Software Security: Principles

CS 161: Computer Security

Prof. David Wagner

February 3, 2014

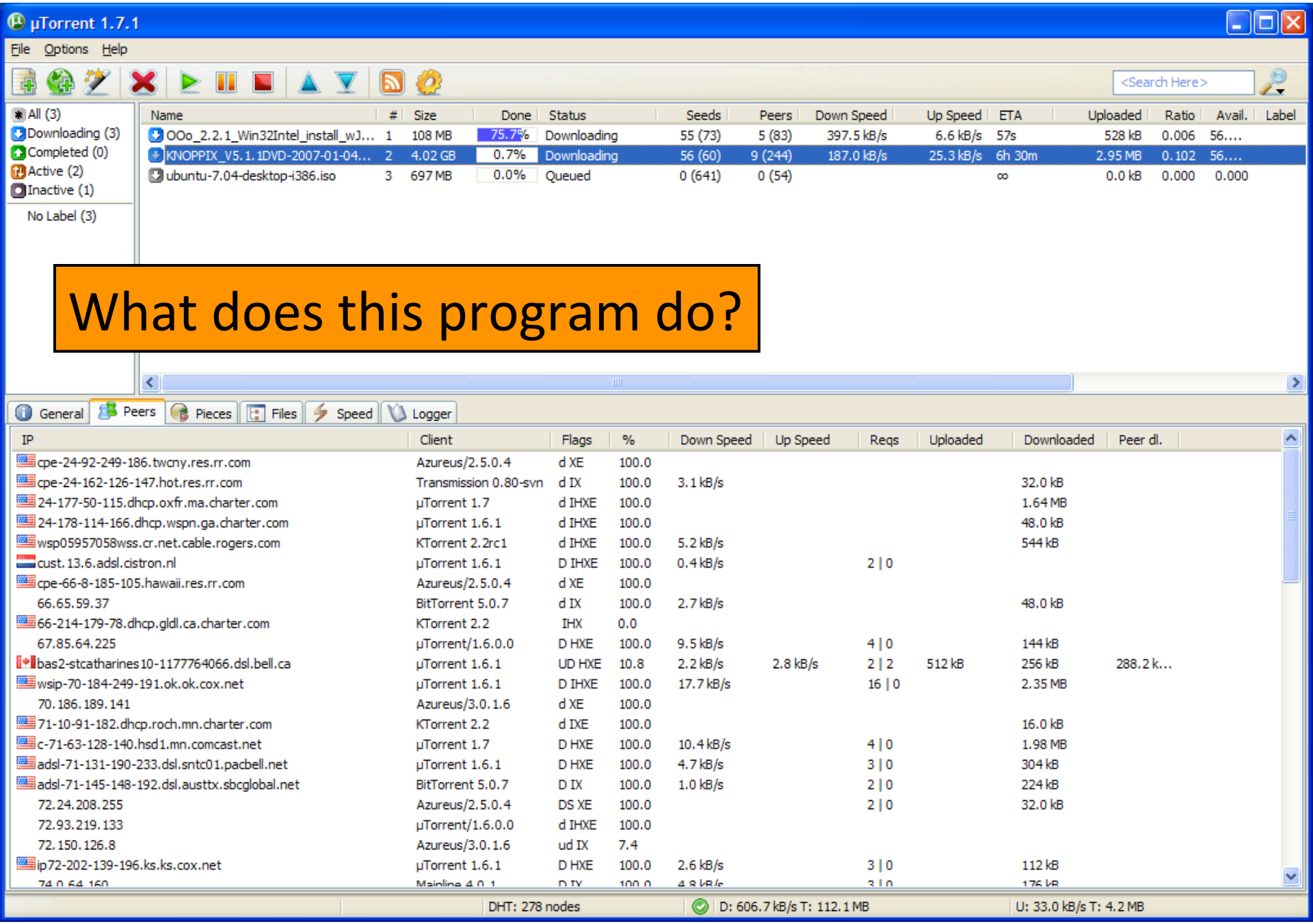
