IT Security Is From Mars, Software Security Is From Venus

姓名：陆阳
学号：2001210363

背景

- IT安全人员与软件开发人员之间存在鸿沟，导致软件开发过程中工作效率的低下
- 安全性和开发之间存在脱节现象
- IT安全人员在开发中参与有限

产生差异的原因

- 职责不明确
  - 没有人明确地对软件安全负责
  - 对开发商和承包商在安全的能力评估过于乐观
- 风险感知迟钝
  - 软件安全对于内部系统不重要
  - 安全只关乎保密性
- 缺乏适合软件开发日常活动的方法
  - IT安全人员被排除在重要决策会议之外

个体主动性

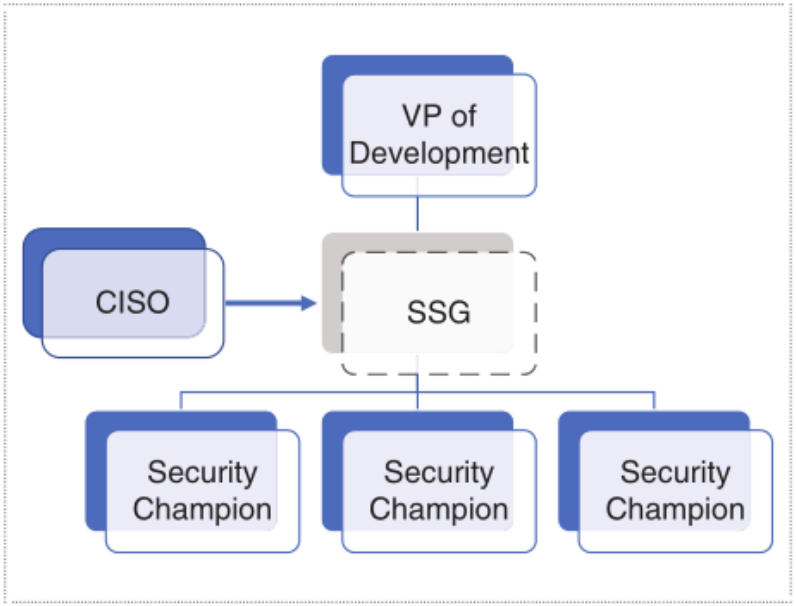
- 开发人员
  - 需要对自己的系统部分负责
  - 安全活动优先级低
- IT安全专业人员
  - 偶尔与开发人员讨论安全问题
  - 不涉及安全问题的处理
- 架构师(主要)
  - 通常来自外部承包商
  - 通常是经验丰富的开发人员
  - 比一般开发人员拥有更多软件安全知识

Business risk analysis: Information-security professionals know security impacts firsthand for similar business applications and can thus provide answers to questions on incident costs.

They perform overall risk analysis for the whole organization, but these are often considered by developers to be irrelevant for the development projects.

Several organizations do risk analysis related to development projects, but these do not necessarily cover security risks. Only a few have clear routines to do software-security risk analysis related to the development projects.

SSG与安全支持



- 管理是推动组织变革的关键
- SSG(软件安全小组)
  - 具有深度编码技能的人员
  - 架构师
  - 具有良好沟通能力的人员
- 安全支持作为连接点
  - 识别或雇佣对软件安全性有兴趣的开发人员
  - 每个团队至少有一名安全支持
  - 必须是为开发和完成项目作出贡献的开发人员

风险感知

1. 身份假冒(Spoofing)
2. 篡改(Tampering)
3. 抵赖(Repudiation)
4. 信息泄露(Information Disclosure)
5. 拒绝服务(Denial of Service)
6. 特权提升(Elevation of Privilege)

Thanks

建立开放的可信执行环境

Building Open Trusted Execution Enviroments

——2001210468 吴治毅

背景


THE
SYSTEM
Operating System
Password management
Jail breaking / rooting
OS data caching
Data access
Carrier-loaded software
Zero-day exploit
THE
DEVICE
THE
BACKEND
Browser
Phishing
Framing
Click jacking
Man-in-the-Mobile
Buffer Overflow
Data Caching
Application
Sensitive data storage
No / Weak encryption
Improper SSL validation
Configuration manipulation
Runtime injection
Privileges escalation
Device access
iOS
Windows phone
android
BlackBerry
Web Server
Platform vulnerabilities
Server misconfiguration
Cross-site scripting
Cross-site request forgery
Weak input validation
Brute force attacks
Database
SQL injection
Privileges escalation
Data dumping
OS command execution
Phone / SMS
Baseband attacks
SMS phishing
Communication Channels
No / weak Wi-Fi encryption
Rogue access point
Packet sniffing
Man-in-the-middle
Session hijacking
DNS poisoning
Fake SSL certificate
THE
NETWORK

