网络空间安全技术

杭州电子科技大学

网络空间安全学院&浙江保密学院

王秋华

01
内容

第一章　网络安全概论

1.1 网络安全的基本概念和目标

1. 网络安全的概念

- 网络安全：网络环境下的信息安全
- 网络安全：网络环境下的信息系统中分布的主机、链路和转发节点中的信息不受威胁，没有威胁、危害和损失。信息系统能够持续提供服务。
- **网络安全：**网络中的硬件、软件得到保护，网络中的信息不会因偶然的或者恶意的原因而遭到破坏、更改和泄露，网络能够持续、不间断地提供服务。

1.1 网络安全的基本概念和目标

从感性认识理解信息安全

- 如果我们计算机的操作系统打过了最新的补丁（Patch）是不是就可[illegible]是安全的?
- 即使操作系统及时打过了补丁，但是系统中一定还有未发现的漏洞
- 0 day漏洞就是指在系统商不知晓或是尚未发布相关补丁前就被掌握或者公开的漏洞信息。

- 纪录片《零日漏洞》 17:55
- 揭秘：地下黑市TheRealDeal提供0day漏洞交易服[illegible]
- http://www.freebuf.com/news/64549.html

JOOMLA	$3,000-20,000
vBulletin	$5,000-30,000
ADOBE READER	$5,000-40,000
MAC OSX	$20,000-60,000
MICROSOFT EXCEL	$40,000-100,000
ANDROID	$40,000-150,000
FLASH OR JAVA BROWSER PLUG-INS	$50,000-120,000
MICROSOFT WORD	$60,000-120,000
MICROSOFT WINDOWSV	$70,000-150,000
FIREFOX OR SAFARI	$70,000-180,000
INTERNET EXPLORER	$80,000-200,000
CHROME	$90,000-200,000
NGINX	$60,000-150,000
APACHE	$80,000-250,000
IOS	$120,000-300,000

从感性认识理解信息安全

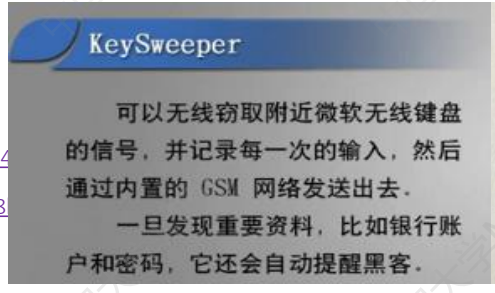
- 如果我们的邮箱账户使用了强口令（Password）是不是就是安全的?
- 即使使用了强口令，但是用户对于口令保管不善，例如遭受欺骗而泄露，或是被偷窥，或遭受撞库攻击
- 另一方面，由于网站服务商管理不善，明文保存用户口令并泄露用户口令，均会造成强口令失效。

- 撞库攻击相关视频：[法治在线]法治故事警惕“撞库”

从感性认识理解信息安全

- 如果我们的计算机从互联网完全断开是不是就可以确保我们计[illegible]?
- 即使我们的计算机完全与互联网断开，机器的硬件仍有被窃或是遭受自然灾害等破坏的风险
- 计算机中的数据仍有通过移动存储设备被传出的威胁。

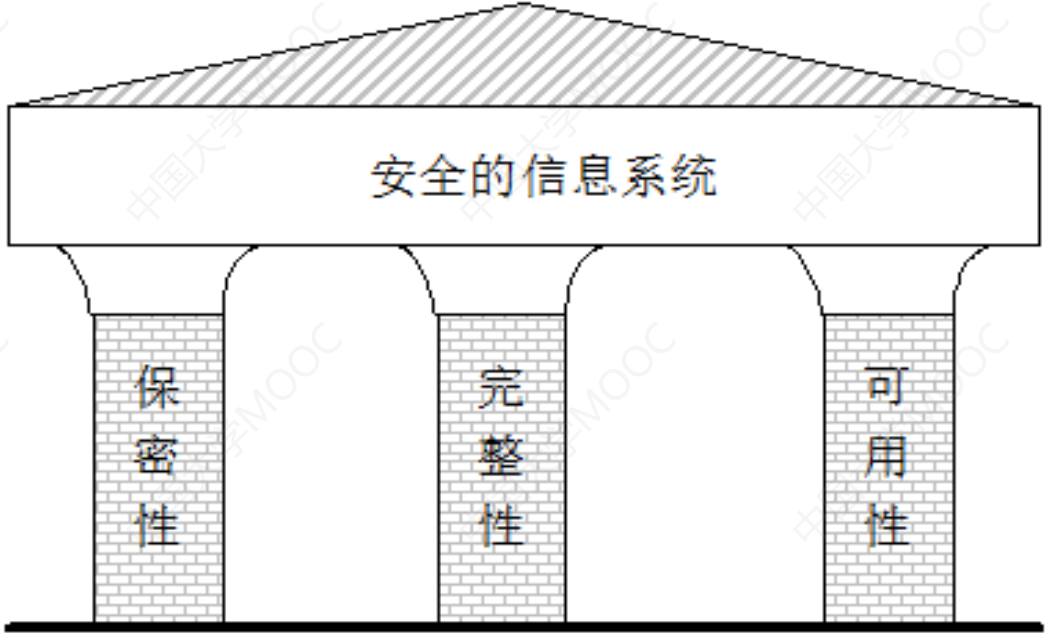
- 案例：视频：震网病毒
- 如何黑掉一台根本不联网的电脑
- https://mp.weixin.qq.com/s?__biz=MzU0ODczMTEwOQ==&mid=2247488548&idx=1&sn=dae8abb4301dc363994927c6f9f25edb49328a3c034ad26a60b3a000&mpshare=1&scene=23&srcid=0808fhS8



