Security Problems of an Eleven Year Old
And How to Solve Them
(v2 - 2016-10-18)
About Me

- I’m eleven, and in the 6th grade
- I started coding when I was six
- I’ve done eight online university courses
  - Python programming, Linux, networking, economics, and symbolic logic
  - ...and some others in progress
- I’ve presented at NorthSec 2016, Pycon Canada 2015, and at the Montreal Python Group
- Today, I’m going to talk about the security problems I face in my life as an eleven year old
Threat Model For the Life of an Eleven Year Old

**Threat #1**: Sibling takes over my laptop and my web accounts

**Threat #2**: Hackers take over my cloud server

**Threat #3**: Sibling enters my room and messes with my stuff

**Threat #4**: My Dad implements Internet filtering

**Threat #5**: My Dad programs my wifi to turn off at 7:30pm every night

Sibling does #3 **A LOT**, and Evil Dad has done #4 and #5...
There are lots of methods, but I decided to use STRIDE and DREAD.

You guys all probably know what these are, but I’ll explain anyway.

STRIDE analyzes threats based on possible methods of attack:
- Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege.

DREAD produces a risk score between one and ten based on the average of five aspects of the threat:
- Damage potential, Reproducibility, Exploitability, Affected Users, Discoverability.
Threat #1: Analysis

**Description:** Sibling takes over my laptop and my web accounts

**S:** Sibling could impersonate me after she had compromised my passwords by shoulder surfing, or if she found my laptop unlocked, possibly with my accounts open

**T:** Sibling probably not capable of SQL injection, or TLS MITM...

**R:** Not applicable

**I:** Would prefer sibling not know my bank balance, email addresses of my friends, etc.

**D:** Sibling could lock me out of my laptop or web accounts

**E:** Sibling could leverage access to laptop to get access to web accounts

**DREAD score:** \( (5 + 5 + 10 + 5 + 5) / 5 = 6 \)
Threat #2: Analysis

**Description:** Hackers take over my cloud server

**S:** If I use strong credentials, and protect them well, this should not be a major risk

**T:** Risk of tampering by cloud provider staff, or by attackers who compromise cloud provider

**R:** I have some basic logging, but it’s not tamper-resistant

**I:** Nothing of much value stored on my server

**D:** Doable, but worst consequence is a minor inconvenience

**E:** I do operate some unprivileged services, they need to be kept up to date and protected

**DREAD Score:** \( \frac{5 + 5 + 5 + 10 + 10}{5} = 7 \)
**Threat #3: Analysis**

**Description:** Sibling enters my room and messes with my stuff

**S:** All she really has to do is walk in, there’s no credential check at the door (maybe I should hire a border guard?)

**T:** If sibling can enter, I don’t have anything to stop her from tampering

**R:** Denial is easy unless I implement some form of logging

**I:** Not applicable — I don’t have any secrets

**D:** I guess she could close the door and lock me out

**E:** My debit card is in there!

**DREAD Score:** \((10 + 5 + 10 + 10 + 10) / 5 = 9\)
**Threat #4: Analysis**

**Description:** My Dad implements Internet filtering

**S:** Not applicable

**T:** My Internet traffic is definitely being tampered with. This is obviously a violation of my basic human rights!

**R:** Not applicable

**I:** Not applicable

**D:** That’s exactly what this is!

**E:** This does give my parents more power :-(

**DREAD Score:** \( (5 + 10 + 10 + 5 + 10) = 8 \)
**Threat #5: Analysis**

**Description:** My Dad programs my wifi to turn off at 7:30pm every night

**S:** Not applicable

**T:** Not applicable

**R:** Not applicable

**I:** Not applicable

**D:** Exactly what this is. Also a human rights issue!

**E:** Again, empowers my parents :-(

**DREAD Score:** \( \frac{5 + 10 + 10 + 5 + 5}{5} = 7 \)
Threat #1: Mitigations

Threat: Sibling Takes Over Laptop and Web Accounts

- Use strong passwords (Windows, bank, Paypal, Google, Coursera, games…)
- One minute screen lock
- Use a password manager with hardware-based Device ID and strong biometrics and multi-factor authentication (hint: the one that is built in Montreal)
Threat #2: Mitigations

Threat: Hackers take over my cloud server

- Always maintain all server software up to date!
- Allow SSH access only
- Disallow root login
- Disallow password authentication
- Use ED25519 keys
- Set a strong password on my SSH key
Mitigating Threat #3: My Sibling Enters My Room Uninvited

