WIRED BLOG NETWORK

THREAT LEVEL — PRIVACY, SECURITY, POLITICS AND CRIME ONLINE

Top Stories ▾ GO

« Bush to Give Senate Panel Some Domestic Spying Docs, But Will It Sway Anti-Immunity Lawmakers? | Main | Nation's Spies Got $43.5 Billion in 2007, Gov Says »

# AT&T Invents Programming Language for Mass Surveillance

By Ryan Singel ✉   October 29, 2007 | 5:58:18 PM   Categories: Surveillance

From the company that brought you the C programming language comes Hancock, a C variant developed by AT&T researchers to mine gigabytes of the company's telephone and internet records for surveillance purposes.

An AT&T research paper published in 2001 and unearthed today by Andrew Appel at Freedom to Tinker shows how the phone company uses Hancock-coded software to crunch through tens of millions of long distance phone records a night to draw up what AT&T calls "communities of interest" -- i.e., calling circles that show who is talking to whom.

The system was built in the late 1990s to develop marketing leads, and as a security tool to see if new customers called the same numbers as previously cut-off fraudsters -- something the paper refers to as "guilt by association."

But it's of interest to THREAT LEVEL because of recent revelations that the FBI has been requesting "communities of interest" records from phone companies under the USA PATRIOT Act without a warrant. Where the bureau got the idea that phone companies collect such data has, until now, been a mystery.
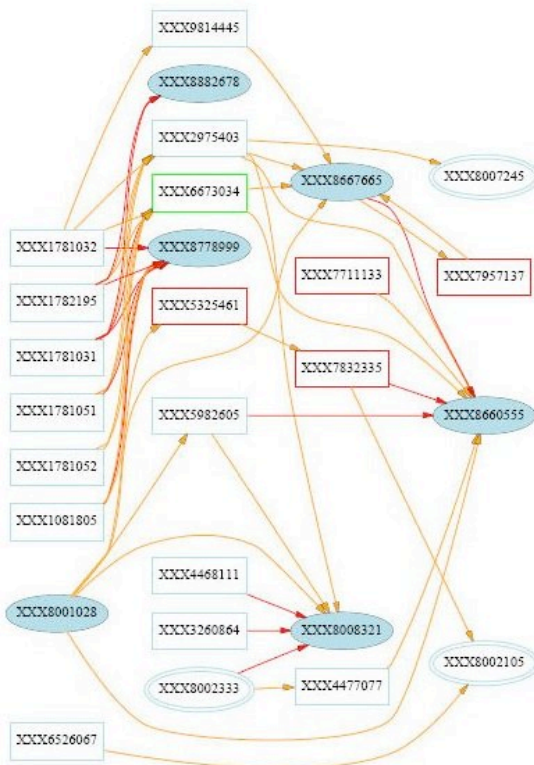
According to a letter from Verizon to a congressional committee earlier this month, the FBI has been asking Verizon for "community of interest" records on some of its customers out to two generations -- i.e., not just the people that communicated with an FBI target, but also those who talked to people who talked to an FBI target. Verizon, though, doesn't create those records and couldn't comply. Now it appears that AT&T invented the concept and the technology. It even owns a patent on some of its data mining methods, issued to two of Hancock's creators in 2002.

Programs written in Hancock work by analyzing data as it flows into a data warehouse. That differentiates the language from traditional data-mining applications which tend to look for patterns in static databases. A 2004 paper published in *ACM Transactions on Programming Languages and Systems* shows how Hancock code can sift calling card records, long distance calls, IP addresses and internet traffic dumps, and even track the physical movements of mobile phone customers as their signal moves from cell site to cell site.

With Hancock, "analysts could store sufficiently precise information to enable new applications previously thought to be infeasible," the program authors wrote. AT&T uses Hancock code to sift 9 GB of telephone traffic data a night, according to the paper.

The good news for budding data miners is that Hancock's source code and binaries (now up to version 2.0)

TEAM

Ryan Singel | e-mail
Kevin Poulsen | e-mail | IM
Sarah Lai Stirland | e-mail
Kim Zetter | e-mail
David Kravets | e-mail

MOST RECENT ENTRIES

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5	6

October 2007

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Nation's Spies Got $43.5 Billion in 2007, Gov Says

AT&T Invents Programming Language for Mass Surveillance

Bush to Give Senate Panel Some Domestic Spying Docs, But Will It Sway Anti-Immunity Lawmakers?

New Oink Not Likely Hog Heaven

Bush Administration Might Weigh in on Yahoo Human Rights Case

are available free to noncommercial users from an AT&T Research website.

