ISC 2019 第七届互联网安全大会

IoT设备脆弱性挖掘技术现状与趋势

喻波

软件安全智能并行分析湖南省重点实验室 研究员

小鹅助理

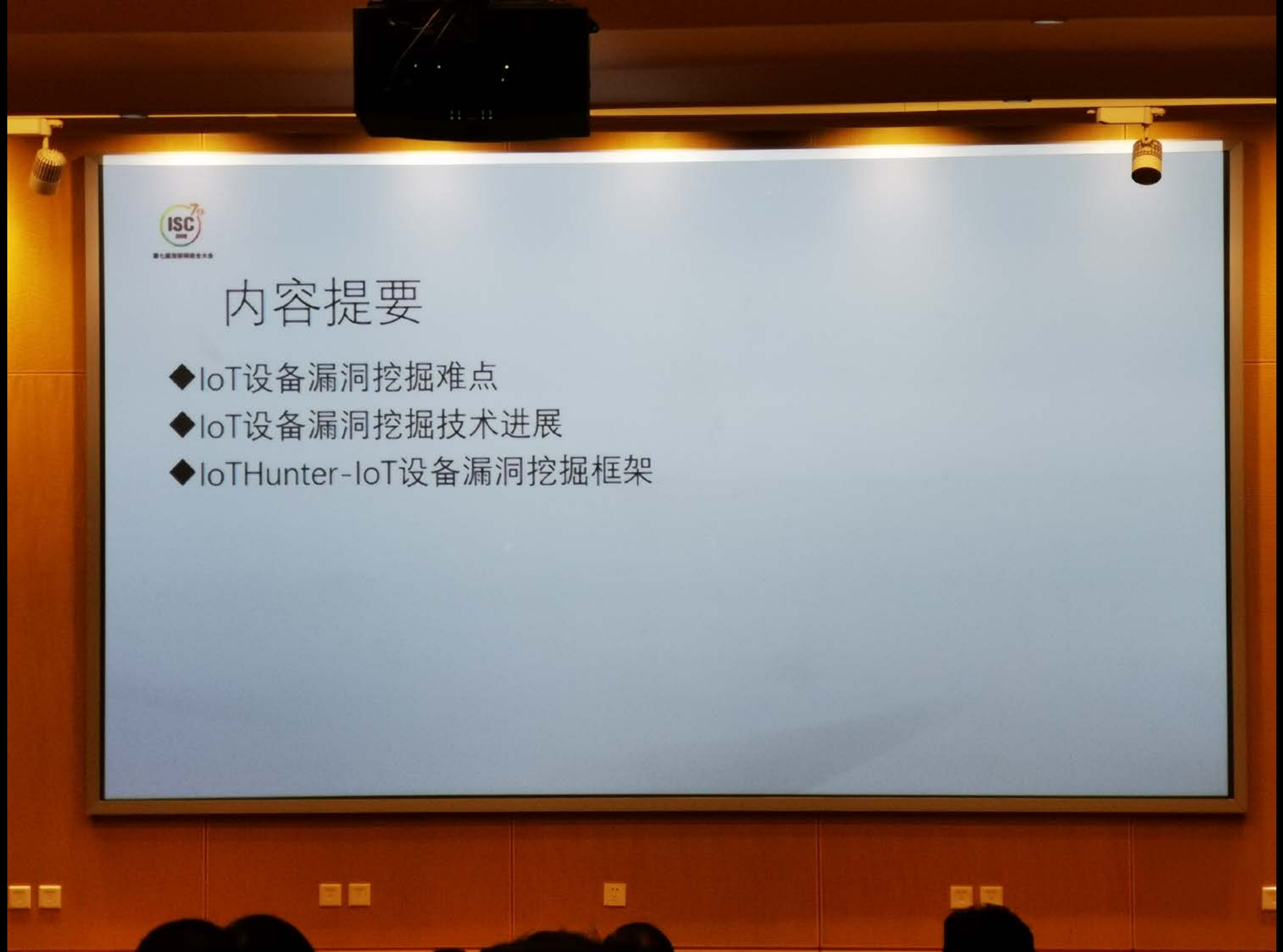
扫码添加小鹅助理，与数万科技圈人士

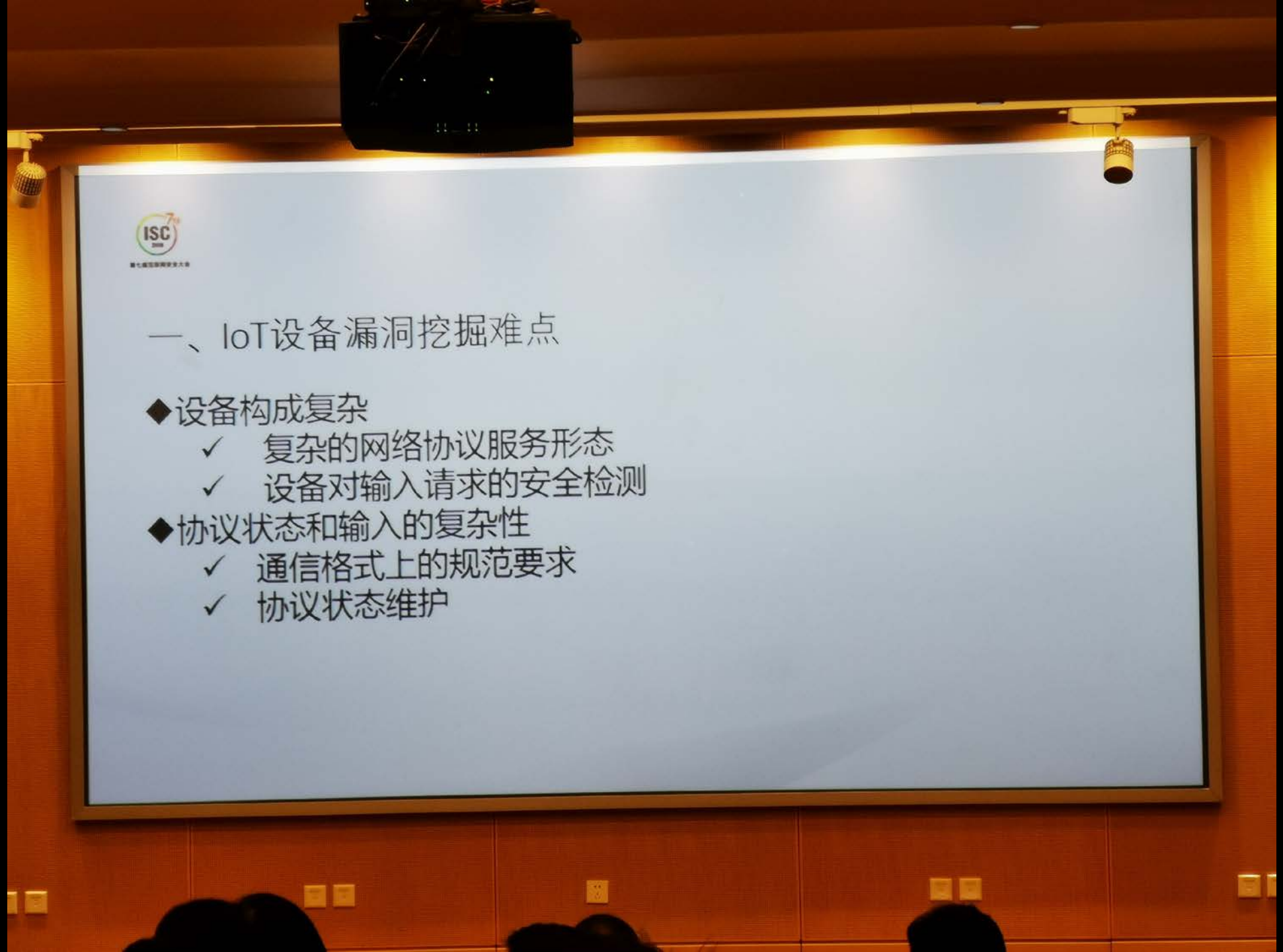
分享重量级活动PPT、干货培训课程、高端会议免费

门票


ISC
2020
360互联网安全中心
喻波
软件安全智能并行分析湖南省重点实验室
研究员

