Lehrstuhl Netzarchitekturen und Netzdienste
Institut für Informatik
Technische Universität München

Attack Taxonomies and Ontologies

Seminar Future Internet
Supervisor: Nadine Herold
Natascha Abrek
02.10.2014

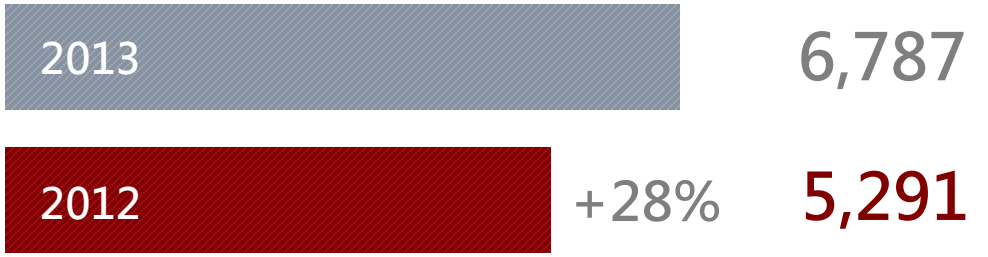
2013 in Numbers

552 MILLION
IDENTITIES EXPOSED

78 PERCENT
OF WEBSITES WITH VULNERABILITIES

62 PERCENT
GROWTH OF DATA BREACHES FROM 2012

New Vulnerabilities



6,787

5,291

SSL and **TLS** protocol renogotiation vulnerabilities were most commonly exploited.

Symantec Security Threat Report 2014

Status, Trends and Challenges Affecting Security

Increased…

- sophistication of attacks
- number of security vulnerabilities
- number of network and computer attacks

> *"Traditional security is not enough to defend against the latest generation of malware[1]."*

To protect against attacks we need

- comprehensive knowledge and understanding of attacks
- a distinctive and clear classification of attacks

