

80 TO 0 IN UNDER 5 SECONDS: FALSIFYING A MEDICAL PATIENT'S VITALS

DOUGLAS MCKEE

WHO AM I?

- DOUGLAS MCKEE
- SENIOR SECURITY RESEARCHER FOR McAfee's ADVANCED THREAT RESEARCH TEAM
- 8+ YEARS EXPERIENCE IN VULNERABILITY RESEARCH, PENETRATION TESTING AND FORENSICS
- @FULMETALPACKETS
- NOT A MEDICAL DOCTOR



OUTLINE

- WHY THESE MEDICAL DEVICES?
- OVERVIEW OF SYSTEMS
- RWHAT?
- REVERSING THE PROTOCOL
- REPLAY ATTACKS
- DEMO
- IMPACT SCENARIOS
- MITIGATIONS



WHY?

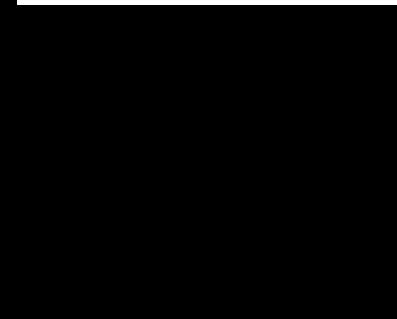
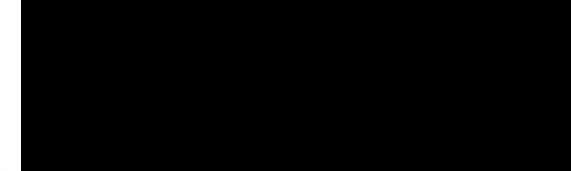
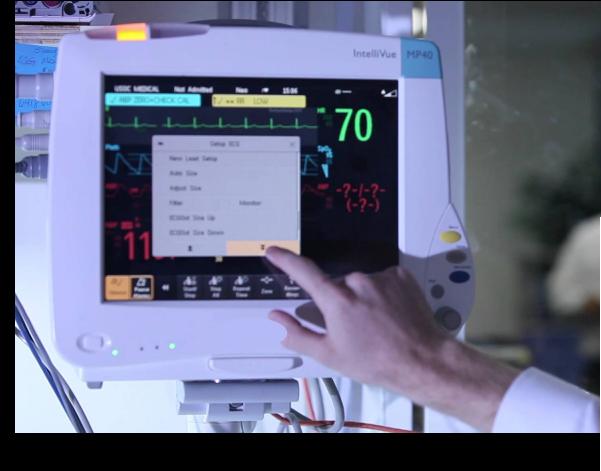
- POTENTIAL IMPACT OF MEDICAL DEVICES
- PATIENT MONITORING WILL ALWAYS BE A NECESSARY
 - “VITAL SIGNS ARE INTEGRAL TO CLINICAL DECISION MAKING” – DR. S. NORDECK
- RELIANCE ON TECHNOLOGY IN MEDICAL FIELD
 - "WE HAVE AN IMPLICIT TRUST IN THESE TYPES OF TECHNOLOGIES," TULLY SAYS. "WE DON'T EVER GET ANY CYBERSECURITY TRAINING IN MEDICAL SCHOOL. IT'S NOT SOMETHING THAT EVER COMES UP IN OUR LITERATURE." DR. JEFF TULLY*



*<https://www.hpe.com/us/en/insights/articles/medical-device-security-hacking-prevention-measures-1806.html>

PATIENT MONITOR (PM)

- BEDSIDE MONITOR
- MONITORS PATIENT'S VITALS – HEARTRATE, BLOOD PRESSURE, O₂ LEVELS, ETC
- HAS WIRED AND WIRELESS (OPTIONAL) NETWORKING
- CONTAINS PERSONAL IDENTIFIABLE INFORMATION (PII)
- *GENERAL PICTURES, NOT TESTED MODEL



CENTRAL MONITORING STATION (CMS)

- RUNS EMBEDDED WINDOWS ON CF CARD
 - WINDOWS XP OR WINDOWS 7
- HAS TWO ETHERNET PORTS FOR TWO NETWORKS
- RUNS MAIN APPLICATION IN LIMITED USER MODE
- A CENTRAL STATION THAT RECEIVES DATA FROM PATIENT MONITORS
- THANKS EBAY!



POTENTIAL ATTACK VECTORS

- OS
- APPLICATION

THINKING...



(PLEASE BE PATIENT)

POTENTIAL ATTACK VECTORS

- OS
- APPLICATION
- FIRMWARE/HARDWARE
- NETWORK
 - MODIFY PATIENT INFORMATION?

THINKING...



(PLEASE BE PATIENT)

RWHAT?

RWHAT packets

All monitoring devices on the [REDACTED] Network periodically broadcast information about themselves in “RWHAT” packets. Among other things, RWHAT packets contain IP address, port number, name, and offered services information about each device.

All monitoring devices listen for RWHAT packets, and maintain a database of information about other devices on the network. When devices need to communicate, the appropriate IP address information is obtained from the database, [REDACTED]. Network-protocol messages are created, and operating system services are used to transmit the message on the network.

For example, when a [REDACTED] computer communicates with a telemetry device, the telemetry device’s IP address is retrieved from the [REDACTED] computer RWHAT database, the [REDACTED] Network messages are created, and the [REDACTED] Windows operating system sends the messages to the telemetry device.

RWHAT?

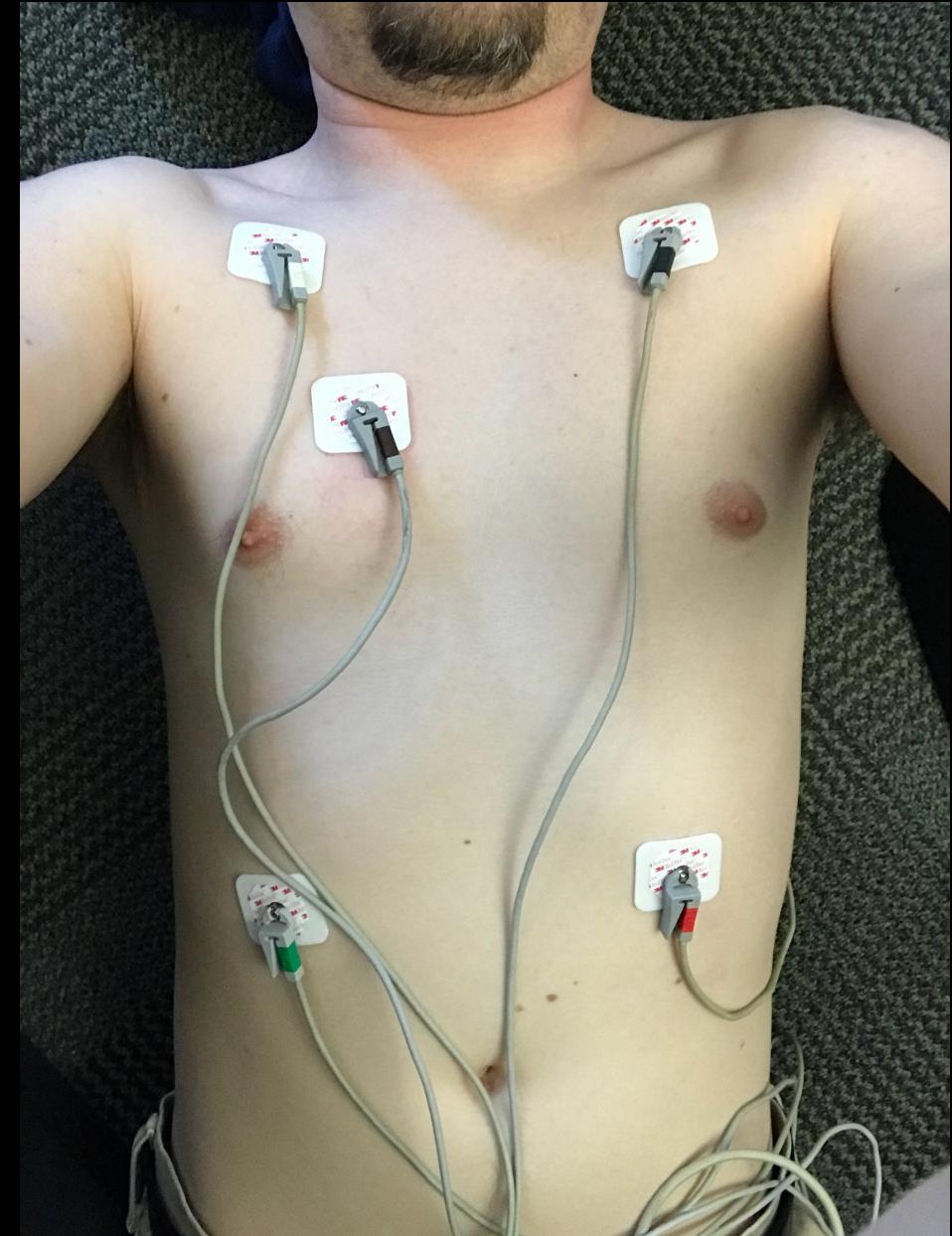
RWHAT packets

All monitoring devices on the [REDACTED] Network periodically broadcast information about themselves in “RWHAT” packets. Among other things, RWHAT packets contain IP address, port number, name, and offered services information about each device.

