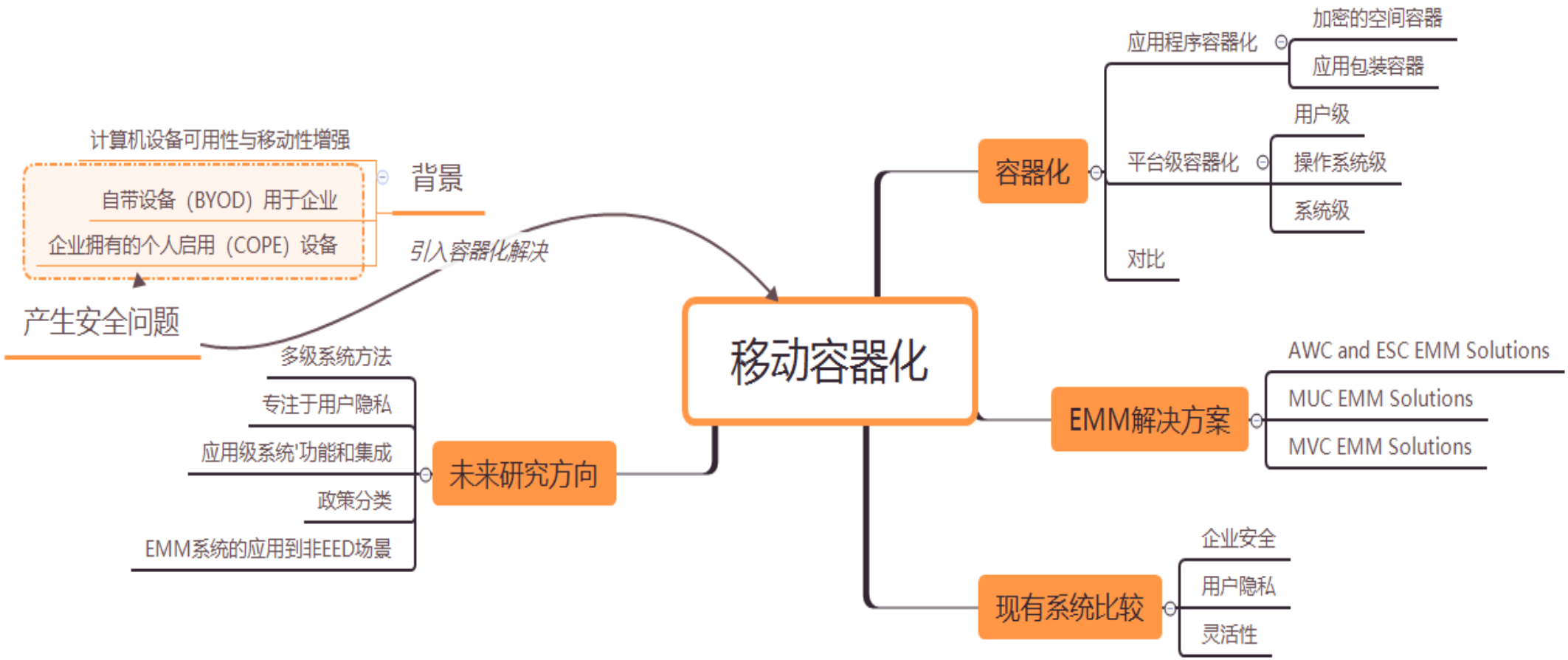
Moving Forward

郭知娇 刘亚楠 许泽昊 黄瑞瑶

移动设备容器化

Overview of Mobile Containerization Approaches and Open Research Directions

郭知娇 1801210826


移动容器化
背景
计算机设备可用性与移动性增强
自带设备（BYOD）用于企业
企业拥有的个人启用（COPE）设备
产生安全问题
引入容器化解决
容器化
应用程序容器化
加密的空间容器
应用包装容器
平台级容器化
用户级
操作系统级
系统级
对比
EMM解决方案
AWC and ESC EMM Solutions
MUC EMM Solutions
MVC EMM Solutions
现有系统比较
企业安全
用户隐私
灵活性
未来研究方向
多级系统方法
专注于用户隐私
应用级系统'功能和集成
政策分类
EMM系统的应用到非EED场景

