

# Security and Usability in Open Source

Gus Andrews  
Secure Usability Senior Fellow  
Simply Secure

# Not speaking for Simply Secure

I wear many hats

So, you want to help  
people encrypt:

So, you want to make  
an encryption tool?

DON'T

DON'T

make a brand new one

So, you want to  
encrypt your stuff?

~~So, you want to  
encrypt your stuff?~~

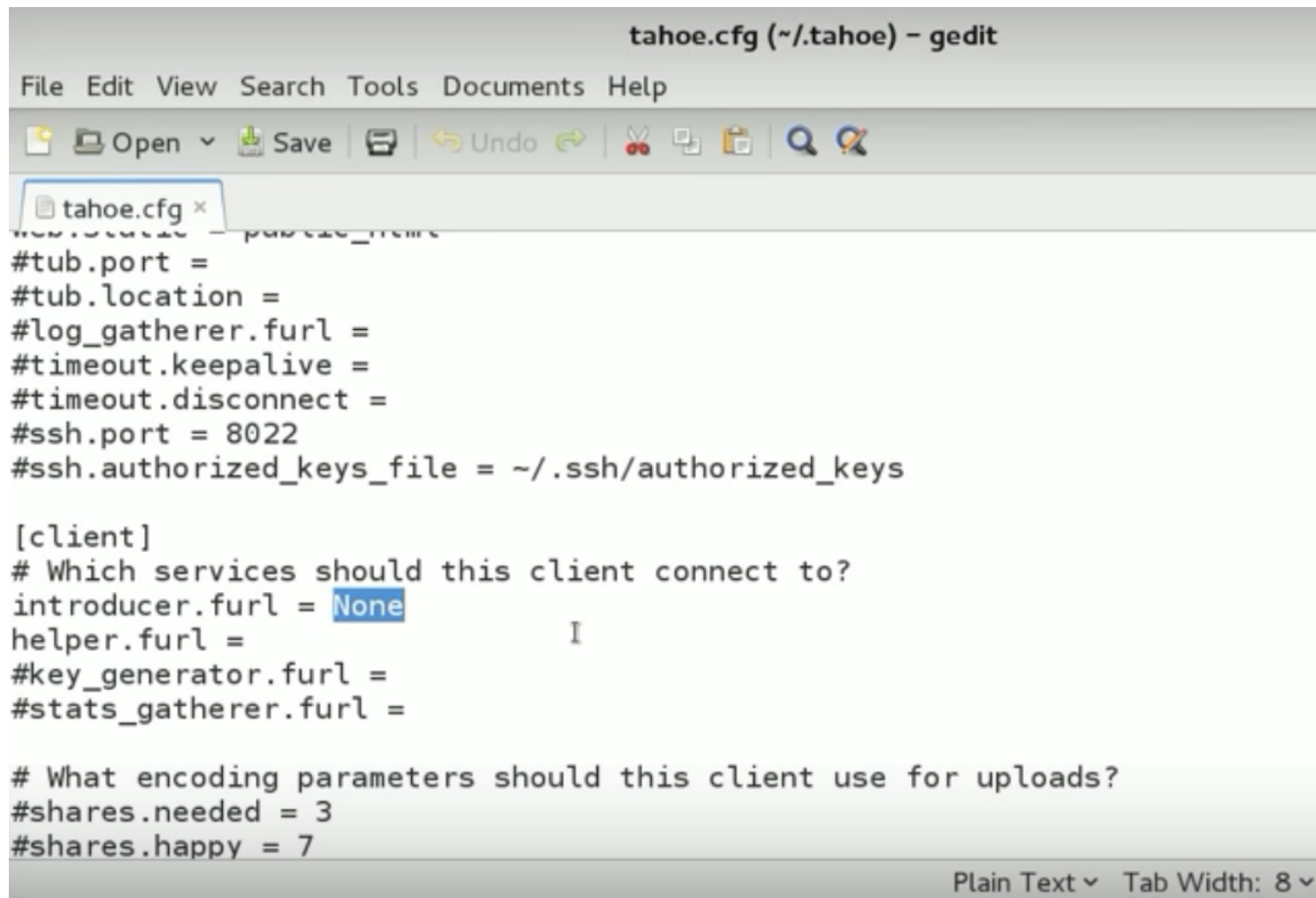
try a different talk  
or better yet a hands-on workshop



