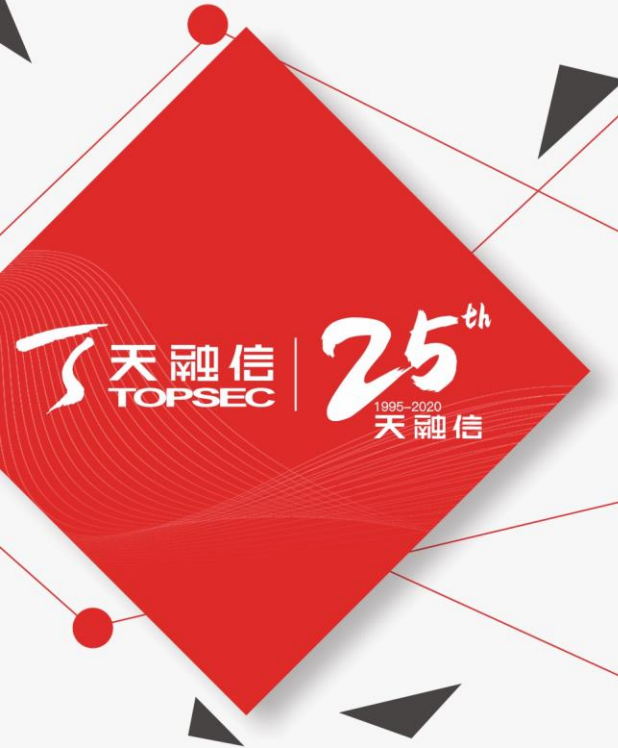


新技术 新思维 催生新安全

--“零信任”安全机制及密码应用

天融信科技集团　景鸿理

目录

CONTENT

新技术新思维 催生新安全

- 民航信息化水平较高，数字化&网络化应用程度较高
- 等保2.0，民航的安全建设已相当成熟，**仍是主战场**
- 5G助力**云计算**、**物联网**，形成泛在互联，催生新认知； [如：SDN、SDP]
- 网络边界**正在瓦解**，基于边界的安全防护体系**正在失效**
- 访问控制，网络安全最基本的保护措施，**应顺应发展趋势**
- 新技术的出现及发展，催生新安全理念—**“零信任”**

网络安全的“零信任”机制

零信任机制的基本思想：

一、**不再以**物理网络边界作为可信任的安全边界，

不再认为我们的内网就是安全的环境；

二、网络中的人及**设备/系统服务**，均应**“全面身份化”**，

其身份属性的**维度需多元化**；

【人； 仪器、设备、智能摄像头、...； 指挥系统 / 调度系统 / 广播系统 ...】

三、所有对网络上仪器/设备/系统服务/业务应用，等资产的访问，

都是不可信任的；

四、任何人对设备及系统服务的访问，

都应该进行“基于身份”的认证和授权，并受到访问控制。

从不信任，总是验证。

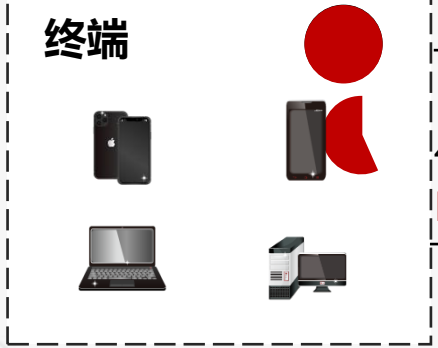
“零信任”安全机制工作过程

- 初始网络不可见，SPA受控可见
- 需要“敲门”

失败流程

成功流程

安装客户端软件



统一身份
控制中心

1.身份认证请求

国密SSL协议[SM2/3/4]

3.客户端授权结果

3.网关授权结果

2.1 认证请求

2.2 认证、授权结果

身份管理
授权管理

- 用户身份
- 用户权限
- 设备状态
- 行为习惯

4.根据授权结果访问网关

国密SSL协议[SM2/3/4]

应用访问控制网关

5.网关控制访问过程

应用系统

“零信任”机制实践经验分享【访问控制范式的颠覆】

- “零信任”安全机制，不是一个独立产品、**是一套“产品s+规则s”的组合应用**
  1.客户端软件【APP】、2.认证/授权系统、3.访问控制网关设备，4.网络协议/控制规范，等；

- **“全面身份化”**是零信任安全**动态访问控制**的基础
  人有身份标识，物和业务系统也有身份标识，信任及**风险度**判定是多维度的；

- 以**身份**为依据，**不再以网络拓扑为依据**，构建基于身份的访问控制体系。
  网络拓扑的边界是固定的，以身份为中心思想的访问控制是泛在的；

- **网络隐藏，服务隐藏**，所有的业务实体都隐藏在零信任**可信接入网关**之后。
  不同于传统的防弹衣，是穿了**“隐身衣”；控制有基于**黑名单 or **白名单的区别；**

- 基于身份的**访问控制是动态的**
  这次你行，下次即便还是你，也不见得行；行也是完成任务的**最小授权**；

- “零信任”机制**注入国产化密码安全基因**，以夯实“信任”基础。

《关保》

重点保护，

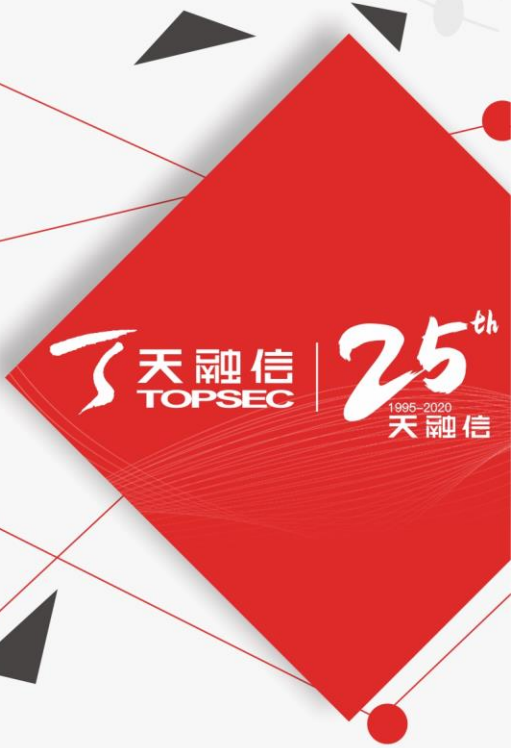
整体防护，

动态风控，

协同参与。

感谢聆听！

天融信科技集团 景鸿理



宣传《密码法》【2019年10月26日 发布】

- **《商用密码管理条例》→《中华人民共和国密码法》**
  - 对核密、普密、商密，都明确了应用规范和管理要求
  - 将在《密码法》的框架下，重新发布《商密条例》，预计明年发布
- 密码是数字信息“**机密性/完整性/真实性/不可否认性**”的根本保证
- 关键信息及系统**应当**使用**商用密码**进行保护。
- 应当使用《网络安全专用**产品目录**》中的密码产品。
  - 商密产品《型号证书》→ **《认证证书》**
- 应**自行或者委托**第三方评估机构开展密码应用安全性评估。

返回

个人简介

- 景鸿理，天融信科技集团，高级副总裁
- **两次荣获“国家科技进步 二等奖”**
- 多次荣获**省部级**科技进步 **一等奖**【包括：密码科技进步、军队科技进步， 等】
- 国家密标委应用专家组成员、北京商密协会监事长
- 中国网安联盟产业合作专委会主任【第一届】
- 发表网安类论文多篇、参与制定网安类标准多个

返回