产生背景

- 计算机设备可用性与移动性日益增强
- 个人设备用于工作-**BYOD**
- bring-your-own device
- 企业设备个人使用-**COPE**
- corporate-owned, personally enabled device
- **企业启用设备（EED）**enterprise-enabled device

EED优势劣势

- 使得员工可以远程访问企业内容
- 设备的双重使用带来了安全和隐私风险。

如何解决以上问题？

- 需要寻求一种用于保护企业数据安全性和用户数据隐私的有效方法，从而确保企业数据和员工的数据彼此完全隔离
- 如何对移动设备进行有效的管理？
- 区分设备？——浪费、操作繁琐、可用性差
- 从设备内部入手进行隔离？

容器化与EMM（Enterprise Mobility Management ）

- **主要目标：**保护企业资源，确保企业数据和员工的数据彼此完全隔离
- **容器化**：一种用于保护企业数据安全性和用户数据隐私的技术，并不直接提供控制或管理容器
- **EMM**：企业移动性管理系统，使企业能够部署，控制，管理和授予或拒绝保护容器的权限
- **主要方式：**通过在**应用程序，平台或硬件**级别或利用云技术与安全技术结合实现（包括身份验证，数据隔离，环境隔离和加密）

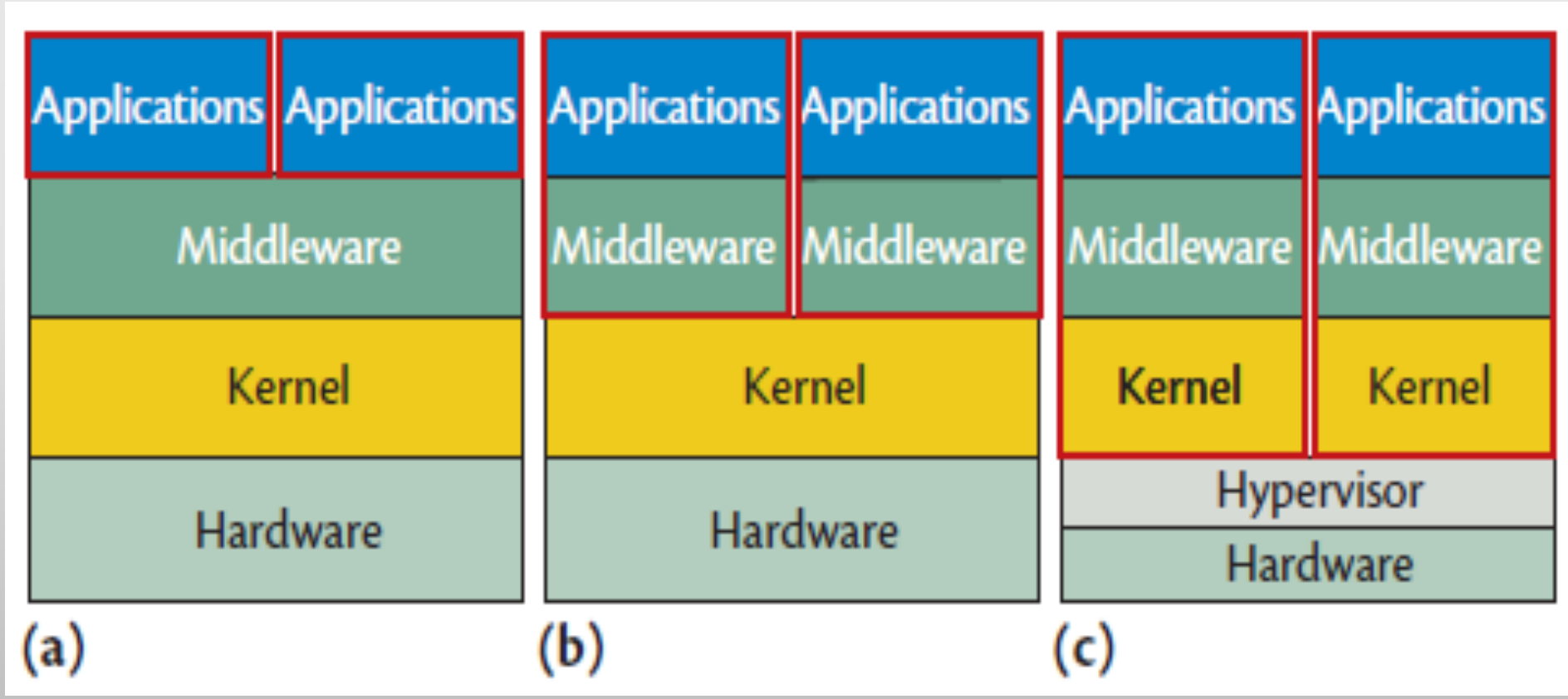
应用程序级容器化

- 以应用程序为中心的方法，涉及用户设备具有一个环境，其中可信和不可信应用程序并排运行
- 加密空间容器（ESC）和应用程序包装容器（AWC）
- ESC技术创建一个单独的加密空间，通常称为气泡，用于托管敏感内容，包括企业应用程序和数据
- AWC技术通过将每个应用程序封装在自己的加密容器中来隔离应用程序级别的企业应用程序和数据。

平台级容器化

- 平台级容器化在数据管理中提供比其对应部分更高的粒度，包括在用户，操作系统和系统级别实现的技术
- 多用户容器（MUC）和移动虚拟化容器（MVC）
- 每个用户都有自己的帐户，应用程序，系统设置，文件和任何其他用户关联数据
- 虚拟化将计算平台上的指定实体设备资源多路复用到一个或多个执行环境中，或者在移动设备下将移动虚拟平台（MVP）复用

平台级容器化


Applications
Applications
Middleware
Kernel
Hardware
(a)
Applications
Applications
Middleware
Middleware
Kernel
Hardware
(b)
Applications
Applications
Middleware
Middleware
Kernel
Kernel
Hypervisor
Hardware
(c)

