信息网络安全的目标

网络安全目标

网络安全的目标是为一个分布式系统中的双方建立安全的通信信道。

保密	认证	不可否认	完整
确保信息不会被未经授权的用户访问	确定对方就是自己想要通话的人	涉及签名，防止对方出尔反尔甚至彻底否认发过的信息	确保收到的信息的真实性，没有在途中被篡改或伪造。

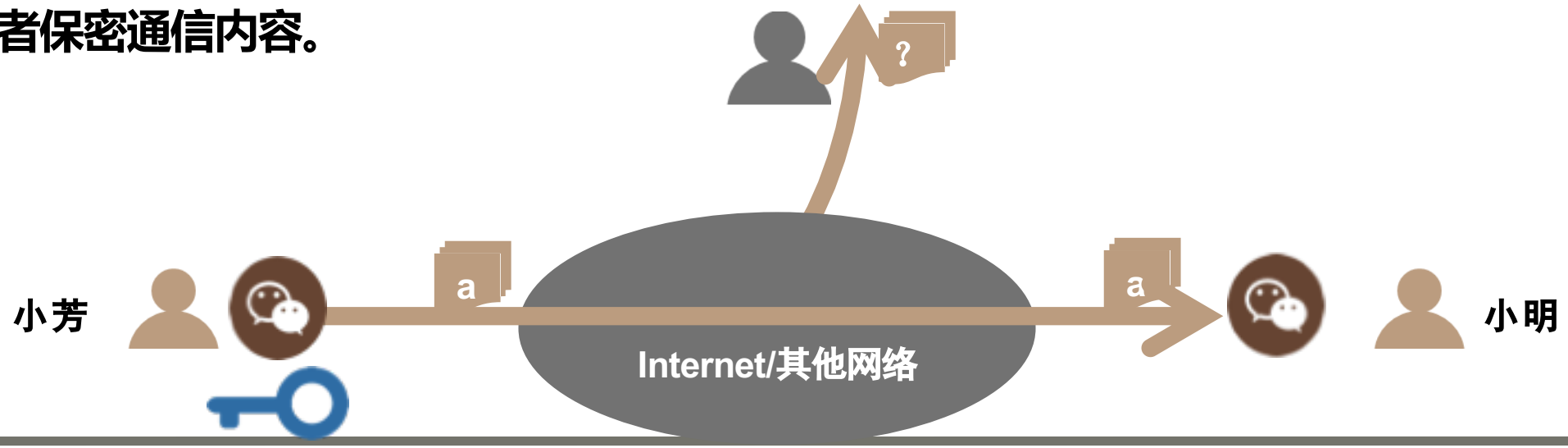
保密性

机密性/保密性（secrecy）：用来确保只有真正的发送者和接收者才能理解被传输消息的内容。

机密途径

- 加密消息（对数据进行伪装）
- 不能被窃取者解密

