



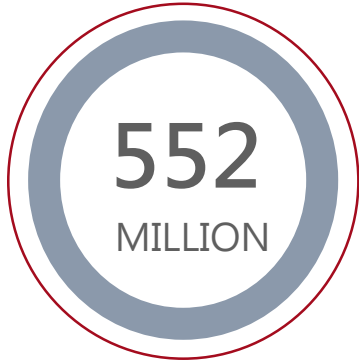
# Attack Taxonomies and Ontologies

Seminar Future Internet  
Supervisor: Nadine Herold  
Natascha Abrek  
02.10.2014

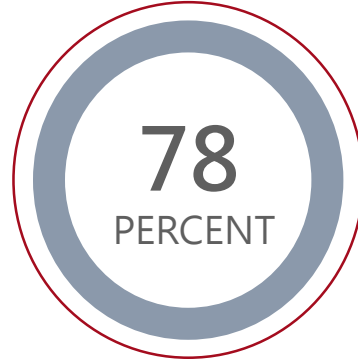




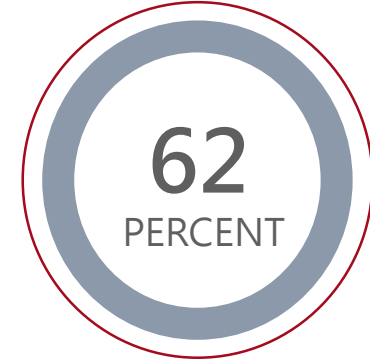
# 2013 in Numbers



IDENTITIES  
EXPOSED

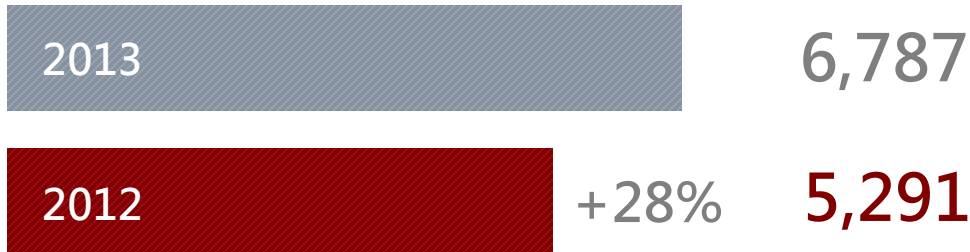


OF WEBSITES WITH  
VULNERABILITIES



GROWTH OF DATA  
BREACHES FROM 2012

## New Vulnerabilities



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



# 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



A taxonomy is a system of classification which allows the unique identification of object

*Bishop, M., Bailey, D.;1996*

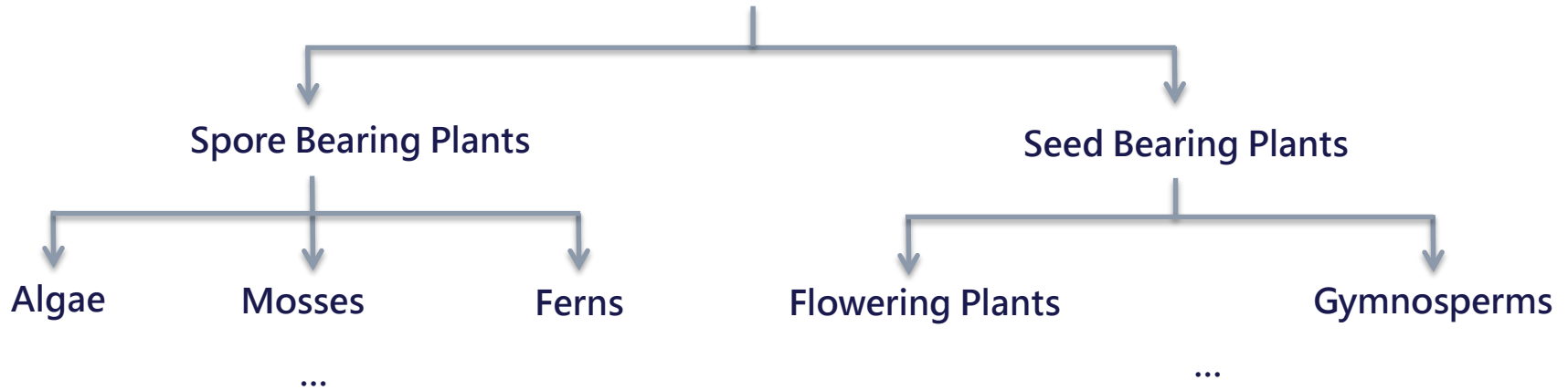
A taxonomy...