[1]Gavin Reid, director of threat intelligence for Cisco

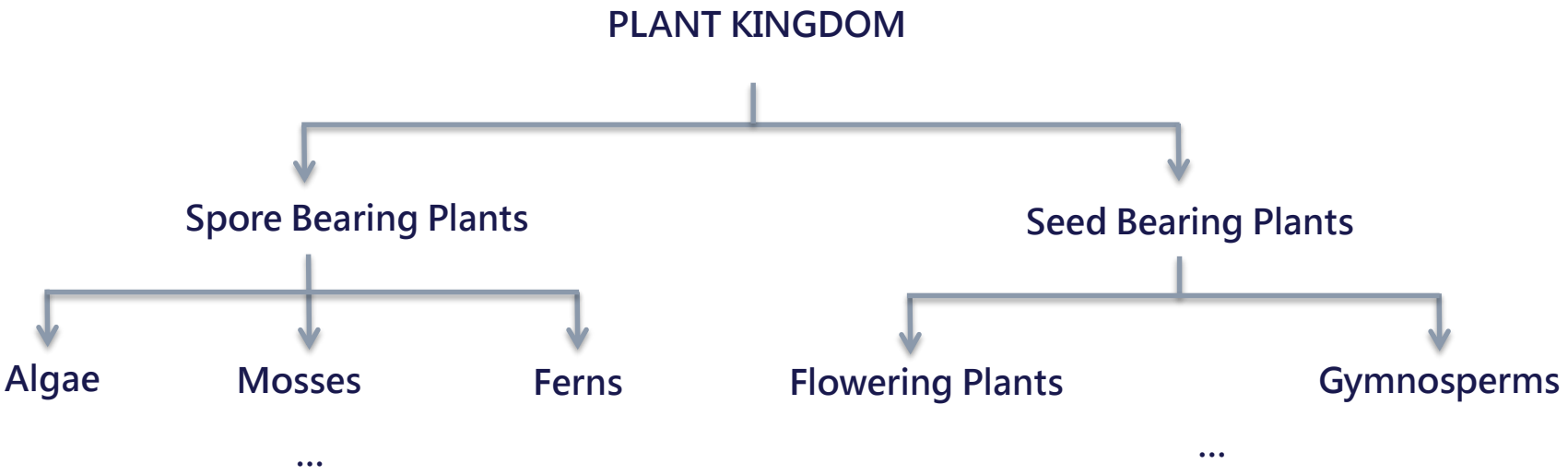
Taxonomies

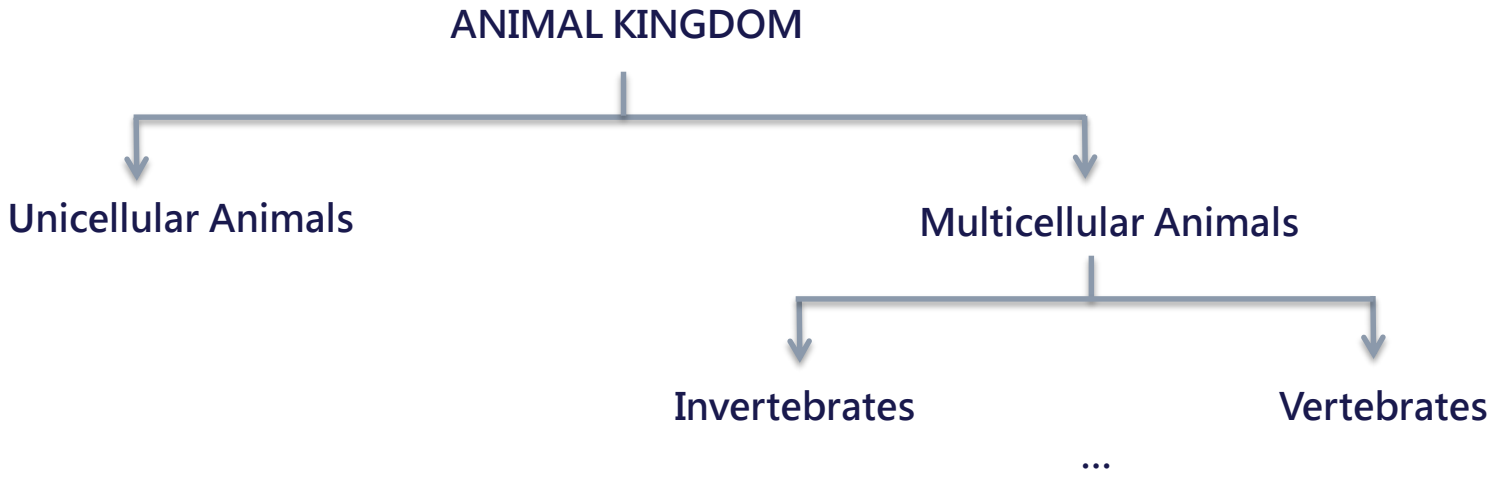
> A taxonomy is a system of classification which allows the unique identification of object
