HOPE 9 – Hotel Pennsylvania
New York City
2012-07-13 – 2012-07-15

Overall Impression:

This was a great HOPE! The theme this time was HOPEland Security. The badge was a passport for Anonymous Hacker. I was a bit disappointed that it wasn't something that we could flesh out with some additional electronic components, but it was well crafted with a bunch of fun things to read inside. There were many opportunities to get it stamped. I didn't come close to getting them all.

The talks (3 concurrent sessions with a 4th additional track) were well run and kept on time this year. This was a big change from The Next HOPE in 2010. There were roughly 100 scheduled talks over the 3 days plus the 4th track as well as workshops and of course the hacker village and lock picking village (just to mention a few). The topics covered ranged from security (which is what too many people think is the only thing hackers do) to mental health. There were old school phone phreaks (Captain Crunch and Cheshire Catalyst), former NSA (William Binney), lawyers (EFF, ACLU, Eben Moglen) and activists (Telecomix) among the speakers. I took in 12 full talks and hit parts of a few others (See talk notes for details).

Personal Impression:

- I fully participated in this HOPE. It was great to leave everything else behind and focus on what the conference had to offer. For me it was a great break.
- Segway – Yes, I rode one of these silly things. They are pretty cool once you grock controlling it: just lean. :)
- Captain Crunch creepily asked me to his hotel room to fix my back. I declined.
- I gave a 4th track talk called 'Disruptive Genomics' to about a dozen people. I got some good questions and had dinner with a guy named Chris. He's a programmer / artist with an art degree from MIT. That was a lot of fun.
- I talked with some of the speakers at random times during the conference. That was pretty interesting.
- Took a Ham radio operators license exam cold. I didn't pass but came close.
- I interacted more with other attendees than I did during previous HOPEs.
- Eben Moglen rocks!

Talk Notes – In order of presentation

2012-07-13 14:00
Keynote: William Binney
Whistle-blower NSA employ with 37 years of Govt. service
Army '65-'69 traffic analysis in Germany. At first thought this was going to be dull and related to streets , stop signs, etc. The Army meant data / systems / code – things that would apply his degree in mathematics.
The Tet offensive in Vietnam had a big impact on him. The intelligence community knew that it was going to happen, but the Military did not believe them. He felt that it was imperative that the intel community get actionable information to the military in a timely fashion in a way that they would understand and believe.

The NSA got big and split into two parts: operations and technical. He worked on the technical side. Operations became about money to keep things going and to get more money. He had to figure out how to get operational support for his technical stuff (automation of analysis in computer code) called Signal Intelligence Automation Research (SIARC). Eventually he took and officers course (COR) that allowed him to get his own operational support. He was so good at his job that Congress gave him (by name) $1.5M that he didn't ask for.

He got 5 countries together to share information freely and had this signed by Congress before they knew what was going on.

SIAR was a multidisciplinary team with good cross communication. They started from scratch because there were many within the organization that liked to saddle people with legacy systems and everything that goes with that. They were therefore free to do what they wanted and how they wanted. They got budget plus from Congress. The project was latent semantic indexing – compare many texts to cluster information.

He was having success with the web (~7/2001) and was told not to brief anyone about it because then it would be clear that it was a solved problem and there would be no reason to get funding to continue the 'military industrial happiness complex'.

The 'military industrial happiness complex' is the system by which elected officials leave office and get big $ jobs in private companies and vice-versa.

Quote I liked: “Miracles don't happen in the computer, they happen in your mind and are penciled out on paper”

9/11 happened. Within weeks the NSA decided to spy on **everyone** using Telecom data (they started asking for those data in 2/2001). This infrastructure was in place in 11/2000. He thought that someone in the government (e.g. House Intelligence Committee) would pull this back into something that followed the constitution. General Hayden (NSA) declared this legal because the White House said so. No documentation was provided by the White House. This surveillance was reauthorized every 45 days.

4 other NSA and 1 HIPSI were also trying to get this program into a legal realm. They all reported this through proper channels. Then the FBI raided all of them.

Note: RDBMS can't deal with Terabytes per second. Their system worked with flat files.

Question: How to look at data but not content and select what to look at in the end.

He was working on an approach to detect medicare and medicaid fraud. This program was stopped by the FBI. He suspects this was because it would have interfered with the military industrial happiness complex. The approach uses graph theory to do these things. The name of the software on the slide is “Graphnavigator lib Beta time line).

