Introduction to Security with respect to Campus Networks

12th June 2018

Workshop on Network Security - 2018

Thilina Pathirana

Based on and Credits: APNIC, APRICOT, NSRC, SANOG Security Tracks

What is a REN

- REN => Research and Education Network
- High bandwidth, Low Latency, open networks with **no** Filtering
- Enable research or services that could not be accomplished otherwise
- Our goal is to build networking capacity to support Research and Education
  - Remember: University = Research & Education
- Buying all service from your local ISP is a losing game – you will spend more money and not have control of the network
- The Campus Network is the foundation for all Research and Education activity
- Without a good campus network, the Research and Education Network can't work as well as it should

What is a Campus Network

- High bandwidth Networks – can be 10G , 40G or may be 100G
- Can be multiple acres of ground, multiple multi-story buildings
- Low latency fiber networks
- High number of L3, L2 devices.
- Can be wired, wireless or both
- High number of services
  - Public
  - Confidential
  - Valuable, Copyrighted
- Large research data volumes
- High User Base – technical / non-technical

Security in Campus Networks

- Securing and monitoring the security of a campus network is difficult
- Campus networks need to be fairly open
- Always will have viruses, attacks, and people generally acting bad

You get a call from some agency (eg. LEARN/ CERT) saying that they have a report that one of your hosts is participating in a Denial of Service (DoS) attack

  – What do you do?
  – How do you find the host (very hard if NAT)?

Security in Campus Networks – the key things

- Assets – What are we protecting?

  - Many sorts of targets:
    - Network infrastructure
    - Network services
    - Application services(money!)
    - Data
    - User machines

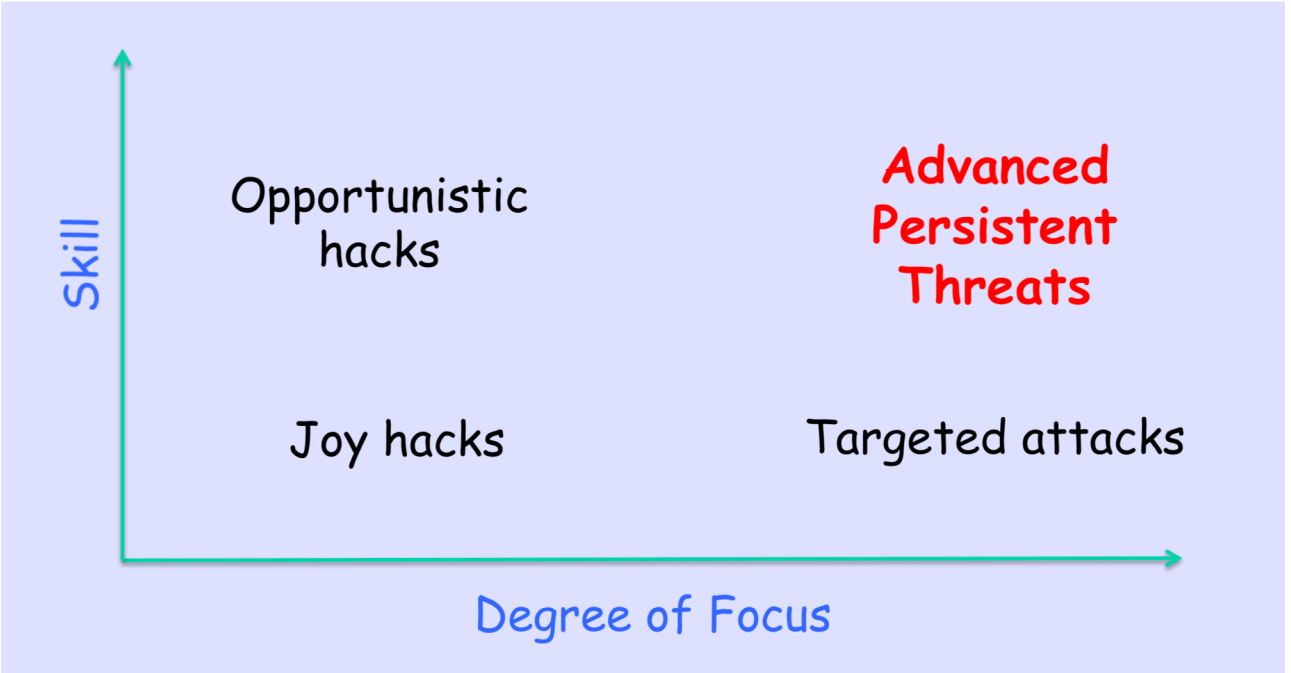
- Attackers – From whom?
- Attacks – Common Attacks
- Defenses - Defenses

