Workshop on
Novel Approaches to Risk and Security Management for Utility Providers and Critical Infrastructures

Using Vulnerable Hosts to Assess Cyber Security Risk in Critical Infrastructures

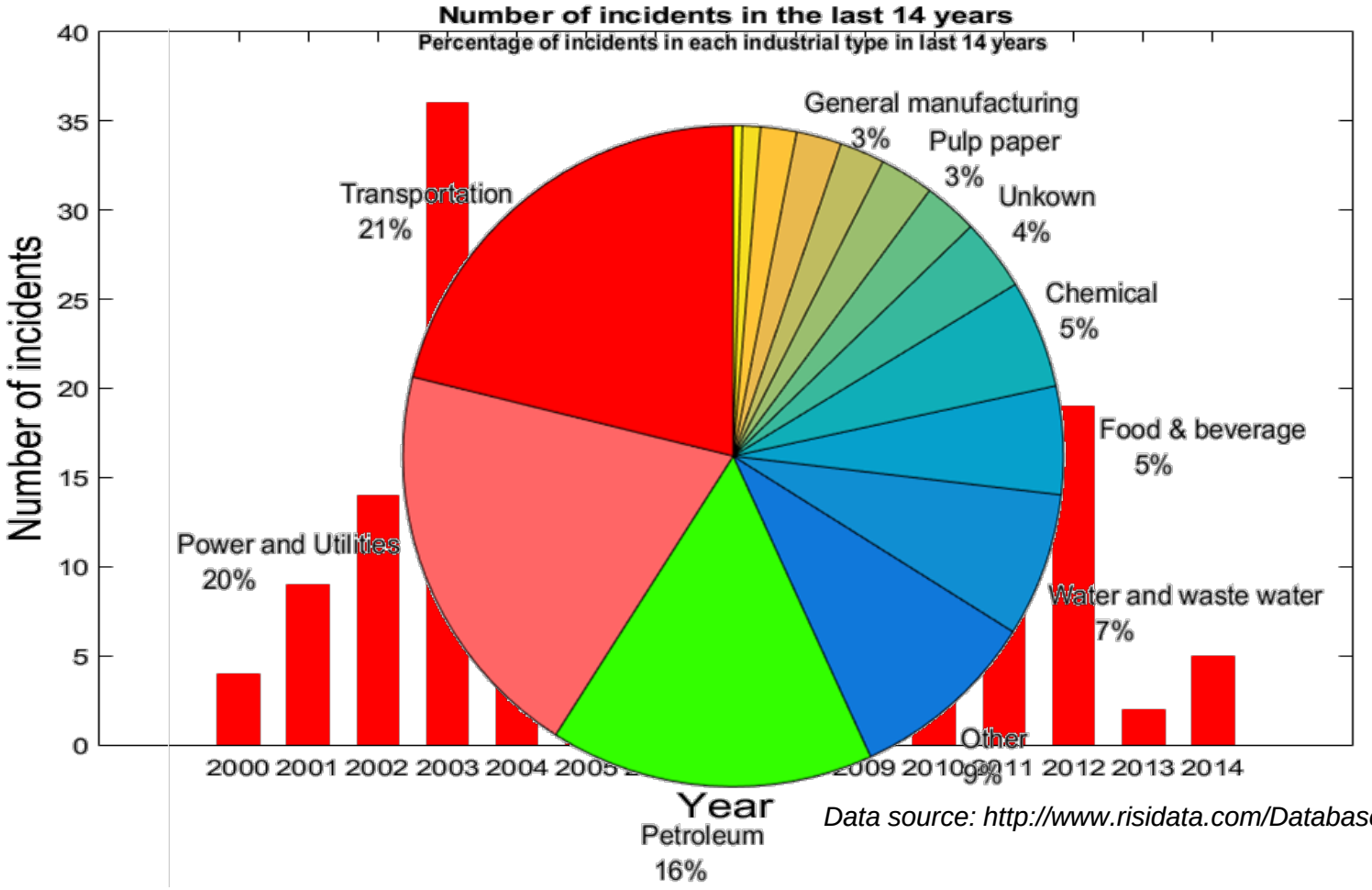
Xiaobing He
Hermann de Meer
University of Passau
Chair of Computer Networking and Communication

Vienna 02.11.2015

Contents

- Motivation
- Problem description
- Vulnerability-centric risk model
- Conclusion and outlook

Motivation (1/2)