机密通信常常依赖于一把或多把密钥来加密或者保密通信内容。

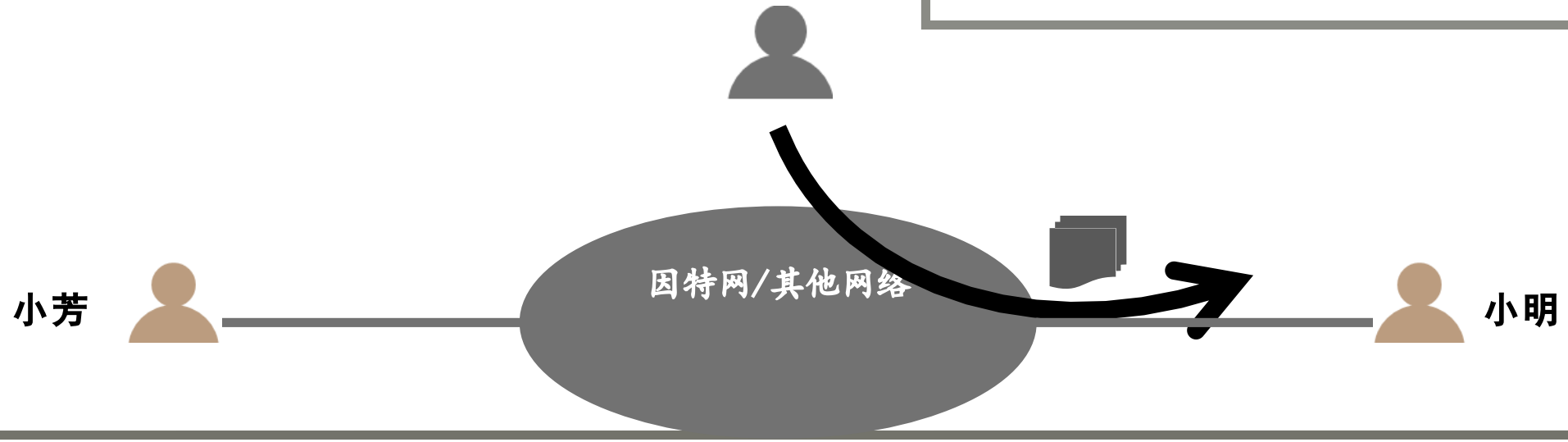


认证

认证性(authentication)：发送者和接收者都必须确认对方就是自己想通信的对象。

认证的目的

- 收到的邮件是来自你认为的那个朋友？
- 有人打电话声称是银行职员，询问银行帐号等私人信息，你会不会回答？

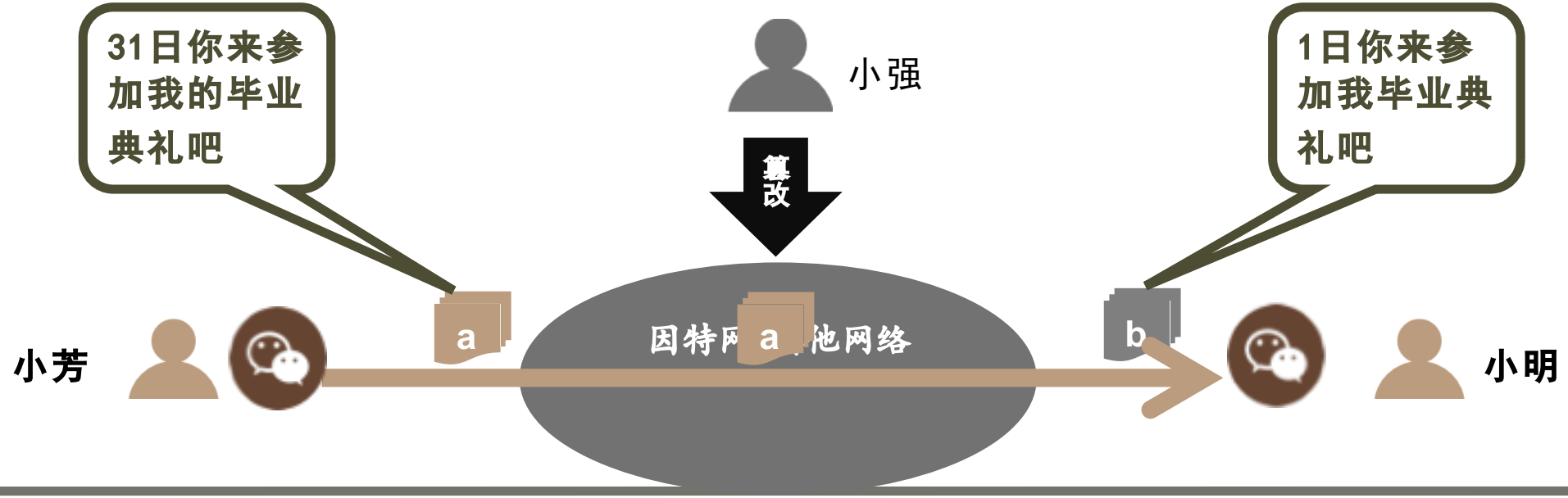


完整性

完整性（message integrity ）：发送者和接收者相互认证对方身份后，还必须确信他们的通信内容在过程中没有被恶意或者偶然修改。