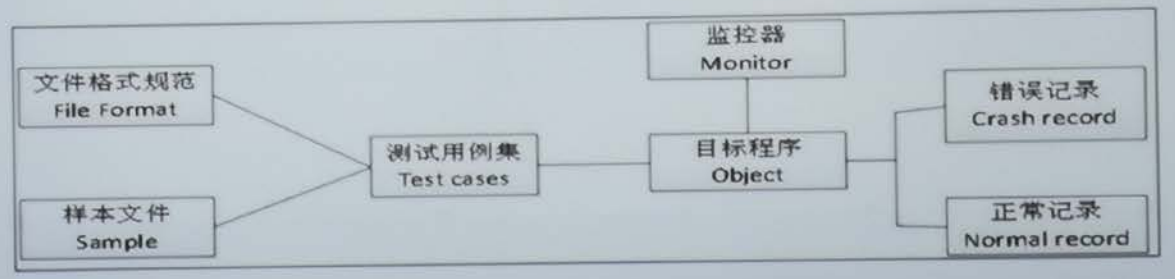

ISC
IoT设备漏洞挖掘技术进展
喻波
HunterGroup@软件安全智能并行分析湖南省重点实验室
290149807@qq.com


ISC
内容提要
◆IoT设备漏洞挖掘难点
◆IoT设备漏洞挖掘技术进展
◆IoTHunter-IoT设备漏洞挖掘框架


一、IoT设备漏洞挖掘难点
◆设备构成复杂
✓ 复杂的网络协议服务形态
✓ 设备对输入请求的安全检测
◆协议状态和输入的复杂性
✓ 通信格式上的规范要求
✓ 协议状态维护

