BEFORE WE START

tech news of interest

- From: Doug Budge
- Let there be Li-Fi: Meet the man who's bringing connectivity to the world through LED
  - Li-Fi: bi-directional networked wireless communication using visible light
  - Connectivity through simple LED bulbs
    - connect to Internet by being within range of LED beam
  - Li-Fi signals: narrowly focused "beams"
    - don't go through walls
  - Security: separate up and down links, eavesdrop: in same room..
  - Use cases:
    - content constrained through "fencing": constrain what data is received by whom
    - spotlights in room: constant connectivity (wifi-like)
    - reading light in airplane..
- http://thenextweb.com/insider/2014/08/21/purelifi-li-fi-vlc-led/

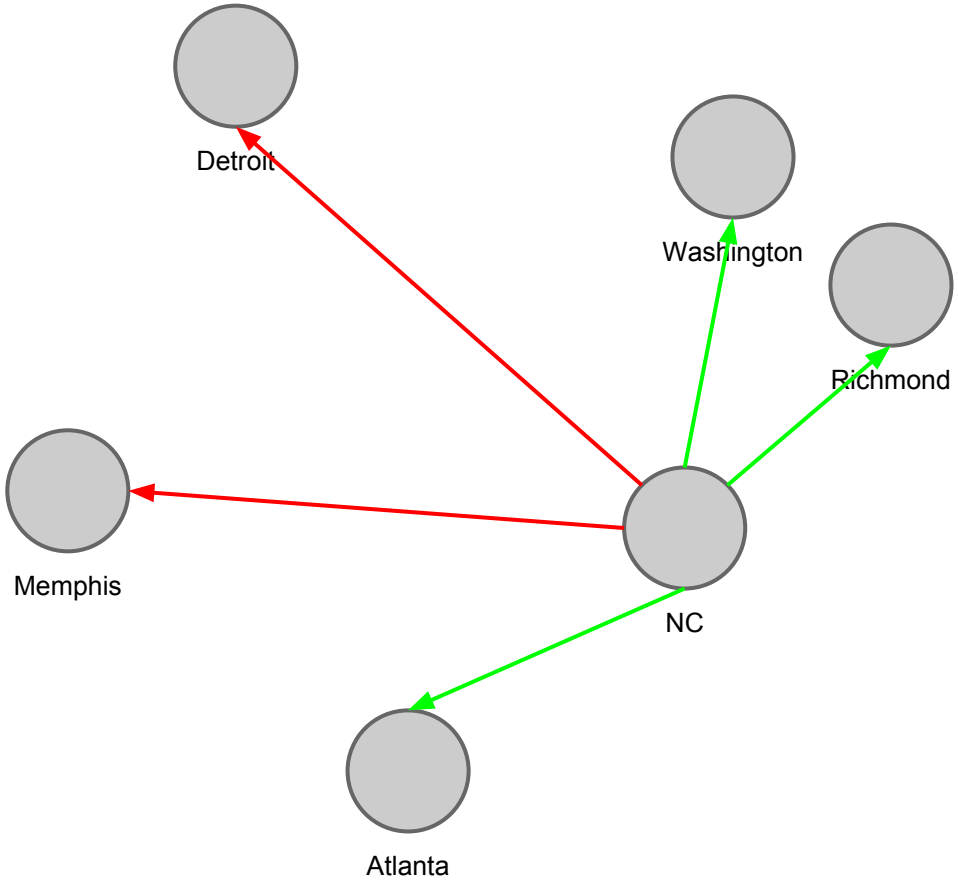
From Kohl Riekhof:

“Spookiness” Confirmed by the First Loophole-free Quantum Test

- Einstein’s theory of ‘hidden variables’ was recently disproved*
- This means that observing one subatomic particle reveals the state of another one regardless of distance between them.
- So, two parties could have entangled particles and use them as the ‘secret’ in their cryptography
- It would be very difficult to intercept and/or tamper with this secret
- MOST IMPORTANTLY this new development proves that if someone did intercept it, both parties would immediately know.
- This was believed to be possible but too uncertain for cryptography until now.
- http://fqxi.org/community/forum/topic/2581

From Guru Annasamymani:

The case of 500-mile email



Privacy Issues in Windows Operating System (From: Praveen Thiraviyarathinam)

- Windows Operating System is one of the commonly used OS in the world.
- Microsoft recently released the version Windows 10.
- Major concern of users upgrading to Windows 10 is the data privacy issue.
- Windows 10 has by default enabled the data tracking and usage tracking details.
- The updates released by Microsoft such as kb3068708, kb3022345, kb3075249 and kb3080149 basically introduces the Diagnostics and Telemetry tracking service for the older Windows versions too.