未来研究方向

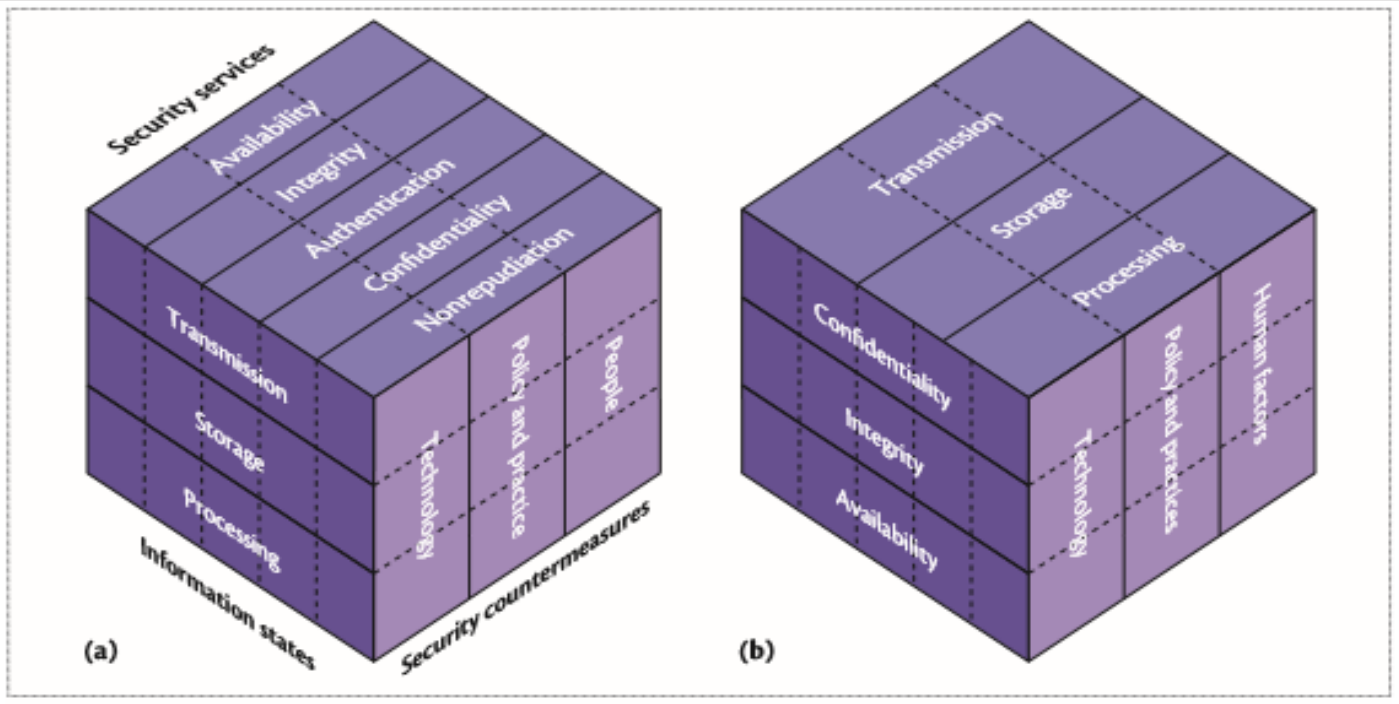
- 多级系统方法
- 专注于用户隐私
- 应用级系统功能和集成
- 政策分类
- EMM系统的应用到非EED场景

