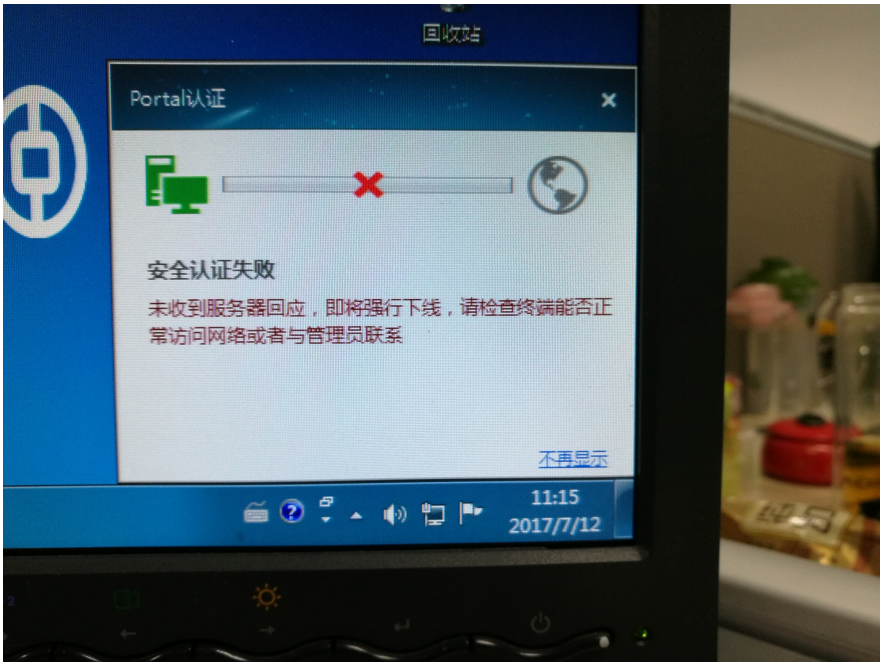
某局点反馈勾选检查Windows补丁后部分终端出现安全认证失败的问题分析

张鑫 2017-09-08 发表

某局点使用iNode配合EIA EAD做认证以及安全检查，近期由于总部要求需要统一检查Windows补丁，但是该局点网管运维人员发现，勾选检查Windows补丁后，部分终端会出现安全认证失败的提示，一旦去勾选Windows补丁检查，用户即可通过安全认证。

服务器侧勾选了Windows补丁检查后，iNode客户端身份认证成功后会出现“安全认证失败，未收到策略服务器回应。即将强行下线”的认证异常提醒。



此时收集iNode客户端的详细日志、iNode客户端侧抓包、策略服务器debug级别日志和策略服务器侧的抓包信息进行分析。

首先，通过查看iNode日志和策略服务器的日志发现，iNode在身份认证成功后。按照正常流程发起了EAD 1号报文，同时策略服务器正常回应了EAD 2号报文。

```
[2017-07-12 11:14:20] [DtlCmn] [1394] SecPkt secPushInner: out-pkt [1]
<data>
   <i n="userName">8264137@OMR</i>
   <i n="hwAddr">00:25:11:E9:55:B9</i>
   <i n="eventSeqID">n1MqMbBr</i>
</data>
[2017-07-12 11:14:20] [DtlCmn] [1394] SecPkt secPushInner: the state send before is  3
[2017-07-12 11:14:20] [Dbg] [1b50] SecPkt secRcvThrd: [21.208.64.40 : 9019] sent me 569 bytes.
[2017-07-12 11:14:20] [Dbg] [1b50] SecPkt secDataProc: The head id is ad878
[2017-07-12 11:14:20] [Dbg] [1b50] SecPkt secDataProc: The type is 2
[2017-07-12 11:14:20] [Dbg] [1b50] SecPkt secDataProc: The id is 21429
[2017-07-12 11:14:20] [DtlCmn] [1b50] SecPkt sndSecMsg: transfer [2] [21429]
<data>
   <i n="strategyMode">autoAdapt</i>
   <i n="userMessage"/>
   <i n="antiIPchange">false</i>
   <i n="antiAgent">false</i>
   <i n="antiProxy">false</i>
   <i n="antiDualNetcard">false</i>
   <i n="ipSetMode">unlimit</i>
   <i n="macCheck">false</i>
   <i n="sameMacCheck">false</i>
   <i n="antiMultiOS">false</i>
   <i n="antiMultiip">false</i>
   <i n="antiVMWareNATservice">false</i>
   <i n="antiVMWareUSBservice">false</i>
   <i n="iSupVMCheck">false</i>
   <i n="iSetWanControl">false</i>
```

