VSRC2017城市沙龙

基于linux的嵌入式设备漏洞自动化分析

VSRC 2017-07-29

峙酿edwardz

246003@qq.com

唯品会安全应急响应中心

关于我

峙酿edwardz

华南理工

Kap0k

密码学

密码算法分析

密码电路设计

懂一点

Web安全

二进制安全

硬件安全

漏洞自动化分析

AEG

CGC

DARPA

人工智能 vs 人

人工智能国际网络攻防竞赛


wemo


THE INTERNET of
THINGS


nest
HEATING
68

家用路由器

家家户户

小型办公室

家用网络的第一道防线

十年不换 少更新

无杀毒软件

安全问题多 难以分析

Linux


CISCO


TP-LINK®
The Reliable Choice


VSRC


D-Link®
Building Networks for People


LINKSYS


net-core 磊科


Tenda®


NETGEAR®

固件

调试方式

硬件

软件

文件系统: Squash JFFS Cramfs

架构：ARM MIPS X86…..

难以分析：

无直接调试接口

种类多、标准不一；难以大规模分析

Avatar: A framework to support dynamic security analysis of embedded systems' firmwares

A large-scale analysis of the security of embedded firmwares

FIRMADYNE

FIRMADYNE

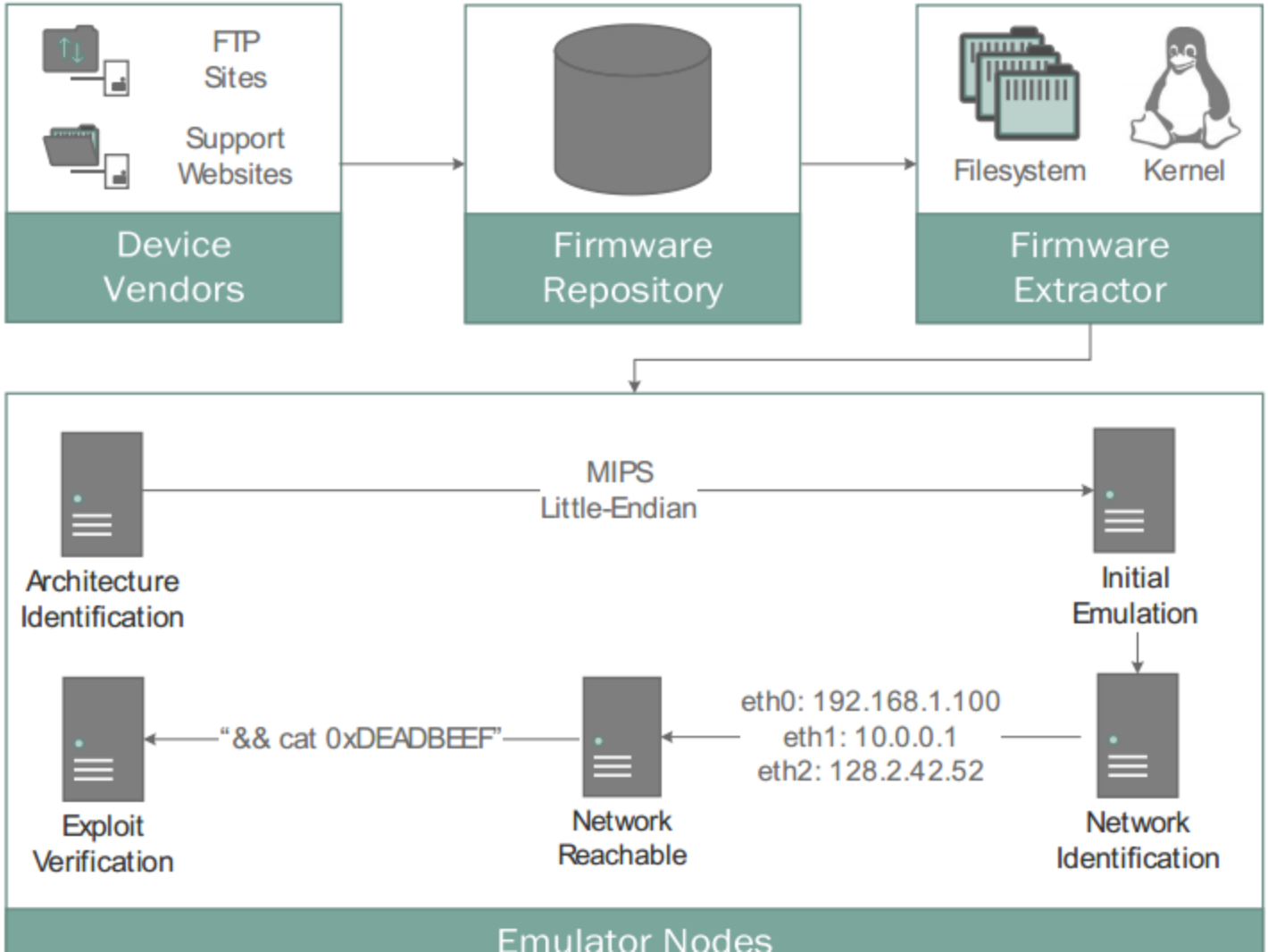
嵌入式Linux系统仿真

大规模动态分析

工具集

流程：

- **固件提取**
- **仿真器运行**
- **安全性测试（metasploits）**


FTP Sites
Support Websites
Device Vendors
Firmware Repository
Filesystem
Kernel
Firmware Extractor
MIPS Little-Endian
Architecture Identification
Initial Emulation
eth0: 192.168.1.100
eth1: 10.0.0.1
eth2: 128.2.42.52
"&& cat 0xDEADBEEF"
Exploit Verification
Network Reachable
Network Identification
Emulator Nodes

漏洞

信息泄露

命令执行

内存破坏

Xss CSRF

Tp-link D-link 电信天翼modern 斐讯 华硕等厂家二十多个安全漏洞

存在问题

VSRC

大量固件无法仿真

主要是利用已知payload

大规模 vs 精细化

下一步： fuzz+符号执行

攻击链

浏览器

网页挂马 + xss + 命令执行

直接控制路由器

fmk、patch sysupgrade

u-boot

factory-boot

永久控制路由器

永久监控

IOT安全

VSRC

安全问题多

不透明

二进制代码

缓解措施少

无处不在

感谢聆听

—

THANKS!

SRC
唯品会安全应急响应中心