>
> *Bishop, M., Bailey, D.;1996*

A taxonomy…

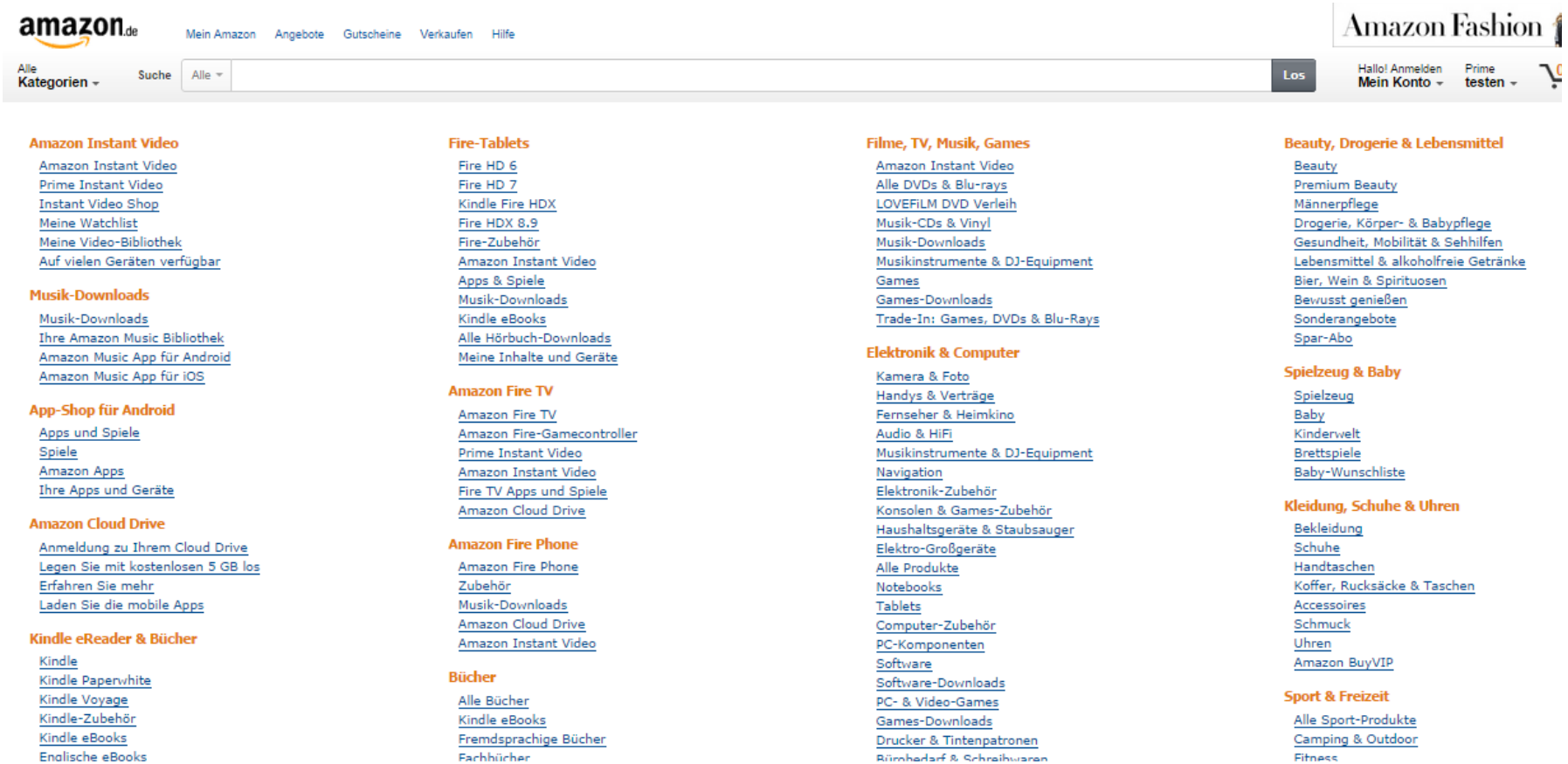
- organizes **domain specific** information
- in a **hierarchically** structure
- over **relationships**.

