Security Ontologies

Rahul Hiran and Anna Vapen
2011-06-07

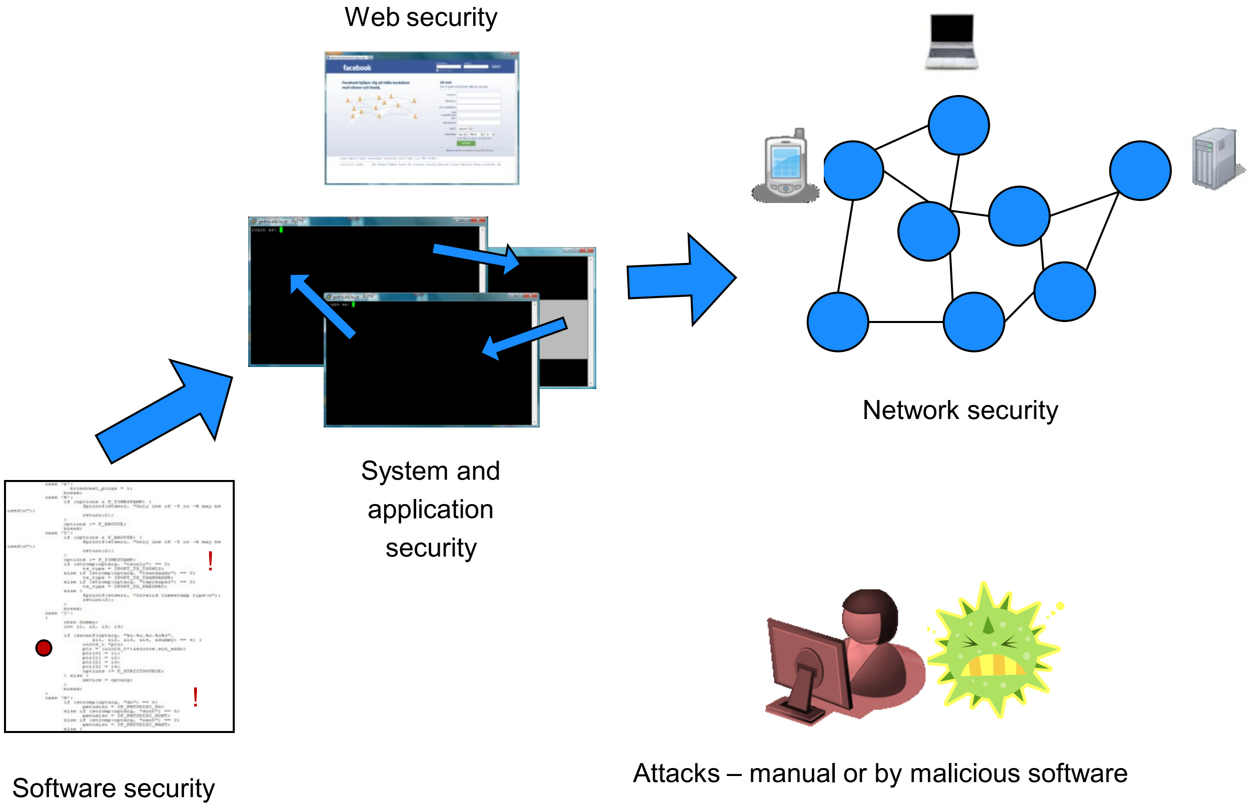
Presentation in the course "*Ontologies and ontology engineering*"

Linköping University
INSTITUTE OF TECHNOLOGY

Agenda

- Overview of information security
- Information security problems
- Security ontology examples
- Requirements of security ontologies
- Conclusions
- Discussion

