



魔法之源——信息世界的配方、符文和咒语



于旻 绿盟科技研究院

Public



《麦克白·第四幕》

绕着大锅把圈儿兜，
毒肝毒脏往里边投。
冷石头底下癞蛤蟆睡大觉，
日夜泡过了三十又一遭，
熬出了满身的毒液和毒膜，
先把你拿来在锅里煮。

沼泽地小蛇切来肉一段，
投到锅里去熬熬又煎煎；
再加上壁虎眼、青蛙脚尖趾，
蜥蜴的腿条、鸱枭的翅，
蝙蝠的绒毛、恶狗的舌，
蝮蛇的牙齿、盲蛇的蜇；
炼出的魔力大到可通神，
象煮地狱汤，沸滚又沸滚。

毒龙的鳞甲、豺狼的牙，
女巫的干尸、苦海的鲨
把什么都掠食鲸吞的肠和胃，
黑夜掘出的毒芹根一堆；
渎神的犹太人肚里的黑心肝、
山羊的苦胆、趁月食还没完
及时从坟头砍下的柏树枝；
土耳其鼻子、鞑靼人嘴唇皮；
卖淫妇偷生孩子在沟道里
狠心就把他掐死的毒手指：
把锅汤烧得浓浓厚，酳脂脂。
再添上一只老虎的肺腑，
加工，加料来煮成一锅糊。

再泼上满锅的猩猩血来一凝，
炼成的魔汤就又好又坚定。





特雷门琴



LEON THEREMIN

RUSSIAN SCIENTIST

PLAYING HIS

Ether-Wave Music Instrument

in Program of: Schubert, Saint-Saens, Scriabine, Rachmaninoff, etc.

