

Hot Topics, Current Events, and Random Observations

HTCIA New England
Chapter meeting August 9th, 2007

Bob Mahoney
bob@zanshinsecurity.com



A quick tour of some current issues and events, with the occasional observation thrown in.

Also available from <http://zanshinsecurity.com>

My Background

- Network Manager, Plymouth State College
- Sr. Network Engineer, MIT Net Ops Group
- Founder and Team Leader, Network Security
- 4 years as IETF working group co-chair
- Member of technical study group, advising the NIAC's "Internet Hardening Working Group"
- Member of several security organizations

technology
changes,
humans
don't.



Cartoon by Hugh Macleod, from <http://gapingvoid.com> (Which is an interesting blog to follow if you are interested in online innovation, communications, marketing or business.)

Used under the terms of the Creative Commons "Attribution-NoDerivs-NonCommercial 1.0" license.

[meta] I worry sometimes that it is easy for us to become distracted by the technology, and we can easily forget along the way what we know about people and their behavior.

Phishing

Phishing email reports are up 35%

Number of URLs used is up 250%

From Anti-Phishing WG data

NOTE: The Phishing/Malware data here is nearly a year old, in the interesting of revealing truth in spite of specific inaccuracies. :-)

Phishing & Malware

Over the previous year:

172% increase in malware variants

324% increase in urls used

There are over 200 new variants of ride-along malware each month

From Anti-Phishing WG data

Us vs. Them

Malware variants increased by 28X

Phishing urls increased by 35X

Defender's work factor is cumulative

Attacker's work factor is the cost of a new variant

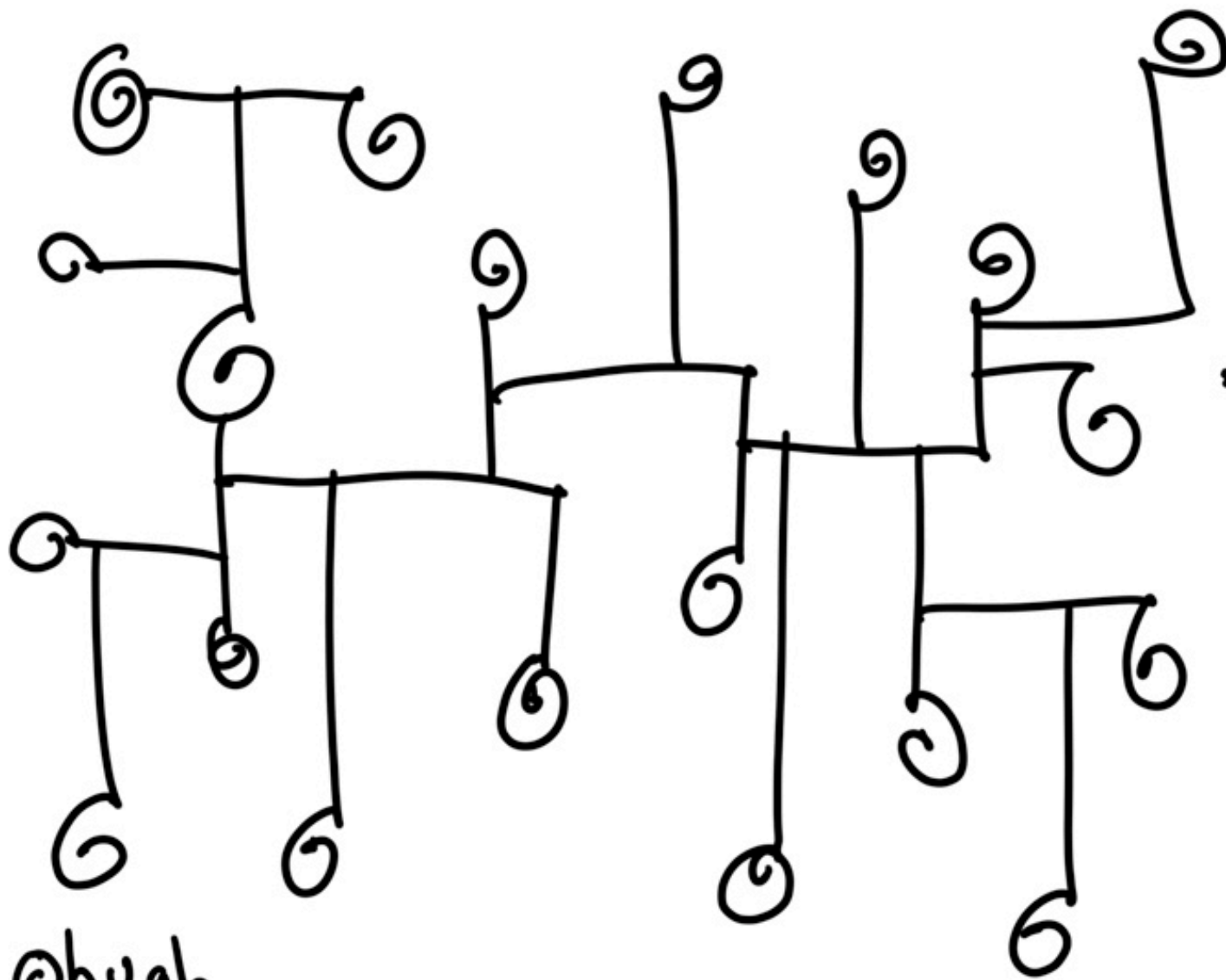
We (defenders) need to work harder as the number of attacks increases.

