《智能网络与计算》期末大报告

2023-2024 学年第一学期

论文 ID：3

英文题目：Exploiting Contactless Side Channels in Wireless Charging Power Banks for User Privacy Inference via Few-shot Learning

中文翻译：基于无线充电宝中的非接触侧信道和小样本学习进行用户隐私推断

姓　　名：张嘉豪

学　　号：2021152005

撰写时间：2024 年 1 月 8 日至 2024 年 1 月 13 日

撰写须知：

1. 请严格按照模板提供的一级大标题撰写报告，可根据需要可自行添加二级、三级小标题。不要更改报告格式、字体等，确保报告格式的统一性。
2. 报告格式统一规定如下：（1）正文部分中文字采用**楷体**、小四，西文字采用 **Times New Roman**；（2）标题采用宋体，各级标题的字号从小二依次递减；（3）正文行间距采用 **1.2 倍行距，**段前 0.25 倍行距，段后 0.25 倍行距。
3. 大报告的评分主要依据是：格式排版、报告内容、独立思考等。其中，报告内容主要从完整性、准确性和丰富性三个方面考察，独立思考则考察是否有对所读内容的批判性思考。**报告中必须包含对于论文中所涉及到的技术点进行展开论述与讲解**。报告尽可能做到图文并茂、内容充实、格式美观。
4. 报告提交时请转化成 **PDF 格式**，并按“paperID-姓名.pdf”方式命名。同时，请将论文 **PPT 一并提交**，PPT 命名方式与大报告命名方式保持一致。
5. 模板中灰色斜体字为报告撰写说明，在最终提交版中需要删除。
6. 除封面和参考文献以外，报告正文部分的页数不少于 20 页。
7. 报告提交的截止时间为：2024 年 1 月 7 日晚 23:59。

目录

摘　要

基于当代兴起的支持无线充电的移动电源，本文的研究者关注其在保护用户隐私方面可能存在的新问题，发现了一种新的非接触式无线充电侧信道，其可通过移动电源为智能手机进行无线充电时发出的线圈噪音和磁场干扰来泄露用户隐私，而不会危害移动电源或受害者智能手机的安全。基于这一发现，研究团队提出了一种名为 BankSnoop 的攻击框架，旨在演示这一无线充电侧信道的实用性。BankSnoop 利用了移动电源在为智能手机进行无线充电时所产生的线圈啸叫和磁场干扰这两种物理现象，并采用小样本学习来识别智能手机上运行的应用程序，并揭示按键输入。论文详细地阐述了物理现象的原理与攻击框架的设计，并通过使用普通的无线充电移动电源和智能手机从不同起始电量，不同行为等（多个数据集）进行测试，研究结果显示，BankSnoop 在识别应用程序启动和按键输入平均准确率上达到了 90%以上，并且应用于不同智能手机型号和移动电源时，BankSnoop 表现出很高的适应性，在 10 次学习的情况下准确率达到了 85%以上。这一无线充电侧信道的新发现对于用户隐私保护和无线充电移动电源的安全性具有非常重要的意义。同时也为未来无线充电技术的发展提供了有益的参考，强调了对新兴技术可能带来的隐私问题的关注。

1. 研究背景及意义

1.1研究背景与动机

如今，移动电源已经成为许多人在户外给智能手机充电的必备设备之一。各种公共场所，如咖啡馆和机场的充电宝租赁站数量都发生了巨大增长，其全球市场价值在 2022 年年中已超过 71 亿美元。而近年来，由于无线充电技术的日益普及，许多新发布的移动电源都开始支持无线充电，这些移动电源大多遵循不同移动操作系统的不同智能手机型号广泛支持的 Qi 无线充电标准。

然而，最近的研究揭示了 Qi 认证无线充电系统的安全漏洞，有关磁基侧信道攻击的研究也得到了发展。这些研究报道了无线充电或纯有线充电宝都可以从充电的智能手机中推断用户隐私，但其并没有引起足够的公众意识。而无线充电宝由于不需要 USB 线，能够根据电量动态调节电源，异构无线充电宝依赖于经过良好训练的模型等原因，被认为似乎能够克服隐私泄露问题。研究者于是针对无线充电宝与其相关的隐私泄露问题展开了研究。

1.2 研究意义

创新性意义：本论文通过发现并深入研究无线充电宝中的侧信道，揭示了一种全新的信息泄露途径。这一侧信道（无线充电时的所产生的物理现象）的发现

本身具有较大的创新性，其否定了无线充电宝不会泄露用户隐私这一观点，为科学界和工业界提供了对于无线充电技术的新认识。此外，通过提出 BankSnoop 攻击框架来说明其实用性，并解决了以前无线充电侧信道攻击中的限制。同时创新地采用了小样本学习技术，快速调整预训练的模型以适应新的攻击场景和环境，提高了 BankSnoop 的自适应能力，成功实现在使用无线充电宝为智能手机充电的场景下对智能手机应用程序和按键输入的准确识别。

实用性意义：移动电源无线充电已经成为人们生活中不可或缺的一部分，而近年来兴起的无线充电宝也逐渐走进了大众的视野，而本研究的成果直接关系到用户的隐私安全。通过 BankSnoop 方法，我们能够更全面地了解无线充电设备可能存在的隐私泄露问题，为制定相应的安全措施提供实质性支持。这对于用户隐私保护、企业产品改进以及行业规范制定都具有直接的实际应用意义。

前瞻性意义：本研究通过对未来移动电源无线充电技术可能带来的隐私问题的深入研究，提前揭示了这一新兴技术的潜在风险。这不仅对当前的无线充电设备提出了警示，同时也为未来的技术研发和安全性防范提供了启示。在技术不断迭代升级的情况下，对于可能的风险有所预见性，将有助于更加健康、安全地推进无线充电技术的发展。本论文提出的 BankSnoop 方法，有利于后续的研究者进行相关的研究，并采取措施来应对新兴技术所带来的安全隐患，为未来安全性研究提供了新的思路。

1.3 核心思想

论文的核心思想是使用新发现的无线充电宝的侧信道来进行用户隐私推断。基于该信道，论文提出了一种名为 BankSnoop 的攻击框架。该攻击框架通过利用移动电源在无线充电时产生的线圈噪音和磁场干扰来对智能手机应用程序和按键输入等用户行为进行识别，并通过采用小样本学习技术来提升其自适应能力。

1.4 本文贡献

新的侧信道攻击引入：论文提出了一种新的侧信道，利用移动电源在无线充电时产生的线圈噪音和感应磁场干扰，实现了对无线充电电源的非接触式攻击。这一发现为侧信道攻击提供了新的攻击手段，对相关研究领域带来了创新。

新的攻击框架 BankSnoop 的提出与实现：论文引入了一个新的攻击框架 BankSnoop，旨在证明新侧信道的可行性。该框架克服了以往无线充电侧信道攻击的限制，为评估和改进无线充电系统的安全性提供了一种新的工具。

磁侧信道攻击的可行性证明：论文通过对磁侧信道攻击的研究并提出 BankSnoop 攻击框架，证明了利用两种磁感应现象攻击无线充电宝的可行性。这一发现拓展了磁侧信道攻击的应用范围，为未来研究提供了新的方向。

2. 国内外研究现状

2.1无线充电宝

部分已有研究主要关注 Qi 协议认证的无线充电系统的安全性。这些研究揭示了 Qi 协议的安全漏洞。Cour 等人提出了一种基于网站指纹的攻击方法，通过分析电源线中的电流痕迹，实现对无线充电器的指纹识别攻击，这需要稳定的充电电压和智能手机高电池电量（例如>80%）[21]。Wu 等人则利用隐藏的线圈获取感应电流，劫持电池并识别应用活动[47]。此外，EM-Surfing 利用外部电阻的感应电压监测隐私泄露，例如应用程序使用和按键输入[24]。然而，这些先前工作存在的局限性在于无法实现非接触式和端到端的侧信道攻击，而 BankSnoop 通过解决这些限制，实现了对用户隐私的细粒度推断和快速适应。

2.2磁侧信道攻击

部分研究工作关注磁基侧信道攻击。MagEar 利用受害者耳机扬声器的磁通量进行音频窃听攻击[23]。MagSnoop 注入恶意软件来捕获磁安全传输（MST）过程中的声音，例如三星支付，以恢复信用卡的令牌[11]。此外，电磁辐射也可以用来提取密钥、重构模型架构、揭示屏幕消息和击键[16, 5, 29, 25, 19, 43]。与这些先前的研究类似，BankSnoop 通过展示利用两种磁感应现象攻击无线充电宝的可行性，拓展了磁侧通道攻击的研究领域。