2012-07-13 16:00
Hactivism, Tools, and the Arab Spring
Telecomix

These people did a lot of work in Egypt and then Syria
In Egypt, they opened back up the dial up internet lines after the government cut other access to the net. They tried HAM radio, but there were not that many operators in Egypt, and those that were seemed mostly to be military. They did FAX spam where they found as many FAX numbers as possible and sent communication information, medical information, etc. They NMAPed all of Egypt (yes they did) and then spammed website logs with information like the FAX spam. They taught many people how to use TOR, VPNs, etc. They had a Morse code to twitter relay from Egypt to Italy.

They main strategy was to through everything they had at the wall and see if it would stick. Also, "Fail big and fail early."

In Syria the NMAPed 186K ip addresses. They found Bluecoat devices which are made in the USA, but are non-exportable technology by law. They found open FTP sites related to these devices and pulled data from them for months.

Bluecoat devices blocked social networking, chatting websites or anything with instant messaging capabilities.

This group had an impact on the law in the E.U. The E.U. Changed their directives in telecom.

They started a project called BlueCabinet. This is an 'Open Source Intelligence Analysis' which looks for and catalogs censorship technologies and deployments.

They were called "The tech support for the Arab Spring."

2012-07-13 18:00
Why You Shouldn't Write Off Higher Education
John Linwood Griffin

This talk was a sales pitch for grad school. He described a pie-in-the-sky type of graduate experience. Best-case-scenario.

His slide was:

1. You get to do what you love.
2. You get to make large structured contributions to the community.
3. You experience personal growth while surrounded by amazing people.
4. You're part of a meritocracy and a close knit social circle.
5. The door is open for interesting opportunities afterward.

Really, that was it. For 1 hour. WTF! I should have got up and called BS on this, but I didn't.

2012-07-13 20:00
Wikileaks, Whistle-blower and The War on the First Amendment

Ben Weisner ACLU
Catherine Crump ACLU
John ?? ACLU
All attorneys.

This was divided into three sections each of the above did one.

Ben:

There have been no prosecutions for torture. There have been man prosecutions of leaks about torture. There have been many leaks about torture that were not prosecuted because they came from and on behalf of the government.

The Espionage Act was used 3 times until the Obama administration. Now there are 6 indictments. There has been a change in the prosecution of publishers. Previously it was considered a 'no go'. Now there is Wikileaks.

How does one argue that Wikileaks is guilty under the Espionage Act, but not the NY Times, the Guardian or Der Speigle?

1. Publishers of leaked information should never be prosecuted for publishing truthful information.
2. Whistle-blowers on Government waste, fraud and coverup or illegal acts should not be prosecuted.
3. Other leaks of secrets must outweigh the benefit to the people to be prosecuted.
4. Leakers should be able to defend on grounds of selective prosecution.

John:

5th Amendment Stuff
Grand Jury – The Government wants to argue that wikileaks is not like the NY times, but rather is the same as Bradley Manning.

The government may seal the indictment produced by the grand jury. This is often the case in the possibility of flight. It is known that there was a grand jury in relation to Julian Assange. It is not known if they are still empaneled or if there is a secret indictment.

Catherine:
4th Amendment – Search, Seizure and Limits

Ways the executive branch has been accessing our personal data:

Search at international border. Any electronic device can be searched and they can keep the device as long as they want and can keep a copy of the data for "any law enforcement purpose." The case law is David House – Bradley Manning Support Network. There are 1st and 4th amendment arguments here. The decision by the Judge: on 1st amendment grounds: If the government targets the search is upheld and continues up the line. On 4th amendment grounds, allows suspicion less search policy, but is limited in time and commensurate with need.

Twitter subpoenas – court cases decided. See notes on Marcia Hofmann's talk

2012-07-14 10:00
Occupy the Airwaves
Anna Martina & Maggie Abner The Prometheus Project

They are providing online support and tools for applying to the FCC for Low Power FM (LPFM) licenses.

The project has held 12 barn-raising projects so so far. There is a new LPFM window and they expect 100s of new stations.

Prometheus was instrumental in the pushing and passing of the Community Radio Act.

RadioSpark.org – Community powered site to support applicants for LPFM and those who already have LPFM & engineers etc. to support this community.

RFREE – tool to find available channel in your location. Basic version is in beta. Engineering version in the works. The engineering version should have enough information for an engineer to apply for a waiver.

These people are doing cool work. I've been following them since they started. For this talk I asked a question: “The last time the FCC was allocating new licenses for LPFM there was a big land grab. Do you anticipate that this time and what are you doing?” The answer is yes they expect one and they are doing the above things and a lot of communication to help grass roots media groups start stations in their communities.

