\\_Document-draft.pdf](http://octotrike.org/papers/Trike_v1_Methodology_Document-draft.pdf)
- [5] <http://octotrike.org/tools.shtml>
- [6] [http://www.sans.org/reading\\_room/whitepapers/securecode/threat-modeling-process-ensure-application-security\\_1646](http://www.sans.org/reading_room/whitepapers/securecode/threat-modeling-process-ensure-application-security_1646)
- [7] [https://www.owasp.org/index.php/OWASP\\_Threat\\_Modelling\\_Project](https://www.owasp.org/index.php/OWASP_Threat_Modelling_Project)
- [8] <http://blogs.technet.com/b/security/archive/2012/08/16/threat-modeling-from-the-front-lines.aspx>

Thank you for the attention!

Questions?