



Hacker Conferences Come To Bloom In Chicago

<http://www.darkreading.com/sophoslabs-insights/hacker-conferences-come-to-bloom-in-chic/240153826>

April 29, 2013

By David Schwartzberg

Chicago was off the hook with two hacker conferences hosting Bruce Schneier, Josh Corman, Jericho, and many others, including a few first-time presenters.

When it's spring in the Chicagoland area, most of the locals think of rain, flowers, and construction. Thinking about how to further enhance their information security repertoire of tools is deep in the back of most Chicagoans' minds. Last weekend, ethical hackers brought new ideas and discoveries to bloom with their friends and colleagues along with the daffodils.

This marks the fourth year for both THOTCON and BSidesChicago, which are two annual hacker conferences that run in succession of each other. As Nicholas Percoco, senior vice president of SpiderLabs, one of the founders of THOTCON stated, "The attendees at this year's conference ranged from CISOs of major corporations to college students." Including the volunteers and speakers, THOTCON had about 750 people, and BSidesChicago had about 250 people attend.

THOTCON 0x4

Pronounced 'thought-con', the name is derived from the beginning letters of the Chicago area code 3-1-2 ('th'-o'-t') followed by a hexadecimal number notating the anniversary. The attendees and speakers define THOTCON. Impossible to describe with a single word, the THOTCON event is a culmination of the local DEF CON chapter, (ISC)² members, as well as anyone who is a student all the way to a seasoned InfoSec professional hungry for unwritten knowledge. Sophomorically, THOTCON speakers are at risk of receiving drinks from the attendees while presenting to throw them off their presentation.

This year marked the first year THOTCON attendees, known as HACKERS, received an electronic badge. The badges use ZigBee technology to join a network in order to receive messages sent from a broadcasting station or other "special" badges only worn by the co-founders. More information about THOTCON and its founders is available on Wikipedia. The THOTCON challenge this year was based on the board game Clue, and every 30 minutes the badges received a challenge clue.

Opening keynote

This year the keynote began with Bruce Schneier who spoke about "Trust, Security, and Society," which was about how social pressure makes security viable in society. I unfortunately missed Schneier's complete talk because I was volunteering, known as an OPER (short for operator), at THOTCON. Taking an objective approach, I decided to ask a range of speakers and attendees their thoughts about the opening keynote.

Individuals who felt that Schneier's talk was "very interesting with deep psychological points" and "really good" were of the caliber with no security background through less than three years in the security field.

On the other hand, anyone with more than six years in the security field commented that nothing relevant or profound was presented. Supporting that, one of the other keynotes, known by the handle "Jericho" and tweets as @attritionorg (the squirrel people), shared his opinion during the first keynote "Schneier's #thotcon keynote seems like it was written for 10 year olds." I'll leave it at that.

The group of individuals in the range from three to six years of experience in the security field had mixed opinions.

Afternoon keynote

Josh Corman and Jericho took the stage for the afternoon keynote with a talk simply titled "Cyberwar." Anyone who absorbs any form of news media has heard the term cyberwar used in the past. Commonly in reference to some other country attempting to attack another country's Internet-facing computers with the intent to do harm.

Corman and Jericho step through the abuse of the term, the lack of definition by the government, and prove how China is less of a risk than squirrels (dubbed as "squirrelmageddon"). Cyberwar has become such an overused term and improperly assigned to most cyberactivities that Jericho stated it's now become a "thought terminating cliché." Well said.

Their talk had so much great content that it truly requires a dedicated blog article followed with a series of podcasts.

Additional talks

A full list of the speakers, along with their talks, is still available on the THOTCON schedule Web page. A couple of talks that I was able to attend and stood out the most to me were Dr. Philip Polstra's and Ben0xa's (pronounced Ben Ten) presentations. Dr. Phil's talk, titled "Mesh Stalkings," was a technical deep dive into all of the elements of how to build a device using ZigBee. Dr. Phil spoke at GrrCON 2012, where he walked through the build process of an open-source tool he created for penetration testing and

forensics he calls "The Deck." Since then, The Deck has been expanded on to include access to ZigBee mesh networks called "The MeshDeck."

Ben0xa brilliantly executed a TURBO talk called "Creating A Powerful User Defense Against Attackers" that was standing room only. Ben0xa modestly purports to be a newcomer to the security industry. His talk may not have been very technical, but he clearly communicates, with passion, where the breakdown in defense against attackers lies; with your users.

Ben0xa emphatically points out he has proven that no matter how much equipment with blinking lights and software is thrown at a security problem, end-user education is the one layer that will consistently provide the best defense as long as the end-users have the right incentives. Interestingly, the seasoned security veteran and THOTCON keynote Bruce Schneier has a different opinion about security awareness training.

Last, this was my fourth year attending THOTCON but first year as an OPER and as a speaker. I want to state that the co-founders and other OPERs are true professionals invoking the motivation for me to OPER again next year. While I wish I could have completed the technical demo portion of my talk, I want to say "Thank you for the drinks" sent to me during the demo and going forward, please do not awkwardly lick my forehead. A prerecorded video is available of the food hacking demo that was used to warm up the crowd.

When asked about the security community in the Midwest, Percoco commented that "THOTCON represents a great opportunity for local Chicago security enthusiasts to interact and collaborate with local and international members of the global community in a very casual setting." The overall consensus from attendees randomly polled was that THOTCON 0x4 was the best year ever.

BSidesChicago

Operating under the SecureChicago banner and driven by the pure mad desire to bring the security community together into a forum of socializing security information, BSidesChicago didn't have a keynote, but was fortunate enough to have Jericho, Josh Corman, and SpaceRogue attend and take the stage for 30 minutes to field questions from the attendees.

Elizabeth Martin and Michael "Moey" Ortega are the coordinators who orchestrated making BSidesChicago an epic success with a lot of help from volunteers and sponsors.

This year's speaker lineup included many well-known names in the local Midwestern security community, such as, Wolfgang Goerlich, Raphael Mudge, Chris Payne, Kyle Maxwell, and first-time speaker Eve Adams, to name a few. There was a lot of great content that spanned across three tracks including a first time speaker track and hands-on workshop.

Spanning is the unofficial theme for this year's BSidesChicago and BSidesDetroit because they are holding the first-ever joint CTF (Capture The Flag) contest that started in Chicago

and will end in Detroit in June. Several first-time CTF participants partook of the challenge, including myself, to crack encrypted messages, reverse engineer compiled code, forensics, network security, and lock picking in the lock picking village to find the answers to earn points.

When Elizabeth Martin, director of security services from RedLegg, was asked what was relevant and different about BSidesChicago, this was her response: "Chicago has a strong emerging community that is active in many different facets and is growing every day. BSidesChicago is an opportunity for people of varied interests to have conversations, learn from each other, and grow personally and professionally. Every year BSidesChicago has inspired individuals new to the community to become more involved and participate. This is made possible by our show of strong support from our sponsors, our volunteers, and most of all our participants who make this event what it is – a demonstration of what the Chicago security community is all about."

Hopefully the next time you see freshly sprung flora, it reminds you of the Chicago security community coming together to help each other grow.

No security, no privacy. Know security, know privacy.