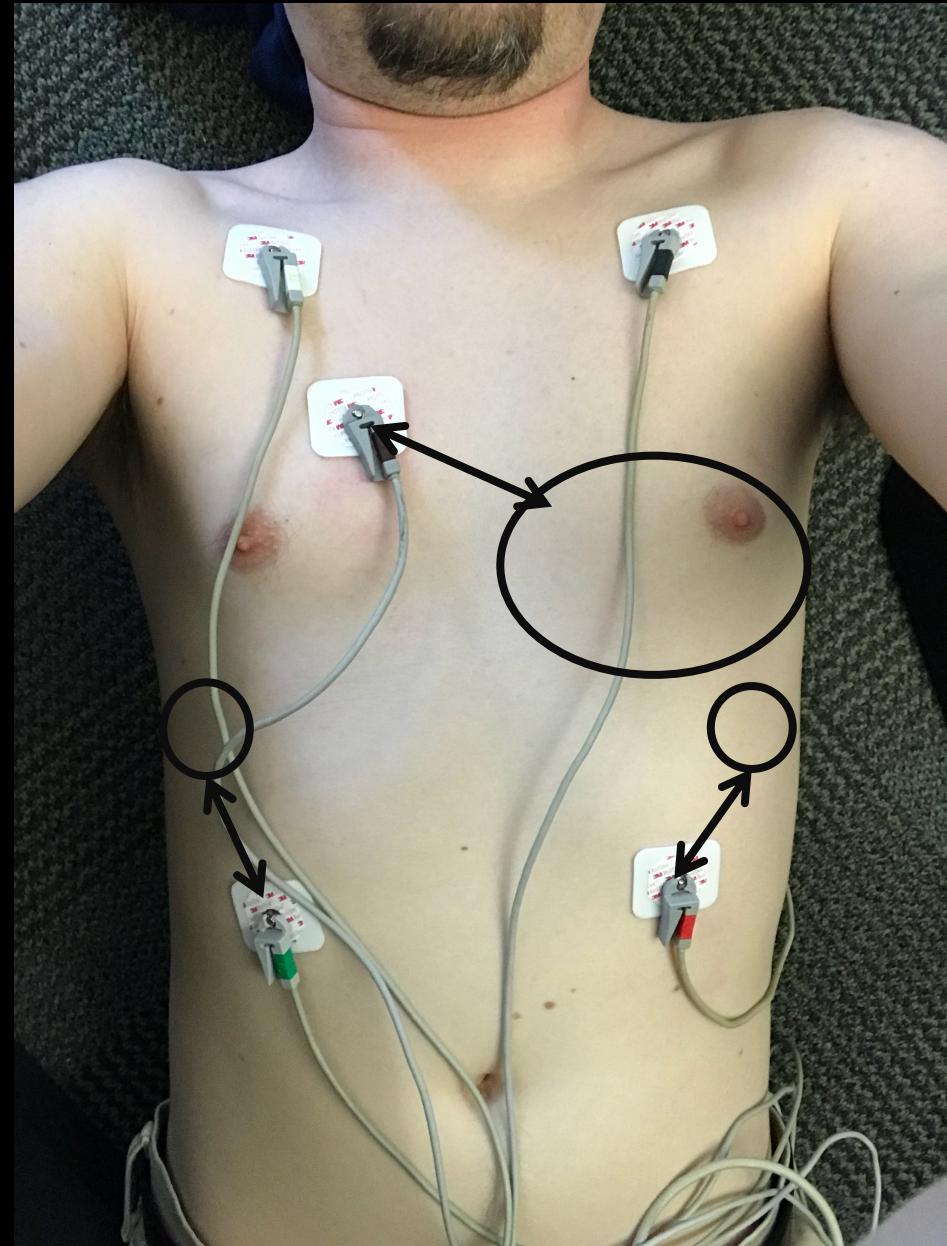
For example, when a [REDACTED] computer communicates with a telemetry device, the telemetry device’s IP address is retrieved from the [REDACTED] computer RWHAT database, the [REDACTED] Network messages are created, and the [REDACTED] Windows operating system sends the messages to the telemetry device.

TESTING SETUP

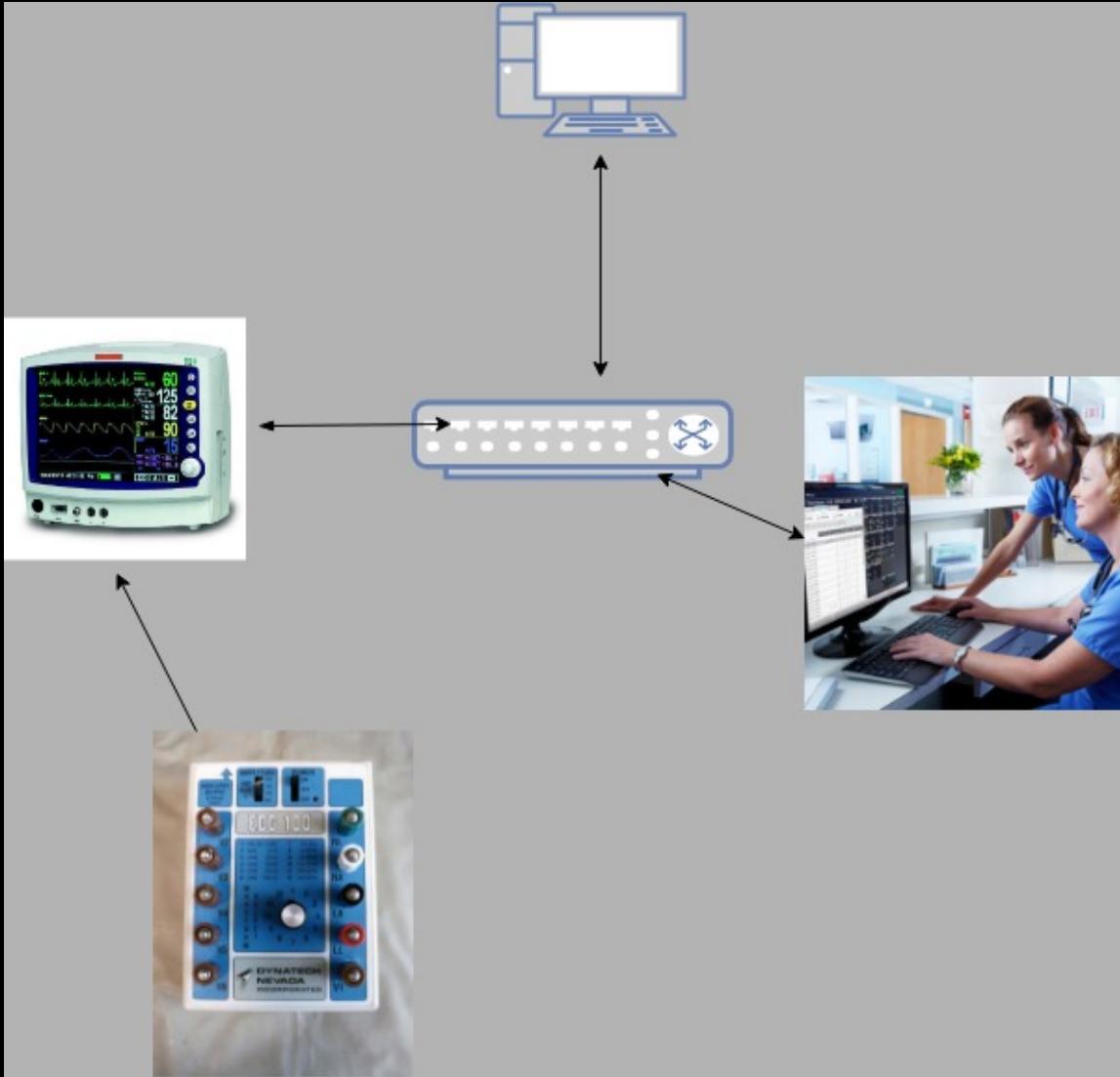
TESTING SETUP



TESTING SETUP



IMPROVED TESTING SETUP



CMS IDLE PACKETS

CMS IDLE PACKETS

- CMS BROADCAST PORT

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
2	0.000003	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
3	0.000005	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
4	10.015240	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
5	10.015243	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
6	10.015245	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88

► Frame 1: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
► Ethernet II, Src: Advantec_97:1f:67 (00:d0:c9:97:1f:67), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
► Internet Protocol Version 4, Src: 126.1.1.1, Dst: 126.255.255.255
► User Datagram Protocol, Src Port: 7000, Dst Port: 7000
▼ Data (88 bytes)
Data: 010400007e0101010000000045447c434943000000000000...
[Length: 88]

0000	ff ff ff ff ff 00 d0	c9 97 1f 67 08 00 45 00g..E.
0010	00 74 ea b2 00 00 80 11	51 c5 7e 01 01 01 7e ff	.t.....	Q.~...~.
0020	ff ff 1b 58 1b 58 00 60	dc b0 01 04 00 00 7e 01	...X.X.~.
0030	01 01 00 00 00 45 44	7c [REDACTED] 00 00 00 00ED [REDACTED]
0040	00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0050	00 00 00 00 09 00 02	07 d0 00 32 04 01 00 172...
0060	04 02 00 1b 04 03 00 21	04 04 00 06 1f 46 00 07!F..
0070	04 05 00 04 1f 42 00 22	07 d0 00 00 00 00 00 00B."
0080	00 00		..	

CMS IDLE PACKETS

- CMS BROADCAST PORT
- EVERY 10 SECONDS

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
2	0.000003	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
3	0.000005	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
4	10.015240	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
5	10.015243	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
6	10.015245	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88

▶ Frame 1: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
▶ Ethernet II, Src: Advantec_97:1f:67 (00:d0:c9:97:1f:67), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 126.1.1.1, Dst: 126.255.255.255
▶ User Datagram Protocol, Src Port: 7000, Dst Port: 7000
▼ Data (88 bytes)

Data: 010400007e0101010000000045447c434943000000000000...
[Length: 88]

0000	ff ff ff ff ff 00 d0	c9 97 1f 67 08 00 45 00g..E.
0010	00 74 ea b2 00 00 80 11	51 c5 7e 01 01 01 7e ff	.t..... Q.~...~.
0020	ff ff 1b 58 1b 58 00 60	dc b0 01 04 00 00 7e 01	...X.X. `
0030	01 01 00 00 00 45 44	7c [REDACTED] 00 00 00 00ED [REDACTED]
0040	00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0050	00 00 00 00 09 00 02	07 d0 00 32 04 01 00 172....
0060	04 02 00 1b 04 03 00 21	04 04 00 06 1f 46 00 07!F..
0070	04 05 00 04 1f 42 00 22	07 d0 00 00 00 00 00 00B."
0080	00 00		...

