智能路由器在家庭网络中的安全考量

家用路由器安全问题

- 家用路由器作为家庭网络的唯一出口，它自身出现安全问题时，影响非常巨大
- 未来物联网时代，大量设备将通过WiFi接入，因此WiFi环境乃至整个家庭局域网本身的安全也变得非常重要。

传统路由器安全情况

- 传统路由器厂商通常没有太多安全概念，安全机制较差。
- 另一方面传统路由器因为功能局限，因此即使被攻破了能做的事情也有限。
  - DNS设置
  - 端口转发

智能路由器的安全挑战

- 厂商的安全意识相对好一点，但实施时候也有可能出问题
- 功能更加复杂，因此出现漏洞的概率提高
- 系统功能多，被攻破了能利用的事情也多

HiWiFi 在路由自身安全方面的考虑

- 增强登录安全机制
  - 目前是luci内建机制，可以防CSRF。将来计划加入其他安全手段，例如验证码
- 逐步实现最小权限
  - 内部进程尽量使用普通账号来运行
  - 实现sandbox用来跑第三方应用
- 增强云平台安全

家庭局域网安全问题

- 路由器自身安全其实只是家庭局域网安全问题的一小部分
  - WiFi 安全问题
  - 物联设备安全问题
- 即使路由器和连接本身没有问题，家庭局域网内任意设备被攻破，都会对家庭局域网安全造成极大隐患。

WiFi安全问题

- WiFi相关协议本身缺陷
  - WEP，WPS
- 弱密码
  - WPA2 离线攻击
- WiFi密码共享软件是很大的安全风险

物联设备安全问题

- 厂商安全意识极为薄弱
- 设备运算能力不足

HiWiFi对家庭局域网安全考量

- 安全和便利经常无法兼顾，只能尽量做到折中
- 计划和安全厂商合作，引入简单 IDS 机制。
- 在能做到的范围内尽量做一些事情。
  - 禁用WPS
  - 加入本地WPA2 enterprise认证方式
  - 对物联设备启用WiFi隔离方式
  - 支持访客模式，不要给共享密码软件以机会

和安全社区关系

- 和安全社区的保持联系，进行互动
- 定期“体检”