They (attackers) need to work only hard enough to make the next variant.

“As [creating new variants] is now automated, the arms race between attacker and defender can be manipulated by the attacker to bankrupt the defender.”

Social Web

Implications for Investigations and forensics



the network
is more
powerful
than the
node etc.

©hugh

Cartoon by Hugh Macleod, from <http://gapingvoid.com>
Used under the terms of the Creative Commons "Attribution-NoDerivs-NonCommercial 1.0" license.

Some Terms

- Open Source Intelligence
- Anonymous and Pseudonymous channels
- Invisible Web/Deep Web
- Social Networking
- Wikis
- Blogs, podcasts, etc...
- RSS Feeds and Aggregators
- Tags and Metadata
- Authority
- Stability

<http://en.wikipedia.org/wiki/Metadata>

“The simplest definition of **metadata** is that it is [data](#) about data - more specifically information (data) about a particular content (data).”

Social Bookmarking In Plain English

August, 2007

An Excellent, short video, much better than having me try and describe things...

(PDF users: <http://www.commoncraft.com/show>)

Video courtesy of [The CommonCraft Show | Common Craft - Video Production and Consulting](#)
Used under the terms of the Creative Commons "Attribution-NonCommercial-NoDerivs 3.0 Unported"
license.

Open Source Intelligence



Consider:

<http://flickr.com/search/?q=accident&d=taken-20070214-20070216&z=t>

These are all the pictures on **flickr** matching on the word "**accident**", in tags and descriptions, AND that were taken between 02/14/2007 and 02/16/2007.

People take pictures of accidents regularly, and may not even know they have taken a picture of something interesting to you, too.

(Fleeing suspect, car involved is later known to have been in a crash... maybe you are lucky and catch a plate number?)

<http://www.flickr.com/search/?q=accident&d=taken-20070214-20070216&z=t>

These are all the pictures on flickr matching on the word "accident", in tags and descriptions, AND that were taken between 02/14/2007 and 02/16/2007.

- 1) Data point: just before 9:00 on Friday, 2/16, there were 136 hits.
- 2) As I send today (February), same search is yields 251 hits. (People may wait to upload)

I can at least imagine possibilities... People take pictures of accidents regularly, and may not even know they have taken a picture of something interesting to you, too. (Fleeing suspect, car involved is later known to have been in a crash... maybe you are lucky and catch a plate number?)

A question: I'm sure you know the procedure and contact method to get info from ISPs, etc. Given the "uploaded from a camera phone" possibility, getting user info quickly might be useful in emergencies, where suspect X's phone can be known to have been in a particular place when it took the picture of interest.

