



Airborne Contagion:

Effects of a Worm on Wireless Networking

Christopher Chin

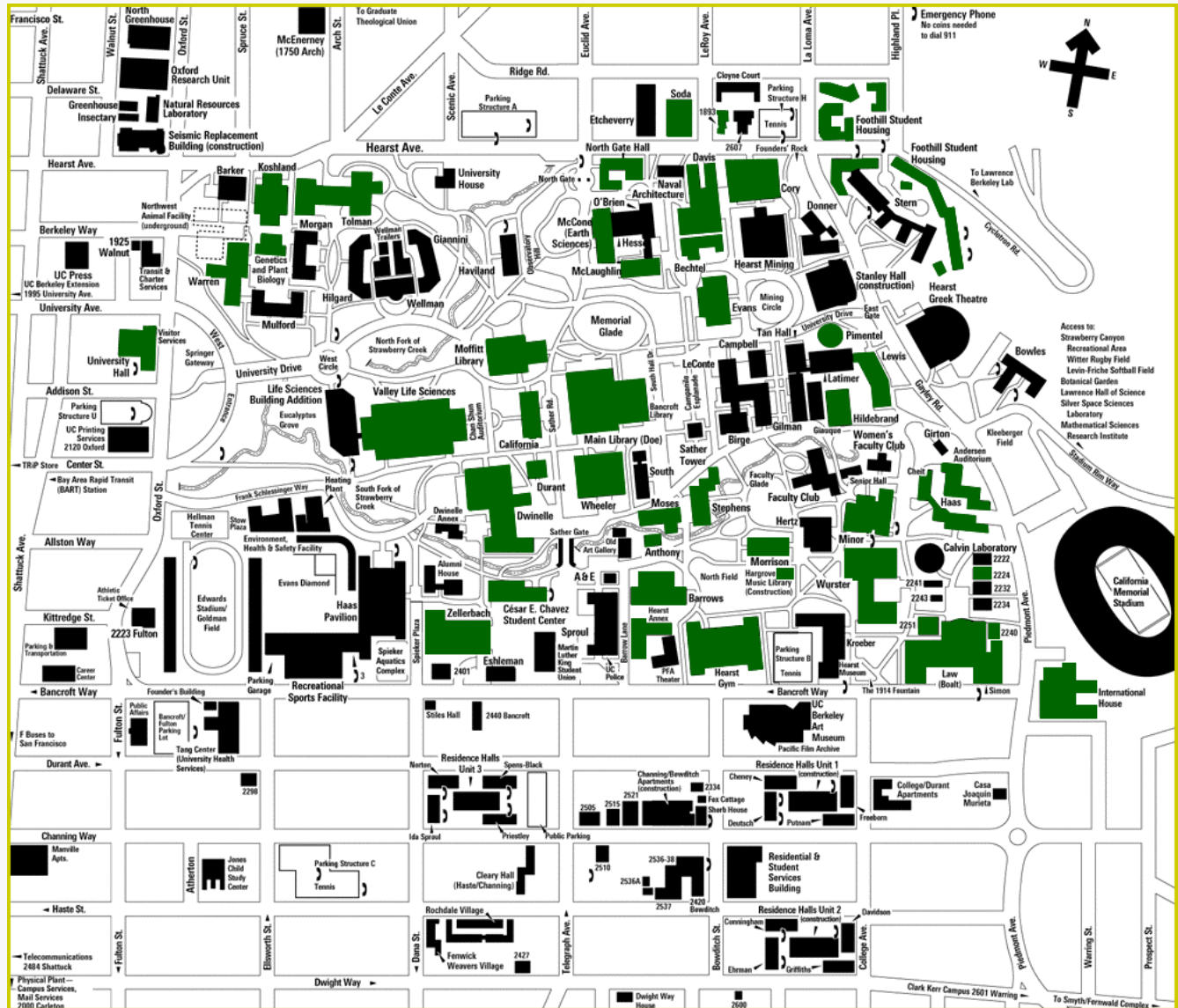
UC Berkeley

Network Services

Overview