CMS IDLE PACKETS

- CMS BROADCAST PORT
- EVERY 10 SECONDS
- IDENTIFIES NAME

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
2	0.000003	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
3	0.000005	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
4	10.015240	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
5	10.015243	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
6	10.015245	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88

► Frame 1: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
► Ethernet II, Src: Advantec_97:1f:67 (00:d0:c9:97:1f:67), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
► Internet Protocol Version 4, Src: 126.1.1.1, Dst: 126.255.255.255
► User Datagram Protocol, Src Port: 7000, Dst Port: 7000
▼ Data (88 bytes)

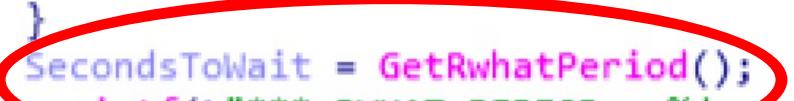
Data: 010400007e0101010000000045447c434943000000000000...
[Length: 88]

0000	ff ff ff ff ff ff 00 d0	c9 97 1f 67 08 00 45 00g..E.
0010	00 74 ea b2 00 00 80 11	51 c5 7e 01 01 01 7e ff	.t. . . . ~.
0020	ff ff 1b 58 1b 58 00 60	dc b0 01 04 00 00 7e 01	.. X. ` ..
0030	01 01 00 00 00 45 44	7c [REDACTED] 00 00 00 00 ED [REDACTED]
0040	00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 ! .. F..
0050	00 00 00 00 09 00 02	07 d0 00 32 04 01 00 17	... B." ..
0060	04 02 00 1b 04 03 00 21	04 04 00 06 1f 46 00 07	
0070	04 05 00 04 1f 42 00 22	07 d0 00 00 00 00 00 00	
0080	00 00		

CMS IDLE PACKETS

```
20     while ( GetExitCodeThread(hThread, &ExitCode) != 1 || ExitCode == 259 )
21     {
22         error = BroadcastRwhat(socket, destPortNum);
23         if ( error == -1 || !error )
24         {
25             winErrorCode = (const wchar_t *)WSAGetLastError();
26             swprintf(&String, (size_t)L"BroadcastRwhat() failed (Err = %d).", winErrorCode);
27             wprintf(L"%s\n", &String);
28             HIDWORD(v5) = &String;
29             LODWORD(v5) = 0;
30             log(v5);
31             break;
32         }
33         SecondsToWait = GetRwhatPeriod();
34         wprintf(L"*** RWHAT PERIOD = %d seconds. ***\n", SecondsToWait);
35         age_rwhat(3 * SecondsToWait);
36         Sleep(1000 * SecondsToWait);
37         if ( dword_405198 > 0 )
38             break;
39     }
```

CMS IDLE PACKETS

```
20     while ( GetExitCodeThread(hThread, &ExitCode) != 1 || ExitCode == 259 )
21     {
22         error = BroadcastRwhat(socket, destPortNum);
23         if ( error == -1 || !error )
24         {
25             winErrorCode = (const wchar_t *)WSAGetLastError();
26             swprintf(&String, (size_t)L"BroadcastRwhat() failed (Err = %d).", winErrorCode);
27             wprintf(L"%s\n", &String);
28             HIDWORD(v5) = &String;
29             LODWORD(v5) = 0;
30             log(v5);
31             break;
32         }
33         SecondsToWait = GetRwhatPeriod();  
    
34         wprintf(L"*** RWHAT PERIOD = %d seconds. ***\n", SecondsToWait);
35         age_rwhat(3 * SecondsToWait);
36         Sleep(1000 * SecondsToWait);
37         if ( dword_405198 > 0 )
38             break;
39     }
```

CMS IDLE PACKETS

```
1 int __usercall GetRwhatPeriod@<eax>(wchar_t *a1@<ebp>)
2 {
3     signed int TimeConfigValue; // esi
4
5     while ( G
6     {
7         error = WaitForSingleObjectCIC(a1, dword_67A7893C, 0xFFFFFFFF, "rwhatutil.cpp", 419);
8         TimeConfigValue = *(_DWORD *)Mapped_RWHT_DB;
9         ReleaseMutex(dword_67A7893C);
10        if ( TimeConfigValue < 100 )
11            return 10;
12        if ( TimeConfigValue < 150 )
13            return 15;
14        if ( TimeConfigValue >= 200 )
15            return TimeConfigValue >= 250 ? 28 : 25;
16        log(v
17        return 20;
18        break;
19    }
20
21    SecondsToWait = GetRwhatPeriod();
22    wprintf(L"*** RWHAT PERIOD = %d seconds. ***\n", SecondsToWait);
23    age_rwhat(3 * SecondsToWait);
24    Sleep(1000 * SecondsToWait);
25    if ( dword_405198 > 0 )
26        break;
27
28
29
30
31
32
33
34
35
36
37
38
39 }
```

CMS IDLE PACKETS

```
1 int __usercall GetRwhatPeriod@<eax>(wchar_t *a1@<ebp>)
2 {
3     signed int TimeConfigValue; // esi
4
5     WaitForSingleObjectCIC(a1, dword_67A7893C, 0xFFFFFFFF, "rwhatutil.cpp", 419);
6     TimeConfigValue = *(_DWORD *)Mapped_RWHT_DB;
7     ReleaseMutex(dword_67A7893C);
8     if ( TimeConfigValue < 100 )
9         return 10;
10    if ( TimeConfigValue < 150 )
11        return 15;
12    if ( TimeConfigValue >= 200 )
13        return TimeConfigValue >= 250 ? 28 : 25;
14    log(v);
15    break;
16 }
17 SecondsToWait = GetRwhatPeriod();
18 wprintf(L"*** RWHAT PERIOD = %d seconds. ***\n", SecondsToWait);
19 age_rwhat(3 * SecondsToWait);
20 Sleep(1000 * SecondsToWait);
21 if ( dword_405198 > 0 )
22     break;
23 }
```

PM IDLE/BROADCAST PACKETS

- EVERY 10 SECONDS
- SRC PORTS INCREMENT
- COUNTER BY 0xA
- PATIENT INFO

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	126.4.153.150	126.255.255.255	UDP	130	3107 → 7000 Len=88
2	9.999642	126.4.153.150	126.255.255.255	UDP	130	3108 → 7000 Len=88
3	19.999584	126.4.153.150	126.255.255.255	UDP	130	3109 → 7000 Len=88
4	29.999393	126.4.153.150	126.255.255.255	UDP	130	3110 → 7000 Len=88

► Frame 1: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
► Ethernet II, Src: Marquett_04:99:96 (00:00:a1:04:99:96), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
► Internet Protocol Version 4, Src: 126.4.153.150, Dst: 126.255.255.255
► User Datagram Protocol, Src Port: 3107, Dst Port: 7000
▼ Data (88 bytes)

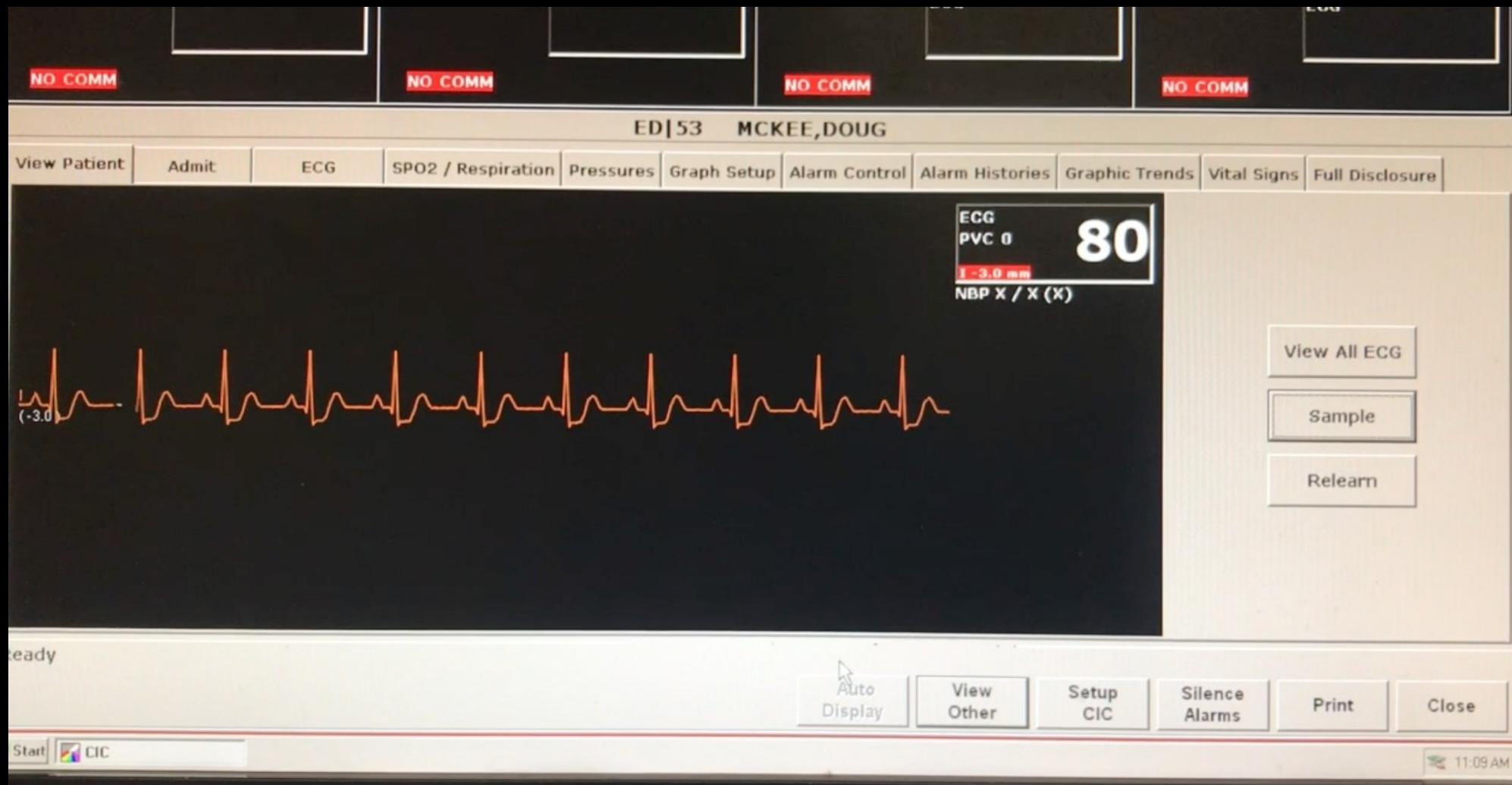
Data: 010400007e0499965a6729b7444d317c3333352d31000000...
[Length: 88]

0000	ff ff ff ff ff ff 00 00	a1 04 99 96 08 00 45 00 E.
0010	00 74 11 8e 00 00 ff 11	13 51 7e 04 99 96 7e ff	.t..... Q ..~.
0020	ff ff 0c 23 1b 58 00 60	00 00 01 04 00 00 7e 04	..# X ..~.
0030	99 96 5a 67 29 b7 44 4d	31 7c 33 33 35 2d 31 00	.Zg DM 1 335-1.
0040	00 00 00 00 00 00 4d 43	4b 45 45 2c 44 4f 55 47	MC KEE, DOUG
0050	00 00 00 00 00 07 00 03	07 d0 00 11 00 2c 00 0d , ,
0060	07 d0 00 0c 07 d0 00 13	0b b8 00 1c 0b b9 00 04 , ,
0070	1f 42 00 00 00 00 00 00	00 00 00 00 00 00 00 00	B.....
0080	00 00		...