How to Stop Data Collection in older versions of Windows

The update KB3068708 mentions two domains which Microsoft is deploying to send the data it has collected to. These domains are:

1. vortex-win.data.microsoft.com
2. settings-win.data.microsoft.com

So to stop this process, simply add these domains to the HOSTS file and they will be blocked completely.

Alternately, the best method to avoid data tracking if the four updates have already been installed on your PC would be to delete them completely. To do this, navigate to Control Panel > View the updates installed and remove the four.

Once you have done this ensure that you "hide" the updates so that they do not reinstall once the PC has been rebooted. To hide you need to do the following:

Step 1: In the list of updates right-click the update you do not want to see.

Step 2: Opt for Hide Update.

PLAN FOR TODAY

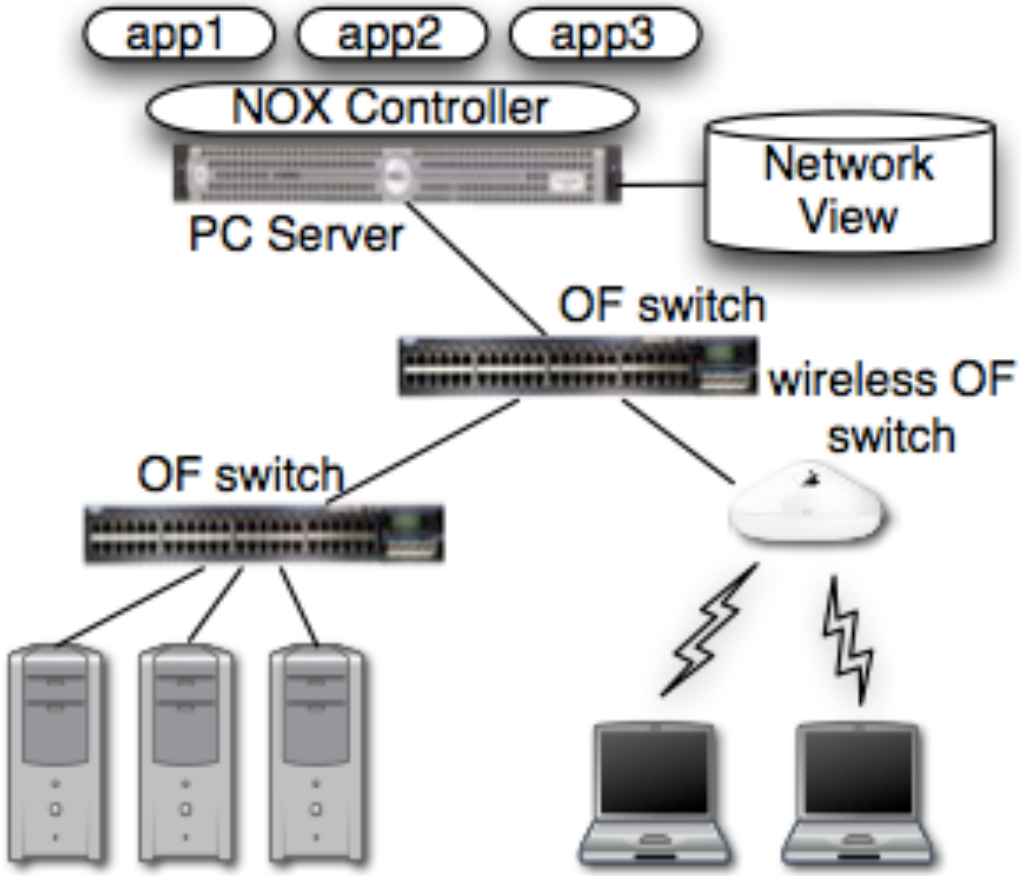
plan for today

- Paper discussion
- Review course project expectations
- Discuss matchmaking process

- Background review…

- For Wednesday
  - Plan to post project ideas by tomorrow
  - Read it before class on Wednesday
    - We will discuss it in class