论文中总结了五个指标与五个最先进的相关作品[12,21,24,45,47]的比较，如图 1 所示。

Attacks	Attack surface	Contactless	No need to Compromise devices	No prior knowledge of devices	Fine-grained user privacy	Domain adaptive
Cour et al. (CCS'21)	Current in power line	✗	✗	✗	✗	✗
Wu et al. (ACSAC'21)	Inductive current	✓	✓	✗	✗	✗
EM-Surfing (TDSC'22)	Inductive voltage	✗	✗	✗	✓	✗
Charger-Surfing (Security'20)	Current in USB cable	✗	✗	✗	✓	✗
GhostTalk (NDSS'22)	Current in USB cable	✗	✗	✗	✓	✗
BankSnoop (Our work)	*Coil whine and Magnetic field*	✓	✓	✓	✓	✓

图 1：从五个指标与相关攻击进行比较：(M1) 非接触式或非接触式；(M2) 无需危及设备；(M3) 不具备充电设备的先验知识；(M4) 细粒度用户隐私推断；(M5) 适应各种条件

3. 研究内容

3.1主要挑战及创新点

使用相关技术推断用户隐私，需要考虑实际的攻击场景。此前研究的侧信道攻击需要稳定的充电电压和智能手机高电池电量以及 USB 线中的充电电流等信息，而与这些相关研究的攻击不同[12,21,24,45,47]，对于使用无线充电宝的用户，攻击者不一定事先知道其正在充电的智能手机和移动电源的基本信息(例如，型号类型，电池状态)，同时我们不认为攻击者可以破坏移动电源或在受害者的智能手机中安装恶意软件来获取电流/电压迹线。因此基于新侧信道的攻击方法无法像此前的研究一样直接使用电流电压等信息。

另外，攻击者没有两台设备的 LoS 视图（即无法直接看到无线充电宝与智能手机），也不知道无线充电宝开始给智能手机充电的具体时间。同时其在攻击前也不可能从不同的条件下收集大量的数据样本来训练多个隐私推理模型。因为这种数据收集的方式具有随机性，同时成本较大。

针对这多个场景与技术挑战，论文考虑了攻击者的场景，攻击者可以在靠近目标移动电源的物理位置放置一个小型攻击设备来记录线圈啸叫并测量环境磁场干扰。因此研究者提出了 BankSnoop 攻击框架，其可以利用测量得到的侧信道（线圈啸叫与环境磁场干扰）来推断用户隐私，同时，由于攻击场景和环境的多样性，其创新地采用了小样本学习技术来提升其自适应能力。

3.2 技术路线及实现

3.2.1 攻击触发识别

无线充电电源在充电过程中，由于其蓄电量有限，持续大的放电电流不可避免地会缩短电池寿命，因此无线充电电源会根据其电池电量的高低来控制线圈内的运行电流$I_P(t)$。这种调节机制可以简单理解为，无线充电宝电量变化，会导致充电电压与电流会发生变化（电量越小充电越慢），这种电流动态变化，最终会导致线圈产生轻微振动，从而引发线圈啸叫和环境电磁场扰动两种物理现象。

论文首先考虑了侧信道攻击的触发条件，即需要识别无线移动电源为智能手机无线充电这一过程。如上文所述，无线充电宝位智能手机充电时，会产生线圈啸叫和磁场干扰两种物理现象。线圈啸叫会在无线充电开始时出现，因此可以将其作为触发攻击的指示器。此外，磁场干扰可以用来推断充电装置的状态。因此攻击框架中会将它们一起使用，通过监测线圈的啸叫来检测充电状态，并通过测量磁场来推断充电宝和充电智能手机的电池电量。

线圈啸叫检测。线圈啸叫又称电磁感应声噪声，是在电磁力(如麦克斯韦应力

张量、磁致伸缩和洛伦兹力)的激励下，线圈振动而产生的微音现象[6]，根据安培力定律，L_P为初级线圈的周长，可以知道该力与线圈特征有关（公式 1)。这些力会引起线圈的扭曲和振动，导致线圈啸叫的现象产生。从公式也可以知道，线圈啸叫存在于不同的频率范围内，人可能听到(频率在 20Hz - 20kHz 之间)，也可能听不到，而只要在攻击框架中添加有足够采样频率的录音麦克风模块，即可捕捉该信息。

$$F_P(t) = N_P \Phi_P(t) I_P(t) L_P \propto \mathrm{B}^2(t) \tag{1}$$

论文中的攻击框架首先利用麦克风模块来检测线圈的啸叫，应用高通滤波器去除低频声音(如人说话、触屏敲击)引起的噪声后，使用周期汉恩窗口利用短时傅里叶变换(STFT)来获得滤波音频的功率谱,从功率谱中可以提取声学特征 Mel-frequency 倒谱系数(MFCCs)[41]，并将其作为一个预训练决策树[38]分类器的输入来确定当前充电状态(未充电或正在充电)。

指纹识别设备。根据无线充电宝的原理，产生线圈啸叫这一现象所需的电磁力与线圈的匝数和周长有关。不同的移动电源和智能手机的线圈具有不同的特性，因此攻击框架可以利用线圈啸叫现象来识别智能手机与电脑。遵循线圈啸叫检测相同的过程,并实现另一个预训练的决策树分类器来确定移动电源和智能手机的设备类型。

电池电量推断。无线充电电源包含有限的电能在电池中。为了识别移动电源的电池电量，以确定其是否有足够的电量来发动攻击，同时智能手机的电池电量是影响机型性能的重要因素，也会影响攻击框架的性能，因此论文中的攻击框架需要推断智能手机电池电量,其利用了磁场干扰来推断智能手机和移动电源的确切电池电量。攻击框架使用了磁强计采集三轴磁信号，测量捕获的三维磁场强度$Mags(t)$在特定时间点t，如式 2 所示。

$$Mag_s(t) = \sqrt{Mag_x^2(t) + Mag_y^2(t) + Mag_z^2(t)} \tag{2}$$

Mag_x，Mag_y，Mag_z分别代表x轴，yz轴的磁场。通过扣除不存在充电装置的情况的磁场得到强度差值，并计算其累积分布函数(CDF)。之后攻击框架会使用 CDF 值来训练一个决策树分类器来推断移动宝和充电智能手机的电池电量。

3.2.2 基于磁的活动识别

在充电过程中，不同的智能手机用户交互会引起感应电流的变化[21]，从而对环境电磁场产生干扰。具体来说，智能手机的高能耗活动(如屏幕动画、按键盘)会使二次线圈上的负荷发生Δr(t)的变化,从而产生电磁场$\Delta\Phi(t)$的扰动，如公式 3 所示。这些变化引起的磁场扰动可以通过监测一段时间内的电磁场来测量。在实践中，特定时间点的电磁场可以被描述为一个 3D (x，y，z)向量，该向量可以被磁强计模块捕获，用于推断智能手机上的各种用户活动。因此在攻击框架中

添加磁强计模块来捕捉该信息。

$$\Delta I(t) = \frac{U_S(t)}{\Delta R(t)}, \Delta \Phi(t) = \frac{\mu_0 N_S \Delta I(t)}{2R_S} = \frac{\mu_0 N_S U_S(t)}{2R_S \Delta r(t)} \propto \frac{\Delta \mathrm{B}(t)}{\Delta r(\mathrm{t})} \tag{3}$$

在识别出攻击触发条件并确定设备类型和电池电量后，BankSnoop 接下来利用预先训练好的深度学习模型与捕获的 3D 磁场信号来识别充电智能手机上的各种用户活动。其识别需要经过以下几个步骤。

- **预处理。**在获得原始磁场信号后，首先会使用 Savitzky-Golay (S-G)滤波器去除采集到的磁场信号中的噪声，同时不使信号形状失真[8, 32, 33]。然后，将前一秒数据的平均值计算为三轴上的静态磁场值，并推导出该偏移值。由于每个活动在每次尝试中都有不同的时间长度(例如，一个应用程序启动需要 1–5 秒[36]，而单个按键可能只需要 0.05–0.2 秒[48])，BankSnoop 通过利用上采样(例如，插值[35])或下采样(例如，抽取因子[20])算法将每个活动尝试的处理信号归一化到相同的时间长度(例如，0.1 秒)。
- **活动识别。**处理后的磁信号为三轴一维时间序列，因此采用一维卷积神经网络(CNN)来构建活动推断分类器(如应用指纹识别、应用内活动识别、单键识别)。在基于 CNN 的网络中，使用两个卷积层从输入时间序列中提取时空特征，并使用两个批处理归一化层来标准化数据并稳定学习过程。然后，两个最大池化层可以减少一半的尺寸，并添加一个 dropout 层来防止过拟合。最后，flatten 层将特征映射转换为一维，最后的全连接层以最高的概率输出预测的类。
- **实现。**该部分主要阐述 CNN 的实现，识别的具体步骤主要包括前两点。

