Ľuboš Mjachky

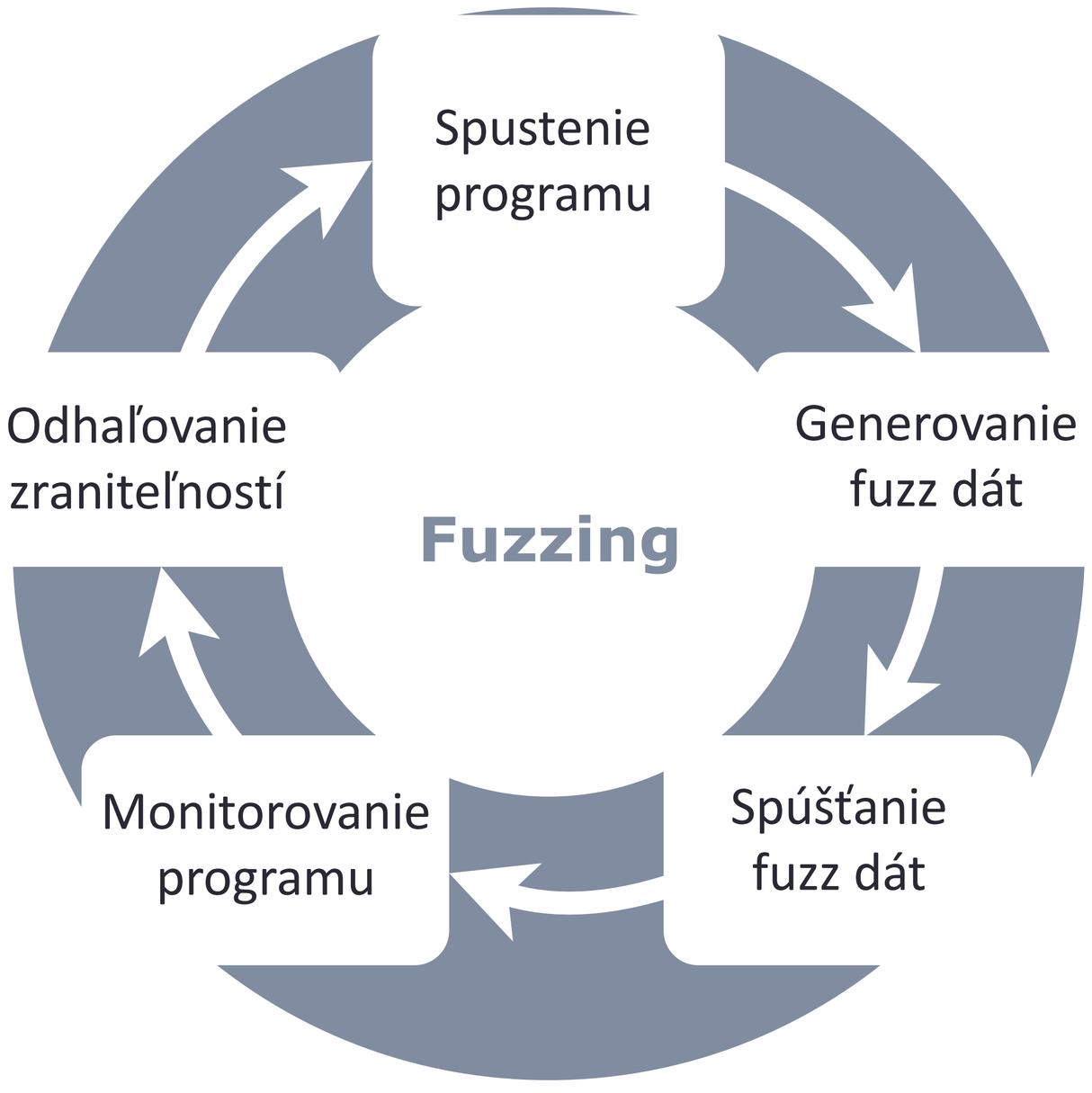
Excel@FIT 2018

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Fuzz testovanie aplikácií komunikujúcich prostredníctvom OData protokolu

Fuzz Testovanie

Fuzz testovanie alebo **fuzzing** môžeme definovať ako automatizovanú techniku testovania softvéru, ktorá používa **neplatné** alebo **náhodné** dáta (fuzz dáta) ako vstup, za účelom odhalenia zraniteľností a chýb.



OData Protokol

OData protokol je webový protokol postavený na HTTP a metodológiách REST (GET, POST, PUT, DELETE, MERGE). Podporuje **dopytovanie** sa na dáta, ktoré sú uložené na vzdialenom serveri, ich **filtrovanie** a **modifikovanie**. Štruktúra dát je definovaná v **dokumente metadát**. Pomocou dokumentu metadát je klientska aplikácia schopná identifikovať typy entít, vlastnosti asociácií či atribútov.

```
<EntityType Name=”Order”>
  <Key>
    <PropertyRef Name=”OrderID”/>
  </Key>
  <Property Name=”OrderID” Type=”Edm.Int32”/>
  <Property Name=”Subtotal” Type=”Edm.Decimal”
    Nullable=”true” Precision=”19” Scale=”4”/>
  <Property Name=”Details” Type=”Edm.String”
    Nullable=”true” MaxLength=”100”/>
</EntityType>
<EntityType Name=”Invoice”>
  <Key>
    <PropertyRef Name=”InvoiceID”/>
  </Key>
  <Property Name=”InvoiceID” Type=”Edm.Int32”
    sap:updatable=“false” sap:sortable="false“
    sap:filterable=“false”/>
</EntityType>
```

ODfuzz

ODfuzz je vyvinutý nástroj na **testovanie** aplikácií komunikujúcich prostredníctvom OData protokolu. Je naprogramovaný v jazyku Python a využíva **genetický algoritmus** na generovanie fuzz dát. Najskôr sa vytvorí počiatočná **populácia požiadaviek**. Tieto požiadavky sa odošlú a ohodnotia sa podľa odpovedi zo servera. Ak požiadavka spôsobí chybu, tým lepšie ohodnotenie získava. Nový jedinci sa do populácie pridávajú krížením a mutovaním existujúcich jedincov, a to výberom najlepšie ohodnotených požiadaviek z náhodného vzorku. Všetky dáta sa ukladajú do NoSQL databázy mongoDB. Výstup je možné vizualizovať a agregovať v kontingenčnej tabuľke.

SAP® mongoDB python™