NOX


app1
app2
app3
NOX Controller
Network View
PC Server
OF switch
wireless OF switch
OF switch

VLAN tagging

```
# On user authentication, statically setup VLAN tagging
# rules at the user's first hop switch
def setup_user_vlan(dp, user, port, host):
    vlanid = user_to_vlan_function(user)
    # For packets from the user, add a VLAN tag
    attr_out[IN_PORT] = port
    attr_out[DL_SRC] = nox.reverse_resolve(host).mac
    action_out = [(nox.OUTPUT, (0, nox.FLOOD)),
                  (nox.ADD_VLAN, (vlanid))]
    install_datapath_flow(dp, attr_out, action_out)
    # For packets to the user with the VLAN tag, remove it
    attr_in[DL_DST] = nox.reverse_resolve(host).mac
    attr_in[DL_VLAN] = vlanid
    action_in = [(nox.OUTPUT, (0, nox.FLOOD)),
                 (nox.DEL_VLAN)]
    install_datapath_flow(dp, attr_in, action_in)
nox.register_for_user_authentication(setup_user_vlan)
```

Scan detection

```
scans = defaultdict(dict)
def check_for_scans(dp, inport, packet):
    dstid = nox.resolve_host_dest(packet)
    if dstid == None:
        scans[packet.l2.srcaddr][packet.l2.dstaddr] = 1
        if packet.l3 != None:
            scans[packet.l2.srcaddr][packet.l3.dstaddr] = 1
        if len(scans[packet.l2.srcaddr].keys()) > THRESHOLD:
            print nox.resolve_user_source_name(packet)
            print nox.resolve_host_source_name(packet)
# To be called on all packet-in events
nox.register_for_packet_in(check_for_scans)
```

discussion question

- Make groups of two or three
- Select a note taker
- Take 1 minute to discuss:

List as many strengths and weaknesses of the "NOX: Towards an Operating System for Networks" as you can

discussion question

- Make groups of two or three
- Select a note taker
- Take 1 minute to discuss:

Given your current understanding of NOX and OpenFlow (versus more traditional networking), what ideas for future work can you think of?

Course project

- Address a significant networking problem
- Be performed in groups of two
  - groups of three also allowed with permission
  - singles only in exceptional circumstances
  - **means that there will be a human aspect involved with the project…**
- Will provide a number of possible projects
  - own project also allowed with permission
- **Important:**
  - **The project ideas are the intellectual property of whoever generated it. (Typically the listed mentor(s).) These ideas are to be explored in collaboration with the mentors only (whether in the course or otherwise). And should not to be distributed to anyone else.**
- Final "deliverable" will be project presentation and short paper
- Paper should be suitable for submission to workshop or poster session at conference
  - clear problem definition and motivation, related work, proposed solution, initial results and/or steps towards solution
  - should target a specific Call for Papers (CFP) (even if not current)
- Be willing to take risks
- **Expect that many projects WILL be submitted for publication**

Project matchmaking process

- Mostly want folks to work on something they are excited about
- Have a few other constraints
  - Want you to be successful in the project you choose
  - Want projects to succeed
  - Want teams to work out
  - Would like to include other mentors
  - Don’t want to over manage the process (Really!)

The "Process"

- Send me email by Friday night with title: **CS6480 project**
  - Plan is to finalize this over the weekend
- **Send to my cs account directly (kobus@cs.utah.edu)**
  - NOT via Canvas
- Include in the email:
  - At least three projects you are interested in working on
    - In priority order
  - For each project indicate your level of interest
    - E.g., very excited about this one, all equally good, only if first choice don't work out etc.
  - If you want to do your own project you also need to send me email
    - Include a brief description of what you want to do
    - Will set up some time to meet with you to discuss
  - If you have someone you want to work with as a team include their name
    - Both of you have to send me email
    - If team only applies if you get a certain project indicate that

Projects discussion

- Things to consider as you read project ideas:
  - Problem scope:
    - Well defined vs. open ended
  - Risk:
    - Sure thing vs. possible dud
  - Potential for publication
    - researchy vs engineering
  - Type:
    - Data analysis, prototype, architectural, simulation
  - Area:
    - SDN, security, cloud, OS, network management, protocol, application
  - Size:
    - Potential for sub-projects
    - Potential for "finishing"
  - Interest level:
  - Tools:
    - Mininet, Emulab, simulation environment
  - Mentors: