Manipulating the Home Network

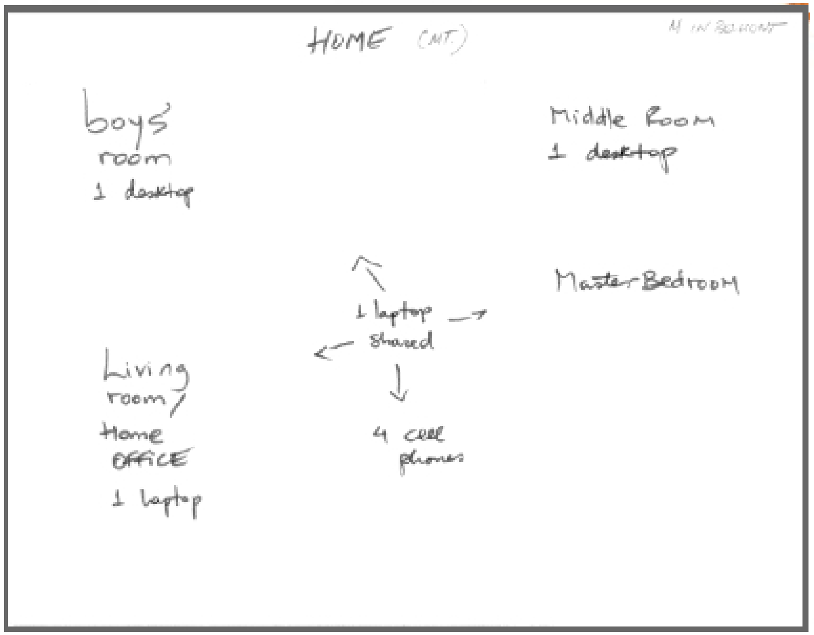
Mark Baugher
Cisco Systems
mbaugher@cisco.com

Overview

- Cisco has a major presence in home networking
  - Linksys is one of the world’s largest vendor of home gateways
  - New products include a media NAS and whole-home audio
- Home network vendors like Cisco have 2 big problems
  - The return rate of all brands of home network gear is huge
  - We want to sell new products for storage, media, remote access
- We learned some things from an ethnographic study
  - I’ll briefly cover some lessons about security that we learned

Security was a small part of this as-yet unpublished study, but through the lens of security, we gained some insights into how people think about and act upon perceived problems on the home network.

Customers are Challenged/Overwhelmed



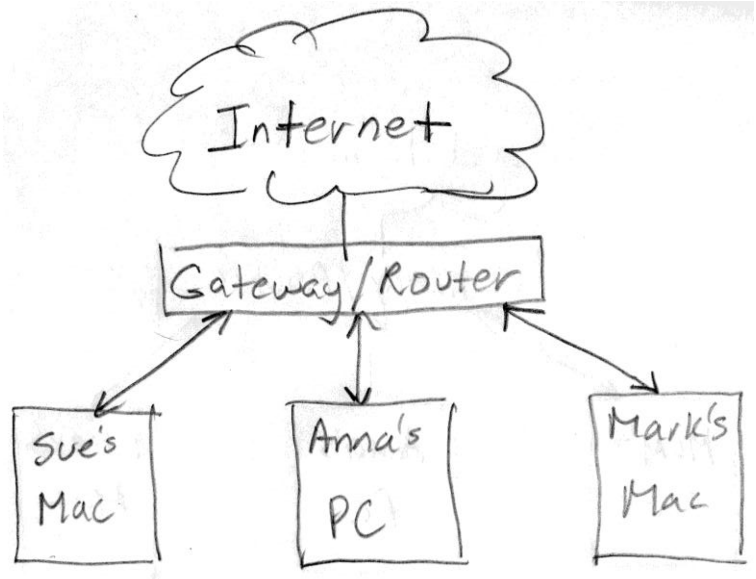
Participants in our study were asked to draw a picture of their home network

- Home networking products are much like enterprise networking products
- Enterprise network devices are maintained by experts
- Efforts such as UPnP to make home networks “plug and play” have had mixed success – and well-publicized security problems

