《物理与网络通信安全》知识点串讲

第 1 节 物理与环境安全

1.场地选择
1.1 场地选择:自然条件、社会条件、其他条件。
1.2 抗震和承重：抗震及承重（国标 《结构抗震设计规范》）
—特殊设防类
—重点设防类
—标准设防类（A 类、B 类、C 类）
—普通机房
2. 环境安全
2.1 防火：燃烧条件、材料、方式
2.2 电力：双电源、UPS、发电、多路供电
2.3 电磁：线路、设备、电源的电磁防护。
2.4 通风空调和供暖（HVAC）：HVAC（下送风、上回风，侧送风、侧回风，正气压等）。
2.5 防静电手段：温度、湿度、接地。
2.6 应急照明。
2.7 应急通道、出口、标识。
3. 区域与设备防护
3.1 物理区域的安全：区域范围、检测措施、访问控制（标识、指纹、IC 卡等）。
3.2 检测报警措施：CCTV、红外监控、特殊监控、声控、振动报警。
3.3 设备存放安全：责任人、环境、授权使用、维护、防丢失等安全。

第 2 节 网络安全基础

1.OSI 七层：物理、链路、网络、传输、会话、表示和应用。
2.安全开放互联体系架构
2.1 **8 个机制**：加密、数字签名、访问控制、完整性、路由控制、流量填充、公证、鉴别交换。
2.2 **5 种服务**：鉴别、完整性、保密性、访问控制、抗抵赖。
2.3 实现关系。

- 加密：保密
- 数字签名：完整性、鉴别、抗抵赖。
- 访问控制：访问控制。
- 完整性：完整。

- 路由控制：访问控制。
- 流量填充：保密性。
- 公证：抗抵赖。
- 鉴别交换：鉴别、访问控制。

2.4 网络层、应用层均实现 5 种服务。
3.封装和解封装：规则的标准化和接口标准化。
4.TCP/IP 四层：网络接口层、网络层、传输层、应用层。
5. 四层的各层安全协议：
5.1 网络接口层：PPTP、L2F、L2TP
5.2 网络层：IPSEC（AH\ESP）
5.3 传输层：SSL、TLS（按照 ISO/OSI 的七层则其属于 4.5 层，按照 TCP/IP 四层划分则其属于应用层）
5.4 应用层：X.509，SSH，PGP、S/MIME、PEM（后三个是电子邮件的安全协议）。
6.无线网络安全
6.1 结构：STA（终端）、AP（接入点）、AS（后端系统）
6.2 无线安全的问题：开发认证、信息泄露、共享密钥等。
6.3 无线网络安全的协议：
（1）WEP：密码管理及加密有缺陷。
（2）WPA/WPA2：加密传输、身份鉴别（AP 对 STA 的鉴别）。
（3）WAPI：WAI 身份认证，WPI 加密封装：
双向三鉴别和高强度传输加密（支持 ECC 算法）。
7. IPV6：地址数量是 2^128，内置 IPSEC 安全协议。
8.蓝牙：解决可信环境中的数据交换。
9.RFID 的安全。RF（10+KHZ-5.8GHZ）

第 3 节 网络安全技术与设备

第 1 部分 防火墙
1. 作用：边界的防护（访问控制）、隔离、访问控制、记录。
2. 实现和分类：

序号	类型	层次	控制规则	优点	缺点	应用场景
1	**包过滤防火墙**	三层（网络）	IP、端口、协议	1.规则简单 2.速度快 3.配置简单	1.不能解决应用攻击 2.不能解决异步攻击 3.不能提供地址隐藏	1.简单网络环境 2.应用少
2	**电路代理防火墙**	三层（网络）	IP、端口、协议、**NAT**	1.规则简单 2.比包过滤略慢 3.配置较简单 4.提供地址隐藏	1.不能解决应用攻击 2.不能解决异步攻击	1.简单网络环境 2.应用较少
3	**应用代理防火墙**	3-7 层(应用)	IP、端口、应用协议、应用数据、NAT	1.细粒度高 2.防护应用攻击 3.识别数据内容 4.提供地址转换	1.**速度慢** 2.不能解决异步攻击 3.**误阻断**问题 4.**漏阻断**问题	1.较复杂的网络环境 2.应用较多 3.**应用攻击环境复杂**
4	**WAF-HTTP** 代理防火墙	3-7 层(应用)	IP、端口、HTTP(S)、应用数据、NAT	1.专业化高 2.HTTP 的过滤粒度细 3.识别应用攻击及数据 4.提供代理	1.速度较慢 2.不能解决异步攻击 3.误阻断问题 4.漏阻断问题	1.较复杂的网络环境 2.web 应用较多 3.web 应用攻击环境复杂