2. 网络安全的目标（需求）

- 保密性
- 完整性
- 可用性
- 不可抵赖性
- 可控性

3. CIA安全模型



Confidentiality　Integrity　Availability

4. 每个安全目标的含义及达到该目标的技术/措施

- **保密性：** 防止信息泄露给非授权的个人或实体，只为授权用户使用的特性。

- 思考：有哪些措施？
  - （1）网络中传输 <---->**加密**
  - （2）计算机中存储<----->**访问控制**

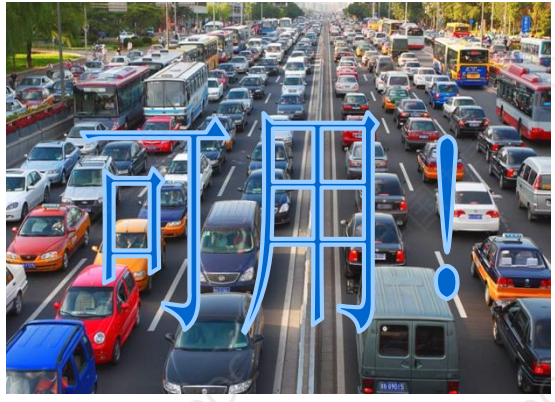
4. 每个安全目标的含义及达到该目标的技术/措施

- **完整性：**指数据未经授权不能进行改变的特性，即确保信息在存储或传输过程中保持不被篡改，删除和伪造的特性。

- 思考：有哪些措施？
  - **预防**和**检测**
  - **预防：**通过阻止任何未经授权的改写企图
  - **检测：**验证数据是否被破坏<-->消息完整性认证 ----**消息认证技术**

4. 每个安全目标的含义及达到该目标的技术/措施

- **可用性：**信息被授权实体访问并按需使用的特性。



- 思考：有哪些措施？
  - 备份与灾难恢复
  - 应急响应
  - 系统容侵等

4. 每个安全目标的含义及达到该目标的技术/措施

- **不可抵赖性**（不可否认性）：在信息交换过程中，所有参与者都不能否认和抵赖曾经完成的操作或承诺的特性。
  - 思考：有哪些措施？
    - **数字签名技术**
    - **可信第三方认证技术**

4. 每个安全目标的含义及达到该目标的技术/措施

- **可控性：**对信息的传播过程及内容具有控制能力的特性。

- 思考：有哪些措施？
  - **信息监控**
  - **审计**
  - **过滤** 等

审计：是通过**对网络上发生的各种访问情况记录日志，并对日志进行统计分析**，是对资源使用情况进行事后分析的有效手段，也是发现和追踪事件的常用措施。

1.2 网络安全的重要性和面临的挑战

没有**网络安全**
就没有**国家安全**。

——习近平

信息化与国家安全——信息战/网络战

- “谁掌握了信息，控制了网络，谁将拥有整个世界。”

——美国著名未来学家阿尔温.托尔勒

- “今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。”

——美国总统克林顿

- “信息时代的出现，将从根本上改变战争的进行方式。”