Without Touching the Instrument

THE PLAYER PRODUCES THE DESIRED MUSIC
BY DEFINITE HAND MOVEMENTS IN THE AIR

Professor Theremin also explains the principles of his invention



SYMPHONY HALL - BOSTON

SUNDAY AFTERNOON AT 3:30 - OCTOBER 7

SEATS NOW ON SALE

PRICES \$1.00 TO \$2.50

CONCERT MANAGEMENT: ARTHUR JUDSON







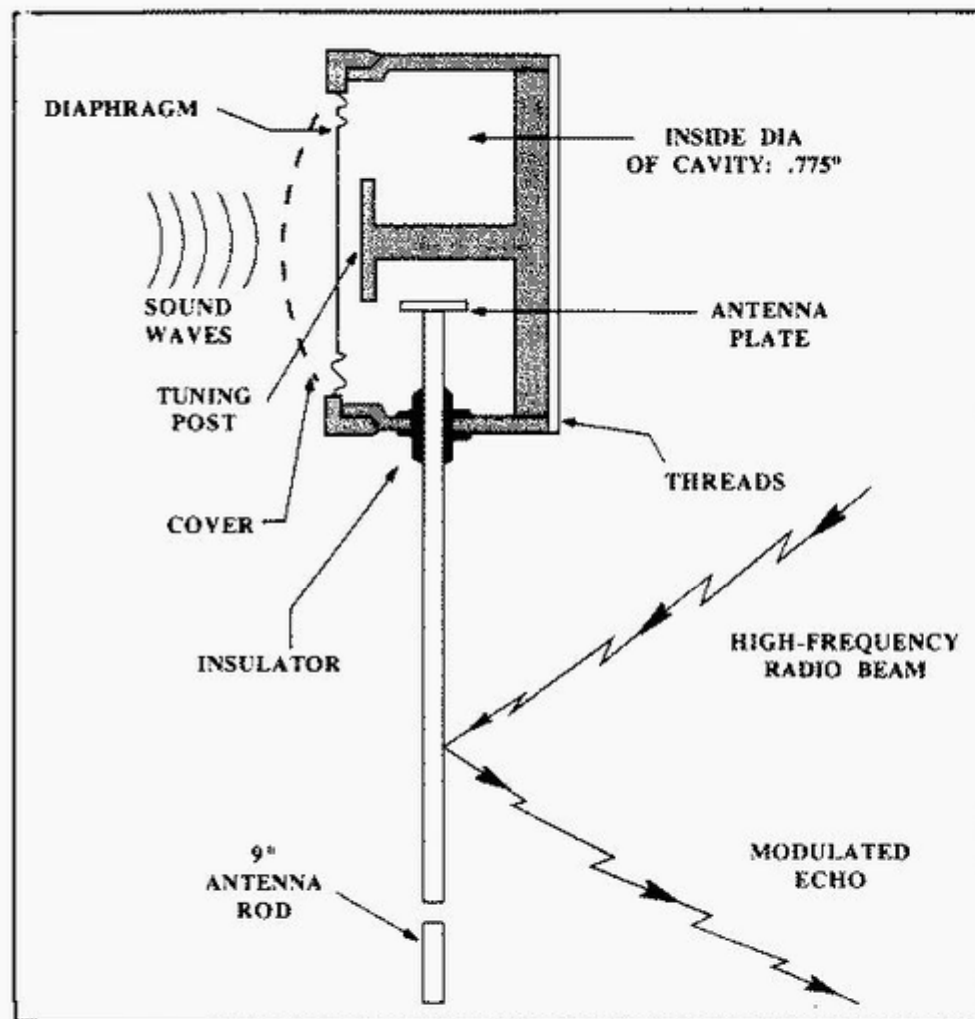




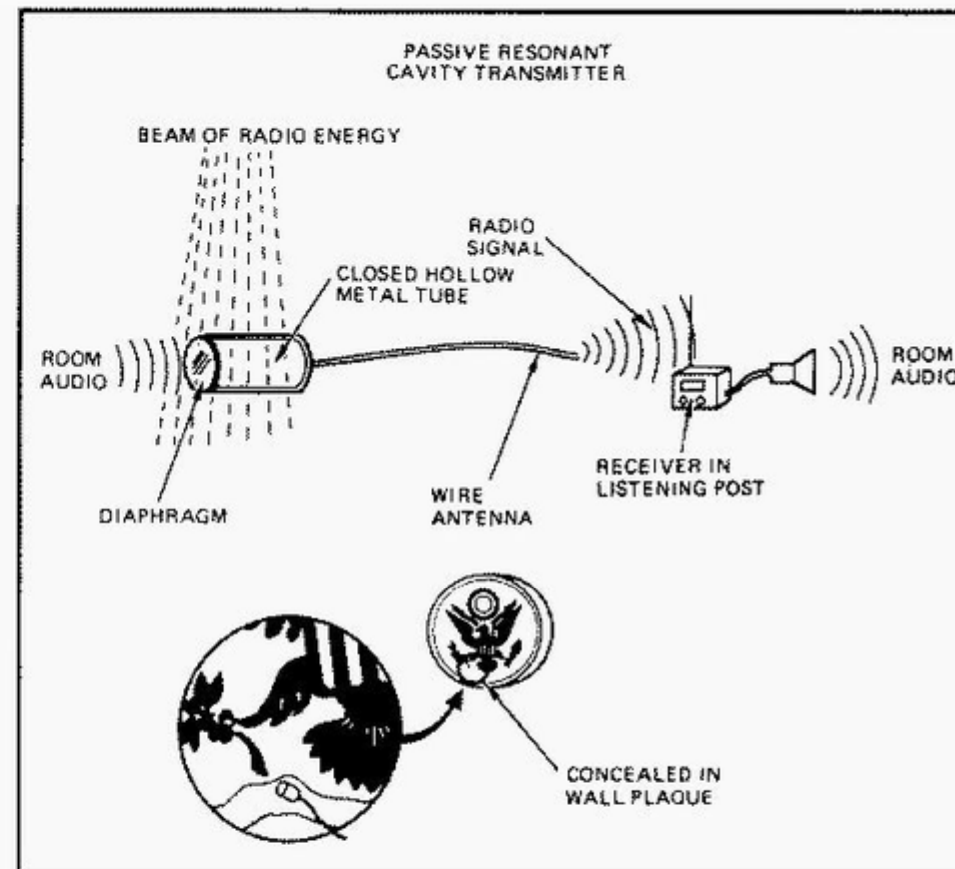








The passive cavity transmitter requires no internal power. It is energized by a high-frequency radio beam aimed at the device.



