University of Maine

Department of Computer Science

Web Neighborhood Watch

George Markowsky[1], Chair
Anatoly Sachenko[2], Director
Gene Connolly[1], Senior

[1] Department of Computer Science
University of Maine
Orono, ME, USA

[2] Institute of Computer Information Technologies
Ternopil Academy of National Economy
Ternopil, Ukraine

What Can You Learn On The Web That is Related to Homeland Security?

- The quest for homeland security has led to wide ranging searches for information
- What information can one get from the Internet
- Here are some examples

News Front Page
World
UK
England
N Ireland
Scotland
Wales
Politics
Business
Entertainment
Science/Nature
Technology
Health
Education

Talking Point

Country Profiles
In Depth

Programmes

BBC SPORT

Thursday, 12 December, 2002, 10:00 GMT

Websites spread al-Qaeda message

Al-Qaeda statements are debuting on the web

By Mark Ward

BBC News Online technology correspondent

The web is becoming a potent weapon in al-Qaeda's bid to win supporters to its cause.

A widespread network of websites are energetically feeding information from those at

INVESTIGATING AL-QAEDA

Full coverage

Key stories
Hunting an Iraqi link
Guantanamo update

European probe
Spanish swoop
Italy on alert
Hamburg connection
Europe's al-Qaeda hunt

Background
Al-Qaeda battle update
Who's who in al-Qaeda
Roots of jihad
Al-Qaeda's origins

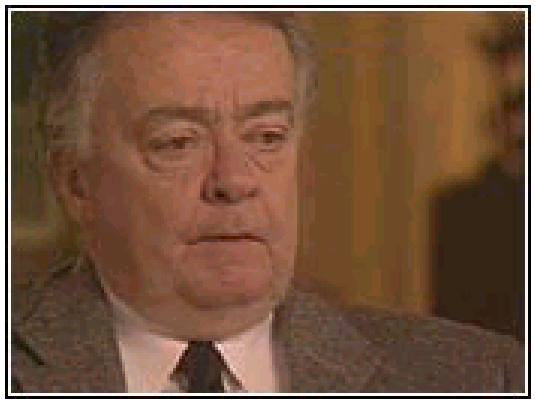
IN DEPTH
The investigation
The money trail

Many site operators actively seek out vulnerable hosts and secretly install their web pages until they are detected and deleted, said Mr Weisburd.

Often they can remain active for months before they are noticed and removed.

"Cluelessness and inattentiveness are widely distributed and abundant resources on the worldwide web," he said.

Columbine: Were There Warning Signs?



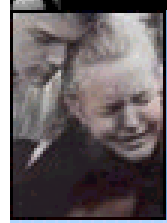
A year before the attack, Howard Cornell wrote a security plan for Columbine's school district. (CBS)

(CBS) A year before the attack, Joe Schallmoser and Howard Cornell were worried that Columbine was just the kind of place where a school shooting might happen. They were in charge of security for the school district that included Columbine. After the shootings in Paducah, Ky., and Jonesboro, Ark., they were afraid that one of their schools might be next.

In August of '98 - a full eight months before the attack on Columbine - Cornell and Schallmoser wrote a security plan

• Archives
• Program Facts
• Bios
• Contact Info
• Up Next
• Tapes and Transcripts

INTERACTIVE



Columbine Tragedy

The 1999 deadly shooting spree at Columbine High School in Colorado left 15 students dead, including the two gunmen.

When Cornell and Schalmoser presented their plan to Columbine, the school had already been alerted that one of its juniors, Eric Harris, might be dangerous. At night, Harris and his friend Dylan Klebold had been building an arsenal and making plans to use it - plans that Harris wrote about on the Internet, on his Web site.

In 1998, Brooks Brown was a junior at Columbine. That March, he found his name on Harris' Web site. Harris was threatening to kill him.

"When I first saw the Web pages, I was utterly blown away," Brown says. "He's not saying that he's gonna beat me up, he's saying he wants to blow me up and he's talking about how he's making the pipe bombs to do it with."

Brooks' parents, Randy and Judy Brown, say they were horrified by the Web site and frightened of Harris, who lived nearby. They decided to take pages from the site to the Jefferson County Sheriff's Office, where an investigator told them that Harris already had a criminal file. He and Dylan Klebold were on a form of probation, for breaking into a van and stealing equipment.

The Affidavit

60 Minutes II obtained the affidavit pertaining to the Web site after families of the victims and **CBS News** complained that some documents were missing from the 11,000 pages Jefferson County District Judge Brooke Jackson ordered released last year.

Warning: document contains graphic language.

"I was utterly dumbfounded that they did nothing with the Web pages," says Brooks Brown. "Eric was saying how he was gonna blow people up. 'Hey, I'm making pipe bombs. I'e got the designs for them on my Web site. I'm gonna kill these people. Here's why.' That's a level beyond making a joke."

At first, the sheriff's department denied its investigators had even met with the Browns in person. But we obtained this police paperwork, showing those investigators not only "met with Mrs. Judy Brown," but then worked on a warrant to search Eric Harris' home. Even more surprising, one document shows a sheriff's deputy found "a pipe bomb... consistent with the devices" Harris described on his site. But the sheriff's department never searched - or even visited-the Harris home. It was April of '98 - a full year before the Columbine massacre.