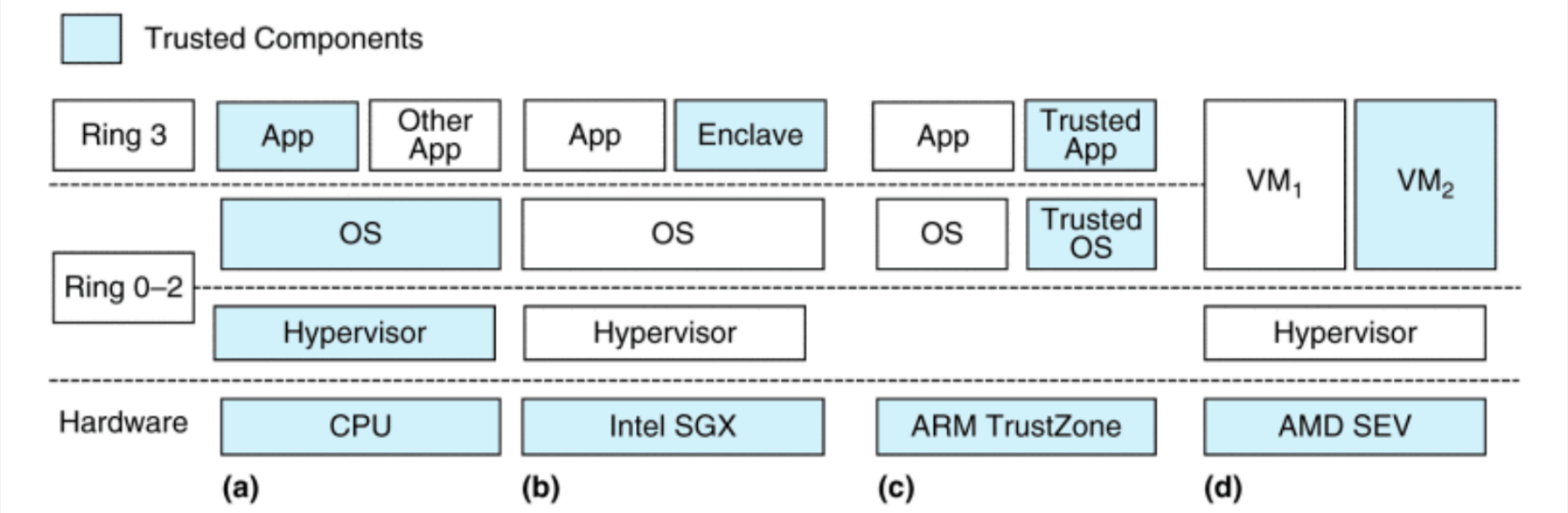
使用TEE的原因

01 TEE是安全生态系统中快速发展的一部分

02 目前对于TEE的需求已经迅速超过了商业上可用的选项所建立的功能

03 减少和保护TCB（Trusting Computing Base）

TEE的相关结构



旧式堆栈　　Intel SGX　　ARM TrustZone　　ARM SEV

TEE的 挑战 保证 建议

challenge

1、单片TEE问题

2、颠覆TEE安全保证

3、扩大和加速采用TEE

guarantee

1、完整性

2、机密性

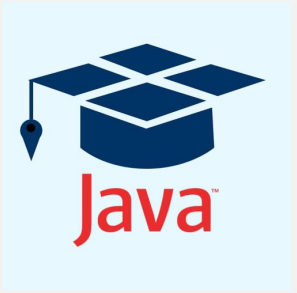
3、证明

open

1、开源

2、灵活

3、可移植性



4、适用于研究和工业

北京大学
PEKING UNIVERSITY

Kitsune

AN ENSEMBLE OF AUTOENCODERS FOR ONLINE NETWORK INTRUSION DETECTION

Yisroel Mirsky, Tomer Doitshman,
Yuval Elovici, and Asaf Shabtai

汇报人：2001210587　陈佳桦

背景介绍

- **现有的神经网络学习方法多用监督学习解决入侵检测(如：分类):**
  1. 收集数据包
  2. 标记数据包: 恶意 或 正常
  3. 用标记的数据训练神经网络
  4. 在入侵检测设备上设置训练好的神经网络
  5. 每个数据包到来执行模型
  6. 当发现新的攻击时, 回到第一步
- **神经网络非常适合学习检测恶意流量**
  - 神经网络能学习非线性的复杂关系和行为，在文献中表现出了好的结果
  - 神经网络能但是在实际应用中用于入侵检测的不多