5	**状态检测防火墙**	3-7 层（**网络-应用层**）	上下文的攻击特征、**IP、端口、协议**、NAT	1.解决异步攻击 2.安全性高 3.代理 4.3-7 的过滤多样性	1.状态空间大 2.性能水平低 3.误阻断问题 4.漏阻断问题	1.较复杂网络环境 2.高级级别攻击领域
6		**下一代防火墙**		1,继承历史上 5 种防火墙的优点，并解决其缺点。 ——>NGFW 类似于下一代 UTM 2.适用于大数据的环境、云计算的环境。 ——>FW 的虚拟化、数据采集分析提高。 3.下一代防火墙本质不是产品，而是新一代网络安全威胁环境中的边界解决方案。		

3. NAT：静态、动态、端口。
优点：节约公网地址资源、隐藏内部网络信息。
缺点：暴漏防火墙外网口地址和网络位置。
4. 部署
4.1 方式：**单、双、DMZ** 的方式。
4.2 方式：**透明**方式、**路由**方式（NAT）。
4.3 方式：**未明确禁止则允许，未明确允许就是禁止**。

第 2 部分 入侵检测系统

1. 组成：事件**产生器**、事件**分析**、事件**响应**、数据库。
2. 技术：
误用检测-特征检测-黑名单检测-标识检测
异常检测-状态检测-白名单检测-行为检测
对比如下：
误用检测技术：MISUSE-黑名单-特征-标识
优点：**准确性**-高，**误报率-低**。
缺点：**完整性-低，漏报率-高**。
异常检测技术：PROFILE-白名单-状态-行为
优点：完整性-高，**漏报率-低**，
缺点：准确性-低，**误报率-高**。
思考问题：在使用环境中，先启动**白名单模式**，再**黑名单模式**。
3. 分类：

序号	对比项	NIDS	HIDS
1	形态	硬件	软件
2	位置	网络	主机
3	部署方式	并联（数据镜像）	安装部署
4	对象性能影响	网络无影响	主机有影响
5	技术原理	误用检测多，异常检测少	异常检测多，误用检测少
6	及时性	低	高
7	攻击目标的识别准确性	低	高

第 3 部分 其他安全产品

1. 网闸：

组成：外网单元、隔离单元、内网单元。
原理：单向或双向的数据交换及摆渡原理，核心是物理隔离。
2. IPS：防火墙和 IDS 功能的综合。
3. UTM：统一威胁管理系统。
4. SOC：资产管理、事件分析与安全态势感知、统一的安全配置部署。
狭义、广义、大数据等之分。
5. VPN 产品
5.1 **IPSEC**：基于网络层实现。
— AH：身份鉴别、完整性校验、抗重放攻击。
— ESP：在 AH 的基础上，数据包和数据流加密。
— IPSEC：传输模式（透明模式）/隧道模式（路由模式）
5.2 **SSL/TLS**：基于 TCP/IP 四层应用层实现，支持对称加密和非对称密码的数字证书技术，TLS1.2/1.3 版本目前最安全。
— **握手协议**：身份鉴别、密钥协商。
— **记录协议**：数据加密、完整性校验。

第 3 节 网络安全设计规划

1. IATF：三个核心是人、技术和操作；四个保护方面是**本地计算环境、区域边界、网络基础设施和支撑性基础设施**。
2. 安全域：共享安全策略的集合，划分方法包括物理位置、部门、业务、数据、生产特性。
3. IP 规划：从上到下、体系化、节约、扩展。
4. VLAN 划分：MAC、端口、IP 组播等划分。
5. 冗余：**链路**安全、**设备**的冗余及安全、**负载均衡**。
6. 网络设备的配置及安全策略：身份鉴别、安全的访问、权限最小化、服务最小化、日志审计、配置备份、补丁升级、流量分析、网络审计等。

（End）