true
false
false
365969448
9029
720
3
2
PluginForbidden
McAfee
McAfee;McAfee VirusScan Enterprise
Upcast
Virus-Engine-Version;Virus-Def-Version;Windows
false
false
afterCheck
Critical,monitor;Important,remind;Moderate,monitor;Low,monitor
false
false
n1MqMbBr
iMCV700R003B04D016SP01
</data>
可以看到EAD报文交互过程中，iNode客户端收到了策略服务器发送的EAD 2号报文，并要求检查Wind
ows补丁的方式为传统方式。
接下来iNode客户端上送检查结果报文，即EAD 3号报文
[2017-07-12 11:14:43] [DtlCmn] [9b8] SecPkt secPushInner: out-pkt [3]
<data>
8264137@OMR
00:25:11:E9:55:B9

n1MqMbBr
true
Windows|7 Enterprise Service Pack
1|0x0804|KB4012215;KB982018;KB976902;KB4012212;KB3112343;KB3046049;KB3039066;KB30351
32;KB3035131;KB3035126;KB3035017;KB3034344;KB3033929;KB3033889;KB3032323;KB3030377;K
B3022777;KB3021674;KB3019978;KB3019215;KB3011780;KB3010788;KB3006226;KB3004375;KB30
04361;KB3003743;KB3000483;KB2993958;KB2993651;KB2992611;KB2991963;KB2984972;KB297957
0;KB2978742;KB2978668;KB2978120;KB2977292;KB2976897;KB2973351;KB2973201;KB2973112;KB
2972280;KB2972211;KB2972100;KB2971850;KB2968294;KB2961072;KB2957509;KB2957503;KB2957
189;KB2943357;KB2939576;KB2937610;KB2936068;KB2931356;KB2930275;KB2929961;KB2929733;
KB2928562;KB2922229;KB2919469;KB2918614;KB2918077;KB2916036;KB2913431;KB2911501;KB2
909210;KB2908783;KB2904266;KB2901112;KB2900986;KB2898857;KB2894844;KB2893519;KB28932
94;KB2892074;KB2891804;KB2888049;KB2887069;KB2884256;KB2882822;KB2876331;KB2876284;K
B2872339;KB2871997;KB2868725;KB2868626;KB2868623;KB2868116;KB2868038;KB2864202;KB28
64058;KB2863240;KB2862973;KB2862966;KB2862335;KB2862330;KB2862152;KB2861855;KB286169
8;KB2861191;KB2859537;KB2855844;KB2853952;KB2852386;KB2849470;KB2847927;KB2847311;KB
2847077;KB2846960;KB2844286;KB2843630;KB2840631;KB2840149;KB2839894;KB2835364;KB2834
886;KB2834140;KB2832414;KB2820331;KB2813430;KB2813347;KB2808679;KB2807986;KB2803821;
KB2800095;KB2799926;KB2798162;KB2789645;KB2786400;KB2786081;KB2785220;KB2773072;KB2
770660;KB2763523;KB2761217;KB2758857;KB2757638;KB2756921;KB2750841;KB2743555;KB27425
99;KB2736422;KB2732500;KB2732487;KB2732059;KB2729452;KB2729094;KB2727528;KB2726535;K
B2719857;KB2718704;KB2712808;KB2709630;KB2705219;KB2699779;KB2698365;KB2691442;KB26
90533;KB2685939;KB2685811;KB2676562;KB2667402;KB2660075;KB2656356;KB2655992;KB265442
8;KB2653956;KB2647753;KB2644615;KB2640148;KB2631813;KB2621440;KB2620712;KB2620704;KB
2619339;KB2604115;KB2585542;KB2584146;KB2579686;KB2570947;KB2564958;KB2563227;KB2560
656;KB2552343;KB2547666;KB2545698;KB2544893;KB2536276;KB2536275;KB2534111;KB2533552;
KB2532531;KB2515325;KB2511455;KB2510531;KB2509553;KB2506928;KB2506212;KB2503665;KB2
491683;KB2479943;KB2670838;KB2841134;KB2841134;KB2849696;KB2849697
Virus-Engine-Version|5800.7501
Virus-Def-Version|2017-07-10
AV-Software|McAfee