TL-15

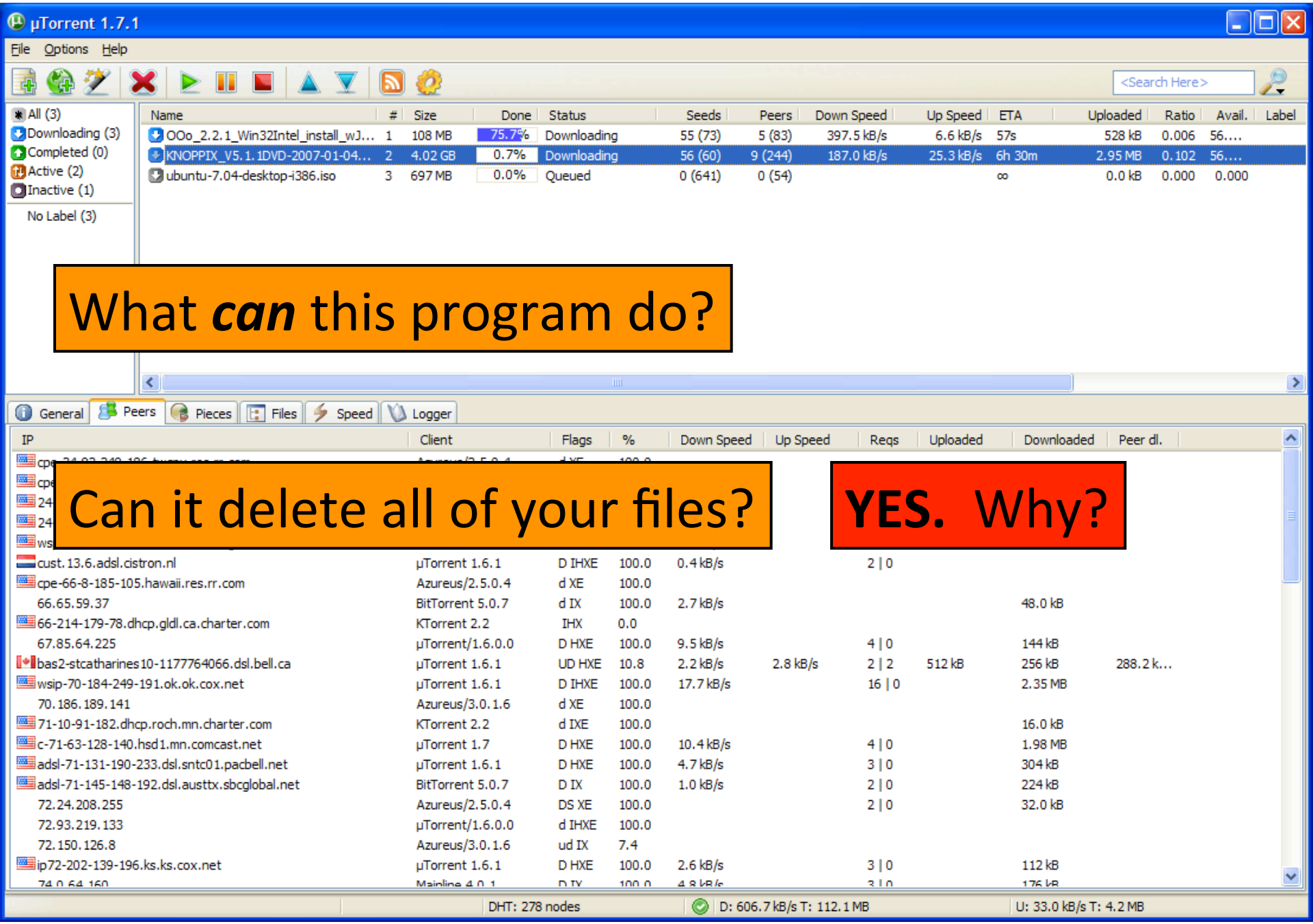
TL-30

TRTL-30

TXTL-60

“Security is economics.”