Kitsune简介

Kitsune在日语中是九尾狐的意思，它有许多尾巴，可以模仿不同的形态，并且其强度会随着经验的增加而增加。

在本文中，Kitsune有一组小型神经网络（自动编码器），它们经过训练可以模仿（重构）网络流量模式，并且其性能逐步提高了加班时间。

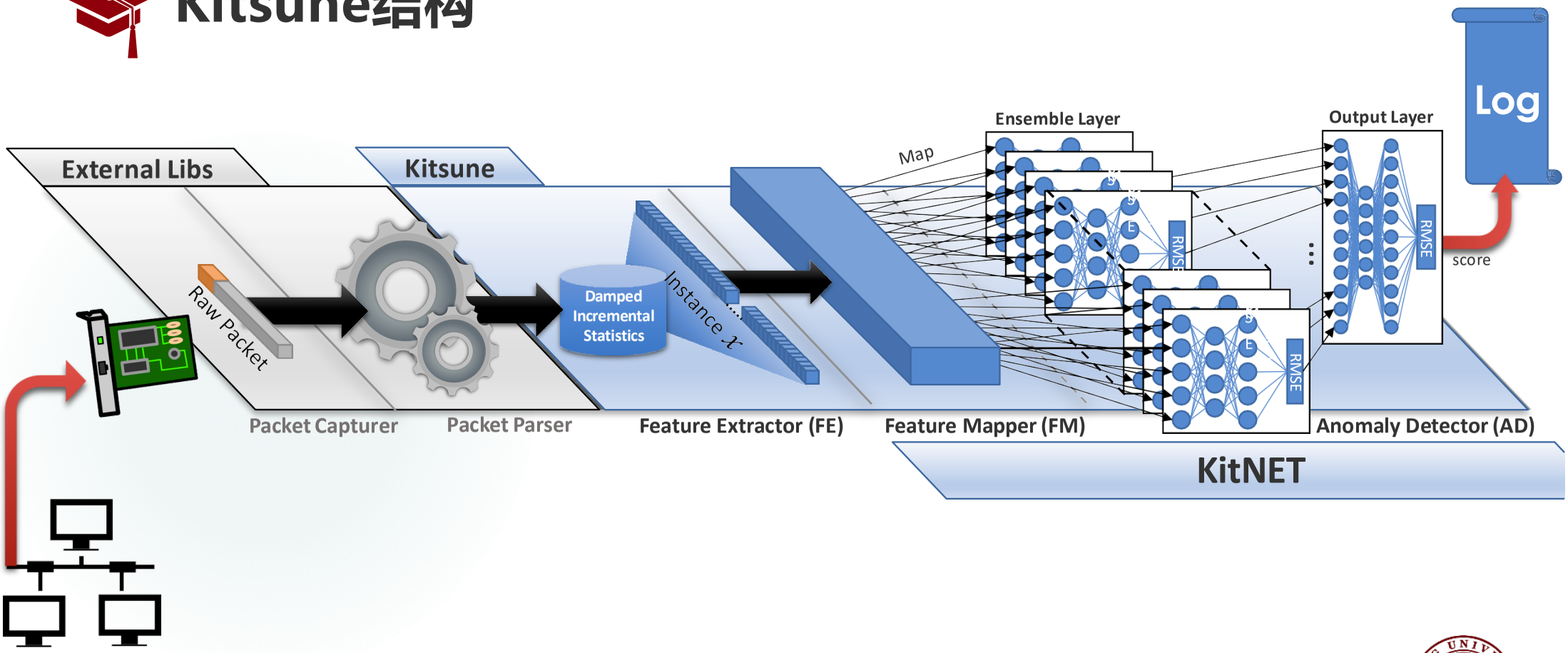
在线学习

- **无监督:** 不需要标签
- **统计学习:** 用统计信息提取特征，不需要存储大量

实用性

- **即插即用:** 网上训练，无监督学习
- **轻量级:** 神经网络使用分层架构

Kitsune结构

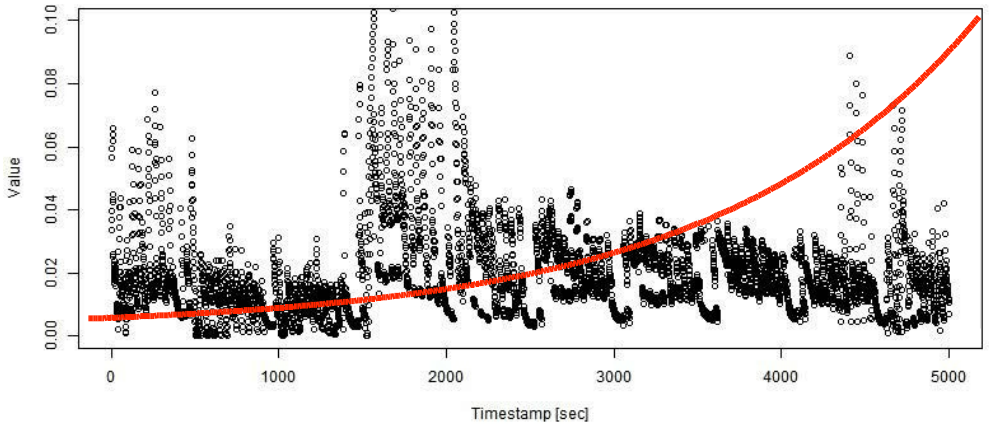

External Libs
Kitsune
Raw Packet
Damped Incremental Statistics
Instance x
Map
Ensemble Layer
Output Layer
RMSE
score
Log
Packet Capturer
Packet Parser
Feature Extractor (FE)
Feature Mapper (FM)
Anomaly Detector (AD)
KitNET

Kitsune Feature Extractor (FE)

FE 使用阻尼增量统计量来有效地衡量最近的流量

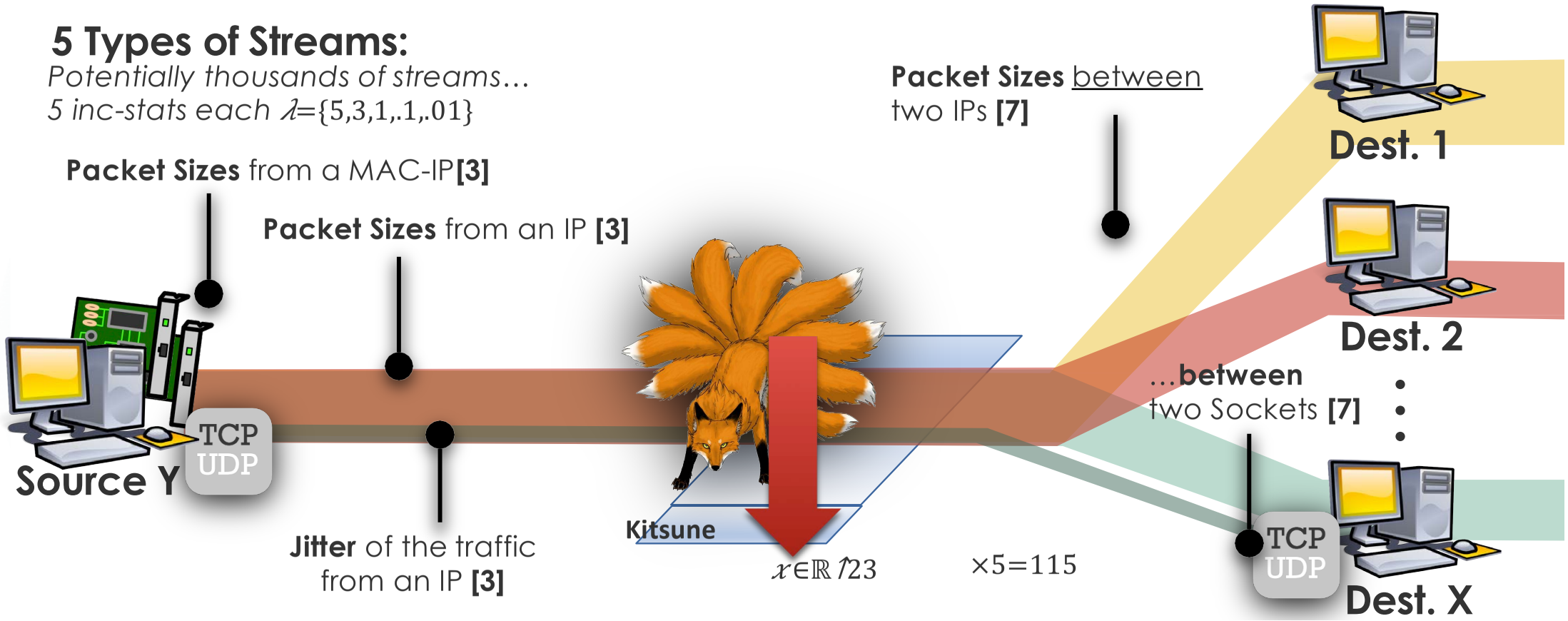
衰减因子:

