HOST IDENTITY PROTOCOL RISK ANALYSIS

WITH VALUE CHAIN DYNAMICS TOOLKIT-BASED RISK IDENTIFICATION METHOD

AGENDA

- › Risk Analysis (RA) Methods
- › Value Chain Dynamics Toolkit (VCDT)
- › VCDT – adaptation for RA
- › HIP RA
- › Conclusion

TERMS:

RA = Risk Analysis

VCDT = Value Chain Dynamics Toolkit

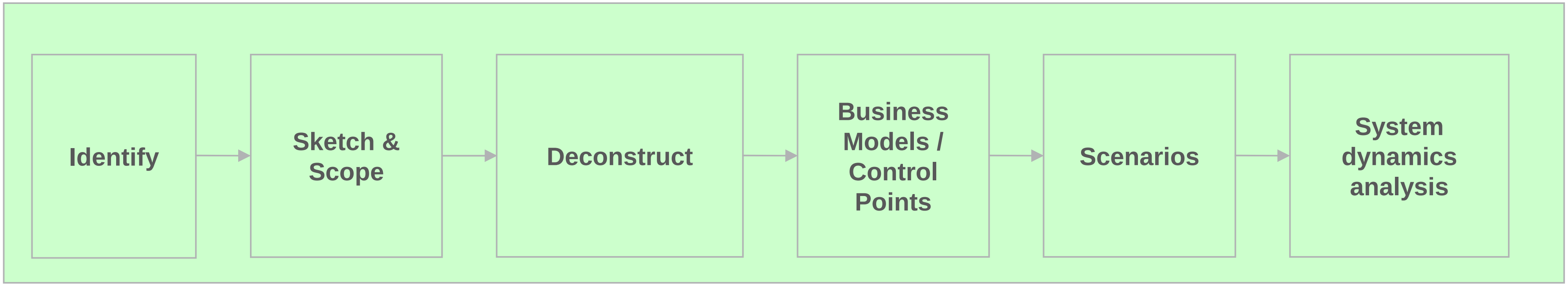
ABOUT RISK ANALYSIS METHODS

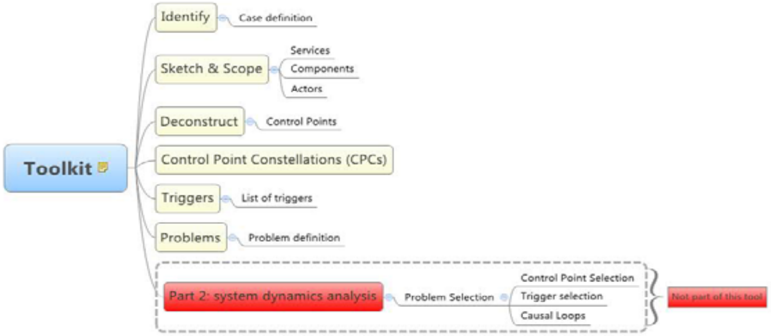
- Vast number of different methods
  - Insurance industry
  - Corporate risks
  - IT risks …
- Often detailed on how to *manage* risks
- Often weak or thin on how to *identify* risks

- Need for:
  - Risk identification methodology for *solution* security evaluation
    - taking systematically into account
      - system-
      - environmental-
      - socio-economical aspects

VALUE CHAIN DYNAMICS TOOLKIT (VCDT)

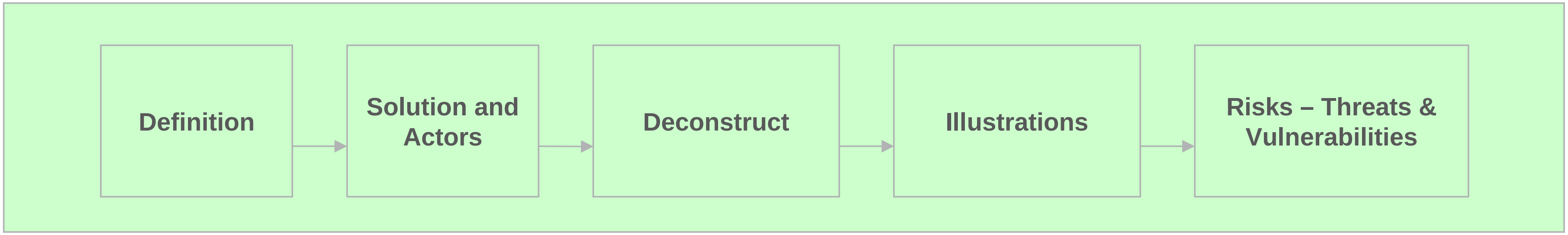
- Developed at the Massachusetts Institute of Technology (MIT) for analyzing value chains and market dynamics of new technologies
  - Mind map templates, recommendations for certain tools and a number of ways applying the process