"People are covering up everything that went wrong and I want those lessons out there," says Judy Brown. "They're doing studies, they're getting profiles. Everybody's trying to get programs going and what we can do. Well guess what? All the signs were there. You know what the lessons are? Do your job."

You do, of course, have to do something once you find a dangerous situation!

Eric Harris and Dylan Klebold were both avid Internet users. Harris had even maintained a website in which he expressed his thoughts about any and every topic he could think of, from three pages of "your mama" jokes, to a page where he ranted about random topics.

> YOU KNOW WHAT I HATE!? ---When there is a group of ***holes standing in the middle of the hallway or walkway, and they are just STANDING there talking and blocking my f***ing way!!! Get the f*** outa the way or i'll bring a friggin sawed-off shotgun to your house and blow your snotty ass head off!! (2)

These rants also talked about how they were going to be the new natural selection. Eric also ended almost every rant with how he was going to kill them.

RELIGION IN THE NEWS

Spring 2001, Vol. 4, No. 1

Contents, Spring 2001

Related Articles:
"Cult Fighting in Massachusetts" *Religion*

Aum Alone

by Ben Dorman

Since its horrific sarin gas attack on the Tokyo subway system on March 20, 1995, the millennialist religious group Aum Shinrikyo has been a constant presence in the

In December, Justice Minister Masahiko Komura announced that jailed guru Asahara continues to wield enormous influence over his followers and that Aum still poses a threat to the public. During the first year of the new law, the PSIA carried out 15 inspections of Aum facilities and Aum submitted four compulsory reports to the agency. In a report of its own, the PSIA declared that Aum was trying to spread its message on the Internet, effectively turning itself into a "cybercult."

What Can We Do About This?

- Extend a trusted concept into Cyberspace:
  - The Neighborhood Watch!
- This program has been in operation for over 30 years and has helped secure many neighborhoods across the US
- What do we mean by a Web Neighborhood Watch!

USAonwatch.org

NATIONAL SHERIFFS' ASSOCIATION
Neighborhood Watch

- HISTORY
- PURPOSE
- LOCATE YOUR LOCAL SHERIFF
- WEEKLY NEWS
- SAFETY TIPS
- OTHER RESOURCES
- JOIN OUR NETWORK

A message from the Department of Justice

LIVE INTERVIEW
Editorial Calendar
Archives

A Secure and Alert Neighborhood is a Secure and Alert Nation.

IN THE NEWS . . .

April 28 - May 5, 2003

Virginia Community Comes Together to Support Homeland Security Efforts

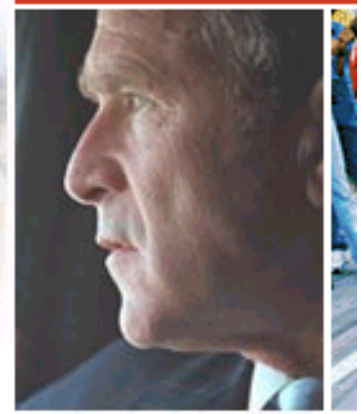
Any community in proximity to Washington, DC, has a new sense of awareness in relation to terrorism. Stafford County, Virginia, has several reasons to be more alert in the face of the September 11, 2001 tragedy.

(continue...)

NEIGHBORHOOD WATCH

For over 30 years, the Neighborhood Watch Program has provided Americans a unique safety infrastructure that brings together local officials, law enforcement and citizens for the

- THE WHITE HOUSE
- CITIZEN CORPS
- DEPARTMENT OF JUST
- FEMA
- NATIONAL SHERIFFS' A
- CENTERS FOR DISEASE
- US POSTAL SERVICE



A Message From The President

citizencor

HELP THE F
AGAINST TERR

The Web Neighborhood Watch

- A wide ranging project that is just getting started
- Some goals are:
  - Spot troubling websites and notify authorities when appropriate
  - Locate web servers geographically
  - Protect vulnerable sites
  - Collate disparate sources of information
- The following is different from what we want to do

ECONOMY
JUSTICE
MILITARY
POLITICS
SOCIETY & CULTURE

USA > Society & Culture
from the May 05, 2003 edition

New police tool: neighborhood watch by Web

By Dean Paton | *Special to The Christian Science Monitor*

SEATTLE – When someone burgled a home in De Pere, Wis., last July, they stole - among other things - a child's plastic Coke-bottle coin bank, bursting with about 1,200 quarters.

Additional Activities

- Can actively disrupt websites
  - Not our plan
- Already we have a quiet cyberwar going on
- Some unusual characters involved

Pornographer says he hacked al Qaeda

'I wanted to do something ... I know the Internet'

August 9, 2002 Posted: 7:54 AM EDT (1154 GMT)

(CNN)

Jon Messner put the Web skills he learned in the adult entertainment business to work against an alleged al Qaeda Web site.

From Mike Boettcher
CNN

OCEAN CITY, Maryland (CNN) -- A self-proclaimed Web warrior says he enlisted in the United States' war on terror by mounting an incursion into an Internet site said to be run by al Qaeda.