——美国前陆军参谋长沙利文上将

1.2 网络安全的重要性和面临的挑战

一、“棱镜计划”事件分析

二、“震网病毒”事件分析

三、“乌克兰停电”事件分析

1.2 网络安全的重要性和面临的挑战

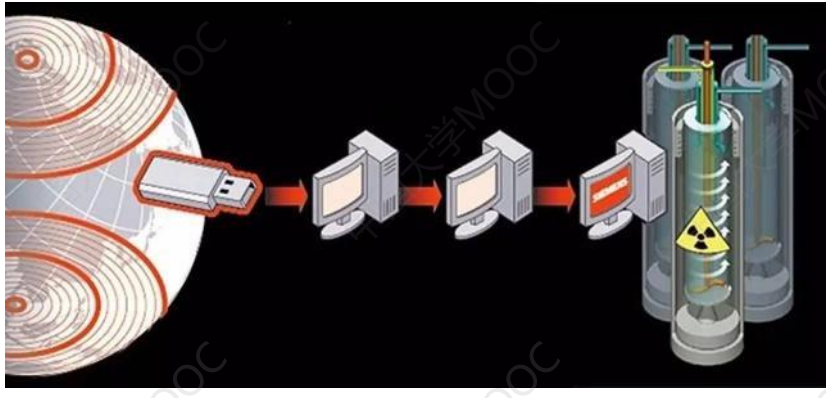
• 典型案例1：棱镜计划

- 棱镜计划是如何实施全球监控的?
- 美国为何能实施这么庞大的监视项目?
- 讨论：美国的霸权主义还体现在哪些方面?
- 棱镜计划给我国网络信息安全的反思?
- 为应对瞬息万变的网络安全局势，近年来，中国在网络安全方面出台哪些法律法规?

1.2 网络安全的重要性和面临的挑战

• 典型案例2：震网病毒

- 1.攻击发起者是谁?
- 2.被攻击目标是什么?
- 3.实施攻击的目的是什么?
- 4.攻击中利用了哪些技术或手段?
- 5.与传统的网络攻击相比较，有哪些新的特点?



• 典型案例3：乌克拉大停电

- 1.攻击发起者是谁?
- 2.被攻击目标是什么?
- 3.实施攻击的目的是什么?
- 4.攻击中利用了哪些技术或手段?

1.3 引发网络安全问题的原因

1. 什么是网络安全问题?

网络环境下发生的破坏信息**可用性、保密性、完整性、不可抵赖性和可控性**等的事件。

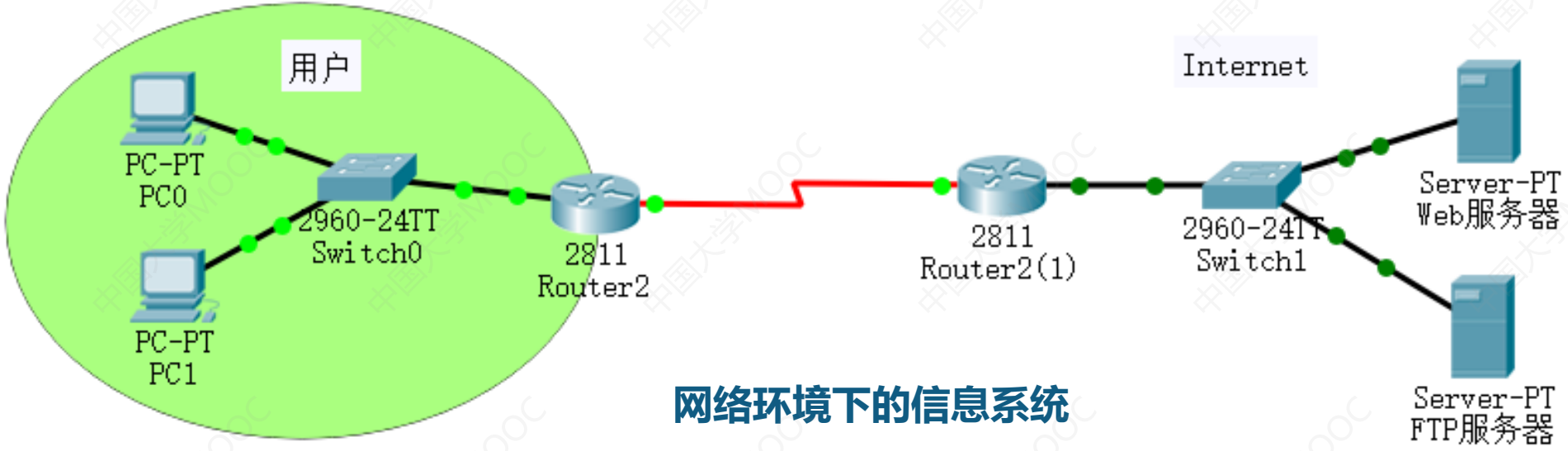
2. 引发网络安全问题的原因?