VCDT ADAPTATION - RISK ANALYSIS (RA)

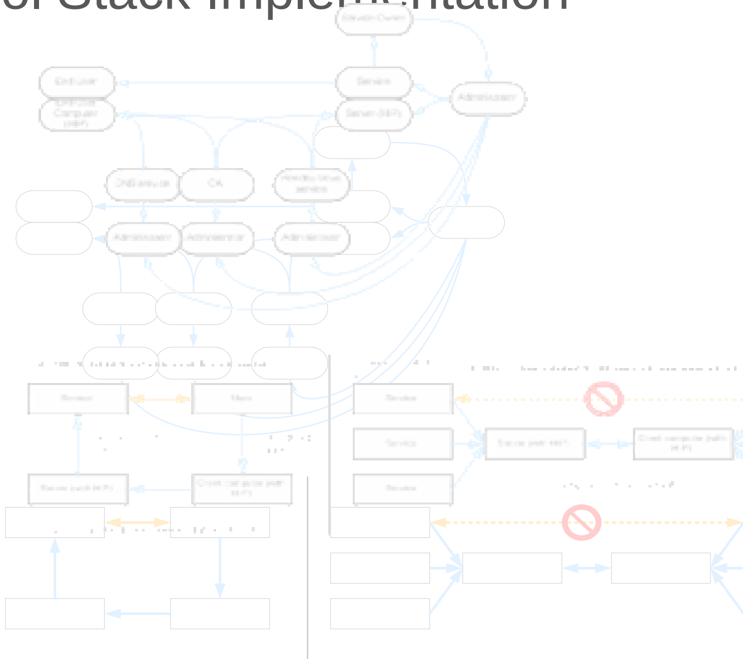
- Steps adapted, templates created/modified, focusing on
  - Value Chain Aspects (socio-economical)
  - System Aspects (environmental factors)

