



第四届全国网络与信息安全防护峰会

基于固件的计算机攻击与防护

孙亮

中电科技（北京）有限公司

目 次

一、 固件安全隐患分析

二、 固件攻击实例介绍

三、 固件安全防护方法

目 次

一、 固件安全隐患分析

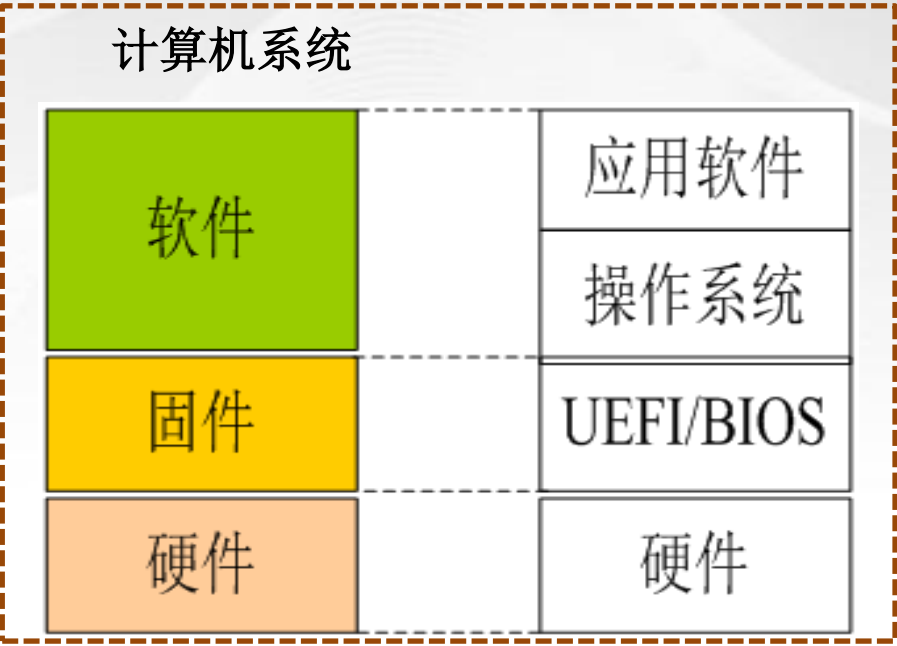
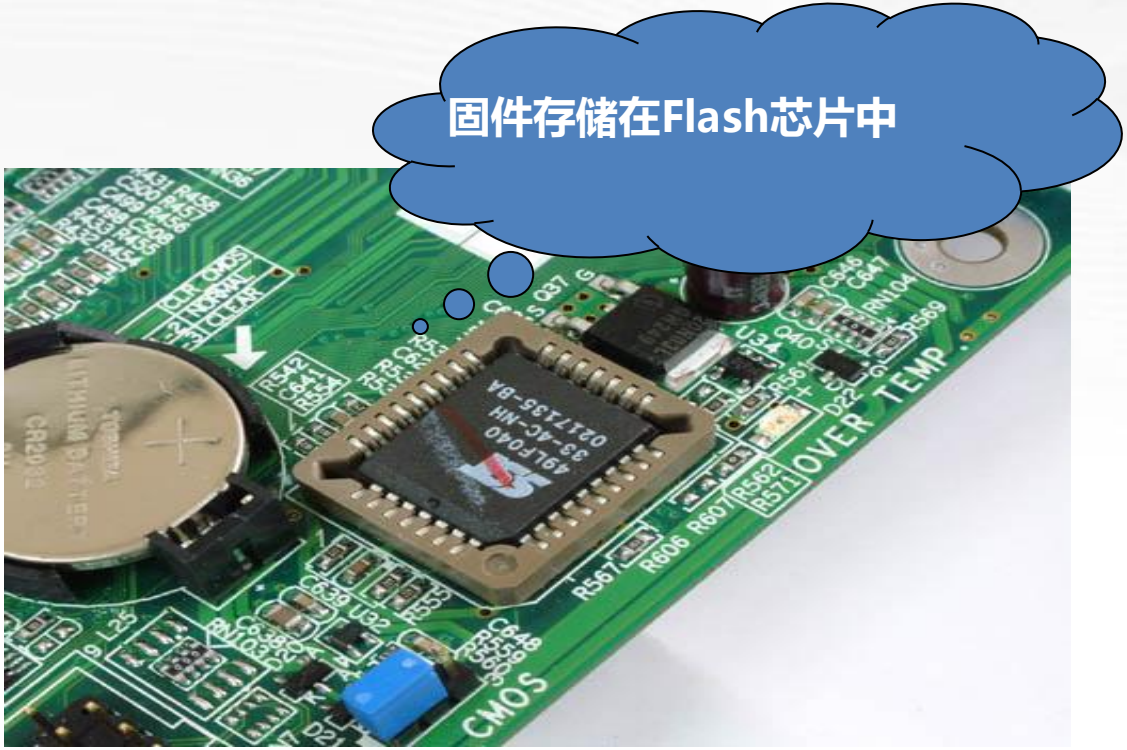
二、 固件攻击实例介绍