Data source: http://www.risidata.com/Database

Motivation (2/2)

- Modern industrial critical infrastructures are
  - Prone to cyber-related vulnerabilities
  - Prone to hard- and software failures (systematic)
  - Interdependent (cascading failures)
- Cyber attacks on critical infrastructures increase in number and impact
  - Annual losses in the range of 260-340 billion €*
  - Recent attacks targeting critical infrastructures: Dragonfly and Shamoon Operations

**ENISA: Cyber Attacks cost over $400 Billion Annually*

Problem description

- Goals
  - Identify and mitigate security incidents
  - Supply security operators with quantitative risk value
- Problems
  - Vulnerability-based risk analysis
    - Potentially ignored vulnerability evolution
    - Challenging to integrate the strategic importance of hosts
  - Accommodating heterogeneous/interdependent hosts in the same model framework
  - Challenges of understanding vulnerability interdependency

Vulnerability-centric risk model

- **Vulnerability-centric risk model** to achieve aforementioned goals
- Features
  - Strategic importance of hosts is respected
    - Novel risk score metric respecting importance of hosts
  - Network topology and resulting interconnectedness
    - Spreading of incidents can be simulated
  - Probability reasoning
    - Calculation of likelihood of vulnerability exploitation

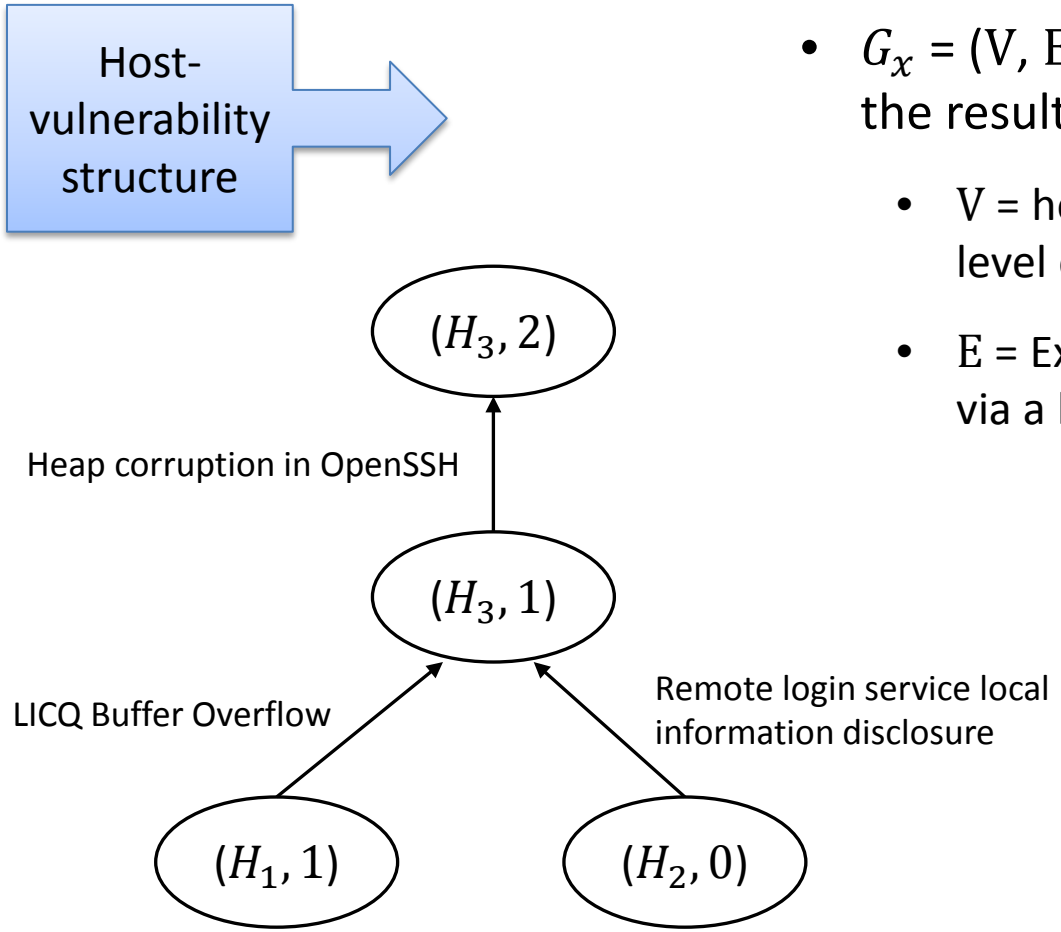
Vulnerability-centric risk model

- Model uses vulnerability-centric approach
  - Vulnerability can be discovered by manual look-ups
  - Vulnerability data can be collected by active/passive scanners
  - Success of an attack depends on the degree of vulnerability

