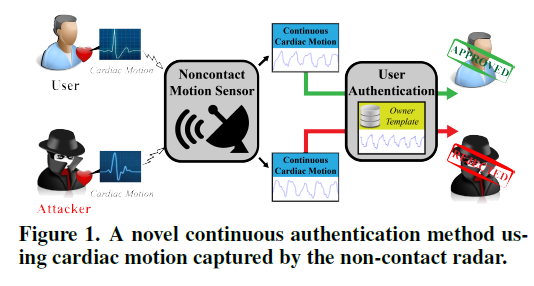
心跳识别黑科技

纽约州立大学布法罗分校和德克萨斯理工大学的研究人员在10月即将召开的MobileCom17上发表了一篇题为“Cardiac Scan: A Non-Contact and Continuous Heart-Based User Authentication System”的论文，讲述了如何根据心跳来进行持续身份认证。

心跳跟指纹、虹膜一样都属于人体的生物特征，具有唯一性，因此可以用于身份识别。



**Cardiac Scan 的几个特性**：

Intrinsic liveness. 需要鉴别给属性是否来自于真实的用户，这可以预防重放攻击。

Unobtrusive Authentication. 用户正常状态下就可以进行验证，无须进行其他特定的操作。

Highly Secure.高安全性和唯一性，很难伪造或者盗取。

Cost-effective and Easy-to-Use. 一些生物特征的获取需要昂贵的专用设备，Cardiac Scan使用的是雷达感应器。

Resilient to Background Noise and Use Conditions. 面部识别等camera-based认证系统对噪声的要求较高。雷达感应器使用的是广播信号，抗干扰能力强。

**检测模型**：

Cardiac Motion是一种类由Cardiac muscle自兴奋产生的3D自动的心脏变形。更重要的是cardiac authentication是非接触式的，实验中使用Doppler radar motion sensor来测量心跳在科学研究中很普遍。本项目中使用的基带信号。

智能的DC CW雷达感应器，实时信号处理和混合的信号设计。

与心跳无关的其他身体部分产生的DC偏移值很容易会产生干扰信号。

Smart DC tuning. 双DC自适应调谐架构包括RF粗调谐和基带微调谐。

RF粗调谐。电子控制的相移和天线能够抵消反射带来的DC偏移，但是不能完全抵消DC偏移。

基带微调谐。可以动态调整放大器的偏压到一定的等级来保证一个最大的动态范围。

最优的运营商频率。测试了从2.4GHz到40GHz，因为超过40GHz会产生谐波干扰。

Radio signal processing scheme无线信号处理

目前用来测量心跳生物特征的方法有ECG，ECG主要是记录心脏的电活动。而非接触式的心跳特征直接来源于RF感应器。

预处理过程。降低心跳信号的噪音等级，噪音包裹低带部分，高带部分和其他。方法有1）one-pass noise reduction，如butterworth bandpass filter，2）adaptive noise canceling技术，如归一化最小均方自适应滤波器。

De-noising-Aware Radar Demodulation

多普勒雷达主要是用于速度检测，有低频率和静态的特点。所以需要提出一种新的信号解调过程。

**持续认证**

从心跳信号中进行特征提取，把周期性地信号序列分割成离散的帧。每个分割后的部分包含5个心跳运动阶段。

**基准方法**

基准方法提取内在的几何描述，例如时间、振幅、角度。基准点包含的应该的生物特征应该是唯一的，而且与感应器的位置、个人的心理状态等都有关系。非基准的方法聚焦与非物理的属性特征，难以反映心脏的本质的生物特征。

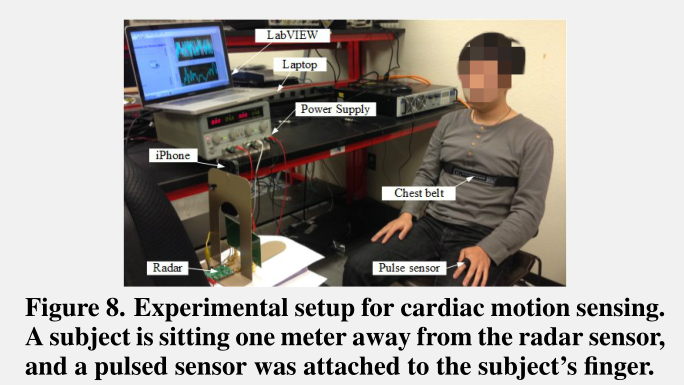
继续认证协议。静态认证易受到攻击。恶意用户可以在认证用户离开后，访问已经登录的系统，因此继续认证协议可以监控用户的特征，并周期性的进行再次认证来确保登录安全。

**持续认证场景**

可信用户在，authentic user登入系统后，在雷达感应器的检测范围内，Cardiac Scan能够检测心跳运动是否来自同一个人。如果来自同一个人，那么就没有中断地持续授权给该用户使用系统。如果连续两次发现不是可信用户，那么系统会登出该用户。并要求通过其他补充生物特征方法来进行鉴别，如PIN，指纹等。

可信用户离开，cardiac scan首先会检测用户是否登出系统和进行锁屏操作。如果进行了上述操作，那么就认为用户的行为是合理的；否则，还判定系统有非授权访问的风险。此时，根据安全策略，会进行形影的操作，如锁定会话，登出用户，通知管理员等。

攻击用户在，图7c中所示，系统在可信用户登入后，有非授权用户在场。这可能是可信用户被胁迫的攻击场景。此时，系统会把攻击用户隔离在系统之外，避免泄露敏感信息。



**潜在的漏洞研究**

心脏运动是不可见的，与其他的认证方法，如PIN、指纹等生物特征相比，可以提供更好的安全性。但是也可能受到direct或spoofing攻击。

1 replay攻击

使用生物特征进行认证的威胁在于，生物token可能会被非认证的第三方进行拦截和重放。与可见的生物特征相比，心跳信号的复制和伪造更加复杂，而且有动态性。然而，在一些极端情况下，仍然可能伪造心跳信号。

如， Eberz et al.[24]使用基于硬件的AWG任意波形产生器和基于AWG软件的计算机声卡来编码和模拟ECG信号来攻击ECG特征。在心跳运动感应中，攻击者也可能黑近数据库，获取心脏运动模型或者制作一样的心跳运动感应设备来提取用户的心跳信号。

2 anti-spoofing liveness artifacts

作者调研了一系列的反欺骗的方法来应对重放攻击。一种反欺骗的方法就是活性检测。因为攻击者很难同时模拟多个生理信号。本模型中我们也利用了心跳运动的活体特征的唯一性来应对攻击模型。首先，硬件方面。在cardiac scan中加入了多个辅助感应器，来检查对象的活体性。第二，就是利用软件方法。来源与活体的感应数据包含呼吸等重要特征和其他的运动特征。而这些运动特征是不保存在数据库作为证书的一部分，所以不能复制和模拟用来攻击。使用这些重要特征检测和运动特征，活性检测可以预防replay攻击。作者用促动器来模拟不同的移动幅度和频率来模拟心跳运动。所有的重放攻击都被活体检测模型识别并拒绝了。