The instruction manual (.pdf) is also free, and old-timers will appreciate its spare Kernighan & Ritchie style. The manual even includes a few sample programs in the style of K&R's Hello World, but coded specifically to handle data collected by AT&T's phone and internet switches. This one reads in a dump of internet headers, computes what IP addresses were visited, makes a record and prints them out, in less than 40 lines of code.

```
#include "ipRec.hh"
#include "ihash.h"

hash_table *ofInterest;

int inSet (ipPacket_t * p)
{
  if (hash_get (ofInterest, p->source.hash_value) == 1)
    return 1;
  if (hash_get (ofInterest, p->dest.hash_value) == 1)
    return 1;
  return 0;
}
void sig_main (ipAddr_s addrs < 1:>,
{
  /* code to set up hash table */
  ofInterest = hash_empty ();
  iterate
    (over addrs) {
    event (ipAddr_t * addr) {
      if (hash_insert (ofInterest, addr->hash_value, 1) < 0)
    }
  }
  /* code to select packets */
  iterate
    (over packets
     filteredby inSet)
  {
    event (ipPacket_t * p)
    {
      printPacketInfo (p);
    }
  };
}
```

Another sample program included in the manual shows how a Hancock program could create historical maps of a person's travels by recording nightly what cell phone towers a person's phone had used or pinged throughout a day.

AT&T is currently defending itself in federal court from allegations that it installed, on behalf of the NSA, secret internet spying rooms in its domestic internet switching facilities. AT&T and Verizon are also accused of giving the NSA access to billions of Americans' phone records, in order to data-mine them to spot suspected terrorists, and presumably to identify targets for warrantless wiretapping.

See Also:

- Legally Questionable FBI Requests for Calling Circle Info More Prevalent Than Previously Known
- Senator Denies AT&T, Verizon Cash Bought Spying Immunity Vote
- Telco Immunity Foes Get Boost as Dem Presidential Contenders Voice ...
- Telcos Respond to Spying Questions; AT&T Says Blame the Government
- Qwest CEO Not Alone in Alleging NSA Started Domestic Phone Record Data Mining 7 Months Before 9/11

(Image: A "guilt by association plot" from the AT&T research paper *Communities of Interest*.)

Reddit It | Digg This | Add to del.icio.us

awesome coverage, as usual.

for all intensive purposes...

"In an unusual ceremony today on the west lawn of the White House, President Bush officially named the telecommunication corporation AT&T the Federal Department of Private Communication Signals.

This new department, tasked with both providing communication technology to American citizens AND monitoring the communications of those same American citizens without their knowledge or consent, was given a broad cloak of immunity from angry customers when President Bush declared that all of it's activities were protected by National Security and Executive Priveledge.
In brief comments to reporters afterword, AT&T's chairman and CEO said, "It's great to be in such a unique position. We're not sure if were a corporate entity, or part of the government. We're still discussing what name should appear on our billing statements."

sorry, a joke. ha ha, funny.

if AT&T is using this software to help the u.s. government spy on us, than this is what corporatism looks like. there couldn't be a clearer example on planet earth.

Posted by: | Oct 29, 2007 5:02:24 PM

Regarding exemplars of corporatism on planet earth, gazprom's intertwining itself with the Kremlin comes to mind...
Back to the subject of data mining, there's a fallacy that terrorists can be discovered using the same methods as those used to catch fraudsters and other criminals: that terrorists can assumed to be social "deviants" that differ from other data-mining targets only in irrelevant, subjective, and qualitative aspects. Social network analysis is fine for some purposes, and particularly when the subjects' aren't actively trying to hide their associations. But while the re-emergence of a fraudster can be deduced from looking at hop centrality and 2nd generation analyses, these techniques would likely be less effective in the GWOT.
Various tradecraft practices would be used to obfuscate associations, cutouts could be used to conceal the actual communicating parties, not all of the networks' traffic might be visible (giving woefully incomplete data), etc, etc.
This seems to me like a "quick-fix" technological solution that was available to the intelligence community as a Commerical Off The Shelf solution, when they had the horsepower but not the brainpower to do a proper analysis on the voluminous amounts of civilian traffic in mant languages, quite a different task than during the Cold War...

Posted by: SPD | Oct 29, 2007 6:43:23 PM

Doh, I (obviously?) meant "many languages."

Posted by: SPD | Oct 29, 2007 6:45:14 PM

While much is being spoken about the government's actions of surveillance on its citizens, not nearly enough is being done to monitor and investigate them ourselves.
I love visual representations that help draw the line between A, B, and corrupt fuck C.
Heres a vid about facebook:
http://www.youtube.com/v/OwnTWZ1-UWY
A nice chart is included that draws the lines between the gov, corp ventures, and facebook in a plain and direct fashion.
http://www.visualcomplexity.com/
All sorts of examples and software on plotting out networks or various data sets in visual form. Amongst the plethora of content is a few listed below.
Skyrails, shows out graphs can be dead sexy:
http://cgi.cse.unsw.edu.au/~wyos/skyrails/index.php
http://www.youtube.com/watch?v=I2d312_dXEs
Piespy, social network bot, maps out relationships between people on IRC:
http://www.jibble.org/piespy/
Myspace friends charter, just for a nice example of a social network:
http://www.lococitato.com/myspacefriends/myspacefriends.html
I'm convinced we need to dig deep. Since a large share of our representatives do little to protect us, we must connect the dots.

Posted by: bt | Oct 29, 2007 7:59:39 PM

Great comments on this...
"...this is what corporatism looks like."
Corporatism is often used as a euphamism for fascism. It seems that barring something extraordinary things are just going to continue in this manner until it will become ridiculous to look at the slogans on our money and monuments, "Liberty.." Yeah, right.

