技术深耕 | 三星手机安全的秘密

三星 KNOX 是防御级移动安全平台 ,内置于三星的设备中。在开机出现三星 Logo 的同时，会同时出现 Secured By KNOX 提示，这表明该设备拥有 KNOX 的安全保护。

1．什么是 KNOX？

三星 KNOX 是一款基于 Android 平台的安全解决方案，通过物理手段和软件体系相结合的方式全方位增强安全性，从硬件到应用层都能提供最高层级的安全保护，同时完美兼容安卓及谷歌生态系统，为企业及员工个人带来行业领先的移动安全解决方案。

三星手机在工厂制造过程中，将强大的 KNOX 平台内置在三星手机的硬件与软件中，这让三星手机成为当前市场中最为可靠的设备。当手机处于关机状态时，所有的数据都会处于加密状态，加密的秘钥则存储在芯片的 TrustZone 中；一旦设备开始启动，KNOX 会检查加载的软件是否经过授权；在运行过程中，KNOX 会持续监测和保护操作系统内核，一旦发现被侵入，系统会自动锁定部分敏感的应用。

在 Gartner 的报告中，三星获得了几乎所有安全项目的 Strong 评价，同时也获得了各国政府和安全组织的认可(点击链接，查看详细报告)。

2．KNOX 的实现原理

KNOX 构建了一个多层的安全体系，从硬件层面开始，直到操作系统，会验证整个设备的

完整性，检测任何可能的入侵，保证用户的数据始终处于安全状态。

KNOX 使用全面的，基于硬件的可信环境解决安全问题，包括：Android 的安全增强功能、实时内核保护（RKP）、基于 TrustZone 的完整性测量架构、基于 TrustZone 的安全性服务、安全启动、可信启动和硬件信任根。

KNOX 的设计原理：

1．首先基于硬件建立一个值得信任的环境

2．一旦设备开始运行，则对这个环境进行维护，保证它一直处于信任的状态

3．并在需要的时候，通过证明设备的完整性来检验设备是可以被继续信任的。

2.1 基于硬件的可信环境

三星设备的可信环境是通过硬件来支撑的，主要包括以下硬件组件：

2.1.1 安全硬件

- **ARM TrustZone Secure World**

- Secure World 主要用于为高度敏感的软件创造运行环境。
- ARM TrustZone 硬件确保内存和标记为安全的组件（例如指纹阅读器）只能在安全的环境中访问。

- **Bootloader ROM**
  - 主引导加载程序（PBL，Primary Bootloader ）是引导过程中运行的第一段代码。为了防止篡改，PBL 保存在安全硬件的只读存储区域（ROM）中。设备硬件在引导时从 ROM 加载和运行 PBL，PBL 启动安全和受信任的引导过程。

2.1.2 硬件秘钥

- **Device-Unique Hardware Key (DUHK)**
  - 这是一个设备唯一的对称秘钥，用来把某些数据与特定的设备进行关联。这个秘钥只能通过硬件加密模块进行访问，任何软件都不能直接访问这个秘钥。通过这个秘钥加密的数据被关联到这台唯一的设备上，这些数据在任何其它的设备上都不能被解密。
- **Device Root Key (DRK)**
  - 这是一个设备唯一的非对称 RSA 秘钥，这个秘钥通过三星的根证书进行签名。这个秘钥被 DUHK 加密后，DRK 只能从安全世界(Secure World)内访问，并受 DUHK 保护。DRK 是信任根的重要部分，因为它会对设备中其它的证书进行签名。因为 DRK 是每台设备唯一的，它能通过签名，将数据与某台具体的设备相关联。
- **Samsung Secure Boot Key (SSBK)**
  - 这是一个非对称秘钥，用来对启动的各个软件组件进行签名。SSBK 的私有部分用

来对 Secondary Bootloder 和 App Bootloader 进行签名，SSBK 的公共部分在设备生产的时候，被存储在硬件中。启动过程中，会利用公钥来验证加载的软件是否是正规授权的软件。

