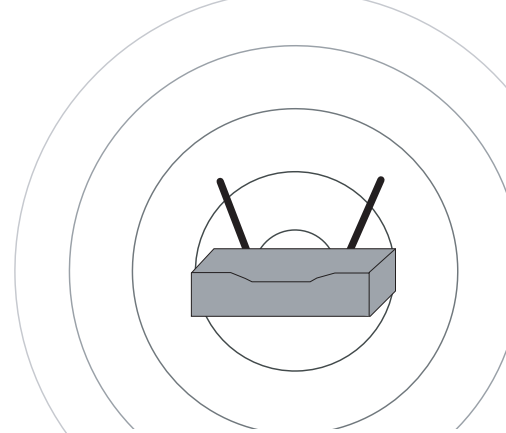


# Easy 802.11 Security Configuration for Home Users

Cynthia Kuo, Vincent Goh, Adrian Tang,  
Adrian Perrig, Jesse Walker



## Study Setup

### Target Population

- Likely consumer of 802.11 home networking equipment:
- ❖ Uses wireless Internet access at home, school, or work on a daily (5+ days/week) basis;
  - ❖ Has broadband access at home; and
  - ❖ Uses a laptop as a primary computer.

### Tasks (pre-WPA / pre-WPA2)

1. Change the default administrator password;
2. Change the SSID;
3. Generate or enter an encryption key on the access point;
4. Enter the encryption key on the client; and
5. Enable MAC filtering.

### Participant Assignment

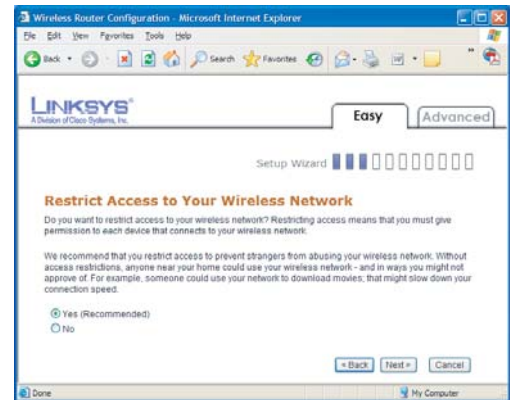
	Low Expertise	High Expertise
Linksys WRT54G	3	3
Netgear WGT624	3	3
Prototype	3	3

## Goals

- ❖ Discover why home consumers do not enable the security features on their 802.11 networks:
  - ◆ Are consumers not aware of the security issues?
  - ◆ Are they simply unconcerned about security?
  - ◆ Are they unable to configure their networks correctly?
- ❖ Enable home users to set and implement their own 802.11 security policies;
- ❖ Illustrate it is possible to improve 802.11 security configuration
  - ◆ By applying user-centered design principles for security applications;
  - ◆ Without hardware enhancements; and
  - ◆ So that "regular" home users - end users without prior experience in networking or security - can use it.

## Prototype

Applying user-centered design principles, we designed an 802.11 network configuration interface. The prototype was implemented on a Linksys WRT54G access point.



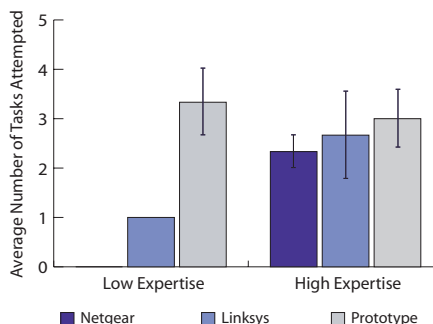
## Evaluation Methodology

Activity	Duration	Description
Interview	25 minutes	(Adapted from mental models interview) Understand where participants use wireless Internet access, their attitudes towards unsecured networks, and to what extent they understand their data is broadcasted.
Questionnaire	5 minutes	(Survey) Gather participants' attitudes towards various aspects of wireless networking: availability, reliability, ease of use, use of open wireless networks, security, privacy, and health.
Tasks	45 minutes	(Hybrid of contextual inquiry and usability study) Ask participants to configure a wireless network as they would at home. Observe participants until they declare they are finished, and then follow up with security-related questions. Ask participants to complete remaining tasks.
Questionnaire	5 minutes	Repeat questionnaire. Used to measure within-subject changes in attitude.
Debriefing	10 minutes	Close up with any remaining questions. Allow participants to provide feedback or ask questions.

## Results

The majority of participants appeared to have a fairly good understanding of (1) how wireless technologies work and (2) wireless network security issues. For example, when asked to list possible consequences of running an unsecured wireless network, 14 out of 18 participants volunteered unauthorized access of computers on the network. However, participants only expressed *concern* about network security issues involving concrete, easily imaginable consequences.

Low expertise users attempted to complete fewer tasks without prompting than high expertise users on the commercial access points. There was no significant difference for prototype users.



Low expertise users completed fewer total tasks than high expertise users on the commercial access points. There was no significant difference for prototype users.