Well-known Taxonomies

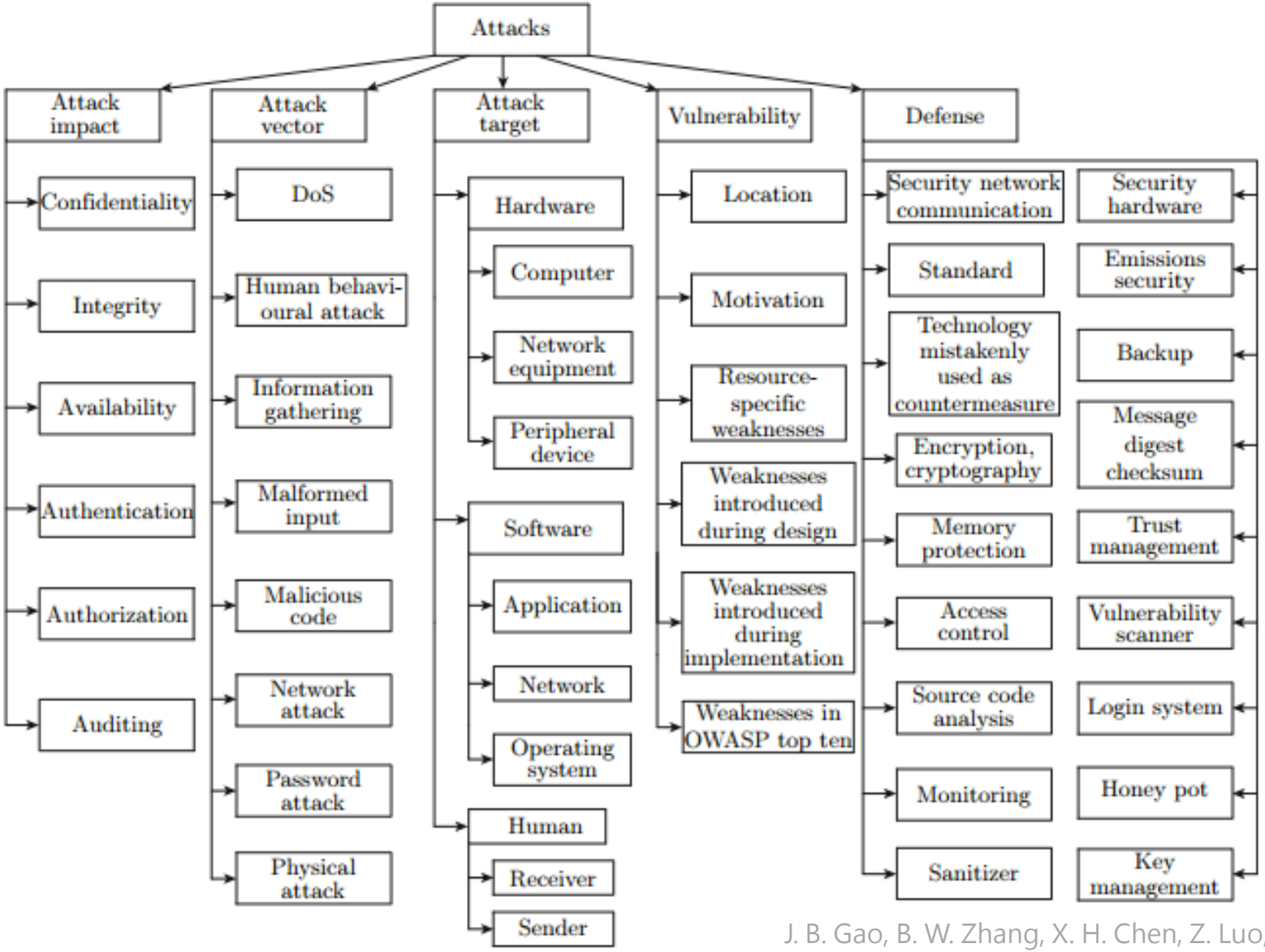




A Commonly Used Taxonomy

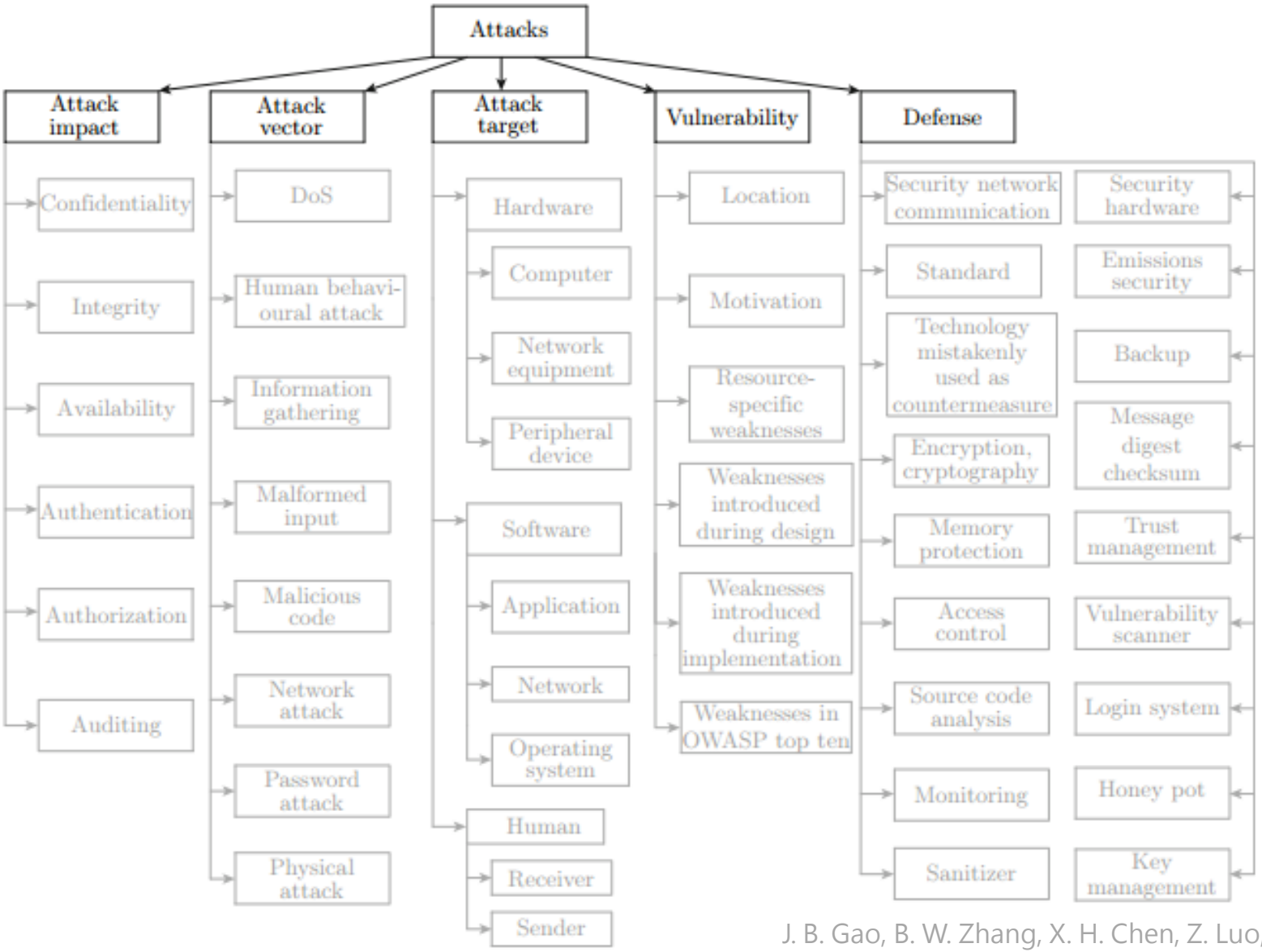


Attack Taxonomy Example



J. B. Gao, B. W. Zhang, X. H. Chen, Z. Luo, 2013

Attack Taxonomy Example



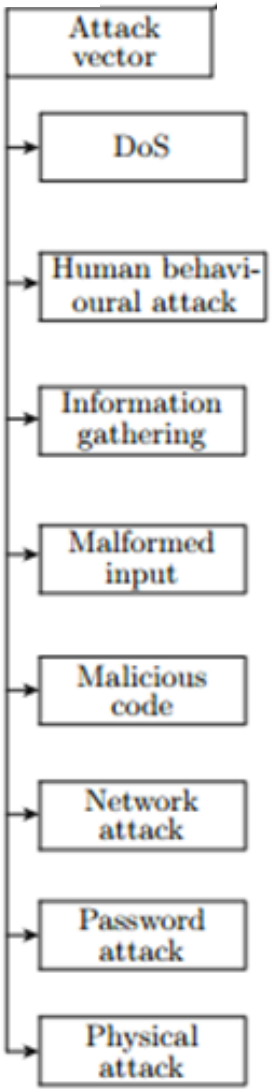
J. B. Gao, B. W. Zhang, X. H. Chen, Z. Luo, 2013

Attack Taxonomy Example

- Attack Impact
  - ↳ attack impacts on security principles
- Attack Vector
  - ↳ path by which an attack is lauched
- Attack Target
  - ↳ attack targets such as hardware, software or users
- Vulnerability
  - ↳ weaknesses and flaws of the system
- Defense
  - ↳ defence and prevention methods

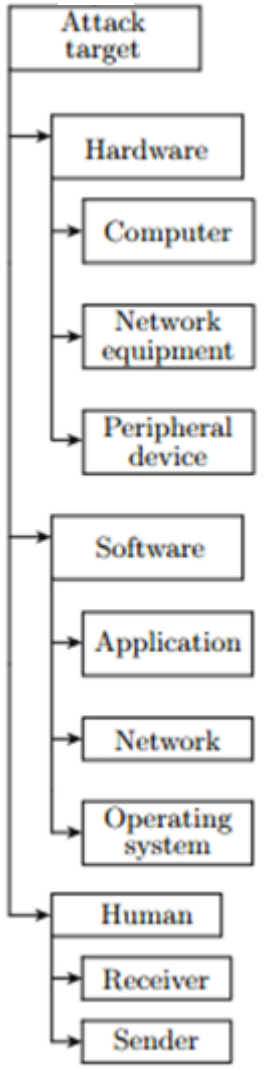