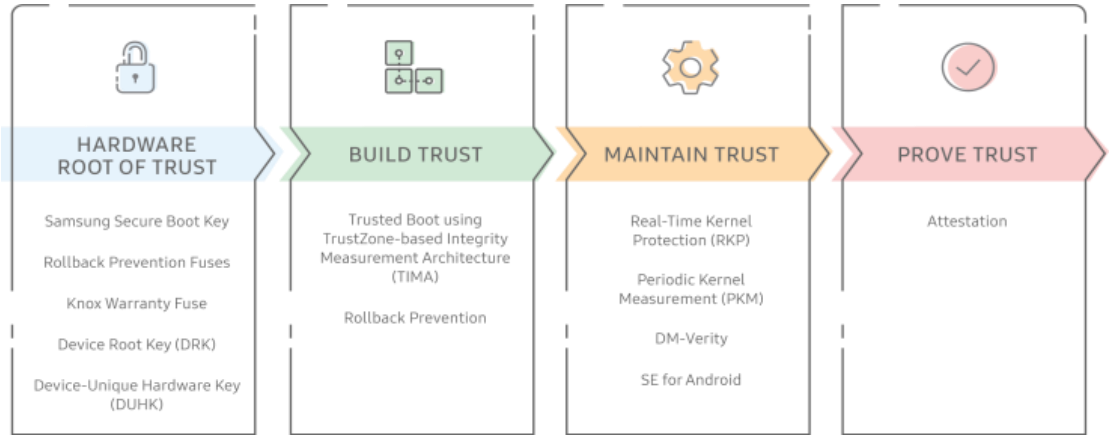
- **Samsung Attestation Key (SAK)**
  - 这是一个设备唯一的非对称秘钥，这个秘钥通过三星的根证书进行签名。在验证设备完整性的时候，需要产生一些数据，这个秘钥用来证明这些数据是来自于三星设备的 Trust Zone。SAK 采用了椭圆曲线数字签名算法，它与 RSA 类似，但是在同样的安全强度下，运行更快。

2.1.3 硬件熔断

- **Rollback Prevention (RP) fuses**
  - 表示该设备最小可接受的软件版本。老的软件版本通常有许多已知的漏洞，一旦这个值被设置，设备将不能使用老的软件版本，因为这些老的软件版本通常有许多软件漏洞。
- **Warranty fuse**
  - 这是一个一次性的熔断位，一旦监测到系统加载了非授权的软件，或者一些关键的安全特性被破坏，比如 SE Linux 被阻止，这个熔断位将会被设置。被设置后，设备敏感数据将不能被继续访问，设备的完整性检测将会失败。

2.2 KNOX 如何确保信任环境？

KNOX 通过独特的，行业领先的方式来构建值得信任的环境，包括以下四个步骤：



2.2.1 第一步：信任根（ROOT OF TRUST）

信任根（ROOT OF TRUST）是现代安全技术的基石。它从硬件级别开始，这项功能为设备增加了一个安全级别，使其难以被攻击，因为硬件比软件更难被改变。

信任根对许多复杂的安全问题给出了答案，比如，怎么知道启动的操作系统是否已被攻击？能否相信设备中存储的安全证书？能否确认系统软件是否被攻击者修改过？

信任根在三星设备中如何工作呢？

KNOX 的安全性开始于工厂，在设备生产的时候，通过硬件随机生成器，生成一个每台设备唯一的硬件秘钥（Device-Unique Hardware Key ，DUHK），因此，在你还没有使用手机的时候，KNOX 的安全性就开始发挥作用了。

紧接着，通过这个设备唯一的硬件秘钥（DUHK），产生并加密这台设备的根秘钥（Device

Root Key ，DRK）和三星的认证秘钥（Samsung Attestation Key ，SAK）。

一旦设备启动，三星使用安全启动秘钥（Samsung Secure Boot Key，SSBK）来验证每一个启动的软件，保证这些软件都是可信任的。软件的一个组成部分是 TrustZone，这是芯片的一部分，用来存储安全性要求极高的代码和数据，只有运行在 TrustZone 中的特权软件才可以访问上述那些秘钥。