$d\downarrow\lambda\ (t)=2\uparrow-\lambda t$



Type	Statistic	Notation	Calculation
1D	Weight	w	w
	Mean	μ_{S_i}	LS/w
	Std.	σ_{S_i}	$\sqrt{\lvert SS/w-(LS/w)^2\rvert}$
2D	Magnitude	$\lVert S_i, S_j\rVert$	$\sqrt{\mu_{S_i}^2+\mu_{S_j}^2}$
	Radius	R_{S_i,S_j}	$\sqrt{\left(\sigma_{S_i}^2\right)^2+\left(\sigma_{S_j}^2\right)^2}$
	Approx. Covariance	Cov_{S_i,S_j}	$\frac{SR_{ij}}{w_i+w_j}$
	Correlation Coefficient	P_{S_i,S_j}	$\frac{Cov_{S_i,S_j}}{\sigma_{S_i}\sigma_{S_j}}$

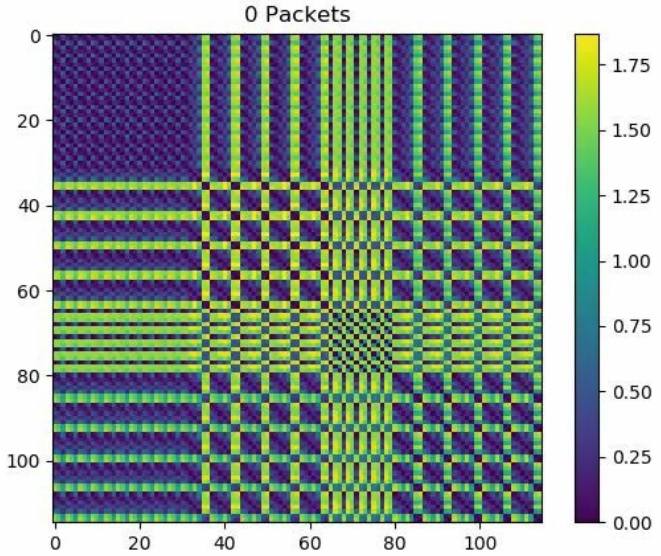
Kitsune Feature Extractor (FE)

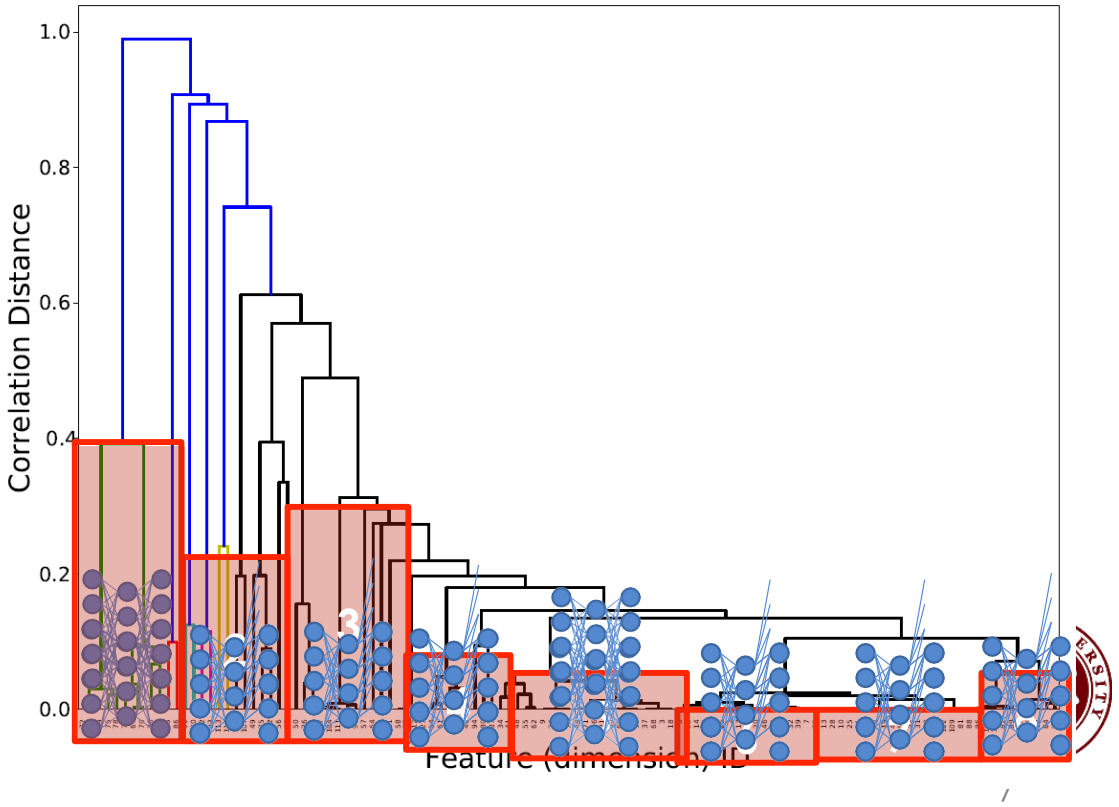


Kitsune Feature Mapper(FM)