（1）网络和网络中信息资源的重要性

（2）技术与管理缺陷

- 信息系统脆弱性（硬件、系统软件和应用软件固有缺陷）
- 协议的脆弱性（通信协议固有缺陷）
- 人为因素（不当使用和管理）

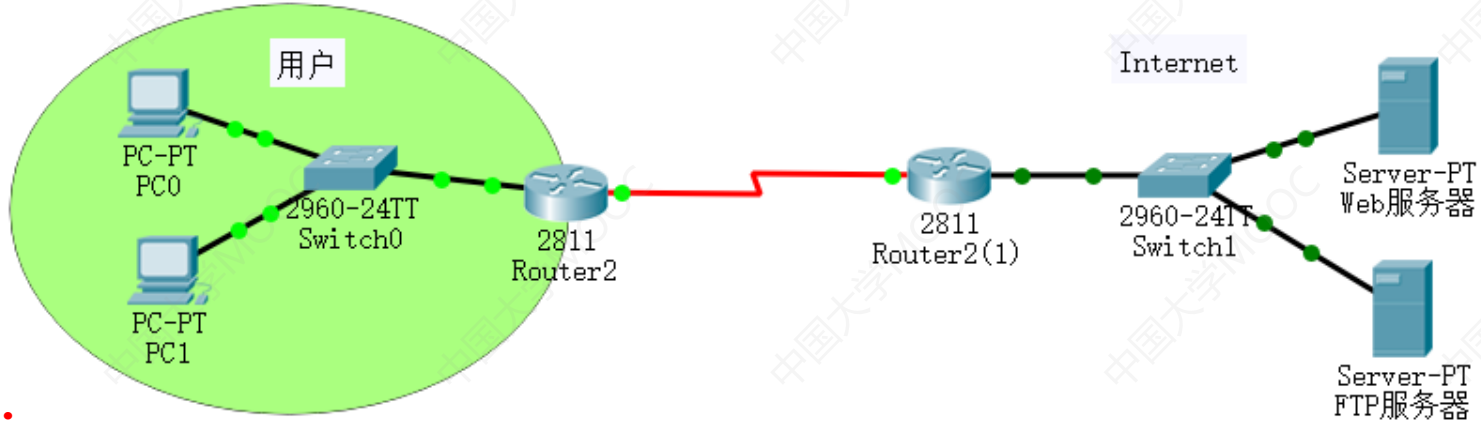
1.4 安全模型



网络环境下的信息系统

- 如果你是**网站的安全管理员**，你会给该网络环境下的信息系统设置怎样的**安全目标**?

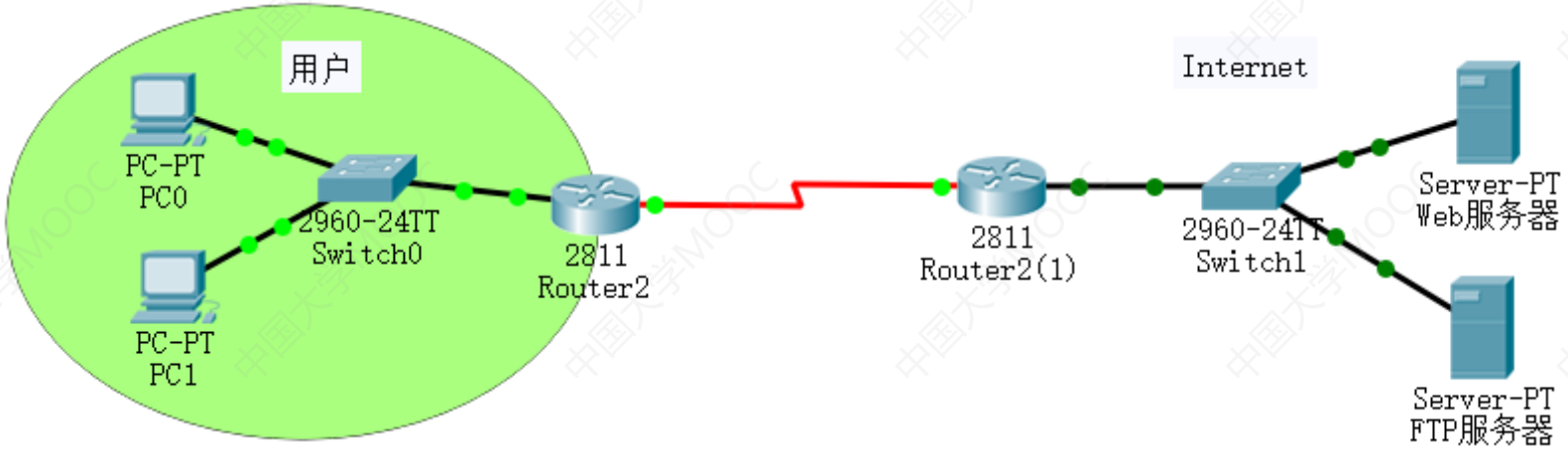
1.4 安全模型



1. 定安全目标：

- 保证网络畅通，保证Web服务器和FTP服务器能够提供服务 **可用性**
- 保证用户登录服务器时使用的私密信息不被泄露 **保密性**
- 保证用户和服务器之间传输的信息没有被篡改，或者能够检测出所有发生的篡改 **完整性**
- 可以对访问服务器的终端实施控制 **可控性**
- 用户不能抵赖向服务器发送的请求消息 **不可抵赖性**