三、 固件安全防护方法

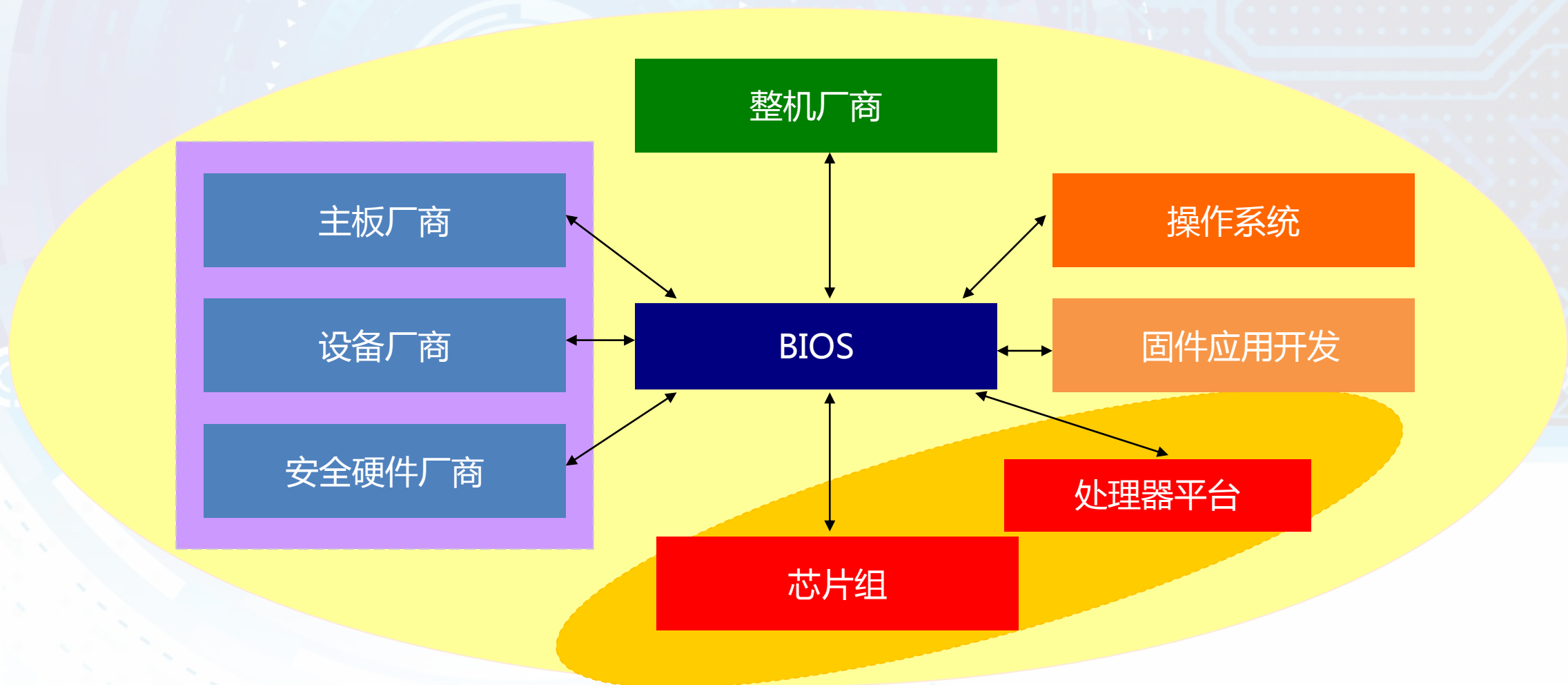
1. 固件和BIOS介绍

固件是固化在Flash芯片中的软件程序。

计算机中**最重要的固件是BIOS**。用于初始化硬件、启动操作系统和管理 计算平台资源，是连接计算机基础硬件和系统软件的桥梁。



2. BIOS的关联性和开放性



引申

固件屏蔽硬件细节，提供了开放的接口。

3. BIOS特点

BIOS的几个特征：

可软件刷写

- 可以通过软件方法对BIOS芯片进行擦除和刷写

具有高权限

- 从上电到操作系统运行前，BIOS具有系统高权限
- 操作系统运行时，BIOS可进入系统管理模式SMM

可操作硬件

- 能够对硬件进行初始化、配置和操作

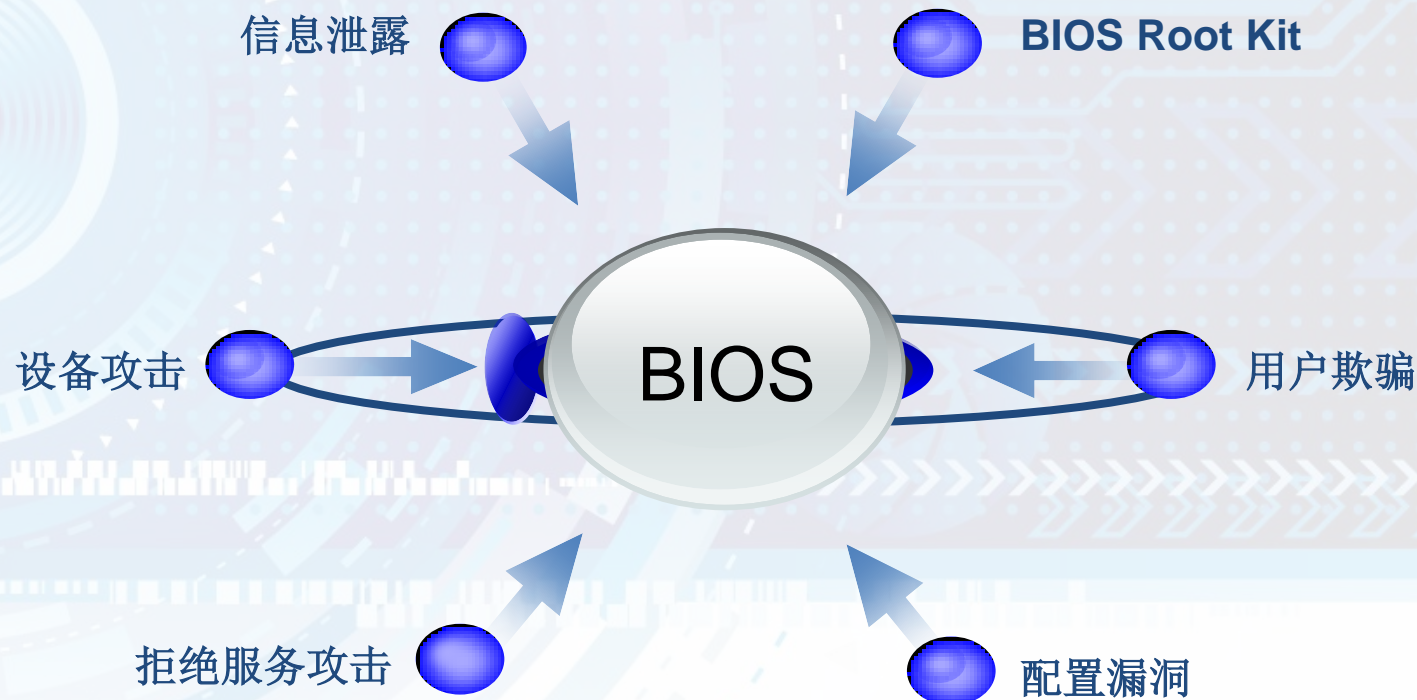
可访问网络

- BIOS可内嵌网络协议栈

4. BIOS安全隐患 (1)

特征

- 可软件刷写
- 具有高权限
- 可操作硬件
- 可访问网络

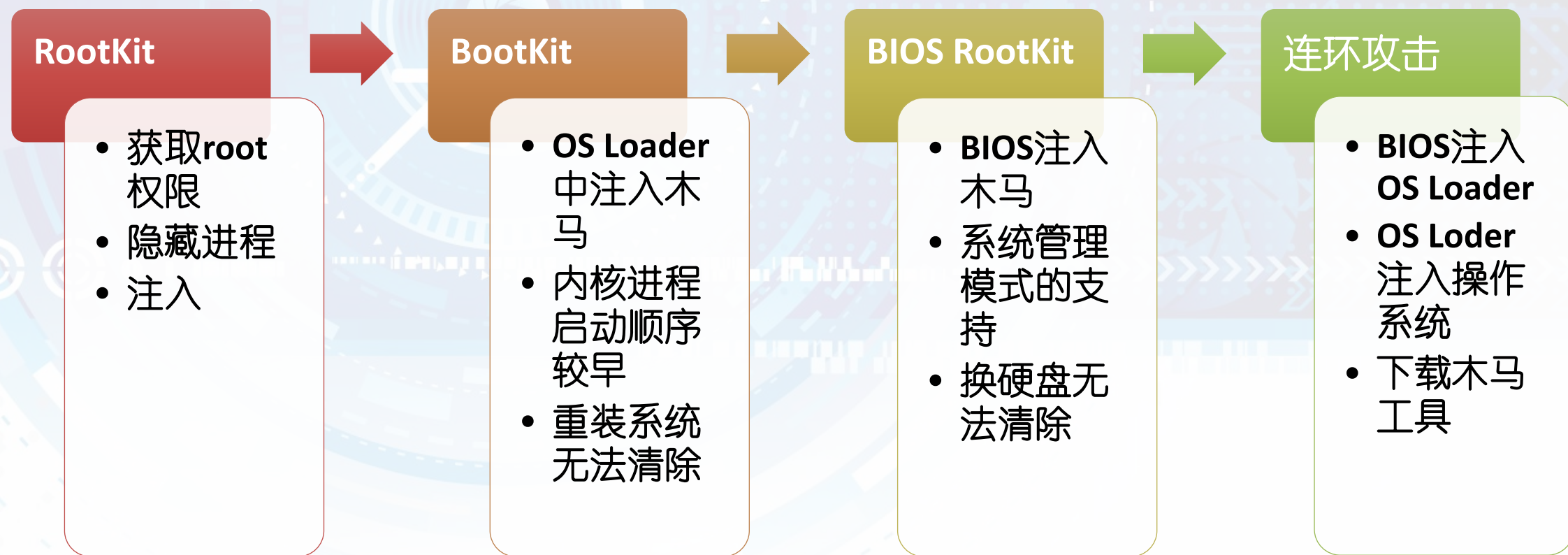


- ✦ 硬盘上看不见
- ✦ 操作系统中找不到
- ✦ 传统查杀毒软件杀不掉
- ✦ 重装系统或更换硬盘清不了

针对固件的攻击难以检测和清除

4. BIOS安全隐患 (2)

BIOS RootKit攻击方式的演变



引申

不易发现、不易清除。

4. BIOS安全隐患 (3)

BIOS其他安全隐患

拒绝服务攻击

- 对BIOS本身进行破坏
- 对OSLoader进行破坏
- 其他

信息泄露

- 键盘监听
- 屏幕监视
- 数据盗窃

设备攻击

- 更改电压
- 更改电流
- 更改频率

配置漏洞

- NetBIOS

用户欺骗

- 旁路操作系统

目 次

一、 固件安全隐患分析

二、 固件攻击实例介绍

三、 固件安全防护方法

1. 固件攻击实例（1）

Implementing and Detecting an ACPI BIOS Rootkit



John Heasman

NGS Consulting

1. 固件攻击实例（2）

Battery Firmware Hacking

Inside the innards of a Smart Battery

Charlie Miller
Accuvant Labs
charlie.miller.com
Twitter: 0xcharlie

1. 固件攻击实例（3）



1. 固件攻击实例 (4)

**瑞星**
WWW.RISING.COM.CN



瑞星香港信息
安全资讯网站

病毒信息

频道首页 | 病毒知识 | 反病毒基地 | **病毒医院** | 病毒 FAQ | 病毒资料库

[>> 宏病毒专科](#)
[>> **CIH病毒专科**](#)
[>> 网络病毒专科](#)
[>> 木马病毒专科](#)
[>> 返回上级](#)

小知识



CIH首先在台湾被发现, 根据台北官方的报告, 计算机病毒是由24岁的陈盈豪 (Chen Ing-Halu) 编制的. 由于其名字第一个字母分别为C、I、H, 所以这可能是计算机病毒名称的由来。

CIH病毒
是迄今为止发现的最阴险的病毒之一。它发作时不仅破坏硬盘的引导区和分区表, 而且破坏计算机系统flashBIOS芯片中的系统程序, 导致主板损坏。CIH病毒是发现的首例直接破坏计算机系统硬件的病毒。

CIH 病毒专科

流行病展示台

- “圣诞CIH”病毒解析
- 比CIH更强的PE_Zerg病毒
- 圣诞节谨防 PE_KRIZ. 4029病毒
- 12月25日当心: W32/Kriz. 3862发作
- CIH病毒回顾

诊断方案

- 瑞星提供的CIH病毒修复工具
- 数据恢复的方法
- 判断是否感染CIH病毒的三种方法

病因分析

CIH病毒发展历程
CIH的特征及行踪
CIH病毒原理的应用——物理内存的读写
病毒是怎样破坏硬件的
CIH使用什么方法进行感染的?