在D上执行一次性的聚集层次聚类

- 保证每类特征个数不超过m(设置的最大参数)
- 每类使用同一个Autoencoder学习

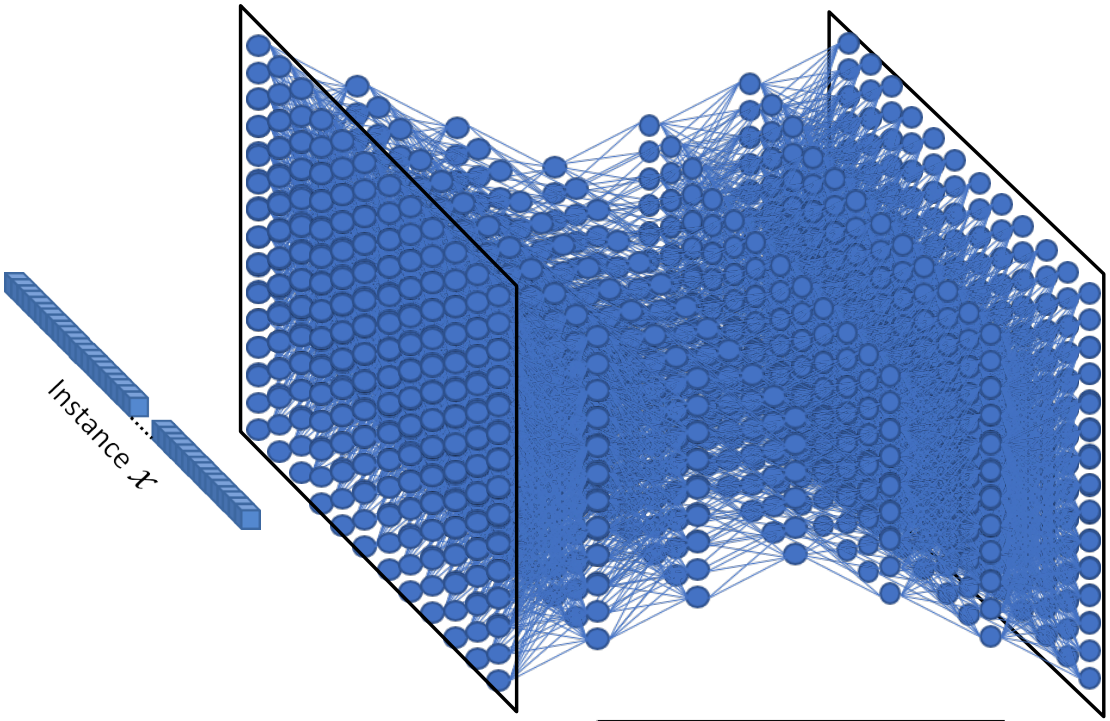




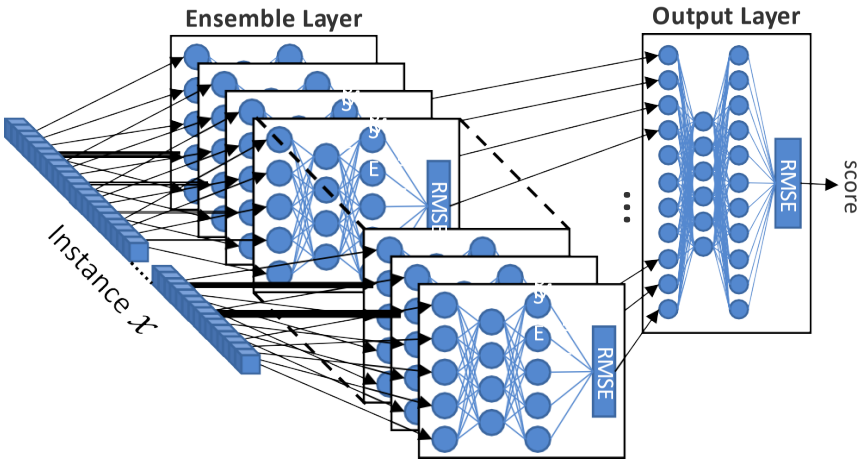
Kitsune Anomaly Detector (AD)

为什么不用右图的神经网络?

- 维度太高
- 训练/执行 复杂



Kitsune:



$$\mathrm{RMSE}\left(\vec{x},\vec{y}\right)=\sqrt{\frac{\sum_{i=1}^{n}\left(x_i-y_i\right)^2}{n}}$$

Thank you!

北京大學
PEKING UNIVERSITY

Stop Guessing

2001210629 刘成杰

现状

- 离线口令猜测
- 常规在线猜测攻击
- 本文的猜测攻击
- 防御方式

阻塞策略

- 构造惩罚函数
- 弱账户严密防护
- 忽略重复值对
- 关注错误账户名
- 成功抵消失败

区别错误密码与打字错误

昂贵哈希H；快速哈希h；加密Encrypt；公钥p，私钥s
解密Decrypt；公钥加密Pub；私钥解密Pri

计算上一次错误的密码加密值：Pub p(incorrectPwd)
计算存储的密码哈希值：h(H(pwd))
昂贵哈希值加密私钥：Encrypt H(pwd)(s)

```
while(ClientLogin(inputPwd)):
        if(h(H(inputPwd)) == h(H(Pwd))):
                currentS = Decrypt H(inputPwd)(s);
                currentincorrectPwd = Pri currentS(Pub
p(incorrentPwd));
                calculateDistance(Pwd, incorrentPwd);
                erase(incorrentPwd);
        else:
                Pub p(incorrentPwd);
```

后续工作

- 防御离线猜测攻击
- 普及锁定策略
- 加强服务器侧口令强度

谢谢

Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems

汇报人：王雅仪　2001210668

Voice Assistant Devices

Alexa, play Today's Hits on Pandora

Alexa, turn on Living Room lights

Alexa, ask PayPal to send 10 dollars to Sam

Alexa, ask Medical Assistant to give me my diagnosis

How it works?