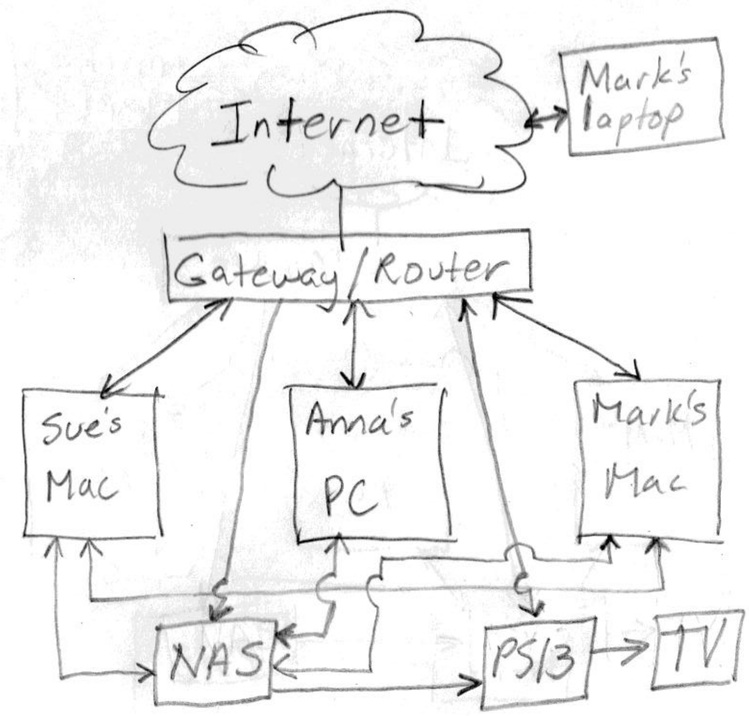
The “early adopters” who participated in our study were more sophisticated than the typical customer. For most, their network drawings tended to be more highly developed than the one shown above.

New Services Require a Paradigm Shift

Home network of web terminals



Home network of home devices



The paradigm shift to use the home network as a network exposes more problems with usability and new risks to the home network.

Home Network Risks

- UPnP, Bonjour etc. automate configuration & control

  Malware such as the Conficker virus use these features too

- Many products have easy-to-use web interfaces

  Malware such as the “Flash Attack” use CSS and CSRF exploits

- Customers say they don’t care about security

  All 10 households in our ethno study said that in a questionnaire

  Later, each showed some “security behaviors” when observed

The ethnographic study of early adopters in the SF Bay Area was led by B. Dalal and D.K. Smetters of PARC in 2008. Following a questionnaire, we interviewed and observed 37 people from 10 households.

Security Behaviors We Observed

User Action	Perceived Threat(s)	Effective?
WLAN privacy	War drivers/neighbor	Yes
Run anti-virus S/W	Virus/malware	Yes
Switch to Mac	Virus/malware	Temporarily
Loan PCs to guests	Virus/malware	Probably not
FOB passwords storage	Virus/malware	Probably not
Disconnect devices (such as web cams)	Internet snooping	Yes
Short-term logging	Attack via open WLAN; government snooping	Yes

The lesson is that people who say they are not interested in security may often take concrete steps to perceived threats on the home network.

Some Observations from the Study

- Most concern was on viruses

  This threat is well known and widely experienced

- Most wireless LANs had access controls

  Some were grappling with giving guests appropriate access

- Most user actions were very concrete

  Loaner PCs, password storage devices, disconnecting devices

In most households, we found users taking concrete actions that allow them to physically manipulate network devices to achieve some desired affect – or to attempt to do so.

Conclusion: Home Networking “Tussles”

- Automation versus Human Action

  “Plug and play” networks may offer people too little control

- Function versus Security

  More function brings more complexity and risks

- Standardization versus Innovation

  Open interfaces promote innovation, but not below the interface

- Legislation versus Engineering

  We tend to ignore the political dimension of privacy and security

Interoperability is of course a real need for home network devices, but premature standardization of ill-advised functions lock users and vendors into an unacceptable status quo.

Acknowledgements

- Brinda Dalal, Nathan Good, Les Nelson and Diana Smetters of PARC designed and organized the ethnographic study with help from Pete Sawyers, Kendra Harrington and Mark Baugher of Cisco
- Thanks to Bruce Davie for an interesting discussion on this presentation and on the “tussles” concept of D.D. Clark et. Al.