QCon 全球软件开发大会
INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

BEIJING 2017

代码未写，漏洞已出

——谈谈设计不当导致的安全问题

SPEAKER / 于旸

主办方 Geekbang. 极客邦科技 InfoQ

演讲者简介

于旸 @tombkeeper

从事安全技术研究 15 年

涉猎较多，研究过网络、软件、硬件、无线等
各类安全技术

精通较少，主要擅长的还是软件安全

腾讯玄武实验室
TENCENT'S XUANWU LAB

公众号和微博“腾讯玄武实验室”
每天推送国际最新安全技术资料

安全问题的成因：设计不当、实现不当、使用不当

设计不当又分两种：单点设计不当、多点耦合不当

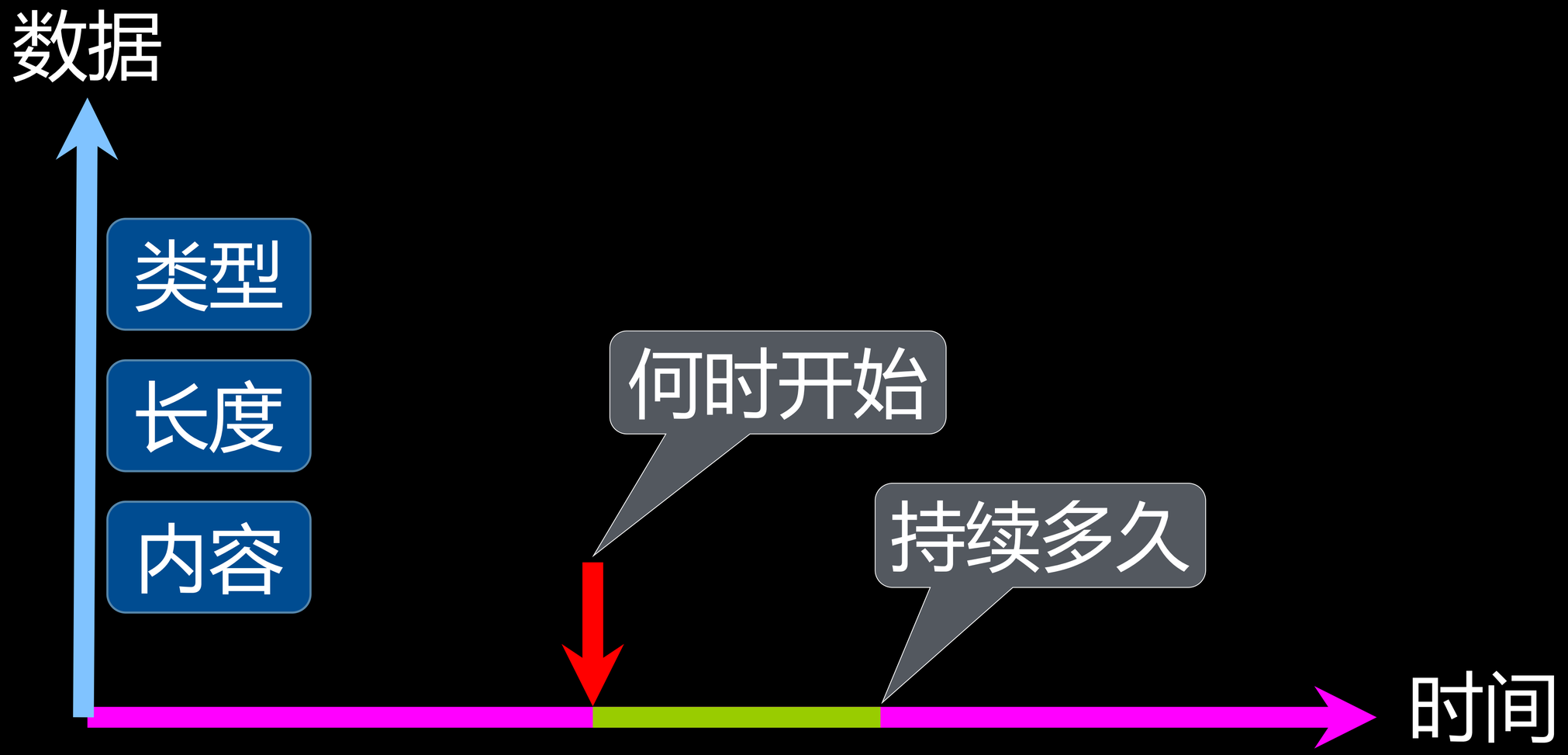
多点耦合要考虑：系统和系统的耦合、系统和人的耦合

比较数据的学问

Java 6.0 的 isEqual()

```
public static boolean isEqual(byte digesta[], byte digestb[]) {
    if (digesta.length != digestb.length)
        return false;
     for (int i = 0; i < digesta.length; i++) {
        if (digesta[i] != digestb[i]) {
            return false;
        }
    }
    return true;
}
```

引发安全漏洞的因素



安全的 isEqual()

```
public static boolean isEqual(byte[] a, byte[] b) {
    if (a.length != b.length) {
        return false;
    }
    int result = 0;
    for (int i = 0; i < a.length; i++) {
      result |= a[i] ^ b[i]
    }
    return result == 0;
}
```

里外不是人的 FTP 协议

被动模式：破坏防火墙策略
主动模式：FTP Bounce 攻击

FTP Bounce

```
# nc 172.0.0.1 21
220 sun8 FTP server (SunOS 5.8) ready.
USER anonymous
331 Password required for anonymous.
PASS user@sun
230 User anonymous logged in.
PORT 192,0,0,1,4,3
200 PORT command successful.
NLST
150 ASCII data connection for /bin/ls (192.0.0.1,1027) (0 bytes).
226 ASCII Transfer complete.
PORT 192,0,0,1,4,4
200 PORT command successful.
NLST
425 Can't build data connection: Connection refused.
```