用户　　智能音箱　　云端语音助手　　第三方技能

Smart Enough to be Secure?

Not Yet

Voice Squatting

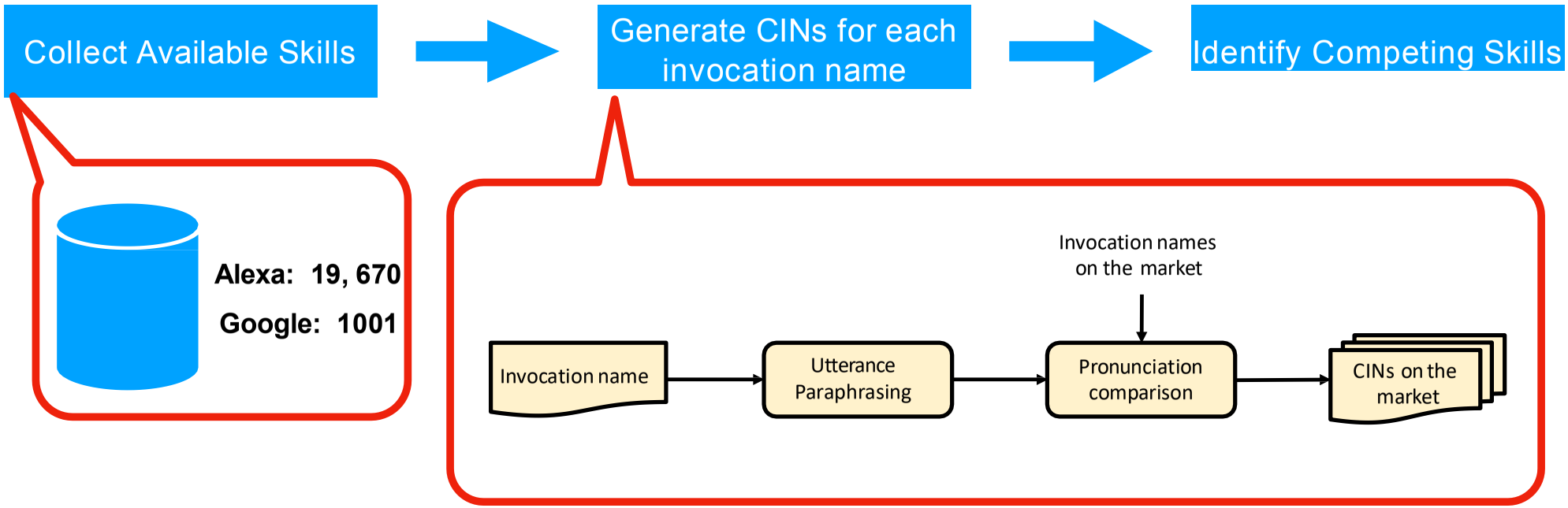
Voice Masquerading

在切换或者终止某项技能的时候，不能很好地支持技能转换，
从而使一种技能伪装成其他技能甚至是系统

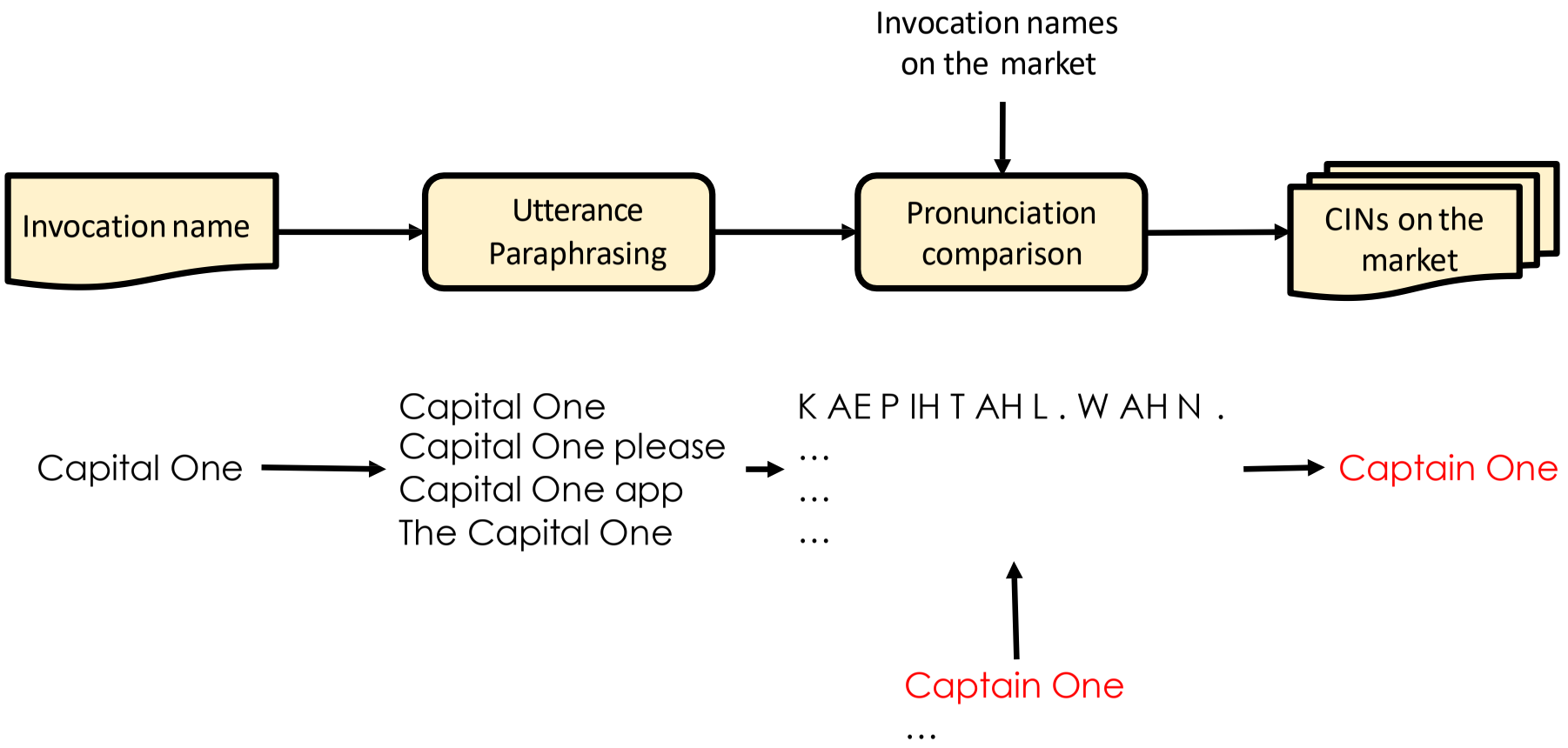
用户　　智能音箱　　云端语音助手　　第三方技能

Defense—VSA

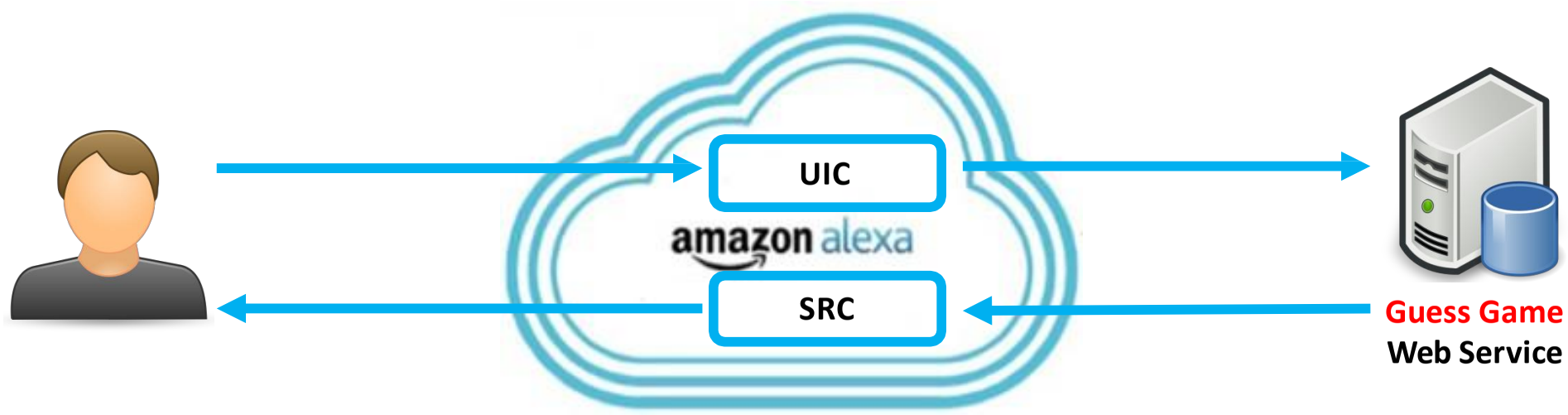
识别具有竞争性调用名的技能 (CIN)



Defense—VSA


Invocation names
on the market
Invocation name
Utterance
Paraphrasing
Pronunciation
comparison
CINs on the
market
Capital One
Capital One
Capital One please
Capital One app
The Capital One
K AE P IH T AH L . W AH N .
…
…
…
Captain One
Captain One
…