Exif via flickr:

Camera: [Canon PowerShot S40](#)

Exposure: 0.002 sec (1/500)

Aperture: f/2.8

Focal Length: 7.1 mm

Exposure Bias: 0/3 EV

Flash: Flash did not fire, auto mode

Orientation: Horizontal (normal)

X-Resolution: 72 dpi

Y-Resolution: 72 dpi

Software: QuickTime 7.1.6

Date and Time: 2007:07:05 15:17:40

Host Computer: Mac OS X 10.4.9

YCbCr Positioning: Centered

Date and Time (Original):

2007:07:03 18:08:57

Date and Time (Digitized):

2007:07:03 18:08:57

Shutter Speed: 287/32

Maximum Lens Aperture:

194698/65536

Metering Mode: Pattern

Color Space: sRGB

Sensing Method:

One-chip colour area sensor

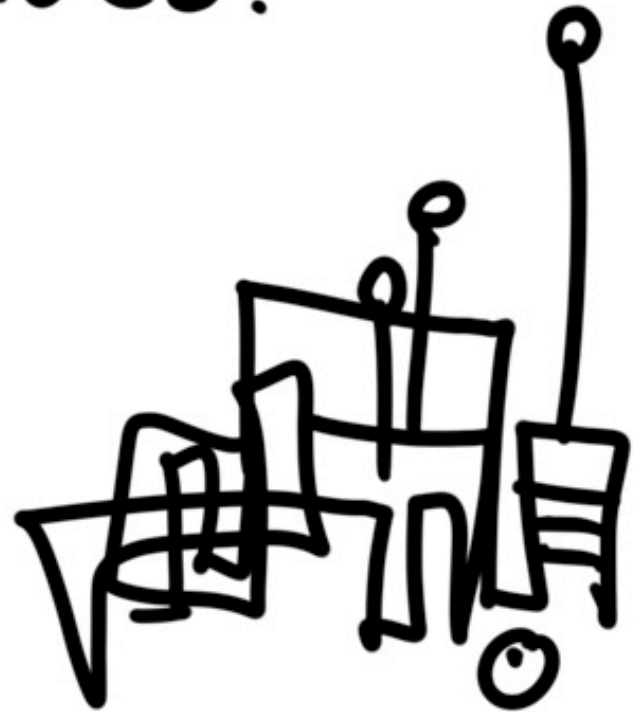
Compression: JPEG



Picture by Bob

it's not what
the software does.
it's what the
user does.

@hugh



Sources for Sources

- Google, Clusty, etc.
- Technorati
- Del.icio.us
- iTunes Podcast Directory
- Feedburner
- Podcast.net
- Podcastalley.com
- Yahoo Podcasts
- Podcastdirectory.com
- Wikipedia.com

Mashups











If there is some information you *wish* you had, like a way to map some data you have, try looking for someone who has already solved the problem with open sources.

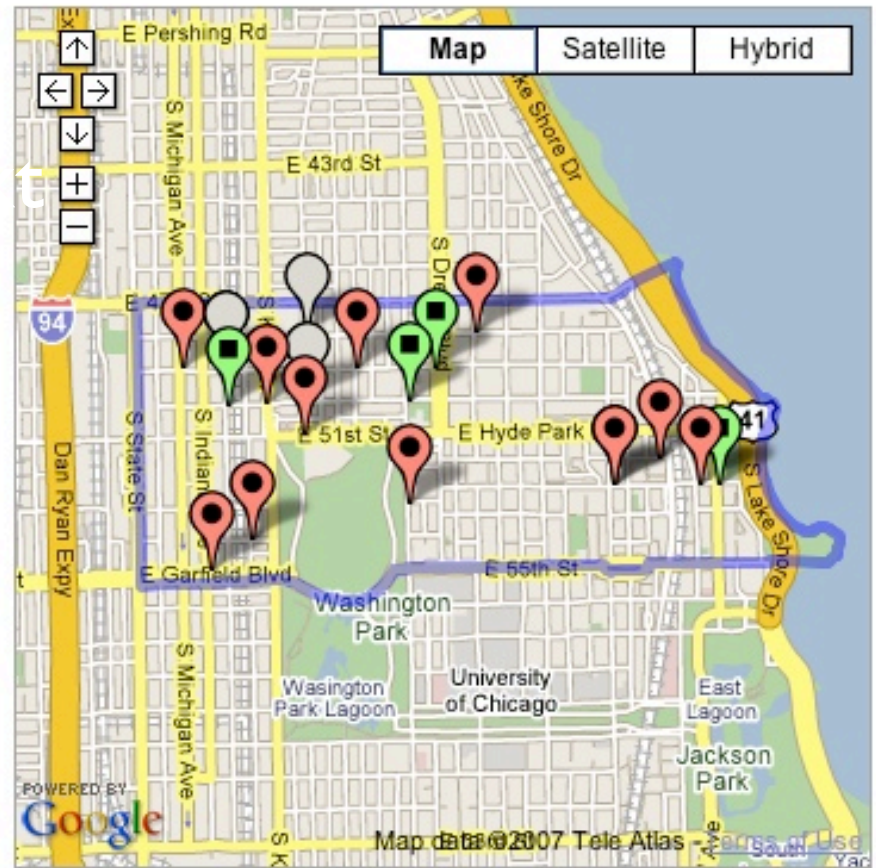
Note: <http://programmableweb.com> lets you search for mashups