在每个 KNOX 的功能运行前，软件都会进行检查，只有确认安全，才会允许这个功能运行。由于这一安全检查从第一次硬件检查开始，因此每个功能都受到了硬件信任根的保护。无论攻击者攻击的目标是哪一个层级，安全检查都会检测到这个攻击。

2.2.2 第二步：建立信任(BUILD TRUST)

可信启动（Trusted Boot）是 KNOX 平台的代表性功能，三星通过它实现了业界领先的启动保护技术。在未授权的 bootloader 损害移动设备前，可信启动就能够提前识别出这种危险。

在设备开始运行后，如果需要验证设备的完整性，可以采用 KNOX 的认证技术，KNOX 将会读取可信启动过程中收集的设备度量数据，对设备的完整性做一个基本的判定。

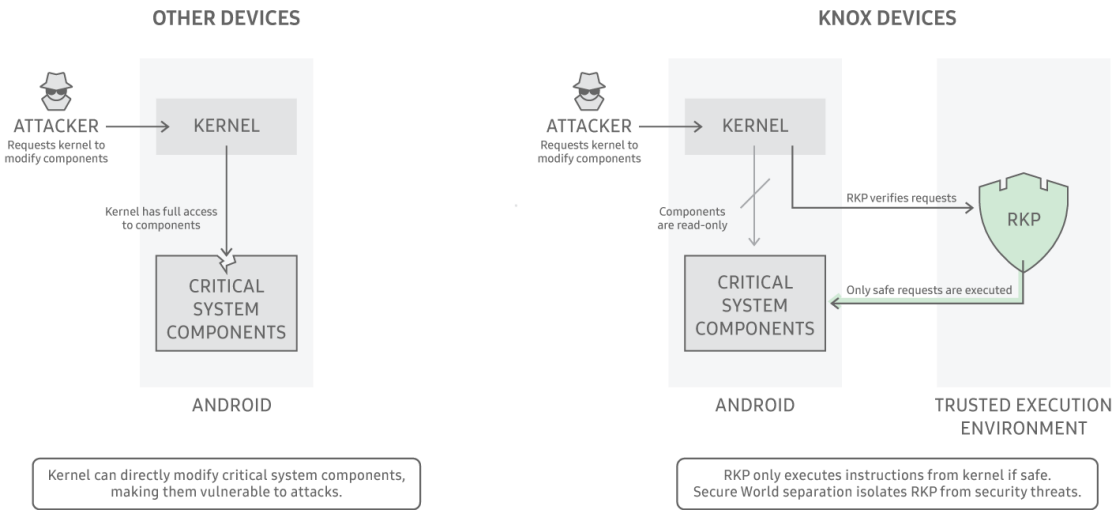
利用上述那些独特的秘钥和证书，KNOX 能够验证软件的每一个部分，如果某一个部分验证失败，KNOX 可以触发一个一次性的硬件熔断(one-time fuse，KNOX Warranty Bit)，从而记录着这一次的软件侵入，或者阻止更进一步的启动。KNOX Warranty Bits 被损坏的设备将不能使用某些 KNOX 的功能，比如三星智付（Samsung Pay），从而防止损害设备主人的利益。

在引入可信启动之前，三星也应用安全启动（secure boot）来阻止未经授权的操作系统在开机的时候启动。安全启动在每一个 bootloader 中实现，每一个 bootloader 都会验证下一个 bootloader 的签名，任何一步的验证失败，都会导致启动终止。安全启动在阻止未经授权的 bootloader 方面很有效，但是它不能对两个合法的版本做出区分，比如有一个软件版本存在已知的漏洞，另一个软件版本针对这个漏洞打了 patch，但是这两个版本都有合法的签名，安全启动无法对这两个版本做出区分。为了解决这种问题，三星引入了可信启动，来突破这种限制。