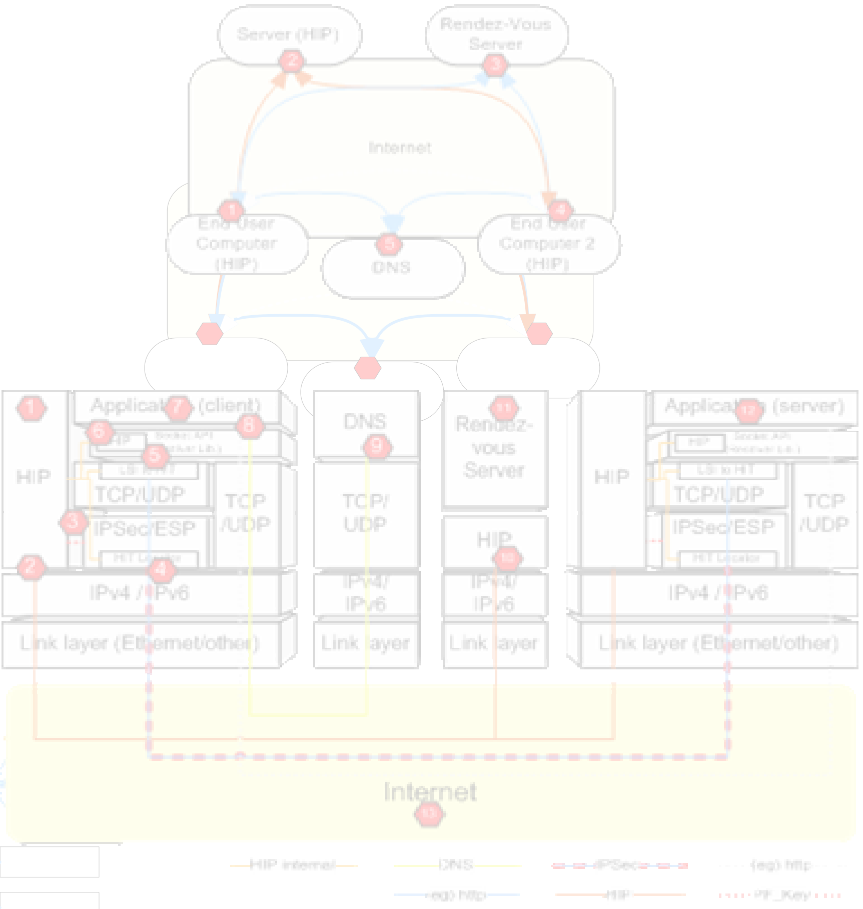


Definition → Solution and Actors → Deconstruct → Illustrations → Risks – Threats & Vulnerabilities

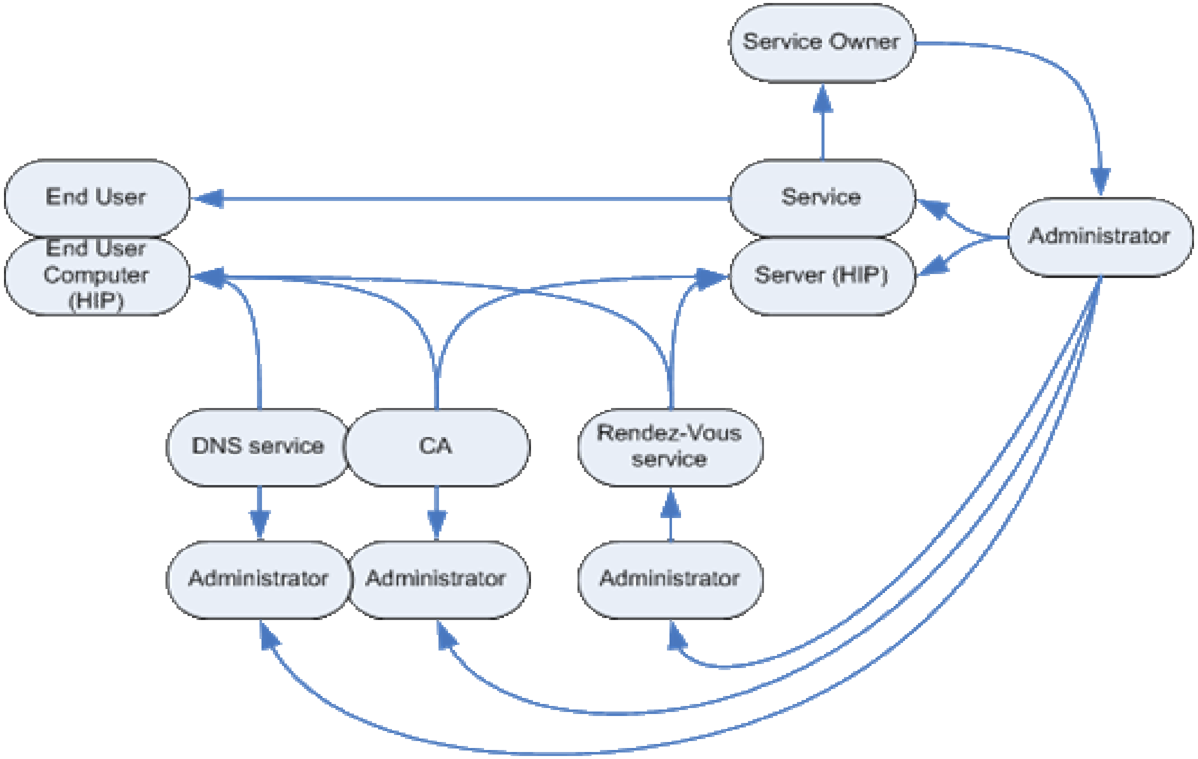
HIP RISK ANALYSIS

- Aspects
  - Communicating Entities
  - Value Chain
  - Trust Aspects
  - Protocol Stack Implementation





