

# 软件安全与漏洞分析

---

## 4.1 软件自我保护技术概述

# Previously in Software Security

---

## □ 其他软件与操作系统防护技术

- 安全数据删除
- 针对不可信操作系统的防护

## □ 软件验证和漏洞检测技术

- 模糊测试
- 具体/符号执行
- 污点传播

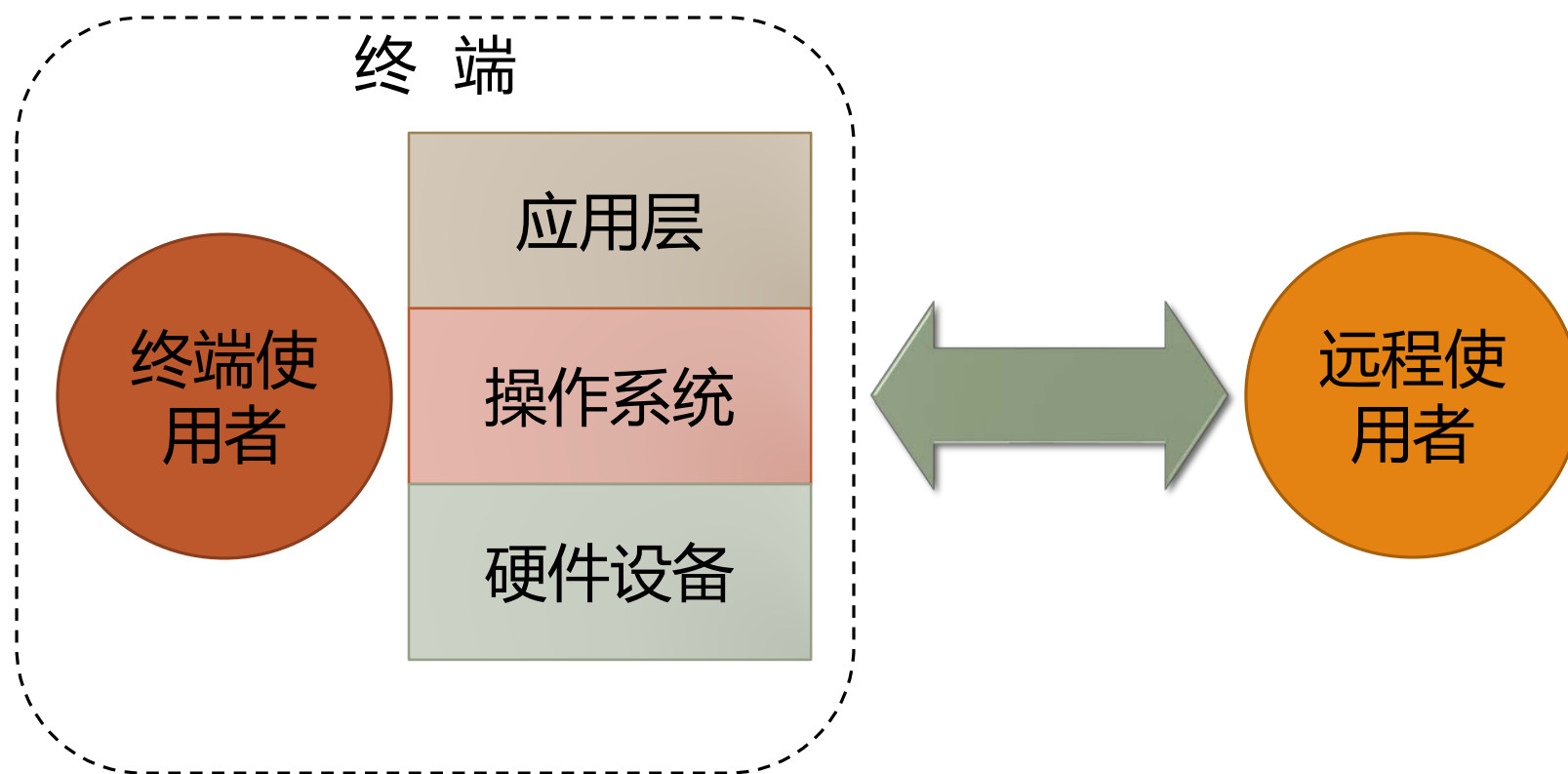
# 软件自我保护技术概述

---

- 本节主题 – 软件自我保护技术
  - Man-At-The-End攻击模型
  - 主要软件自我保护技术：代码混淆
  - 主要软件自我保护技术：软件防篡改
  - 主要软件自我保护技术：软件水印
  - 主要软件自我保护技术：软件胎记

