Android:
Is It Secure Enough?

sierraware

Android (in)Security

- Up until version 4.2, Android offered very little security
  - Apps can access data and functions in other apps
  - Malware has proliferated
    - 12,000 unique strains of malware found for mobile devices, mostly Android

Source: McAfee Threat Report, 2Q 2012

sierraware

Security Enhanced Android

- In version 4.2, Google added SE Linux capabilities to Android
- SE Linux addressed major gaps
  - Prevents privilege escalation by apps
  - Prevents bypass of security functions
  - Avoid data leakage from apps
  - Protects data from being accessed by other applications

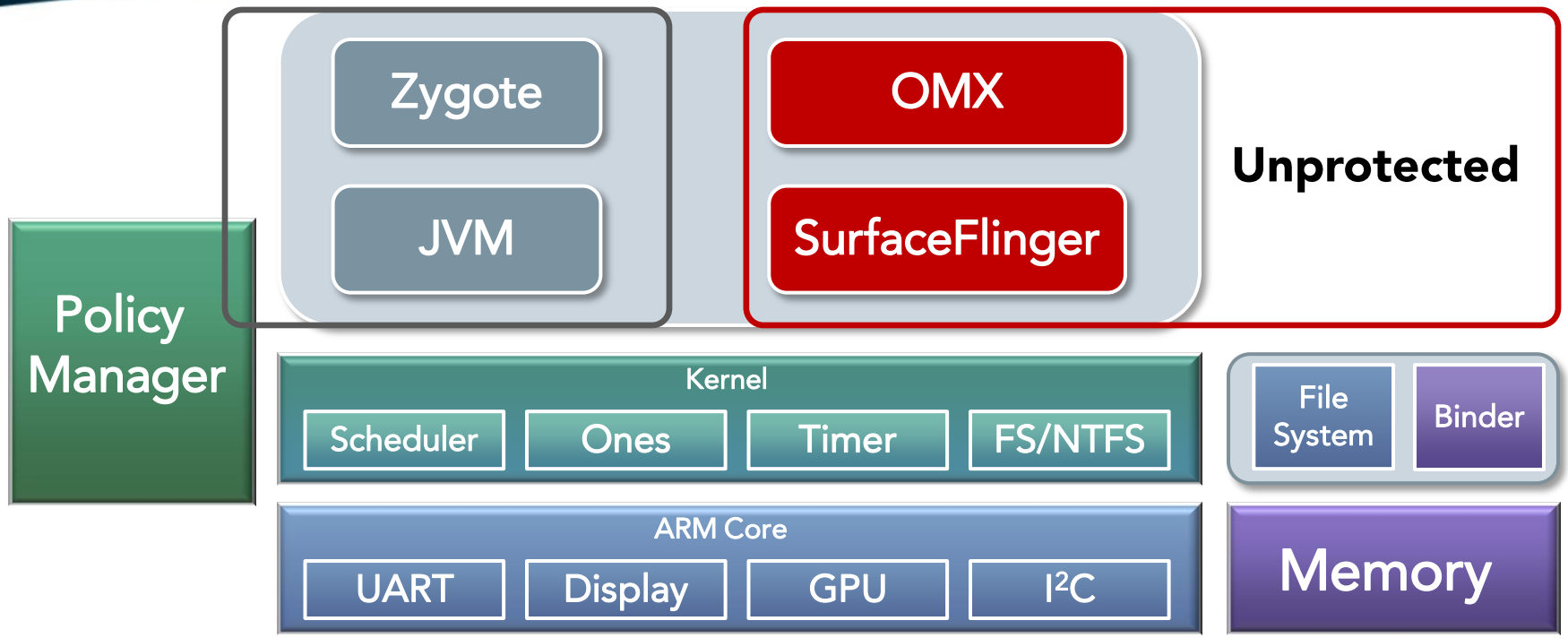
sierraware

Are We Secure Yet?