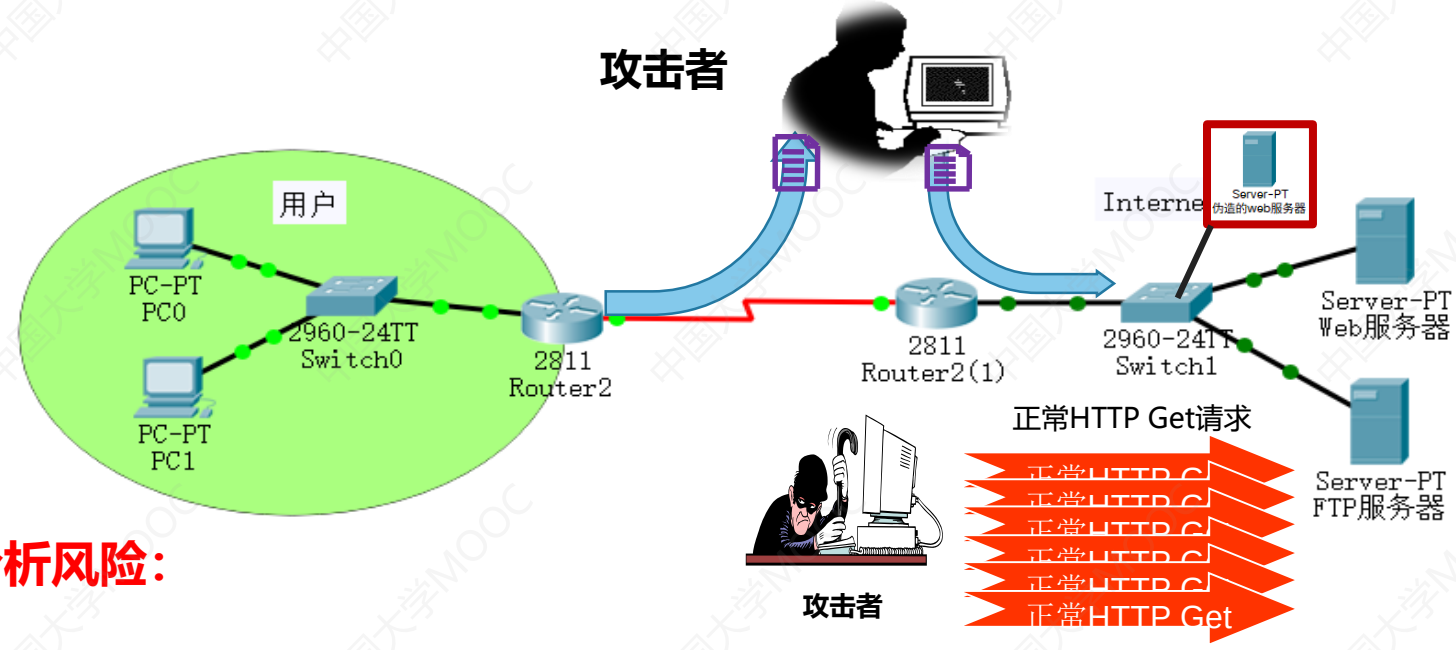
1.4 安全模型



风险：发生安全问题的可能性

- **分析该信息系统可能存在或遭遇的风险有哪些?**
- **或者你以一个攻击者的视觉来看，你会采用哪些措施来攻击该系统。**

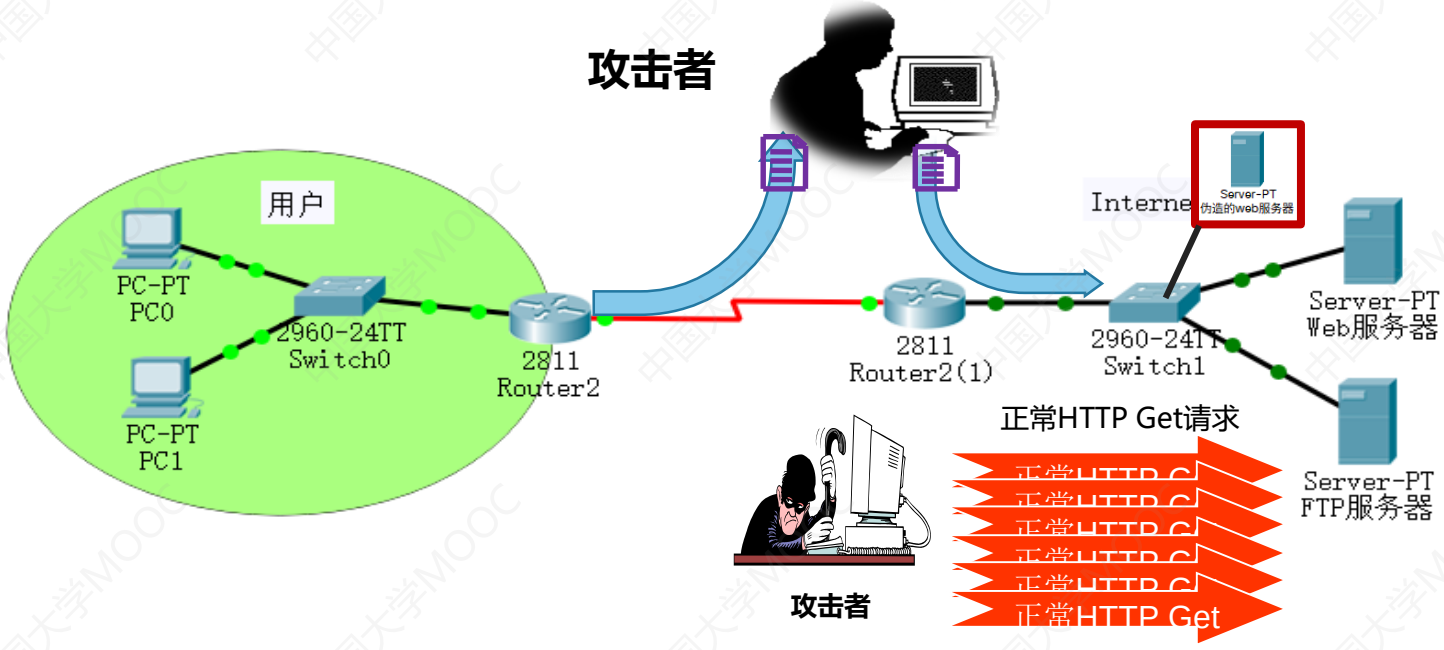
1.4 安全模型