  在获得识别中的在按键推断的情况下，由于用户经常以不同长度的序列键入密码或敏感按键，论文将两次相邻按键之间的每个时间间隔定义为一个新的按键类，并将其添加到上述两个软键盘的训练过程中

  已知 SoftMax 函数可以生成一个数组，该数组包含每个类的概率，并输出具有最高概率值（也称为 argmax）的预测标签。论文的实现利用了 softmax 预测序列中的 top k 个概率最高的元素来评估模型的准确性。

3.2.3 小样本学习

基于 CNN 的磁信号分类器具有良好的准确率，但其性能会受到移位条件的影响。以前的侧信道攻击试图限制先决条件(例如电源电量等[21])或针对不同配置(例如，智能手机模型[12])训练多个深度学习模型。然而，这些方法不仅需要大规模的数据集来保证良好的性能，而且还限制了攻击场景。而论文中考虑到实践中各种攻击场景，基于模型不可知元学习 (model-agnostic meta-learning, MAML)的概念，在 BankSnoop 中设计了一个小样本学习模块[15]。其主要包括**元训练**和**适应**这两个阶段。

元训练最终输出是具有优化参数θ^*的分类器，其步骤如下

- 将磁信号分类器表示为f，网络参数为θ
- 从不同条件下收集到的包含磁信号样本的元数据集中生成一组任务$\mathcal{T}$
- 对于其中的每个任务$\mathcal{T}_i$，分类器通过使用每个类中很少数量的 K 个标记样本来学习识别 N 个类
- 每个任务 $\mathcal{T}_i$ 包括一个支持集$\mathcal{S}_{\mathcal{T}i}$和一个查询集$\mathcal{S}_{Qi}$
- 分类器f以随机的参数θ进行初始化，然后由每个任务 $\mathcal{T}_i$ 相关的支持集 $\mathcal{S}_{\mathcal{T}i}$ 进行训练
- 然后分类器通过更新梯度下降，如式 4 所示，会学习到一个新的任务特定的参数 θ'（每个任务对应一个）

$$\theta'_{\mathcal{T}_i} = \theta_0 - a\nabla_\theta \mathcal{L}_{\mathcal{T}_i}(f_{\theta_0}, S_{\mathcal{T}_i}) \tag{4}$$

其中，a为单个任务的预设学习率；$\mathcal{L}_{\mathcal{T}_i}(f_{\theta_0}, S_{\mathcal{T}_i})$是在支持集$\mathcal{S}_{\mathcal{T}i}$上的特定于任务的交叉熵损失，其表达式如式 5 所示，(x_j, y_j)是$S_{\mathcal{T}_i}$中的样本。

$$\mathcal{L}_{\mathcal{T}_i}(f_{\theta_0}, S_{\mathcal{T}_i}) = \sum_{(x_j,y_j)\in S_{\mathcal{T}_i}} y_j log f_\theta(x_j) + (1-y_j) log f_\theta(1-x_j) \tag{5}$$

- 得到每个任务对应的参数后，定义式 5 的元目标函数，**根据此目标函数来寻找能使任务损失总和最小的参数**

$$argmin_\theta \sum_{\mathcal{T}_i \in \mathcal{T}} \mathcal{L}_{\mathcal{T}_i}(f_{\theta_0}, S_{Q_i}) \tag{6}$$

- 获得评估分类器在该任务的查询集$\mathcal{S}_{Qi}$上的性能。最后通过应用随机梯度下降获得 θ*

$$\theta^* \leftarrow \theta_0 - \beta\nabla_\theta \mathcal{L}_{\mathcal{T}_i}(f_{\theta_0}, S_{\mathcal{T}_i}) \tag{7}$$

适应。在获得优化后的初始化参数θ^*后，磁信号分类器只需从新场景中收集K×N 标记的训练样本对预训练模型进行微调，即可快速适应各种攻击场景(例如，不同的无线充电电源，电池电量等)。

例如，当从不同的无线充电库($D_{new} \cap D_S = \emptyset$)收集到一个新的目标数据集$\mathcal{T}_{new}$时，优化的分类器$f_{\theta^*}$可以快速适应这个新的任务，并在几个梯度下降更新中获得新的参数，其更新的式子如式 8 所示。

$$\theta_{\text{new}} = \theta^* - a\nabla_\theta \mathcal{L}_{\mathcal{T}_i} D_{new}(f_{\theta^*})$$

3.2.4 BankSnoop 攻击框架

论文中先展示了攻击框架，再叙述框架中流程的设计与原理。这里笔者更换了一下顺序，综合上述的过程，很容易可以得到如图 2 所示的攻击框架。

攻击者首先获取线圈啸叫和磁场信号来确定充电状态，触发攻击来识别智能

手机和移动电源的类型和电池电量。然后，利用收集到的磁信号，使用预训练的深度神经网络模型进行细粒度的活动识别。此外，BankSnoop 还包含了一个快速适应各种攻击场景的几次学习模块(例如，不同的智能手机型号，移动电源)。最后，攻击者可以推断出细粒度的用户活动和隐私，如解锁密码、敏感击键和应用程序内活动。

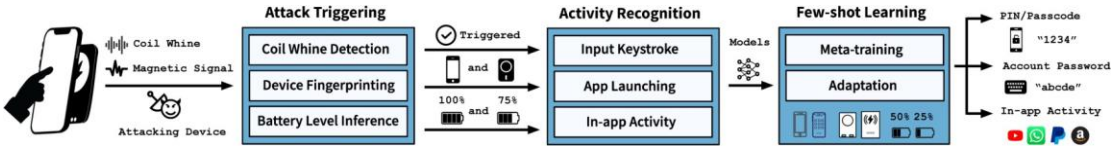

图 2：BankSnoop 攻击框架

3.2.5 便携式攻击装置

综合上述成果,研究者最终设计并制作了如图 3 所示的一个便携式攻击装置。其包括以下四个组件：微控制器单元（MCU)、麦克风、磁力计、SD 卡。总尺寸约为 1.8×1.3 英寸（4.6×3.3 厘米），接近苹果 AirPods 充电仓的尺寸

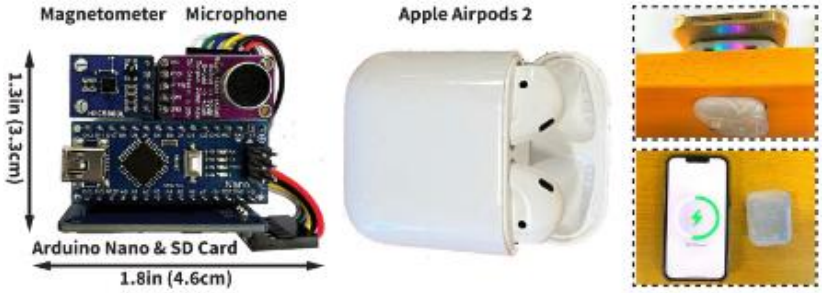

图 3：攻击装置示意图

3.3 相关技术介绍

3.3.1 无线充电宝

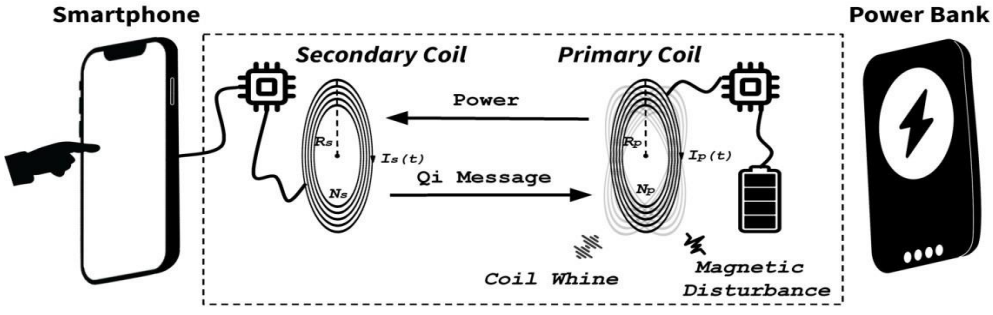

图 4 无线充电宝工作原理图

无线充电宝的工作原理图如图 2 所示。当移动电源连接到智能手机上，它会利用电磁感应[46]将电源从其线圈(初级线圈)传输到智能手机的线圈(次级线圈)。首先，移动电源根据 Biot-Savart 定律(公式 2)在初级线圈和次级线圈中产生感应电磁场$\Phi_P(t)$和$\Phi_s(t)$，然后根据法拉第定律，感应电磁场$\Phi_s(t)$产生感应电压$U_s(t)$