2.2.3 第三步：维护信任（MAITAIN TRUST）

在启动中被验证的软件依然有可能被用户修改，比如下载和安装恶意的软件。KNOX 保证系统软件一旦被加载和启动，就不会被修改。KNOX 采用一系列的技术来保护操作系统内核，阻止 ROOT，这能保护系统进程和资源免受恶意的攻击。

为了维护信任，三星导入了内核实时检测（Real-time Kernel Protection ，RKP）技术。**RKP 是三星的专利技术**，代表了业界在内核保护方面的最高水平。RKP 在设备启动的时候就开始运行，不需要任何的设置。



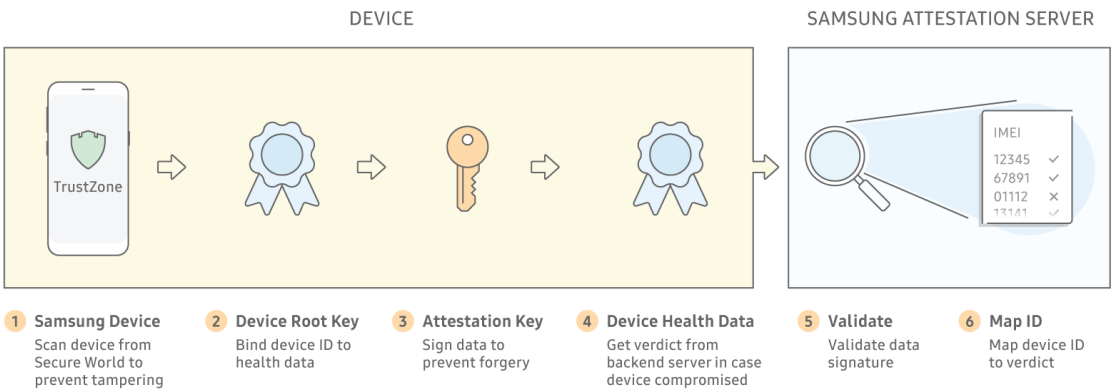
作为 KNOX 安全的一部分，RKP 在一个隔离的环境里运行一个安全监测器。取决于设备型号，这个隔离环境可能是一个专用的管理程序，也可能是硬件支持的安全空间，比如 ARM TrustZone。

这项独特的技术能够防止绝大部分的内核攻击。RKP 会保护内核代码和数据，防止被篡改。RKP 同时保护了内核的控制流，它防止了 ROP(Return Oriented Programming)和 JOP（Jump-Oriented Programming）攻击，这些攻击会重用现有的内核逻辑，将内核原有的代码进行拼凑达到攻击的目的。

2.2.4 第四步：认证信任（PROVE TRUST）

在设备运行过程中，你可能想查看你的设备是否曾经被非法侵入过，然后你可以决定是否继续信任你的设备，决定是否继续处理敏感数据。KNOX 通过提供认证机制来让你处理这种情况。

当你对设备进行健康检查的时候，恶意软件可能会截获或篡改检查结果，让你误以为你的设备是安全的，但实际上设备已经被入侵了。KNOX 使用硬件支持的可信环境来检查和报告被入侵的设备。



因为 DRK（Device Root Key）对每一台设备是唯一的，它能通过签名将数据与设备绑定在一起。SAK（Samsung Attestation Key）对要校验的数据进行签名，以证明这些数据来源于 TrustZone 的安全空间。

从基于硬件的信任根开始，KNOX 通过建立信任，维护信任，认证信任一起工作，以确保设备在启动和操作期间设备的完整性。KNOX 的最终目的是提供一个值得用户信任的平台，以满足用户和大小企业的安全需求。

3．联系我们

如果您对三星 KNOX 有任何问题和想法欢迎发邮件到：

rdtpservice@samsung.com

邮件主题：三星 KNOX

后续我们会分享更多技术内容，敬请期待。

感谢您的关注和参与！