Attack Taxonomy Example

- Attack Impact
  - ↳ attack impacts on security principles
- Attack Vector
  - ↳ path by which an attack is lauched
- Attack Target
  - ↳ attack targets such as hardware, software or users
- Vulnerability
  - ↳ weaknesses and flaws of the system
- Defense
  - ↳ defence and prevention methods



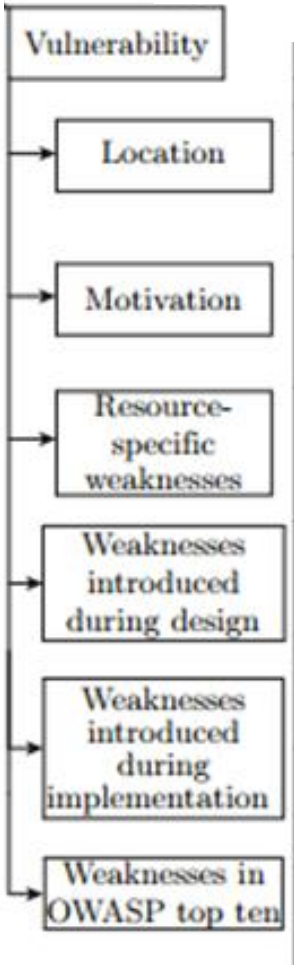
Attack Taxonomy Example

- Attack Impact
  - ↳ attack impacts on security principles
- Attack Vector
  - ↳ path by which an attack is lauched
- Attack Target
  - ↳ attack targets such as hardware, software or users
- Vulnerability
  - ↳ weaknesses and flaws of the system
- Defense
  - ↳ defence and prevention methods