为智能手机充电，如公式 3 所示。式中$I_P(t)$为初级线圈的运行电流，p和R_P为初级线圈的匝数和半径，s和R_s为次级线圈的匝数和半径，η为能量传输系数，μ_0为磁常数。

$$\Phi_P(t) = \frac{\mu_0 N_P I_P(t)}{2R_P},\ \Phi_S(t) = \eta\Phi_P(t) \tag{8}$$

$$U_S(t) = N\frac{\Delta\Phi_S(t)}{\Delta t} = \eta\frac{N_S}{N_P}\cdot\frac{\mu_0\Delta I_p(t)}{2R_S\Delta \mathrm{t}} \tag{9}$$

3.3.2 卷积神经网络(CNN)

卷积神经网络（Convolutional Neural Network，CNN）是一种专门用于处理和分析具有网格结构数据的深度学习模型。它主要应用于图像处理、计算机视觉和模式识别等领域。CNN 的设计灵感来源于生物学中视觉皮层的工作方式。

CNN 主要包括输入层，卷积层，激活层，池化层，光栅化，全连接层，激活层，输出层。其中，**卷积层、激活层**和**池化层**可叠加重复使用，这是 CNN 的核心结构。

- **卷积层**由一组滤波器组成，滤波器为三维结构，其深度由输入数据的深度决定，一个滤波器可以看作由多个卷积核堆叠形成。这些滤波器在输入数据上滑动做**卷积运算**，从输入数据中提取特征。在训练时，滤波器上的权重使用随机值进行初始化，并根据训练集进行学习，逐步优化。

  卷积运算是指以一定间隔滑动卷积核的窗口，将各个位置上卷积核的元素和输入的对应元素相乘，然后再求和（有时将这个计算称为乘积累加运算），将这个结果保存到输出的对应位置。其式子如下所示。

  连续形式：$x(t)h(t)(\tau) = \int_{-\infty}^{+\infty} x(\tau)\,h(\tau - t)dt$ (10)

  离散形式：$x(t)h(t)(\tau) = \sum_{\tau=-\infty}^{\infty} x(\tau)h(\tau - t)$ (11)

- **池化层**的作用是进行**下采样降维**，用来缩小高、长方向的尺寸，减小模型规模，提高运算速度，同时提高所提取特征的鲁棒性。简单来说，就是为了提取一定区域的主要特征，并减少参数数量，防止模型过拟合。池化层通常出现在卷积层之后，二者相互交替出现，并且每个卷积层都与一个池化层一一对应。

  常用的池化函数有：均值池化、最大池化、最小池化和随机池化（等。均值池化是对所有特征点求平均值，而最大值池化是对特征点的求最大值。而随机池化则介于两者之间，通过对像素点按数值大小赋予概率，再按照概率进行亚采样

- **激活层**中，使用激活函数，在模型中**引入非线性**。激活函数是运行时激活神经网络中某一部分神经元，将激活信息向后传入下一层的神经网络。主要分为饱和激活函数和非饱和函数。

  这里介绍使用到的饱和激活函数 **Softmax 函数**。Softmax 是 soft 的 max，是用于多类分类问题的激活函数。在多类分类问题中，超过两个类标签则需要类成员关系。对于长度为 K 的任意实向量，Softmax 可以将其压缩为长度为 K，值在（0，1）范围内，并且向量中元素的总和为 1 的实向量，其式子如

下所示。

$$S_i = \frac{e^i}{\sum_{j=1}^{j} e^j} \tag{12}$$

3.3.3 决策树分类器

决策树（Decision Tree），它是一种以树形数据结构来展示决策规则和分类结果的模型，作为一种归纳学习算法，其重点是将看似无序、杂乱的已知数据，通过某种技术手段将它们转化成可以预测未知数据的树状模型，每一条从根结点（对最终分类结果贡献最大的属性）到叶子结点（最终分类结果）的路径都代表一条决策的规则。其流程如图 5 所示。

- 首先从开始位置，将所有数据划分到一个节点，即根节点。
- 然后经历橙色的两个步骤，橙色的表示判断条件：
- 若数据为空集，跳出循环。如果该节点是根节点，返回 null；如果该节点是中间节点，将该节点标记为训练数据中类别最多的类
- 若样本都属于同一类，跳出循环，节点标记为该类别；
- 如果经过橙色标记的判断条件都没有跳出循环，则考虑对该节点进行划分。既然是算法，则不能随意的进行划分，要讲究效率和精度，选择当前条件下的最优属性划分（什么是最优属性，这是决策树的重点，后面会详细解释）
- 经历上步骤划分后，生成新的节点，然后循环判断条件，不断生成新的分支节点，直到所有节点都跳出循环。
- 结束。这样便会生成一棵决策树。

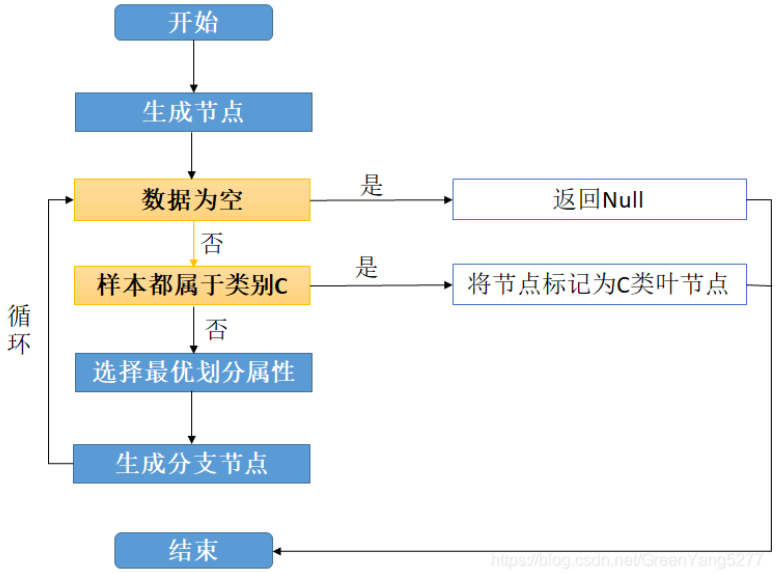

图 5：决策树流程图（来源于网络）

3.3.4 Mel-frequency 倒谱系数

频谱图往往是很大的一张图，为了得到合适大小的声音特征，需要把它通过梅尔标度滤波器组（Mel-scale filter banks），变换为梅尔频谱。

人耳听到的声音高低和实际频率不呈线性关系，用 Mel 频率更符合人耳的听

觉特性（这正是用 Mel 声谱图的一个动机，由人耳听力系统启发），即在 1000Hz 以下呈线性分布，1000Hz 以上呈对数增长，Mel 频率与 Hz 频率的关系为：

$$f_{mel} = 2595 \cdot \lg\left(1 + \frac{f}{700Hz}\right) \tag{13}$$

我们将频谱通过一组 Mel 滤波器就得到 Mel 频谱，公式为

$$logX(k) = \log\left(Mel - Spectrum\right) \tag{14}$$

在$logX(k)$上进行倒谱分析

取对数：$logX(k) = logH(k) + logE(k)$ (15)

进行逆变换：$X(k) = H(k) + E(k)$ (16)

在 Mel 频谱上面获得的倒谱系数$H(k)$就称为 Mel 频率倒谱系数，简称 MFCC。

3.3.5 梯度下降法

梯度下降法（Gradient descent，简称 GD）是一阶最优化算法。 要使用梯度下降法找到一个函数的局部极小值，必须向函数上当前点对应梯度（或者是近似梯度）的反方向的规定步长距离点进行迭代搜索。梯度下降法是迭代法的一种，可以用于求解最小二乘问题（线性和非线性都可以）。在求解机器学习算法的模型参数，即无约束优化问题时，梯度下降法和最小二乘法是最常采用的方法。在求解损失函数的最小值时，可以通过梯度下降法来迭代求解，得到最小化的损失函数和模型参数值。

在当前位置求偏导，即梯度，正常的梯度方向类似于上山的方向，是使值函数增大的，下山最快需使 J(w)最小，从负梯度求最小值，这就是梯度下降。梯度上升是直接求偏导，梯度下降则是梯度上升的负值。