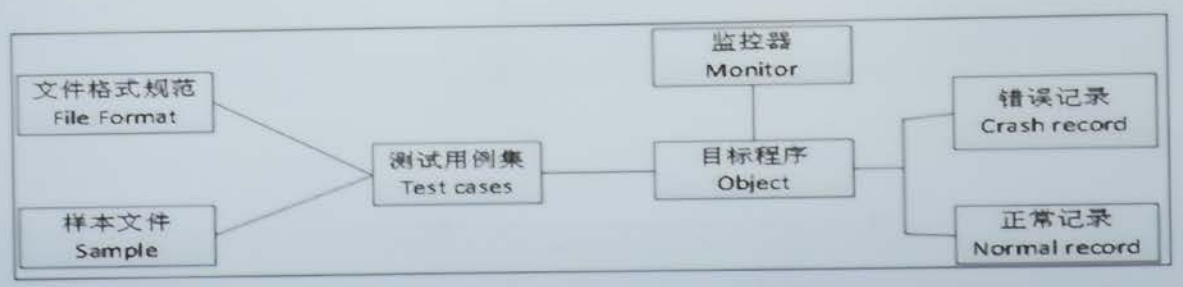
IoT设备漏洞挖掘难点

文件Fuzz



IoT设备漏洞挖掘难点

文件Fuzz



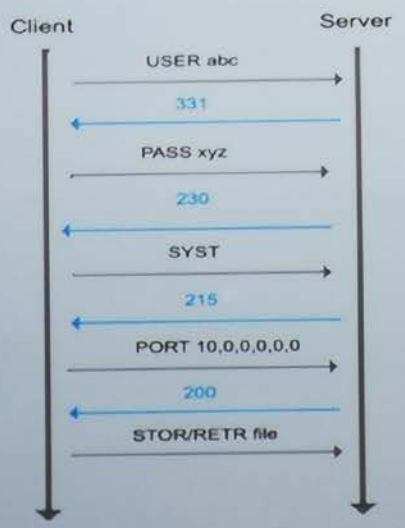
VS

设备协议Fuzz

不同	文件Fuzz	协议Fuzz
格式	少量未知格式	大量未知协议或私有协议
监视	在一个进程空间感知	可能在多个进程空间感知，比如ASA防火墙的snmp协议，Get、Set、Trap报文分别由不同进程负责处理
异常	多为Crash	Crash以外，还有信息泄露、认证绕过等高危漏洞