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

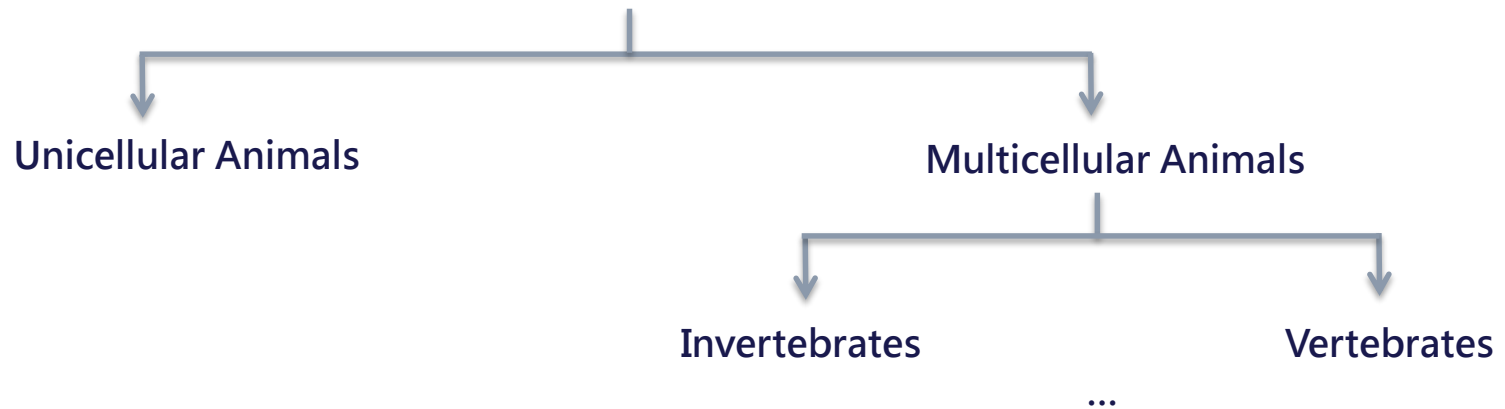


# Well-known Taxonomies

## PLANT KINGDOM



## ANIMAL KINGDOM





# A Commonly Used Taxonomy

amazon.de [Mein Amazon](#) [Angebote](#) [Gutscheine](#) [Verkaufen](#) [Hilfe](#)

Alle Kategorien ▾ Suche   [Hallo! Anmelden Mein Konto ▾](#) [Prime testen ▾](#)

## Amazon Instant Video

- [Amazon Instant Video](#)
- [Prime Instant Video](#)
- [Instant Video Shop](#)
- [Meine Watchlist](#)
- [Meine Video-Bibliothek](#)
- [Auf vielen Geräten verfügbar](#)

## Musik-Downloads

- [Musik-Downloads](#)
- [Ihre Amazon Music Bibliothek](#)
- [Amazon Music App für Android](#)
- [Amazon Music App für iOS](#)

## App-Shop für Android

- [Apps und Spiele](#)
- [Spiele](#)
- [Amazon Apps](#)
- [Ihre Apps und Geräte](#)

## Amazon Cloud Drive

- [Anmeldung zu Ihrem Cloud Drive](#)
- [Legen Sie mit kostenlosen 5 GB los](#)
- [Erfahren Sie mehr](#)
- [Laden Sie die mobile Apps](#)

## Kindle eReader & Bücher

- [Kindle](#)
- [Kindle Paperwhite](#)
- [Kindle Voyage](#)
- [Kindle-Zubehör](#)
- [Kindle eBooks](#)
- [Enlische eBooks](#)

## Fire-Tablets

- [Fire HD 6](#)
- [Fire HD 7](#)
- [Kindle Fire HDX](#)
- [Fire HDX 8.9](#)
- [Fire-Zubehör](#)
- [Amazon Instant Video](#)
- [Apps & Spiele](#)
- [Musik-Downloads](#)
- [Kindle eBooks](#)
- [Alle Hörbuch-Downloads](#)
- [Meine Inhalte und Geräte](#)

## Amazon Fire TV

- [Amazon Fire TV](#)
- [Amazon Fire-Gamecontroller](#)
- [Prime Instant Video](#)
- [Amazon Instant Video](#)
- [Fire TV Apps und Spiele](#)
- [Amazon Cloud Drive](#)