From his beachfront home, Jon Messner uses his keyboard as a weapon against the enemy's site -- first reported by CNN four months ago -- that posts statements from high-ranking al Qaeda

Messner, using the aggressive tactics he's employed to run his adult site, said he "hijacked" Al Neda for five days and recorded a "virtual who's-who of every hostile message board and site on the Internet."

Progress To-Date

- So far have worked extensively on the geographical location piece
- Have looked only at the problem of geographically locating a website based on the IP address
- Content analysis can also help, but this is for future work
- The following work was done by Gene Connolly, a senior in the UM CS Dept

IP Locater Prototype

- Written in perl
- Combines use of traceroute from multiple locations with Whois information
- Multiple traceroute runs permit bracketing websites
- Whois can provide very detailed information

```
C:\>tracert umcs.maine.edu

Tracing route to umcs.maine.edu [130.111.112.21]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2    16 ms    16 ms    16 ms  142.167.3.11
  3    17 ms    17 ms    17 ms  142.167.4.1
  4    26 ms    25 ms    28 ms  500.Serial3-11.GW8.BOS1.ALTER.NET [63.111.121.197]
  5    40 ms    41 ms    36 ms  196.ATM3-0.XR2.BOS1.ALTER.NET [152.63.25.134]
  6    32 ms    36 ms    29 ms  290.at-1-0-0.XR2.BOS4.ALTER.NET [152.63.16.158]
  7    38 ms    33 ms    32 ms  0.so-4-0-0.XL2.BOS4.ALTER.NET [152.63.16.133]
  8    82 ms    84 ms    85 ms  0.so-2-0-0.XL2.NYC9.ALTER.NET [152.63.21.74]
  9    36 ms    39 ms    39 ms  POS7-0.BR1.NYC9.ALTER.NET [152.63.18.221]
 10    41 ms    37 ms    40 ms  204.255.174.130
 11    43 ms    50 ms    54 ms  ewr-core-02.inet.qwest.net [205.171.17.129]
 12    39 ms    39 ms    39 ms  bos-core-01.inet.qwest.net [205.171.8.28]
 13    46 ms    54 ms    42 ms  bos-brdr-01.ip.qwest.net [205.171.28.38]
 14    48 ms    50 ms    51 ms  65.126.246.218
 15    60 ms    68 ms    64 ms  GW-P-C65-int.unet.maine.edu [130.111.2.33]
 16    51 ms    51 ms    55 ms  gw-portland-int.unet.maine.edu [130.111.33.33]
 17    89 ms   291 ms   190 ms  ATMPOR-9003.unet.maine.edu [130.111.33.69]
 18    52 ms    55 ms    56 ms  GW-O-C65-int.unet.maine.edu [130.111.33.6]
 19    62 ms    72 ms    62 ms  GW-O-C65-int.unet.maine.edu [130.111.33.6]
 20    81 ms    75 ms    89 ms  130.111.112.21

Trace complete.
```

Host Name Pattern Matching

- Geographical Information is embedded in the hostnames:

```
0.so-4-0-0.XL2.BOS4.ALTER.NET [152.63.16.133]
0.so-2-0-0.XL2.NYC9.ALTER.NET [152.63.21.74]
```

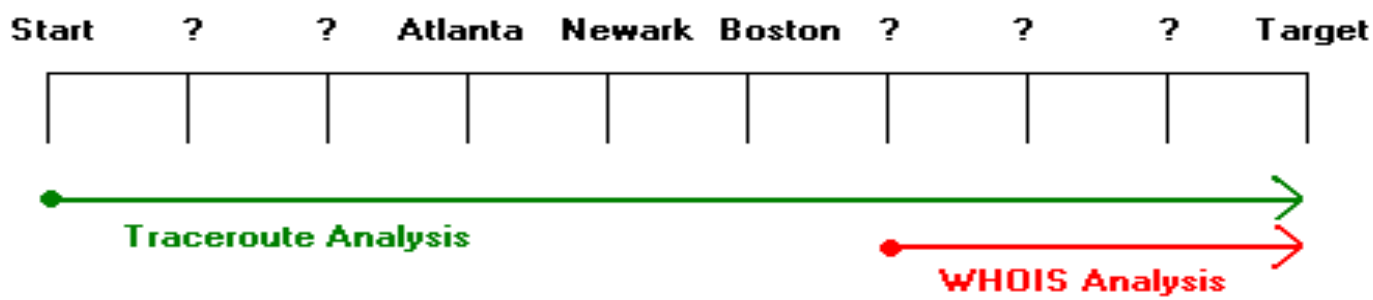
- City, State, and Country codes are used in some network naming schemes.

Properties of Hostname Pattern Matching

- Location Codes not available in local networks.
- Examination of Entire Traceroute:
  - Creates a geographical path of data.
  - Uncertainty exists where location codes are not available.
  - Best case: The Location of the closest city to the target computer
  - Direction from which the target was approached.

Properties of Traceroute Approach

- WHOIS Data is an effective tool for confirming the accuracy of the traceroute results.
- Results of Traceroute Approach:
  - Is ‘Closest City’ enough information?
  - What is the position relative to the ‘Closest City’?