IoT设备漏洞挖掘难点

IoT设备协议漏洞挖掘的困难-面临通信请求方面的安全检测



- 协议会话对状态序列有要求
- 协议会话要避开IoT设备的安全机制，避开DOS检测、重放攻击检测

IoT设备漏洞挖掘难点

IoT设备协议漏洞挖掘的困难-协议状态的复杂性

- 以SSL握手协议为例

IoT设备漏洞挖掘难点

IoT设备协议漏洞挖掘的困难-通信格式上的强规范要求

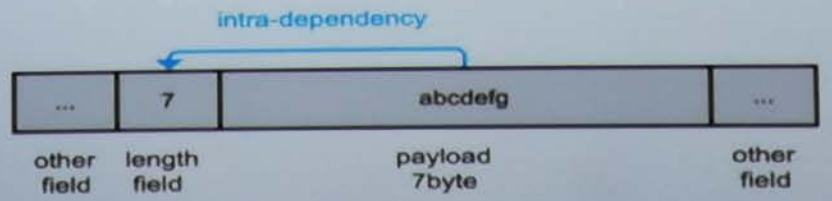
- 以SSL ClientHello消息为例

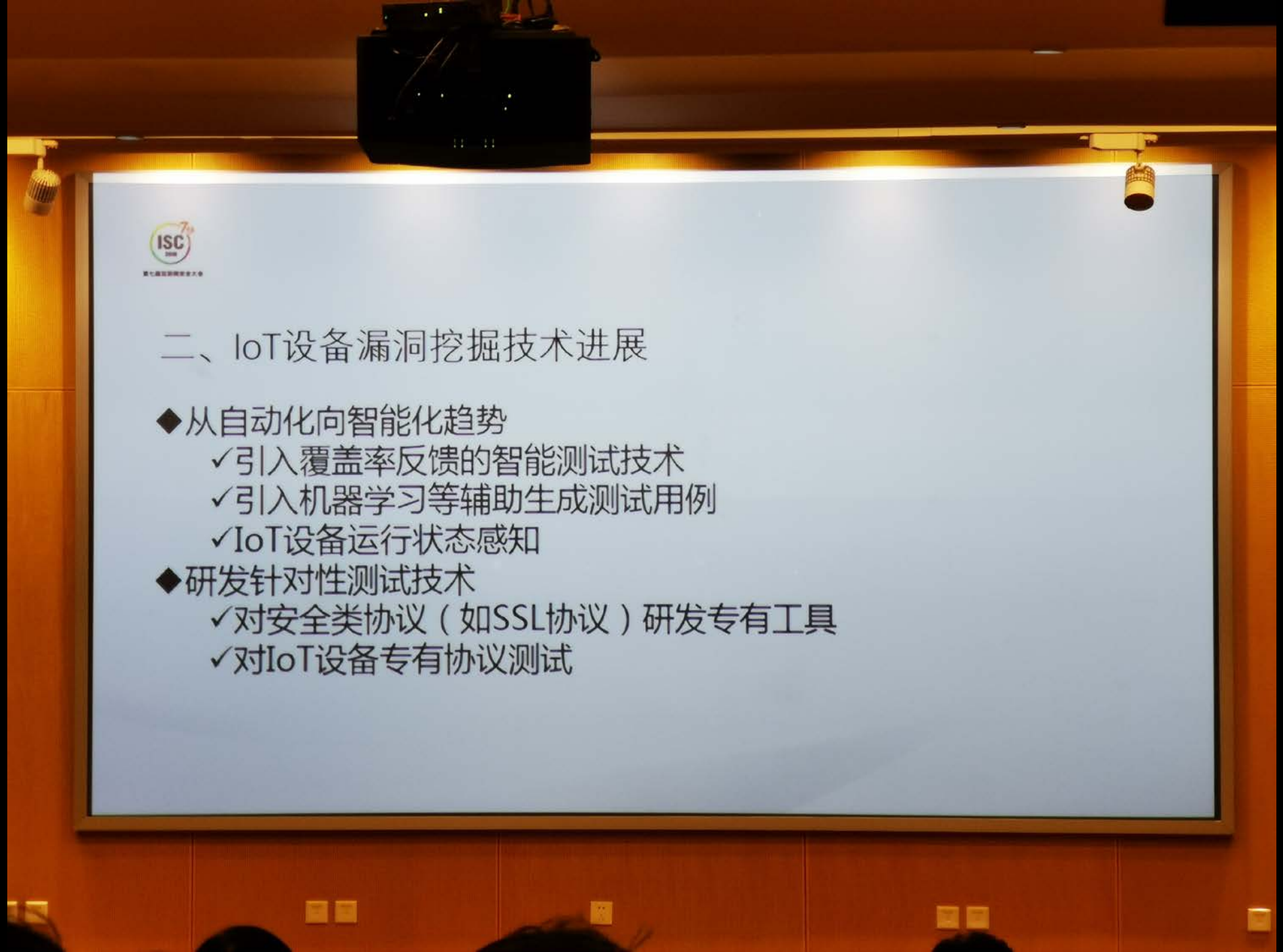
```
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 62
    ▼ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 58
        Version: TLS 1.2 (0x0303)
      ▸ Random: 4f70656e53534c20312e302e3220436c69656e7448656c6c...
        Session ID Length: 0
        Cipher Suites Length: 4
      ▸ Cipher Suites (2 suites)
        Compression Methods Length: 1
      ▸ Compression Methods (1 method)
        Extensions Length: 13
      ▸ Extension: signature_algorithms (len=4)
      ▸ Extension: renegotiation_info (len=1)
```