## Amazon Fire Phone

- [Amazon Fire Phone](#)
- [Zubehör](#)
- [Musik-Downloads](#)
- [Amazon Cloud Drive](#)
- [Amazon Instant Video](#)

## Bücher

- [Alle Bücher](#)
- [Kindle eBooks](#)
- [Fremdsprachige Bücher](#)
- [Fachbücher](#)

## Filme, TV, Musik, Games

- [Amazon Instant Video](#)
- [Alle DVDs & Blu-rays](#)
- [LOVEFILM DVD Verleih](#)
- [Musik-CDs & Vinyl](#)
- [Musik-Downloads](#)
- [Musikinstrumente & DJ-Equipment](#)
- [Games](#)
- [Games-Downloads](#)
- [Trade-In: Games, DVDs & Blu-Rays](#)

## Elektronik & Computer

- [Kamera & Foto](#)
- [Handys & Verträge](#)
- [Fernseher & Heimkino](#)
- [Audio & HiFi](#)
- [Musikinstrumente & DJ-Equipment](#)
- [Navigation](#)
- [Elektronik-Zubehör](#)
- [Konsolen & Games-Zubehör](#)
- [Haushaltsgeräte & Staubsauger](#)
- [Elektro-Großgeräte](#)
- [Alle Produkte](#)
- [Notebooks](#)
- [Tablets](#)
- [Computer-Zubehör](#)
- [PC-Komponenten](#)
- [Software](#)
- [Software-Downloads](#)
- [PC- & Video-Games](#)
- [Games-Downloads](#)
- [Drucker & Tintenpatronen](#)
- [Richtbedarf & Schreibwaren](#)

## Beauty, Drogerie & Lebensmittel

- [Beauty](#)
- [Premium Beauty](#)
- [Männerpflege](#)
- [Drogerie, Körper- & Babypflege](#)
- [Gesundheit, Mobilität & Sehhilfen](#)
- [Lebensmittel & alkoholfreie Getränke](#)
- [Bier, Wein & Spirituosen](#)
- [Bewusst genießen](#)
- [Sonderangebote](#)
- [Spar-Abo](#)

## Spielzeug & Baby

- [Spielzeug](#)
- [Baby](#)
- [Kinderwelt](#)
- [Brettspiele](#)
- [Baby-Wunschliste](#)

## Kleidung, Schuhe & Uhren

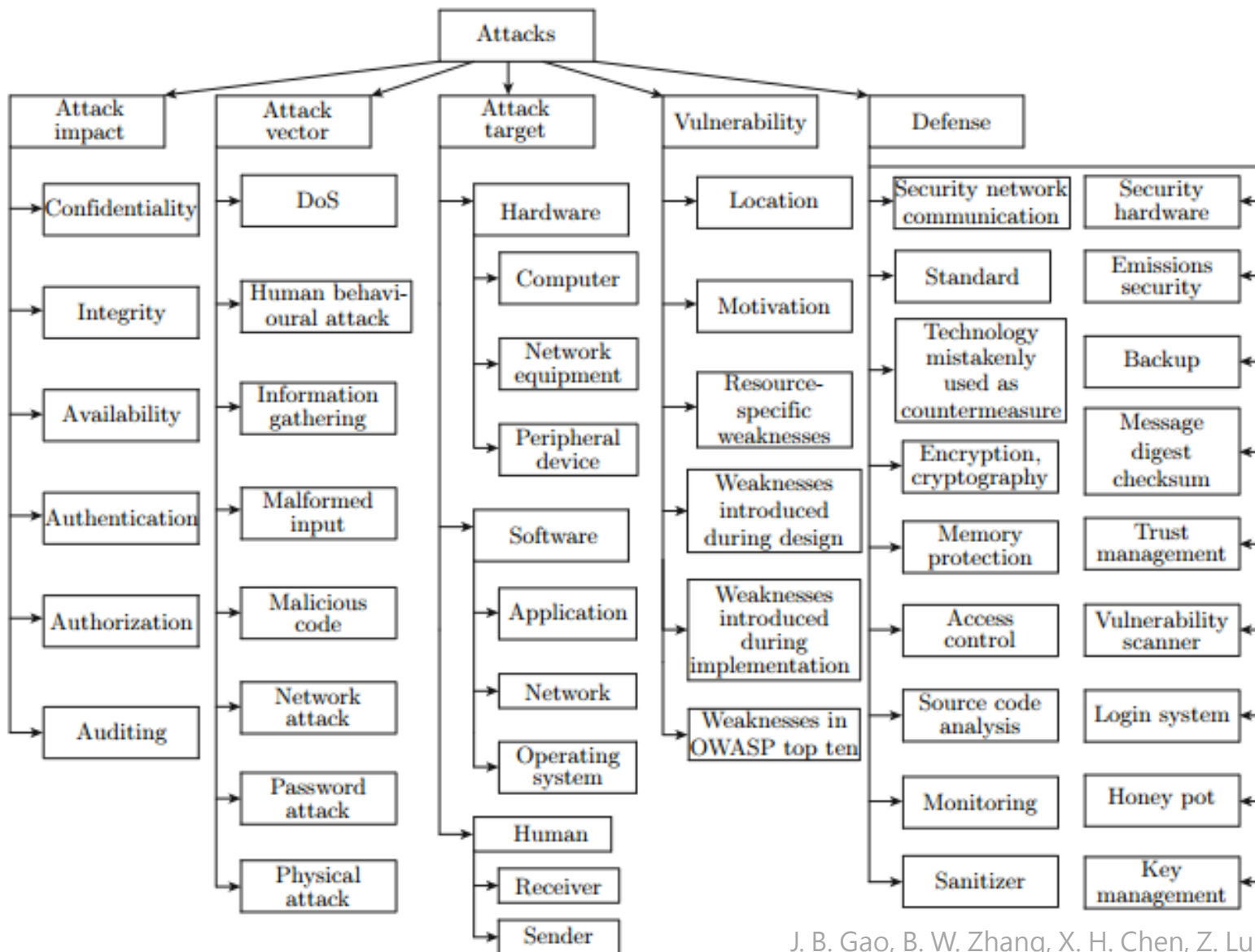
- [Bekleidung](#)
- [Schuhe](#)
- [Handtaschen](#)
- [Koffer, Rucksäcke & Taschen](#)
- [Accessoires](#)
- [Schmuck](#)
- [Uhren](#)
- [Amazon BuyVIP](#)

## Sport & Freizeit

- [Alle Sport-Produkte](#)
- [Camping & Outdoor](#)
- [Fitness](#)



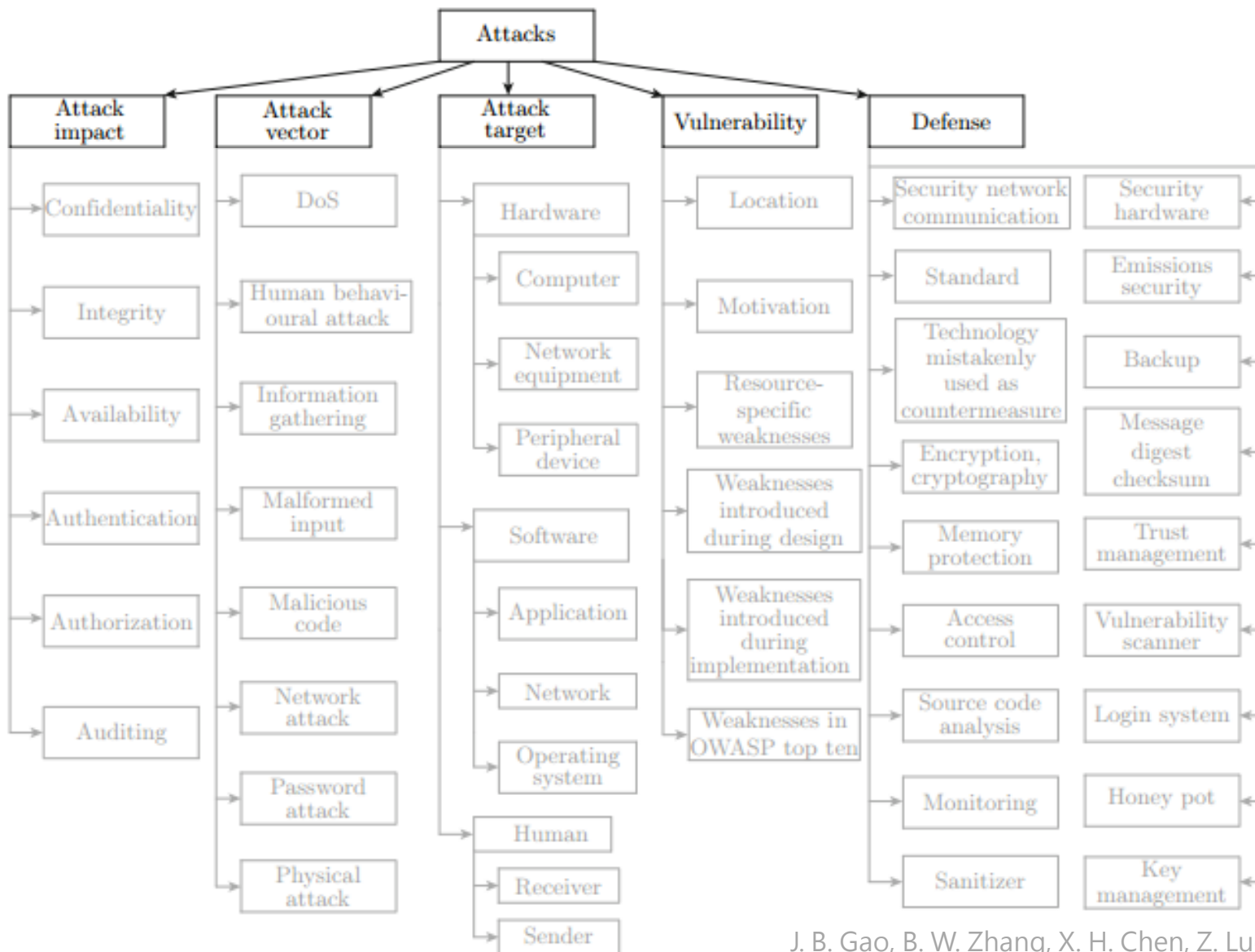
# Attack Taxonomy Example



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

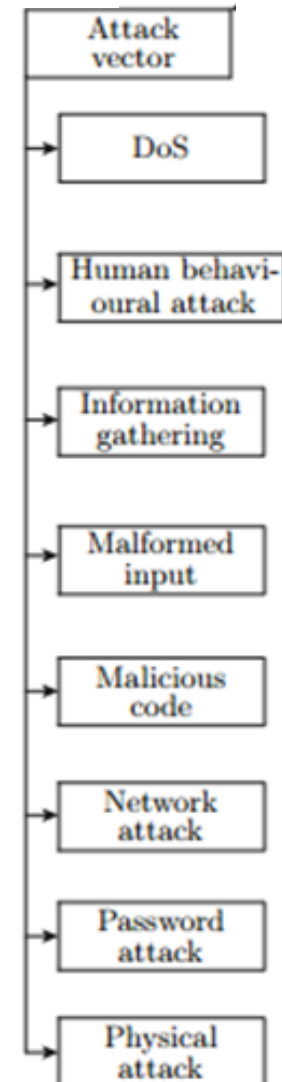
- **Attack Impact**  
↳ attack impacts on security principles
- **Attack Vector**  
↳ path by which an attack is launched
- **Attack Target**  
↳ attack targets such as hardware, software or users
- **Vulnerability**  