</data>
[2017-07-12 11:14:43] [DtlCmn] [9b8] SecPkt secPushInner: the state send before is 11
[2017-07-12 11:14:48] [DtlCmn] [9b8] SecPkt secPushInner: out-pkt [3] <data><i
n="userName">8264137@OMR00:25:11:E9:55:B9</i
>n1MqMbBrtrueWindows|7 Enter
prise Service Pack
1|0x0804|KB4012215;KB982018;KB976902;KB4012212;KB3112343;KB3046049;KB3039066;KB30351
32;KB3035131;KB3035126;KB3035017;KB3034344;KB3033929;KB3033889;KB3032323;KB3030377;K
B3022777;KB3021674;KB3019978;KB3019215;KB3011780;KB3010788;KB3006226;KB3004375;KB30
04361;KB3003743;KB3000483;KB2993958;KB2993651;KB2992611;KB2991963;KB2984972;KB297957
0;KB2978742;KB2978668;KB2978120;KB2977292;KB2976897;KB2973351;KB2973201;KB2973112;KB
2972280;KB2972211;KB2972100;KB2971850;KB2968294;KB2961072;KB2957509;KB2957503;KB2957
189;KB2943357;KB2939576;KB2937610;KB2936068;KB2931356;KB2930275;KB2929961;KB2929733;
KB2928562;KB2922229;KB2919469;KB2918614;KB2918077;KB2916036;KB2913431;KB2911501;KB2
909210;KB2908783;KB2904266;KB2901112;KB2900986;KB2898857;KB2894844;KB2893519;KB28932
94;KB2892074;KB2891804;KB2888049;KB2887069;KB2884256;KB2882822;KB2876331;KB2876284;K
B2872339;KB2871997;KB2868725;KB2868626;KB2868623;KB2868116;KB2868038;KB2864202;KB28
64058;KB2863240;KB2862973;KB2862966;KB2862335;KB2862330;KB2862152;KB2861855;KB286169
8;KB2861191;KB2859537;KB2855844;KB2853952;KB2852386;KB2849470;KB2847927;KB2847311;KB
2847077;KB2846960;KB2844286;KB2843630;KB2840631;KB2840149;KB2839894;KB2835364;KB2834
886;KB2834140;KB2832414;KB2820331;KB2813430;KB2813347;KB2808679;KB2807986;KB2803821;
KB2800095;KB2799926;KB2798162;KB2789645;KB2786400;KB2786081;KB2785220;KB2773072;KB2
770660;KB2763523;KB2761217;KB2758857;KB2757638;KB2756921;KB2750841;KB2743555;KB27425
99;KB2736422;KB2732500;KB2732487;KB2732059;KB2729452;KB2729094;KB2727528;KB2726535;K
B2719857;KB2718704;KB2712808;KB2709630;KB2705219;KB2699779;KB2698365;KB2691442;KB26
90533;KB2685939;KB2685811;KB2676562;KB2667402;KB2660075;KB2656356;KB2655992;KB265442
8;KB2653956;KB2647753;KB2644615;KB2640148;KB2631813;KB2621440;KB2620712;KB2620704;KB
2619339;KB2604115;KB2585542;KB2584146;KB2579686;KB2570947;KB2564958;KB2563227;KB2560
656;KB2552343;KB2547666;KB2545698;KB2544893;KB2536276;KB2536275;KB2534111;KB2533552;