µTorrent 1.7.1
File Options Help
<Search Here>
All (3)
Downloading (3)
Completed (0)
Active (2)
Inactive (1)
No Label (3)
Name # Size Done Status Seeds Peers Down Speed Up Speed ETA Uploaded Ratio Avail. Label
OOo_2.2.1_Win32Intel_install_wJ... 1 108 MB 75.7% Downloading 55 (73) 5 (83) 397.5 kB/s 6.6 kB/s 57s 528 kB 0.006 56....
KNOPPIX_V5.1.1DVD-2007-01-04... 2 4.02 GB 0.7% Downloading 56 (60) 9 (244) 187.0 kB/s 25.3 kB/s 6h 30m 2.95 MB 0.102 56....
ubuntu-7.04-desktop-i386.iso 3 697 MB 0.0% Queued 0 (641) 0 (54) ∞ 0.0 kB 0.000 0.000
What does this program do?
General Peers Pieces Files Speed Logger
IP Client Flags % Down Speed Up Speed Reqs Uploaded Downloaded Peer dl.
cpe-24-92-249-186.twcny.res.rr.com Azureus/2.5.0.4 d XE 100.0
cpe-24-162-126-147.hot.res.rr.com Transmission 0.80-svn d IX 100.0 3.1 kB/s 32.0 kB
24-177-50-115.dhcp.oxfr.ma.charter.com µTorrent 1.7 d IHXE 100.0 1.64 MB
24-178-114-166.dhcp.wspn.ga.charter.com µTorrent 1.6.1 d IHXE 100.0 48.0 kB
wsp05957058wss.cr.net.cable.rogers.com KTorrent 2.2rc1 d IHXE 100.0 5.2 kB/s 544 kB
cust.13.6.adsl.cistron.nl µTorrent 1.6.1 D IHXE 100.0 0.4 kB/s 2 | 0
cpe-66-8-185-105.hawaii.res.rr.com Azureus/2.5.0.4 d XE 100.0
66.65.59.37 BitTorrent 5.0.7 d IX 100.0 2.7 kB/s 48.0 kB
66-214-179-78.dhcp.gldl.ca.charter.com KTorrent 2.2 IHX 0.0
67.85.64.225 µTorrent/1.6.0.0 D HXE 100.0 9.5 kB/s 4 | 0 144 kB
bas2-stcatharines10-1177764066.dsl.bell.ca µTorrent 1.6.1 UD HXE 10.8 2.2 kB/s 2.8 kB/s 2 | 2 512 kB 256 kB 288.2 k...
wsip-70-184-249-191.ok.ok.cox.net µTorrent 1.6.1 D IHXE 100.0 17.7 kB/s 16 | 0 2.35 MB
70.186.189.141 Azureus/3.0.1.6 d XE 100.0
71-10-91-182.dhcp.roch.mn.charter.com KTorrent 2.2 d IXE 100.0 16.0 kB
c-71-63-128-140.hsd1.mn.comcast.net µTorrent 1.7 D HXE 100.0 10.4 kB/s 4 | 0 1.98 MB
adsl-71-131-190-233.dsl.sntc01.pacbell.net µTorrent 1.6.1 D HXE 100.0 4.7 kB/s 3 | 0 304 kB
adsl-71-145-148-192.dsl.austtx.sbcglobal.net BitTorrent 5.0.7 D IX 100.0 1.0 kB/s 2 | 0 224 kB
72.24.208.255 Azureus/2.5.0.4 DS XE 100.0 2 | 0 32.0 kB
72.93.219.133 µTorrent/1.6.0.0 d IHXE 100.0
72.150.126.8 Azureus/3.0.1.6 ud IX 7.4
ip72-202-139-196.ks.ks.cox.net µTorrent 1.6.1 D HXE 100.0 2.6 kB/s 3 | 0 112 kB
DHT: 278 nodes D: 606.7 kB/s T: 112.1 MB U: 33.0 kB/s T: 4.2 MB