↳ weaknesses and flaws of the system
- **Defense**  
↳ defence and prevention methods





# Attack Taxonomy Example

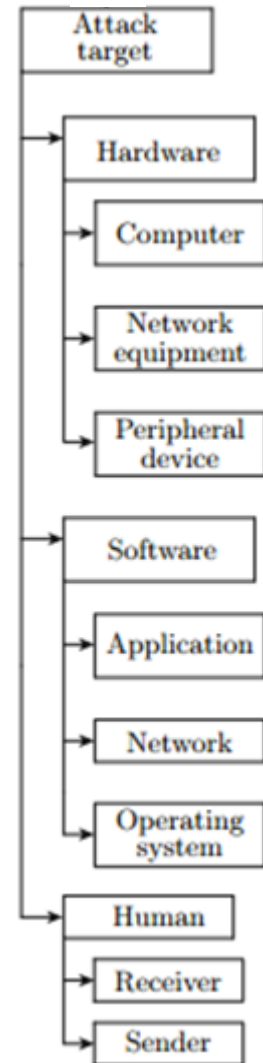
- Attack Impact
  - ↳ attack impacts on security principles
- Attack Vector
  - ↳ path by which an attack is launched
- Attack Target
  - ↳ attack targets such as hardware, software or users
- Vulnerability
  - ↳ weaknesses and flaws of the system
- Defense
  - ↳ defence and prevention methods