2. 分析风险：

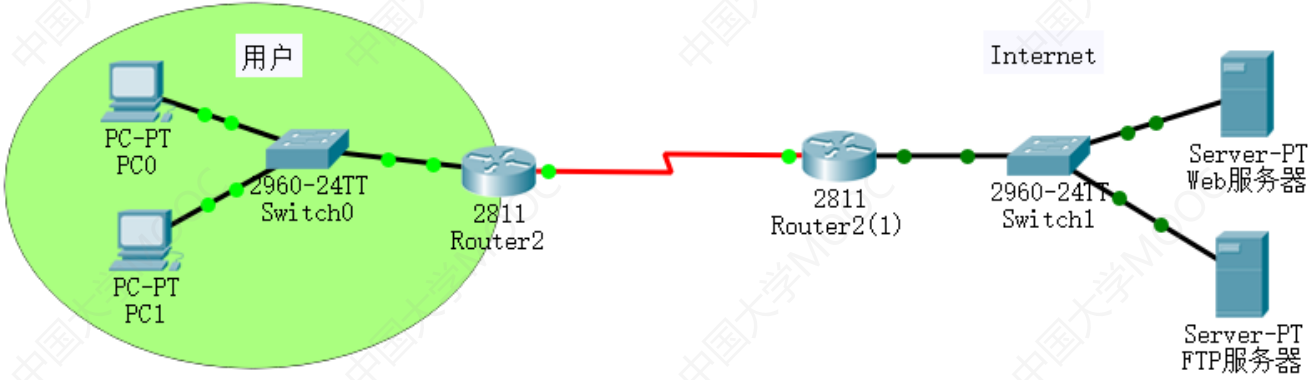
1. **伪造服务器**骗取用户登录用的私密信息（如钓鱼网站）
2. 截获用户与服务器之间传输的数据
3. 对服务器实施攻击，如SQL注入、XSS，拒绝服务器等

1.4 安全模型



- 你会制定哪些规则（**安全策略**）来实现信息系统的安全目标，消除或降低信息系统存在的安全风险?