Information Security Problems



Web security

System and application security

Network security

Software security

Attacks – manual or by malicious software

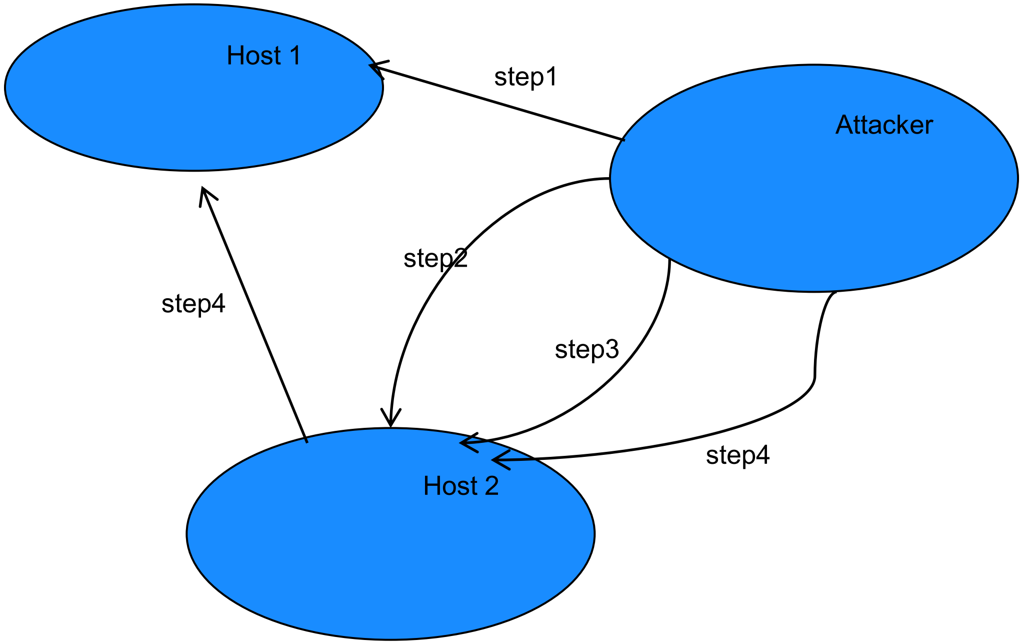
Web Service Security

- Security Attack Ontology for Web Services
- Web services Popularity
- New security threats
- How Attackers do it? Easy…Easy…Easy…!
- Example: XML Injection attack, DoS

Solutions

- Solutions to attacks just discussed
- Distributed Firewall/Intrusion Detection Systems
- Problems: Interoperability
- Rescue→ Ontologies
- Why Ontology?

Example: Mitnick attack and variation called XML Mitnick attack



OWL class for Mitnick attack

- <owl:Class rdf:ID="&WSAttacks;WSMittnick">
- <owl:intersectionOf rdf:parseType="Collection">
- <owl:Class rdf:about=”#SynFlood”/>
- <owl:Class rdf:about=”#WSProbing”/>
- <owl:Class rdf:about=”#Probing”/>
- <owl:Class rdf:about=”#XMLInjection”/>
- </owl:intersectionOf>
- </owl:Class>