# Attack Taxonomy Example

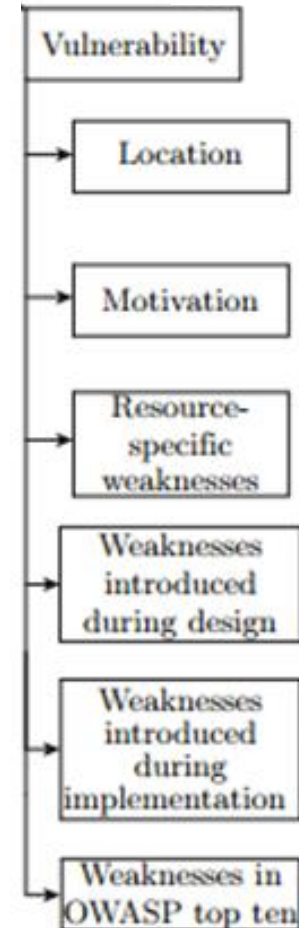
- Attack Impact
  - ↳ attack impacts on security principles
- Attack Vector
  - ↳ path by which an attack is launched
- Attack Target
  - ↳ attack targets such as hardware, software or users
- Vulnerability
  - ↳ weaknesses and flaws of the system
- Defense
  - ↳ defence and prevention methods





# Attack Taxonomy Example

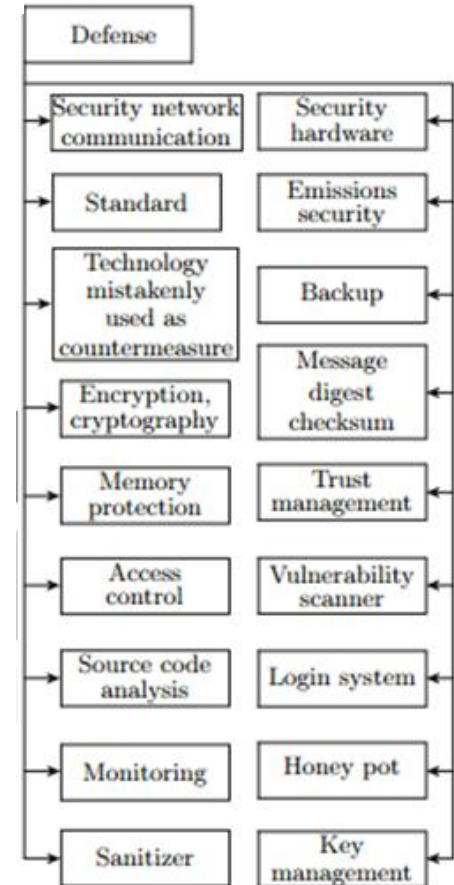
- Attack Impact
  - ↳ attack impacts on security principles
- Attack Vector
  - ↳ path by which an attack is launched
- Attack Target
  - ↳ attack targets such as hardware, software or users
- Vulnerability
  - ↳ weaknesses and flaws of the system
- Defense
  - ↳ defence and prevention methods





# Attack Taxonomy Example

- Attack Impact  
↳ attack impacts on security principles
- Attack Vector  
↳ path by which an attack is launched
- 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
- inconsistent vocabulary/ no formal language
- only represent hierarchical relationships



An ontology is an explicit specification of conceptualization.

*Gruber, T. R., 1993*

An ontology consists of...

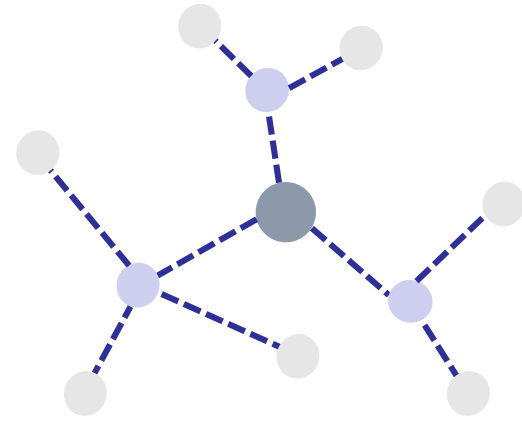
- **classes** to describe a domain
- **slots** to describe relationships in a **taxonomy**
- **facets** to describe restrictions for slots