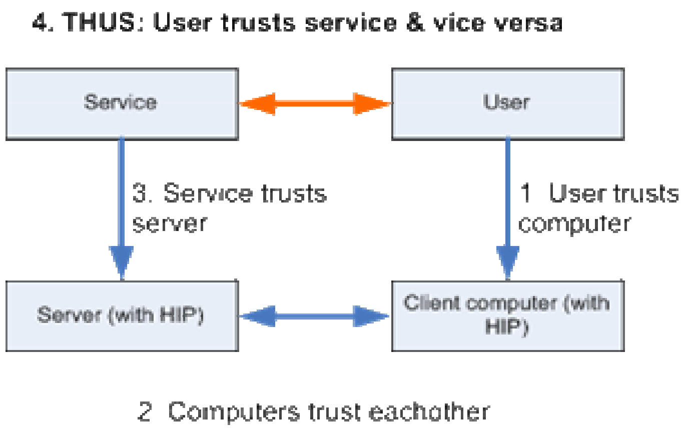
HIP RA – VALUE CHAIN ASPECTS

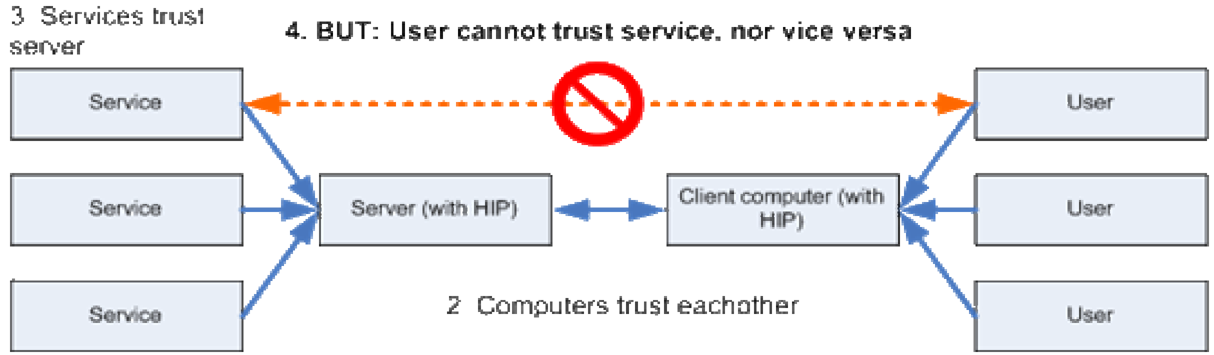


- Social attacks towards HIP system -serious threat
  - HIP administrator has the 'biggest power'
  - Also service owner, end user & administrators can be compromised