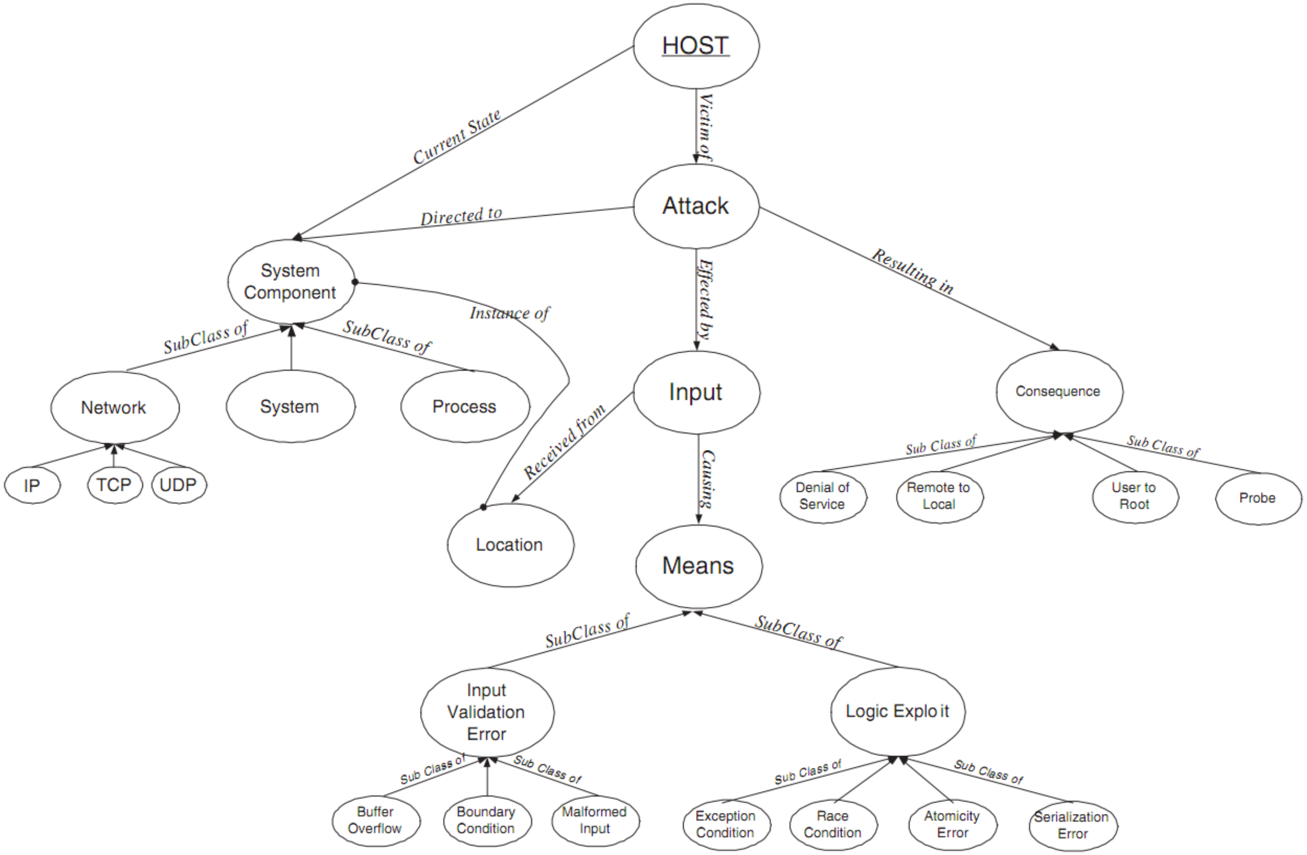
Modeling Computer Attacks: an Ontology for Intrusion Detection

- Issues with current IDS systems:
  - Changes necessitates change to the software system
  - Lacking reasoning capabilities
  - Interportability
- Ontologies to the rescue and how?

Target Centric Ontolgoy

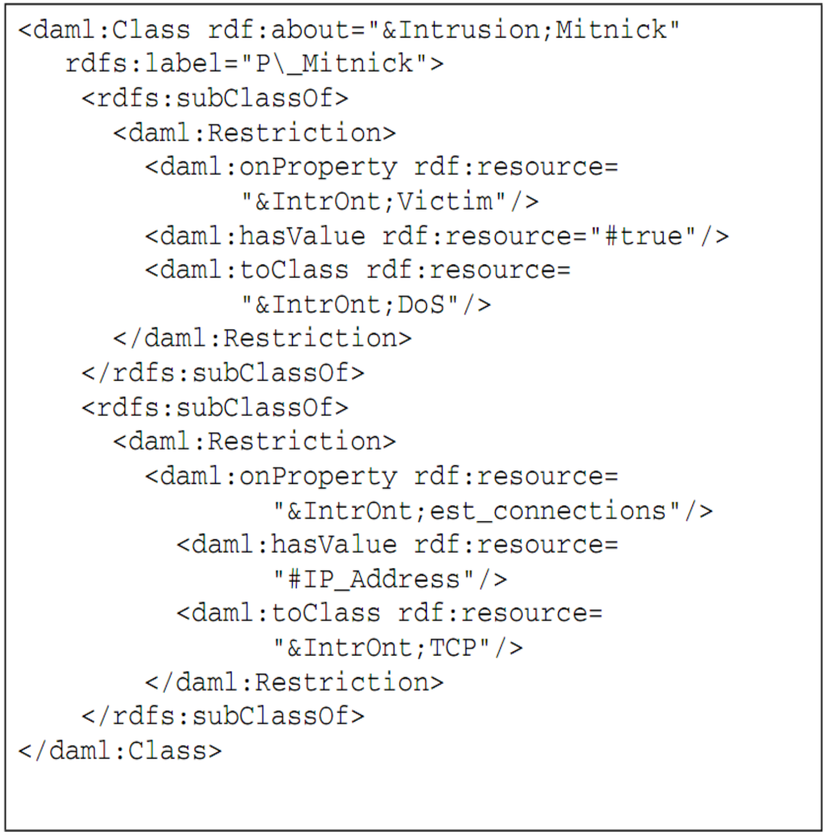
- From Taxonomy to Ontology
    - Taxonomy categorized according to genesis, time of introduction and location
    - Weber defined category *consequence*
    - Target Centric IDS from Lindqvist and Jonsson