Security in Campus Networks – the key things

- Assets – What are we protecting?
- Attackers – From whom?
  - Script kiddies: little real ability, but can cause damage if you're careless
  - Money makers: hack into machines; turn them into spam engines; etc.
  - Government intelligence agencies, AKA Nation State Adversaries
- Attacks – Common Attacks
- Defenses - Defenses

Security in Campus Networks – the key things

- Assets – What are we protecting?
- Attackers – From whom?
- Attacks – Common Attacks – The Threat matrix



- Defenses - Defenses

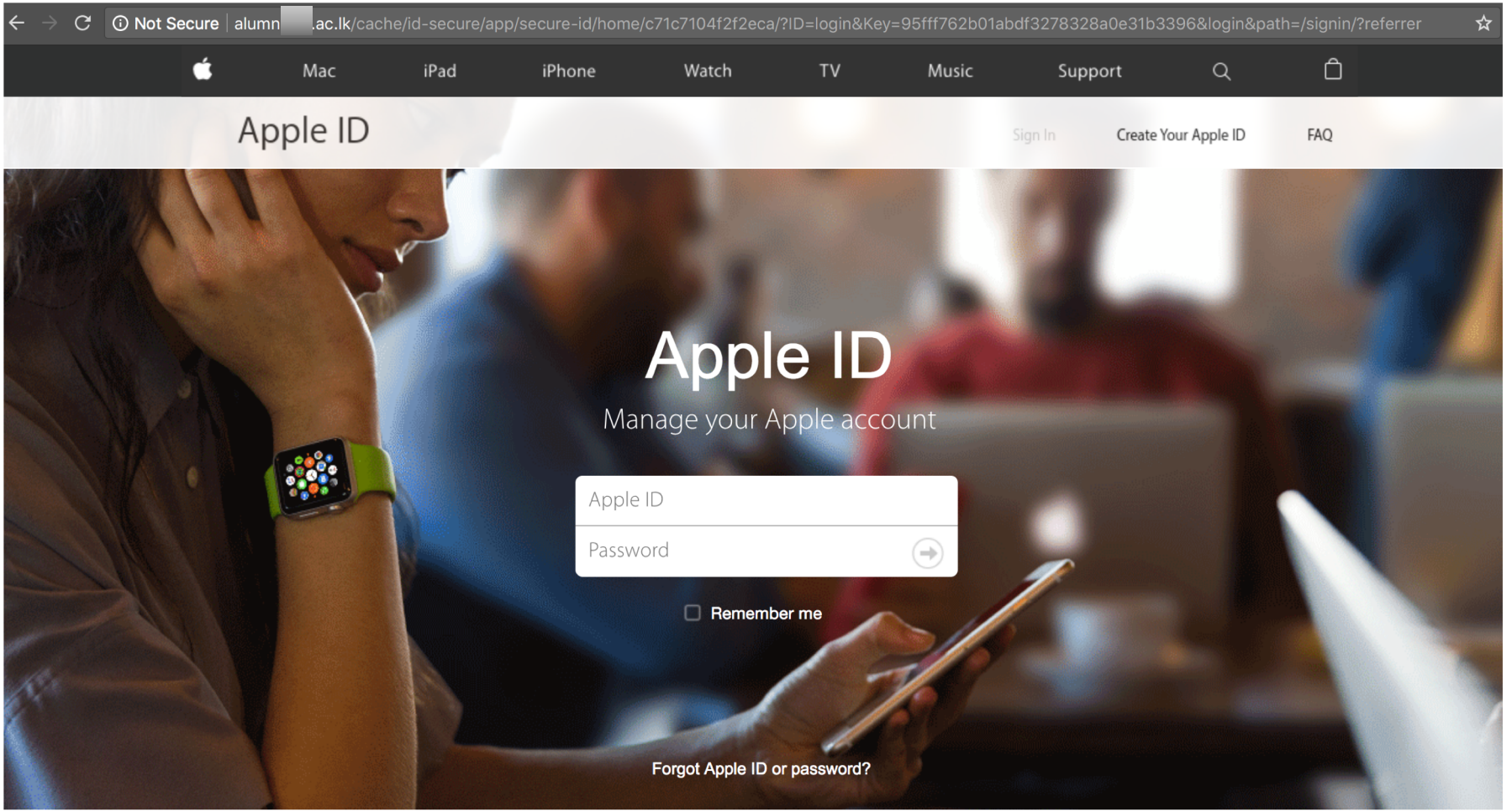
Security in Campus Networks – the key things