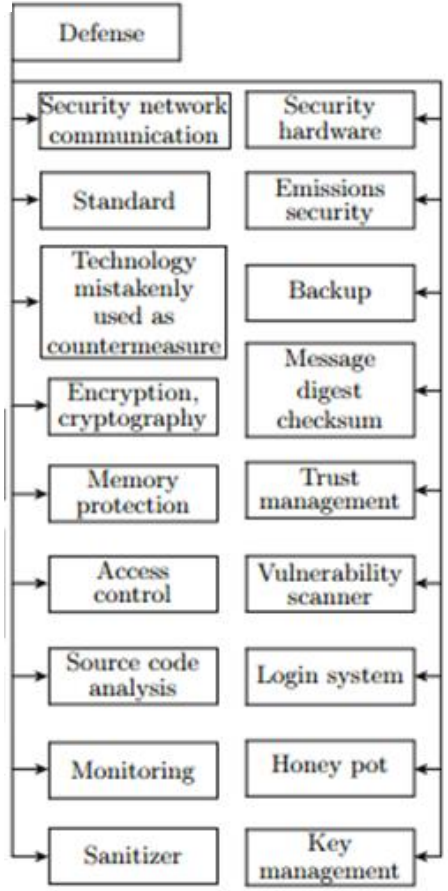
Attack Taxonomy Example

- Attack Impact
  - ↳ attack impacts on security principles
- Attack Vector
  - ↳ path by which an attack is lauched
- Attack Target
  - ↳ attack targets such as hardware, software or users
- Vulnerability
  - ↳ weaknesses and flaws of the system
- Defense
  - ↳ defence and prevention methods



Attack Taxonomy Example

- Attack Impact
  - ↳ attack impacts on security principles
- Attack Vector
  - ↳ path by which an attack is lauched
- Attack Target
  - ↳ attack targets such as hardware, software or users
- Vulnerability
  - ↳ weaknesses and flaws of the system
- Defense
  - ↳ defence and prevention methods



Attack Example SQL Slammer

A standalone malicious program which uses computer or network resources to make complete copies of itself. May include code or other malware to damage both the system and the network.

Attack Impact	Attack Vector	Attak Target	Vulnerability	Defense
Availability Integrity	UDP Buffer Overflow Worm (Malicious code) DoS	MS SQL server 2000 (Software - Network)	CVE-2002-0649 (Implementation)	Patch System

Limitations of Taxonomies

- developed only for specific domains
- reusability in other fields difficult
- difficult extend or update
- inconsistant vocabulary/ no formal language
- only represent hierarchical relationships

From Taxonomies to Ontologies

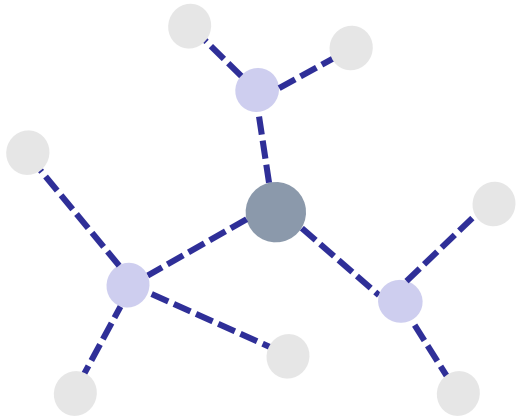
> An ontology is an explicit specification of conceptualization.
>
> *Gruber, T. R., 1993*

An ontology consists of…

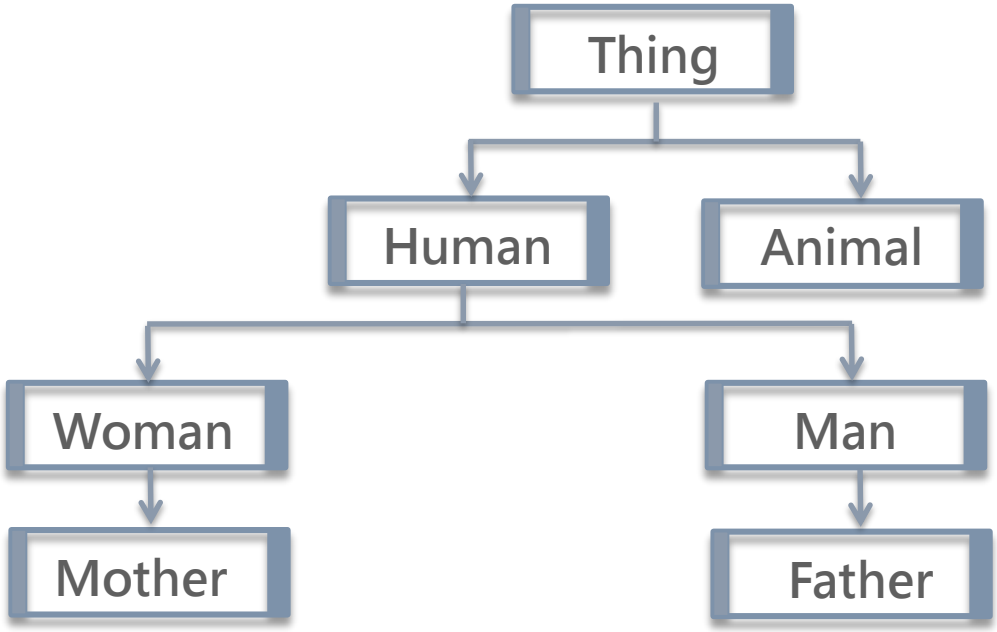
- **classes** to describe a domain
- **slots** to describe relationships in a **taxonomy**
- **facets** to describe restrictions for slots

Ontologies vs. Taxonomies

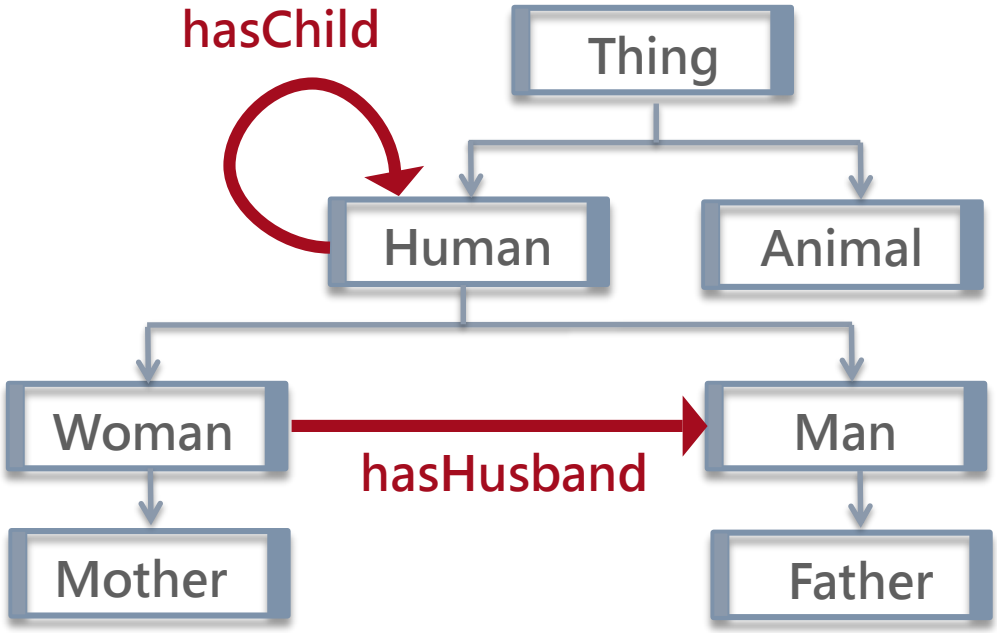
- Use hierarchical and semantical relationships between classes
- Provide machine interpretable semantic and syntax (RDF, OWL)
- They enable easy extension and sharing of knowledge