PM IDLE/BROADCAST PACKETS

```
35 PatientNameAndBedName = (unsigned __int16 *)((char *)payload + 12);
36 v8 = (unsigned __int16 *)v6;
37 v9 = wcslen((const wchar_t *)payload + 6);
38 if ( v9 < 32 )
39     fill((unsigned __int16 *)payload + v9 + 6, 32 - v9, 0);
40 parse_logical_name(PatientNameAndBedName, 0x20u, &PatientName, &UnitName);
41 al = wcscpy;                                // nonsense
42 if ( !PatientName )
43 {
44     wcscpy(&PatientName, noname);
45     v19 = 0;
46     if ( UnitName )
47         goto LABEL_10;
48     goto LABEL_9;
49 }
50 if ( !UnitName )
51 {
52 LABEL_9:
53     wcscpy(&UnitName, nounit);
54     v17 = 0;
55 LABEL_10:
56     logicalName = (wchar_t *(__cdecl *)(wchar_t *, const wchar_t *))make_logical_name(&UnitName, &PatientName);
```

CMS – NORMAL OPERATION WITH ECG SIMULATOR



CMS – NORMAL OPERATION WITH ECG SIMULATOR



NORMAL TRAFFIC

197	267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
198	267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
199	268.083724	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
200	268.083727	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
201	268.333882	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
202	268.333886	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
203	268.584087	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
204	268.584091	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
205	268.833867	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
206	268.833870	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
207	269.083717	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
208	269.083720	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
209	269.333925	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
210	269.333928	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
211	269.334592	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
212	269.334594	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
213	269.592066	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
▶ Frame 197: 681 bytes on wire (5448 bits), 681 bytes captured (5448 bits)							
▶ Ethernet II, Src: Marquett_04:99:96 (00:00:a1:04:99:96), Dst: Advantec_97:1f:67 (00:d0:c9:97:1f:67)							
▶ Internet Protocol Version 4, Src: 126.4.153.150, Dst: 126.1.1.1							
▶ User Datagram Protocol, Src Port: 3008, Dst Port: 3627							
0000	00 d0 c9 97 1f 67 00 00	a1 04 99 96 08 00 45 00g..E.			
0010	02 9b 00 0e 00 00 ff 11	22 a7 7e 04 99 96 7e 01	"..~...~.			
0020	01 01 0b c0 0e 2b 02 87	00 00 04 a9 00 00 07 0b+			
0030	ff ff 00 00 00 00 ff ff	08 0b ff fe ff ff 00 00			
0040	ff ff 09 0b 00 00 00 01	00 01 00 00 0a 0b ff fe			

NORMAL TRAFFIC

PM

267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
268.083721	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
201 268.083727	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
201 268.333882	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
202 268.333886	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
203 268.584087	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
204 268.584091	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
205 268.833867	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
206 268.833870	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
207 269.083717	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
208 269.083720	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
209 269.333925	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
210 269.333928	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
211 269.334592	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625 Len=474
212 269.334594	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625 Len=474
213 269.592066	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639

- ▶ Frame 197: 681 bytes on wire (5448 bits), 681 bytes captured (5448 bits)
- ▶ Ethernet II, Src: Marquett_04:99:96 (00:00:a1:04:99:96), Dst: Advantec_97:1f:67 (00:d0:c9:97:1f:67)
- ▶ Internet Protocol Version 4, Src: 126.4.153.150, Dst: 126.1.1.1
- ▶ User Datagram Protocol, Src Port: 3008, Dst Port: 3627

0000	00 d0 c9 97 1f 67 00 00	a1 04 99 96 08 00 45 00g..E.
0010	02 9b 00 0e 00 00 ff 11	22 a7 7e 04 99 96 7e 01 " .~...~.
0020	01 01 0b c0 0e 2b 02 87	00 00 04 a9 00 00 07 0b+..
0030	ff ff 00 00 00 00 ff ff	08 0b ff fe ff ff 00 00
0040	ff ff 09 0b 00 00 00 01	00 01 00 00 0a 0b ff fe

NORMAL TRAFFIC

CMS

PM

267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
268.083721	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
201 268.083727	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
201 268.333882	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
202 268.333886	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
203 268.584087	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
204 268.584091	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
205 268.833867	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
206 268.833870	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
207 269.083717	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
208 269.083720	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
209 269.333925	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
210 269.333928	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
211 269.334592	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625 Len=474
212 269.334594	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625 Len=474
213 269.592066	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639

► Frame 197: 681 bytes on wire (5448 bits), 681 bytes captured (5448 bits)
► Ethernet II, Src: Marquett_04:99:96 (00:00:a1:04:99:96), Dst: Advantec_97:1f:67 (00:d0:c9:97:1f:67)
► Internet Protocol Version 4, Src: 126.4.153.150, Dst: 126.1.1.1
► User Datagram Protocol, Src Port: 3008, Dst Port: 3627

0000	00 d0 c9 97 1f 67 00 00	a1 04 99 96 08 00 45 00g..E.
0010	02 9b 00 0e 00 00 ff 11	22 a7 7e 04 99 96 7e 01	"~...~"
0020	01 01 0b c0 0e 2b 02 87	00 00 04 a9 00 00 07 0b+..
0030	ff ff 00 00 00 00 ff ff	08 0b ff fe ff ff 00 00
0040	ff ff 09 0b 00 00 00 01	00 01 00 00 0a 0b ff fe

NORMAL TRAFFIC

CMS

PM

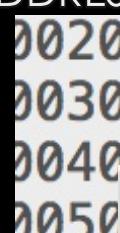
Data
Packets

267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
268.083721	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
201 268.083727	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
201 268.333882	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
202 268.333886	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
203 268.584087	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
204 268.584091	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
205 268.833867	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
206 268.833870	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
207 269.083717	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
208 269.083720	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
209 269.333925	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
210 269.333928	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
211 269.334592	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625 Len=471
212 269.334594	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625 Len=474
213 269.592066	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639

- ▶ Frame 197: 681 bytes on wire (5448 bits), 681 bytes captured (5448 bits)
- ▶ Ethernet II, Src: Marquett_04:99:96 (00:00:a1:04:99:96), Dst: Advantec_97:1f:67 (00:d0:c9:97:1f:67)
- ▶ Internet Protocol Version 4, Src: 126.4.153.150, Dst: 126.1.1.1
- ▶ User Datagram Protocol, Src Port: 3008, Dst Port: 3627

```
0000  00 d0 c9 97 1f 67 00 00  a1 04 99 96 08 00 45 00  ....g.. ....E.  
0010  02 9b 00 0e 00 00 ff 11  22 a7 7e 04 99 96 7e 01  ..... ".~...~.  
0020  01 01 0b c0 0e 2b 02 87  00 00 04 a9 00 00 07 0b  .....+.. ....  
0030  ff ff 00 00 00 00 ff ff  08 0b ff fe ff ff 00 00  .....  
0040  ff ff 09 0b 00 00 00 01  00 01 00 00 0a 0b ff fe  .....
```

BASIC OBSERVATIONS

- UDP PACKETS
 - UTILIZATION OF BROADCAST ADDRESS
 - COUNTERS
 - VARYING PORT NUMBERS
 - NOT ENCRYPTED

User Datagram Protocol, Src Port: 3107, Dst Port: 7000
Source Port: 3107
Destination Port: 7000
Length: 96
[Checksum: [missing]]
[Checksum Status: Not present]

[Header checksum status: Unverified]

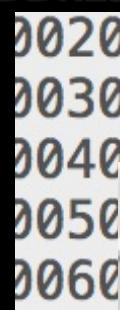
~~Source: 126.4.153.150~~

Destination: 126.255.255.255

Length	Info
130	3107 → 70
130	3108 → 70
130	3109 → 70
130	3110 → 70

..Zg).DM 1|335-1.
MC KEE, DOUG

BASIC OBSERVATIONS

- UDP PACKETS
 - UTILIZATION OF BROADCAST ADDRESS
 - COUNTERS
 - VARYING PORT NUMBERS
 - NOT ENCRYPTED
 - DATA PACKETS

User Datagram Protocol,

~~Source Port: 3107~~

Destination Port: 7000

Length: 96

[Checksum: [missing]]

[Checksum Status: Not present]

[Header checksum]

Source: 126.4.153

Destination: 126

ES C TP H

0c 23 1b 58 00 60

5a 67 29 b7 44 4d

00 00 00 00 4d 43

Info

A red rounded rectangular button placeholder located at the bottom of the page.

3107 70 11

5107

3109 7

5100 11

3100 70

3109 → / ..

2110 34 B

3110 → 7

... .

For more information about the study, please contact Dr. Michael J. Hwang at (319) 356-4530 or via email at mhwang@uiowa.edu.

Src P	3	Len=639
00	3008 → 3627	Len=639
	3008 → 3627	Len=639
- pres.	3008 → 3627	Len=639
sum	3008 → 3627	Len=639
153	3008 → 3627	Len=639
126.	3008 → 3627	Len=639
60	3008 → 3627	Len=639
4d	3008 → 3627	Len=639
43	3008 → 3627	Len=639
	3010 → 3625	Len=174

..Zg) DM 1|335-1.
..... MC KEE, DOUG

Data Packets

BASIC OBSERVATIONS

- UDP PACKETS
- UTILIZATION OF BROADCAST ADDRESS
- COUNTERS
- VARYING PORT NUMBERS
- NOT ENCRYPTED
- DATA PACKETS
- REPLAY ATTACK ?



SIMPLE REPLAY!!!!

SIMPLE REPLAY!!!!