KB2532531;KB2515325;KB2511455;KB2510531;KB2509553;KB2506928;KB2506212;KB2503665;KB2
491683;KB2479943;KB2670838;KB2841134;KB2841134;KB2849696;KB2849697<i n="checkRe
sult">Virus-Engine-Version|5800.7501Virus-Def-Version|2017-07-10<i n=
"checkResult">AV-Software|McAfee<i n="F
WcheckResult"></i
></data>
[2017-07-12 11:14:53] [DtlCmn] [9b8] SecPkt secPushInner: out-pkt [3] <data><i
n="userName">8264137@OMR00:25:11:E9:55:B9</i
>n1MqMbBrtrueWindows|7 Enter
prise Service Pack
1|0x0804|KB4012215;KB982018;KB976902;KB4012212;KB3112343;KB3046049;KB3039066;KB30351
32;KB3035131;KB3035126;KB3035017;KB3034344;KB3033929;KB3033889;KB3032323;KB3030377;K
B3022777;KB3021674;KB3019978;KB3019215;KB3011780;KB3010788;KB3006226;KB3004375;KB30
04361;KB3003743;KB3000483;KB2993958;KB2993651;KB2992611;KB2991963;KB2984972;KB297957
0;KB2978742;KB2978668;KB2978120;KB2977292;KB2976897;KB2973351;KB2973201;KB2973112;KB
2972280;KB2972211;KB2972100;KB2971850;KB2968294;KB2961072;KB2957509;KB2957503;KB2957
189;KB2943357;KB2939576;KB2937610;KB2936068;KB2931356;KB2930275;KB2929961;KB2929733;
KB2928562;KB2922229;KB2919469;KB2918614;KB2918077;KB2916036;KB2913431;KB2911501;KB2
909210;KB2908783;KB2904266;KB2901112;KB2900986;KB2898857;KB2894844;KB2893519;KB28932
94;KB2892074;KB2891804;KB2888049;KB2887069;KB2884256;KB2882822;KB2876331;KB2876284;K
B2872339;KB2871997;KB2868725;KB2868626;KB2868623;KB2868116;KB2868038;KB2864202;KB28
64058;KB2863240;KB2862973;KB2862966;KB2862335;KB2862330;KB2862152;KB2861855;KB286169
8;KB2861191;KB2859537;KB2855844;KB2853952;KB2852386;KB2849470;KB2847927;KB2847311;KB
2847077;KB2846960;KB2844286;KB2843630;KB2840631;KB2840149;KB2839894;KB2835364;KB2834
886;KB2834140;KB2832414;KB2820331;KB2813430;KB2813347;KB2808679;KB2807986;KB2803821;
KB2800095;KB2799926;KB2798162;KB2789645;KB2786400;KB2786081;KB2785220;KB2773072;KB2
770660;KB2763523;KB2761217;KB2758857;KB2757638;KB2756921;KB2750841;KB2743555;KB27425
99;KB2736422;KB2732500;KB2732487;KB2732059;KB2729452;KB2729094;KB2727528;KB2726535;K
B2719857;KB2718704;KB2712808;KB2709630;KB2705219;KB2699779;KB2698365;KB2691442;KB26
90533;KB2685939;KB2685811;KB2676562;KB2667402;KB2660075;KB2656356;KB2655992;KB265442