IoT设备漏洞挖掘难点

IoT设备协议漏洞挖掘的困难-维护协议字段间的关联性

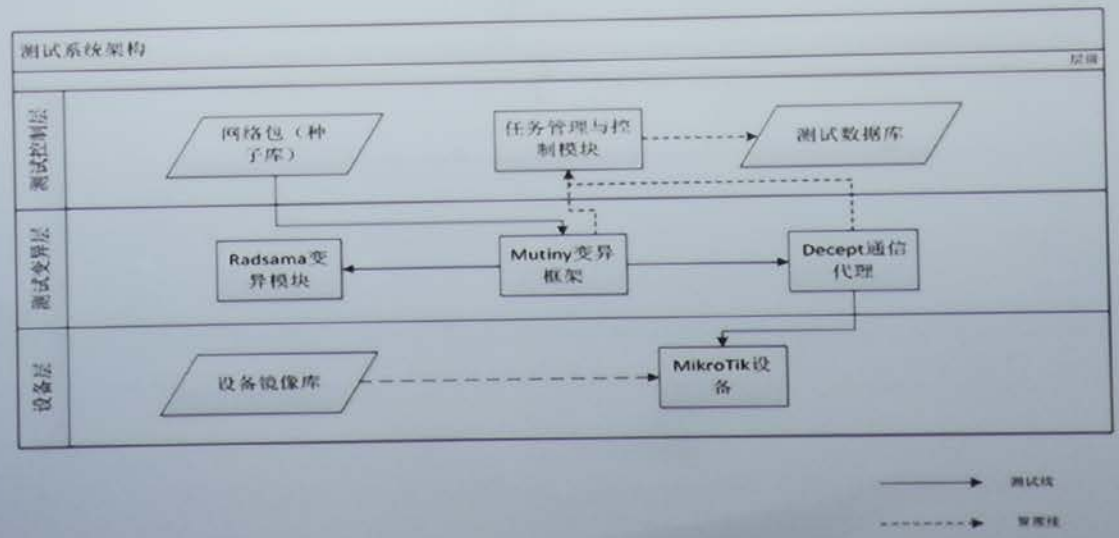
- 消息内数据字段依赖
- 消息间数据字段依赖
- 环境要素依赖




二、IoT设备漏洞挖掘技术进展
◆从自动化向智能化趋势
✓引入覆盖率反馈的智能测试技术
✓引入机器学习等辅助生成测试用例
✓IoT设备运行状态感知
◆研发针对性测试技术
✓对安全类协议（如SSL协议）研发专有工具
✓对IoT设备专有协议测试

IoT设备漏洞挖掘技术框架

设备协议的漏洞挖掘- 例如MikroTik路由器漏洞挖掘



IoT设备漏洞挖掘技术框架

设备协议的漏洞挖掘- 例如MikroTik路由器漏洞挖掘

- 框架组成
  - ✓ 采用Cisco Talos团队的Mutiny测试工具
  - ✓ 采用合法网络流量作为样本
  - ✓ 采用Radamsa作为突变模糊器，变异样本

IoT设备漏洞挖掘技术框架

设备协议的漏洞挖掘- 例如MikroTik路由器漏洞挖掘

- 框架组成
  - ✓ 采用Cisco Talos团队的Mutiny测试工具
  - ✓ 采用合法网络流量作为样本
  - ✓ 采用Radamsa作为突变模糊器，变异样本
- 发现SMB中未经验证的RCE(CVE-2018-7445)

```
▸ Frame 2486: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0
▸ Ethernet II, Src: IntelCor_fb:e0:aa (84:ef:18:fb:e0:aa), Dst: PcsCompu_6d:16:84 (08:00:27:6d:16:84)
▸ Internet Protocol Version 4, Src: 192.168.0.176, Dst: 192.168.0.66
▸ Transmission Control Protocol, Src Port: 56102, Dst Port: 445, Seq: 1, Ack: 1, Len: 108
▾ NetBIOS Session Service
    Message Type: Session request (0x81)
  ▾ Flags: 0x00
      .... ...0 = Extend: Add 0 to length
    Length: 32
    Called name: Illegal NetBIOS name (1st character not between A and Z in first-level encoding)
    Calling name: Illegal NetBIOS name (1st character not between A and Z in first-level encoding)
▾ NetBIOS Session Service
    Message Type: Unknown (0x20)
  ▾ Flags: 0x00
      .... ...0 = Extend: Add 0 to length
    Length: 32
▾ NetBIOS Session Service
    Message Type: Session message (0x00)
  ▾ Flags: 0x00
      .... ...0 = Extend: Add 0 to length
    Length: 0
```