完整性要求

被传输消息没有在途中被篡改

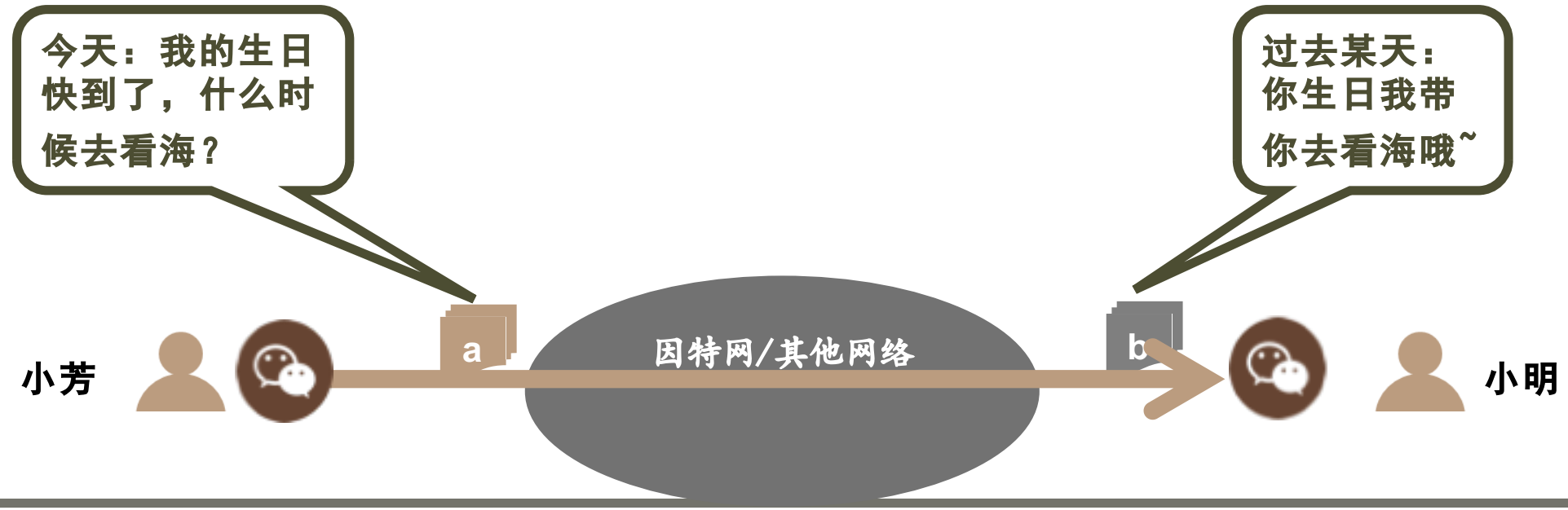


不可否认性

不可否认性/认可性（Nonrepudiation）：发送者不可否认自己发送的信息内容。

认可性/不可否认性

接收者能“证明”消息就是声称的发者发出的。



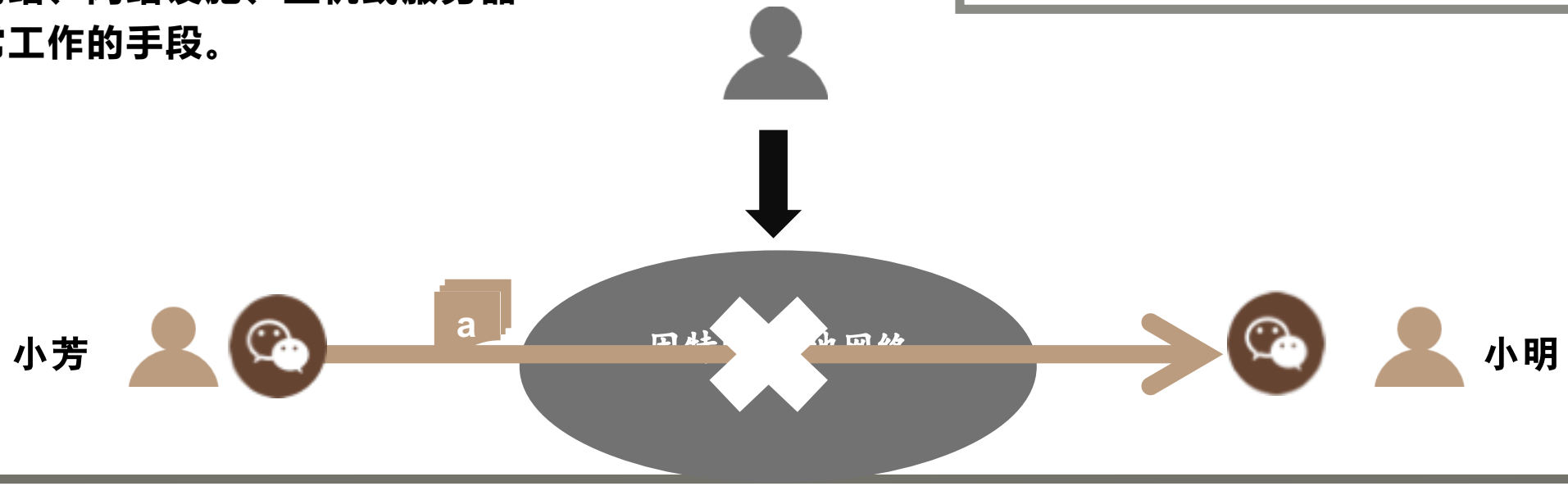
可用性和访问控制

可用性和访问控制（availability & access control）：确保合法用户能使用网络基础设施进行通信。

