IP地址匿名化进展

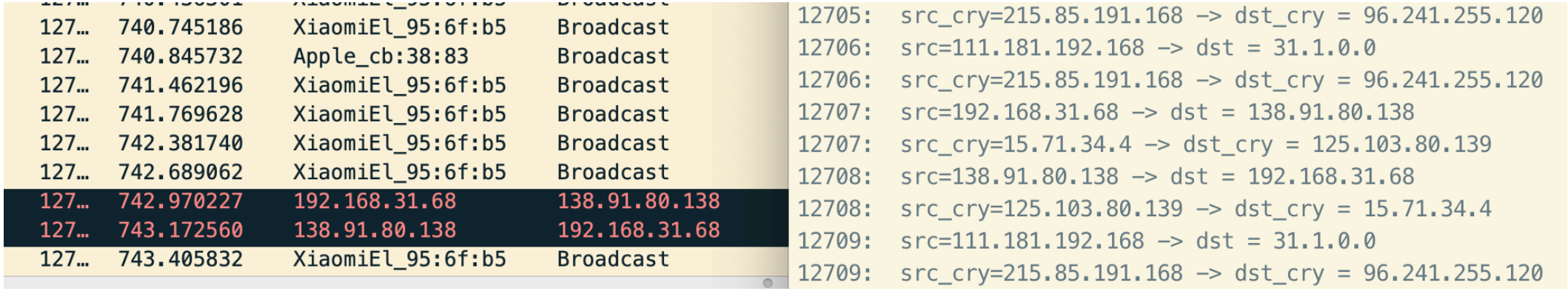
李映辉

目前进展

- 完成Pcap文件的Ipv4地址解析（其他包头信息）
- 基本完成Ipv4地址匿名化（Crypto-PAn.1.0一些问题）
- 完成Pcap文件的Ipv6地址解析（其他包头信息）

验证分析

- Ipv4地址解析正确性验证



127…	740.745186	XiaomiEl_95:6f:b5	Broadcast
127…	740.845732	Apple_cb:38:83	Broadcast
127…	741.462196	XiaomiEl_95:6f:b5	Broadcast
127…	741.769628	XiaomiEl_95:6f:b5	Broadcast
127…	742.381740	XiaomiEl_95:6f:b5	Broadcast
127…	742.689062	XiaomiEl_95:6f:b5	Broadcast
127…	742.970227	192.168.31.68	138.91.80.138
127…	743.172560	138.91.80.138	192.168.31.68
127…	743.405832	XiaomiEl_95:6f:b5	Broadcast

```
12705:  src_cry=215.85.191.168 -> dst_cry = 96.241.255.120
12706:  src=111.181.192.168 -> dst = 31.1.0.0
12706:  src_cry=215.85.191.168 -> dst_cry = 96.241.255.120
12707:  src=192.168.31.68 -> dst = 138.91.80.138
12707:  src_cry=15.71.34.4 -> dst_cry = 125.103.80.139
12708:  src=138.91.80.138 -> dst = 192.168.31.68
12708:  src_cry=125.103.80.139 -> dst_cry = 15.71.34.4
12709:  src=111.181.192.168 -> dst = 31.1.0.0
12709:  src_cry=215.85.191.168 -> dst_cry = 96.241.255.120
```

验证分析

- Ipv4地址匿名化唯一性验证
- 当匿名化算法确定，key值确定时
- 相同的IP地址匿名结果一致

```
12701:  src=111.181.192.168 -> dst = 31.1.0.0
12701:  src_cry=215.85.191.168 -> dst_cry = 96.241.255.120
12702:  src=56.131.192.168 -> dst = 31.218.0.0
12702:  src_cry=223.114.191.168 -> dst_cry = 224.99.255.120
12703:  src=111.181.192.168 -> dst = 31.1.0.0
12703:  src_cry=215.85.191.168 -> dst_cry = 96.241.255.120
12704:  src=111.181.192.168 -> dst = 31.1.0.0
12704:  src_cry=215.85.191.168 -> dst_cry = 96.241.255.120
```

验证分析

- Ipv4地址匿名化性能分析（12709 * 2 / 0.14 = 181,557）
- 大约每秒20w个Ipv4地址左右

```
[root@bgp Crypto-PAn.1.0]# ./sample
open pcap file success
open output file success

read end of pcap file
Use Time :0.140000 s
```

一些问题

- Crypto-PAn.1.0 并不支持Ipv6的匿名化
- Crypto-PAn.1.0 并没有提供反匿名化的接口
- Ipv6地址中包含很多全0段，全0段的匿名化处理仍需调研

cryptopANT-1.2.0

- 与Crypto-PAn.1.0为统一团队开发
- 使用crypto-PAn算法进行前缀IP地址匿名化的C库
- 支持Ipv4、Ipv6、MAC地址的匿名化和反匿名化（有key）
- 最新2019-01-22（Crypto-PAn.1.0已停止维护）

两种工具的比较

		CryptopANT	Crypto-PAn
	Language	C	C++
	Library requirements (1)	SSL	none
	IPv4 class awareness (2)	**yes**	no
√	Optional partial anonymization (3)	**yes**	no
	IPv4 encrypt	yes	yes
√	IPv6 and MAC encrypt	**yes**	no
√	decryption (4)	**yes**	no
√	Key generation (5)	automated or user-provided	user-provided
	Crypto function (6)	Blowfish/AES/SHA1SUM/MD5SUM	AES
	Caching (7)	**yes**	no

未来目标

- 将已有的工作扩展到cryptopANT-1.2.0上去
- 对比Ipv4和Ipv6的性能、效果等方面
- 调研并解决Ipv6全0段匿名的问题
- 总结Ipv4、Ipv6匿名化工作中的经验教训

THANKS