Joy Hacks:

- ⚠ Hacks done for fun, with little skill
- ⚠ Some chance for damage, especially on unpatched machines
- ⚠ Targets are random; no particular risk to your data (at least if it's backed up)
- ⚠ Ordinary care will suffice
- ⚠ Most hackers start this way
- ⚠ Common in many Campus Networks

Security in Campus Networks – the key things

Something very recent:



Security in Campus Networks – the key things

Opportunistic Hacks:

- ⚠ Most phishers, virus writers, etc.
- ⚠ Often quite skilled, but don't care much whom they hit
- ⚠ May have some "zero-days" attacks
- ⚠ The effects are random but can be serious
- ⚠ Consequences: bank account theft, Social account theft, machines turned into bots, etc.

Have your users reported these kind of attacks???

Security in Campus Networks – the key things

Recent Example:

We are happy to inform you that you have been registered to participate in the workshop on "**Workshop on Network Security**" going to be at the Information Technology Center, University of Peradeniya from 12th to 14th June 2018.

The Workshop will start at 08.30 am.

Detailed program agenda can be found at https://ws.learn.ac.lk/wiki/netsec2018. We would also like to remind you to bring a laptop (20GB free disk space and at least 4GB RAM).

```
We are happy to inform you that you have been registered to participate in
the workshop on "*Workshop on Network Security*" going to be at the
*Information
Technology Center, University of Peradeniya* from 12th to 14th June 2018.

The Workshop will start at 08.30 am.

Detailed program agenda can be found at
https://ws.learn.ac.lk/wiki/netsec2018
<https://ws.learn.ac.lk/wiki/ipv62017>. We would also like to remind you to
bring a laptop (20GB free disk space and at least 4GB RAM).
```

Security in Campus Networks – the key things

Targeted Attacks:

- ⚠ Attackers want you. Sometimes, you have something they want;
- ⚠ other times, it's someone with a grudge
- ⚠ Background research—learn a lot about the target
- ⚠ May do physical reconnaissance
- ⚠ Watch for things like "spear-phishing" or other carefully-targeted attacks

Have your users reported these kind of attacks???

Security in Campus Networks – the key things

Advanced Persistent Threats (APT):

- ⚠ Very skillful attackers who are aiming at particular targets
- ⚠ Sometimes — though not always — working for a nation-state
- ⚠ Very, very hard to defend against them
- ⚠ May use non-cyber means, including burglary, bribery, and blackmail
- ⚠ Note: many lesser attacks blamed on APTs

Have your users reported these kind of attacks???