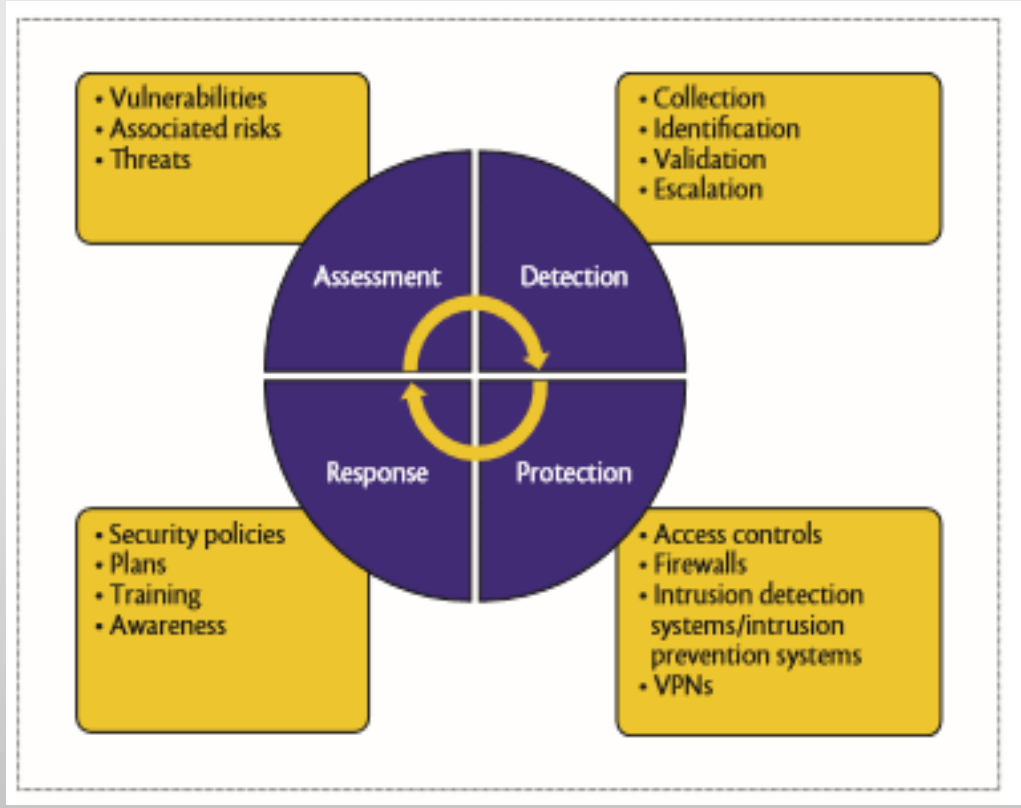
认证政策和认证标准下的安全开发生命周期

The Security Development Lifecycle in the Context of Accreditation Policies and Standards

刘亚楠 1801210591

McCumber立方体模型是第一个正式建立并评估信息安全的模型.它通过合并政策，教育和技术将信息安全理论与实际实现相结合。由于信息必须是安全的，因此该安全模型还承认信息的三个基本状态：存储，处理和传输。 而由于安全从业者不断增长的需求，McCumber立方体模型被扩展到了包括信息安全保障（IA）的可用性，完整性，机密性和身份验证和不可否认性方面。





SecDLC的目标是：维持，保存，监控和改进信息安全的实践，策略和标准。信息安全是保护信息免受未经授权的访问，使用，披露，破坏，修改，检查的做法。一般而言，信息安全保障寻求保护数据的三个重要属性：机密性，完整性和可用性 - 通常称为“CIA三角形”。SecDLC周期如下：

- ■评估
- ■检测
- ■保护
- ■回应

现有的信息安全模型。虽然这些模型提供了类似的实现程序和信息安全管理程序，但它们并未完全实现四个SecDLC阶段。生命周期管理记录与安全相关的决策，并确保管理在所有阶段都要充分考虑安全性。系统管理员可以使用这些信息来提醒他们为什么做出某些决定，从而更容易评估环境变化的影响。

NIST 800-64模型的主要阶段包括：

■启动。在启动期间，考虑了功能和集成方面的威胁，要求和潜在限制。
■获得。此阶段主要用于风险评估，安全要求分析，安全认证和资格认证，以及完整的安全架构设计。
■实现。在组织的运营环境中安装和评估信息系统。
■操作和维护。随着系统的到位和操作，系统的增强和修改被开发和测试，并且添加或替换硬件和软件。
■处理。与信息和系统处置相关的信息安全问题得到明确解决。

微软安全开发生命周期模型主要阶段包括：

■要求。产品团队与安全团队协商，并接收建议和计划审核以及最佳计划策略。
■设计。此阶段确定了软件的总体要求和结构。
■实施。此阶段的主要目标是减少安全漏洞。
■验证。该产品在此阶段进行了beta测试。
■发布。最终的软件产品将全面检查所有安全合规性 - 所谓的FSR或最终安全审查 - 从而确保向客户提供优质产品。

Table 1. Comparison of the NIST and Microsoft security lifecycle models according to the four security development lifecycle (SecDLC) phases.

SecDLC phase	NIST	Microsoft
Assessment	Yes	Yes
Detection	No	No
Response	No	Yes
Protection	No	No

根据SecDLC框架的四个阶段对NIST和Microsoft的模型进行了比较。如此比较显示，当前模型不关注检测和保护阶段。但是，这些阶段包括必须实施的关键子功能，以便在初始评估之后和最终响应或验证阶段之前实现有效的安全生命周期。