家族成员

PE_CIH

换硬盘也杀不掉的“**BMW病毒**”现身 危害远超**CIH**

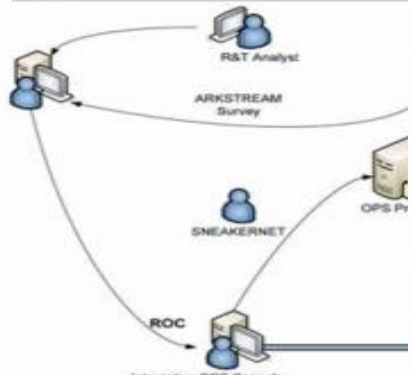
来源：360安全中心 发布日期：2011-09-01 已有286条评论 我要评论

北京时间9月1日，360安全中心发布2011年首个红色安全警报称，一种新型的BMW病毒正在大量发作，已攻击上万台电脑。据分析，该病毒能够感染电脑主板的BIOS芯片和硬盘MBR（主引导区），再控制Windows系统文件加载恶意代码，使受害用户无论重装系统、格式化硬盘，甚至换掉硬盘都无法彻底清除病毒。

2. NSA的固件木马 (1)

SECRET//COI

(TS//SI//REL) DEITYBOUNCE provides sol PowerEdge servers by exploiting the motha Management Mode (SMM) to gain periodic loads.



(TS//SI//REL) DEITYBOUNCE I

(TS//SI//REL) This technique supports multi and Microsoft Windows 2000, 2003, and XI 1850/2850/1950/2950 RAID servers, using 1.2.0, or 1.3.7.

(TS//SI//REL) Through remote access or in flash the BIOS on a target machine to impli implant installer). Implantation via interdici technical operator though use of a USB th DEITYBOUNCE's frequency of execution (will occur when the target machine powers

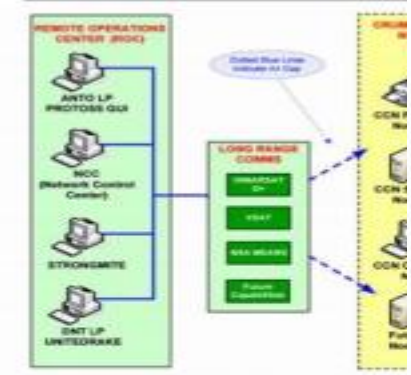
Status: Released / Deployed. Ready for Immediate Delivery

POC: [REDACTED] S32221, [REDACTED]

SECRET//COI

TOP SECRET//

(TS//SI//REL) IRONCHEF provides acces exploiting the motherboard BIOS and utili communicate with a hardware implant tha



(TS//SI//REL) IRONCHEF B

(TS//SI//REL) This technique supports the a hardware implant has been installed the (WAGONBED).

(TS//SI//REL) Through interdiction, IRON hardware implant are installed onto the sy removed from the target machine. IRONC determine the reason for removal of the s from a listening post to the target system.

Status: Ready for Immediate Delivery

POC: [REDACTED] S32221, [REDACTED]

TOP SECRET//

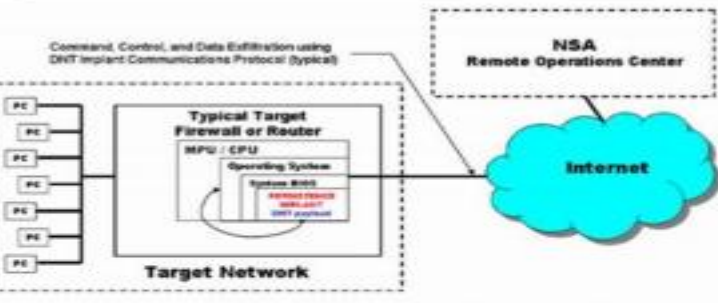
TOP SECRET//COMINT//REL USA, FVEY

FEEDTROUGH

ANT Product Data

06/24/08

(TS//SI//REL) FEEDTROUGH is a persistence technique for two software implants, DNT's BANANAGLEE and CES's ZESTYLEAK used against Juniper Netscreen firewalls.



(TS//SI//REL) Persistence Operational Scenario

(TS//SI//REL) FEEDTROUGH can be used to persist two implants, ZESTYLEAK and/or BANANAGLEE across reboots and software upgrades on known and covered OS's for the following Netscreen firewalls, ns5xt, ns25, ns50, ns200, ns500 and ISG 1000. There is no direct communication to or from FEEDTROUGH, but if present, the BANANAGLEE implant can receive and transmit covert channel comms, and for certain platforms, BANANAGLEE can also update FEEDTROUGH. FEEDTROUGH however can only persist OS's included in it's databases. Therefore this is best employed with known OS's and if a new OS comes out, then the customer would need to add this OS to the FEEDTROUGH database for that particular firewall.

(TS//SI//REL) FEEDTROUGH operates every time the particular Juniper firewall boots. The first hook takes it to the code which checks to see if the OS is in the database, if it is, then a chain of events ensures the installation of either one or both implants. Otherwise the firewall boots normally. If the OS is one modified by DNT, it is not recognized, which gives the customer freedom to field new software.

Status: (TS//SI//REL) FEEDTROUGH has on the shelf solutions for all of the listed platforms. It has been deployed on many target platforms

POC: [REDACTED] S32222, [REDACTED] [REDACTED] @nsa.ic.gov

Derived From: NSA/CSSM 1-62
Dated: 20070108
Declassify On: 20220108

TOP SECRET//COMINT//REL USA, FVEY

引申

产品目录共计48页，每页介绍一个工具。

2. NSA的固件木马 (2)

固件木马数量 (16)

- DEITYBOUNCE、IRONCHEF、FRRDTROUGH、GOURMETTROUGH、HALLUXWATER、JETPLOW、Eudemon、SOUFFLETROUGH、HEADWATER、SCHOOLMONTANA、SIERRAMONTANA、STUCCOMONTANA、SWAP、WISTULTOLL、GINSU、IRATEMONK