2012-07-14 11:00
Protecting Your Data From the Cops
Marcia Hofmann – Electronic Frontier Foundation

Legal rights when a device is seized / searched falls under the 4th amendment

1. Is the government physically intruding?
2. Does the person have reasonable expectation of privacy
    1. Does the person subjectively believe that it is private?
3. Does society objectively believe the expectation of privacy is reasonable?

If the above holds, then the police need a warrant under probable cause. If they have a warrant, then you get to read it.

Exceptions to requirement for a warrant:

1. Consent
2. Plain view
3. Automobile
4. Exigent circumstances
5. Brief detention on reasonable suspicion and the search is incident to arrest

Courts are split about searching cell phones.

What can you do?

1. Leave device at home or with a friend.
2. Back up your data
3. Password protect.
4. Encrypt – Full Disk.

Special case – the border: All searches are reasonable there. No suspicion is needed. Check out EFF white paper "Defending Privacy at the US Border"
What to do at the border?

1. Carry as little data as possible.
2. Consider laptop / hard drive with minimal data.
3. Store data in the cloud. (is this really advisable??? maybe if well encrypted)
4. Use strong password / full disk encryption.

Police efforts to get data from 3rd party service providers.

1. 3rd party doctrine – no reasonable expectation of privacy. Data voluntarily disclosed to someone else.
2. But see: U.S. v. Warshak – reasonable expectation of privacy in email stored with providers.
3. Sotomayor's opinion in U.S. V Jones: 'Let's look at the premise here again'.

Federal stored communications actionable
Regulates when law enforcement can get records.

- Content (email) v. non-content (ip address)
- recent v. old content (over 180 days old stored with provider has less protection)
- Providers of 'electronic communication service' v. 'remote computer services'
- State laws can apply too.

Twitter in Wikileaks investigation – did not go well. New York vs. Harris (Occupy Wall St.): Police wanted content, tweets and private content. Court didn't recognize privacy interest of Haris.

See further: eff.org Who-has-your-back. TOR info on 3rd parties and how much they watch out for customers.

What can you do?

- Understand what you are disclosing
- Be selective about your service provider.
- Encrypt before you upload. If you can.
- Keep an eye out for and build technical solutions.

Interactions with law enforcement

- You don't have to answer their questions (generally see below).
- Use the right to an attorney.
- 1 caveat to this *some state* request for identity during a *Terry Stop* (temporary detention). Ask "Am I free to go?" If the answer is no, then it is a *Terry Stop* must the provide ID
- You don't have to help.
- Be polite at all times.

Eff.org – Know your rights.

Bad ideas: don't do these

- Lying
- Interfering with a search

- Destroying / deleting / altering anything to frustrate an investigation.

Compelled disclosure of password / pass phrases.

- Can not be compelled by police. Can be compelled by a judge.
- There is a difference between mind / physical: For example Combination lock (non-physical / mind) and Key (physical).
- Applies to an act with testimonial aspects. e.g. existence, possession, control or authenticity of evidence.
- Can only be invoked to protect you, not another person.
- Protects the innocent as well as the guilty.

Exceptions:

- If they already know, then no privilege
- Immunity – no possibility of incrimination. But, the immunity must be as broad as the privilege.

What can you do?

- Choose strong pass phrases that you can remember.
- Consider the right to remain silent
- Contact a lawyer.

2012-07-14 13:00
Keynote – Yes Men
Andy

The Yes Men started out with the WTO protests. They didn't go, but created a satirical website that looked just like the WTO website. They got invitations, etc. meant for WTO because their website got up to the top of the existing search engines. Their first talk as officials of WTO was at a conference in Austria. They said the most efficient capitalist democracy would be to have "Corporations pay money directly to the citizens for their vote." They pitched that and nothing happened. It wasn't crazy enough for those people to react.

They went to a textiles future meeting – demonstrated a management leisure suite – see youtube for the video. This was absolutely over the top.

Bhopal chemical disaster – They set up a fake Dow Chemical website. Eventually had a press conference with the BBC. Said they would not give money to the people of Bhopal because they were too poor to be shareholders in the company. See further youtube.

At this talk, they announced the Million Meme March for Internet Freedom. The idea is to march on the RNC and DNC meetings this year.

Some audience ideas:

- All their base are belong to us.
- No internet, no cats.
- Should be open source / as open as goat.se
- Fisting & Bumblebees

Look at hash tag Millionmemes

Vermin supreme showed up at this point.

This whole thing devolved into weirdness. Some audience participation. Not sure what the point here was, except for the lulz.