UNDERSTANDING THE PACKETS: HANDSHAKE

UNDERSTANDING THE PACKETS: HANDSHAKE

173	260.261351	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
174	260.261353	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
183	263.893005	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000	Len=62
184	263.893007	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000	Len=62
185	265.318585	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
186	265.318588	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
187	265.318590	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
188	265.318592	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
189	265.334402	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
190	265.334405	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
191	265.381835	126.1.1.1	126.4.153.150	UDP	104	3626 → 2000	Len=62
192	265.381838	126.1.1.1	126.4.153.150	UDP	104	3626 → 2000	Len=62
193	267.334357	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
194	267.334360	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
195	267.421811	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000	Len=62
196	267.421813	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000	Len=62
197	267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
198	267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639

UNDERSTANDING THE PACKETS: HANDSHAKE

173	260.261351	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
174	260.261353	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
183	263.893005	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000	Len=62
184	263.893007	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000	Len=62
185	265.318585	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
186	265.318588	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
187	265.318590	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
188	265.318592	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
189	265.334402	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
190	265.334405	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
191	265.381835	126.1.1.1	126.4.153.150	UDP	104	3626 → 2000	Len=62
192	265.381838	126.1.1.1	126.4.153.150	UDP	104	3626 → 2000	Len=62
193	267.334357	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
194	267.334360	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
195	267.421811	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000	Len=62
196	267.421813	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000	Len=62
197	267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
198	267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639

CMS Opens
Channel
“SYN”

UNDERSTANDING THE PACKETS: HANDSHAKE

173	260.261351	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
174	260.261353	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
183	263.893005	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000	Len=62
184	263.893007	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000	Len=62
185	265.318585	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
186	265.318588	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
187	265.318590	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
188	265.318592	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
189	265.334402	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
190	265.334405	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
191	265.381835	126.1.1.1	126.4.153.150	UDP	104	3626 → 2000	Len=62
192	265.381838	126.1.1.1	126.4.153.150	UDP	104	3626 → 2000	Len=62
193	267.334357	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
194	267.334360	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
195	267.421811	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000	Len=62
196	267.421813	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000	Len=62
197	267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
198	267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639

CMS Opens
Channel
“SYN”

PM
“SYN, ACK”

UNDERSTANDING THE PACKETS: HANDSHAKE

173	260.261351	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
174	260.261353	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
183	263.893005	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000	Len=62
184	263.893007	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000	Len=62
185	265.318585	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
186	265.318588	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
187	265.318590	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
188	265.318592	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
189	265.334402	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
190	265.334405	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
191	265.381835	126.1.1.1	126.4.153.150	UDP	104	3626 → 2000	Len=62
192	265.381838	126.1.1.1	126.4.153.150	UDP	104	3626 → 2000	Len=62
193	267.334357	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
194	267.334360	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
195	267.421811	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000	Len=62
196	267.421813	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000	Len=62
197	267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
198	267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639

CMS Opens
Channel
“SYN”

PM
“SYN, ACK”

UNDERSTANDING THE PACKETS: HANDSHAKE

173	260.261351	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
174	260.261353	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
183	263.893005	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000	Len=62
184	263.893007	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000	Len=62
185	265.318585	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
186	265.318588	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
187	265.318590	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
188	265.318592	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
189	265.334402	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
190	265.334405	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
191	265.381835	126.1.1.1	126.4.153.150	UDP	104	3626 → 2000	Len=62
192	265.381838	126.1.1.1	126.4.153.150	UDP	104	3626 → 2000	Len=62
193	267.334357	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
194	267.334360	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
195	267.421811	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000	Len=62
196	267.421813	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000	Len=62
197	267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
198	267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639

CMS Opens
Channel
“SYN”

PM
“SYN, ACK”

CMS
“ACK”

UNDERSTANDING THE PACKETS: HANDSHAKE

173	260.261351	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
174	260.261353	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
183	263.893005	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000 Len=62
184	263.893007	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000 Len=62
185	265.318585	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000 Len=88
186	265.318588	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000 Len=88
187	265.318590	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000 Len=88
188	265.318592	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000 Len=88
189	265.334402	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625 Len=474
190	265.334405	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625 Len=474
191	265.381835	126.1.1.1	126.		104	3626 → 2000 Len=62
192	265.381838	126.1.1.1	126.		104	3626 → 2000 Len=62
193	267.334357	126.4.153.150	126.		516	3010 → 3625 Len=474
194	267.334360	126.4.153.150	126.1.		516	3010 → 3625 Len=474
195	267.421811	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000 Len=62
196	267.421813	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000 Len=62
197	267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
198	267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639

PM
What port you
want to use?

CMS Opens
Channel
“SYN”

PM
“SYN, ACK”

CMS
“ACK”

UNDERSTANDING THE PACKETS: HANDSHAKE

173	260.261351	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
174	260.261353	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
183	263.893005	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000 Len=62
184	263.893007	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000 Len=62
185	265.318585	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000 Len=88
186	265.318588	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000 Len=88
187	265.318590	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000 Len=88
188	265.318592	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000 Len=88
189	265.334402	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625 Len=474
190	265.334405	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625 Len=474
191	265.381835	126.1.1.1	126.		104	3626 → 2000 Len=62
192	265.381838	126.1.1.1	126.		104	3626 → 2000 Len=62
193	267.334357	126.4.153.150	126.		516	3010 → 3625 Len=474
194	267.334360	126.4.153.150	126.1.		516	3010 → 3625 Len=474
195	267.421811	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000 Len=62
196	267.421813	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000 Len=62
197	267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
198	267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639

PM
What port you
want to use?

CMS Opens
Channel
“SYN”

PM
“SYN, ACK”

CMS
“ACK”

CMS
This one! 3627

UNDERSTANDING THE PACKETS: HANDSHAKE

173	260.261351	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
174	260.261353	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000 Len=88
183	263.893005	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000 Len=62
184	263.893007	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000 Len=62
185	265.318585	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000 Len=88
186	265.318588	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000 Len=88
187	265.318590	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000 Len=88
188	265.318592	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000 Len=88
189	265.334402	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625 Len=474
190	265.334405	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625 Len=474
191	265.381835	126.1.1.1	126.		104	3626 → 2000 Len=62
192	265.381838	126.1.1.1	126.		104	3626 → 2000 Len=62
193	267.334357	126.4.153.150	126.		516	3010 → 3625 Len=474
194	267.334360	126.4.153.150	126.1.		516	3010 → 3625 Len=474
195	267.421811	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000 Len=62
196	267.421813	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000 Len=62
197	267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639
198	267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627 Len=639

PM
What port you
want to use?

CMS Opens
Channel
“SYN”

PM
“SYN, ACK”

CMS
“ACK”

CMS
This one! 3627

PM
Ok, Here
some Data!

HANDSHAKE HACKED!!

HANDSHAKE HACKED!!



CLOSER LOOK AT “SYN,ACK” PACKETS

CLOSER LOOK AT “SYN,ACK” PACKETS

173	260.261351	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
174	260.261353	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
183	263.893005	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000	Len=62
184	263.893007	126.1.1.1	126.4.153.150	UDP	104	3625 → 2000	Len=62
185	265.318585	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
186	265.318588	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
187	265.318590	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
188	265.318592	126.4.153.150	126.255.255.255	UDP	130	3015 → 7000	Len=88
189	265.334402	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
190	265.334405	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
191	265.381835	126.1.1.1	126.4.153.150	UDP	104	3626 → 2000	Len=62
192	265.381838	126.1.1.1	126.4.153.150	UDP	104	3626 → 2000	Len=62
193	267.334357	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
194	267.334360	126.4.153.150	126.1.1.1	UDP	516	3010 → 3625	Len=474
195	267.421811	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000	Len=62
196	267.421813	126.1.1.1	126.4.153.150	UDP	104	3627 → 2000	Len=62
197	267.833922	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639
198	267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639

CLOSER LOOK AT “SYN,ACK” PACKETS

173	260.261351	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
174	260.261353	126.1.1.1	126.255.255.255	UDP	130	7000 → 7000	Len=88
182	262.202005	126.1.1.1	126.1.1.1	UDP	181	2625 → 20200	Len=62
0020	01 01 0b c2 0e 29 01 e2 00 00	7e 04 99 96 00 00)... .~.....				
0030	7e 04 99 96 00 00 00 00 c9 00 14 00 01 00 00 13 00 00	~.....				
0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				
0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				
0060	00 00 00 00 01 9e 00 04 00 01 06 00 01 3a c0 00				
0070	00 50 00 00 00 00 00 00 0c 3a e2 80 80 80 80 80 80 80 80	.P.....				
0080	80 80 80 80 03 3a 90 80 00 00 00 28 00 96 00 00(....(....				
0090	00 06 00 00 00 00 00 00 15 3a 00 00 40 21 40 00@!@.@!@.				
00a0	00 00 02 3a 20 05 00 00 40 09 00 04 01 3a 01 00	...: ... @....	...: ... @....				
00b0	01 18 c0 80 80 00 80 00 80 00 0c 18 80 01 00 00				
00c0	00 00 00 00 00 00 00 00 03 18 00 20 00 0f 00 28(....(....				
198	267.833926	126.4.153.150	126.1.1.1	UDP	681	3008 → 3627	Len=639

EMULATION OR REPLAY ATTACK STEPS

1. SEND BROADCAST PACKETS TO ALLOW CMS TO DETECT DEVICE
2. PERFORM HANDSHAKE
 1. ACCOUNTING FOR PORT CHANGES AND COUNTERS
3. SEND CAPTURED HEARTBEAT PACKETS