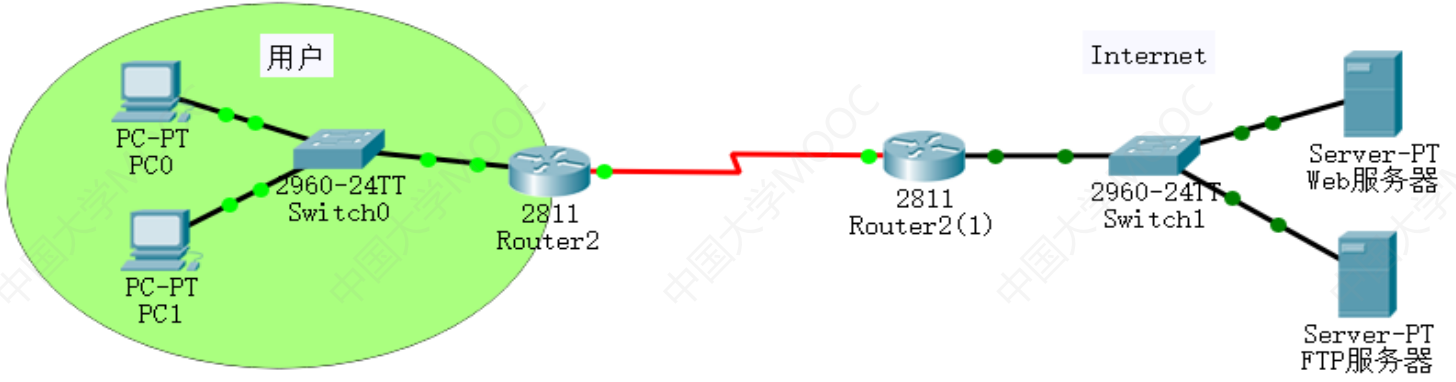
1.4 安全模型



3. 制定安全策略：

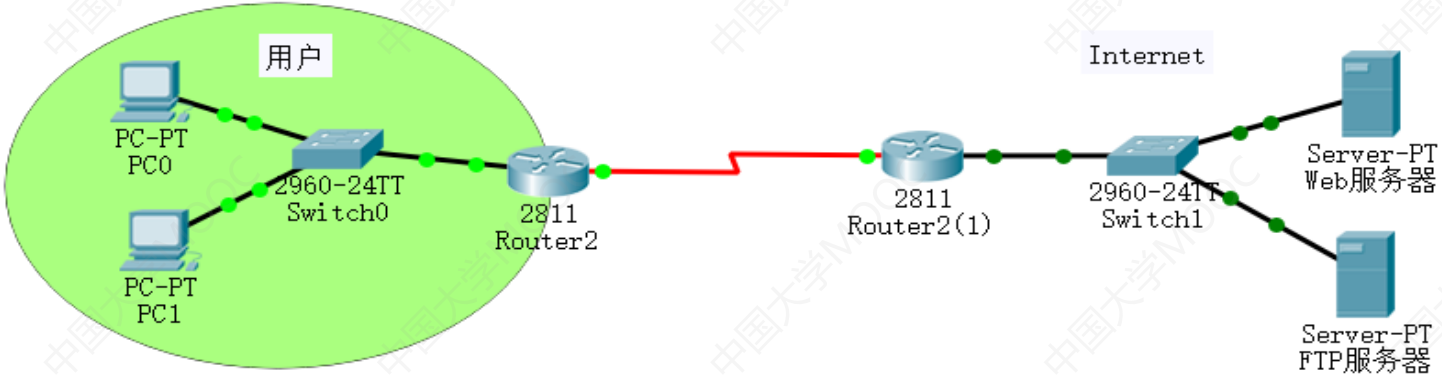
1. **限制**向服务器发送数据的**终端范围和数据类型**，只允许特定终端向Web服务器发送超文本传输协议（HTTP）请求消息
2. 实现终端用户与服务器之间的**双向身份鉴别**
3. 终端**加密**传输登录服务器时使用的私密信息
4. 终端对发送给服务器的请求消息进行**数字签名**
5. 对终端与服务器之间传输的数据进行**完整性检测**
6. 网络和服务器对黑客入侵行为进行**监控**

1.4 安全模型



- 你会采用哪些网络**安全技术**来保障上述你制定的安全策略的实施?