DoS（Denial-of-service）攻击：一种使得网络、网络设施、主机或服务器不能正常工作的手段。

安全通信的关键要求

- 首先要能通信
- 防止“坏蛋”破坏网络的有效途径是阻止他们的包进入网络（例如，防火墙）

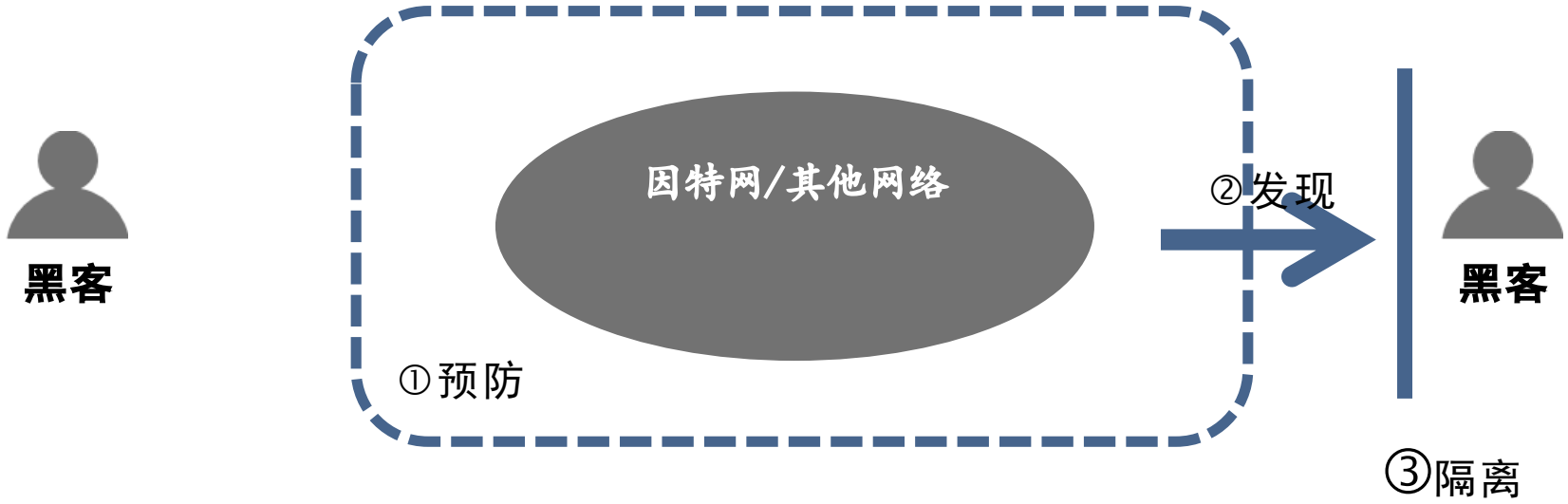


网络协议栈能做什么

- 用户级：用户认证和消息不可否认性
- 端-端加密：对整个连接进行加密，即从进程到进程的加密。
- 防火墙：区分数据包的好坏，让好的数据包正常通过而阻止有问题的数据包进出。
- 链路加密：点对点线路上传输的数据包在离开机器前被加密处理，进入另一台机器时被解密。