Passive cavity transmitter found in the American Embassy, Moscow, was a "gift" from the Soviets. The CIA was startled to discover the advanced technology being used by the Soviets for eavesdropping in this 1951 discovery. The device transmitted on a frequency of 330 MHz.

基础资源对抗 à 关键知识对抗

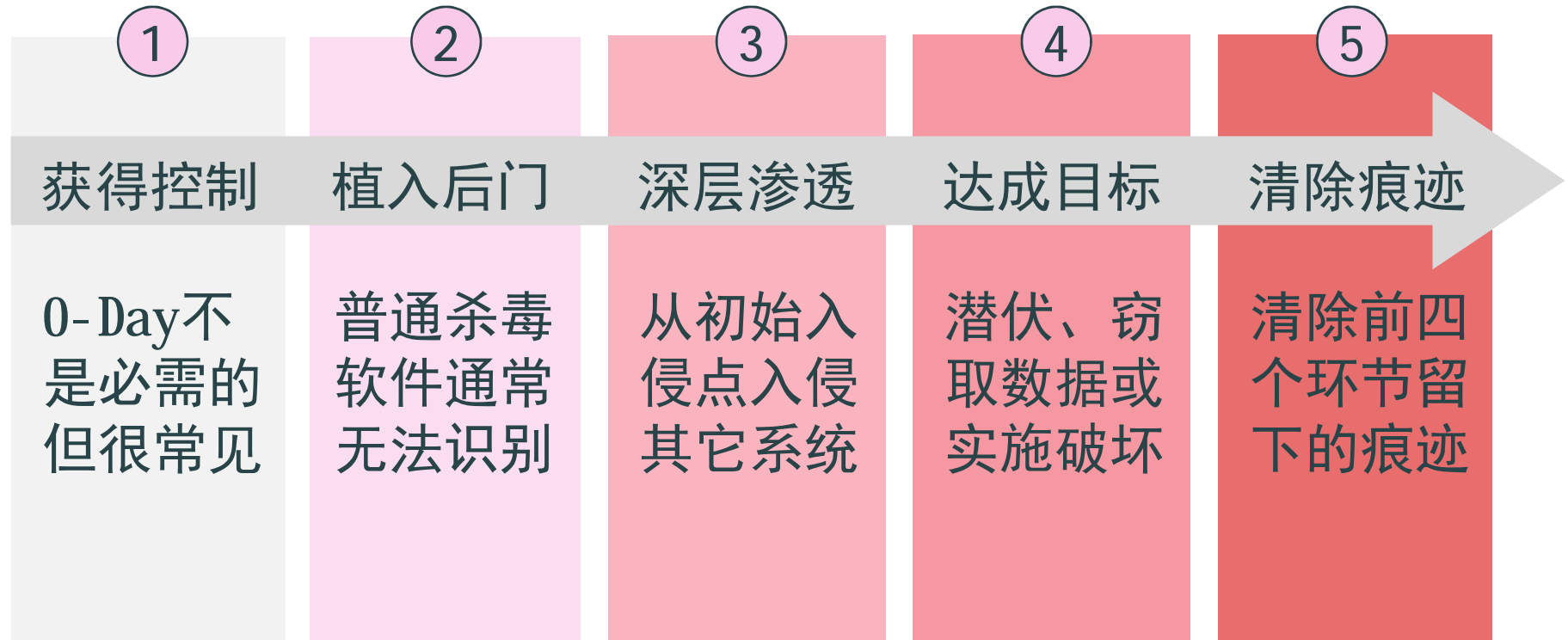
早期漏洞的利用方法简单，涉及的知识量少，易掌握。相应的检测手段也较简单。

现在无论Web还是系统漏洞，利用方法越来越复杂。攻击和防御都需要相应关键知识。

安全产品从早期的偏向于追求签名数量和性能，到今天越来越看重实际对抗能力。

一个关键的攻击知识，或一个关键的防御知识，就可以改变对抗双方的实力对比。

APT攻击



——每个环节都充满了关键知识对抗

NAME OF OFFEROR OR CONTRACTOR


VUPEN SECURITY

ITEM NO.	SUPPLIES/SERVICES
0001	VUPEN Binary Analysis and Exploits Service 12 months subscription
AA	ACR: AA PR # 001684510000 ITEM # 0001 9720100.4500 112519 2573 S18119 NSBXX C6131 C613 IAD04
001684510000	OBLIGATE - <input type="text"/>

合同上显示：美国国家安全局在2012年9月14日，向Vupen购买了为期一年的“二进制分析和攻击代码服务”。

4075369

Approved for Release by NSA on 09-09-2013, FOIA Case # 74643

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30			1. REQUISITION NUMBER 001684510000
2. CONTRACT NO. H98230-12-P-2740	3. AWARD/EFFECTIVE DATE 9/14/12	4. ORDER NUMBER	5. SOLICITATION NUMBER H98230-12-T-4346
7. FOR SOLICITATION INFORMATION CALL: 	a. NAME <input type="text"/>	b. TELEPHONE NUMBER (No cell calls) <input type="text"/>	
9. ISSUED BY Buyer/Symbol: <input type="text"/> (BA342) Marland Procurement Office	CODE H98230	10. THIS ACQUISITION IS <input type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMA BUSINESS ENTERPRISE	