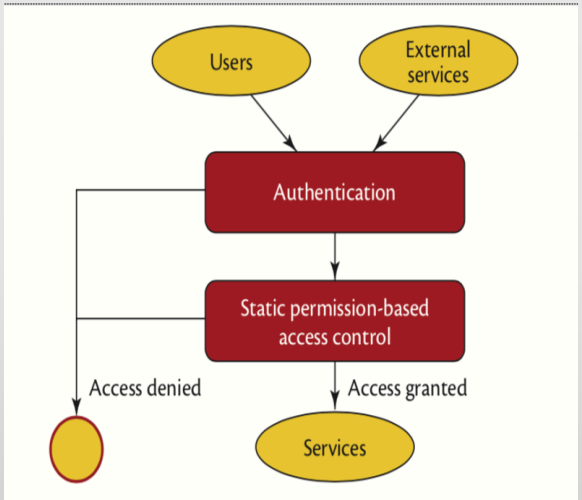
网络系统安全机制的实践评价

Practical Evaluation of Internet Systems' Security Mechanisms

许泽昊 1801210904

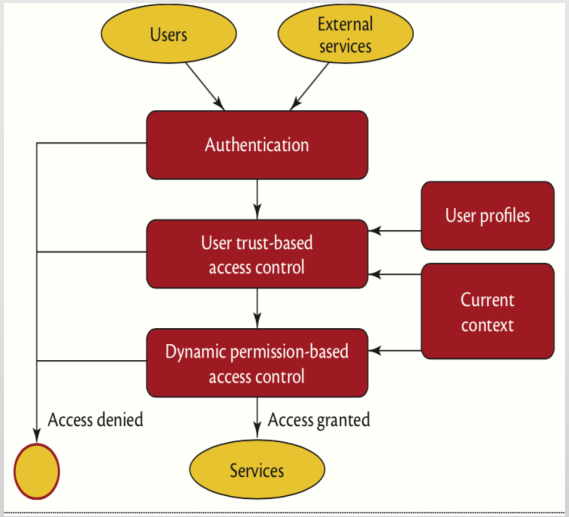
CoRBAC 和 RBAC

RBAC
（基于角色的访问控制）



现在传统的RBAC安全方法是静态的，在快速变化的领域中不灵活。首先，执行认证过程。接下来，根据用户的连接，角色，角色的权限以及保护服务的权限，根据权限配置执行权限验证。

CoRBAC
（面向环境的基于角色的访问控制）



面向环境的基于角色的访问控制则被认为是创建动态和灵活的访问控制机制。为了满足不同的需求的用户，该方法增加了额外的属性。他是RBAC模型的拓展，广泛清楚的背景被考虑在内。 与RBAC相比，增加了用户信任的访问控制，并且考虑了当前环境和用户资料。

STL（系统信任级别分数）

Table 2. Detected vulnerabilities in GUT Instinct system and their risk score.*

ID	Detected vulnerability	System with role-based access control (RBAC)			System with context-oriented role-based access control (CoRBAC)		
		CVSS v2 vector	Score**		CVSS v2 vector	Score**	
v1	Cross-site scripting—vulnerability 1	(AV:N/AC:M/Au:S/C:C/I:C/A:N)	7.9	H	(AV:N/AC:M/Au:S/C:P/I:P/A:N)	4.9	M
v2	Cross-site scripting—vulnerability 2	(AV:N/AC:L/Au:S/C:P/I:P/A:N)	5.5	M	(AV:A/AC:L/Au:S/C:P/I:P/A:N)	4.1	M
v3	Cross-site scripting—vulnerability 3	(AV:N/AC:L/Au:N/C:P/I:P/A:N)	6.4	M	(AV:N/AC:L/Au:N/C:N/I:P/A:N)	5.0	M
v4	Cross-site scripting—vulnerability 4	(AV:N/AC:M/Au:S/C:C/I:C/A:N)	7.9	H	(AV:A/AC:M/Au:S/C:P/I:P/A:N)	3.8	L
v5	SQL injection—vulnerability 1	(AV:N/AC:H/Au:S/C:C/I:C/A:C)	7.1	H	(AV:A/AC:H/Au:S/C:C/I:C/A:C)	6.5	M
v6	SQL injection—vulnerability 2	(AV:N/AC:H/Au:S/C:C/I:C/A:C)	7.1	H	(AV:A/AC:H/Au:S/C:C/I:C/A:C)	6.5	M
v7	SQL injection—vulnerability 3	(AV:N/AC:H/Au:S/C:C/I:C/A:C)	7.1	H	(AV:A/AC:H/Au:S/C:C/I:C/A:C)	6.5	M
v8	Cross-site request forgery (CSRF)—vulnerability 1	(AV:N/AC:M/Au:S/C:N/I:P/A:N)	3.5	L	(AV:N/AC:M/Au:S/C:N/I:P/A:N)	3.5	L
v9	CSRF—vulnerability 2	(AV:N/AC:M/Au:S/C:N/I:C/A:N)	6.3	M	(AV:A/AC:M/Au:S/C:N/I:P/A:N)	2.3	L
v10	Session ID—vulnerability 1	(AV:N/AC:H/Au:S/C:C/I:C/A:N)	6.6	M	(AV:N/AC:H/Au:S/C:P/I:P/A:N)	3.6	L
v11	Session ID—vulnerability 2	(AV:N/AC:H/Au:S/C:C/I:C/A:N)	6.6	M	(AV:A/AC:H/Au:S/C:C/I:C/A:N)	5.9	M
v12	Password reset procedure	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0	M	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0	M