Vulnerability-centric risk model

- Model assumptions
  - Does not account for the time interval of vulnerability exploitation
  - Consider the design and system flaws
  - Intelligent/adaptive behaviors of attackers are not included
  - The influence of different environments on the risk is omitted

Vulnerability-centric risk model

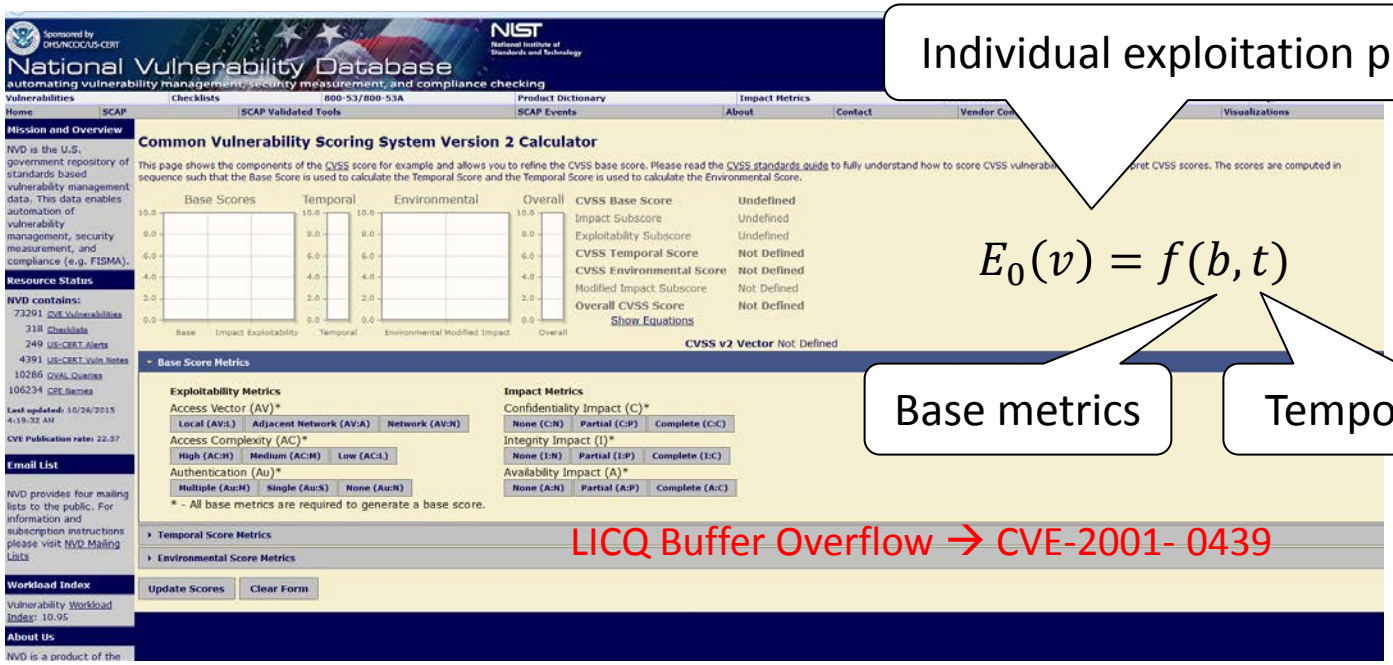


- G_x = (V, E) represents a graph showing the result of an attack A:
  - V = hosts (H_x) and the obtained privilege level of a given attack A (0, 1, 2)
  - E = Exploitation of a given vulnerability via a logical network connection