EMULATION DEMO

IMPACT SCENARIO

- LOADED ONTO RASPBERRY PI
- PLUG PI INTO ETHERNET JACK
- CAN HARM PATIENT UNNOTICED



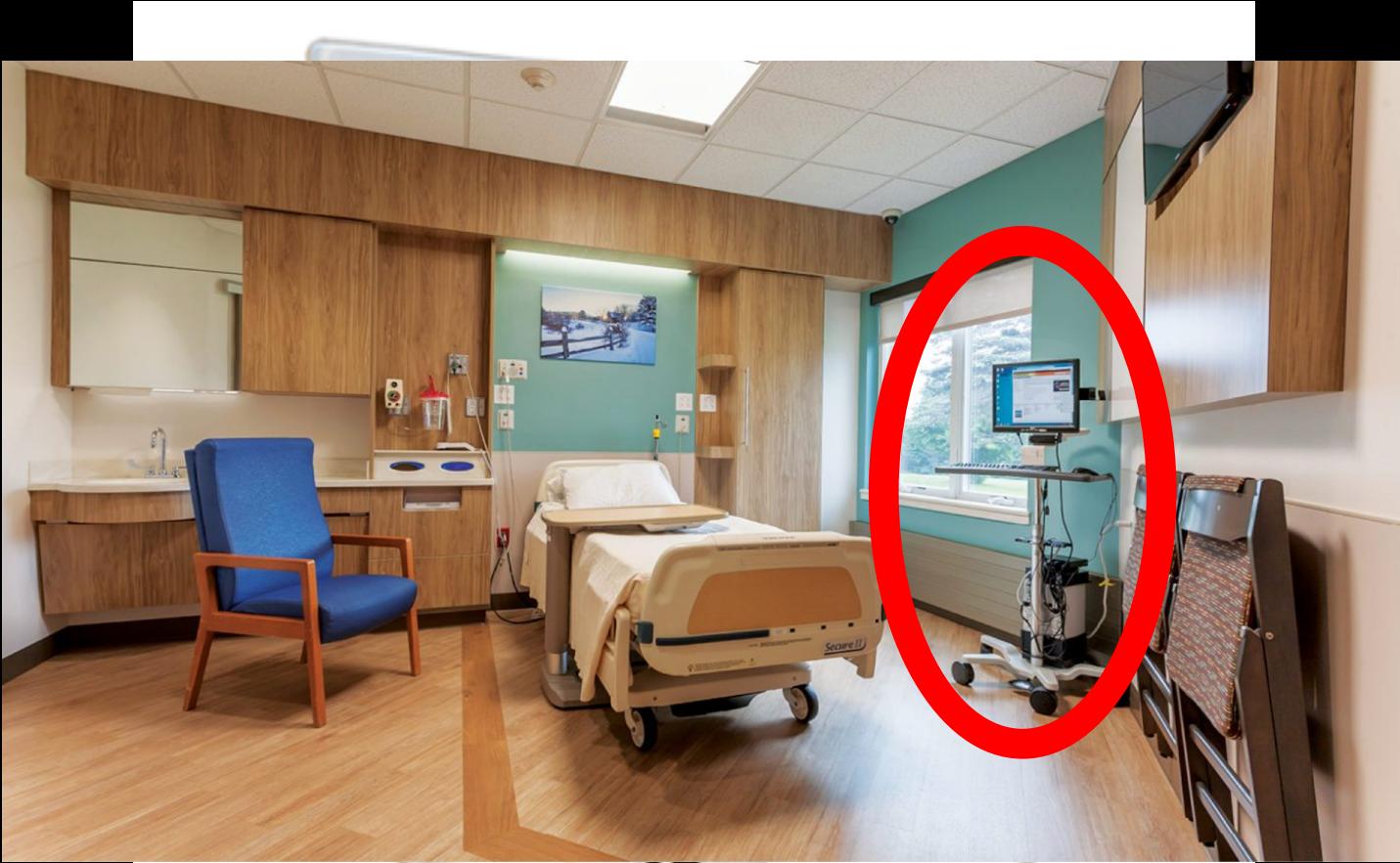
IMPACT SCENARIO

- LOADED ONTO RASPBERRY PI
- PLUG PI INTO ETHERNET JACK
- CAN HARM PATIENT UNNOTICED



IMPACT SCENARIO

- LOADED ONTO RASPBERRY PI
- PLUG PI INTO ETHERNET JACK
- CAN HARM PATIENT UNNOTICED



WHAT ABOUT MODIFYING EXISTING DATA?

- HANDSHAKE IS ALREADY COMPLETED
- DATA PORT? RESPOND PACKET PORT?
 - ARP SPOOF
- SEND NEW DATA ON SAME PORT

INJECTION

433	39.502117	126.4.153.150	126.1.1.1	UDP	516	3008 → 3293	Len=474
434	39.502119	126.4.153.150	126.1.1.1	UDP	516	3008 → 3293	Len=474
► Frame 433: 516 bytes on wire (4128 bits), 516 bytes captured (4128 bits)							
► Ethernet II, Src: Marquett_04:99:96 (00:00:a1:04:99:96), Dst: Advantec_97:1f:67 (00:d0:c9:97:1f:67)							
► Internet Protocol Version 4, Src: 126.4.153.150, Dst: 126.1.1.1							
► User Datagram Protocol, Src Port: 3008, Dst Port: 3293							
▼ Data (474 bytes)							
0020	01 01 0b c0 0c dd 01	7e 04 99 96 00 00 00	19 99 96 00 00~	
0030	00 00 00 00 00 00 00	00 00 00 00 00 00 00	6 c0 00 00	~	
0040	00 00 00 00 00 00 00	00 00 00 00 00 00 00	00 00 00	
0050	00 00 00 00 00 00 00	00 00 00 00 00 00 00	00 00 00	
0060	00 00 00 00 00 00 00	00 00 00 00 00 00 00	3a c0 00:	
0070	00 50 00 00 00 00 00	00 00 00 00 00 00 00	80 80 80 80	P.:	
0080	80 80 80 80 03 3a 90	80 00 00 00 28 00 96	80 80 80 80:(....
0090	00 06 00 00 00 00 00	00 00 00 00 15 3a 00	40 21 40 00@!	@.
00a0	00 00 02 3a 20 05 00	00 40 09 00 04 01 3a	01 00:@:

Heartbeat
Value
(80 base 10)



INJECTION

Kali Box
MAC

	433 39.502117	126.4.153.150	126.1.1.1	UDP	516 3008 → 3294 Len=474
518	44.230408	126.4.153.153	126.1.1.1	UDP	681 3008 → 3294 Len=639
519	44.250825	126.4.153.150	126.1.1.1	UDP	681 3006 → 3294 Len=639
520	44.250827	126.4.153.150	126.1.1.1	UDP	681 3006 → 3294 Len=639
521	44.402360	Vmware_a1:6e:bf	Marquett_04:99:96	ARP	60 126.1.1.1 is at 00:0c:29:a1:6e:bf
522	44.402363	Vmware_a1:6e:bf	Marquett_04:99:96	ARP	60 126.1.1.1 is at 00:0c:29:a1:6e:bf
523	44.484103	126.4.153.153	126.1.1.1	UDP	681 3008 → 3294 Len=639
524	44.484105	126.4.153.153	126.1.1.1	UDP	681 3008 → 3294 Len=639

- ▶ Frame 522: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
- ▶ Ethernet II, Src: Vmware_a1:6e:bf (00:0c:29:a1:6e:bf), Dst: Marquett_04:99:96 (00:00:a1:04:99:96)
- ▼ [Duplicate IP address detected for 126.1.1.1 (00:0c:29:a1:6e:bf) – also in use by 00:d0:c9:97:1f:67 (frame 428)]
 - ▶ [Frame showing earlier use of IP address: 428]
[Seconds since earlier frame seen: 5]
- ▶ Address Resolution Protocol (reply)

0090 00 00 00 00 00 00 00 00 15 5d 00 00 40 21 40 00:..@:..
00a0 00 00 02 3a 20 05 00 00 40 09 00 04 01 3a 01 00 ...: ... @....:

INJECTION

-	463	41.681800	126.4.153.153	126.1.1.1	UDP	516	3010 → 3293	Len=474
	464	41.681803	126.4.153.153	126.1.1.1	UDP	516	3010 → 3293	Len=474
► User Datagram Protocol, Src Port: 3010, Dst Port: 3293								
▼ Data (474 bytes)								
Data: 7e04999600007e049996000000c900140001001800000000... [Length: 474]								
0020	01 01 0b c2 0c dd 01 e2 80 cd	7e 04 99 96 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0030	7e 04 99 96 00 00 00 00 c9 00	14 00 01 00 18 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0040	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0050	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0060	00 00 00 00 00 00 01 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0070	00 78 00 00 00 00 00 00 00 00	00 80 80 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0080	80 00 80 80 00 03 3a 00 00 00	96 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0090	00 06 00 00 00 00 00 00 00 00	40 21 40 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00

Heartbeat
Value
(120 base 10)



DEMO PACKET INJECTION

DEMO PACKET INJECTION 2

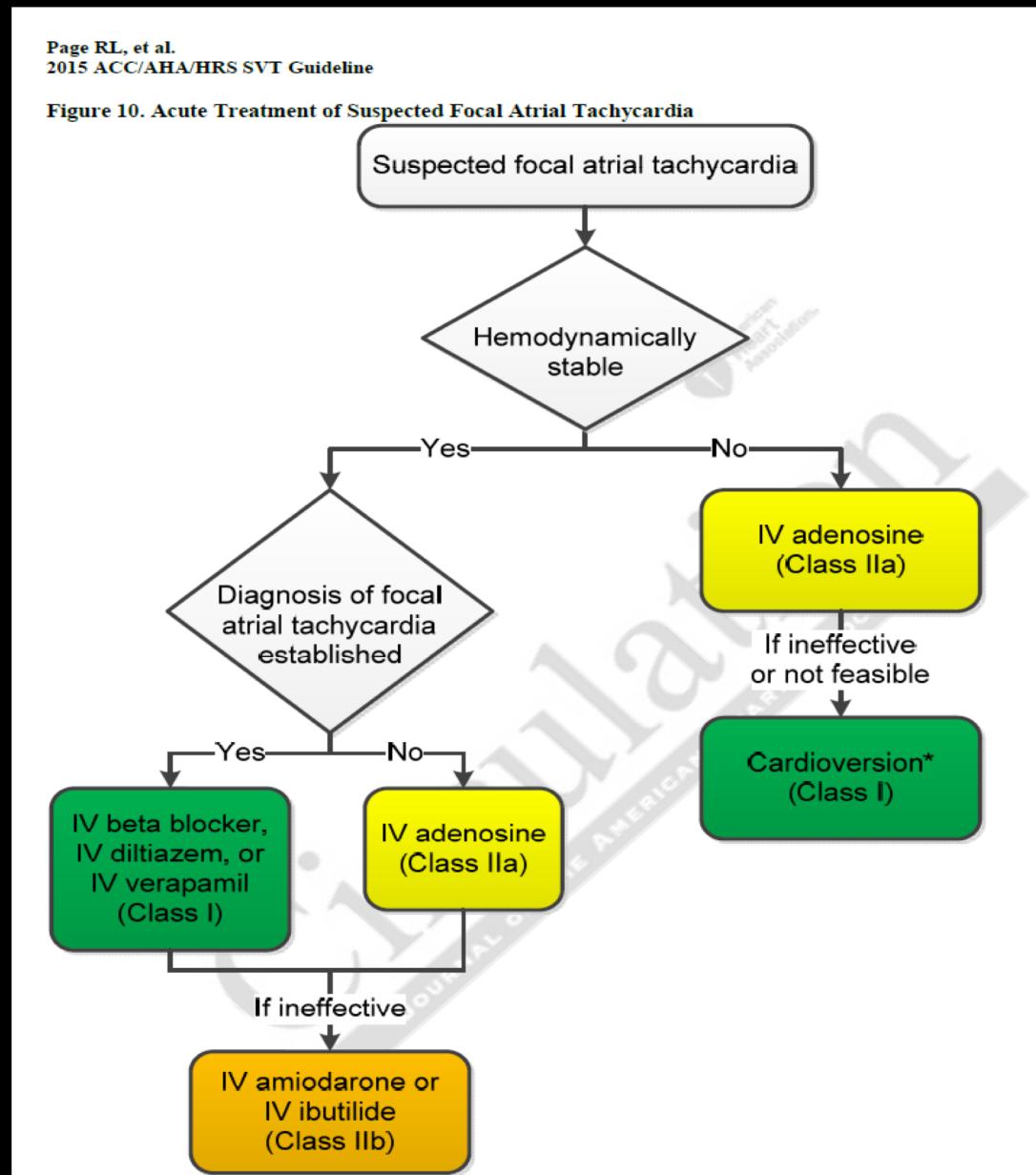
IMPACT SCENARIO

- POWER OF MISINFORMATION
- UNCONSCIOUS PATIENT
- RELIANCE ON TECHNOLOGY
- SMALLER CHANGES, LARGER IMPACT

“Fictitious cardiac rhythms, even intermittent, could lead to extended hospitalization, additional testing, and side effects from medications to control heart rhythm and/or prevent clots. The hospital could also suffer resource consumption.”