8;KB2653956;KB2647753;KB2644615;KB2640148;KB2631813;KB2621440;KB2620712;KB2620704;KB2619339;KB2604115;KB2585542;KB2584146;KB2579686;KB2570947;KB2564958;KB2563227;KB2560656;KB2552343;KB2547666;KB2545698;KB2544893;KB2536276;KB2536275;KB2534111;KB2533552;KB2532531;KB2515325;KB2511455;KB2510531;KB2509553;KB2506928;KB2506212;KB2503665;KB2491683;KB2479943;KB2670838;KB2841134;KB2841134;KB2849696;KB2849697Virus-Engine-Version|5800.7501Virus-Def-Version|2017-07-10AV-Software|McAfee</data>

[2017-07-12 11:14:58] [DtlCmn] [9b8] SecPkt secPushInner: out-pkt [3] <data>8264137@OMR00:25:11:E9:55:B9n1MqMbBrtrueWindows|7 Enterprise Service Pack 1|0x0804|KB4012215;KB982018;KB976902;KB4012212;KB3112343;KB3046049;KB3039066;KB3035132;KB3035131;KB3035126;KB3035017;KB3034344;KB3033929;KB3033889;KB3032323;KB3030377;KB3022777;KB3021674;KB3019978;KB3019215;KB3011780;KB3010788;KB3006226;KB3004375;KB3004361;KB3003743;KB3000483;KB2993958;KB2993651;KB2992611;KB2991963;KB2984972;KB2979570;KB2978742;KB2978668;KB2978120;KB2977292;KB2976897;KB2973351;KB2973201;KB2973112;KB2972280;KB2972211;KB2972100;KB2971850;KB2968294;KB2961072;KB2957509;KB2957503;KB2957189;KB2943357;KB2939576;KB2937610;KB2936068;KB2931356;KB2930275;KB2929961;KB2929733;KB2928562;KB2922229;KB2919469;KB2918614;KB2918077;KB2916036;KB2913431;KB2911501;KB2909210;KB2908783;KB2904266;KB2901112;KB2900986;KB2898857;KB2894844;KB2893519;KB2893294;KB2892074;KB2891804;KB2888049;KB2887069;KB2884256;KB2882822;KB2876331;KB2876284;KB2872339;KB2871997;KB2868725;KB2868626;KB2868623;KB2868116;KB2868038;KB2864202;KB2864058;KB2863240;KB2862973;KB2862966;KB2862335;KB2862330;KB2862152;KB2861855;KB2861698;KB2861191;KB2859537;KB2855844;KB2853952;KB2852386;KB2849470;KB2847927;KB2847311;KB2847077;KB2846960;KB2844286;KB2843630;KB2840631;KB2840149;KB2839894;KB2835364;KB2834886;KB2834140;KB2832414;KB2820331;KB2813430;KB2813347;KB2808679;KB2807986;KB2803821;KB2800095;KB2799926;KB2798162;KB2789645;KB2786400;KB2786081;KB2785220;KB2773072;KB2770660;KB2763523;KB2761217;KB2758857;KB2757638;KB2756921;KB2750841;KB2743555;KB2742599;KB2736422;KB2732500;KB2732487;KB2732059;KB2729452;KB2729094;KB2727528;KB2726535;KB2719857;KB2718704;KB2712808;KB2709630;KB2705219;KB2699779;KB2698365;KB2691442;KB2690533;KB2685939;KB2685811;KB2676562;KB2667402;KB2660075;KB2656356;KB2655992;KB2654428;KB2653956;KB2647753;KB2644615;KB2640148;KB2631813;KB2621440;KB2620712;KB2620704;KB2619339;KB2604115;KB2585542;KB2584146;KB2579686;KB2570947;KB2564958;KB2563227;KB2560656;KB2552343;KB2547666;KB2545698;KB2544893;KB2536276;KB2536275;KB2534111;KB2533552;KB2532531;KB2515325;KB2511455;KB2510531;KB2509553;KB2506928;KB2506212;KB2503665;KB2491683;KB2479943;KB2670838;KB2841134;KB2841134;KB2849696;KB2849697Virus-Engine-Version|5800.7501Virus-Def-Version|2017-07-10AV-Software|McAfee</data>

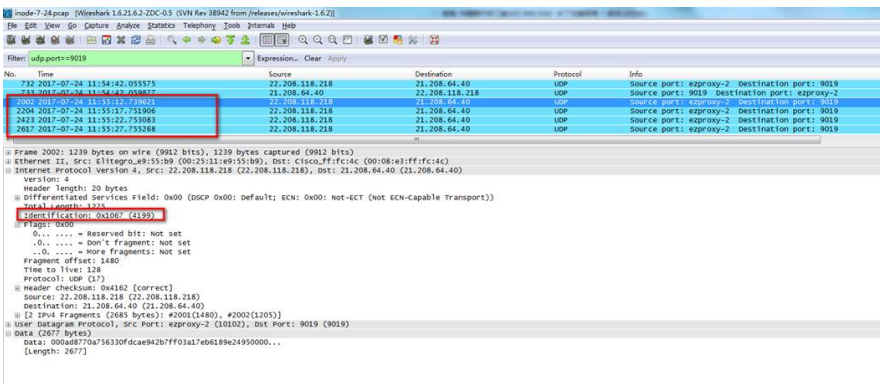
[2017-07-12 11:15:03] [Warn] [13a8] SecPkt pushSecRslt(3) returned 4.