Browse by: [Crime type](#) · [Street](#) · [Date](#) · [Police district](#) · [ZIP code](#) · [Ward](#) · [Location](#) · [Route](#) · [City map](#)

Crimes by ZIP code / 60615

Latest reported crimes

-  **JULY 29** [Theft](#)
10:45 p.m. 5000 block S. Cottage Grove Ave. [Restaurant](#)
-  **JULY 29** [Battery](#)
9:25 p.m. 4900 block S. Champlain Ave. [Apartment](#)
-  **JULY 29** [Battery](#)
8:50 p.m. 4900 block S. Prairie Ave. [School grounds \(public\)](#)
-  **JULY 29** [Battery](#)
8:09 p.m. 4800 block S. Ellis Ave. [Street](#)
-  **JULY 29** [Non-criminal](#)
8 p.m. 4900 block S. Prairie Ave. [Other](#)
-  **JULY 29** [Criminal trespass](#)
6:30 p.m. 4900 block S. Drexel Blvd. [Street](#)
-  **JULY 29** [Non-criminal](#)
11:35 a.m. 500 block E. 50th St. [Residence](#)
-  **JULY 29** [Theft](#)
10 a.m. 5300 block S. Hyde Park Blvd. [Street](#)
-  **JULY 29** [Battery](#)
5:26 a.m. 500 block E. 51st St. [Hospital building/grounds](#)
-  **JULY 29** [Battery](#)
4 a.m. 5300 block S. Cornell Ave. [Sidewalk](#)