Developed IDS Ontology



Detecting attacks with Ontology: Example

- A basic Denial of Service attack
- Mitnick attack (combination of DoS, TCP sequence number prediction and IP spoofing)
- DAML+OIL specification of Mitnick attack



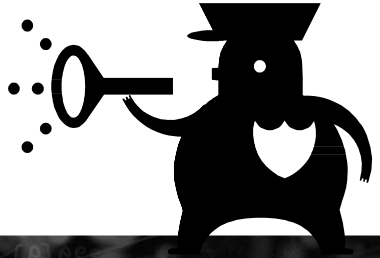
```
<daml:Class rdf:about="&Intrusion;Mitnick"
   rdfs:label="P\_Mitnick">
    <rdfs:subClassOf>
      <daml:Restriction>
        <daml:onProperty rdf:resource=
              "&IntrOnt;Victim"/>
        <daml:hasValue rdf:resource="#true"/>
        <daml:toClass rdf:resource=
              "&IntrOnt;DoS"/>
      </daml:Restriction>
    </rdfs:subClassOf>
    <rdfs:subClassOf>
      <daml:Restriction>
        <daml:onProperty rdf:resource=
                "&IntrOnt;est_connections"/>
          <daml:hasValue rdf:resource=
                "#IP_Address"/>
          <daml:toClass rdf:resource=
                "&IntrOnt;TCP"/>
        </daml:Restriction>
    </rdfs:subClassOf>
</daml:Class>
```

Qualitative Risk Analysis

- Assets – costs – attacks – countermeasures
- Risk: *Likelihood * impact*

- Example: Physical security
  - Company building
  - Valuable assets
  - Theft, fire, power loss etc.

  - *What to protect and how?*



Risk Analysis Ontology

- Handles the problems with:
- Large information sets
- Gaps between roles
  - Information security professionals, physical security staff, economy experts…
- Security threats vs. other threats
- Business focus

Malicious Software (Malware)

- Viruses, worms, Trojan horses
  - Shares features between types
  - Varies depending on the platform
- Anti-malware protection
  - Requires resources
  - Not suitable for resource constrained systems
- *What about mobile phone malware?*

Malware Ontology

- Defines malware depending on features
  - Suitable for hybrid malware
  - Adapted to mobile applications
- Fast processing in mobile devices
- Combined with a checklist for mobile users

Why Security Ontologies?

- *How can ontologies be useful in the information security field?*

- Creating a common terminology between groups
- Helpful in analysis of complex scenarios
- Part of the actual data processing

- Separate ontologies for different security fields or one large security ontology?

Summary

- Why ontologies are used in security
- Ontologies for:
  - Mobile malware
  - Web service security
  - Intrusion detection
  - Risk analysis

References

- ”*Security Attack Ontology for Web Services*” (2006), A. Vorobiev and J. Han
- ”*Modeling Computer Attacks: An Ontology for Intrusion Detection*” (2003), J. Undercoffer, A. Joshi and J. Pinkston
- “*Mobile Malware Behavioral Analysis and Preventive Strategy Using Ontology*” (2010), H-S. Chiang and W-J. Tsaur
- “*Security Ontologies: Improving Quantitative Risk Analysis*” (2007), A. Ekelhart, S. Fenz, M. Klemen and E. Weippl
- “*An ontology of information security*” (2007), A. Herzog, N. Shahmehri and C. Duma

Thank you!

Any questions?