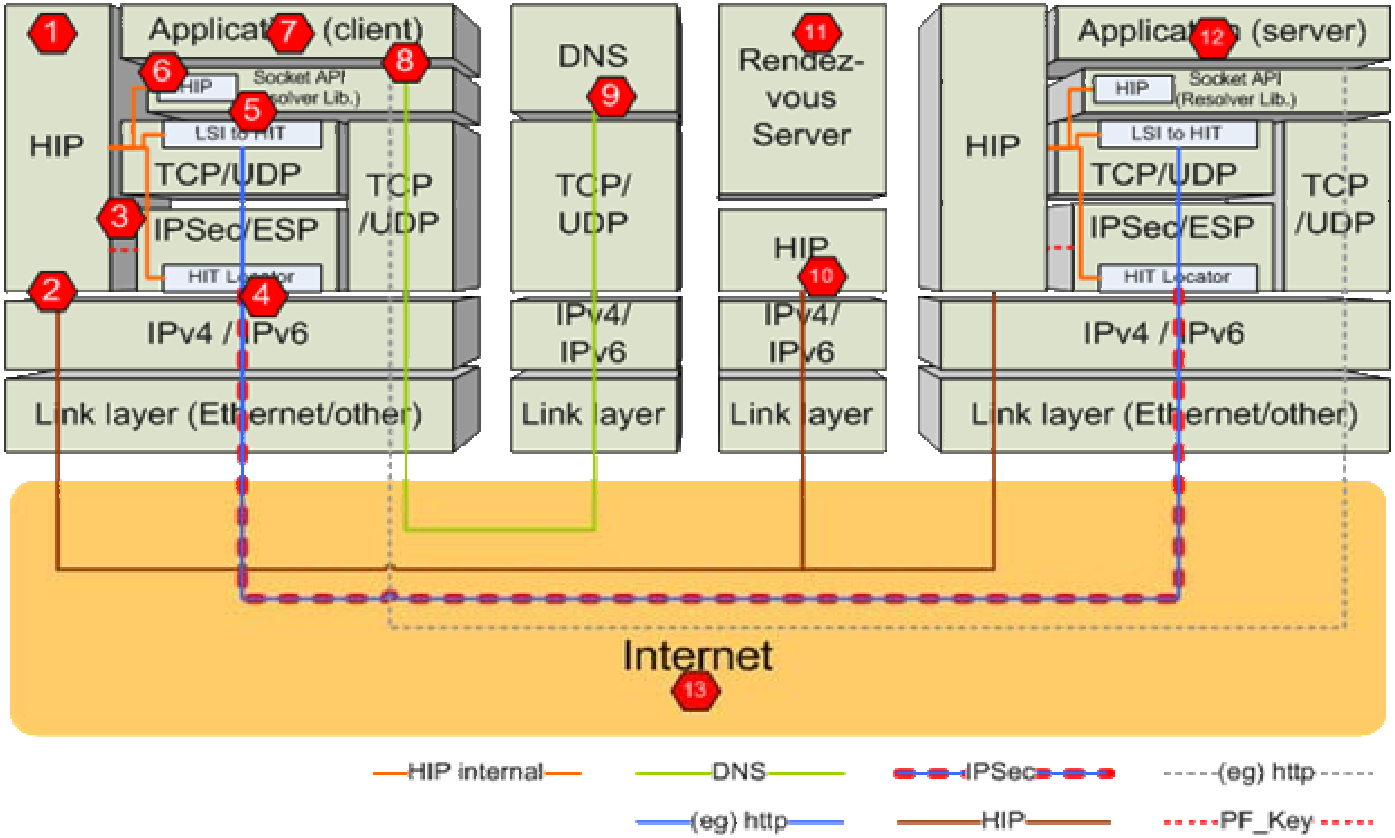
HIP RA – TRUST ASPECTS

› Single User Computer vs. Multi User Computer


4. THUS: User trusts service & vice versa
Service
User
3. Service trusts server
1 User trusts computer
Server (with HIP)
Client computer (with HIP)
2 Computers trust eachother


3 Services trust server
4. BUT: User cannot trust service, nor vice versa
Service
Service
Service
Server (with HIP)
Client computer (with HIP)
User
User
User
2 Computers trust eachother

HIP RA – PROTOCOL STACK ASPECTS



- Risk areas:
  - Administration
  - Internal interfaces
  - Implementation flaws
  - HIP / non-HIP traffic in same node

HIP RA – SUMMARY

- HIP inherent risks – low
  - No new flaws found in protocol design (not in the focus of the study)

⇒ **Good protocol**

- Social attack risks – high
  - A number of parties, which can be compromised
  - Trust chain must be thoroughly understood
  - A VCDT –based risk analysis recommended of planned use scenario
- HIP implementation –related risks – high
  - Implementation flaws; many interfaces, many components, third party components
  - User interface
  - Encryption visibility
  - Recommend thorough analysis & testing in production implementations
- HIP system risks – medium
  - Many possible targets for a number of attacks
  - Protocol design mitigates part, but it is recommended to make a risk analysis of the planned use scenario
- HIP and non-HIP traffic in same system – risk high

⇒ **But requires careful implementation and use scenario understanding and planning**

CONCLUSIONS

- VCDT –based Risk Identification method is promising
  - Understanding system level Risk Picture
  - Discovering ‘out-of-box’ Risks (vulnerabilities)
  - Visualizations
  - Documentation is still challenging
- For Further Study (VCDT –based RA method):
  - Use cases
  - Simulations
  - Trust aspects
  - Privacy aspects
  - Automated documenting
  - From risks to testing

ERICSSON