Posted by: m | Oct 29, 2007 8:08:05 PM

So, what's the problem with a little data mining? Since the telco owns the call records, and you don't, they can mine all the data they want, and give it to whomever they want. If you don't want the telco to know you are calling hookers, or pushers, then don't call them.
It's not called the Public Switched Telephone Network for nothing!
bb

Posted by: bb | Oct 29, 2007 9:07:42 PM

If Ghadi was president. If this administration, amongst others, was not rank with corruption. If the military industrial complex did not dictate our foreign and domestic policy.
If all those things manage to freakishly happen, I doubt there would be as much outcry as there has been. The extent that the tools dig into our existence is only really about 20% of the issue in my eyes, the other

80% is the people using those tool.

Posted by: bt | Oct 29, 2007 9:48:36 PM

"could create historical maps of a person's travels by recording nightly what cell phone towers a person's phone had used or pinged throughout a day."
The list of everyone participating in the war protests yesterday have been compiled and filtered.

Posted by: anon23 | Oct 29, 2007 9:57:08 PM

Anyone who imagines that the Secret Police agencies are always saintly must have been on some other planet or imagine that somehow American secret agencies won't behave as all other secret police agencies always have. Secret police agencies always are tempted to harass, steal, rape, libel, slander, blackmail, maim, and murder. Their targets are always any vulnerable persons, in addition to those they consider political opposition and those they hope to blackmail.
Since I became politically active in opposition to the war in Iraq, the spooks have stolen large quantities of clothing, put caustic substances in my soaps and shampoos and on my water bottles, run into the side of my van, cut a bolt half way on my car so that I narrowly escaped death, turned the lights on in my car numerous times, stolen books, stolen bras, tee-shirts, and jackets, damaged many pieces of electronic equipment, pushed so hard on my front door trying to get in while I was in the shower that they splintered the tops and bottoms off my dining room chairs that I had under the door knob, attempted to enter a motel room with an electronic card while I was in the restroom (but I had furniture pushed up against the door), shut off my cell phone remotely numerous times, censored my e-mail, and committed many other serious crimes with the aid of electronic surveillance equipment.
No logical person would think I was a threat to the security of the US. Some high ranking person (or persons) with secret police powers is (or are) mad. There is no greater threat to the United States than unchecked secret police with electronic surveillance powers and the keys to everything. It must be stopped and those involved must be removed from power and held accountable.

Posted by: spiedupon | Oct 29, 2007 11:08:00 PM

Dude, youre just paranoid. why the hell would they go to such lengths to keep "you" quiet. You are either seriously and certifiably paranoid or you have a very bad case of feeling very inferior and very self important. Get over yourself man and stop reading conspiracy theory oriented media.

Posted by: the truth | Oct 30, 2007 2:37:28 AM

welcome to the information age. glad you could make it.

Posted by: welcome wagon | Oct 30, 2007 6:48:16 AM

This is bull shit..... and thing is, no ones going to do jack shit about it. Sure people will moan and cry, but in the end the people dont have power. It was nice having some sense of privacy while it lasted.

Posted by: Living in 1984 | Oct 30, 2007 7:18:19 AM

Your logic seems to be
* FBI requests info about "communities of interest" from telcos.
* Verizon can't create these records.
* AT&T has technology that *could* do this, ergo...
* Hancock is "Programming Language for Mass Surveillance"
The intellectual rigor here is stunning.

Posted by: Socrates | Oct 30, 2007 10:07:45 AM

This is a massively bad thing for personal privacy and the only way to fight it is to hit them were it hurts I know I will be selling all the ATT stock I own and would encourage everyone else to do the same

Posted by: Damian | Oct 30, 2007 11:19:35 AM

So, listen up all you complainers. You use the phone book right? You pay your phone bills right? When you need to check your bill to make sure it's correct, you call up the phone company and ask them to verify that you did X and Y. They can say... gee, I'll get back to you when I can talk my DBA in to running that for us, or something, or they can figure out how to grok everything real quicklike, by writing a macro language. I'd hope when they're talking to me about some data I need about myself that they're using something good to get at it in a timely fashion, after all, they work for me, I don't work for them. Now, as for the government being able to see all that, they've been able to see all that anyway.
By the way to the first poster: There is no such thing as "Intensive Purposes" it's "intents and purposes."

Posted by: hey | Oct 30, 2007 11:29:05 AM

Free and easy to use s/w is available to prevent this datamining. Obviously, the majority of your communications are not sensitive enough that you care. But, when/if they are: turn on encrypted vpn or ssh tunnel between you and other guy. talk over private voip, exchange data by windows file shares or nfs and instant msg using jabber....completely secure. Maybe mom and pop don't know how to do it but I do and so do the majority of the terrorists...

Posted by: bobsuruncle | Oct 30, 2007 12:01:13 PM

POST A COMMENT

Name:

Email Address: (Not Required, Not Published)

Comments:

Post

See more Threat Level