如果函数为一元函数，梯度就是该函数的导数：

$$\nabla f(x) = f'(x) \tag{17}$$

如果为二元函数，梯度定义为：

$$\nabla f(x_1, x_2) = \frac{\partial y}{\partial \chi_1} i + \frac{\partial y}{\partial \chi_2} i \tag{18}$$

梯度下降法公式：

$$\theta_i = \theta_i - \alpha \frac{\partial J(\theta_0, \theta_1, \theta_2, \ldots, \theta_n)}{\partial \theta_i} \tag{19}$$

4. 性能评估

本论文通过控制变量法，设计了一系列实验评估其所提出的 BankSnoop 攻击框架的性能，如活动识别的正确率和小样本学习模块的正确率，验证了该攻击框架的可行性与实用性。

4.1 实验设置

实验中的**硬件设置**如下：

- 麦克风和磁力计的预设采样频率分别为 40kHz 和 100Hz
- 所有数据处理都是在运行 Windows 10 的台式机上进行的，该台式机具有 32GB 内存、Intel i7-9700K CPU 和 NVIDIA GeForce RTX 2080Ti GPU
- 注：实验是在不受控制的环境中进行的，低频噪声（例如人类说话）会产生微小的影响，因为线圈振动声具有高频范围。

实验中在不同条件下的商品设备上构建了六个不同的**数据集：**

- $\mathcal{D}_{CW}$：线圈啸叫数据集包含了两种情况下的 1 秒音频片段：充电中和未充电。其中在充电状态下，收集了屏幕在打开和关闭状态下的样本
- $\mathcal{D}_{DF}$：设备识别数据集遵循以上相同的收集过程
- $\mathcal{D}_{BL}$：电池电量数据集是从两个无线充电宝中收集的，当给 4 部不同电量的智能手机充电时，这两个充电宝呈现不同的电池水平
- $\mathcal{D}_{App}$：移动应用数据集是从 120 个不同应用程序中收集的，我们收集每个应用程序启动前的 0.1 秒为样本。此外，以 5 个最受欢迎的应用程序作为数据样本以训练用于应用程序内活动识别的分类器
- $\mathcal{D}_{UK}$、$\mathcal{D}_{QWERTY}$：这两个击键数据集是从解锁键盘和 QWERTY 全键盘中收集的

4.2 评价指标

论文中使用准确率和混淆矩阵作为指标来评估 BankSnoop 在线圈噪声检测、设备指纹识别、电池电量推断、应用启动/应用内活动识别和击键识别上的性能。

准确率是一个常用的评价指标，即正确识别次数与总识别次数之比。

混淆矩阵是一种多分类问题的性能评价表格，以矩阵形式展示模型对不同类别样本的分类结果。以二分类问题为例，混淆矩阵如图 6 所示。矩阵中的元素为对应的分类概率。

	预测为正类别	预测为负类别
正类别	真正例 (True Positive, TP)	假负例 (False Negative, FN)
负类别	假正例 (False Positive, FP)	真负例 (True Negative, TN)

图 6 混淆矩阵示意图

4.3 性能评价

4.3.1 衡量 BANKSNOOP 在各方面的表现

- **线圈啸叫的检测**。根据数据集$\mathcal{D}_{CW}$训练决策树分类器。在测试集上，总体准确率达到了 99%。
- **设备类型识别**。根据数据集$\mathcal{D}_{DF}$训练决策树分类器。如图 7 所示，结果表明达到 98.3%的准确性。

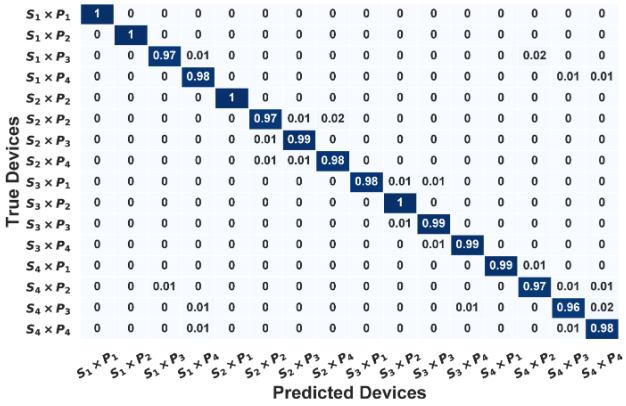

图 7：设备类型识别混淆矩阵

- **电池电量推断**。根据 4.1 中的研究结果和数据集$\mathcal{D}_{BL}$，生成磁场强度差异的 CDF 函数以训练决策树分类器。结果表明，准确率达到了 99.8%。

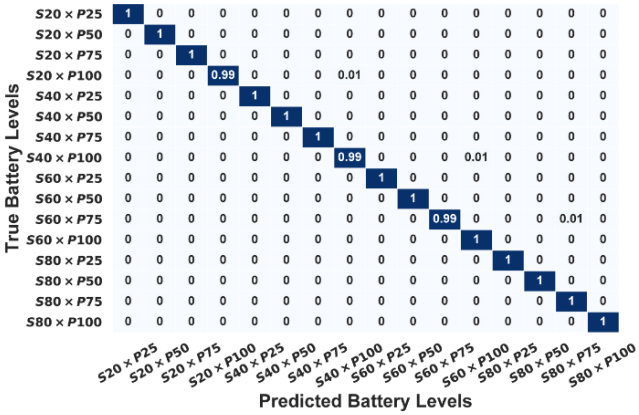

图 8：电量推断混淆矩阵

- **应用程序启动识别**。使用数据集$\mathcal{D}App$中 80%的数据以训练识别模型，20%数据评估模型性能。总体来说，达到了 93.1 ± 2.9%的准确率。具体而言，在识别“书籍”和“教育”等类别的应用程序表现最好，在识别“社交网络”类别的应用时表现最差。

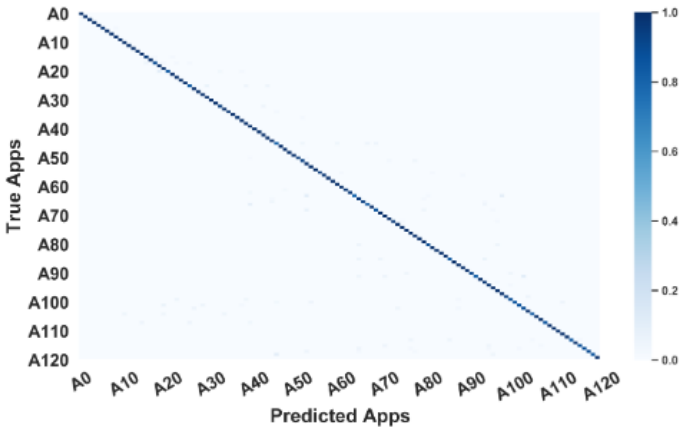

图 9：应用程序启动识别混淆矩阵

- **应用内活动识别**。在*DApp* 中，我们还收集了在五个流行的应用程序中执行五个应用特定的活动时的数据，并实现了基于 CNN 的应用内活动识别分类模型。BankSnoop 在识别评估分别达到 85.2%、84.0%、86.2%、82.2%和 81.4%的准确率。

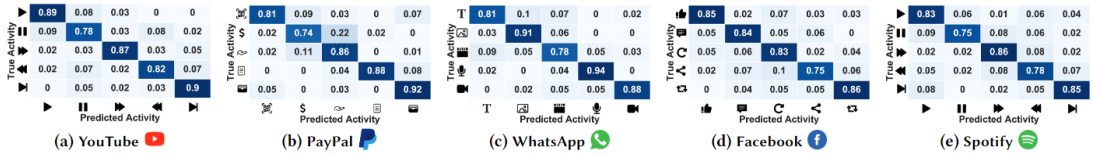

图 10：应用内活动识别混淆矩阵

- **按键识别**。我们为每个键盘随机生成三个数字和特征序列，长度从 1 到 10 不等。每个随机生成的序列重复 100 次（例如，QWERTY 键盘长度为一的测试用例的三个例子是“c”、“o”和“e”）。我们生成预测序列的前 10 个候选者，并且如果前 10 个候选中的一个是正确的，则获得相应的精度。长度为 1 和 10 的序列的总准确率分别为 94.9%和 86.9%。前 10 位候选者的准确性随着序列长度的增加而降低，而按键识别的准确性仍然与其他识别工作相当。

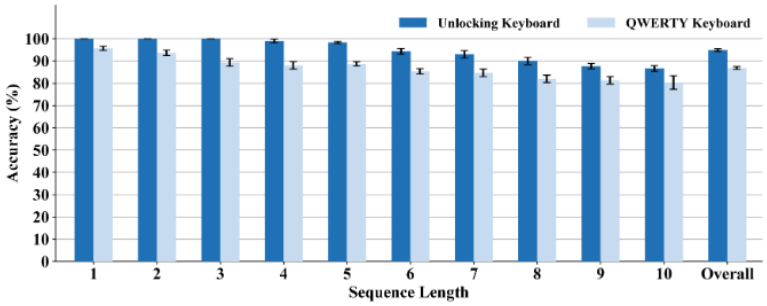

Figure 11: Keystroke uncovering results of the unlocking and the QWERTY keyboards with top-10 candidates.