WHOIS Database

- Database containing a record of every network and domain on the Internet:
  - Network Information
  - Administrative & Technical Contacts
  - Name Servers
  - Registration Info
- Used for Allocation of Domain Names and as a means of contacting network administrators.

WHOIS Geographical Information

- The Address of Administrative Contacts?
  - Maine.edu
    - Administrative contact: Orono, ME
    - Network spans the state of Maine.
  - UMaine network.
    - Administrative contact: Orono, ME
    - Network spans the University of Maine.
- WHOIS Database can be useful for confirming the location computers on local networks

Benefits of Traceroute & WHOIS Database

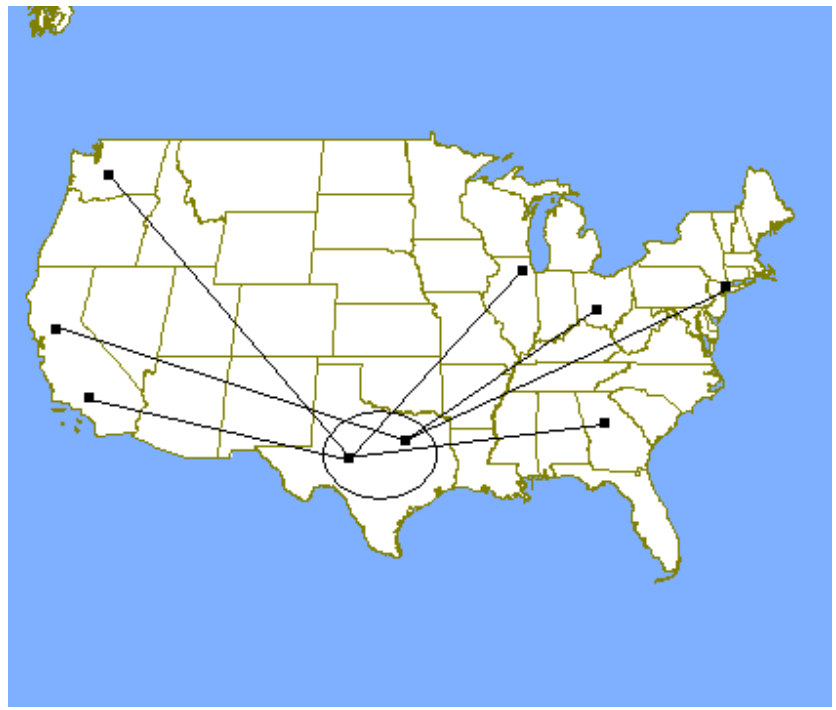
- Traceroute:
  - Effective on large networks.
  - Determine a route to the target computer
  - Result: Closest City to Target Computer
- WHOIS:
  - Effective on small networks.
  - Determine the region of the target computer
  - Result: Network HQ of Target Computer

Distributed Approach

- Traceroutes from multiple geographically and network-diverse computers.
- Some public
  - University of Washington
  - University of California-Berkeley
  - New York Net
  - Iowa State
  - AboveNet Communications

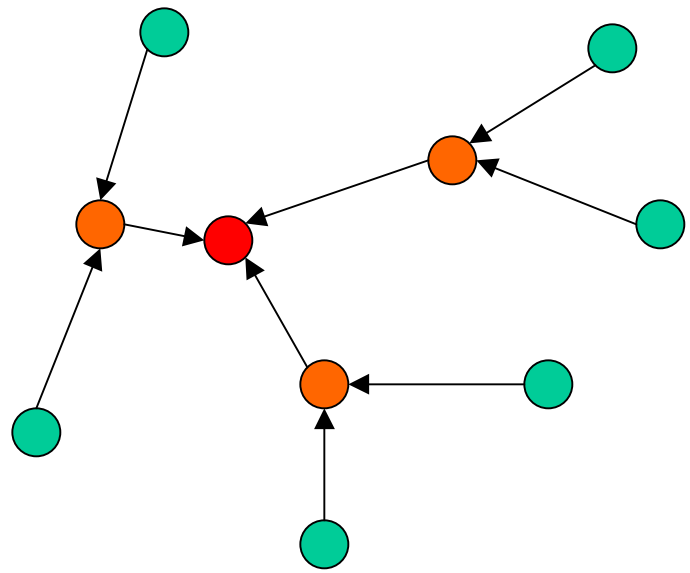
Proposed Distributed Approach

- Extension of Traceroute Approach.
- Stronger Analysis of Networks Surround Target.
- Different Approaches offer Geographical Basis.



Location Graph

- Synthesis of a Multiple Traces:
- Red: Target Computer
- Orange: Local City
- Blue: Location of Geographical Basis



Scenario #1: IEEE.org

Actual Location:	Piscataway, New Jersey
Location Tree Destination:	Unknown
Possibly Cities:	
Three Degrees Anonymous:	New York, NY (Philadelphia, PA) Pennsauken, NJ (Fort Worth, TX; Newark, NJ)

Accuracy: Piscataway is located 30 miles west-southwest of New York, and 51 miles Northeast of Pennsauken. Using each of the two possible cities as focal point in this example, the target zone could be reduced to between the two cities. Either of the traces standalone would offer no more information regarding the position of the target relative to the final possible city.