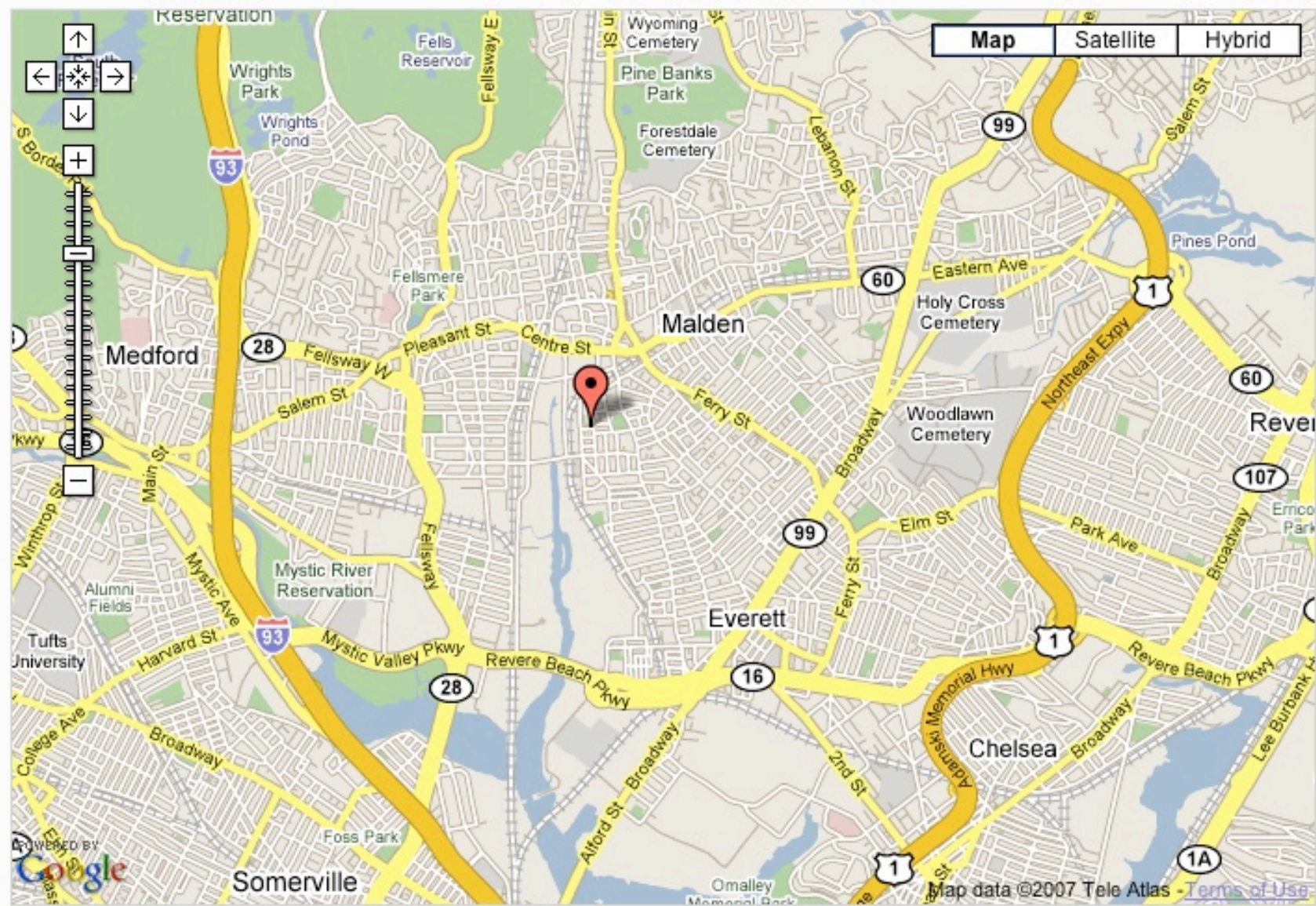


NPA-NXX Geolocator

USA/Canada phone prefix location lookup tool

Ads by Google [NPA NXX Map](#) [NPA](#) [Lookup NPA](#) [Phone Number](#) [Pay Phone](#)

(781) 396 -XXXX



“Knowing Early”

You *know* there will be a security problem announced by Microsoft with the name “MS08-001 vulnerability”... so:

- Set a google news alert for that string.
- Track likely tags ("MS08") at places like del.icio.us
- Do the same for *any* specific information you might want, or which might have special meaning

Don't Forget HUMINT

Let your human social network (online or not)
know what you're interested in, and why.

Online Information: Authenticity, Accuracy, and Integrity

“Candy from Strangers?”