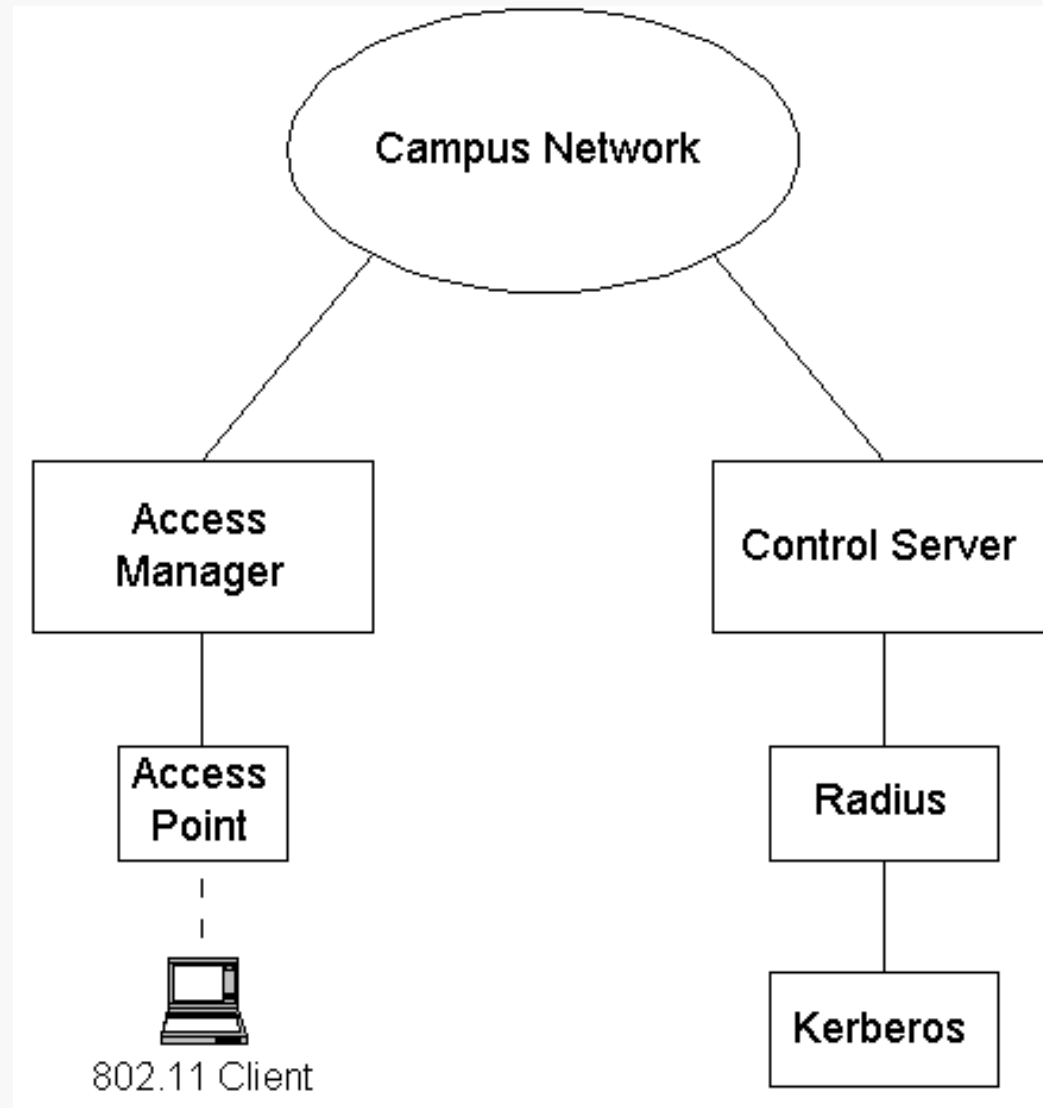
- Wireless coverage at UCB
- Logical topology
- Network detail
- Welchia/Nachi infection & spread
- Effects
- Quelling the noise
- Cleaning up
- Retrospective