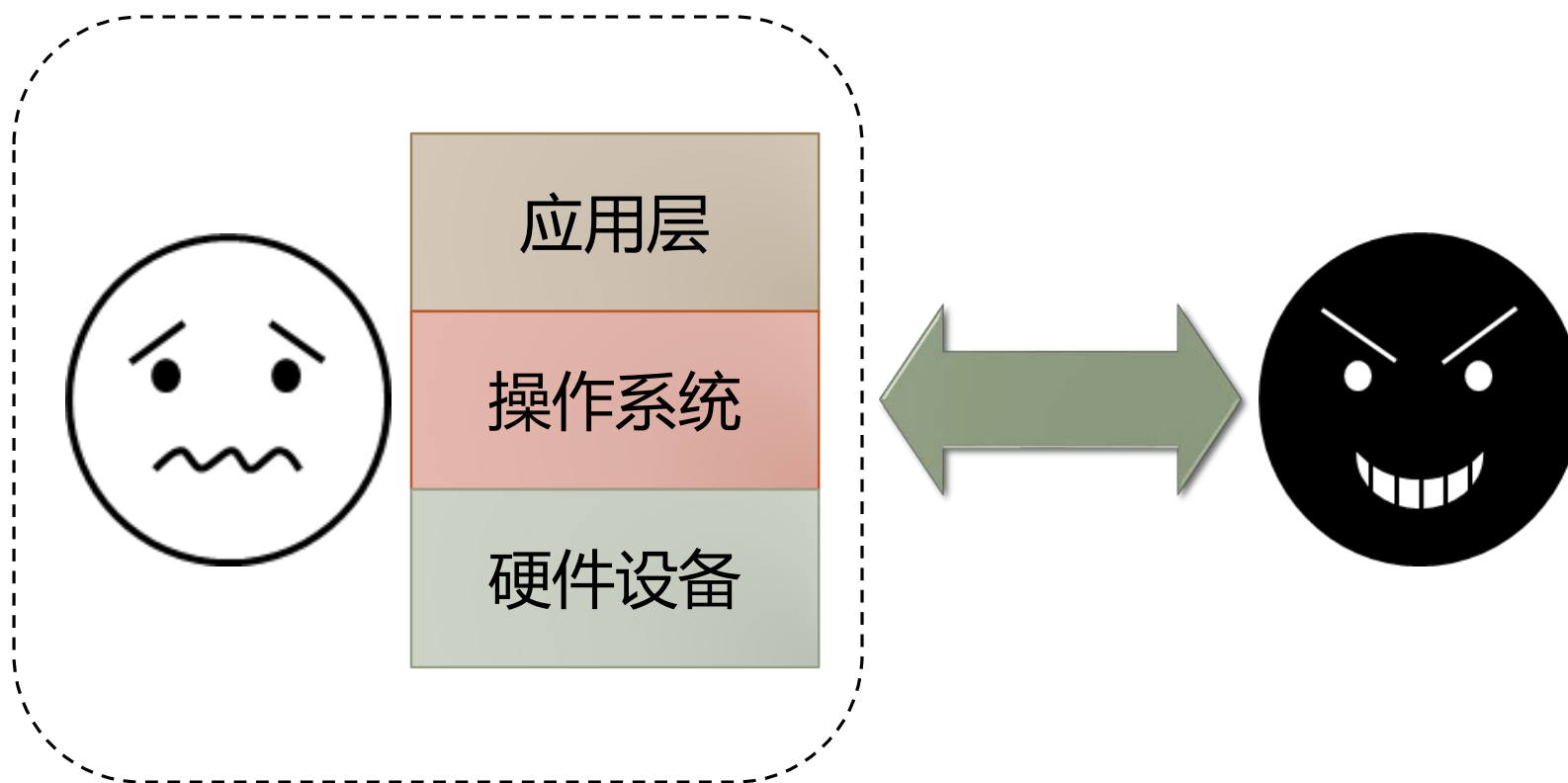
# Man-At-The-End攻击

---



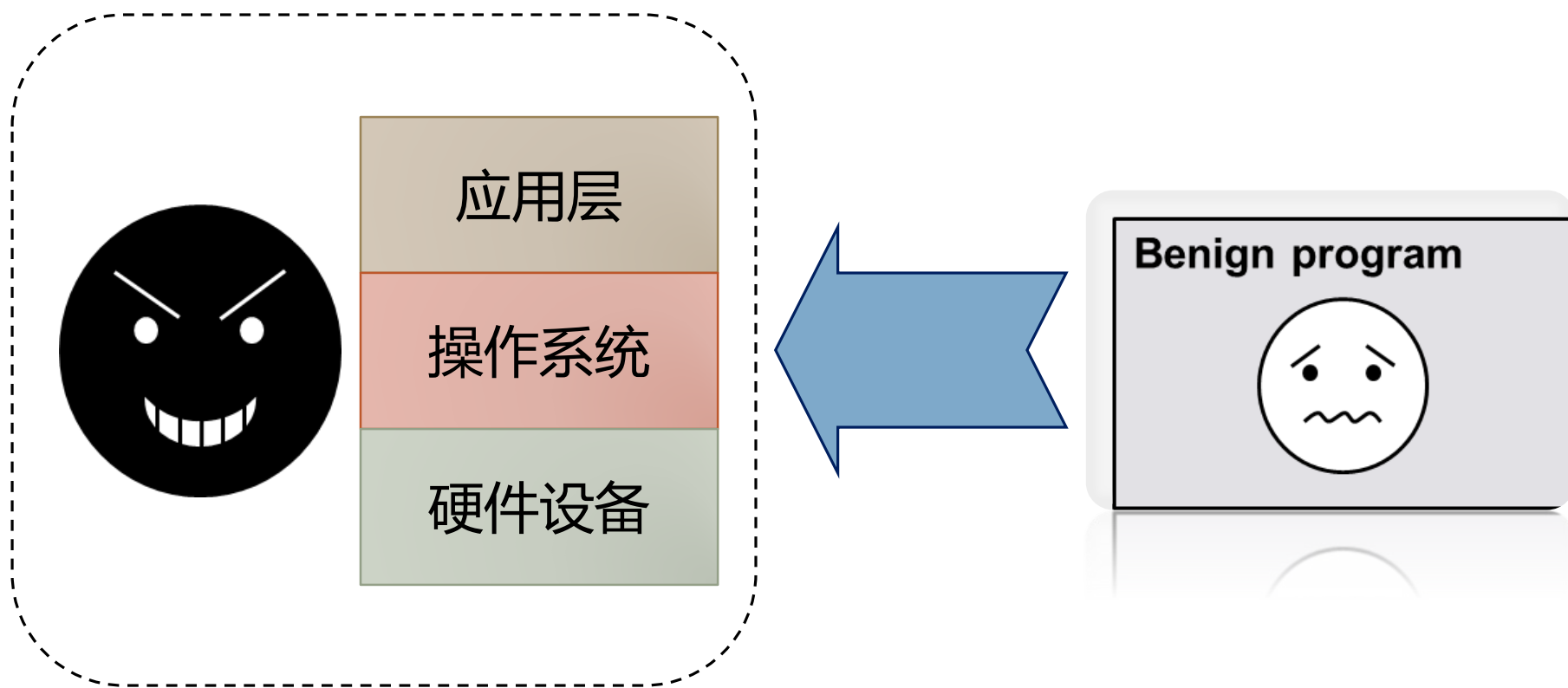
# Man-At-The-End攻击

---



# Man-At-The-End攻击

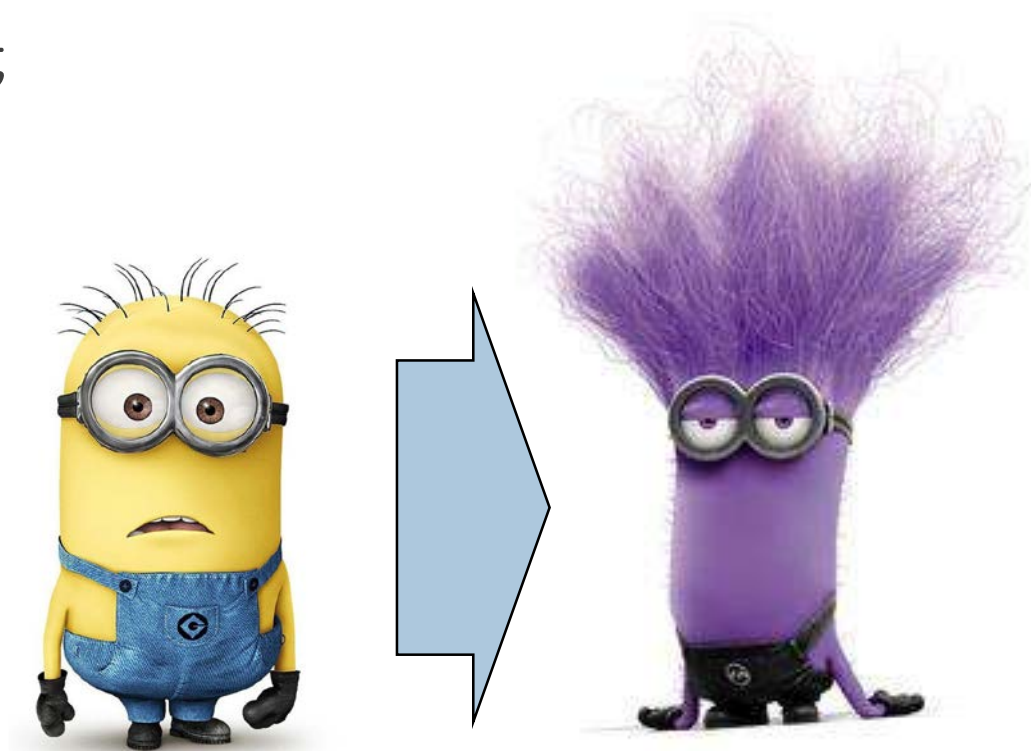
---



# Man-At-The-End攻击

---

- 攻击者：位于终端，对终端计算资源有最高控制权限
- 攻击对象：安装在受控终端上的软件程序
- 攻击目的：获悉、篡改软件的内部逻辑




# Man-At-The-End攻击

## 实际攻击场景1：盗版/破解



### UpdateGroup



### 游侠工作组

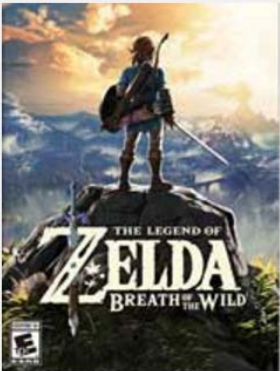
帖子	17196
精华	0
积分	12364
金钱	43110
荣誉	361
人气	1561
评议	0