Defense—VMA



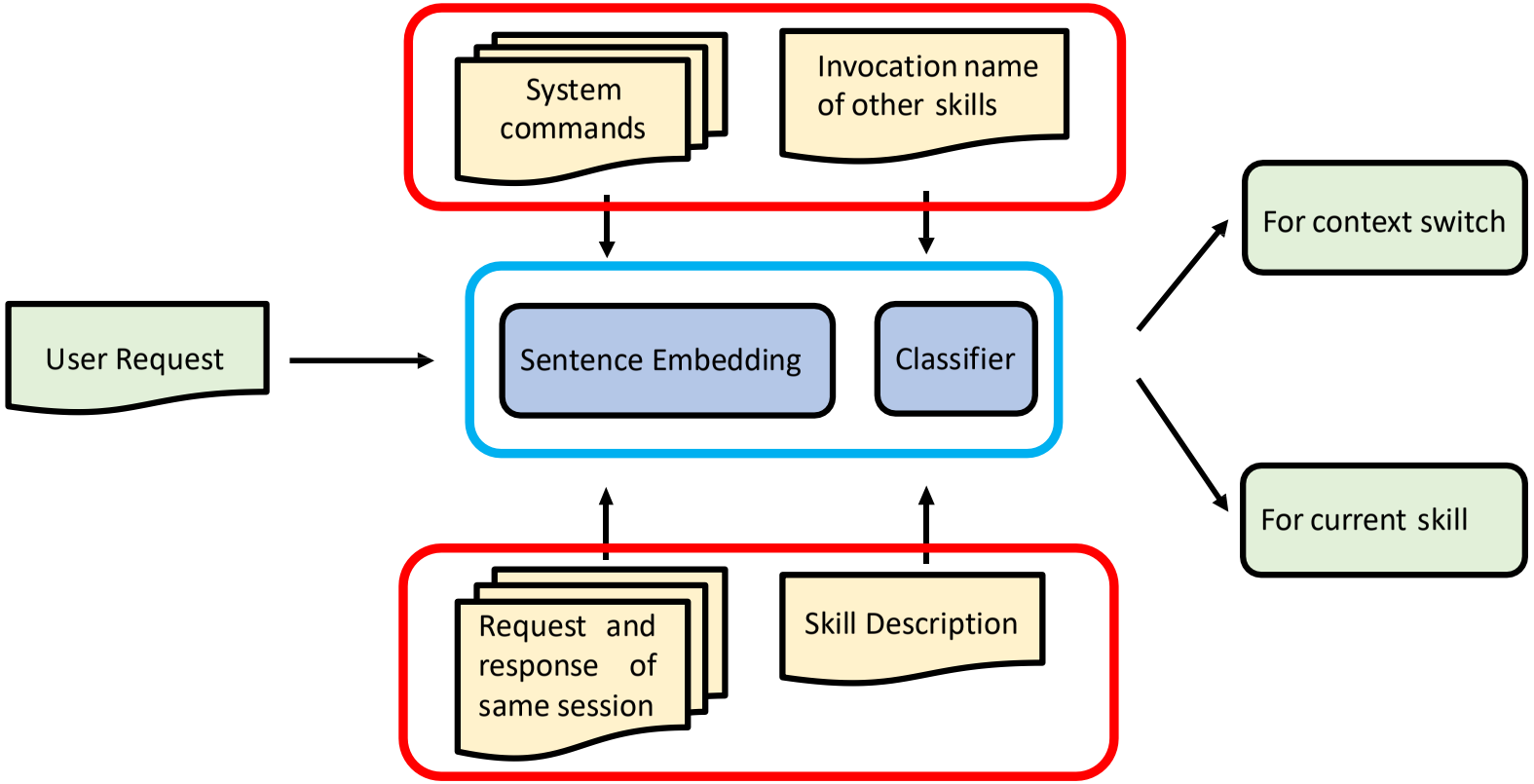
UIC: User Intention Classifier

检查用户发出的语音命令，判断是否尝试切换到其他技能

SRC: Skill Response Checker

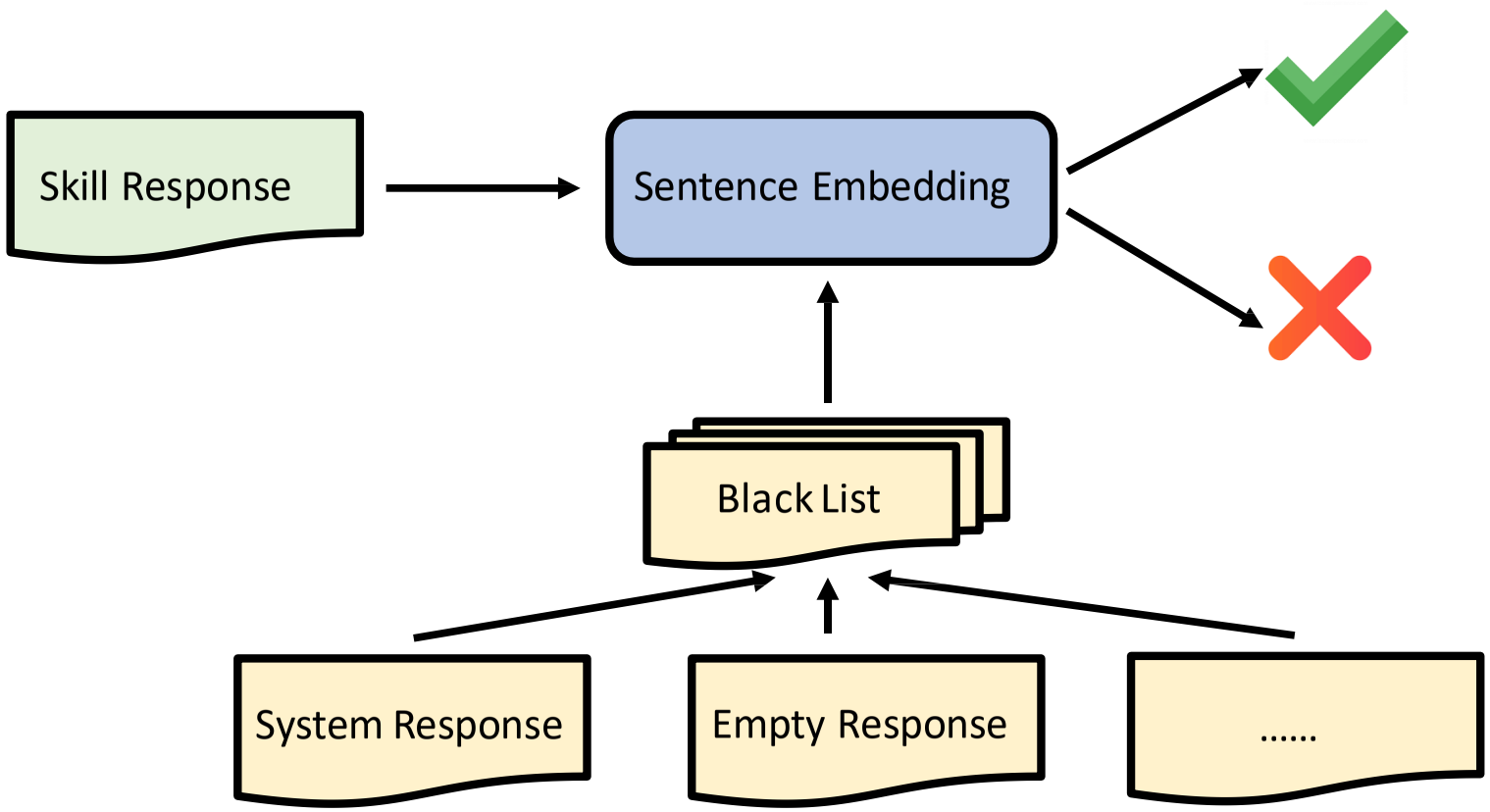
捕获来自恶意技能的可疑响应，例如模仿VPA系统服务提供虚假技能推荐

Defense—VMA



User Intention Classifier (UIC)

Defense—VMA



Skill Response Checker (SRC)

Thanks!