1.4 安全模型



4. 采用防护技术：

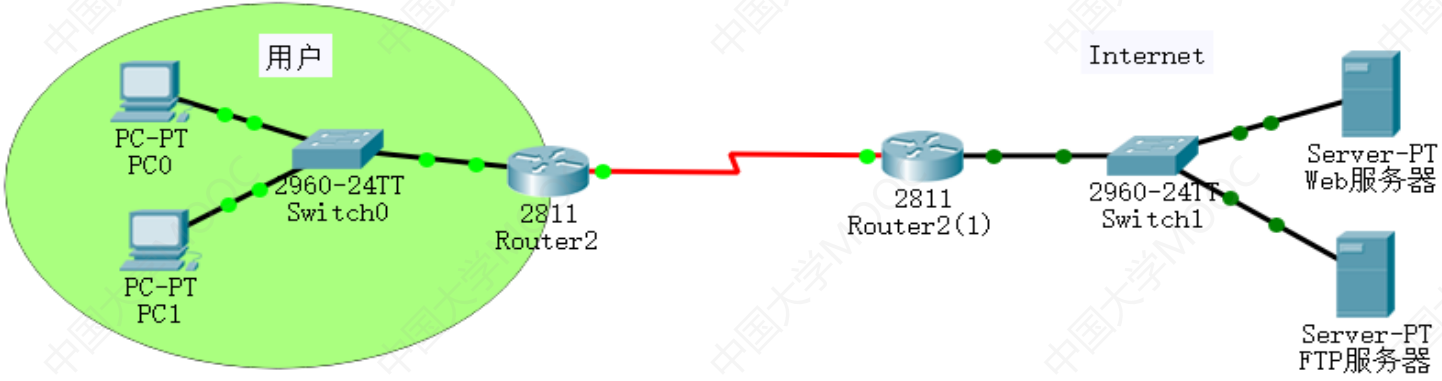
1. 在路由器内嵌**防火墙**，控制与服务器交换数据的终端范围和数据类型

2. 用户和服务器之间**采用安全协议**，由安全协议实现双向身份鉴别、数字签名、数据加密和完整性检测等安全功能

3. 网络关键链路安装**网络入侵检测系统**，服务器安装**主机入侵检测系统**

4. 通过服务器的**日志和审计功能**，记录下发生在服务器上的所有访问过程。

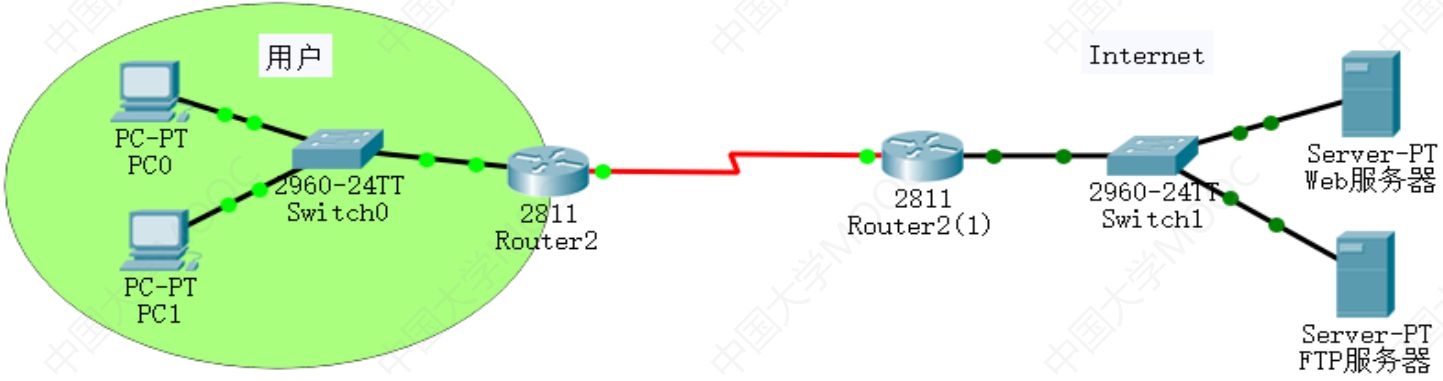
1.4 安全模型



5. 检测：

- 检测过程是通过网络**入侵检测系统**和主机入侵检测系统发现黑客入侵行为的过程。由入侵检测系统实时监控网络行为和数据访问服务器过程，一旦发现异常行为，立即**报警**，并在日志服务器中记录下与异常行为相关的信息。

1.4 安全模型



6. 响应：

- 响应过程是发现网络异常行为的情况下，使**信息系统恢复正常服务**功能的过程。

为了使上图所示的网络环境下的信息系统**具备响应能力**，你需要做到那几点?

1.4 安全模型

安全模型：以建模的方式给出**解决安全问题的方法和过程**。

P2DR安全模型

核心要素

策略：为实现信息系统的**安全目标**，对所有与信息系统安全相关的活动所制订的规则。

防护：信息系统的安全保护措施，由安全技术实现。

检测：了解和评估信息系统的安全状态，发现信息系统异常行为的机制。

响应：发现信息系统异常行为后采取的行动。

安全=风险分析+安全策略+安全措施+漏洞监测+实时响应

有问题及时反馈，加强沟通交流！