图 11：按键识别准确率直方图

4.3.2 小样本学习模块评估

论文将提出的小样本学习模块与三个基准进行了比较：

Source-Only（SO）：我们使用仅从源数据集 *DS* 训练的模型，并在不进行适

应的情况下评估其在目标数据集 $\mathcal{DT}$ 上的性能。

Target-Only（TO）：我们使用目标数据集 $\mathcal{DT}$ 训练基于 CNN 的神经网络，并使用 $\mathcal{DT}$中的其余样本对其进行评估。

Transfer-convolutional (TrC) ：转移卷积是用于领域自适应的最先进的转移学习方法之一，它假设类似问题的上层表示是可转移的。

之后其控制变量，进行了以下的实验并获得了相应的结果。最终的结果图如图 12 所示，其中对每个图的分析如下。

a) 不同的充电宝电量。在 25%、50%、75%、100%的电池级别下分别收集了数据集$\mathcal{D}_{App}$， $\mathcal{D}_{UK}$ 和 $\mathcal{D}_{QWERTY}$。以电池级别为 100%的数据集作为$\mathcal{DS}$以构建基本模型并且将其余样本作为 $\mathcal{DT}$。

b) 不同的手机电量。在先前的实验中表明，智能手机电池的百分比会影响型号的性能。我们使用从 EGO MAGPOWER 2 为 80%电量的 iPhone 13 Pro 进行充电所收集的数据集作为 $\mathcal{DS}$ ，60%，40%，20%的数据作为$\mathcal{DT}$。

c) 不同型号的充电宝。由于不同的线圈参数（例如，线圈匝数、材料），不同的无线充电宝可能呈现相似任务下的不同线圈鸣鸣声和磁信号模式。利用在 p1 中收集到的数据集作为 $\mathcal{DS}$，p2、p3、p4 的数据作为 $\mathcal{DT}$。

d) 不同型号的手机。不同型号的智能手机的次级线圈参数不同，电池容量不同，这导致感应电流变化的模式不同。先前针对不同型号训练不同的模型。使用 S1 中收集的数据作为 $\mathcal{DS}$，S2、S3、S4 的数据作为$\mathcal{DT}$。

e) 不同用户。智能手机用户可能有不同的打字模式。招募了四名志愿者（*U1，U2，U3*，以及*U4*） 加入这项研究，并收集数据进行评估以调查不同用户的影响。以 *U1* 作为$\mathcal{DS}$，其他三个作为$\mathcal{DT}$

f) 不同屏幕亮度。触摸屏的亮度在大部分电池消耗中占主导地位。因此，亮度可能会影响识别用户活动的性能，尤其是当屏幕亮度变化很大时。以 75%的数据集设置为$\mathcal{DS}$，以其他三个亮度数据集（25%，50%，100%）作为$\mathcal{DT}$

g) 不同壁纸。使用从纯白色壁纸中收集的数据作为$\mathcal{DS}$以及从纯黑色、多色和动态壁纸中收集的其他数据集作为$\mathcal{DT}$。动态壁纸最低（SO 低于 30%，小样本 77.7%）

h) 不同的桌面。在我们的实验设置中，桌子表面的特性可能会影响 BankSnoop 的性能。因此，我们通过放置设备（P1 × S1）在其他三个桌面上收集数据进行评估：0.31 英寸的玻璃、1.38 英寸的大理石和 0.43 英寸的塑料。同样，我们使用从橡木中收集的数据作为$\mathcal{DS}$并在其他表面收集数据作为$\mathcal{DT}$

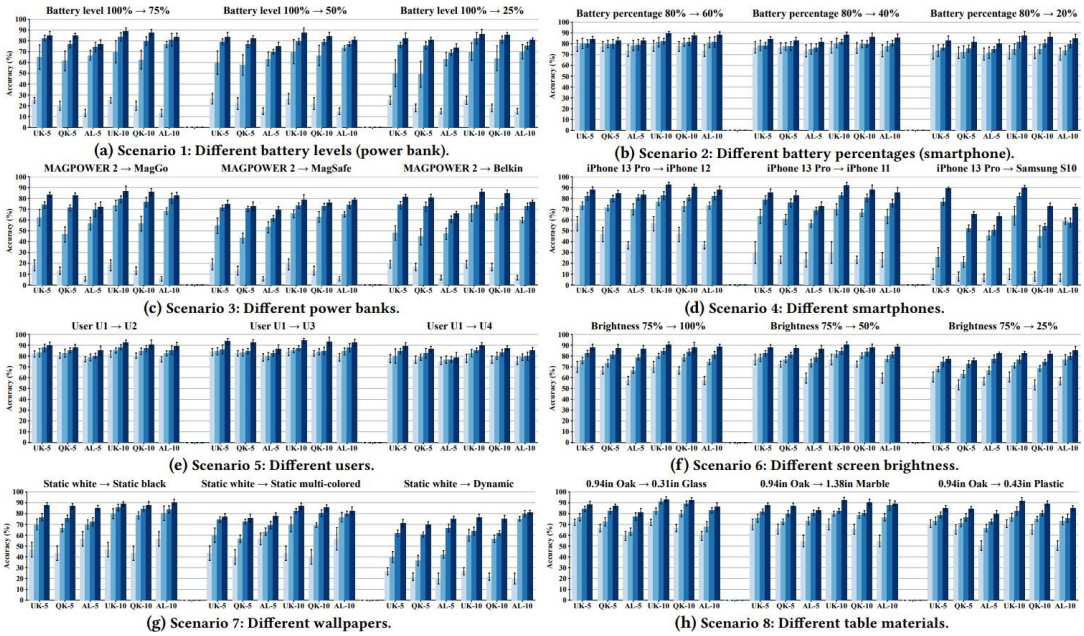

图 12：不同场景下的小样本学习模块评估结果(包含 5 个样本和 10 个样本)。UK：解锁键盘击键准确率。QK：QWERTY 键盘击键准确率。AL：应用启动识别准确率。-K：K-shot 学习。每个图中的四个不同颜色的柱状依次表示三个基准方法 SO， TO，TrC 和小样本学习。

5. 论文评述

5.1优缺点分析

本论文发现了无线充电宝中的一种新的侧信道，并基于此信道提出了 BankSnoop 攻击框架，揭示了一种全新的信息泄露途径。这一侧信道（无线充电时的所产生的物理现象）的发现否定了无线充电宝不会泄露用户隐私这一观点，并且为科学界和工业界提供了对于无线充电技术的新认识。其有以下优点：

- **逻辑性强，分析严密：**本文在对框架设计进行阐述之前，首先阐述了一项激励其工作的例子，该例子初步直观地展现了线圈啸叫和磁场扰动与无线充电宝充电过程存在关系，并在设计框架之前严密地分析了攻击者的限制与能力，这使得攻击框架的设计更加符合现实逻辑。之后根据攻击框架逐步分析与阐述，逻辑明确，层层递进。每一步的流程都具有详细的理论分析，并设计了相关的实验以证明其正确性。
- **采用小样本学习来提高攻击框架的适应能力：**此前的侧信道攻击研究往往受到许多的限制，如手机电量，USB 线以及其他因素等，而文中提出的 BankSnoop 攻击框架采用了小样本学习的方法，通过收集新环境下的小样本信息来快速适应，提高了攻击框架的鲁棒性和自适应能力，这一定程度上解决了此前研究的诸多限制。

- **严谨与完善的实验设计：**文中使用准确率与混淆矩阵作为评估指标。衡量了BankSnoop在线圈啸叫检测，用户活动检测等多方面的表现，并通过比较其他三种基准方法，从8个角度对小样本学习模块进行评估。设计的实验非常严谨完善，取得的结果更能令人信服。
- **前瞻性与现实意义强：**当今充电宝的使用已成为生活中不可缺少的一部分，无线充电宝也逐渐走入人们的生活。但其所涉及到的隐私泄露问题，尚未引起研究者以及大众的关注。本论文提出的BankSnoop攻击框架，有利于后续的研究者进行相关的研究，并采取措施来应对新兴技术所带来的安全隐患，为未来安全性研究提供了新的思路。这不仅对当前的无线充电设备提出了警示，同时也为未来的技术研发和安全性防范提供了启示。