Security in Campus Networks – the key things

- Assets – What are we protecting?
- Attackers – From whom?
- Attacks – Common Attacks
- Defenses – Defenses
  - Defense strategies depend on the class of attacker, and what you're trying to protect
  - Tactics that keep out script kiddies won't keep out an intelligence agency
  - But stronger defenses are often much more expensive, and cause great inconvenience

Defense Strategies

- Joy Hackers:
  - By definition, joy hackers use existing tools that target known holes
    - Patches exist for most of these holes
    - These hacking tools are known to AV companies
  - The best defense is staying up to date with patches
  - Also, keep antivirus software up to date
  - Ordinary enterprise-grade firewalls will also repel them

Defense Strategies

- Opportunistic Hackers:
  - Sophisticated techniques used
    - Possibly even some 0-days
  - You may need multiple layers of defense
    - Up-to-date patches and anti-virus
    - Multiple firewalls
    - Intrusion detection
    - Lots of attention to logfiles
  - Goal: contain the attack

Defense Strategies

- Targeted Attacks:
  - Targeted attacks exploit knowledge; try to block or detect the reconnaissance
  - Security procedures matters a lot
  - How do you respond to phone callers?
  - What do people do with unexpected attachments?
  - USBs in the parking lot
  - Hardest case: disgruntled employee or ex-employee

Defense Strategies

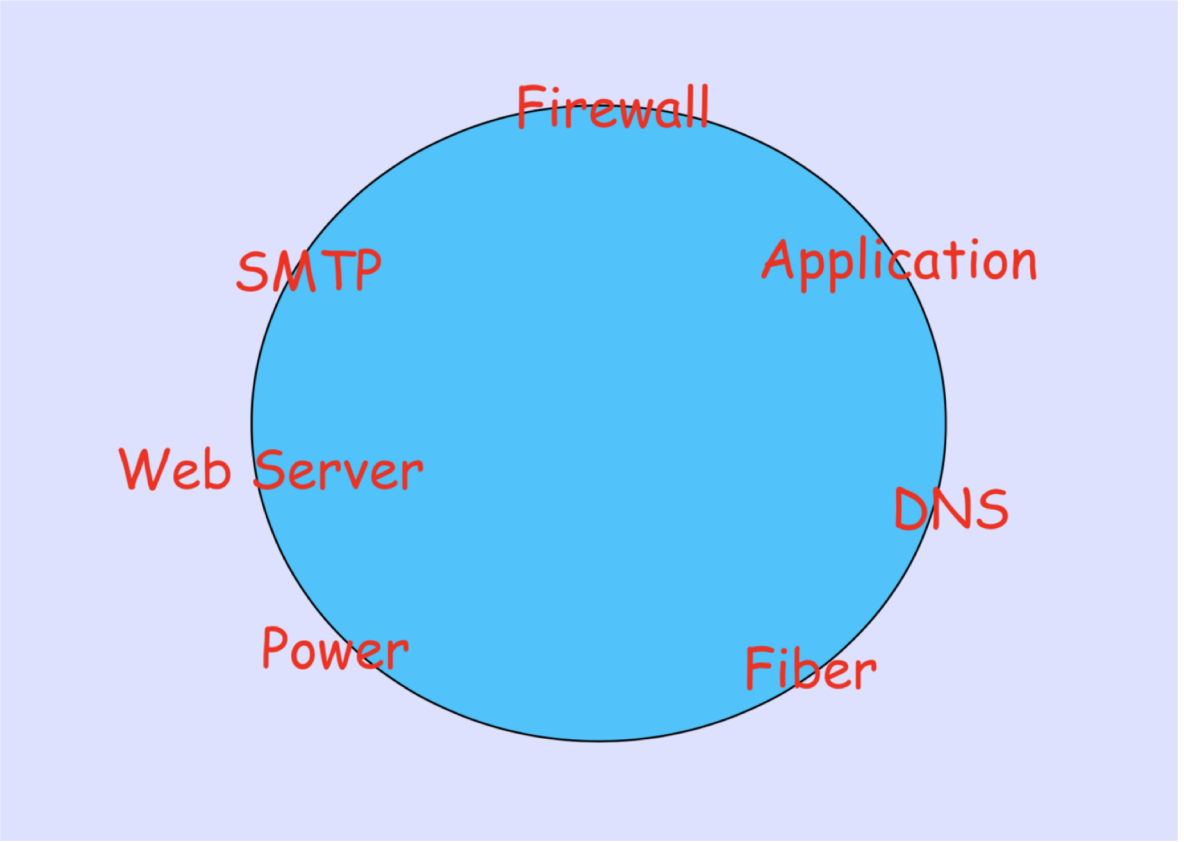
- Advanced Persistent Threats :
  - Very, very hard problem!
  - Use all of the previous defenses
  - There are no sure answers — even air gaps aren't sufficient (Google Stuxnet)
  - Pay special attention to procedures
  - Investigate all oddities