(4 x 256) + 3 = 1027

(4 x 256) + 4 = 1028

支付系统和交易系统的耦合不当

BadBarcode 问题

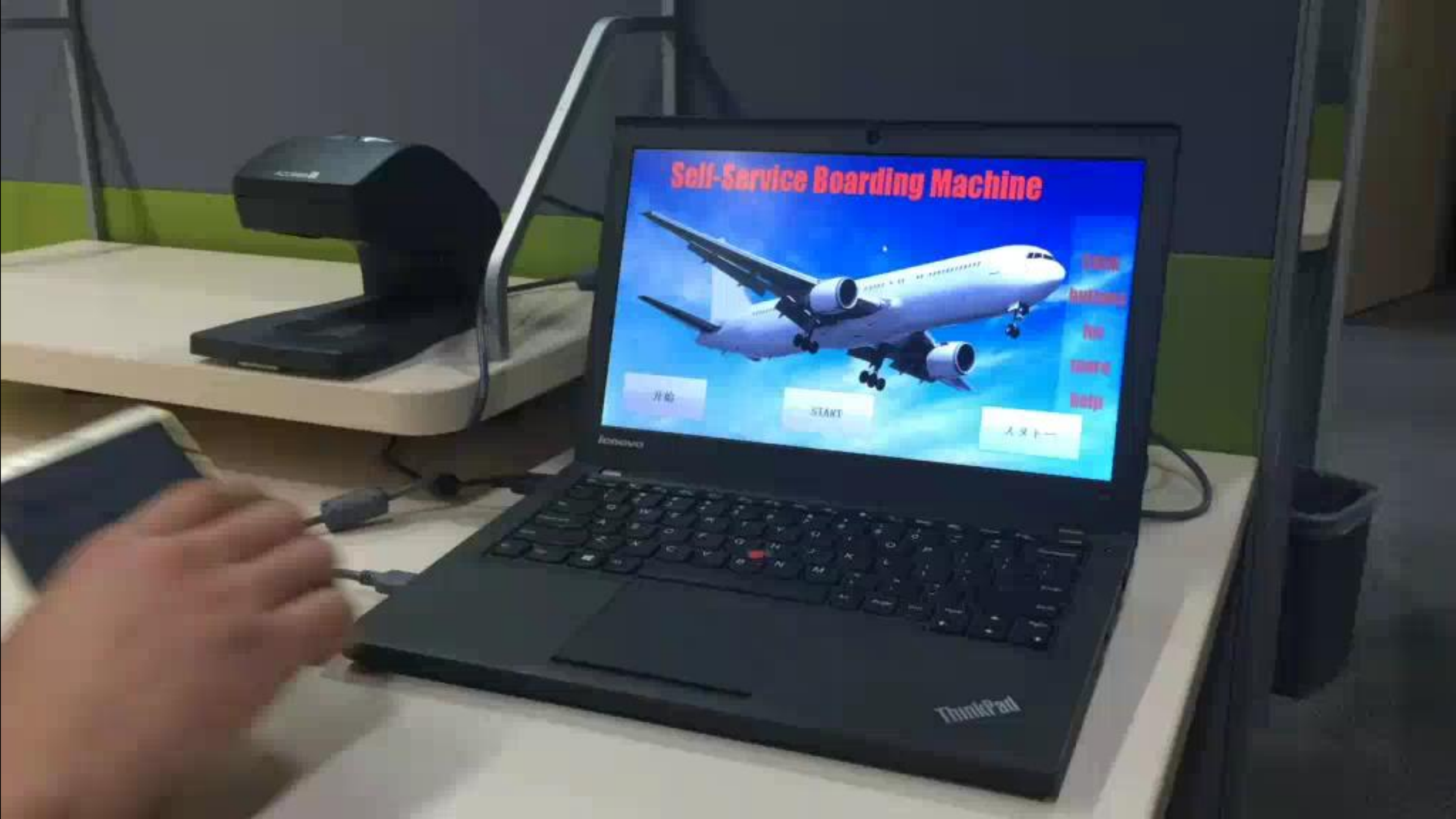
条码阅读器

条码阅读器的原理

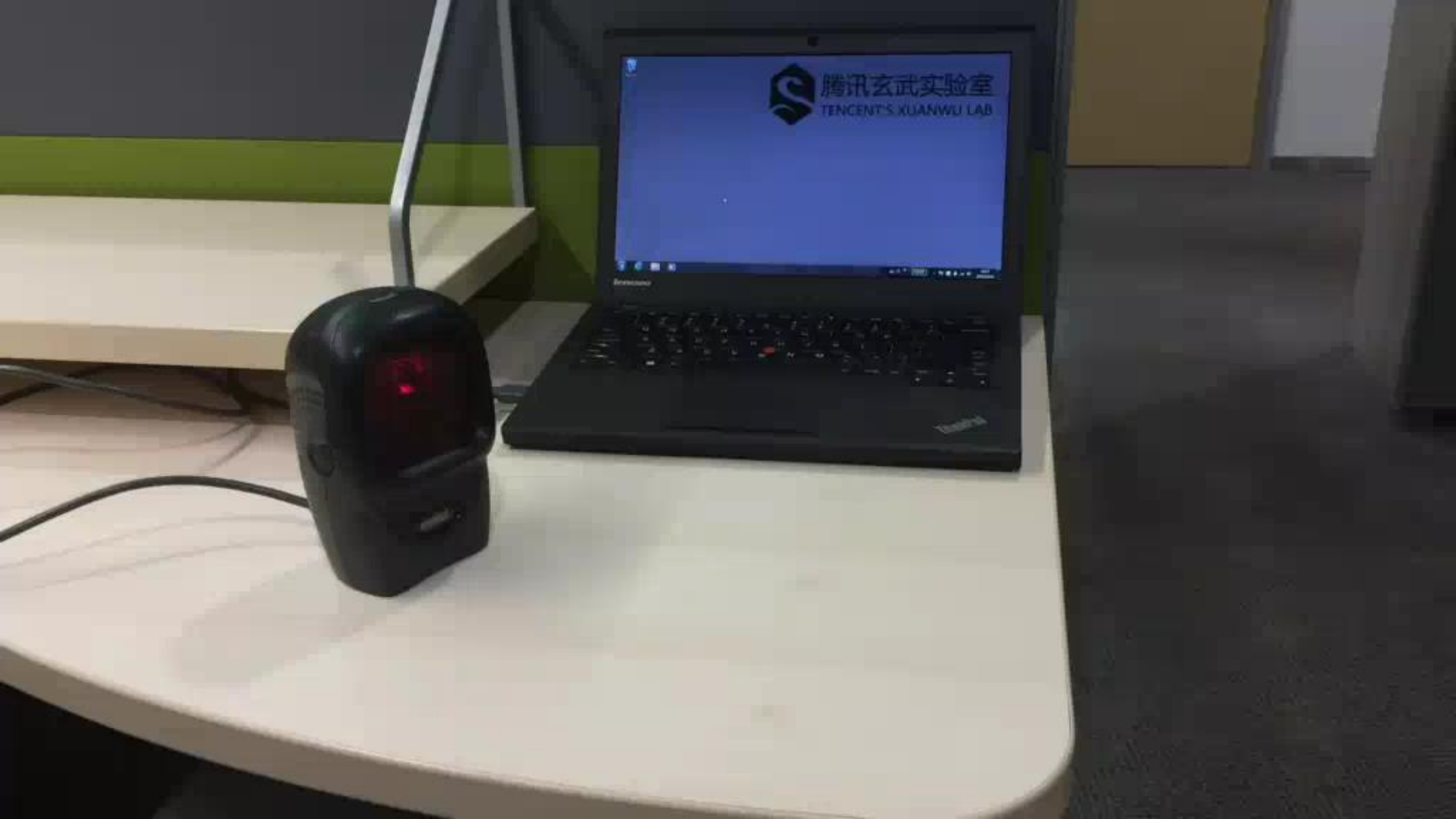
Laser/LED
CCD/CMOS
…

UPC/EAN
Code 39
Code 128
…

RS232
PS/2
USB HID
…


Self-Service Boarding Machine
START
ThinkPad