固件攻击目标

- 防火墙、服务器、路由器、主机、台式机

配套工具

- 刷写工具：ASKSTREAM
- 攻击载荷：BANANAGLEE、ZESTYLEAK、PBD
- 硬件工具：板卡、硬盘、U盘等

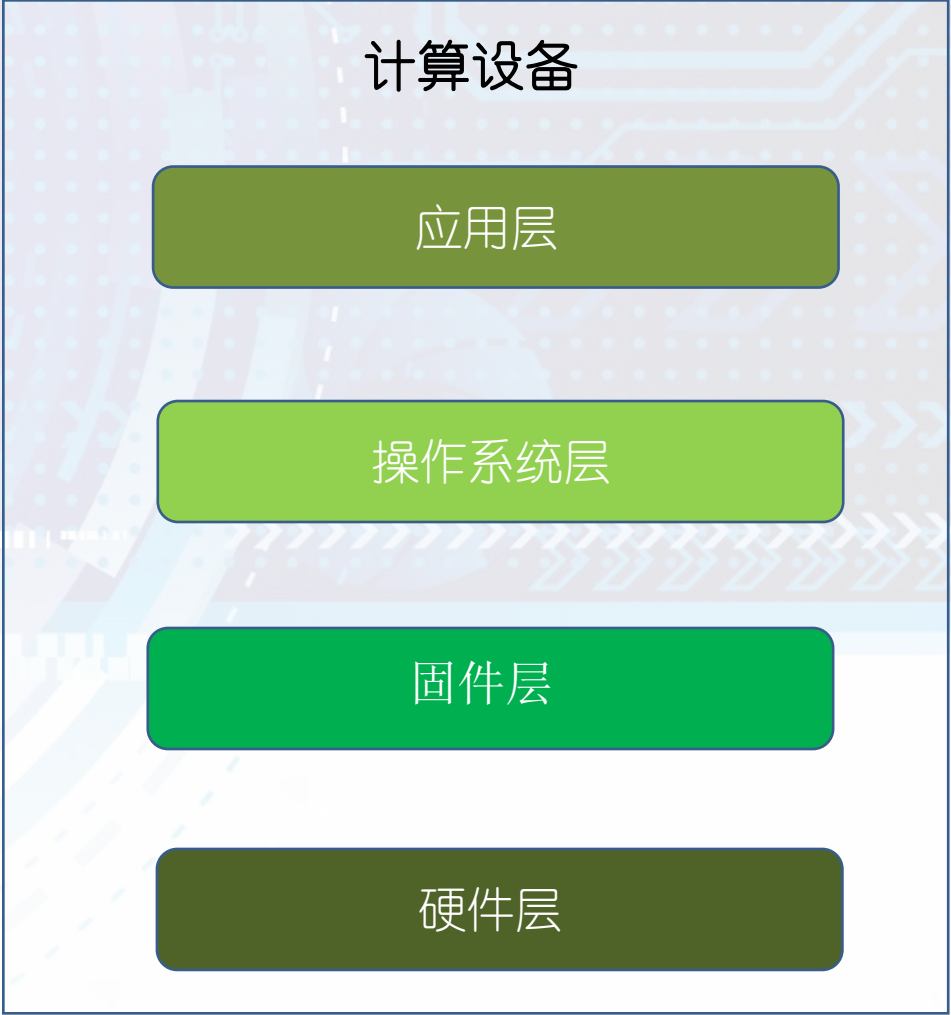
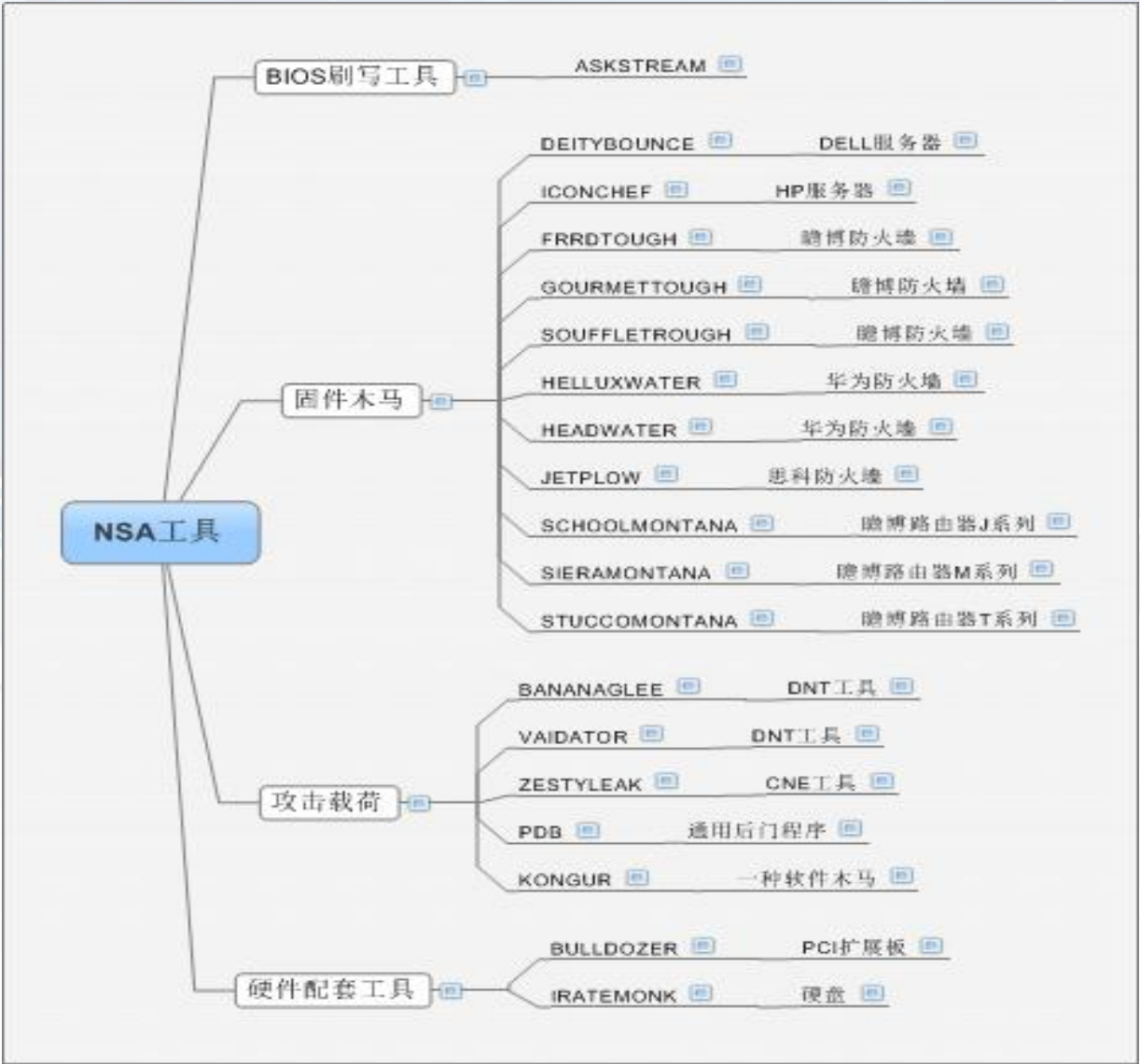
引申

植入固件木马，是NSA最喜欢的渗透方式之一。

固件木马列表

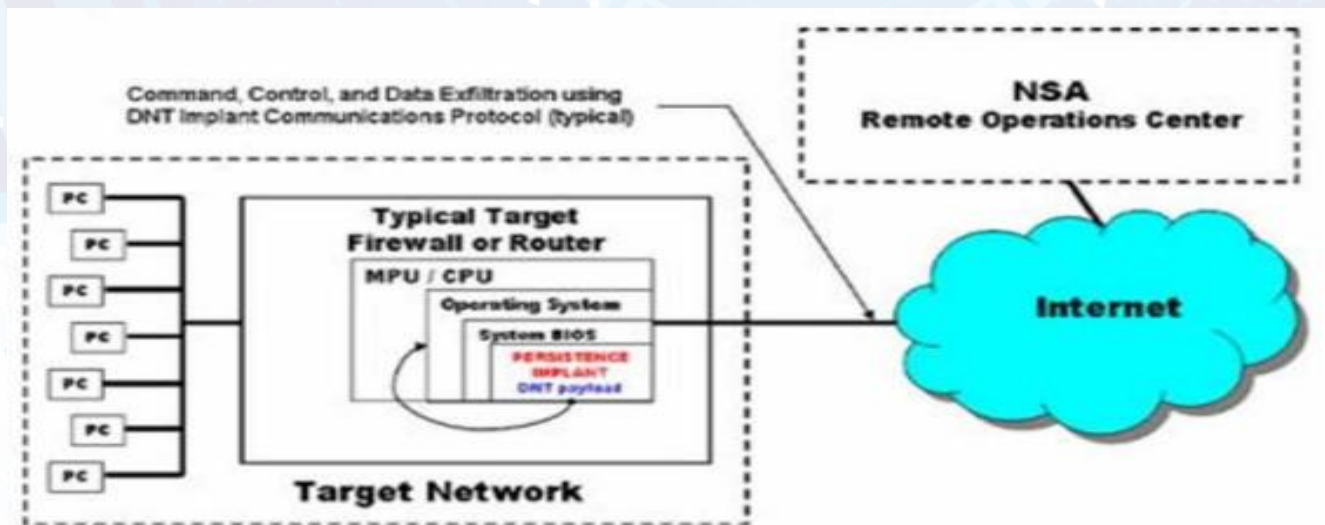
序号	木马类型	名称	目标机型	功能
1	更新工具	ASKSTREAM	计算机设备	通过网络、U盘等方式将木马刷入固件。
2	固件木马	DEITYBOUNCE	DELL	该工具能够在系统管理模式SMM下进行执行，其功能是在运行时与嵌入的硬件木马工具进行通信，进行信息传输。当该软件被删除时，能够自动恢复。
3		IRONCHEF	HP	
4		FRRDTROUGH	瞻博	
5		HALLUXWATER	华为	
6		JETPLOW	思科	
7		SWAP	计算机设备	将TWISTEDKILT写入HPA区。支持操作系统包括Windows、Linux、FreeBSD、Solaris。文件系统支持FAT32、NTFS、EXT2、EXT3、UFS1.0。
8	板卡木马	GINSU	计算机设备	在主机重启后重新恢复攻击载荷
9	硬盘的固件	IRATEMONK	计算机设备	在开机时加载，将木马植入目标主机，

2. NSA的固件木马 (4)



2. NSA的固件木马 (5)

- 固件木马植入一般包括三个阶段
 - 准备阶段
 - 固件植入阶段
 - 操作系统植入阶段



计算设备

应用层

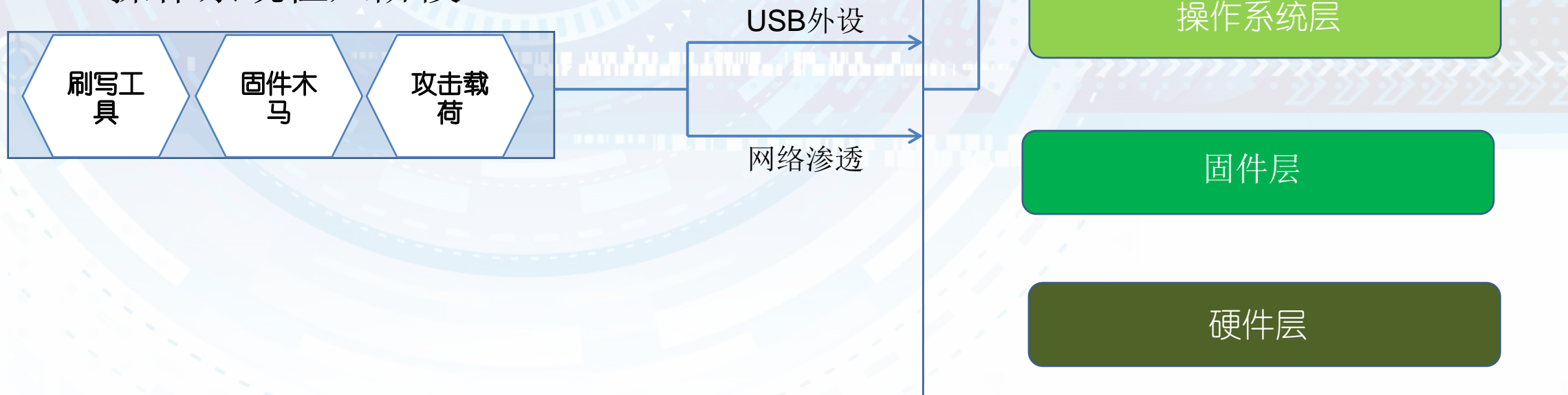
操作系统层

固件层

硬件层

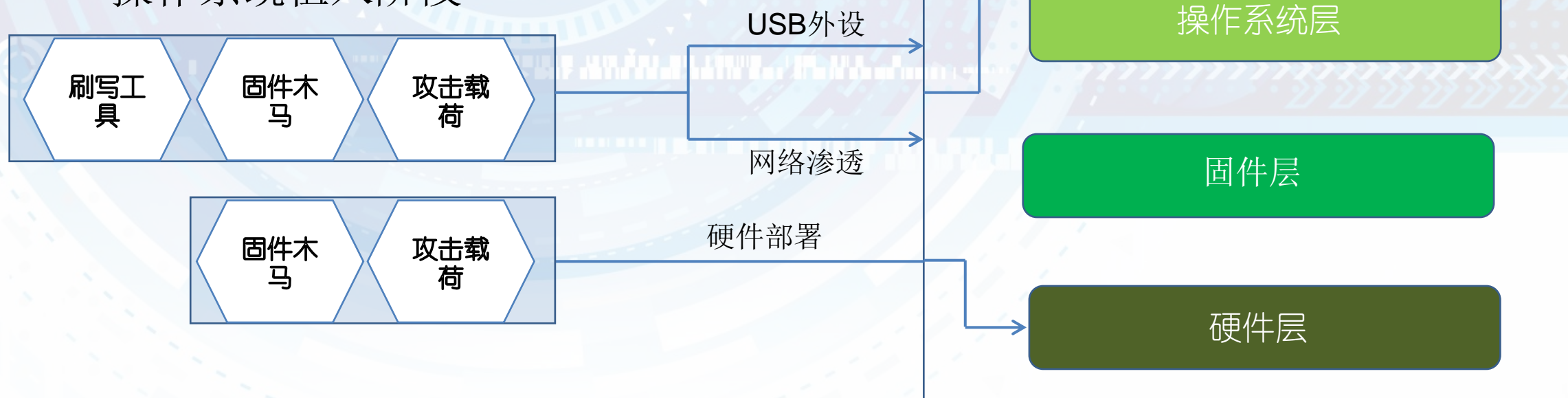
2. NSA的固件木马 (5)

- 固件木马植入一般包括三个阶段
 - 准备阶段
 - 目标：将刷写工具ASKSTREAM植入目标机
 - 方法：网络渗透、U盘摆渡、硬件工具
 - 固件植入阶段
 - 操作系统植入阶段



2. NSA的固件木马 (5)

- 固件木马植入一般包括三个阶段
 - 准备阶段
 - 目标：将刷写工具ASKSTREAM植入目标机
 - 方法：网络渗透、U盘摆渡、硬件工具
 - 固件植入阶段
 - 操作系统植入阶段



2. NSA的固件木马 (5)

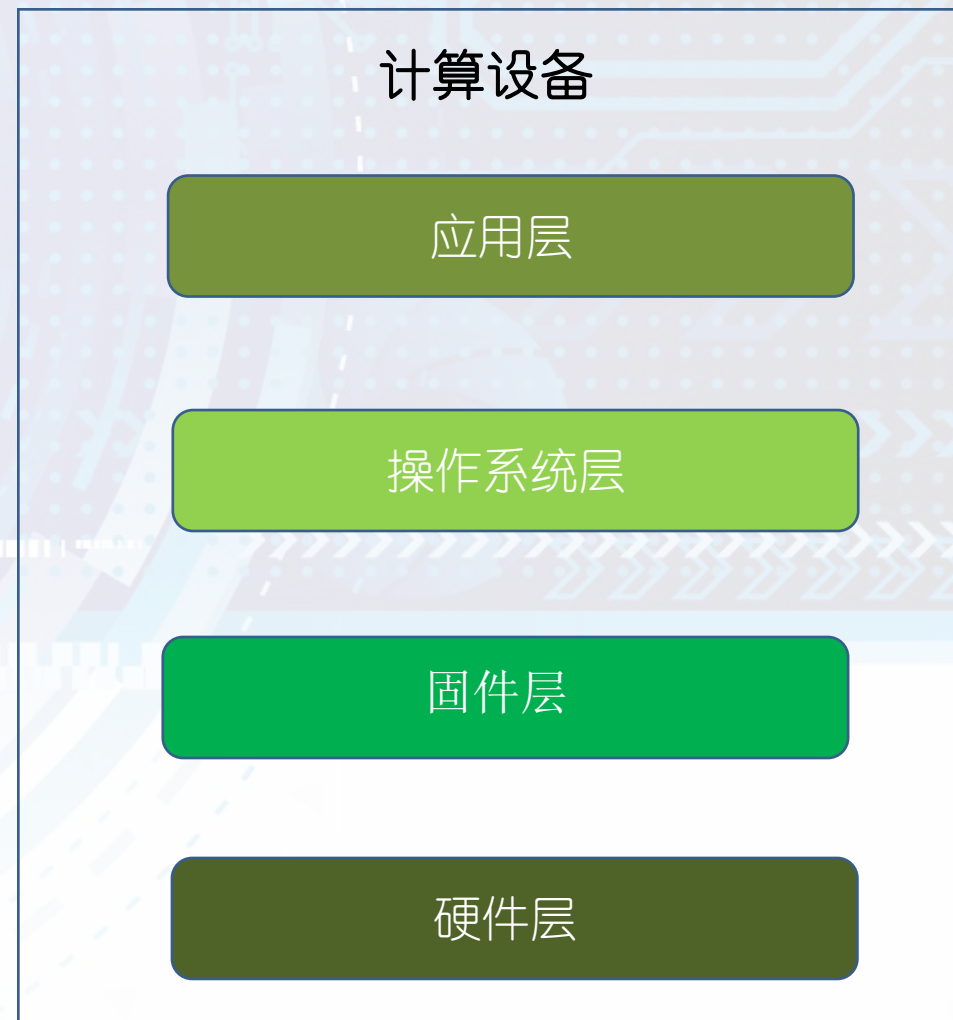
- 固件木马植入一般包括三个阶段

- ✓ 准备阶段

- 固件植入阶段

- 目标：加载固件木马
 - 方法：固件更新、OPROM

- 操作系统植入阶段



2. NSA的固件木马 (5)

✧ 固件木马植入一般包括三个阶段

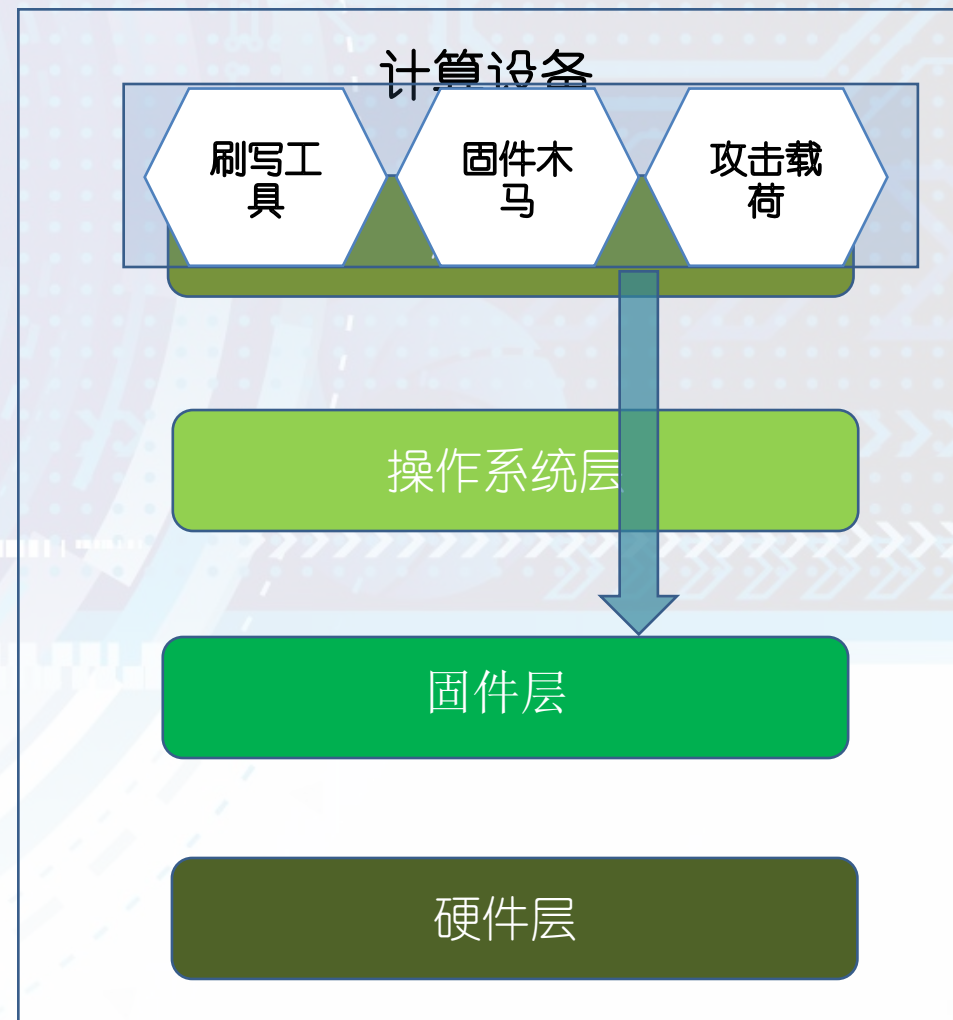
✓ 准备阶段

— 固件植入阶段

- 目标：加载固件木马

- 方法：固件更新、OPROM

— 操作系统植入阶段



2. NSA的固件木马 (5)

✧ 固件木马植入一般包括三个阶段

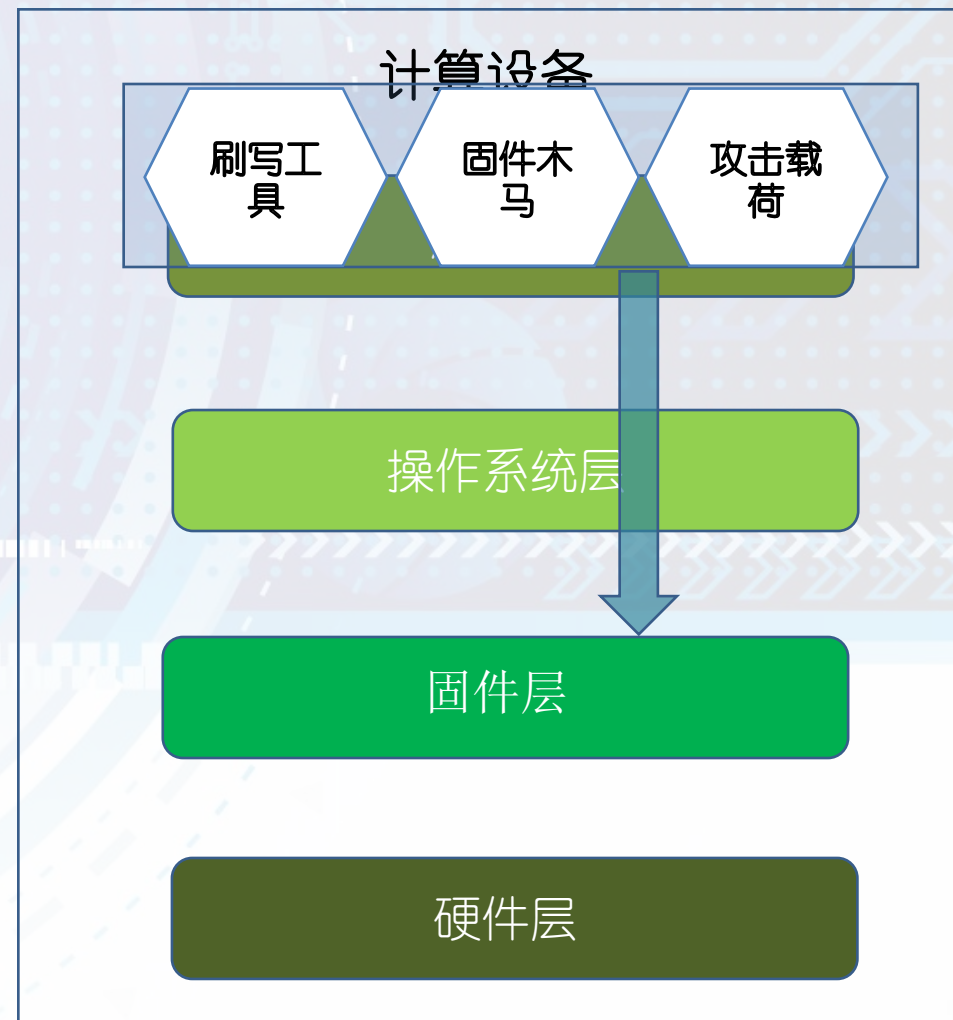
✓ 准备阶段

✓ 固件植入阶段

- 目标：加载固件木马

- 方法：固件更新、OPROM

— 操作系统植入阶段



2. NSA的固件木马 (5)

✧ 固件木马植入一般包括三个阶段

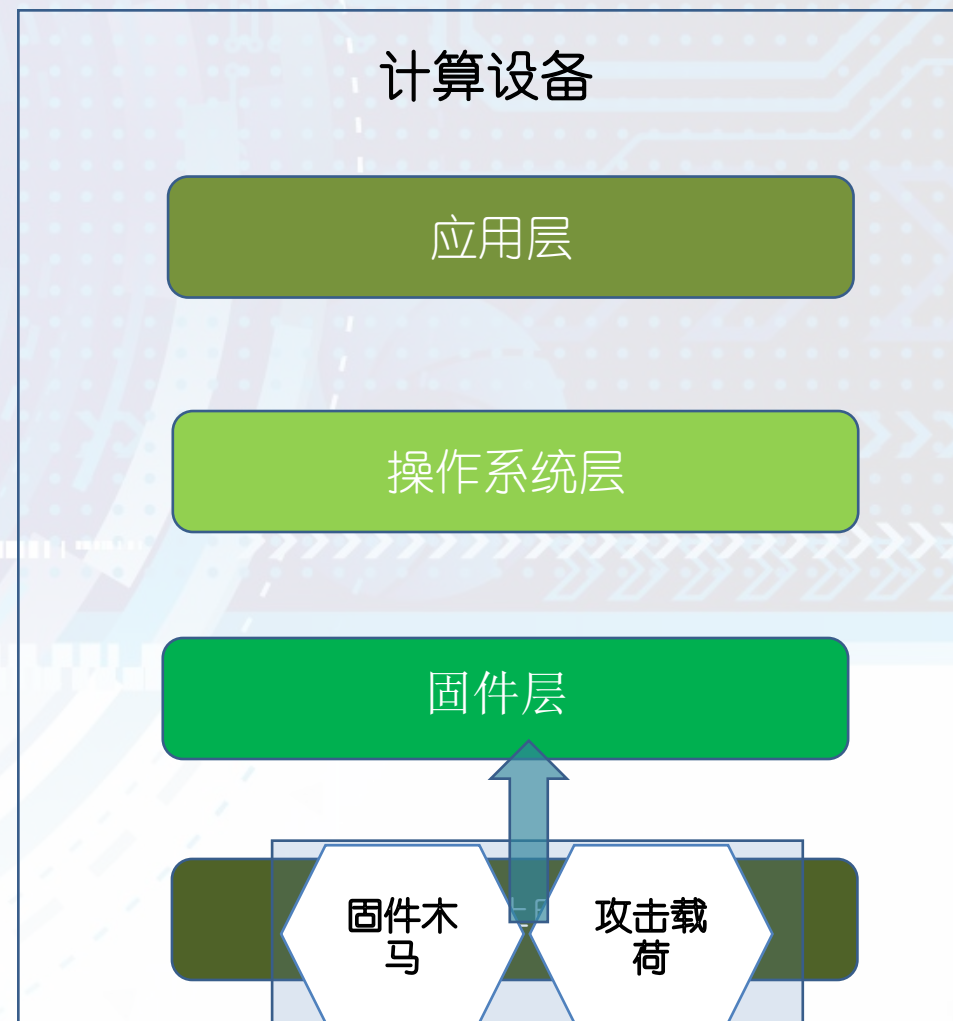
✓ 准备阶段

✓ 固件植入阶段

- 目标：加载固件木马

- 方法：固件更新、OPROM

— 操作系统植入阶段



2. NSA的固件木马 (5)

✧ 固件木马植入一般包括三个阶段

✓ 准备阶段

✓ 固件植入阶段

✓ 操作系统植入阶段

■ 目标：执行攻击载荷，植入间谍木马

■ 方法：系统识别、网络下载、远程控制



2. NSA的固件木马 (5)

✧ 固件木马植入一般包括三个阶段

✓ 准备阶段

✓ 固件植入阶段

✓ 操作系统植入阶段

■ 目标：执行攻击载荷，植入间谍木马

■ 方法：系统识别、网络下载、远程控制



2. NSA的固件木马 (5)

✧ 固件木马植入一般包括三个阶段

✓ 准备阶段

✓ 固件植入阶段

✓ 操作系统植入阶段

■ 目标：执行攻击载荷，植入间谍木马

■ 方法：系统识别、网络下载、远程控制

■ 步骤：

① 检测当前OS是否支持

② 远程下载PDB

③ 与配套工具协作，回传信息



2. NSA的固件木马 (5)

✧ 固件木马植入一般包括三个阶段

✓ 准备阶段

✓ 固件植入阶段

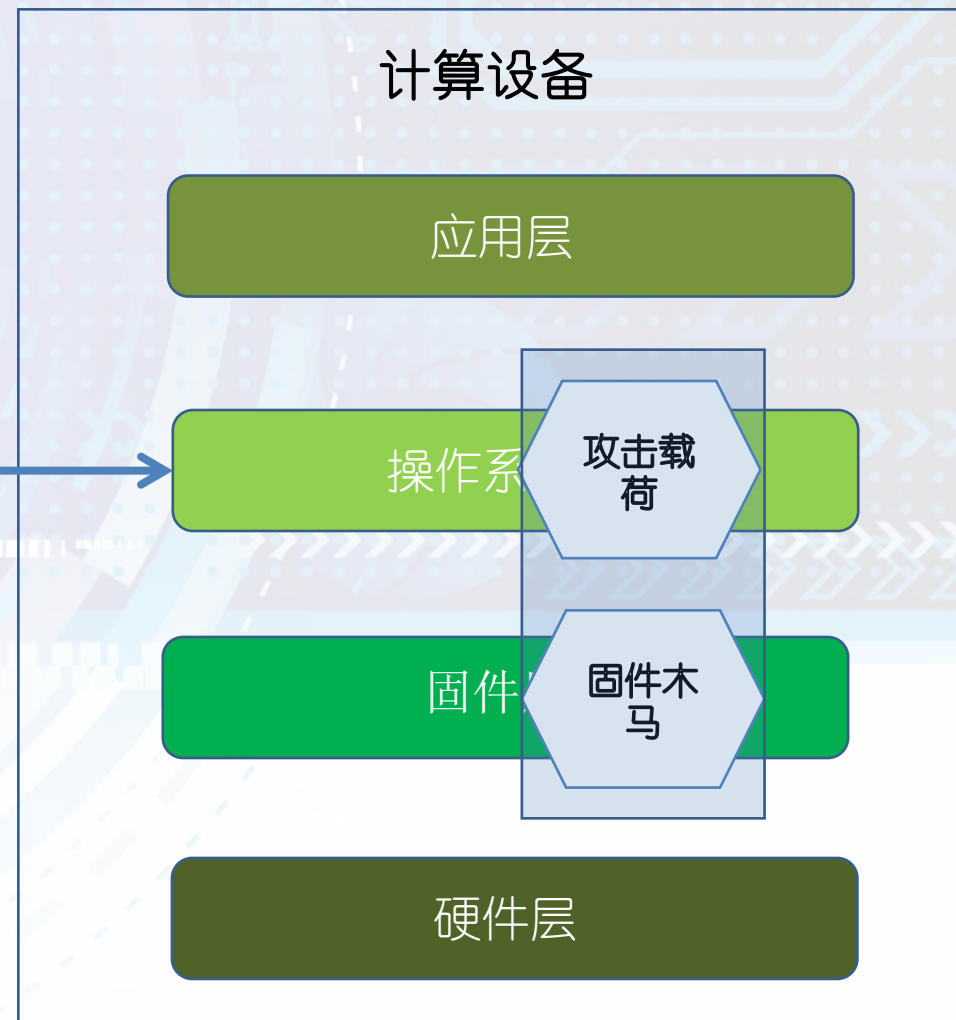
✓ 操作系统植入阶段

■ 目标：执行攻击载荷，植入间谍木马

■ 方法：系统识别、网络下载、远程控制

■ 步骤：

- ① 检测当前OS是否支持
- ② 远程下载PDB
- ③ 与配套工具协作，回传信息
- ④ 固件层实时监控和恢复



目 次

一、 固件安全隐患分析

二、 固件攻击实例介绍

三、 固件安全防护方法

1. 固件安全防护----防止固件被篡改

硬件写保护