文中举例一个系统，左边是使用RBAC安全机制，右边使用的是CoRBAC安全机制，通过CVSS计算器计算系统STL得分，左边得分0.9909，右边0.9928，一个安全系统的得分趋近于1。

STL计算公式为如下，其中Z L M H分别代表不同情况的漏洞。

$$STL = \frac{nZ + nL + 0.6 + nM + 0.3 + nH + 0.1}{nT},$$

驾驶习惯数据：位置隐私问题与解决方案

Driving Habits Data :

Location Privacy Implications and Solutions

黄瑞瑶 1801210835

问题背景

- 车辆保险公司推出驾驶习惯分析项目。

  项目中使用车载传感器采集用户驾驶行为数据，并给予项目参与者保险折扣优惠。
- 对于项目发起者（保险公司）：

  可以根据数据分析结果，对每一个用户设定具有针对性的定价。
- 对于项目参与者（驾车用户）：

  获得优惠，在分析结果的指导下改善自己的驾驶习惯。

核心问题

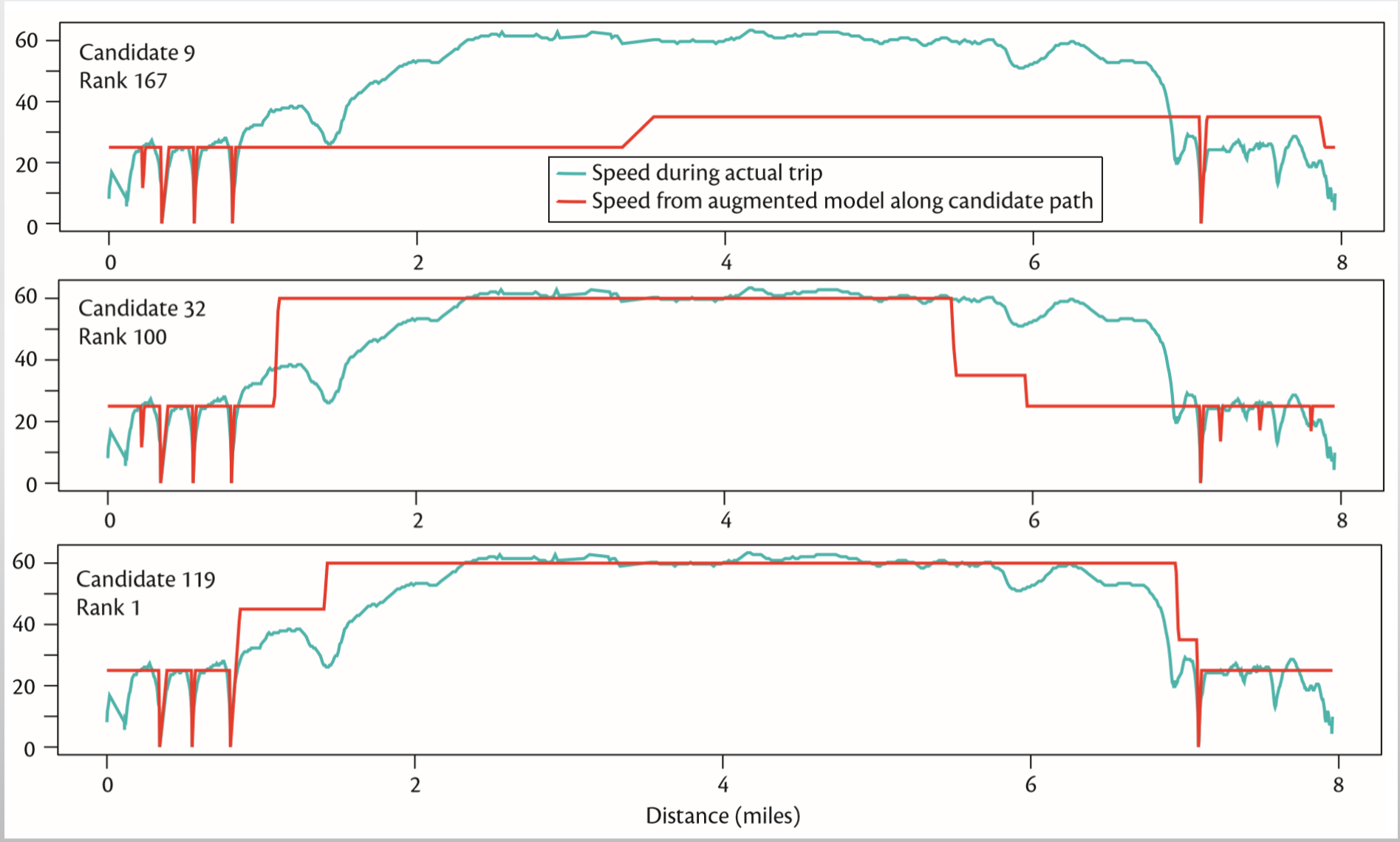
1. 项目发起者采集的数据是否会侵犯用户的位置隐私？
2. 项目发起者是否可以在不侵犯用户位置隐私的情况下完成用户驾驶习惯的分析？

实验验证 – 数据采集

1. 实验路线：
   路线场景：工作路线，购物路线，旅行路线等。
   路线长度：单次旅程距离1~25英里不等。
   覆盖道路：洲际高速公路，城市公路，住宅区道路。
2. **数据类型**：
   原始数据GPS,
   实际使用行驶路程(d)，行驶时间(t)，行驶速度(s)
3. 采集设备：
   每秒采集一次原始数据

实验验证 – 实验步骤

1. 依据地图构建图
   设置节点，边，边的长度，边的限速。
2. 清洗数据
   去掉部分受交通状态（例：交通拥堵）影响的点
3. 生成候选路径
   使用DFS，根据限制条件（例：转弯速度限制）生成候选路径
4. **对候选路径打分排序**
   计算速度的条件概率的对数和。


Candidate 9
Rank 167
Speed during actual trip
Speed from augmented model along candidate path
Candidate 32
Rank 100
Candidate 119
Rank 1
60
40
20
0
0
2
4
6
8
Distance (miles)

实验结果

1. 30次行驶过程中有18次成功，18次成功结果中，有16次排名前三的候选路径中包括实际行驶路径。
2. 针对每个数据点平均计算耗时88ms。

项目发起者采集的数据有很大的可能性会侵犯用户的位置隐私。

在不侵犯用户隐私的条件下，分析用户驾驶习惯的方法是存在的。