# SPEAKER SCHEDULE

| Time | Speaker | Title |
|---|---|---|
| **Description** | | |
| 10:15 | Christopher Elisan | **Modern Malware** |
| *I will talk about how malware production has moved on from the traditional manual method to a more efficient automated assembly line method. I will talk about the tools used by the attackers to accomplish this and then do a live demo.* | | |
| 11:30 | Denny Deaton | **Mobile Device Security** |
| *Learn about common threats with mobile devices such as the iPhone, Android and Blackberry. This talk will cover mobile threat modeling, tips and demos for performing mobile security assessments and security best practices for mobile devices.* | | |
| 12:30 | Lunch | |
| On your own | | |
| 1:30 | Doug Burks | **Security Onion: Peeling Back the Layers of Your Network in Minutes** |
| *Security Onion is a Linux distribution for Intrusion Detection and Network Security Monitoring. In just a few minutes, we'll install and configure a distributed server/sensor solution. Attendees will see how quickly and easily they can deploy Security Onion and the power it gives them in defending their own networks.* | | |
| 2:45 | Martin Fisher | **Bringing The Sexy Back To…Defense In Depth** |
| *"Defense In Depth" is considered by most to be a useless marketing trope that vendors used to sell you more boxes with blinky lights that showed you were "serious" about security. Forget that the boxes may or may not do what was advertised, may not provide usable data, or even fail open when they crap the bed.*<br>*Instead we decided to build The Perimeter. Higher walls, bigger locks, more money. That didn't work. The Perimeter Is Dead, Long Live The Perimeter!*<br>*So what do we do now? What amazing boxes with blinky lights do we need to convince our bosses to fund next quarter?*<br>*In this talk I will posit that, more than likely, you actually have (or can easily get) most (if not all) of what you need to create an effective, pragmatic, and resilient security program. I will show that by changing our thinking, our perception of "Fail vs. Win" we can provide real value to our business.* | | |
| 4:00 | Frank J. Hackett | **Why Your IT Bytes** |
| *IT Sec and InfoSec professionals are necessary in this day and age. IT always looks for the quick and dirty fix. They want to keep the end user/manager/C-level happy. InfoSec pros know this isn't the way. So why the difference? It's simple, IT doesn't know. Malware to them is an inconvenience - not a sign of something bigger might be at stake and that's it's a deterrent. IT worries too much about losing their job and not enough about what's really at stake, the data. So how do we educate IT, get help from IT, let IT work for us? First we identify the problems, second we educate, and lastly we implement. Often times many of us don't want to get our hands dirty with IT work. Many of us left it in a world behind and don't want to return. It's time we return to our roots and lift up our computer brethren.* | | |
| 5:15 | Redvers Davies | **I've been hacked, now what?** |
| *I want to give the small/mid size businesses (ie, those without a security department) some basics around how to respond to a hack and more importantly the decisions and preparations they can make before the hack which will make it less painful.* | | |

May 24th, 2013