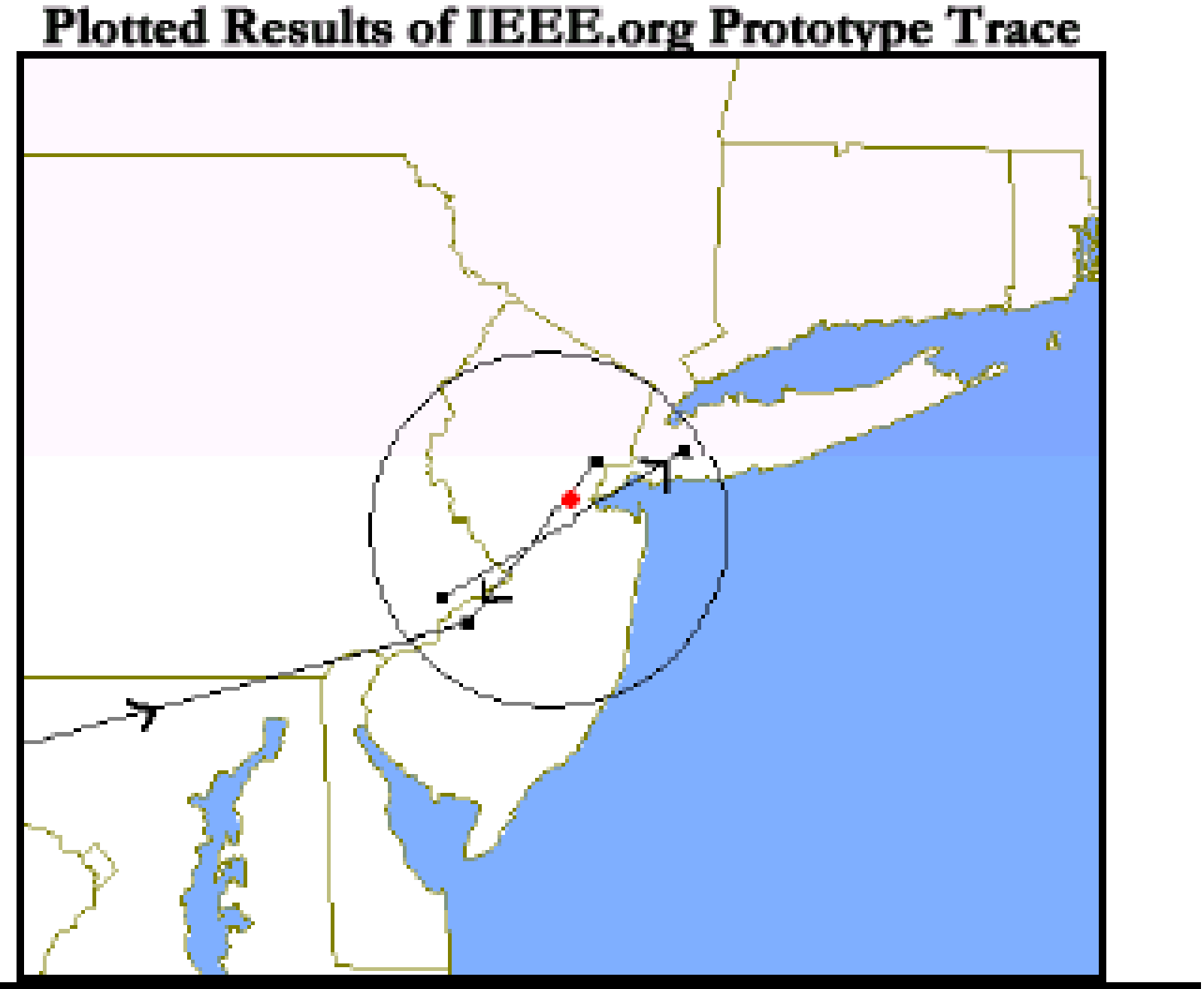


Figure 6.1: Prototype Results of IEEE.org
Maps Courtesy of TIGER [20].

Scenario #2: ICANN.org

Actual Location:	Marina Del Rey, CA
Location Tree Destination:	Unknown
Possibly Cities:	
Two Degrees Anonymous:	Los Angeles, CA (San Jose, CA; Milpitas, CA; Dallas, TX)

Accuracy: Marina Del Rey is located 9 miles north-northeast of Los Angeles. Because the only possible city is approached by three separate traces, one may conclude that the destination is strongly correlated to the particular city. With each additional approach the correlation grows stronger. In the case of a single trace, the correlation is weak.