[串个门](#) [加好友](#)

[打招呼](#) [发消息](#)

发表于 2017-3-27 14:50:57 | 只看该作者 | 倒序浏览

《游侠云盒》正式版发布！最智能最专业的游戏云平台，诚邀体验！



游戏名称：塞尔达传说：荒野之息  
英文名称：The Legend of Zelda: Breath of the Wild  
游戏类型：动作游戏ACT  
游戏制作：Nintendo  
游戏发行：Nintendo  
游戏平台：WIIU, SWITCH, PC  
游戏语言：英文  
发售日期：2017-03-03



# Man-At-The-End攻击

## 实际攻击场景2：病毒/恶意代码分析



# Man-At-The-End攻击

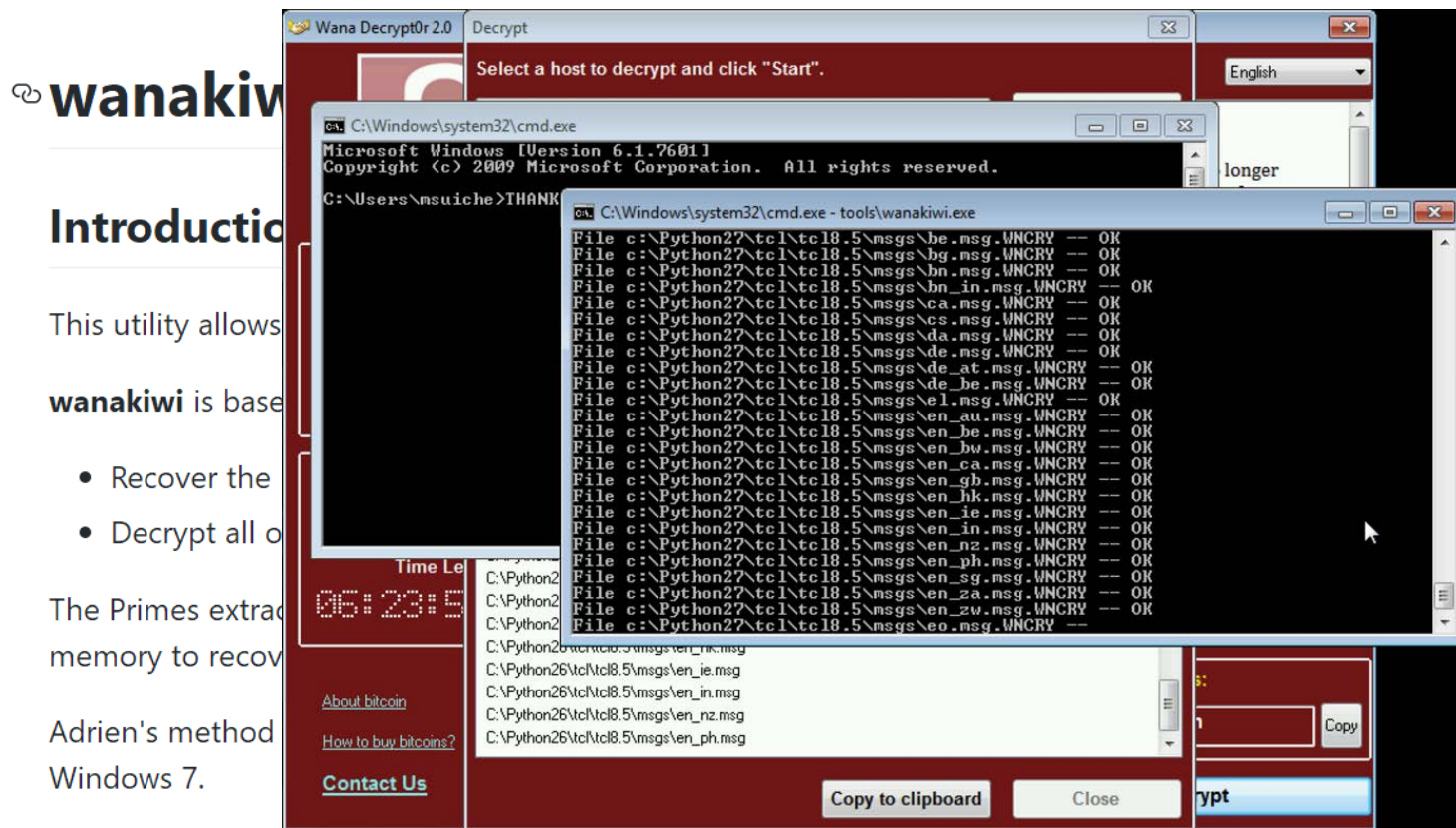
## □ 实际攻击场景2：病毒/恶意代码分析

```
qmemcpy(&szUrl, sinkholeddomain, 0x39u); // previously unregistered domain, now sinkholed
v8 = 0;
v9 = 0;
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0); // do HTTP request to previously unregistered domain
if ( v5 ) // if request successful quit
{
    InternetCloseHandle(v4);
    InternetCloseHandle(v5);
    result = 0;
}
else // if request fails, execute payload
{
    InternetCloseHandle(v4);
    InternetCloseHandle(0);
    detonate();
    result = 0;
}
return result;
```

|

# Man-At-The-End攻击

## 实际攻击场景2：病毒/恶意代码分析



WanaCrypt process

can be extended to

# Man-At-The-End攻击

---

## □ MATE攻击的动机之一：信仰

- 互联网精神 -- 开放、分享
- 商业软件 -- 闭源、收费授权

伟大领袖毛主席教导我们：哪里有压迫，哪里就有反抗

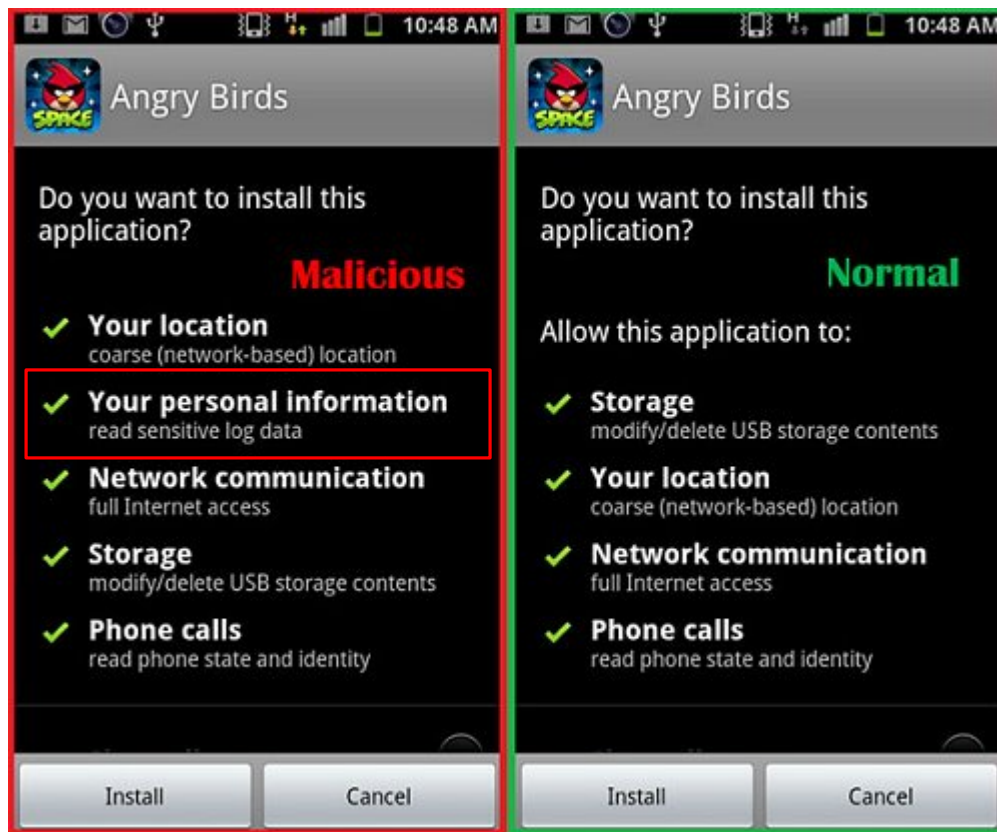
# Man-At-The-End攻击

## □ MATE攻击的动机之二：利益



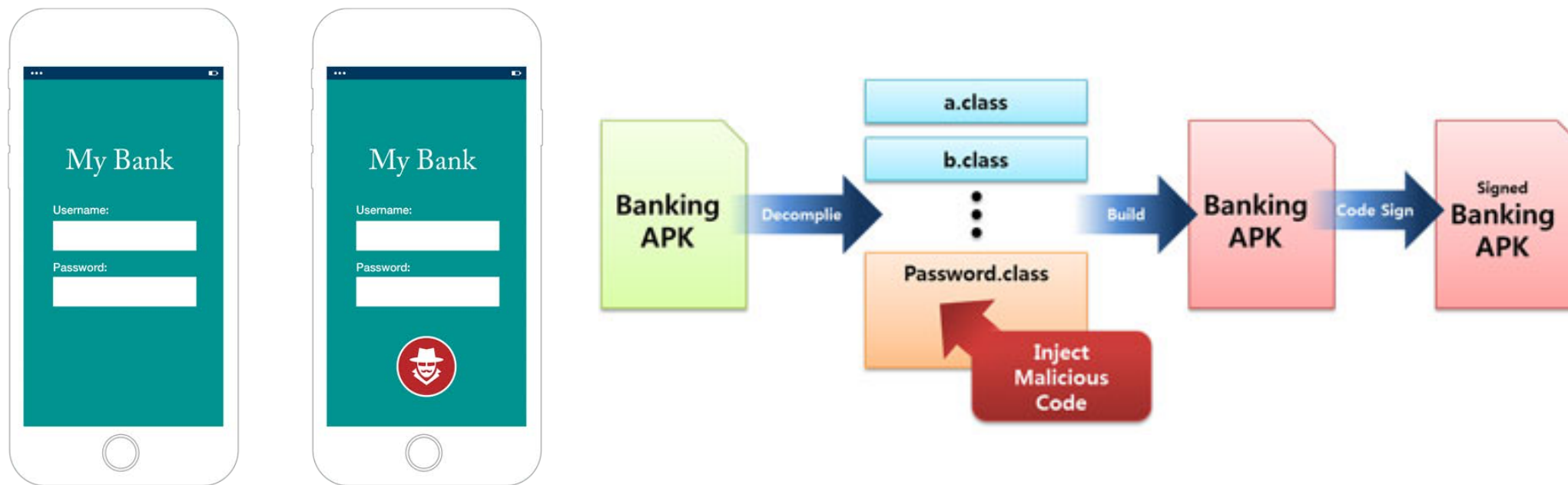
# Man-At-The-End攻击

## □ MATE攻击的动机之二：利益



# Man-At-The-End攻击

## □ MATE攻击的动机之二：利益





# Man-At-The-End攻击

## □ MATE攻击的动机之二：利益





# Man-At-The-End攻击

---

- 危害：合法收益的损失



# Man-At-The-End攻击

---

## □ 危害：合法收益的损失

Cybersecurity has become a top concern for companies and other organizations around the world. These and other factors — including increased awareness of the importance of proper SAM, and years of education and enforcement — contributed to a modest decrease in unlicensed software use in more than a decade, from 43 percent to 39 percent.

Accompanying the global decline in the use of unlicensed software was a corresponding drop (4 percent in constant-dollar terms) in the commercial value of unlicensed software, to \$52.2 billion.

Yet despite these positive developments, for 72 of the 116 markets covered in the study, more than half of the total PC software deployed in 2015 was unlicensed; in 37 markets, 75 percent or more was unlicensed. There is still much more to be done.

# Man-At-The-End攻击

## □ 危害：与网络攻击高度关联



Cyberattacks cost businesses more than \$400 billion in 2015.



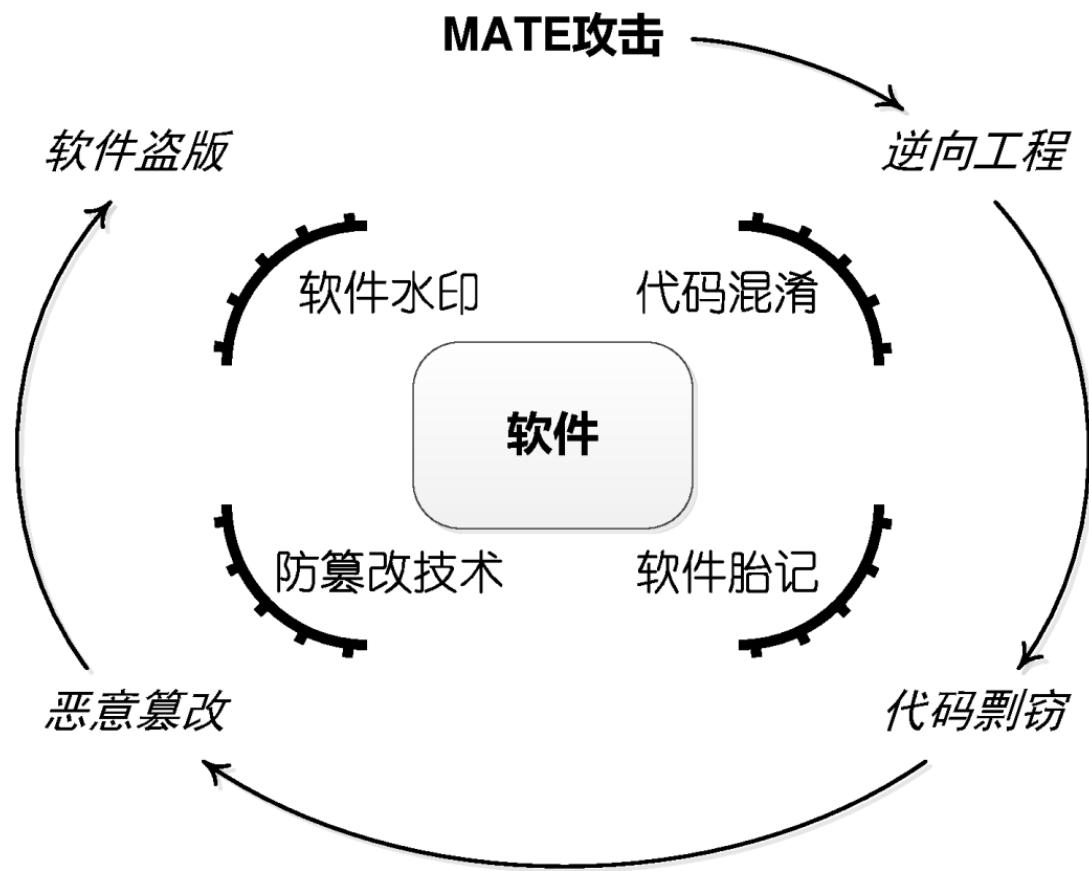
A strong connection exists between cyberattacks and the use of illegitimate or unlicensed software (see A Strong Correlation: Malware and Unlicensed Software on page 4).