Useful Conference Rule – Announced Occasionally
5:2:1

5 hours of sleep every night.
2 Square meals / day
1 Shower / day.

2012-07-14 19:00
Project Byzantium – An Ad-Hoc Mesh network for the Zombie Apocalypse

The project was designed with two cases in mind:

1. Katrina – massive infrastructure fail.
2. Egypt – Deliberate compromise of network infrastructure.

While it is said that the internet is a decentralized network, this is not strictly true. Addresses are hierarchical, not really decentralized / redundant.

Design Goals

- Cheap
- Commodity hardware
- Rapidly deploy-able
- Extensible
- Robust & reliable
- Secure
- Low maintenance

Constraints

- Solve Katrina 1st , Egypt 2nd
- Must work for small groups of low skilled people (Not just for the HOPE crowd)
- Support all users
- Sufficient tools to accomplish arbitrary tasks
- Minimize collusion
- Not all devices run mesh net software
- Compatible with wide range of communication gear

Ad Hoc Networking

- Almost any device can do it
- No central Access Point required
- Clients communicate via peer-to-peer
- Does not implement multihop
- Good potential for obscurity – think network advertised as “Free Wireless Network”

Mesh Routing – OSI Layer 3

- >70 protocols exist
- Not all have same features / problems
- Some have big flaws

Protocols

- 802:11S – poor choice even though it is the 'standard'
- OCSR – not so good either
- BATMAN – advanced / bact contrl utility required / steep learning curve
- BABEL – this is the one they chose (… config file)

Where to get information / software / support:

- IRC – freenode #byzantium
- Github Byzantium

2012-07-14 20:00
Take a Bite Out of Logs With SAGAN
Champ Clark II

Goal of this project is to write the best log analysis engine. Leverage SNORT (packet analysis engine) Make it multi-threaded so it can keep analyzing and log into database.

Essentially this tool enhances and IDS with information from log files. It presents the information in a clear way such that it is much more useful than the typical log information.

This is a very cool log analysis tool for large scale networks, IDS and NOC environments. Well beyond my needs. Pass this info to James VanEe.

2012-7-15 10:00
Countermeasures Against Ubiquitous Surveillance
Lisa Shay & Greg Conti – Instructors Engineering & Computer Science West Point

1. Network surveillance systems threaten our privacy and way of life.
2. People should protect themselves
3. This community (HOPE) has the knowledge to deflect the trajectory of surveillance in the future.

Instrumented people: track via cell phone
Instrumented home: TVs that watch you.
Instrumented communities: $1B Scientific 'Ghost town'

New applications – emperor penguins counted from space
New applications police – surveillance drones
New power sources – robots / drones – long running time / easy recharge

Minneapolis / Saint Paul Airport $20M HD video surveillance
Increased capabilities – sound hound – What is this song?
Increased capabilities – facial recognition

Increased capabilities – man / machine hybrid (think captchas)
Increased tech – Real time video thru walls – exists now, but low quality
Increased incentives – GPS / Insurance discounts
Old Reasons – Enhance 'your' experience
Coercive Disclosure of identity
Same System Vulnerabilities – systems exploited illegally
"Blue Sky" ideas – Postal trucks as a fleet of sensors

Deconstructing a Surveillance System

- Sensors (passive receive energy from environment) – analog
- Sensors (active emit energy & then measure what comes back) – analog
- Convert analog to digital then store then extract features.
  - Storage is local and hard to get to
  - Network is much more vulnerable
- Access --- Legit and Illegit users.
- Networked systems
  - Easy pass – credit card

Countermeasures

- Technology based – See "Smart Parking Meter" Defcon 17
  - Detect the sensor – understand range and coverage
- How to circumvent – Mythbusters #59
  - Shielding – RFID Wallet, WiFi shielding wallpaper
  - Cloaking – graphene based invisibility cloak.
  - Chatting – deflect radiation
  - Absorbing – absorb radiation
  - Jamming
  - Destroy Sensor
- Deny, Degrade, Defeat processing
  - Spoofing – inflatable weapons (tanks etc.)
  - Camo http://cudazzle.com
  - Degrade information quality
  - Overcome processing (e.g. everyone go to trial – crash the justice system)
  - Secure data in transit and at rest
  - Destroy data – overflow or corrupt storage
  - Avoid generating data – neo-luddite / 19th century / 20th century
- Communications Command and Controlling
  - Take control
    - Turn off cameras
    - Privacy settings online
    - Be careful these could provide an illusion of control
  - Denial of Service – human communication channel
    - e.g. Reverse Robocall
  - Understand the actors
    - Owners – vested interest in getting data
    - Enablers / providers – corporate people $ incentive

        - Information customer – who, why, what
        - Regulators
        - Targets – often us

Can compromises be made where owners, users and enablers get the benefit they want and the targets can retain the privacy they want?