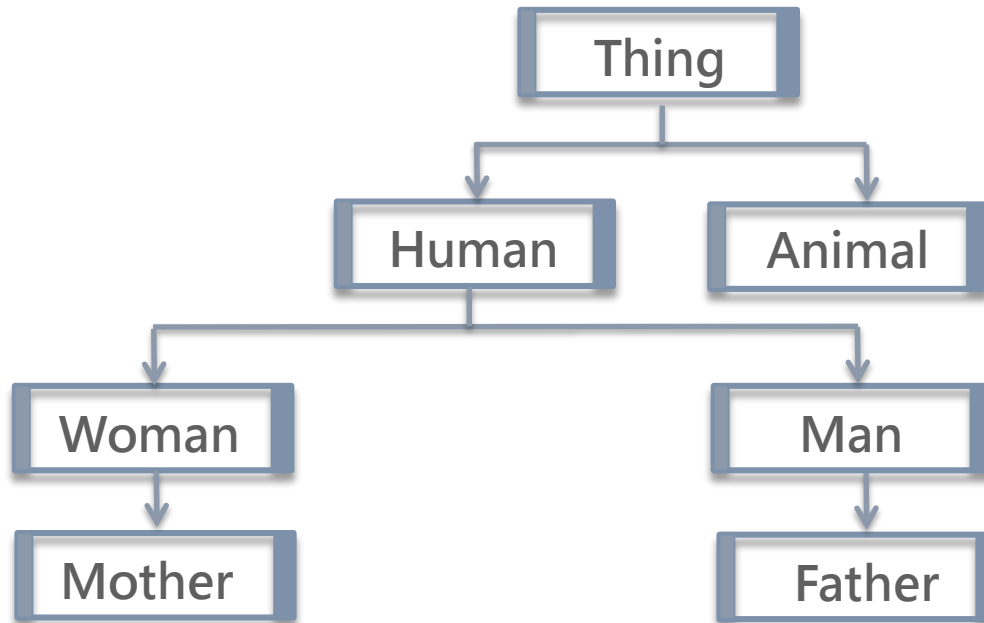
# Ontologies vs. Taxonomies

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



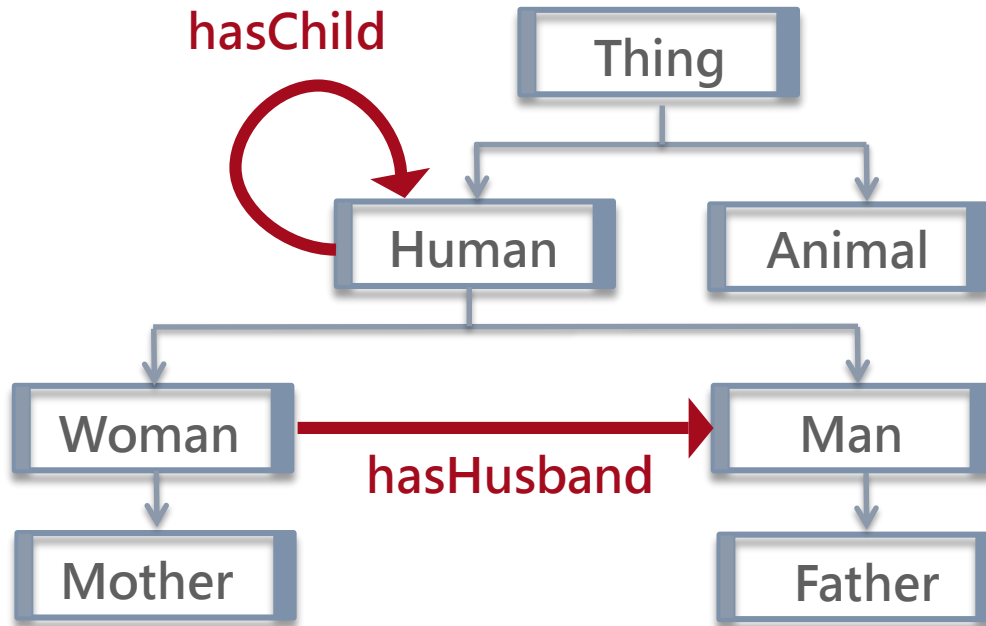


# Example Ontology



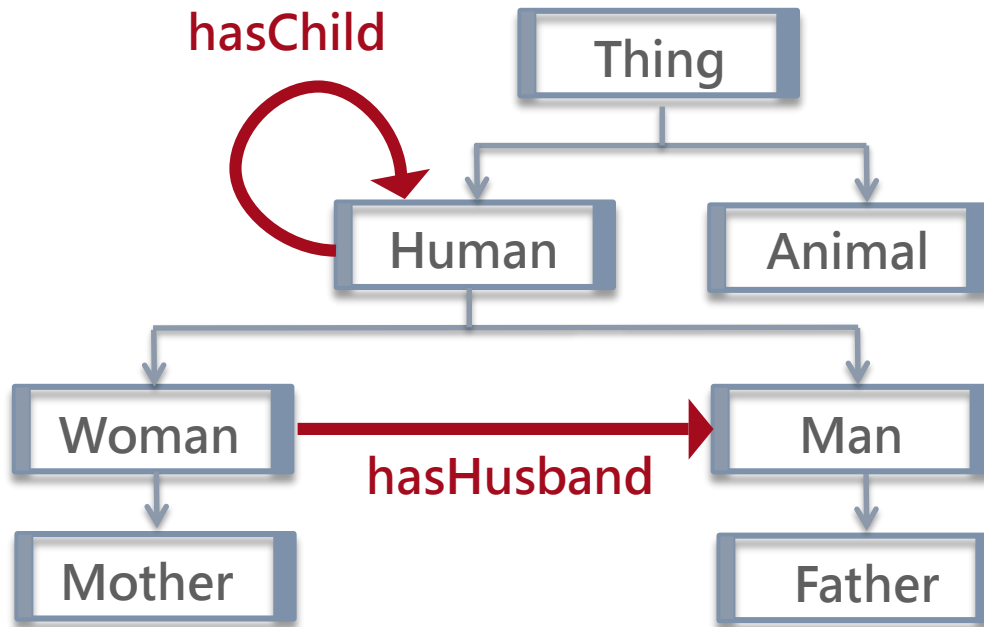


# Example Ontology





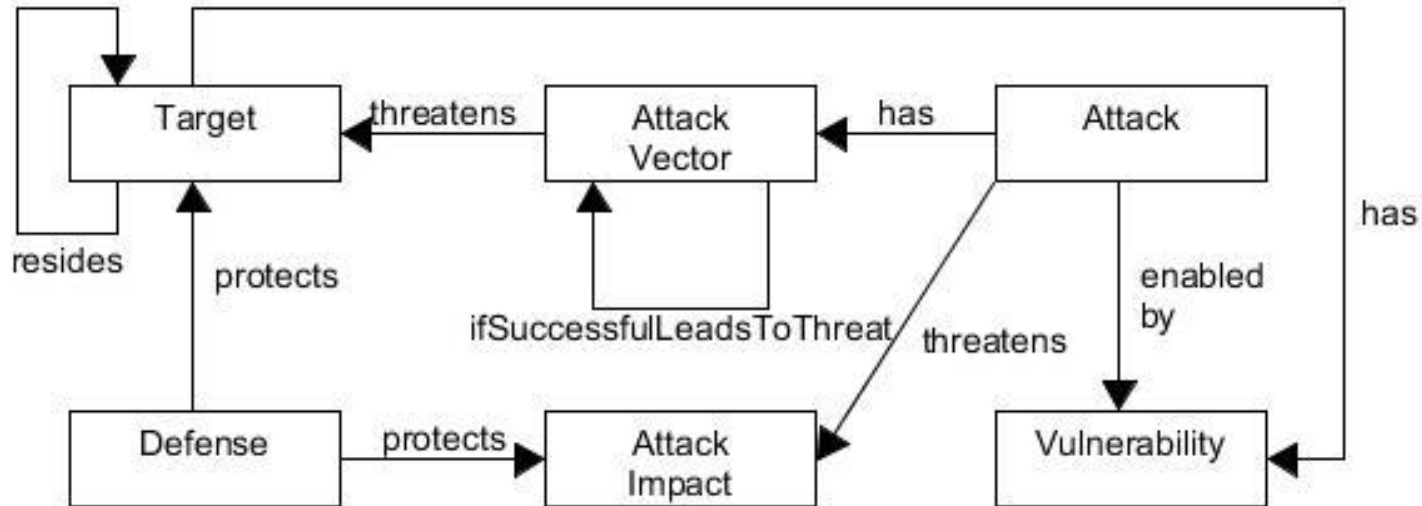
# Example Ontology



1. A woman can have 0 or 1 husband.
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.



# 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 necessary 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 limitations.
- A large variety of attack taxonomies and ontologies exists focusing on different fields of research.
- Existing taxonomies and ontologies need to be combined to create a flexible, extensible and standard classification scheme.



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 specifications, Knowledge acquisition, 5. Jg., Nr. 2, pages 199-220, 1993

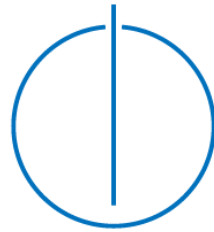
J. Undercoer, A. Joshi, J. Pinkston: Modeling computer attacks: An ontology for intrusion detection, In: Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, pages 113-135, 2003

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





Fakultät für  
Informatik



Informatik VIII: Lehrstuhl  
für Netzarchitekturen und  
Netzdienste

Natascha Abrek  
[abrek@in.tum.de](mailto:abrek@in.tum.de)