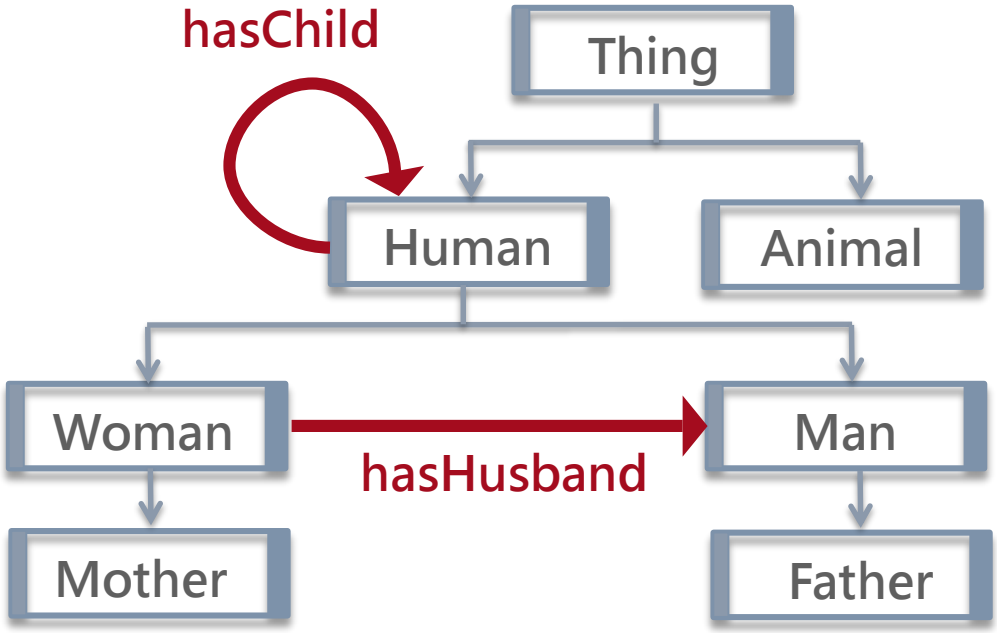
Example Ontology



Example Ontology

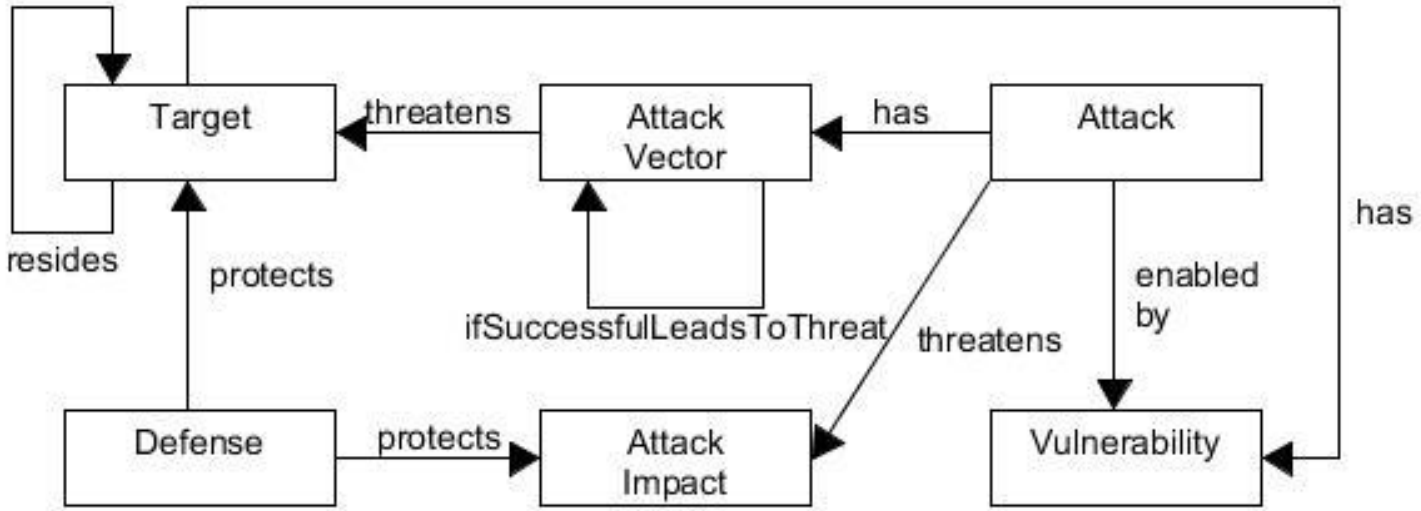


Example Ontology



1. A woman can have 0 or 1 huband.
2. A human can have 0 or n children.
3. Every mother must have at least 1 child.

Attack Ontology Example



The SQL Slammer **is** a computer worm and **has** the attack vectors buffer overflow and denial of service. The attack **is enabled** by the vulnerabilities due to implementation flaws. **Threatened** targets are networks. If a Slammer attack **succeeds** he can cause further DoS attacks.

J. B. Gao, B. W. Zhang, X. H. Chen, Z. Luo, 2013

Utility of Ontologies

- Locate IT security vulnerabilities and risks
  - Detect vulnerabilities (Vulnerabilities) on system (Attack Target)
  - Query what attacks can occur based on the , vulnerabilities(Attack Vector)
  - Determine risks (Attack Impact)
  - Determine neccessary defense methods (Defense)

- Uses of other ontologies
  - Intrusion Detection Systems (IDS) and application fire walls :

    Monitoring component collects data(traffic, requests, packets) and alerting system provides response on attempted attack and countermeasures

Conclusion

- Taxonomies are important building blocks in a full function information architecture.
- Ontologies extend taxonomy functionalities by overcoming their limitiations.
- A large variety of attack taxonomies and ontologies exists focusing on different fields of research.
- Existing taxonomies and ontologies need to be comined to create a flexible, extensible and standard classification scheme.

Literatur

M. Bishop, D. Bailey: A critical analysis of vulnerability taxonomies, California University Davis, Department of Computer Science, 1996

J. B. Gao, B. W. Zhang, X. H. Chen, Z. Luo: Ontology-based model of network and computer attacks for security assessment Journal of Shanghai Jiaotong University (Science), 18. Jg., pages 554-562, 2013

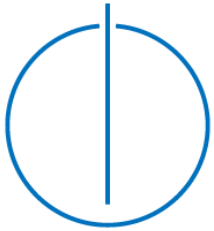
T. R. Gruber: A translation approach to portable ontology specications, Knowledge acquisition, 5. Jg., Nr. 2, pages 199-220, 1993

J. Undercoer, A. Joshi, J. Pinkston: Modeling computer attacks: An ontology for intrusion detection, In: Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, pages 113-135, 2003

R. P. van Heerden, B. Irwin, I. D. Burke: Classifying network attack scenarios using an Ontology, In: Proceedings of the 7th International Conference on Information Warfare and Security. Academic Conferences Limited, pages 331-324, 2012

Contact

Fakultät für Informatik



Informatik VIII: Lehrstuhl für Netzarchitekturen und Netzdienste

Natascha Abrek

abrek@in.tum.de