安全问题涉及网络协议栈各个层次，没有哪一层能确保网络信息安全，需要综合各层的协同。

完善的网络安全关键要素



保护

- 保护通信和网络资源

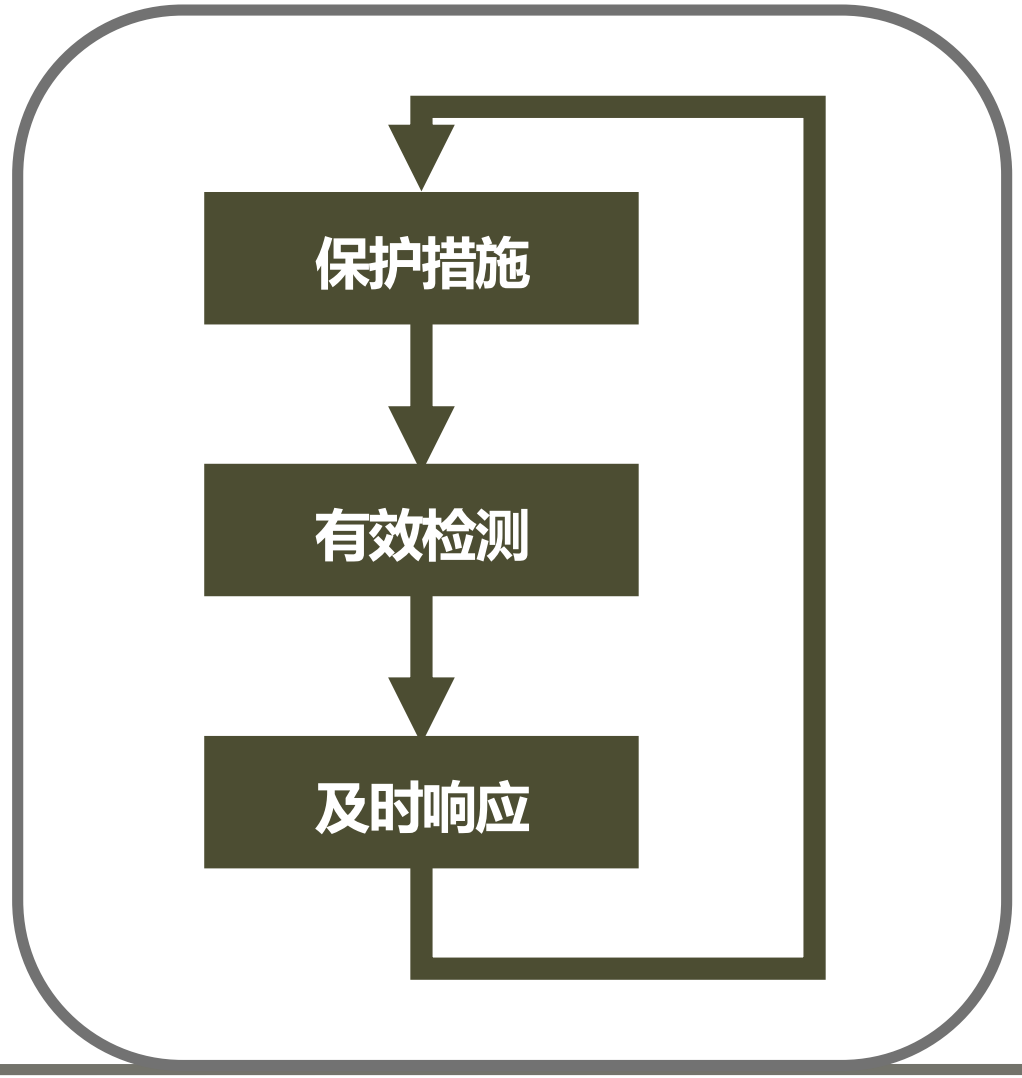
检测

- 检测安全通信是否有漏洞以及网络基础设施是否遭到攻击

响应

- 发现漏洞和攻击时如何反应

完善的网络安全需要多方协同



网络多方协同工作才能提供绿色的通信环境。

- 加密
- 完整性
- 不可否认性
- 用户认证
- 网络安全