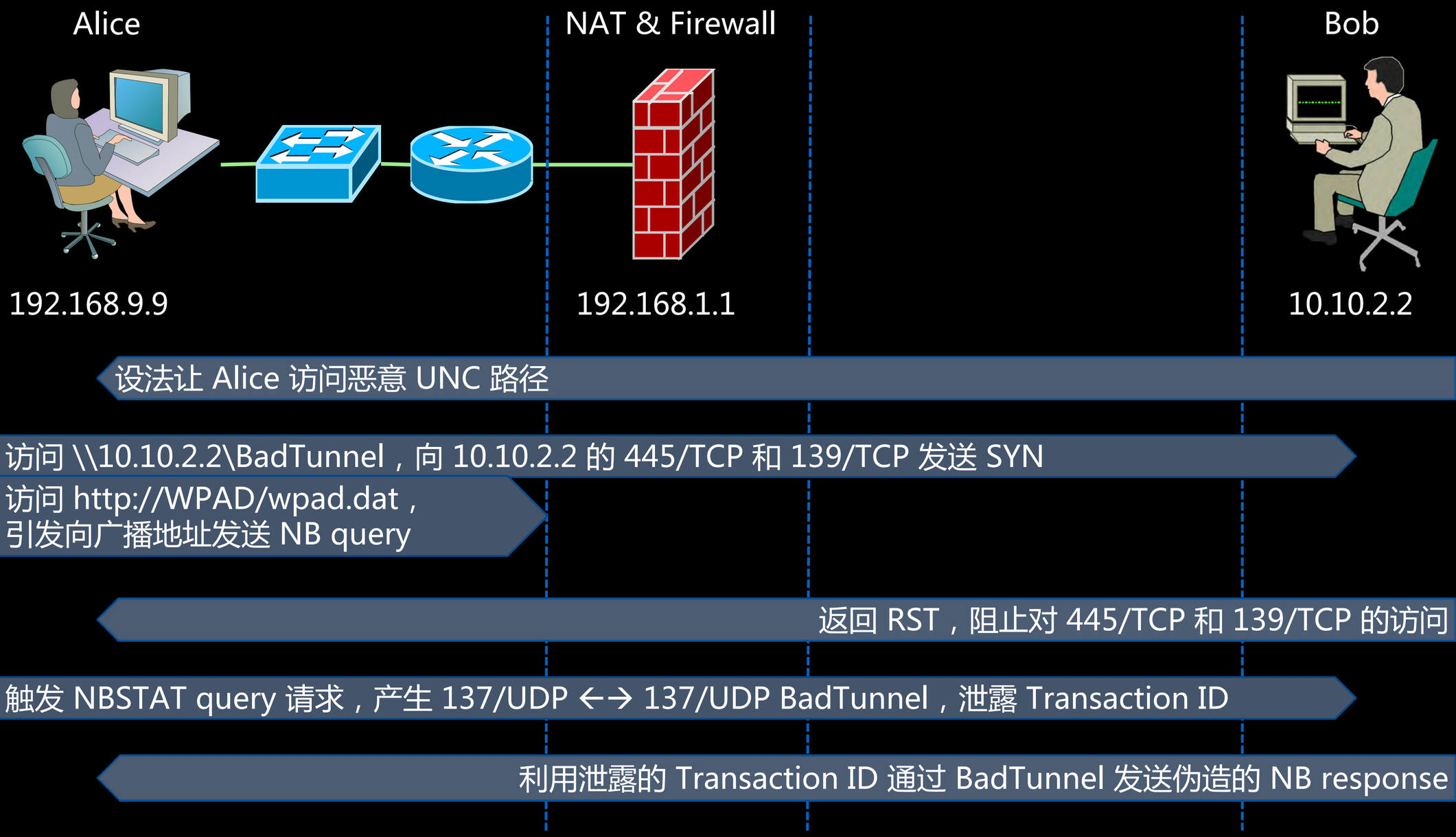

腾讯玄武实验室
TENCENT'S XUANWU LAB


腾讯玄武实验室
TENCENT'S XUANWU LAB

BadTunnel 问题

以下全都是正常的协议、系统设计：

1. UDP 协议无会话
2. 广播请求可接受网段外回应
3. Windows 默认开启 WPAD
4. Windows 文件处理 API 默认支持 UNC path
5. Windows 连接 139 和 445 端口失败后会发起 NBSTAT query
6. NBNS 无论作为服务端还是客户端，都使用同一个端口号
7. NBNS Transaction ID 递增而不是随机
8. NBSTAT query 和 NB query 共享同一个计数器
9. 系统在实现 WPAD 时也使用WEB缓存机制和 NBNS 缓存机制


Alice
NAT & Firewall
Bob
192.168.9.9
192.168.1.1
10.10.2.2
设法让 Alice 访问恶意 UNC 路径
访问 \\10.10.2.2\BadTunnel，向 10.10.2.2 的 445/TCP 和 139/TCP 发送 SYN
访问 http://WPAD/wpad.dat，
引发向广播地址发送 NB query
返回 RST，阻止对 445/TCP 和 139/TCP 的访问
触发 NBSTAT query 请求，产生 137/UDP ←→ 137/UDP BadTunnel，泄露 Transaction ID
利用泄露的 Transaction ID 通过 BadTunnel 发送伪造的 NB response

“短信保管箱”

“自助换卡”

“是故圣人不治已病治未病，不治已乱治未乱”

关注QCon微信公众号，
获得更多干货！

Thanks!

INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

主办方 Geekbang. 极客邦科技 InfoQ