公开的0-Day：各种“可执行文件”

可执行文件（.EXE）

批处理文件（.BAT）

屏幕保护文件（.SCR）

~~碎片对象文件（.SHS）~~

~~已编译HTML帮助文件（.CHM）~~

~~Windows帮助文件（.HLP）~~

.....

公开的0-Day: MS06-001

摘自微软系统开发工具包:

```
/* Metafile Functions */
#define META_ESCAPE                                0x0626

/* GDI Escapes */
#define MFCOMMENT                                  15
#define SETABORTPROC                              9

int Escape(
    HDC hdc,                // handle to DC
    int nEscape,            // escape function
    int cbInput,            // size of input structure
    LPCSTR lpvInData,       // input structure
    LPVOID lpvOutData       // output structure
);
```

公开的0-Day: WiFi “捞鱼”

如果无线客户端配置了希望连接的无线网络或者**曾成功连接过一个无线网络**，客户端发送的探查请求帧中会携带希望连接的SSID。攻击者可根据这个SSID伪造AP，使无线客户端自动接入。



Probe Request
(SSID = "MyHome")



高级同步设置



同步所有数据类型 ▼

☒ 应用

☒ 扩展程序

☒ 设置

☒ 自动填充

☒ 历史记录

☒ 主题背景

☒ 已保存的书签

☒ 密码

☒ 打开的标签页

加密选项

为提高安全性，Google Chrome会对您的数据进行加密。

☐ 使用您的 Google 凭据加密已同步的密码

☒ 所有数据都已使用您的 Google 密码加密，加密时间为：2013-4-9 [了解详情](#)

[使用默认设置](#)

确定

取消

设置 iTunes Store 和 App Store

Apple ID:

自动下载的项目



应用程序



自动下载在其他的设备上新购买的项目
(含免费项目)

使用蜂窝移动数据



将蜂窝移动网络用于自动下载。

未知生，焉知死？



未知攻，焉知防？

The background of the slide consists of a light gray, stylized globe centered behind a dark gray horizontal bar. To the left of the globe, there is a fan-like pattern made of several curved, overlapping segments in shades of gray and white.

谢谢！