IoT设备漏洞挖掘技术框架

IoT固件模糊测试系统：FIRM-AFL（2019），引入AFL进行智能测试

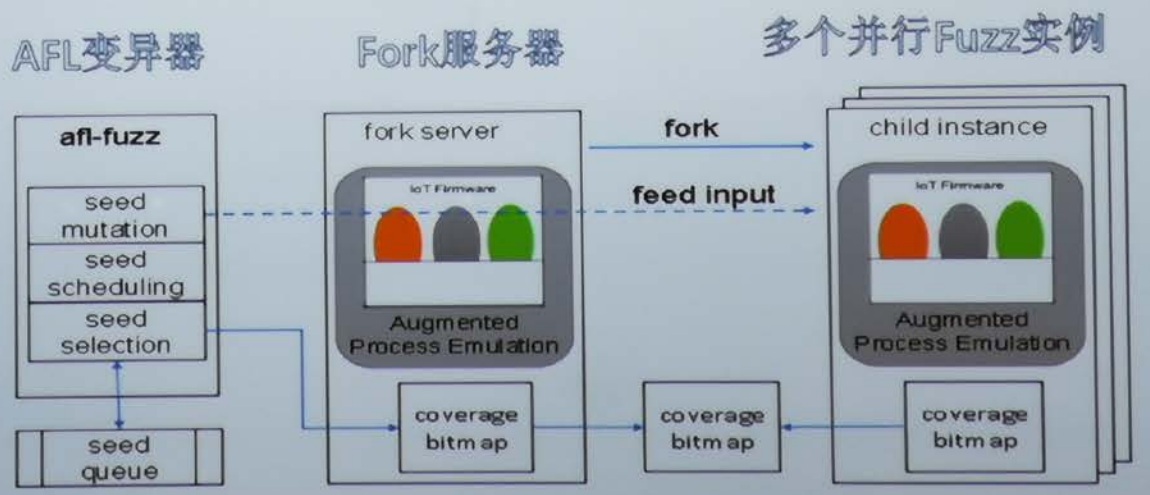
- FIRM-AFL：高吞吐量IoT固件灰盒Fuzz*

*Yaowen Zheng and Ali Davanian and Heng Yin and Chengyu Song and Hongsong Zhu and Limin Sun, FIRM-AFL: High-Throughput Greybox Fuzzing of IoT Firmware via Augmented Process Emulation 28th [USENIX] Security Symposium