- Security enhancements make it much more difficult to hack Android, but…

sierraware

SE Android Partial Coverage



- Policy Manager does not protect SurfaceFlinger, which helps render images to the screen

sierraware

Impact of Partial Coverage

- DRM-managed content cannot be secured without protecting SurfaceFlinger
  - Hackers could just capture raw content sent to SurfaceFlinger
- Even if Google fully implements SELinux controls across all user space apps later, hackers can disable the Policy Manager

Hacking SE Android

Linux » Linux Kernel : Security Vulnerabilities (CVSS score between 7 and 7.99)

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : Cve Number Descending Cve Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **215** Page : 1 (This Page) 2 3 4 5

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Confidentiality	Integrity	Availability
1	CVE-2012-3412	189		DoS	2012-10-03	2012-10-30	7.8	None	Remote	Low	Not required	None	None	Complete
The sfc (aka Solarflare Solarstorm) driver in the Linux kernel before 3.2.30 allows remote attackers to cause a denial of service (DMA descriptor consumption and network-controller outage) via crafted TCP packets that trigger a small MSS value.														
2	CVE-2012-3400	119		DoS Overflow	2012-10-03	2012-10-30	7.6	None	Remote	High	Not required	Complete	Complete	Complete
Heap-based buffer overflow in the udf_load_logicalvol function in fs/udf/super.c in the Linux kernel before 3.4.5 allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted UDF filesystem.														
3	CVE-2012-2744			DoS	2012-08-09	2012-11-06	7.8	None	Remote	Low	Not required	None	None	Complete
net/ipv6/netfilter/nf_conntrack_reasm.c in the Linux kernel before 2.6.34, when the nf_conntrack_ipv6 module is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via certain types of fragmented IPv6 packets.														
4	CVE-2012-2319	264		Overflow +Priv	2012-05-17	2012-05-17	7.2	None	Local	Low	Not required	Complete	Complete	Complete
Multiple buffer overflows in the hfsplus filesystem implementation in the Linux kernel before 3.3.5 allow local users to gain privileges via a crafted HFS plus filesystem, a related issue to CVE-2009-4020.														
5	CVE-2012-2136	20		DoS Overflow +Priv	2012-08-09	2012-11-06	7.2	None	Local	Low	Not required	Complete	Complete	Complete
The sock_alloc_send_pskb function in net/core/sock.c in the Linux kernel before 3.4.5 does not properly validate a certain length value, which allows local users to cause a denial of service (heap-based buffer overflow and system crash) or possibly gain privileges by leveraging access to a TUN/TAP device.														
6	CVE-2012-2123	264		Bypass	2012-05-17	2012-10-30	7.2	None	Local	Low	Not required	Complete	Complete	Complete
The cap_bprm_set_creds function in security/commoncap.c in the Linux kernel before 3.3.3 does not properly handle the use of file system capabilities (aka fcaps) for implementing a privileged executable file, which allows local users to bypass intended personality restrictions via a crafted application, as demonstrated by an attack that uses a parent process to disable ASLR.														
7	CVE-2012-2100	189		DoS	2012-07-03	2012-08-13	7.1	None	Remote	Medium	Not required	None	None	Complete
The ext4_fill_flex_info function in fs/ext4/super.c in the Linux kernel before 3.2.2, on the x86 platform and unspecified other platforms, allows user-assisted remote attackers to trigger inconsistent filesystem-groups data and possibly cause a denial of service via a malformed ext4 filesystem containing a super block with a large FLEX_BG group size (aka s_log_groups_per_flex value). NOTE: this														

- Hackers can exploit Linux kernel flaws to gain control and disable Policy Management

sierraware

The Bad News

- SE Android still has huge holes
  - Not all user space apps are protected
  - Hackers can exploit zero-day flaws or escalate privileges to circumvent policy management
- Apps like HD video & mobile payment make hacking phones more lucrative
  - More attacks and attack toolkits
  - One attack could expose millions of devices