Vulnerability-centric risk model

Host-vulnerability structure

CVSS-based Individual Score Assignment



Individual exploitation probability

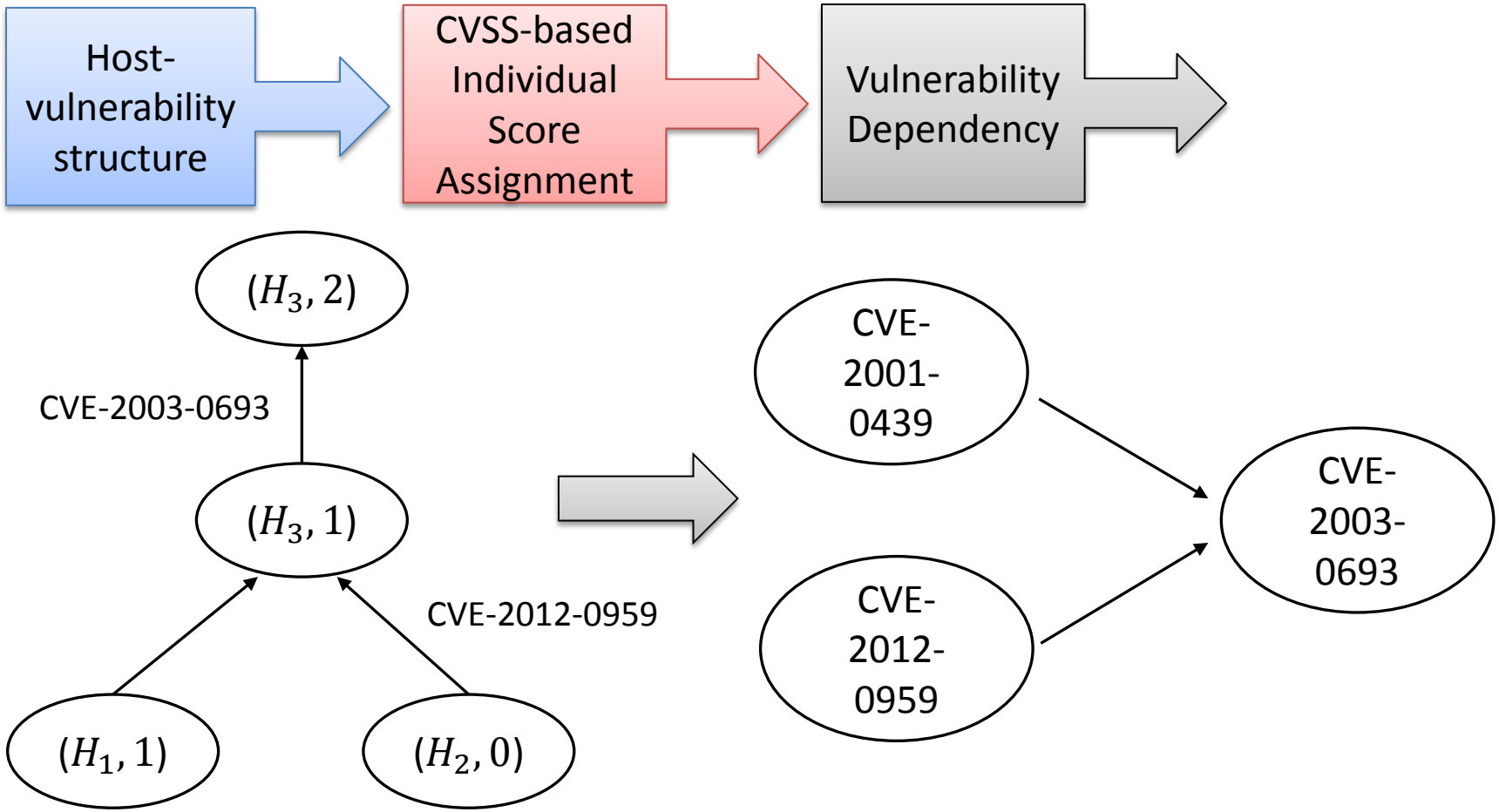
$$E_0(v) = f(b, t)$$

Base metrics

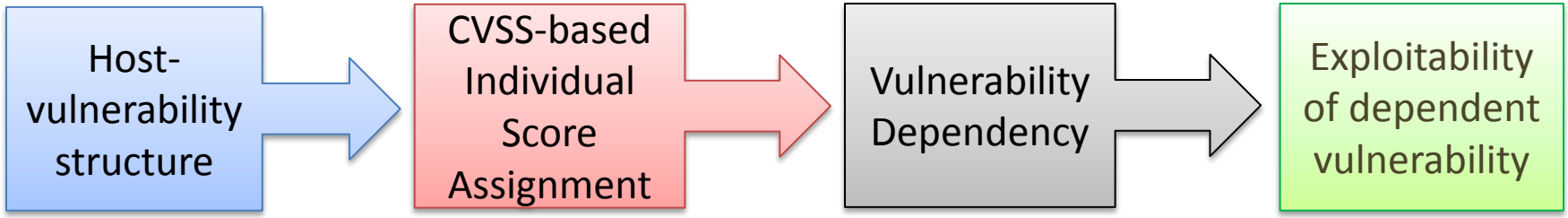
Temporal metrics

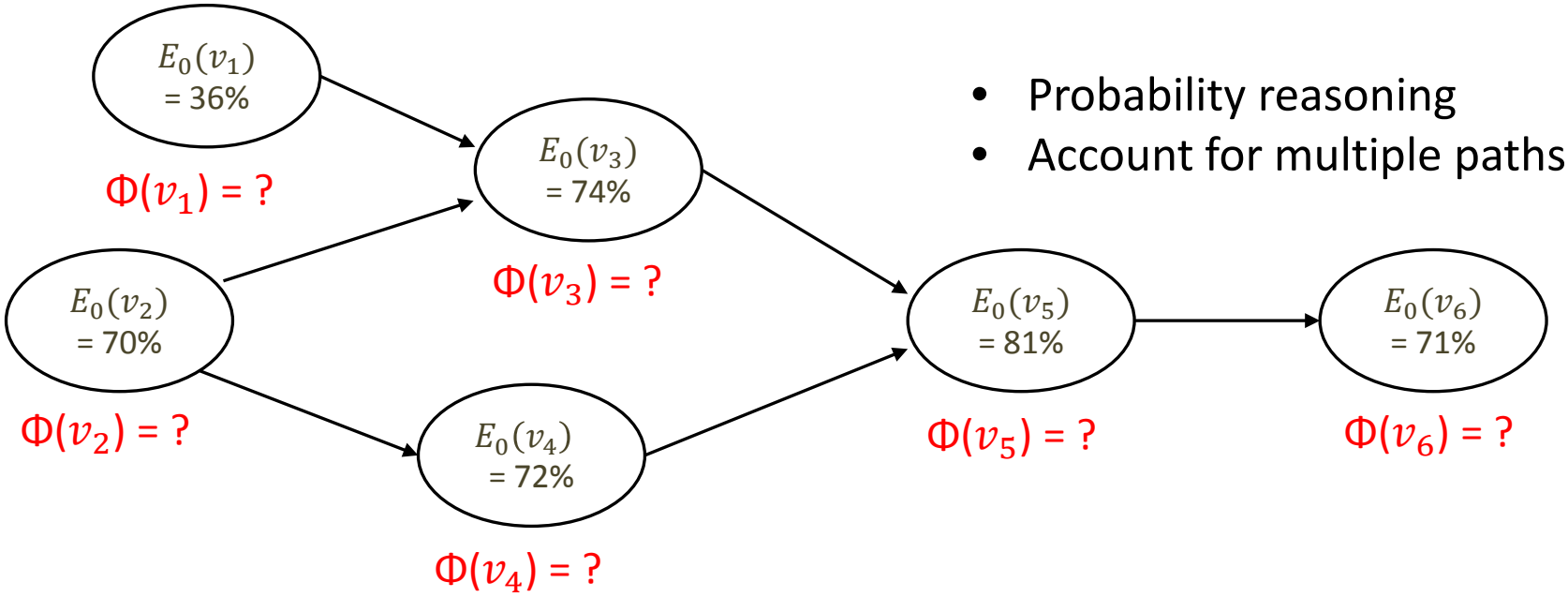
LICQ Buffer Overflow → CVE-2001- 0439

Vulnerability-centric risk model



Vulnerability-centric risk model





- Probability reasoning
- Account for multiple paths

Vulnerability-centric risk model

- Qualitative risk

$$R_h = \epsilon \sum_{i=1}^{M} (D_i \times \Phi(v_i))$$

Where:

- ϵ = the strategic importance level of host *h* [0,1]
- D_i = the estimate of potential damage [€] after exploiting v_i
- $\Phi(v_i)$ = the cumulative exploitability probability [0,1]

Conclusion and outlook

- A quantitative risk analysis
  - Focuses on system's topology structure and a list of vulnerabilities
  - Uses a probability reasoning algorithm to induce the likelihood of vulnerability exploitation
- Possible future extensions
  - A supporting tool to automate the analysis
  - Integrate costs of exploiting vulnerabilities to calculate risk
  - Risk analysis for zero-day vulnerabilities

EUROPEAN COMMISSION

UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

Thank you for listening!

Questions?