IoT设备漏洞挖掘技术框架

- FIRM-AFL：高吞吐量IoT固件灰盒Fuzz

IoT固件模糊测试系统：FIRM-AFL（2019），引入AFL进行智能测试

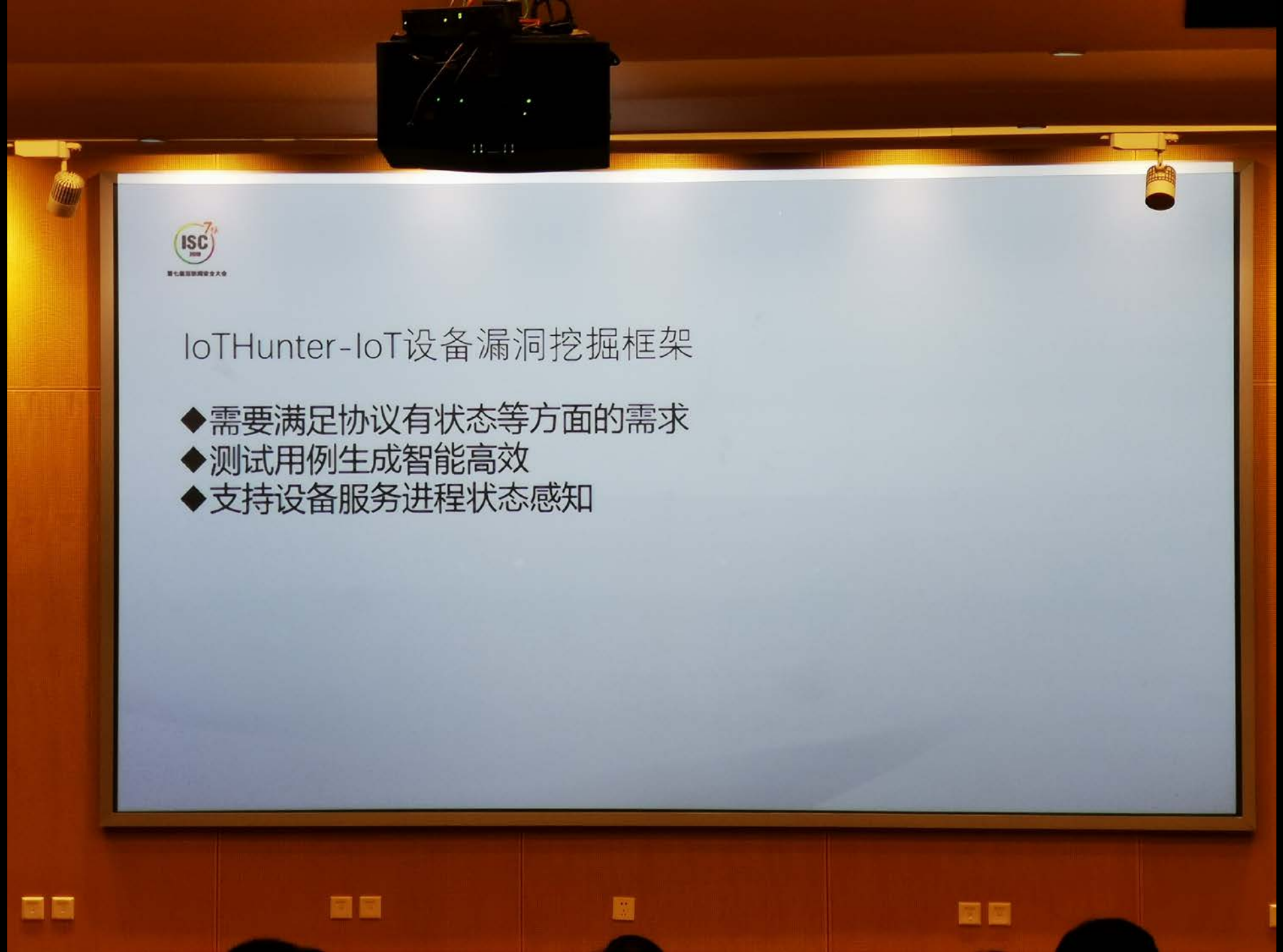


IoT设备漏洞挖掘技术框架

- FIRM-AFL：高吞吐量IoT固件灰盒Fuzz

IoT固件模糊测试系统：FIRM-AFL（2019）

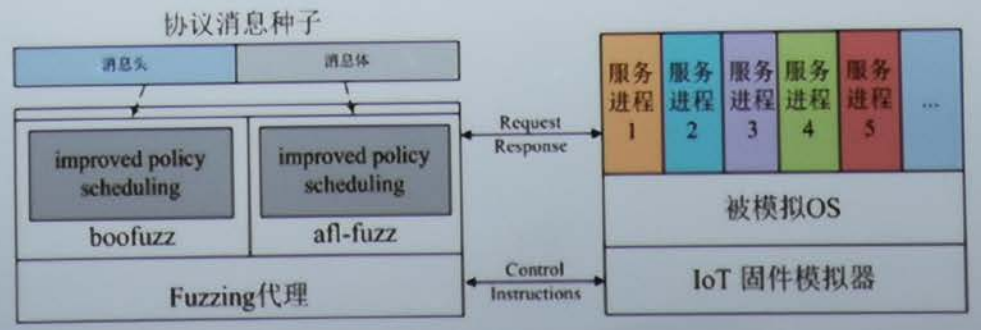
Exploit ID	Vendor	Model	Version	Device	Program	Full-System Time to crash	FIRM-AFL Time to crash
CVE-2018-19242	Trendnet	TEW-632BRP	1.010B32	Router	httpd	21h43min	6h2min
CVE-2013-0230	Trendnet	TEW-632BRP	1.010B32	Router	miniupnpd	>24h	9h16min
CVE-2018-19241	Trendnet	TV-IP110WN	V.1.2.2	Camera	video.cgi	19h13min	4h55min
CVE-2018-19240	Trendnet	TV-IP110WN	V.1.2.2	Camera	network.cgi	12h0min	2h21min
CVE-2017-3193	DLink	DIR-850L	1.03	Router	hnap	21h3min	2h54min
CVE-2017-13772	TPLink	WR940N	V4	Router	httpd	>24h	>24h
EDB-ID-24926	DLink	DIR-815	1.01	Router	hedwig.cgi	16h38min	1h22min
EDB-ID-38720	DLink	DIR-817LW	1.00B05	Router	hnap	4h26min	1h29min
EDB-ID-38718	DLink	DIR-825	2.02	Router	httpd	>24h	22h3min
CVE-2016-1558	DLink	DAP-2695	1.11.RC044	Router	httpd	16h24min	2h32min
CVE-2018-10749	DLink	DSL-3782	1.01	Router	tcapi	247s	20s
CVE-2018-10748	DLink	DSL-3782	1.01	Router	tcapi	252s	22s
CVE-2018-10747	DLink	DSL-3782	1.01	Router	tcapi	249s	20s
CVE-2018-10745	DLink	DSL-3782	1.01	Router	tcapi	236s	25s
CVE-2018-8941	DLink	DSL-3782	1.01	Router	tcapi	281s	24s