- 通过跳线等方式，对固件芯片进行物理写保护。

双BIOS

- BIOS进行分块，其中部分受到写保护，对其他部分进行验证和恢复。

软件写保护

- 通过安全升级软件配置寄存器，禁止或允许刷写固件芯片。

1. 固件安全防护----NIST (1)

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-141
(Draft)

BIOS Protection Guidelines for Servers (Draft)

Recommendations of the National Institute
of Standards and Technology

Andrew Regenscheid

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-147

BIOS Protection Guidelines

Recommendations of the National Institute
of Standards and Technology

David Cooper
William Polk
Andrew Regenscheid
Murugiah Souppaya

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-155
(Draft)

BIOS Integrity Measurement Guidelines (Draft)

Recommendations of the National Institute
of Standards and Technology

Andrew Regenscheid
Karen Scarfone

1. 固件安全防护----NIST (2)

签名机制

- BIOS升级机制使用数字签名确保BIOS升级镜像文件是经过授权的。

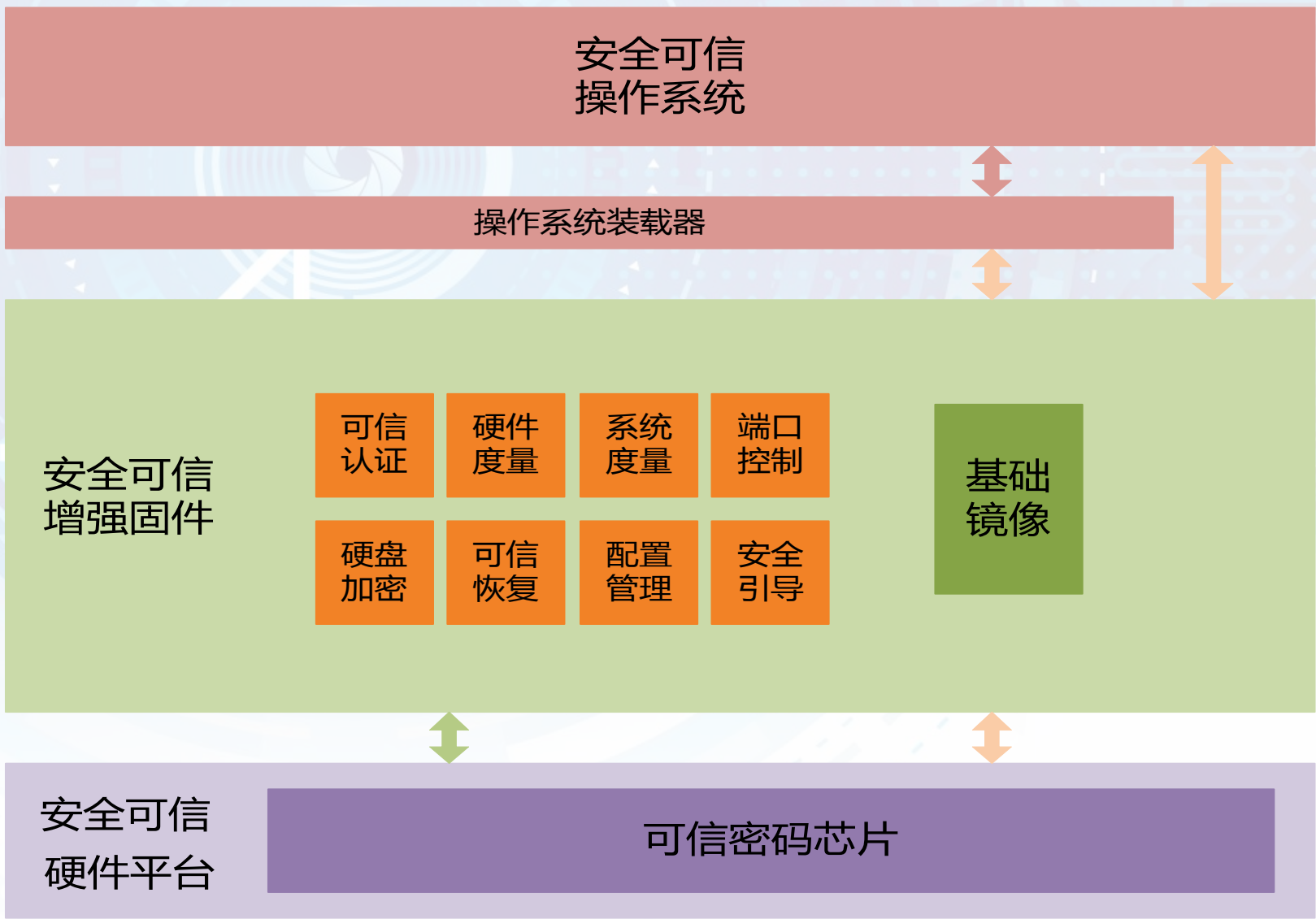
安全升级

- 验签算法和密钥应被存储在计算机中一块受保护的区域，并只能被安全升级软件访问。

禁止非授权回滚

- 版本号检测
- 授权机构确认对BIOS进行升级或回滚

2. 主动度量



5. 可信固件解决方案（1）

在固件系统中加入可信计算架构，支持国家/军用可信计算标准，提供可信度量、身份认证和数据加密等安全功能，为国产计算平台提供可信、安全的运行环境。

主要功能



桌面机

服务器

嵌入式

移动终端

2. 可信固件解决方案（2）

安全可信方案

军用固件安全方案

- 符合军用可信计算规范
- 支持军用TCM芯片
- 接口：PCI、PCIE、MiniPCIE、USB、CPCI
- 功能：身份认证、可信度量、可信恢复、硬盘加密等