µTorrent 1.7.1
File Options Help
<Search Here>
All (3)
Downloading (3)
Completed (0)
Active (2)
Inactive (1)
No Label (3)
Name # Size Done Status Seeds Peers Down Speed Up Speed ETA Uploaded Ratio Avail. Label
OOo_2.2.1_Win32Intel_install_wJ... 1 108 MB 75.7% Downloading 55 (73) 5 (83) 397.5 kB/s 6.6 kB/s 57s 528 kB 0.006 56....
KNOPPIX_V5.1.1DVD-2007-01-04... 2 4.02 GB 0.7% Downloading 56 (60) 9 (244) 187.0 kB/s 25.3 kB/s 6h 30m 2.95 MB 0.102 56....
ubuntu-7.04-desktop-i386.iso 3 697 MB 0.0% Queued 0 (641) 0 (54) ∞ 0.0 kB 0.000 0.000
What can this program do?
General Peers Pieces Files Speed Logger
IP Client Flags % Down Speed Up Speed Reqs Uploaded Downloaded Peer dl.
Can it delete all of your files?
YES. Why?
cust.13.6.adsl.cistron.nl µTorrent 1.6.1 D IHXE 100.0 0.4 kB/s 2 | 0
cpe-66-8-185-105.hawaii.res.rr.com Azureus/2.5.0.4 d XE 100.0
66.65.59.37 BitTorrent 5.0.7 d IX 100.0 2.7 kB/s 48.0 kB
66-214-179-78.dhcp.gldl.ca.charter.com KTorrent 2.2 IHX 0.0
67.85.64.225 µTorrent/1.6.0.0 D HXE 100.0 9.5 kB/s 4 | 0 144 kB
bas2-stcatharines10-1177764066.dsl.bell.ca µTorrent 1.6.1 UD HXE 10.8 2.2 kB/s 2.8 kB/s 2 | 2 512 kB 256 kB 288.2 k...
wsip-70-184-249-191.ok.ok.cox.net µTorrent 1.6.1 D IHXE 100.0 17.7 kB/s 16 | 0 2.35 MB
70.186.189.141 Azureus/3.0.1.6 d XE 100.0
71-10-91-182.dhcp.roch.mn.charter.com KTorrent 2.2 d IXE 100.0 16.0 kB
c-71-63-128-140.hsd1.mn.comcast.net µTorrent 1.7 D HXE 100.0 10.4 kB/s 4 | 0 1.98 MB
adsl-71-131-190-233.dsl.sntc01.pacbell.net µTorrent 1.6.1 D HXE 100.0 4.7 kB/s 3 | 0 304 kB
adsl-71-145-148-192.dsl.austtx.sbcglobal.net BitTorrent 5.0.7 D IX 100.0 1.0 kB/s 2 | 0 224 kB
72.24.208.255 Azureus/2.5.0.4 DS XE 100.0 2 | 0 32.0 kB
72.93.219.133 µTorrent/1.6.0.0 d IHXE 100.0
72.150.126.8 Azureus/3.0.1.6 ud IX 7.4
ip72-202-139-196.ks.ks.cox.net µTorrent 1.6.1 D HXE 100.0 2.6 kB/s 3 | 0 112 kB
DHT: 278 nodes
D: 606.7 kB/s T: 112.1 MB
U: 33.0 kB/s T: 4.2 MB

“Least privilege.”

Touchstones for *Least Privilege*

- When assessing the security of a system's design, identify the *Trusted Computing Base* (**TCB**).
  - What components does security rely upon?
- Security requires that the TCB:
  - Is correct
  - Is complete (can't be bypassed)
  - Is itself secure (can't be tampered with)
- Best way to be assured of correctness and its security?
  - **KISS** = *Keep It Simple, Stupid!*
  - Generally, Simple = ***Small***
- One powerful design approach: privilege separation
  - Isolate privileged operations to as small a component as possible
  - (See lecture notes for more discussion)

Check for Understanding

- We've seen that PC platforms grant applications a lot of privileges
- Quiz: Name a platform that does a better job of least privilege

“Ensure complete mediation.”

Ensuring Complete Mediation

- To secure access to some capability/resource, construct a *reference monitor*
- Single point through which all access must occur
  - E.g.: a network firewall
- Desired properties:
  - Un-bypassable ("complete mediation")
  - Tamper-proof (is itself secure)
  - Verifiable (correct)
  - (Note, just restatements of what we want for TCBs)
- One subtle form of reference monitor flaw concerns *race conditions* …

TOCTTOU Vulnerability

```
procedure withdrawal(w)
    // contact central server to get balance
    1. let b := balance

    2. if b < w, abort

    // contact server to set balance
    3. set balance := b - w

    4. dispense $w to user
```

TOCTTOU = Time of Check To Time of Use

```
public void buyItem(Account buyer, Item item) {
   if (item.cost > buyer.balance)
     return;
   buyer.possessions.put(item);
   buyer.possessionsUpdated();
   buyer.balance -= item.cost;
   buyer.balanceUpdated();
 }
```