与此同时，论文也存在着一些不周之处：

- 在介绍部分的阐述中，作者提及此前充电过程泄露用户隐私的研究没有引起公众关注，与其后面阐述无线充电宝为何被认为能够克服用户隐私泄露问题的原因不直接相关。
- **未进一步研究与说明应用活动识别准确率的下降：**在分析应用程序启动识别的实验结果时，识别“社交网络”类别的应用时准确率较低，而应用内活动识别的准确率也显著低于其他活动识别(按键识别等)，论文并没有对该问题进行深入的研究，分析与解释。
- **论文中所提到的局限性：**论文中的实验设计都是将攻击设备放在桌子下面或将其放在目标移动电源旁边来进行评估，而没有评估攻击设备在其他可能场景下的性能。论文中考虑了一个近距离和实际的攻击距离来证明其可行性，研究表明其性能随距离增加性能急剧下降，但未给出详细的说明。
- **其他实验的欠缺：**除距离与位置之外，论文中对用户隐私的推断包括应用程序启动和几种内部活动，实际上的用户活动种类繁多，缺乏一些典型用户活动的设计，如通话与听音乐等。在按键的识别中，考虑了两种键盘，但未进一步研究随机键盘（键盘中的字母位置随机）所带来的影响。
- **未从用户角度去评价与说明：**论文在讨论部分从制造者的角度阐述了针对于BankSnoop攻击框架的措施，包括屏蔽磁场和混淆两种方式。但未从用户的角度去阐述相关的用户隐私泄露问题的严重性和应对措施，这部分的缺失可能降低论文的警示能力，难以引发大众意识。

5.2改进方向

- **用户隐私泄露问题的进一步说明：**当今社会中，用户隐私泄露问题无疑是非常普遍且严重的。论文可以对此类问题的严重性进行详细的说明，并阐述其缺乏大众意识关注的原因，给予后续研究者一定的研究方向，并提高论文的警示能力，提高大众的隐私保护意识。

- **识别活动准确率差异研究：**论文中的部分结果（部分应用启动识别，应用内活动识别）的准确率与其他活动识别的准确率存在一定的差异（较低），后续的研究可以对该现象进行深入的研究与分析，提高攻击框架在该方面的准确率与鲁棒性。
- **距离与位置的考虑：**论文中基于移动电源旁的研究结果准确率较高，但攻击设备的性能随距离增加性能急剧下降，后续的研究可以考虑通过多设备的协作学习，多样本学习等方式来解决该方面的限制，使攻击框架的各方面性能进一步增强。
- **用户等角度的分析与评价：**论文提出的 BankSnoop 攻击框架，揭示了一种全新的信息泄露途径。应对此类信息泄露问题的措施也是一个非常重要的研究方向，后续的研究者可以从用户，制造商等角度进行考虑，从多方面对该问题进行研究与分析。
- **其他侧信道的研究：**论文的研究者发现了无线充电宝中的一种新的侧信道，线圈啸叫和磁场干扰，对该侧信道其他作用的研究，以及研究无线充电宝或传统充电电源是否具有其他侧信道无疑也是一个有重大意义的研究方向。

5.3阅读收获

传统移动电源存在一定的隐私泄露问题，而本论文在此基础上，对最近兴起的无线充电宝进行了研究，发现了一种新的侧信道，并设计出 BankSnoop 攻击框架来证明该信道在泄露用户隐私上的实用性。

于学术角度而言，通过阅读与分析该论文，我对其提出的侧信道与 BankSnoop 攻击框架有了深刻的理解与认识。我了解到导致相关隐私泄露的原因可能只是简单却时刻存在的物理现象，其可能是线圈啸叫，磁场干扰，甚至电压电流变化。这一认知一定程度上激发了我对相关领域的研究。

同时这篇文章不仅研究了最新的技术（无线充电宝），还结合小样本学习这一重要的训练数据集包含有限信息的机器学习技术。在大多数机器学习应用中，输入更多的数据训练能使模型的预测效果更好。然而，小样本学习的目标是使用数量较少的训练集来构建准确的机器学习模型。论文提出的框架很好的利用了小样本学习来使用少量的数据信息，提高框架的自适应能力。这一优化思路有非常的研究意义，可以应用在其他领域的研究中。

在研究这篇论文的过程中，我产生过许多疑问，通过分析各类参考文献与资料最终解决，同时我也有了提高该攻击框架性能的其他思路，如多设备的协作学习，可以考虑结合其他设备或其他的侧信道来优化该攻击框架，提高其性能，适应更长距离和其他用户活动的识别。

于现实角度而已，阅读与分析该论文，一定程度上提高了我的英语能力，也

提高了我的文章分析能力与逻辑思维，翻译与原文都存在部分细微的逻辑不顺的问题，我结合上下文，并通过与队友的论坛与辩论，最终产生了合理的认知与理解。同时在分析文章内容时，我遇到了非常多不熟的技术与概念，大部分与机器学习相关，这加强了我相关方面的知识储备与理解。我在机器学习方面有了进一步的研究与进步。

分析论文并制作相关的报告，提高了我的核心提取能力，也帮助我熟悉了论文的写作过程，提高了我的各种办公能力，这无疑对我后续完成个人的研究有非常重要的意义。

论文围绕着无线充电宝中新的侧信道展开了阐述，通过分析这篇论文，我了解到其泄露用户隐私的原理，这也给予了我一定的警示，在使用前沿技术的过程中，往往可能存在不可知而普遍的隐私泄露问题，提醒我要提高保护隐私的意识。

综上所述，通过阅读这篇论文，我对无线充电宝及充电电源的工作原理，用户隐私泄露的原理有了进一步的了解，同时在小样本学习等机器学习专业的知识有了深入的理解，也给予了我相关的研究思路，我在该过程受益匪浅。

6. 参考文献

[1] Adafruit. 2021. Electret Microphone Amplifier - MAX9814 with Auto Gain Control. (2021). https://www.adafruit.com/product/1713.

[2] ANKER. 2020. Anker MagGo. (2020). https://us.anker.com/pages/maggo.

[3]appfigures.2021.Top Ranked iOS App Store Apps.(2021). https://appfigures.com/top-apps/ios-app-store/unitedstates/iphone/top-overall.

[4]Apple.2022. MagSafe Battery Pack. (2022). https://support.apple.com/kb/SP846?viewlocale=en_US&locale=en_US.

[5] Lejla Batina, Shivam Bhasin, Dirmanto Jap, and Stjepan Picek. 2019.CSI NN: Reverse engineering of neural network architectures through electromagnetic side channel. In Proceedings of the 28th USENIX Security Symposium. 515–532.

[6] Anouar Belahcen et al. 2004. Magnetoelasticity, magnetic forces and magnetostriction in electrical machines. Helsinki University of Technology.

[7] Belkin. 2022. Magnetic Wireless Power Bank 2.5K. (2022).https://www.belkin.com/us/chargers/wireless/boost-chargemagnetic-wireless-power-bank-2-5k/p/p-bpd002/.

[8] Jin Chen, Per Jönsson, Masayuki Tamura, Zhihui Gu, Bunkei Matsushita, and Lars Eklundh. 2004. A simple method for reconstructing a high-quality NDVI time-series data set based on the Savitzky–Golay filter. Remote sensing of Environment 91, 3-4 (2004), 332–344.

[9] Xiang Chen, Yiran Chen, Zhan Ma, and Felix CA Fernandes. 2013.How is energy consumed in smartphone display applications?. In Proceedings of the 14th Workshop on Mobile Computing Systems and Applications. 1–6.

[10] Yushi Cheng, Xiaoyu Ji, Wenyuan Xu, Hao Pan, Zhuangdi Zhu,Chuang-Wen You, Yi-Chao Chen, and Lili Qiu. 2019. Magattack: Guessing application launching and operation via smartphone. In Proceedings of the ACM Asia Conference on Computer and Communications Security(AsiaCCS). 283–294.

[11] Myeongwon Choi, Sangeun Oh, Insu Kim, and Hyosu Kim. 2022.MagSnoop: listening to sounds induced by magnetic field fluctuations to infer mobile payment tokens. In Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services (MobiSys). 409–421.

[12] Patrick Cronin, Xing Gao, Chengmo Yang, and Haining Wang. 2021.Charger-Surfing: Exploiting a Power Line Side-Channel for Smartphone Information Leakage. In Proceedings of the 30th USENIX Security Symposium. 681–698.