Wireless Coverage at UCB

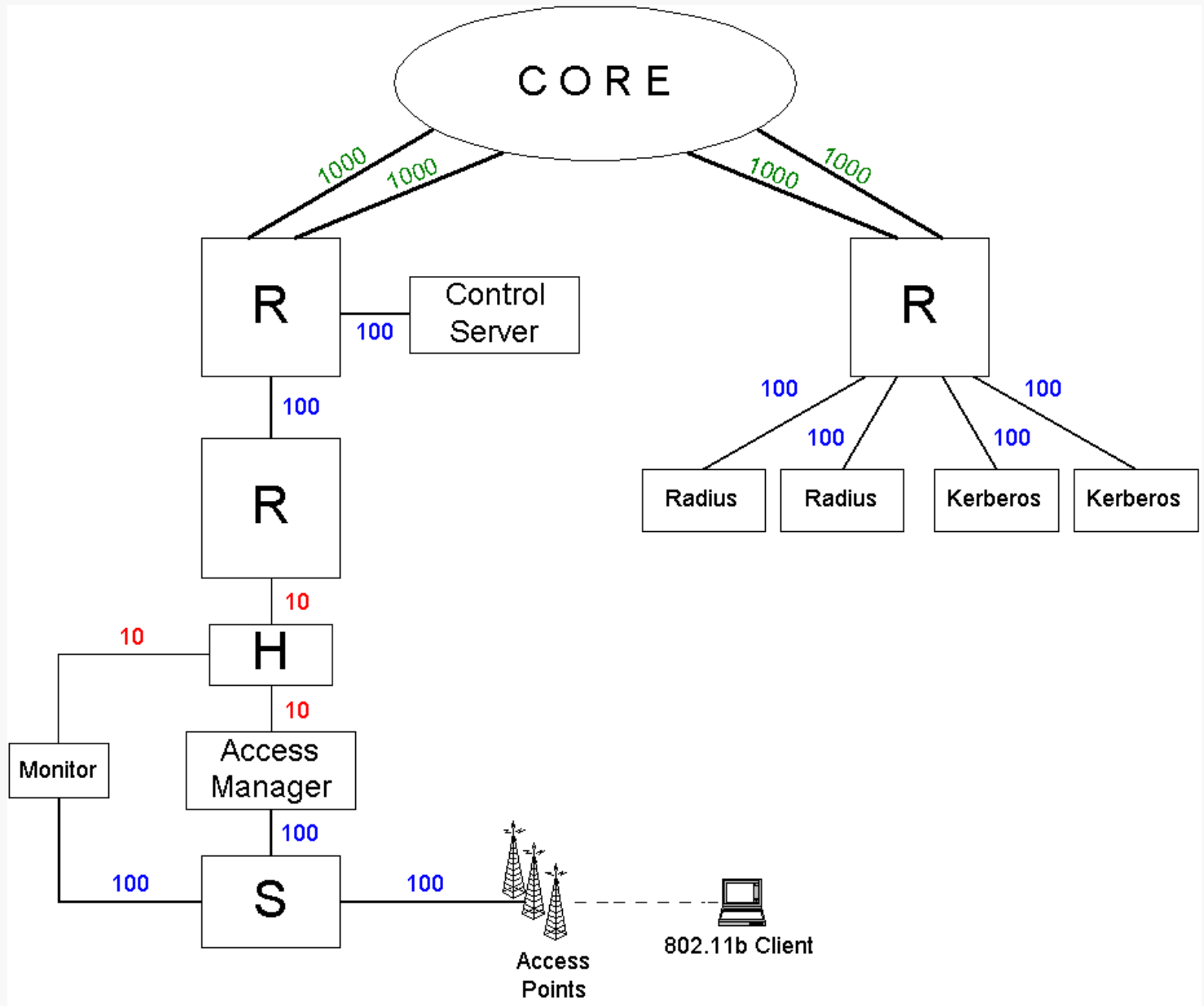


217 APs, 14 AMs, 3900 users (2200 in May 03)

Logical Topology



Network Detail



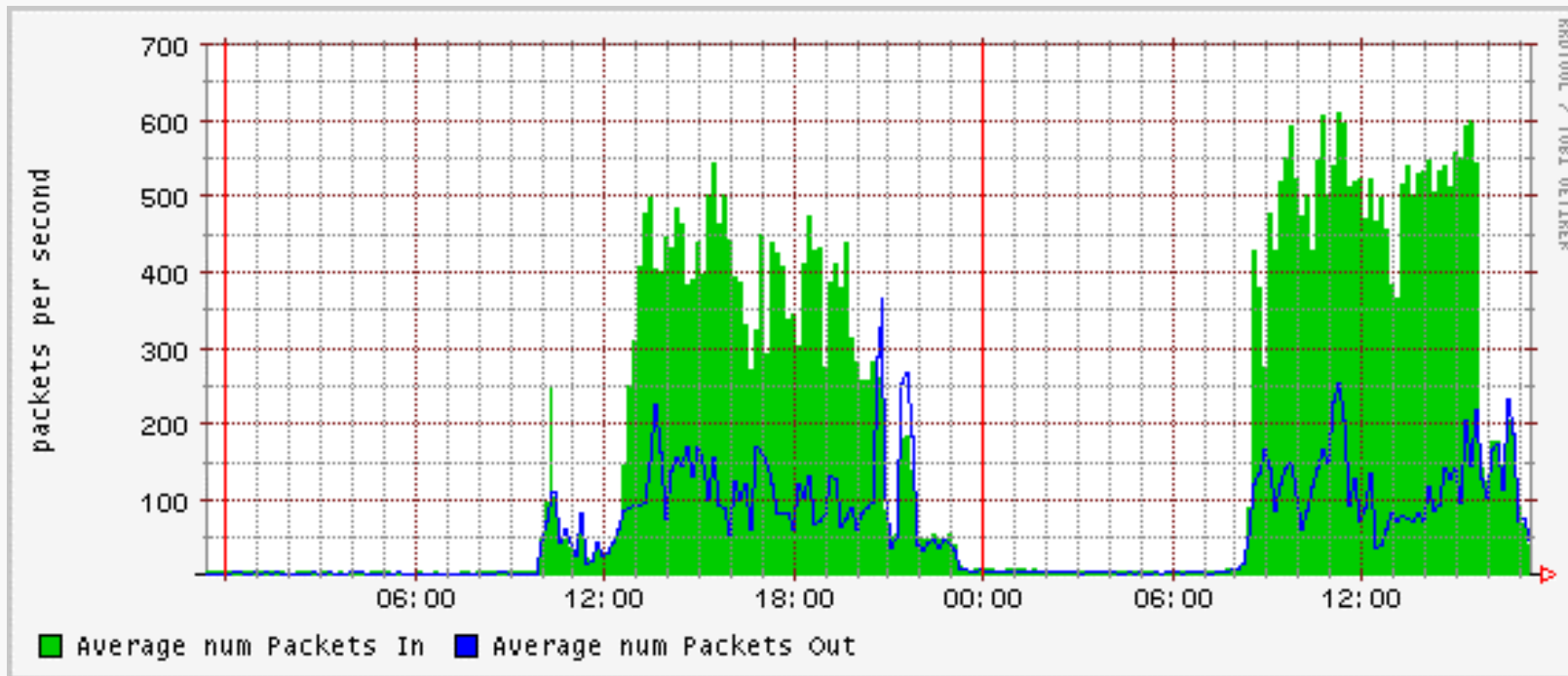


Welchia/Nachi: Infection and Spread

- Blaster released on 11 August 2003
- Welchia: 18 August (1st day of semester!)
 - ICMP scan of local /16 (then others)
 - DCOM RPC 135/tcp
 - IIS WebDav 80/tcp (discovered in March)
 - multithreaded: up to 300 simultaneous targets

Effects

- Internal DOS: bandwidth saturation
- Authentication hindered
- CS \Leftrightarrow AM connection lost.



Quelling the Noise

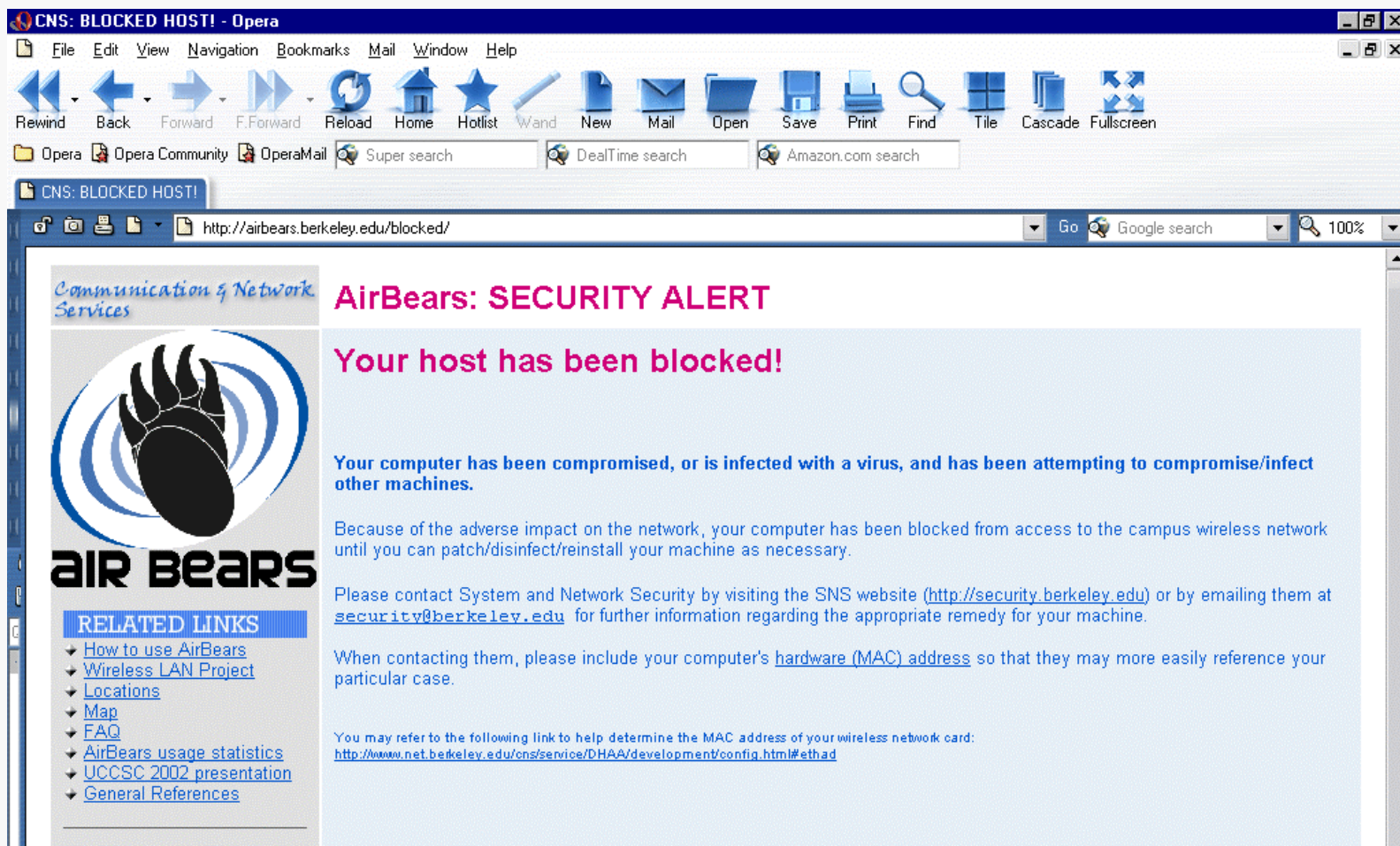
- ICMP signature
 - echo request (type 8, code 0)
 - 92 byte datagram
 - payload filled with "0xAA" (decimal 170)

```
0x0000  4500 005c 2dc8 0000 7901 66a6 xxxx xxxx  E..\-...y.f.....
0x0010  xxxx xxxx 0800 3318 0200 6d92 aaaa aaaa  .....3...m.....
0x0020  aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa  .....
0x0030  aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa  .....
0x0040  aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa  .....
0x0050  aaaa aaaa aaaa aaaa aaaa aaaa  .....
```

- Packet filtering using tcpdump rules

Cleaning Up

- MAC address blocking
 - redirection to information page



The screenshot shows an Opera browser window with the title "CNS: BLOCKED HOST! - Opera". The address bar displays "http://airbears.berkeley.edu/blocked/". The page content includes the AirBears logo (a black paw print on a blue circular background) and the text "Communication & Network Services". The main heading is "AirBears: SECURITY ALERT" in pink, followed by "Your host has been blocked!" in pink. Below this, a blue box contains the text: "Your computer has been compromised, or is infected with a virus, and has been attempting to compromise/infect other machines." The page also provides instructions on how to contact System and Network Security, including a list of "RELATED LINKS" such as "How to use AirBears", "Wireless LAN Project", "Locations", "Map", "FAQ", "AirBears usage statistics", "UCCSC 2002 presentation", and "General References".

Retrospective

- Dropped connections not logged
- Shared wireless cards (e.g., library)
- Dependence on distinct signature
- Topological improvements
- Upgrade, upgrade, upgrade . . .