其中包含了操作系统的补丁信息，可以在iNode日志中看到，发送EAD 3号报文时，报文并未收到服务器回应，因此按照5s为间隔重传了报文，多次未收到回应后，iNode报错未收到策略服务器回应，安全认证失败。

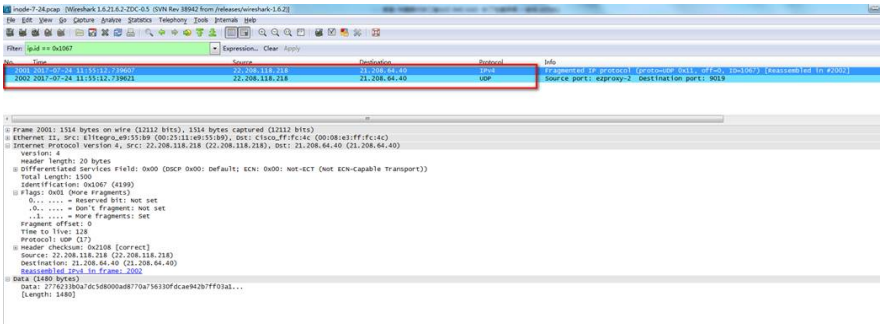
此时查看策略服务器日志，未收到客户端发送的EAD 3号报文，因此需要抓包进行分析。

在客户现场复现问题多次抓包对比安全认证成功和失败的报文情况发现，安全认证成功的客户端发送EAD 3号报文时小于网络环境的MTU 1473，且报文为加密形式。认证异常的终端3号报文发送时报文大小大于1473，且明文传送，即报文在传输过程中进行了分片处理。

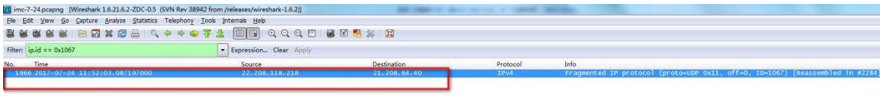
抓包分析安全认证失败时，客户端3号报文的发送过程，首先整体看抓包情况，客户端每5s就会发送一个报文给策略服务器的9029端口。

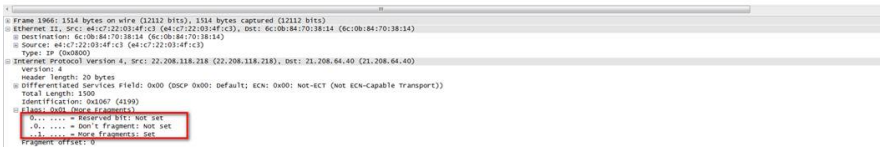


单独以报文的identification过滤会发现，客户端每个报文会分2片发送，



此时查看服务器侧的抓包信息，以报文的identification过滤会发现，策略服务器仅收到了1片报文，





由此可以判断，从客户端到策略服务器的网络设备中，有设备存在将分片报文丢弃的情况。

从客户端到策略服务器经过得所有网络设备接口中，逐个进行端口镜像抓包过滤确认分片报文在哪个设备中被丢弃，最终导致服务器侧无法将分片报文重组。

确认设备侧丢弃报文的原因并解决即可。

现场问题最终定位为设备产品问题，联系设备解决后所有终端均可以正常检查Windows的补丁安装情况。

1.策略服务器1号2号报文交互完成后网络情况是否正常可以通过在认证过程中长ping策略服务器的地址确认网络是否可达；

2.iNode客户端和策略服务器报文交互的加密与否有2个环节可以控制，首先策略服务器侧可以配置是否启用报文的加密压缩，若启用该参数，iNode客户端收到策略服务器的2号报文后，判断客户端上传的3号报文是否满足3000字节大小，若上传的报文大于3000字节，则iNode客户端会将3号报文加密并且压缩传送。若iNode客户端上送3号报文时检测到客户端报文大小不足3000字节，即便服务器下发了加密压缩的属性，客户端发送EAD 3号报文时仍会保持明文不加密发送；由于iNode日志报文的压缩比例较高，现场EAD 3号报文大于3000字节的报文被压缩后小于1500字节，不会网络分片，因此不存在此异常情况；

3.还需排查网络中是否存在防火墙可能会拦截较大的报文的情况