[13] Mian Dong and Lin Zhong. 2011. Chameleon: A color-adaptive web browser for mobile OLED displays. In Proceedings of the 9th International Conference on Mobile systems, Applications, and Services. 85–98.

[14] ElectronicWings. 2022. HMC5883L Magnetometer Module. (2022).https://www.electronicwings.com/sensors-modules/hmc5883lmagnetometer-module.

[15] Chelsea Finn, Pieter Abbeel, and Sergey Levine. 2017. Model-agnostic meta-learning for fast adaptation of deep networks. In Proceedings of the International Conference on Machine Learning (ICML). 1126–1135.

[16] Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Tromer, and Yuval Yarom. 2016. ECDSA key extraction from mobile devices via nonintrusive physical side channels. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS). 1626–1638.

[17] Spherical Insights. 2022. Global Power Bank Rental Services Market Size, Share and Trends, Analysis and Forecast 2021–2030.(2022). https://www.sphericalinsights.com/reports/power-bankrental-services-market.

[18] Hassan Ismail Fawaz, Germain Forestier, Jonathan Weber, Lhassane Idoumghar, and Pierre-Alain Muller. 2019. Deep learning for time series classification: a review. Data mining and knowledge discovery 33, 4 (2019), 917–963.

[19] Wenqiang Jin, Srinivasan Murali, Huadi Zhu, and Ming Li. [n. d.].Periscope: A Keystroke Inference Attack Using Human Coupled Electromagnetic Emanations. In

Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS).

[20] David M Kreindler and Charles J Lumsden. 2016. The effects of the irregular sample and missing data in time series analysis. In Nonlinear Dynamical Systems Analysis for the Behavioral Sciences Using Real Data.CRC Press, 149–172.

[21] Alexander S La Cour, Khurram K Afridi, and G Edward Suh. 2021.Wireless Charging Power Side-Channel Attacks. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security(CCS). 651–665.

[22] Mengyuan Li, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang, YaoLiu, and Na Ruan. 2016. When CSI meets public WiFi: inferring your mobile phone password via WiFi signals. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS).1068–1079.

[23] Qianru Liao, Yongzhi Huang, Yandao Huang, Yuheng Zhong, HuitongJin, and Kaishun Wu. 2022. MagEar: Eavesdropping via audio recovery using magnetic side channel. In Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services(MobiSys). 371–383.

[24] Jianwei Liu, Xiang Zou, Leqi Zhao, Yusheng Tao, Sideng Hu, Jinsong Han, and Kui Ren. 2022. Privacy Leakage in Wireless Charging. IEEE Transactions on Dependable and Secure Computing (2022).

[25] Zhuoran Liu, Niels Samwel, Léo Weissbart, Zhengyu Zhao, Dirk Lauret, Lejla Batina, and Martha Larson. 2020. Screen gleaning: A screen reading TEMPEST attack on mobile devices exploiting an electromagnetic side channel. Proceedings of the Network and Distributed System Security Symposium (NDSS).

[26] CrioSoft LLC. 2022. Amperes - battery charge info. (2022). https://apps.apple.com/us/app/amperes-battery-charge-info/id1245475416.

[27] EGO INNOVATION LTD. 2021. EGO MAGPOWER Gen.2 6000mAh 15W magsafe powerbank. (2021).https://www.egoshop.co/en/products/ego-magpower-15w-magsafe-6000mah-powerbank-1.

[28] Danyue Ma, Jixi Lu, Xiujie Fang, Ke Yang, Kun Wang, Ning Zhang, Bangcheng Han, and Ming Ding. 2021. Parameter modeling analysis of a cylindrical ferrite magnetic shield to reduce magnetic noise. IEEE Transactions on Industrial Electronics 69, 1 (2021), 991–998.

[29] Henrique Teles Maia, Chang Xiao, Dingzeyu Li, Eitan Grinspun, and Changxi Zheng. 2021. Can one hear the shape of a neural network?:Snooping the GPU via Magnetic Side Channel. (2021).

[30] Francisco Javier Ordóñez Morales and Daniel Roggen. 2016. Deep convolutional feature transfer across mobile activity recognition domains, sensor modalities and locations. In Proceedings of the 2016 ACM International Symposium on Wearable Computers. 92–99.

[31] Arduino Nano.2022.Arduino Nano Document.(2022). https://docs.arduino.cc/hardware/nano.

[32] Tao Ni, Yongliang Chen, Keqi Song, and Weitao Xu. 2021. A Simple and Fast Human Activity Recognition System Using Radio Frequency Energy Harvesting. In Adjunct Proceedings of the 2021 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2021 ACM International Symposium on Wearable Computers. 666–671.

[33] Tao Ni, Guohao Lan, Jia Wang, Qingchuan Zhao, and Weitao Xu.2023. Eavesdropping Mobile App Activity via Radio-Frequency Energy Harvesting. In Proceedings of the 32nd USENIX Security Symposium.

[34] Rui Ning, Cong Wang, ChunSheng Xin, Jiang Li, and Hongyi Wu. 2018. Deepmag: Sniffing mobile apps in magnetic field through deep convolutional neural networks. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom).IEEE, 1–10.

[35] Rukundo Olivier and Cao Hanqiang. 2012. Nearest Neighbor Value Interpolation. International Journal of Advanced Computer Science and Applications 3, 4 (2012). https://doi.org/10.14569/ijacsa.2012.030405

[36] Hao Pan, Lanqing Yang, Honglu Li, Chuang-Wen You, Xiaoyu Ji, YiChao Chen, Zhenxian Hu, and Guangtao Xue. 2021. MagThief: Stealing private app usage data on mobile devices via built-in magnetometer. In Proceedings of the 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). IEEE, 1–9.

[37] US Energy Products. 2023. US Energy Products (AD3) Reflective Foam Insulation Shield.(2023).https://www.amazon.com/US-EnergyProducts-Reflective-Insulation/dp/B07R1S669V.

[38] J Ross Quinlan. 1996. Learning decision tree classifiers. ACM Computing Surveys (CSUR) 28, 1 (1996), 71–72.

[39] RIGOL. 2022. Rigol DS1052E. (2022). https://www.batronix.com/shop/oscilloscopes/Rigol-DS1052E.html.

[40] Seyed Ali Rokni, Marjan Nourollahi, and Hassan Ghasemzadeh. 2018. Personalized human activity recognition using convolutional neural networks. In

Proceedings of the AAAI Conference on Artificial Intelligence, Vol. 32.

[41] Md Sahidullah and Goutam Saha. 2012. Design, analysis and experimental evaluation of block based transformation in MFCC computation for speaker recognition. Speech communication 54, 4 (2012), 543–565.

[42] Dries Van Wageningen and Toine Staring. 2010. The Qi wireless power standard. In Proceedings of 14th International Power Electronics and Motion Control Conference (EPE-PEMC). IEEE, S15–25.

[43] Martin Vuagnoux and Sylvain Pasini. 2009. Compromising electromagnetic emanations of wired and wireless keyboards.. In Proceedings of the USENIX Security Symposium, Vol. 8. 1–16.

[44] Jindong Wang, Vincent W Zheng, Yiqiang Chen, and Meiyu Huang.2018. Deep transfer learning for cross-domain activity recognition. In Proceedings of the 3rd International Conference on Crowd Science and Engineering. 1–8.

[45] Yuanda Wang, Hanqing Guo, and Qiben Yan. 2022. GhostTalk: Interactive Attack on Smartphone Voice System Through Power Line. In Proceedings of the Network and Distributed System Security Symposium(NDSS).

[46] Wikipedia. 2022. Inductive charging. (2022). https://en.wikipedia.org/wiki/Inductive_charging.

[47] Yi Wu, Zhuohang Li, Nicholas Van Nostrand, and Jian Liu. 2021. Time to Rethink the Design of Qi Standard? Security and Privacy Vulnerability Analysis of Qi Wireless Charging. In Proceedings of the Annual Computer Security Applications Conference (ACSAC). 916–929.

[48] Boyuan Yang, Ruirong Chen, Kai Huang, Jun Yang, and Wei Gao. 2022.Eavesdropping user credentials via GPU side channels on smartphones. In Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS).285–299.

[49] Shengqi Yang, Wayne Wolf, Narayanan Vijaykrishnan, Dimitrios NSerpanos, and Yuan Xie. 2005. Power attack resistant cryptosystem design: A dynamic voltage and frequency switching approach. In Design, Automation and Test in Europe. IEEE, 64–69.

[50] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. 2017. Dolphinattack: Inaudible voice commands. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS). 103–117.

7. 附录

其他不能归属上面章节的内容，如果没有可不填写。