LAWN
Local Area Wireless Network

DCIS/LCSR
Wireless Zone

This area has wireless coverage using an 802.11b (Wi-Fi) network.

http://please.rutgers.edu/show/wireless
wireless@dcis.rutgers.edu

Laboratory for Computer Science Research
Division of Computer and Information Sciences
Rutgers University

5/19/03
LCSR Wireless (LAWN)

- 2 years of operational experience as of May 2003
- 145,000 sq ft (two buildings, 7 floors today — 11 floors by September 2003) indoor/outdoor coverage
- 27 access points today (20 in September 2002, 35 by September 2003)
- 372 users today (125 one year ago)
  - DCS (184), non-DCS Undergrad (115), non-DCS faculty (73)
- One authentication server, one firewall (two of each by September, 2003), 21 distinct authentication sources
Who, What, Where

• RU New Brunswick (CoRE & Hill)
  – DCIS, IE, DIMACS, Math, BioMAPS
  – Location sensors (based on AP signal strength signatures)
  – Wireless soccer-playing robot dogs

• RUCS Newark
• RUCS Camden (wired)
• Lafayette College (summer 2003)
LawnUsage

![Graph showing lawn usage over time with specific data points for each month from January 2002 to April 2003.]

5/19/03
LAWN Design Goals

- Designed for a university environment
  - Distributed control of the infrastructure
    Authenticate against a variety of trusted servers
  - Research and infrastructure coexist
    Five cooperating 802.11b networks (SSIDs) sharing same physical space
  - Hassle free network access for visitors
    Workshops, visiting collaborators, etc.
  - Support encryption — but don’t require it
  - Research project — must support detailed monitoring
LAWN Design Goals

• Flexibility: One size doesn’t fits all, especially in a university environment
  – Authenticators cannot all be the same
    Each authentication server has a unique set of authentication sources.
  – Must support a variety of clients.
    WIN-95/98, WIN-ME/2k/XP, MacOS-9 & -X, Linux,
    Wireless PDAs (e.g., IPAQ, WinCE), soccer playing robot dogs
LAWN Design Goals

• Federated Authentication Servers
  – Trusted, but distinct, servers
    Each authentication server has a unique set of authentication sources, determined by the local sysadmin.
    Collaborators from other members of the federation can visit one another and automatically are accepted without having to register as guests.
LAWN Design Goals

• Low cost of development and ownership
  – Commercial, off the shelf, components
  – Free software
  – Inexpensive hardware
  – Leverage existing software & network infrastructure
  – Minimize operational overhead
LAWN Authentication

- User must know network name (SSID)
- All authentication transactions are secure
  - Identify yourself and your authentication source
  - Provide password
- User is authenticated by the authentication server against the identified authentication source
LAWN encryption

- LAWN supports many user-chosen security protocols
  - WEP – Not currently supported. Could be supported but this is not recommended
    - LAWN security is not reliant on WEP
  - vpn, ssh, ssl are supported and recommended
    - Clients use their own preferred security method
    - Requiring a particular security model is redundant and can be problematic (e.g., remote VPN conflicts with required local VPN)
LAWN for wired connections

- Ideal for wired computer labs, e.g. libraries.
- Functionally identical to wireless, but
  - Provides higher bandwidth
  - eliminates RF interference issues.
- Security implementation is identical to wireless
Services over wireless

Servers on the “wireless side” are supported
- Not recommended but easily handled
- Uses one-to-one NAP translator, and fixed MAC
LAWN Management
adding authentication servers

• Uses text tables
  
  math, math.rutgers.edu : math.rutgers.edu : imap, pop3
dimacs, dimacs.rutgers.edu : dimacs.rutgers.edu : imap, pop3
mail.cs.lafayette.edu : mail.cs.lafayette.edu : imap

• Supports various authentication methods
  – kerberos, radius, imap(secure, insecure), pop3 (secure, insecure), plaintext password file

• Working on support for more
  – SMB/CIFS, LDAP
Measurement & Monitoring

- Track usage
  - By user id (static)
  - Not just by IP address (dynamic)

- Optional IDS can monitor “top talkers” and other potentially suspicious behavior.
Cost of ownership

• **Hardware**
  – Old, obsolete workstations for authentication server and firewall.
  – Optional IDS may need to be big/fast/not-cheap
  – Inexpensive “cots” Access Points

• **Software**
  – Open Source, Free Software
  – Installation takes about 1/2 day
    • Mostly taken up with installing Linux, Apache, and Tomcat.
    • Actual LAWN software is small and easily configured.

• **Administration**
  – About 1/2 hour per week at LCSR during periods of growth
  – About 1/2 hour/month to install patches during stable times
Security issues

- Use trusted, distributed, authentication servers
- User functionality is the most crucial aspect
  - Visitors and collaborators must be more than guests
  - Security must be the user’s responsibility - encryption should be supported but not required
  - User must be free to choose her own security model
- If the situation calls for encryption, security experts recommend encrypting end-to-end
Stats and technical papers.

http://please/show/wireless