What to do?

- Influence the regulators – VOTE
- Educate the regulators and other targets / owners / etc.
- Look at history for examples
    - Culture Jamming
    - Rally support – e.g. SOPA Internet Blackout Day
    - 'Cry Foul' loudly when things deserve it
- Communicate the issues effectively
    - Context matters here – who is the audience?
    - Art is powerful
    - Science fiction – See further Eben Moglen's talk
    - Highlight cost/benefit analysis (effectiveness / health risks, etc.)
    - Transparency & Disclosure
    - Conduct & share (admissible in court) research don't forget executive summary
    - Take it to Congress
    - Take it to the Courts
    - Take it to the White House
- Sometime more extreme measures (not recommended)
    - Non violent civil disobedience
    - Hactivism
    - Pirate Party
    - Etc.
- Support EFF / EPIC
- Common Sense
    - See Slashdot Article communities against terrorism
    - Panopticlick – EFF

2012-07-15 11:00
Hackers and Media Hype – Big Hacks That Never Really Happened.
Space Rogue – formerly of L0pht Heavy Industries

Intro:

- What is media hype
- Examples
- How to ID hype
- How to be part of REALITY

Media – defined here as any means of communication that reaches / influences people widely.
Hype – defined here as intensify by ingenious use of media.

Examples:

Mitnick & NORAD

- Articles claimed that he could whistle over the phone and launch missiles
- Articles claimed that Mitnick had infiltrated NORAD
  - Also that this inspired the movie War Games
  - He never infiltrated NORAD and in fact, War Games inspired him
- Reality – this rumor was started by a prosecutor in a court case against Mitnick.

Satellite held for ransom 1999

- No named sources for an article by Reuters
  - He comments repeatedly about the unreliability of articles without named sources.
- There were retractions published, but they are very hard to find.
- This showed up again in a PC Magazine article in 2008

Al Qaeda uses Stenography

- Hype: USA today 2001, Wired 2001
- Reality Center for Information Technology Int. and New Scientist article 9/25/2001 reported that this never happened.
- Hype Again: Zeit online 2012 – same untrue claim was made

Brazilian Power Blackout

- Hype saying that hackers did this
  - Wired 10/28/2009
  - 60 Minutes 11/8/2009
- Reality Wired 11/9/2009
  - The cause was actually bad insulators, not hackers.

Twitter or: Hackers Shot a photo of my Weiner

- Congressman Weiner said that hackers sent a picture of his weiner to a college co-ed.
  - NBC4 5/30/2011
  - Reuters 5/31/2011
  - Huffington Post 5/31/2011
- Reality – He did it himself
  - ABC News 6/6/2011

Satellite Hack 2010

- Hype – OMG Chinese hackers caused a satellite to be off position
  - Business Week 10/27/2011
- Reality – nothing really happened
  - NASA Watch (blog post) 10/31/2011
  - Reuters 10/31/2011 – China Denies Hacking Satellite.

Illinois water utility – pump failed

- Hype – we don't know what happened, there was a login from Russia, it must have been hackers
  - The Register

    - Wired
    - Krebs on Security
- Reality – a pump just failed
    - Remote login from Russia was done by a former contractor. Why did he still have access?
    - Published 11/25/2011

Northwest Rail Company

- Hype – there was a hacking attack on the rail infrastructure
    - Nextgov.com TSA Memo 1/23/2012
- Reality – there was no targeted attack
    - Wired magazine

US Hacks Al-Qaeda

- ABC News – US hacked website in Yemen.
- *Right...* big hack...

2012-07-15 13:00
How to Retrofit the 1st Law of Robotics
Eben Moglen

Eben Moglen is one of my favorite lawyers. He was the attorney for the Free Software Foundation (FSF) before and during the drafting of GPL 3. He is the founder of the Software Freedom Law Center and teaches law at Columbia University Law School. I have a personal bias here. I really like the way he thinks and how he gives speeches. It was impossible to take notes during this talk. I have ordered the audio for the whole conference. He did not use PowerPoint, so the audio will be enough.

Even though this was not billed as a keynote talk, it was for me and I suspect many others. This was the only talk that I saw at HOPE 9 where the speaker was given a standing ovation. It was powerful!