Defense Strategies

- Don’t use the same defenses for everything
- Layer them; protect valuable systems more carefully
- Maybe you can’t afford to encrypt everything—but you probably can encrypt all communications among and to/from your high-value machines
- The defender has to think about the entire perimeter, all the weakness
- Because the attacker has to find only one weakness and it is not a good news for defenders

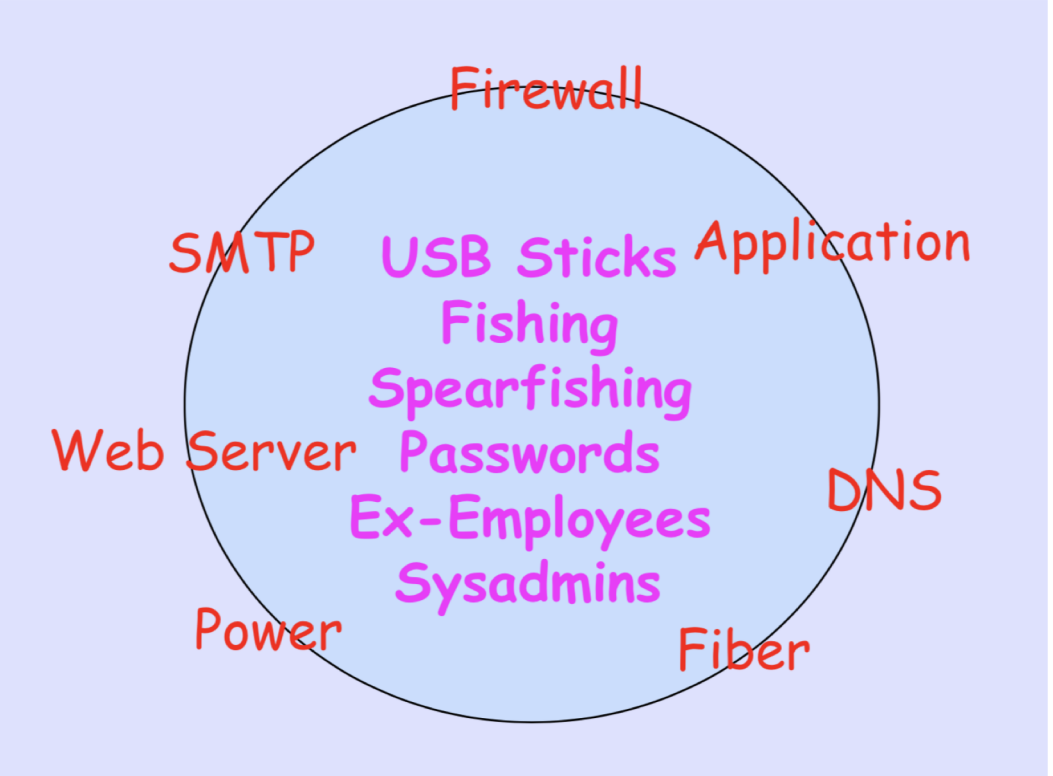
Attack Surface

- You have to cover all



Attack Surface

- Not only the perimeter but also;



Security in a process

You can never achieve security – it is a process that you have to continually work on

– Assessment – what is at risk
– Protection – efforts to mitigate risk
– Detection – detect intrusions or problem
– Response – respond to intrusion or problem

– Do it all over again

Thank You

Thilina Pathirana/LEARN

thilina@learn.ac.lk
www.thilinapathirana.xyz

Based on and Credits: APNIC, APRICOT, NSRC, SANOG Security Tracks