ISC
IoTHunter-IoT设备漏洞挖掘框架
◆需要满足协议有状态等方面的需求
◆测试用例生成智能高效
◆支持设备服务进程状态感知

IoTHunter-IoT设备漏洞挖掘框架

针对网络协议模糊测试采用层次化调度框架

- 需求1：设备模拟与状态感知
  - ✓ 固件OS模拟执行与服务进程状态感知
  - ✓ 头部变异和消息体变异分离



IoTHunter-IoT设备漏洞挖掘框架

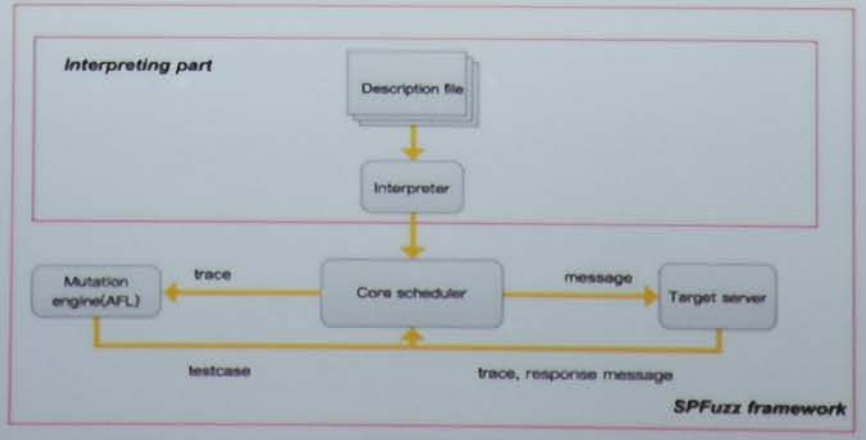
针对网络协议模糊测试采用层次化调度框架

- 需求2：保持变异报文的有效性
  - ✓ 协议会话序列可描述
  - ✓ 协议字段依赖可描述

IoTHunter-IoT设备漏洞挖掘框架

针对网络协议模糊测试采用层次化调度框架

- 需求2：保持变异报文的有效性
  - ✓ 协议会话序列可描述
  - ✓ 协议字段依赖可描述



IoTHunter-IoT设备漏洞挖掘框架

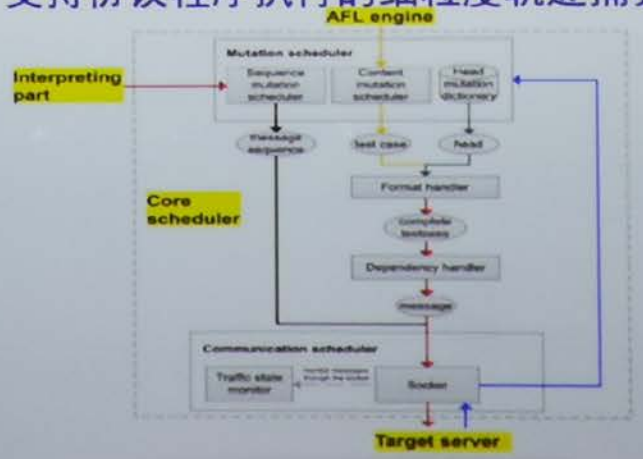
针对网络协议模糊测试采用层次化调度框架

- 需求3：支持灰盒Fuzz
  - 利用文件Fuzz的经验
  - 支持协议程序执行的细粒度轨迹捕获

IoTHunter-IoT设备漏洞挖掘框架

针对网络协议模糊测试采用层次化调度框架

- 需求3：支持灰盒Fuzz
  - 利用文件Fuzz的经验
  - 支持协议程序执行的细粒度轨迹捕获



IoTHunter-IoT设备漏洞挖掘框架

针对网络协议模糊测试采用层次化调度框架

- 实际测试结果
  - 覆盖率提高50%
  - 支持OpenSSL等有状态协议Fuzz

IoTHunter-IoT设备漏洞挖掘框架

针对网络协议模糊测试采用层次化调度框架

- 实际测试结果
  - 覆盖率提高50%
  - 支持OpenSSL等有状态协议Fuzz

		Proftpd	Oftpd	OpenSSL
Boofuzz	Function coverage	26.56%	28.23%	8.52%
	Basic block coverage	14.86%	26.55%	8.80%
	Edge coverage	7.13%	10.58%	2.05%
SPFuzz/C	Function coverage	29.46%	33.67%	14.13%
	Basic block coverage	17.03%	34.74%	10.67%
	Edge coverage	8.16%	13.73%	2.11%
SPFuzz/F	Function coverage	35.48%	58.50%	17.60%
	Basic block coverage	20.32%	54.20%	14.40%
	Edge coverage	9.00%	15.86%	2.38%

IoTHunter-IoT设备漏洞挖掘框架

- 第一款能支持复杂网络会话协议的灰盒Fuzz系统
- 能支持32位和64位 IoT系统

针对网络协议模糊测试采用层次化调度框架

IoTHunter-IoT设备漏洞挖掘框架

- 第一款能支持复杂网络会话协议的灰盒Fuzz系统
- 能支持32位和64位 IoT系统

针对网络协议模糊测试采用层次化调度框架

*) sms - allow specifying multiple "allowed-number" values;
*) sms - fixed long message parsing (introduced in v6.45beta19);
*) sms - improved delivery report logging;
*) snmp - added "dot1dStpPortTable" OID;
*) snmp - added OID for neighbor "interface";
*) snmp - added "write-access" column to community print;
*) snmp - allow setting interface "adminStatus";
*) snmp - improved reliability on SNMP service packet validation;
*) snmp - properly return multicast and broadcast packet counters for IF-MIB OIDs;
*) ssh - accept remote forwarding requests with empty hostnames;
*) ssh - added new "ssh-exec" command for non-interactive command execution;
*) ssh - fixed non-interactive multiple command execution;

小鹅助理

谢谢！

扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费门票