- I must do something about this!
- Things I considered:
  - Landmines
  - Vicious dogs
  - Armed guards
- Budget issues... so:
  - Decided to build a light activated Nerf gun
Threat #3... Building the Nerf Gun Alarm System

- My design:
  - Two Edison robots
  - A Snap Circuits circuit board
  - A Nerf gun
  - Some pieces of Lego

- The idea was that if my sibling entered, a light sensor on the circuit board would set off a siren triggering the Edisons’ sound sensors. The Edisons would be programmed to then turn their wheels (their only moving parts), to somehow fire the Nerf gun through a Lego linkage.
Threat #3... Problems With the Nerf Gun Alarm System

- I remembered that I had given away the Nerf gun a few weeks before
- To replace it, I decided to use a Lego spring-loaded shooter
- It turned out not to shoot far enough
- The mechanics of the firing mechanism, with the rotating motors driving the Lego linkage, didn’t work

- So, this was what scientists call “a flop”
Threat #3... Second Idea

- Time to get high-tech!
- I decided to build a motion-activated security camera using my Raspberry Pi
- Plusses: Solves the Repudiation problem (i.e. sibling intrusion into my room without consequences)
- Minuses: Lacks the satisfaction of shooting sibling :-(

Threat #3... Building The Raspberry Pi Security Camera

- It turns out there is a Linux distro for the Pi built specifically for this, called MotionEye
- My dad bought me an SD card to put the new operating system on
- I installed an SD card formatter and Win32 Disk Imager on my laptop
Threat #3...Building The Raspberry Pi Security Camera

- Next step: install MotionEye on the SD card
- First problem: my laptop didn’t have a SD card slot, but my dad pulled some weird USB gizmo out of a drawer and that always solves everything
- Ran the Win32 Disk Imager ... elevation prompt required my Dad’s password... after elevation, the MotionEye ISO was not in the Downloads folder!
- After a few minutes of head-scratching and age-appropriate swearing, we found out that it was looking in my dad’s (the administrator’s), folders
  - Win32 Disk Imager bug!
- After that everything went smoothly
Threat #3...Building The Raspberry Pi Security Camera

- Put the imaged SD card into the Raspberry Pi
- Connected the Pi to ethernet
- It worked immediately!
- Motioneye hosts an admin webpage with which I could access it
- Tried to connect to it from my laptop, but had to get my dad to turn off wifi client isolation (more parental interference)
- After that it worked!
Threat #3… Raspberry Pi Security Camera - Settings

- Set the admin password, default is blank (not very secure for a security camera!)
- Connect to Wifi so I can remove wired Ethernet
Connect the USB camera, perform some basic configuration.

Worked right away, didn’t expect that!
Threat #3... Raspberry Pi Security Camera - Capture Setup

- Configure still image capture and movie capture
Threat #3...Raspberry Pi Security Camera - Hardening

- Turn off FTP and Samba servers
Threat #3…Raspberry Pi Security Camera - Notifications

- Uses email to send notifications to me when it sees something
Threat #3... Raspberry Pi Security Camera - Tuning

- Had to do some tuning
  - Adjust frame change threshold
  - Adjust motion gap
  - Reduced minimum frame capture from 20 to 5
  - Enable auto noise reduction and light switch detection
- My Raspberry Pi (model B) can only capture about 2 frames/sec, but that’s enough to be effective
Threat #3... Raspberry Pi Security Camera - In Use

- Caught in the act! (red boxes outline detected motion)
- Also captures reflections
Mitigating Threat #4: My Dad Limits My Internet Access

- Some sites are filtered!

- First I needed to figure out how it works...
$ dig snapchat.com
;; DiG 9.10.3-P4 <<>> snapchat.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29715
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:
;snapchat.com.                  IN      A

;; ANSWER SECTION:
snapchat.com.           0       IN      A       146.112.61.106

;; Query time: 19 msec
;; SERVER: 10.248.0.1#53(10.248.0.1)
;; WHEN: Sat Apr 23 10:31:29 EDT 2016
;; MSG SIZE  rcvd: 57
$ dig snapchat.com @8.8.8.8

; <<< DIG 9.10.3-P4 >>> snapchat.com @8.8.8.8
; global options: +cmd
; Got answer:
; ->HEADER<- opcode: QUERY, status: NOERROR, id: 50336
; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; QUESTION SECTION:
; snapchat.com. IN A