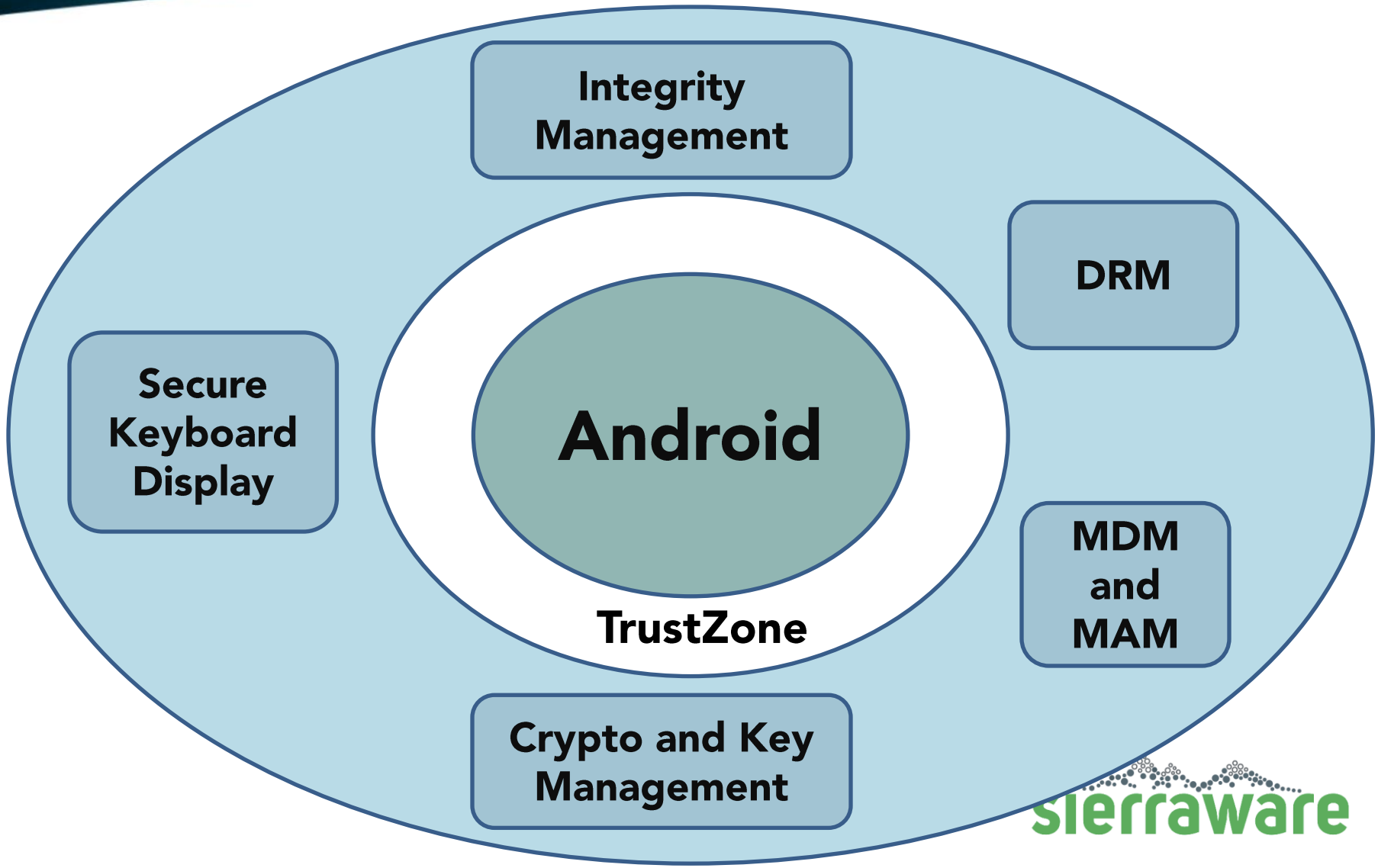
sierraware

How Can We Secure Android?

- Solution:
  - Create a hardened operating system outside of Android using ARM TrustZone
  - Secure OS
    - Cannot be compromised with malware rootkits
    - Protects sensitive data and applications like device keys, crypto keys, HDCP keys
    - Provides tamper-proof environment for integrity management and AV software

sierraware

Secure Architecture



sierraware

Is Hash-based Rootkit Scanning Enough?

- Hacks can come from network, from internal vulnerabilities
- Scanners themselves can be compromised
- Shortcoming with signatures
  - Challenging to store a huge signature database
  - Roaming and limited Internet access makes signature updates prohibitively expensive
  - Malware morphs continuously, rendering signature detection useless
    - Android 4.2's built-in malware scanner detects only 15% of threats