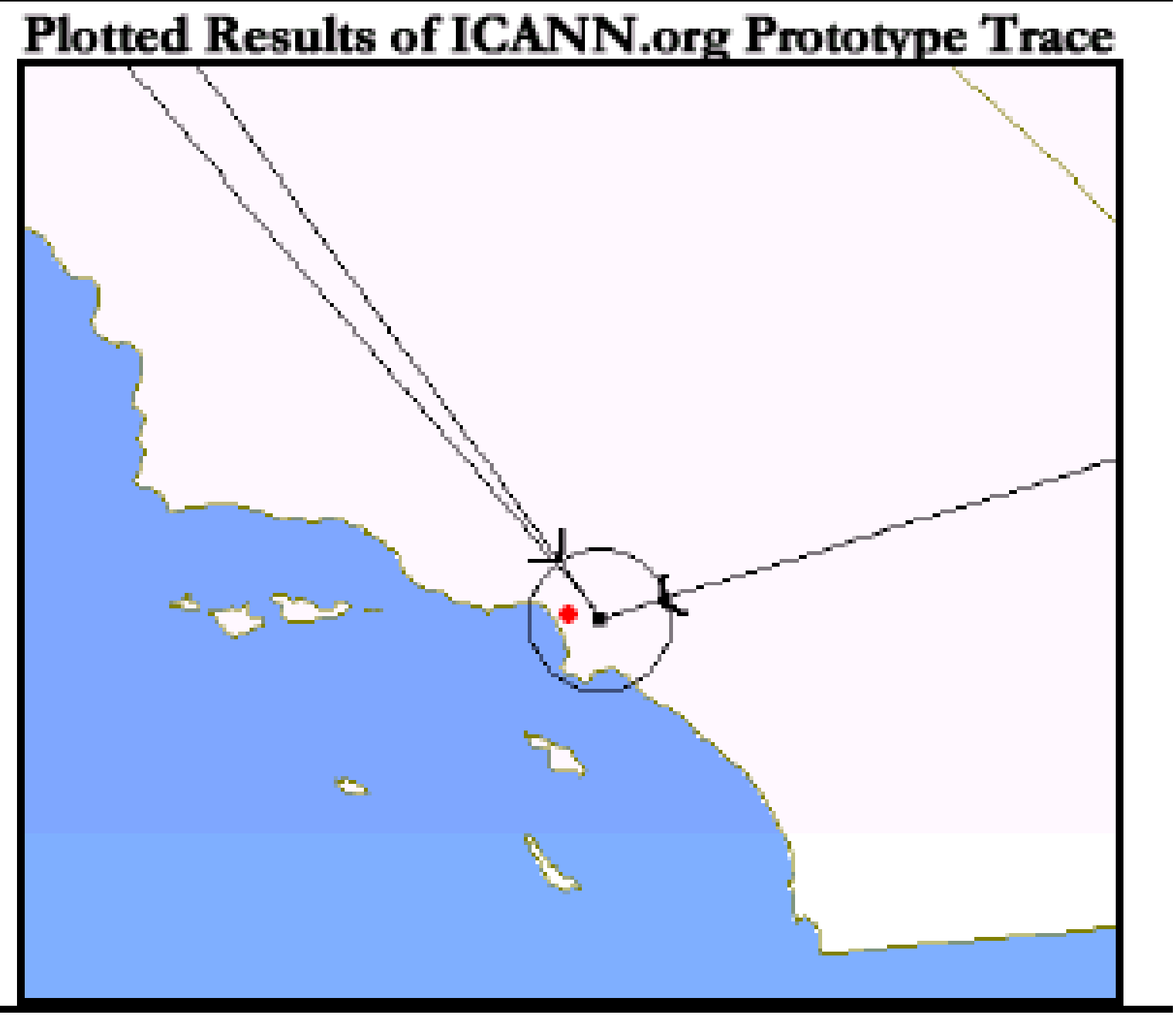


Figure 6.2: Prototype Results of ICANN.org
Maps Courtesy of TIGER [20].

Scenario #3: CNN.com

Actual Location:	Atlanta, GA
Location Tree Destination:	Unknown
Possibly Cities:	
One Degree Anonymous:	Atlanta, GA (Houston, TX; Charlotte, NC)

Accuracy: The only possible city correctly identifies the city if the target computer. Although every trace individually concluded upon Atlanta as the destination, each additional trace confirms that information, and confirms the general location by offering direction.

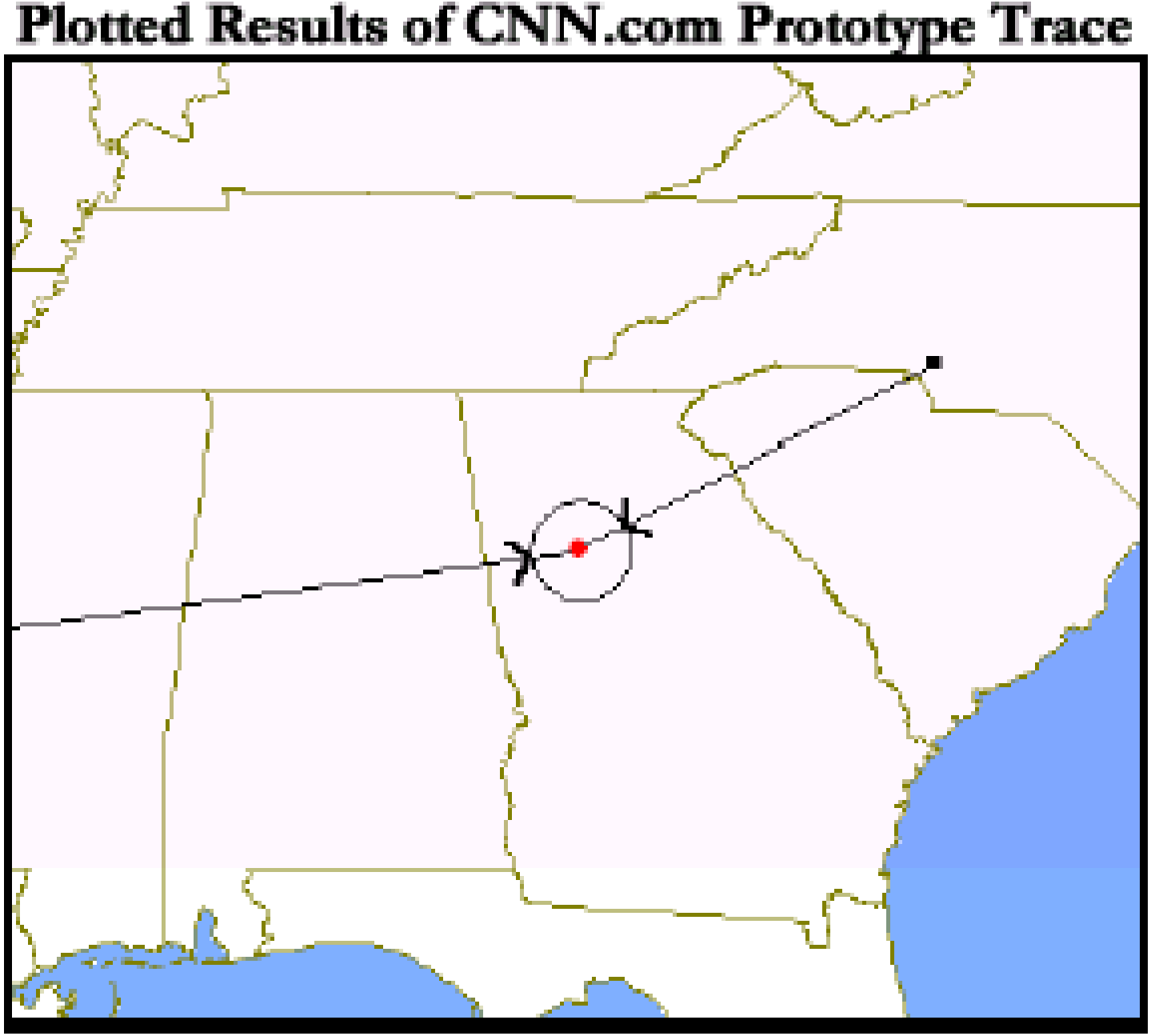


Figure 6.3: Prototype Results of CNN.com
Maps Courtesy of TIGER [20].

Scenario #4: Residential Computer

Actual Location:	South Berwick, ME
Location Tree Destination:	Unknown
Possibly Cities:	
One Degree Anonymous:	Dover, NH (Portsmouth, NH; Cambridge, MA)

Accuracy: South Berwick is located 5 miles northeast of Dover. The intent of this trace was to demonstrate that traces are also very accurate in tracing individual machines, as well as domain servers.

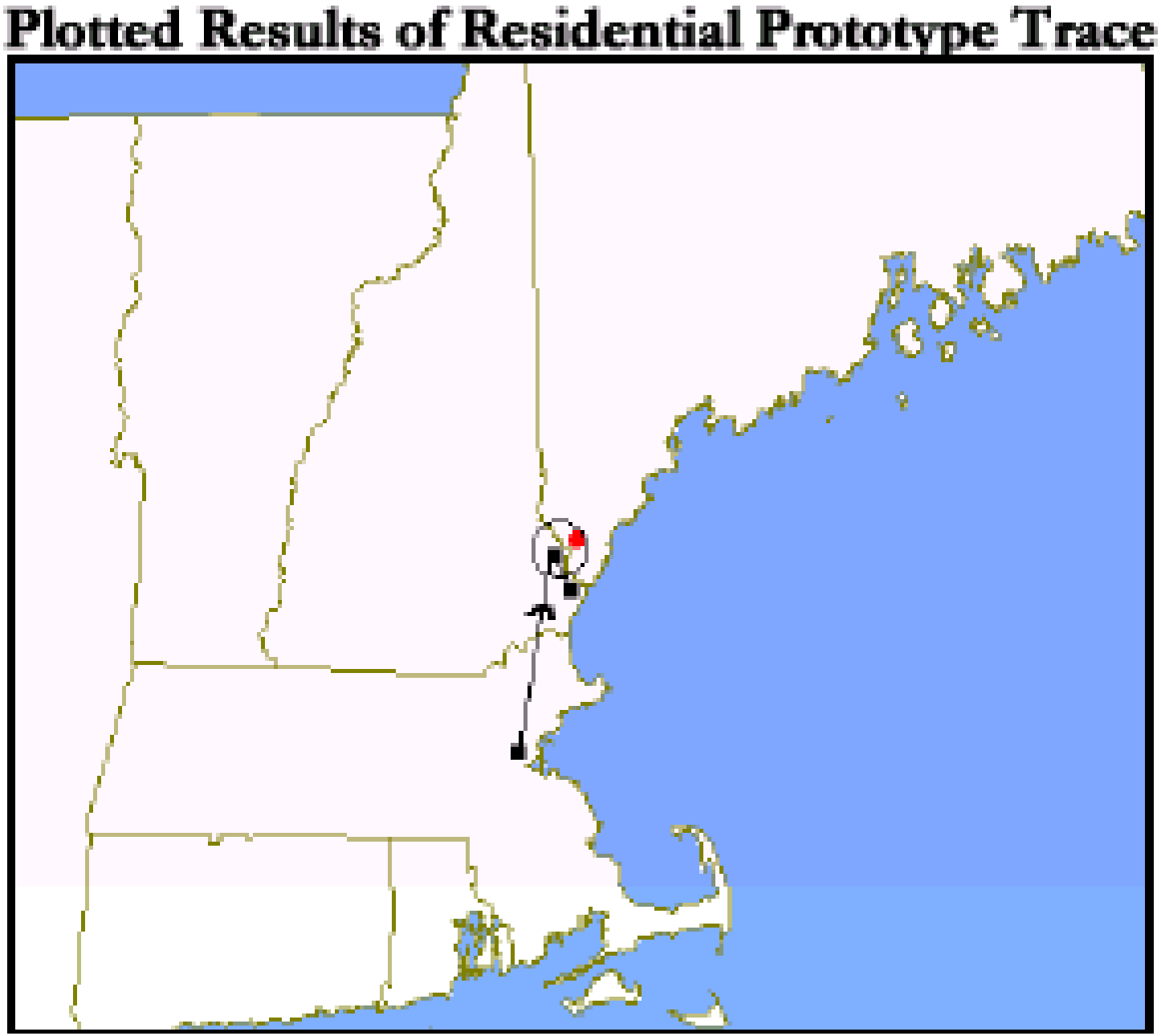


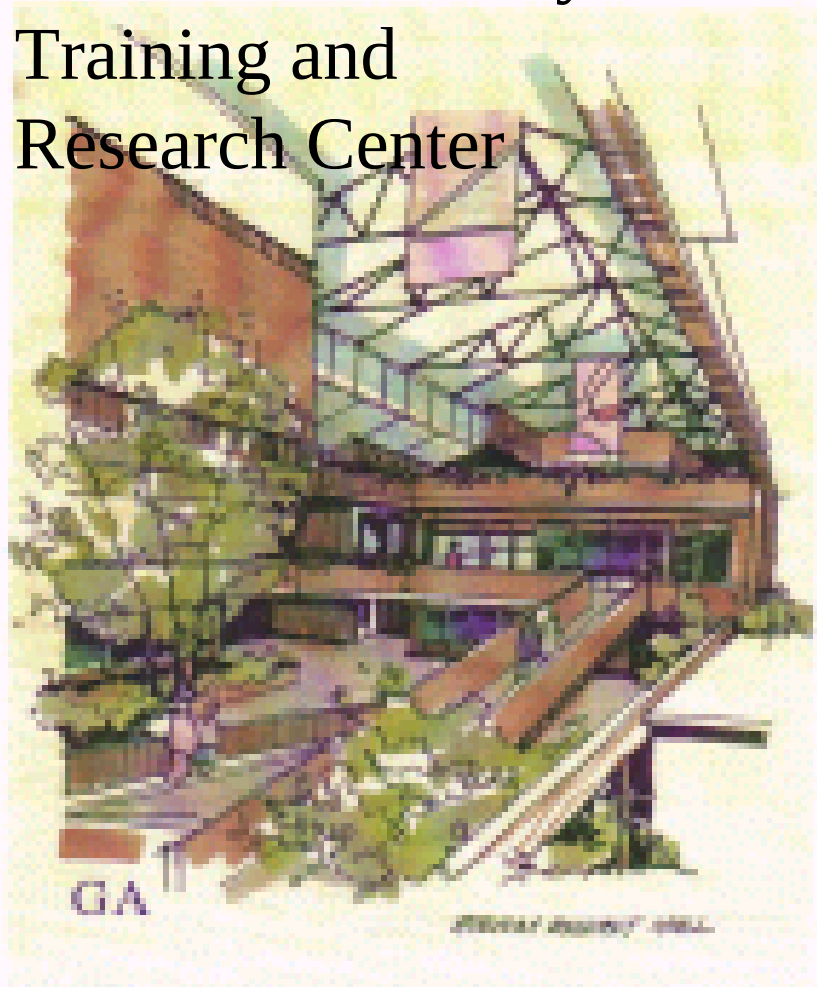
Figure 6.4: Prototype Results of Residential Computer Maps Courtesy of TIGER [20].

Other Projects

- Traceroute Based:
  - NetGeo/GTrace
  - VisualRoute
  - SarangWorld Traceroute Project
- Other Projects
  - GeoBytes
  - DNS LOC
  - Zooknic

Ayers Island, Orono, Maine

Ayers Island Homeland Security Training and Research Center



More Information

- Project is part of the UMaine Homeland Security Lab
- More details in Gene Connolly's Honors Thesis which will be available within two weeks at
- http://homeland.maine.edu