- Dr. S. Nordeck

AMER. HEART ASSOC. & AMER. COLLEGE OF CARDIOLOGY – ARRHYTHMIA MANAGEMENT GUIDELINES

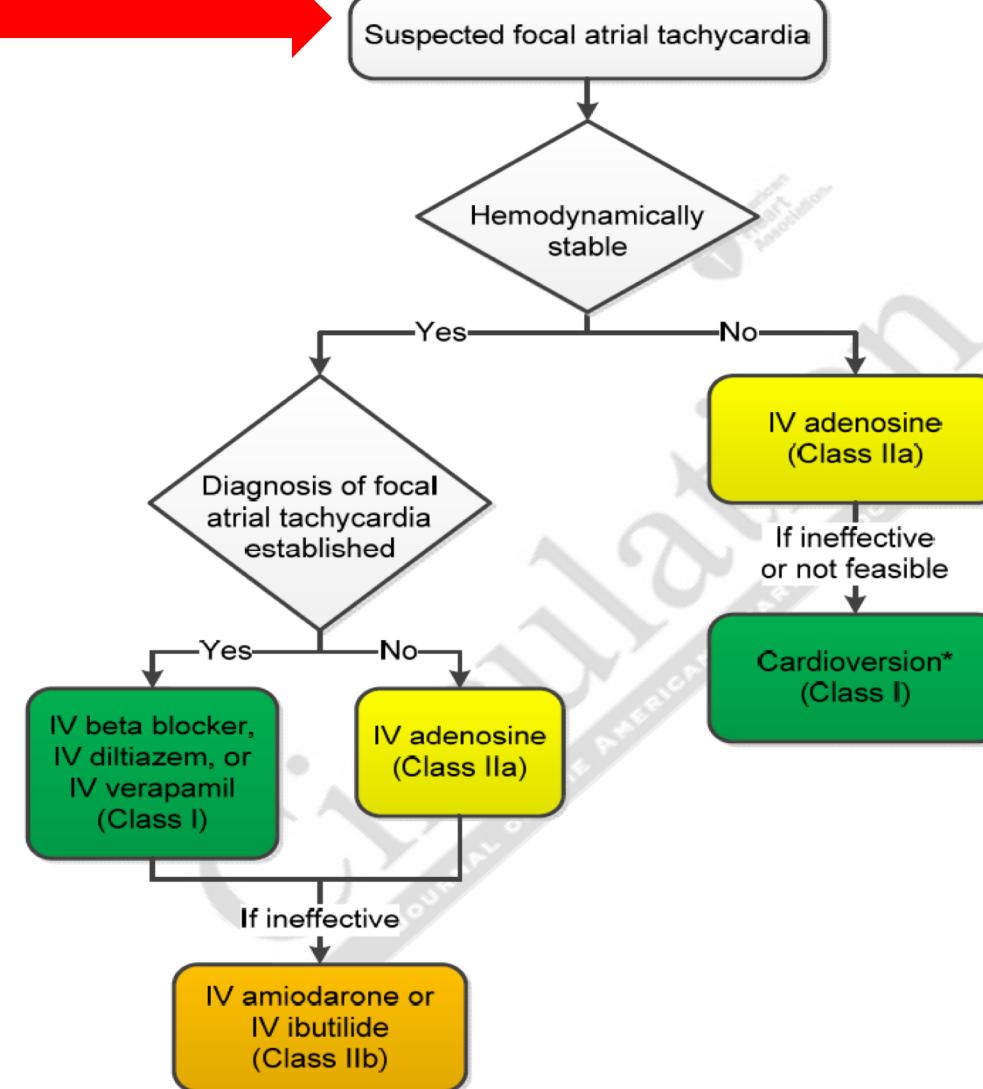


AMER. HEART ASSOC. & AMER. COLLEGE OF CARDIOLOGY – ARRHYTHMIA MANAGEMENT GUIDELINES

Fictitious intermittent
cardiac rhythms

Page RL, et al.
2015 ACC/AHA/HRS SVT Guideline

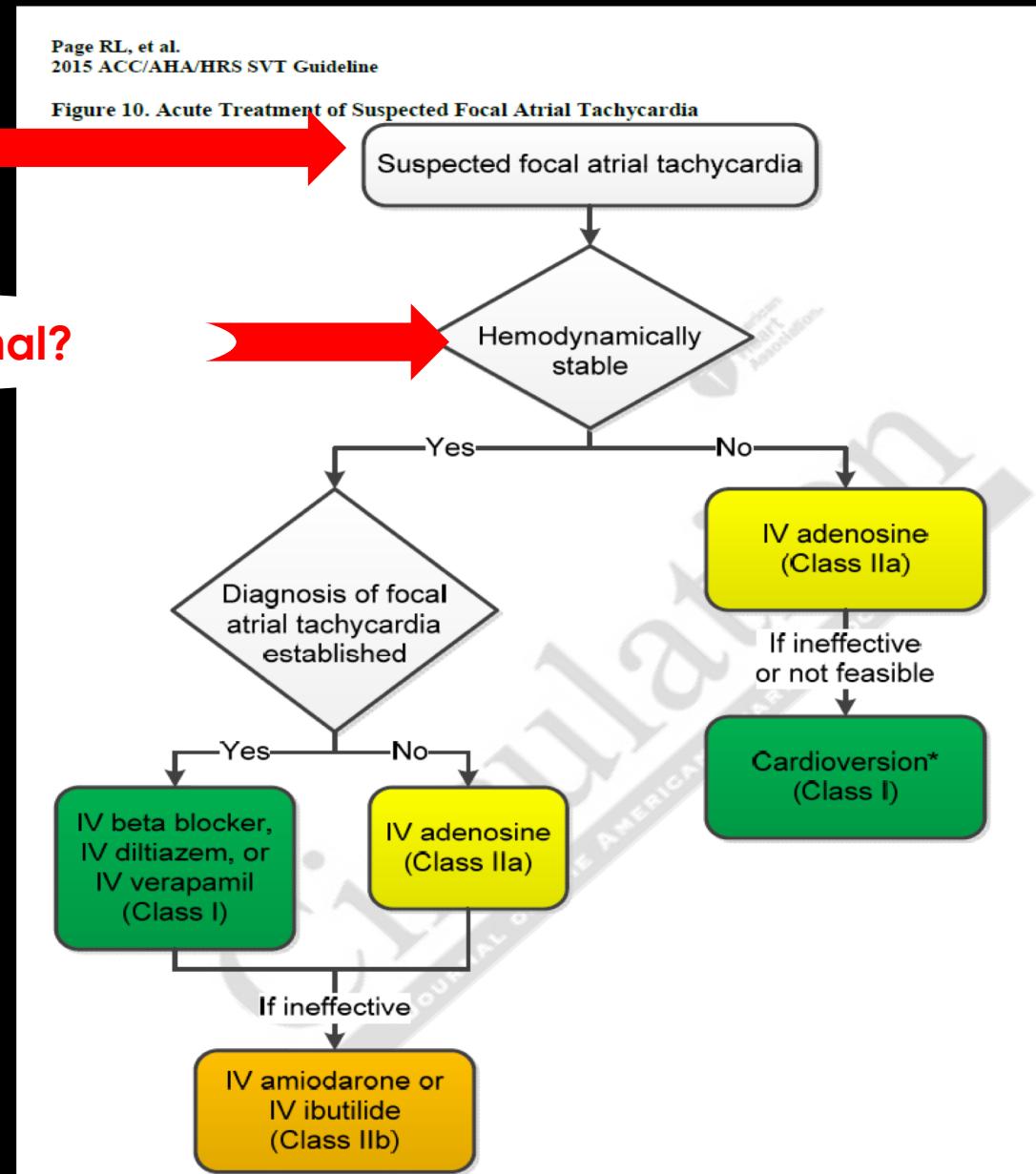
Figure 10. Acute Treatment of Suspected Focal Atrial Tachycardia



AMER. HEART ASSOC. & AMER. COLLEGE OF CARDIOLOGY – ARRHYTHMIA MANAGEMENT GUIDELINES

Fictitious intermittent cardiac rhythms

Blood Pressure Normal?



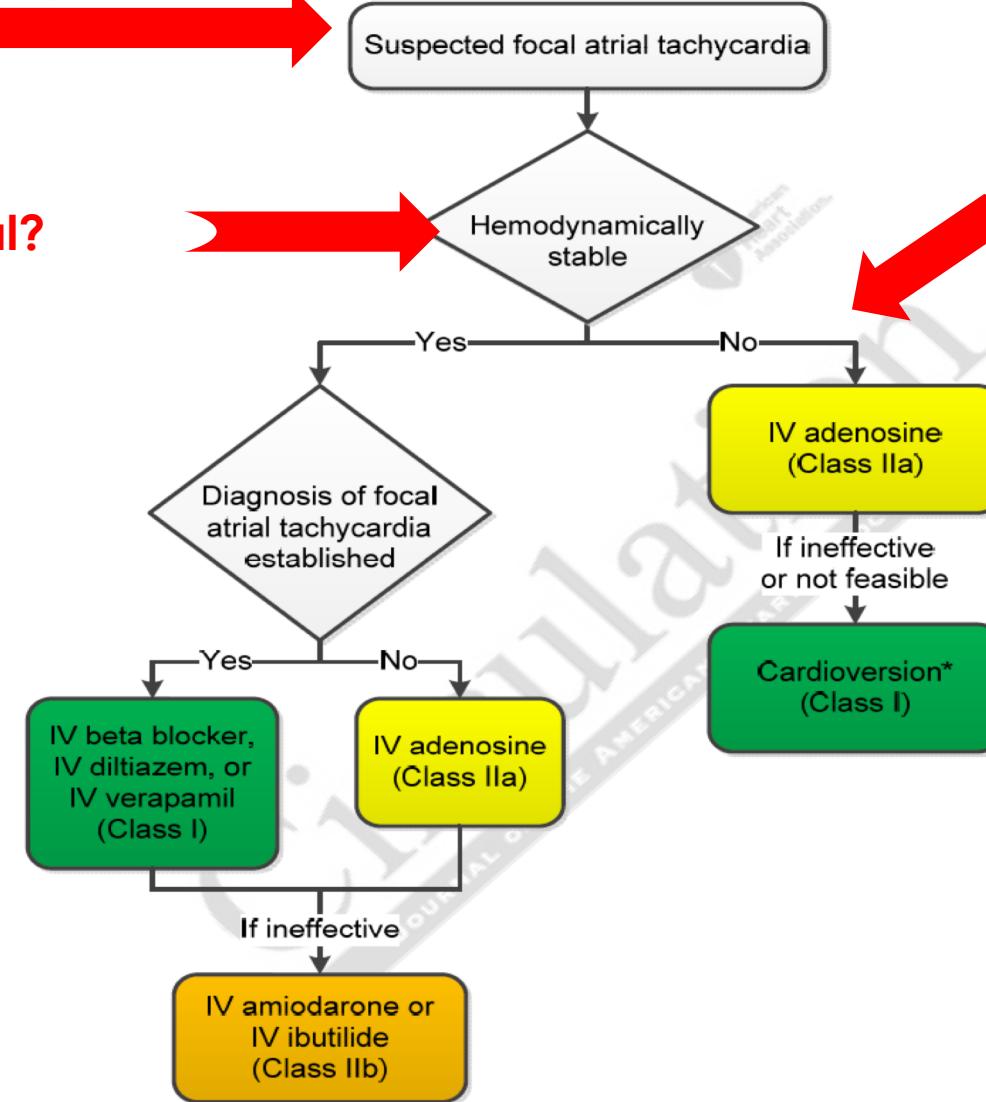
AMER. HEART ASSOC. & AMER. COLLEGE OF CARDIOLOGY – ARRHYTHMIA MANAGEMENT GUIDELINES