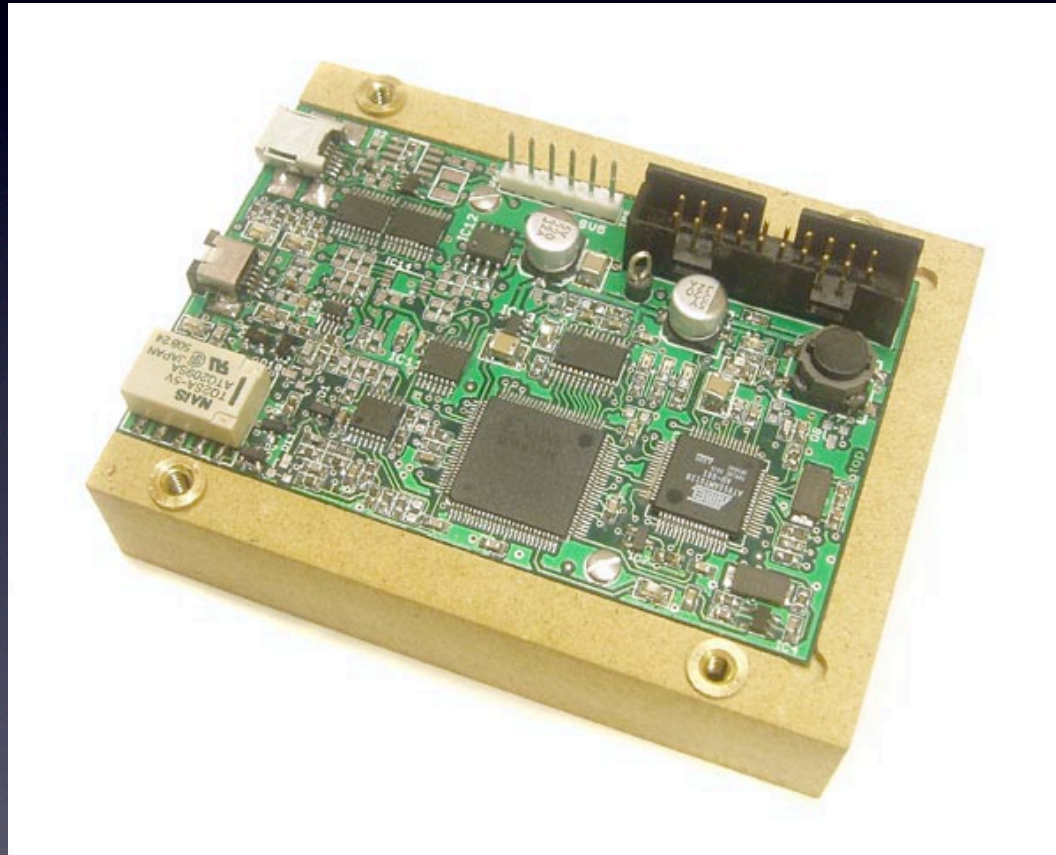
Presentation at the RSA show last winter, slides available at:
http://zanshinsecurity.com/archive/CONS-108_CFS07.ppt

- *Candy from Strangers* tag: CFS07
- <http://del.icio.us/tag/cfs07>

Other High Tech Crimes

Prox card cloning

“A Test Instrument for HF/LF RFID”



This device can do almost anything involving almost any kind of low-(~125 kHz) or high-(~13.56 MHz) frequency RFID tag. It can act as a reader. It can eavesdrop on a transaction between another reader and a tag. It can analyze the signal received over the air more closely, for example to perform an attack in which we derive information from the tag's instantaneous power consumption. It can pretend to be a tag itself. It is also capable of some less obviously useful operations that might come in handy for development work.

<http://cq.cx/proxmark3.pl>

Acoustic keystroke monitoring

Berger, Wool, Yeredor (2006)

- Dictionary attack
- Recovers 7-13 character words from recordings
- Only 5 seconds needed, 20 seconds to process
- **90%** success rate in top 50 candidates

Digital Forensic 'Tricorder'?



The NIJ grant proposal we submitted (along with SAIC) was for a "portable forensics knowledge base".

We had for training models and setting up a info-sharing wiki for NEMLEC.

A single proof-of-concept device could be put together for not too much, and I think the full project could be attempted for a fraction of the original project estimate, mostly because some key work has since been done and is now freely-available.

Some questions

A growing forensics wiki exists now:

<http://www.forensicswiki.org/>

which could easily serve as a starter database.

Is the local judicial/prosecutorial environment friendly to open source tools?

What would a realistic deployment look like?

Resources & Links

ZanshinSecurity's del.icio.us tags

[apple](#) [article](#) [blog](#) [blogs](#) [certification](#) [cfs07](#)
[CISSP](#) [exploit](#) [forensics](#) [government](#) [guide](#) [hack](#)
[hacking](#) [howto](#) [internet](#) [mac](#) [malware](#)
[network](#) [news](#) [osx](#) [privacy](#) [reference](#)
[research](#) [resources](#) [security](#) [software](#)
[tools](#) [web](#)

Thank you!

More info and cool links:

<http://del.icio.us/zanshinsecurity>

<http://zanshinsecurity.com>

Bob Mahoney
bob@zanshinsecurity.com



Released under Creative Commons license *"Attribution-NonCommercial-NoDerivs 3.0 Unported"*

You are free to copy, distribute and transmit the work for Noncommercial use, with attribution. You may not alter, transform, or build upon this work.

<http://creativecommons.org/licenses/by-nc-nd/3.0/>