Too many CIOs are not controlling their networks and, in fact, underestimate significantly how much unauthorized software has been deployed.

# Man-At-The-End攻击

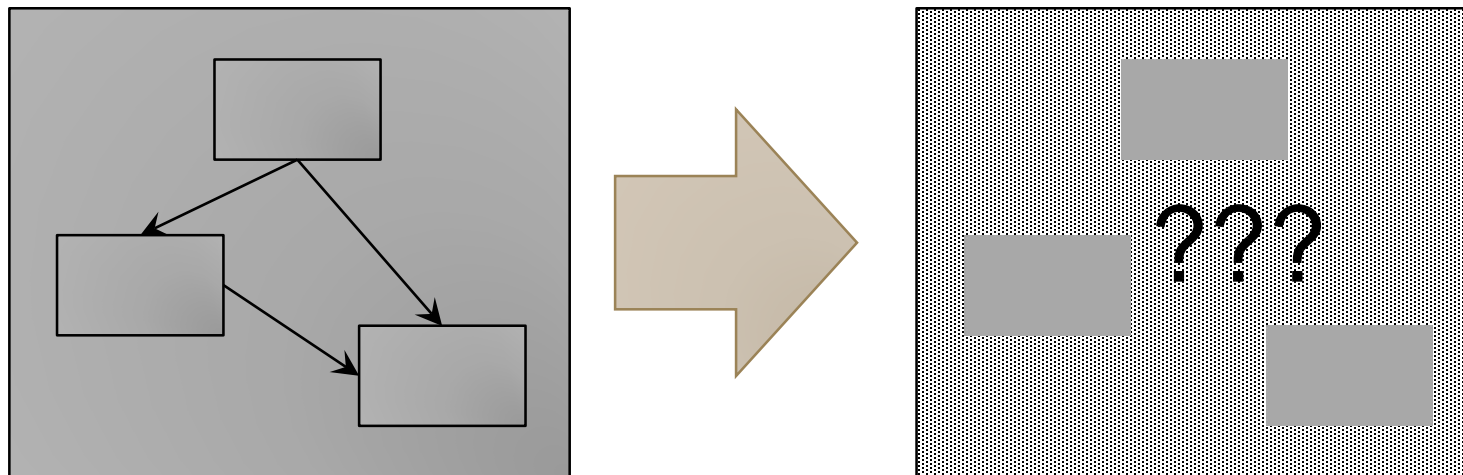
□ 反制措施:



# 代码混淆

---

- 目标：阻止对软件实施非授权的逆向分析



- 核心方法：语义保留的程序变换

# 代码混淆

---

□ 案例：



# 代码混淆

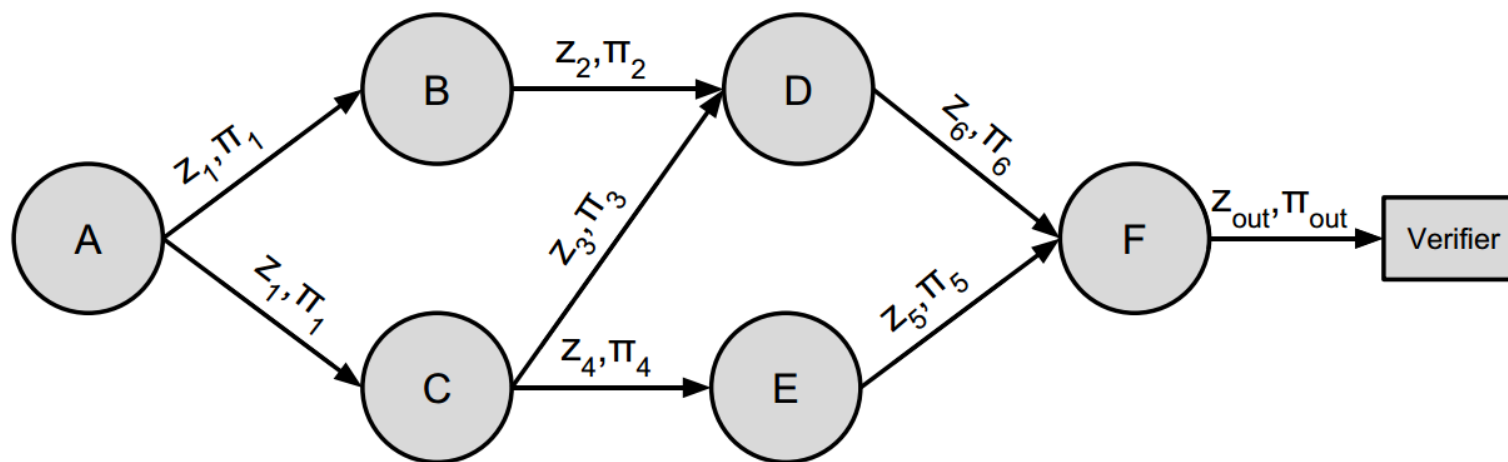
---

## □ 相关知识：

- 安全性理论（安全目标及其可实现性）
- 一些主要的代码混淆方法
- 局限性

# 软件防篡改

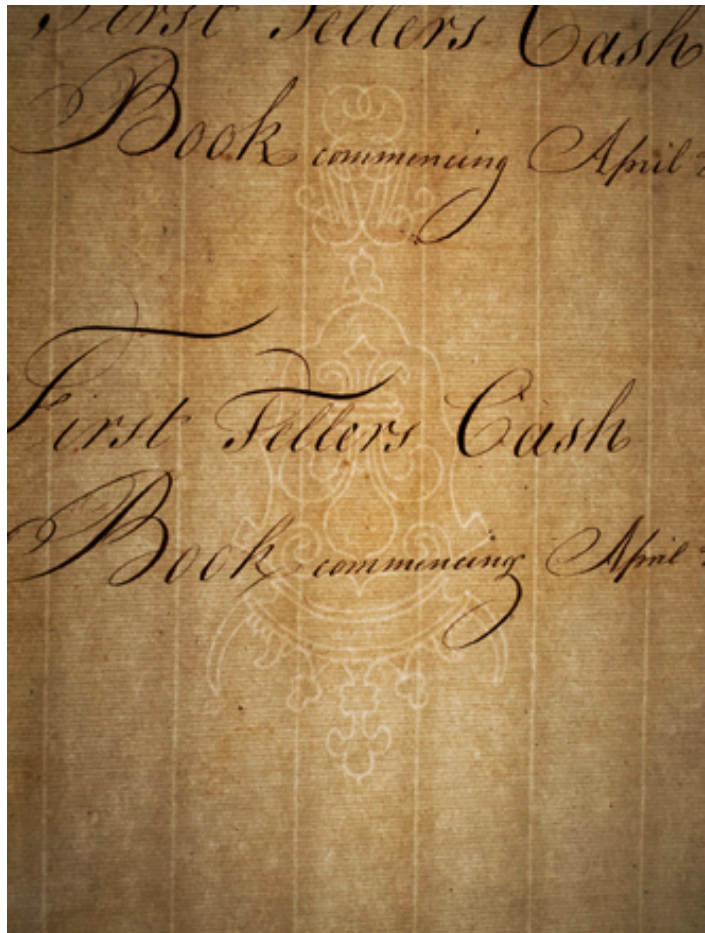
- 目标：使软件能够自行发现（甚至阻止）对自身的恶意篡改
- 举例：Proof-Carrying Data



- 相关知识：现有的几种软件防篡改技术概览

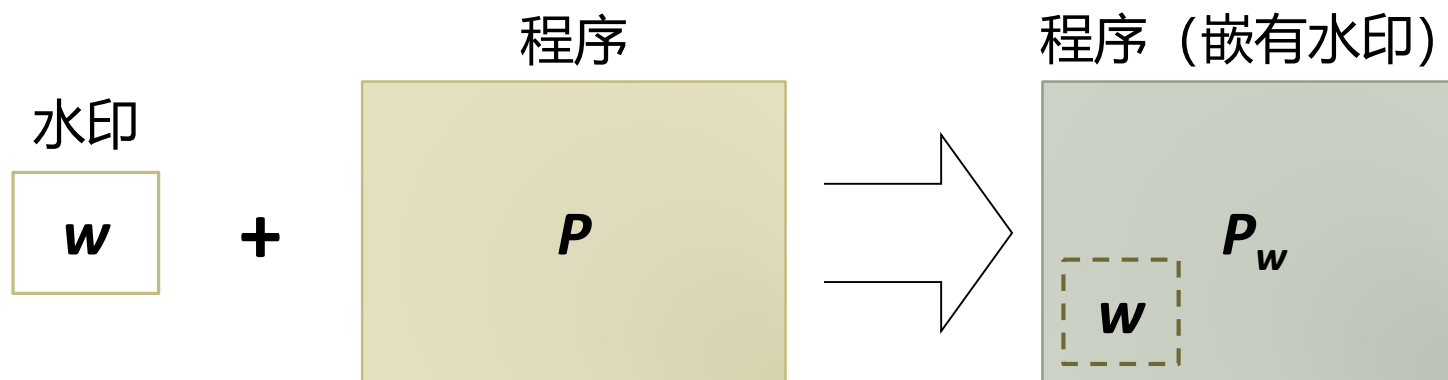


# 软件水印



# 软件水印

- 目标：在软件中嵌入用于标识其版权归属的秘密信息



- 相关知识：
  - 几项关键的安全性指标
  - 主要方法及其不足等

# 软件胎记



照着代码?  
**搞不定!**



但是.....



# 软件胎记

---

- 目标：对指定程序功能抽象出本质性的特征组合，作为该程序的唯一标识
- 与软件水印的区别：
  - 水印是人为嵌入的声明信息（信息由嵌入者决定，与目标软件无关）
  - 胎记是对软件的某种“侧写”（信息完全取决于软件语义，不可控）
- 相关知识：现有基于软件胎记的代码剽窃检测技术概览

# What's next?

---

## □ 代码混淆

- 安全性理论（安全目标及其可实现性）
- 一些主要的代码混淆方法
- 局限性