Fictitious intermittent cardiac rhythms

Blood Pressure Normal?

Page RL, et al.
2015 ACC/AHA/HRS SVT Guideline

Figure 10. Acute Treatment of Suspected Focal Atrial Tachycardia



If PM monitor was modified

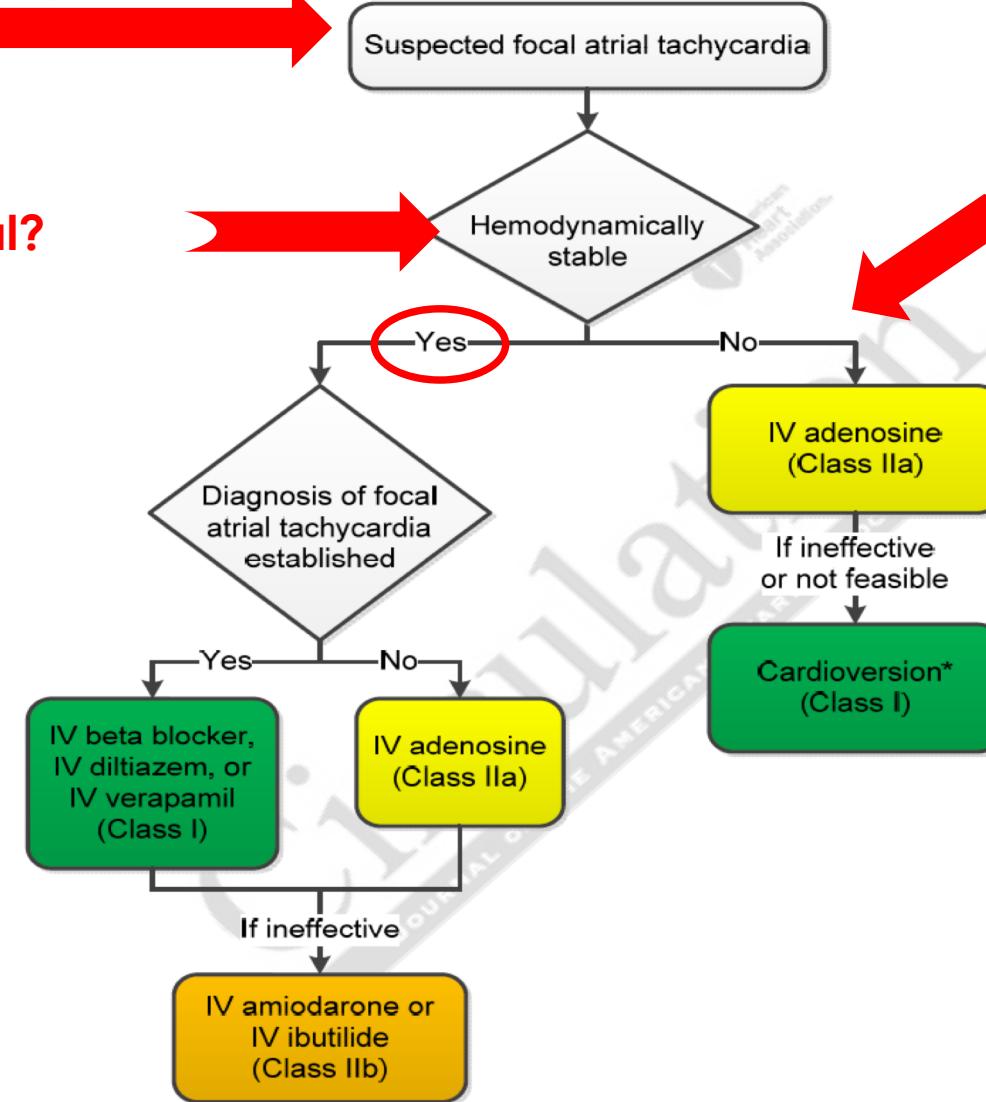
AMER. HEART ASSOC. & AMER. COLLEGE OF CARDIOLOGY – ARRHYTHMIA MANAGEMENT GUIDELINES

Fictitious intermittent cardiac rhythms

Blood Pressure Normal?

Page RL, et al.
2015 ACC/AHA/HRS SVT Guideline

Figure 10. Acute Treatment of Suspected Focal Atrial Tachycardia



If PM monitor was modified

AMER. HEART ASSOC. & AMER. COLLEGE OF CARDIOLOGY – ARRHYTHMIA MANAGEMENT GUIDELINES

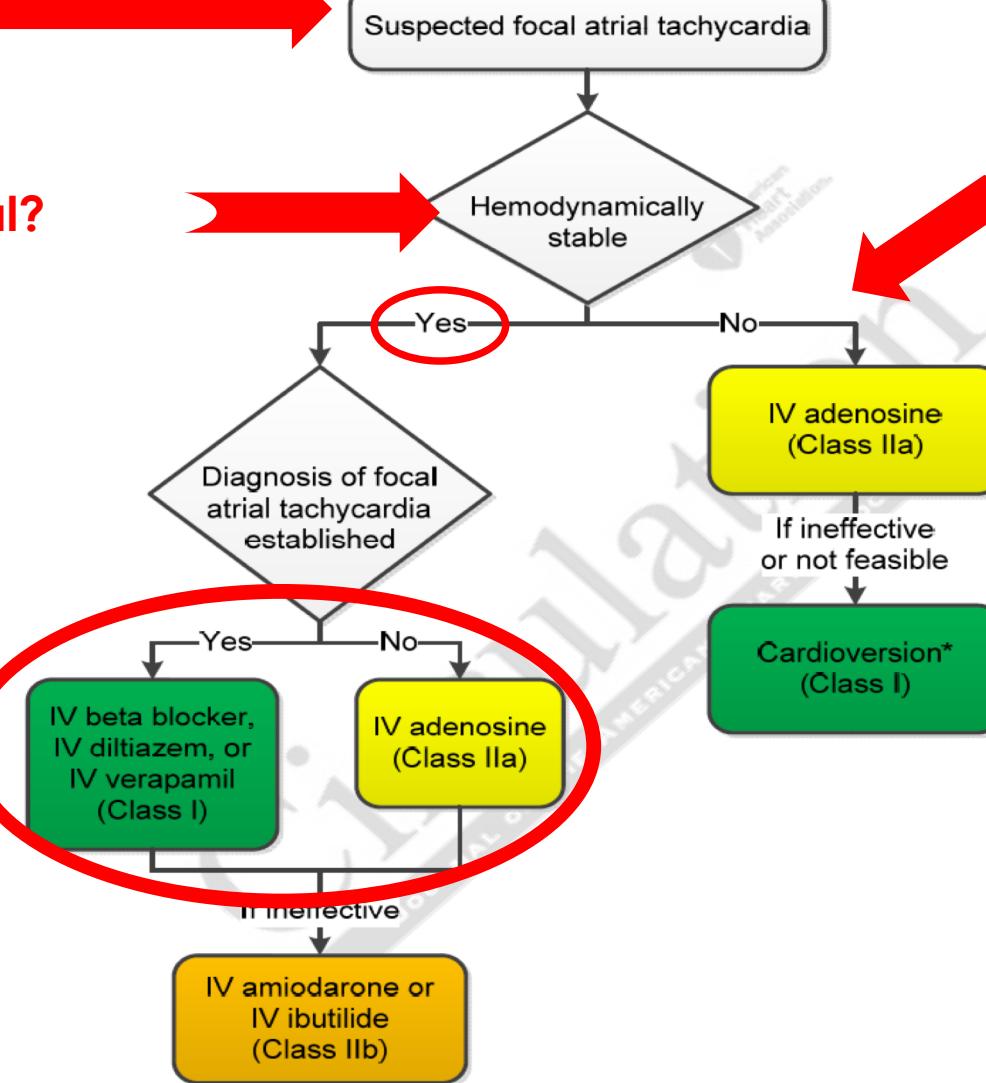
Fictitious intermittent cardiac rhythms

Blood Pressure Normal?

Medications Administered

Page RL, et al.
2015 ACC/AHA/HRS SVT Guideline

Figure 10. Acute Treatment of Suspected Focal Atrial Tachycardia



MITIGATIONS

- ENCRYPTION
- AUTHENTICATION/AUTHORIZATION
- ISOLATION
 - NETWORK ACCESS CONTROLS
 - PHYSICAL ACCESS CONTROL



OTHER CONSIDERATIONS

- ATTACKER WOULD REQUIRE FULL KNOWLEDGE OF ALL ASPECTS OF THE PROTOCOL AND MUST CREATE A FULL CONSISTENT SET OF PARAMETERS TO AVOID DETECTION
- LOCAL MONITOR CONTINUES TO SHOW THE TRUE STATE OF THE PATIENT AND CANNOT BE ALTERED BY THIS ATTACKER
 - MONITORS DO NOT REQUIRE A NETWORK TO FUNCTION PROPERLY

SPECIAL THANKS

- SHAUN NORDECK, MD
- CHARLES MCFARLAND
- McAFFEE PRODUCTION TEAM
- ATR

QUESTIONS?