sierraware

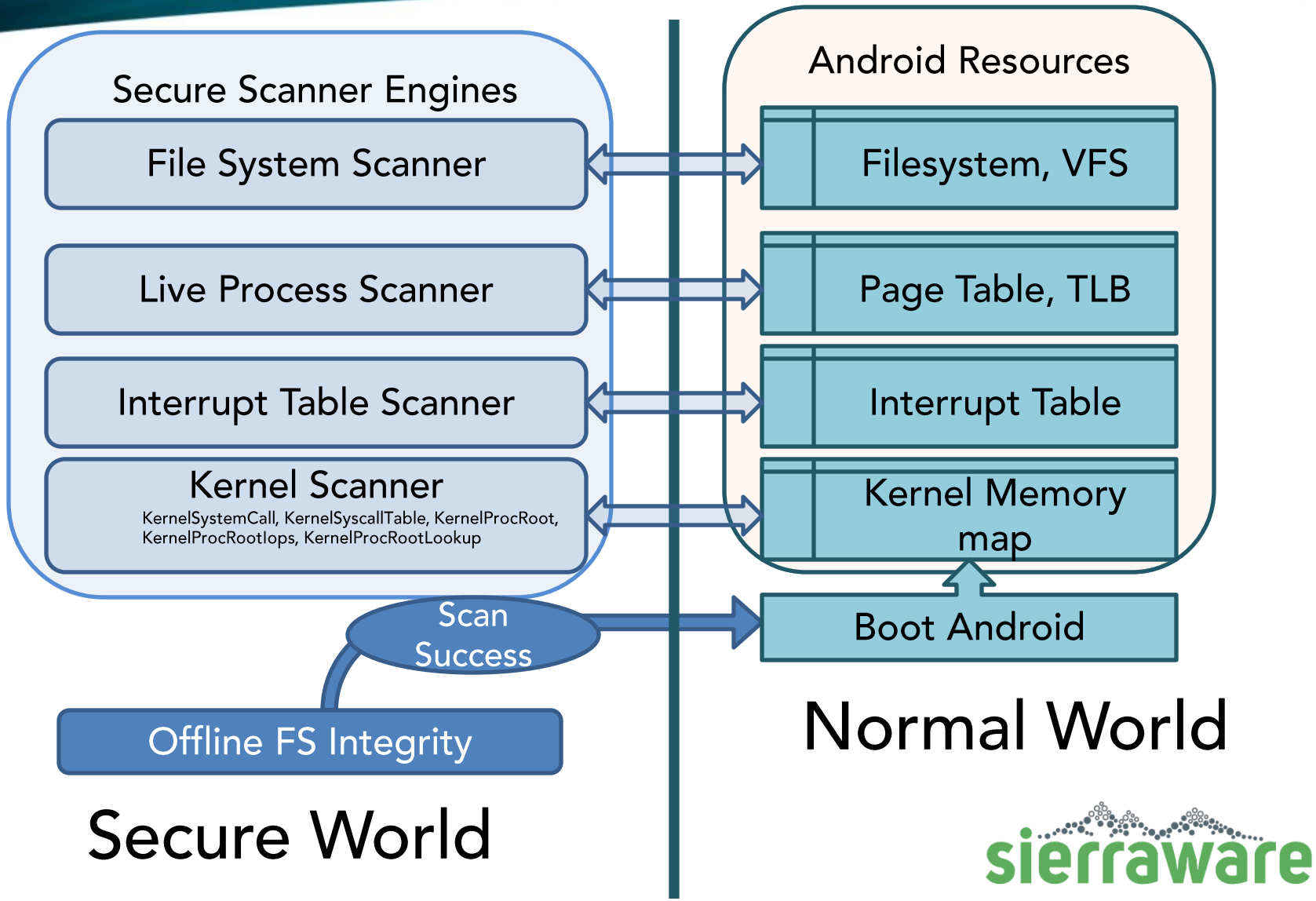
Integrity Management

Comprehensive integrity management requires:

- Offline File system scanner
- Live Application Scanner Engine
- Kernel Scanner
- Keylogger and Sniffer Scanners

sierraware

Architecture



Kernel Scanner

Kernel can't be monitored with simple Checksum

Integrity checks for rootkits and kernel hacks requires:

- Monitor Syscall interrupt and interrupt handler to ensure that core syscalls are not tampered with
- Code Segment validation of all syscalls to validate that there is no malicious code is injected inside the kernel
- Scan filesystem inode table to detect root kits like 'adore-ng'; there are some root kits that over ride the VFS layer than the syscall layer

sierraware

Security Solutions from Sierraware

Sierraware offers:

- SierraTEE, a Trusted Execution Environment for ARM architectures
  - Dual licensed: GNU GPL and commercial licenses
- Integrity Management
  - Live and offline file and kernel scanners
  - Keylogger and sniffer scanners
  - Developed for the SierraTEE secure OS

sierraware

For more information, visit
www.sierraware.com