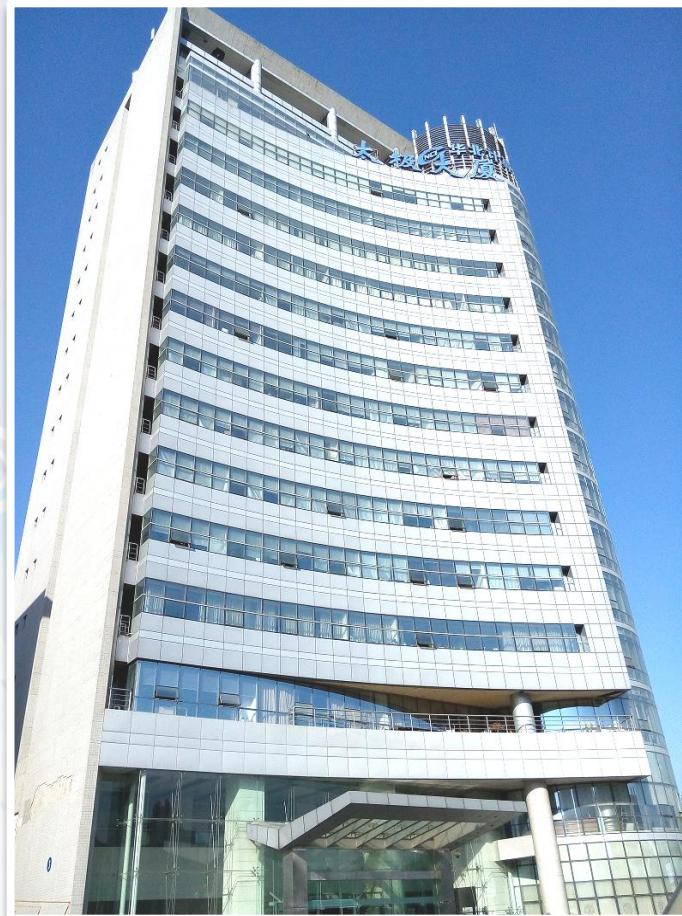
民用固件安全方案

- 符合民用可信计算规范
- 支持国民技术、同方微电子TCM芯片
- 接口：LPC
- 功能：身份认证、可信度量、可信恢复、硬盘加密等

安全可信增强方案

- 符合军用可信计算规范
- 接口：PCI、PCIE
- 功能：身份认证、可信度量、可信恢复等

3. 基本情况介绍



中电科技（北京）有限公司

在中国电子科技集团公司支持下，于2005年4月成立，简称“中电科技”，是一家面向政府、国防、金融等领域提供信息技术服务的高新技术企业。

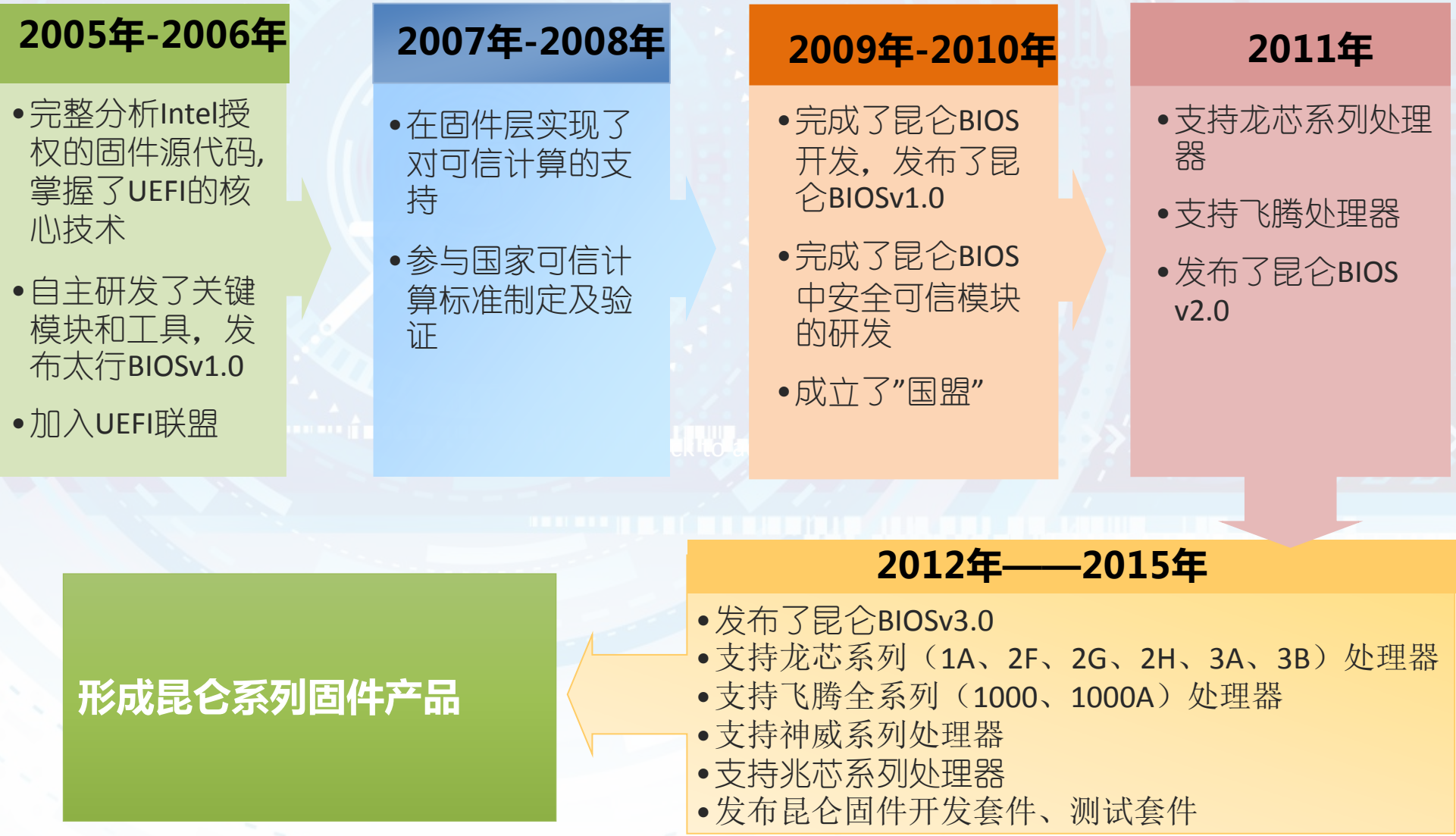
固件产品开发和服务是中电科技一项重要业务。

注册资本：1250万元

网 站：<http://www.zd-tech.com.cn>

地 址：北京市海淀区北四环中路211号太极大厦13、14层

4. 昆仑固件产品演进过程



5. 固件产品方案

固件产品方案列表

平台	处理器	形态	操作系统	小结
飞腾	FT1000	服务器	麒麟操作系统	4款参考固件 10种解决方案
	FT1000A	桌面机、笔记本、一体机、服务器		
	FT1500A	桌面机、服务器		
	FT1500A-4	桌面机、笔记本、一体机		
龙芯	LS1A	手持机	中标麒麟、普华、锐华、道等国产操作系统	8款参考固件 14种解决方案
	LS2F	桌面机		
	LS2H	平板电脑		
	LS3A (单、双路)	桌面机、笔记本、一体机、服务器		
	LS3B (单、双路)	桌面机、笔记本、一体机、服务器		
兆芯	ZX-A	桌面机、笔记本、一体机	支持Windows、中科方德等操作系统	4款参考固件 6种解决方案
	ZX-C	桌面机、笔记本、一体机		
申威	SW410	桌面机、笔记本、一体机	中标麒麟、道等国产操作系统	2款参考固件 6种解决方案
	SW410B	桌面机、笔记本、一体机		
	SW1610	服务器		
众志	PKUnity	桌面机、笔记本、一体机	支持Windows、中标麒麟等操作系统	1款参考固件 1种解决方案



感谢您的关注！

Thank you for your attention