; ANSWER SECTION:
snapchat.com. 59 IN A 54.192.18.94
snapchat.com. 59 IN A 54.192.18.44
snapchat.com. 59 IN A 54.192.18.109
snapchat.com. 59 IN A 54.192.18.16
snapchat.com. 59 IN A 54.192.18.60
snapchat.com. 59 IN A 54.192.18.224
snapchat.com. 59 IN A 54.192.18.178
snapchat.com. 59 IN A 54.192.18.204

; Query time: 62 msec
; SERVER: 8.8.8.8#53(8.8.8.8)
; WHEN: Sat Apr 23 10:32:09 EDT 2016
; MSG SIZE  rcvd: 169
Threat #4... How it Works

- Using default DNS server allocated by DHCP:
  - snapchat.com. 0 IN A 146.112.61.106
  - poker.com. 0 IN A 146.112.61.106

- Using dig @8.8.8.8:
  - snapchat.com. 0 IN A 52.192.144.209 (amongst others)
  - poker.com. 0 IN A 104.28.4.103

- All DNS queries for filtered sites return 146.112.61.106!
- That is the block page of the OpenDNS filtering service
- So our router is resolving via OpenDNS, and Evil Dad has configured nasty filters
Threat #4... Idea #1

- Configure laptop to use a static DNS resolver (not the one assigned by DHCP)
- Pros:
  - Easy
  - Would work
- Cons:
  - I don’t have admin permissions on my laptop
  - Foiled again!
Threat #4... Idea #2

- Hack my laptop to get admin permissions to perform Idea #1 (static DNS resolver)
- Pros:
  - Would work
- Cons:
  - I don’t know how (yet)
  - My Dad would be mad
- So... next!
Threat #4... Idea #3

- Add sites to hosts file (C:\Windows\System32\drivers\etc\hosts)
- Pros:
  - Would work
- Cons:
  - Fairly tedious
    - Dig each site and then add it to file
  - %$!!@#$^ file permissions
  - Foiled again, again!
Threat #4... Idea #4

- I have a Linux VM with admin rights
  - I can perform Idea #1 (static DNS resolver) on my VM!
- Pros:
  - Easy
  - Works
- Cons:
  - Surfing in the VM is slow and clumsy
  - There must be a better way...
  - (Ominous musical crescendo)
Threat #4... Idea #5

- Set up a proxy server on my cloud server
- Configure browser to use it
- Pros:
  - Works
  - No VM
- Cons:
  - May take a while to set up, but should work fine
- Conclusion: Best solution
Threat #4 ... Idea #5 ... Install tinyproxy

Jake@jakerizer1:~$ apt-get install tinyproxy
E: Could not open lock file /var/lib/dpkg/lock - open (13: Permission denied)
E: Unable to lock the administration directory (/var/lib/dpkg/), are you root?
Jake@jakerizer1:~$ sudo apt-get install tinyproxy
[sudo] password for jake:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  tinyproxy
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 60.7 kB of archives.
After this operation, 202 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty/universe tinyproxy amd64 1.8.3-3ubuntu1 [60.7 kB]
Fetched 60.7 kB in 0s (448 kB/s)
Selecting previously unselected package tinyproxy.
(Reading database ... 93090 files and directories currently installed.)
Preparing to unpack .../tinyproxy_1.8.3-3ubuntu1_amd64.deb ...
Unpacking tinyproxy (1.8.3-3ubuntu1) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Processing triggers for ureadahead (0.100.0-16) ...
ureadahead will be reprofiled on next reboot
Setting up tinyproxy (1.8.3-3ubuntu1) ...
Starting tinyproxy: tinyproxy.
Processing triggers for ureadahead (0.100.0-16) ...
But it didn’t work:

The proxy server is refusing connections

Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.
Needed this in /etc/tinyproxy.conf:

```
# Allow: Customization of authorization controls. If there are any
# access control keywords then the default action is to DENY. Otherwise,
# the default action is ALLOW.
#
# The order of the controls are important. All incoming connections are
# tested against the controls based on order.
#
Allow 127.0.0.1
Allow 198.84.235.83
#Allow 192.168.0.0/16
#Allow 172.16.0.0/12
#Allow 10.0.0.0/8
```
Threat #4 ... Idea #5 ... Victory!
Mitigating Threat #5: My Wifi Turns off at 7:30

- Not solved yet... but I have some ideas...
  - Drill hole in wall, run surreptitious Ethernet cable into my room?
  - Find way to use the other, non timed wifi network?
  - Hack router clock?
  - Hit router with stick, hope for the best?
Thanks