Jeff's Crystal Ball
(and other related matters)

Jeffrey I. Schiller

Information Services and Technology

Introduction

- Thank you for coming to a session where the agenda wasn't published!
- I'm going to do some crystal ball gazing
- And then discuss some of the problems (mostly security) that we face as we follow the smoke...

It's Time for Ubiquity!

- The network should be everywhere!
- People want it everywhere
- We have laptops, palmtops, PDAs and some even have network enabled clothing
  - (uh oh, watch out for “big brother”)

Wireless Everywhere

- Have to be careful, the word “Wireless” is used for everything from 802.11 through cell phones
- From high speed (aka 1Mb/sec) to really slow speed (SMS)
- WiMAX?

Fundamental Limitations

- The humans
- Are eyes are only so good and our hands are only so small!
- But all devices can benefit from high speed service

Drivers (Consumer)

- Most network applications can survive on modest bandwidth
- And then you get entertainment...
  - Audio
  - Video
- Entertainment will drive bandwidth requirements
  - HD movies will drive the top end

Drivers (Research)

- Research “market” is tiny winy
  - But important
- Real-time experiments generating vast amounts of data which needs to move globally
- Physics big consumer here

Wireless Deployment

- entrepreneurial newcomers vs. Entrenched Interests
- Newcomers: “Gigabit access everywhere for free (or for a small fee)”
- Entrenched Interests: “High speed is 300Kb/sec and you get 600 free minutes a month...”
- Big battle here
  - Entrenched interests may loose, I hope so

Wireless (Data) Technologies

- 802.11(a/b/g): Here today, deployed on campus
  - Independently owned “hot spots.” Some free some not
  - campus and enterprise deployable
    - No license needed
- EVDO: Cell system based
  - Owned by few carriers
  - Wide area
  - Slower then 802.11, but faster then previous cell based tech. (300-900Kb/sec)

Wireless (Data) Technologies

- WiMAX: Similar to 802.11 technology, next generation
  - licensed or unlicensed spectrum
  - Probably over-broad term
    - If you get a WiMAX card will it talk to all WiMAX networks? (I don't know)
- Big claim: Wide Area Coverage
  - this implies licensed spectrum and carrier control

Prognosis

- We will continue to see a mixture of networking technologies
- 802.11(b/g/a) will continue to grow (there is the issue of which of the sub-standards “g” or “a” will dominate) [I have an a/b/g card!]
- WiMAX and EVDO are still works in progress
  - For now, they provide a different service, for a different price

MIT's Network

- THIS IS NOT AN OFFICIAL IS&T STATEMENT!!!
- I see the network evolving into two or three different networks
- Commodity: What we use to get most of our work down
  - This will primarily be a wireless network
  - Will offer 10-100Mb/sec capability
- Research: For selected high speed needs
  - Will not be ubiquitous on campus
  - Will be separately “cost recovered”

Will we have an optical network?

- There are national initiatives to build an “optical” network
- Instead of an Internet Protocol network, you get a “lambda” to your destination
  - Do whatever you want with it
- This is EXPENSIVE technology
- Not clear that it offers anything more beyond what could be offered by a high speed IP network
- Too early to tell if this is “real”

Security Privacy and the Internet

- Ubiquitous networking introduces some interesting security problem
- Can you trust the network?
  - Simple answer: NO
- In the “good ole days” The network (phone) was and could be trusted
- “Bad guys” didn't in general have access to enough of it to matter
- The Internet, by contrast is an untrustable technology

Why no trust?

- There is no single administrative entity
- In general you do not know where your data is going or who has access to it.
- Wireless makes this worse
  - "Evil Twin" Attack
- You cannot differentiate the good actors from the bad actors
  - And there is a range between them!

Stupid Security

- WEP/WPA/802.1x
  - They protect the wireless portion (which is good)
  - But encryption ends at the access point, and you cannot trust the guy who runs that!
- Public Key Infrastructure (PKI) doesn't help
  - Expect the PKI companies, who are hungry to start proposing their technologies as the answer (never mind the question)
- Airport Screeners: (Oops, wrong talk...)

Why PKI doesn't help

- Basic idea behind PKI is having “Trust Anchors” organizations that you trust
- You then get a certificate path from where you are to a trust anchor
- practical experience: This is notoriously hard to do
- On a global scale, one organization cannot declare who is trusted
  - They can only declare who paid them $$$!
- PKI can bind an action to a name, but what does the name mean?

Example

- You go to the airport and open your laptop and associate with a local wireless network
- You discover that you have to register (read: pay) to use the network. The network claims to be owned by “Airport Networks Unlimited”
- Well who is that? Is that the airport officially, or the guy three chairs down with an access point in his briefcase whose purpose is to steal your credit card number?!

What can you do?

- Developers: Assume that the network is untrusted (because it is!)
- Develop applications that encryption all information from client to server
- Web based applications should use “https” URL's
  - Although some subtlety is required, this isn't hard to do

What can you do?

- Users: Beware of “http” applications that ask for interesting information
- NEVER FILL OUT A FORM IN E-MAIL
  - This is almost always a “phishing” attack
- Use the MIT VPN service to access MIT services, particularly when traveling
  - more on this in a bit
- Use virtual credit cards

Virtual Credit Cards

- Some credit card companies offer these (AT&T Universal does)
- You get a “one time” use credit card from their website
  - Obviously doesn't help if what you want it for is to pay for internet access, that you don't have yet!

VPN

- Virtual Private Network
- Sets up an encrypted “tunnel” through the public network
- Its like you are on MIT's network, even when you are not
  - You do get a net 18 address
- You wind up with a direct path to a “cleaner” part of the MIT network

The network is not equal...

- There are “dirty” portions of the MIT network, and cleaner portions.
- Most building networks are “dirty”
  - We have no idea what is connected to them, and anything can be turned into an eavesdropping box
- The Backbone is “clean”
  - Only a limited number of things directly connected and we have control of them
- Server networks are mostly clean

More observations

- Federated Authentication is really needed
- But will it take off in time?
  - Its SSL vs. SET all over again, but worse.
- Ad-hoc federation is already happening, and it is a security disaster waiting to happen!
- Example: IPASS and “Education First”
- You give your “credentials” (read: password) to foreign services to get access to resources

We have authentication technology

- Kerberos, X.509 certificates all have the feature that your password (or other secret) isn't sent over the network to prove your identity
- SAML (Security Assertion Markup Language) is a big help
  - Foundation of Federated Identity
- Expedia Gets it right
  - When ready, you will be able to safely authenticate without revealing your password

Too many federations now...

- Shibboleth, Liberty Alliance, whatever Microsoft is currently doing...
- All do the same thing, but differently!
- Everyone wants to be the infrastructure... so we all loose as the “default” is passwords again

Recent “issues”

- Too many cases of personal information being compromised
- Congress may get into the act
- PKI Companies are likely lobbying to make their technology required by law
  - But it doesn't solve the problem
  - Congress doesn't know that

Conclusions...

- Networking will be ubiquitous
- Wireless will likely be the medium
- Security, as always, isn't on par
- So we will go through some “bad years” security wise
- We will have to fix the security problems, or have them “fixed” for us.
- So is the glass half full (yeah, networking everywhere) or half empty (oops, my SSN everywhere...)