# Trade-Offs

(The Perfect Should Not Be The Enemy of the Good)

# Supporting experts vs. supporting newcomers



```
tahoe.cfg (~/.tahoe) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
tahoe.cfg x
#tub.port =
#tub.location =
#log_gatherer.furl =
#timeout.keepalive =
#timeout.disconnect =
#ssh.port = 8022
#ssh.authorized_keys_file = ~/.ssh/authorized_keys

[client]
# Which services should this client connect to?
introducer.furl = None
helper.furl =
#key_generator.furl =
#stats_gatherer.furl =

# What encoding parameters should this client use for uploads?
#shares.needed = 3
#shares.happy = 7
Plain Text Tab Width: 8
```

# Education

VS.

just make it @#\*\$&#\$ work

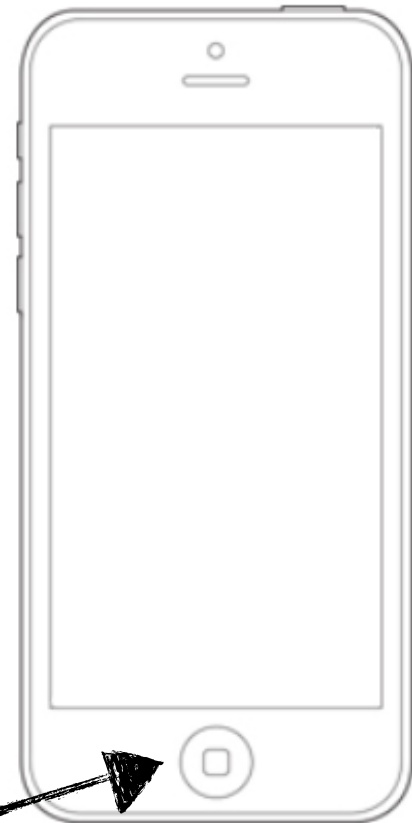
[level-up.cc](http://level-up.cc)

[ssd.eff.org](http://ssd.eff.org)

[tacticaltech.org](http://tacticaltech.org)

Cryptoparties?

VS.



(it has one button.  
you poke it.)

Education  
VS.  
just make it  
@#\*\$&#\$ work

Account Registration Wizard

SIP

Account Connection Security Presence Encodings

Registrar ostel.co Port 5061

Authorization name

Client TLS certificate <none> (use regular authentication)

Proxy options

Configure proxy automatically

Proxy ostel.co Port 5061

Preferred transport TLS

Keep alive

Keep alive method OPTIONS

Keep alive interval 25  
Between 1 and 3600 seconds

Voicemail

Message Waiting (MWI)

Voicemail Subscription URI

Voicemail check URI

DTMF

DTMF method Auto: Choose automatically between RTP and Inband (no SIP INFO)

Minimal RTP DTMF tone duration (ms) 70  
Default RTP DTMF duration is 70 ms

Previous Next Cancel

Click the **Next** button. Confirm the settings are correct on the next screen. Click **Sign In**

You should see it read "Registering" for a few seconds until the bar to the right of your account name turns Green and reads **SIP ON Online**.

CRYPTOCAT

Group Chat Facebook

conversation name

nickname connect

Enter the name of a conversation to join.

**Private Conversations for Everyone.**

Welcome to Cryptocat. Here are some helpful tips:

- Cryptocat is not a magic bullet. You should never trust any piece of software with your life.
- Cryptocat can't protect you against untrustworthy people or key loggers, and does not anonymize your connection.

2.2.2 Custom server English

# Ideal security vs. ease of use

## Login to Your Account

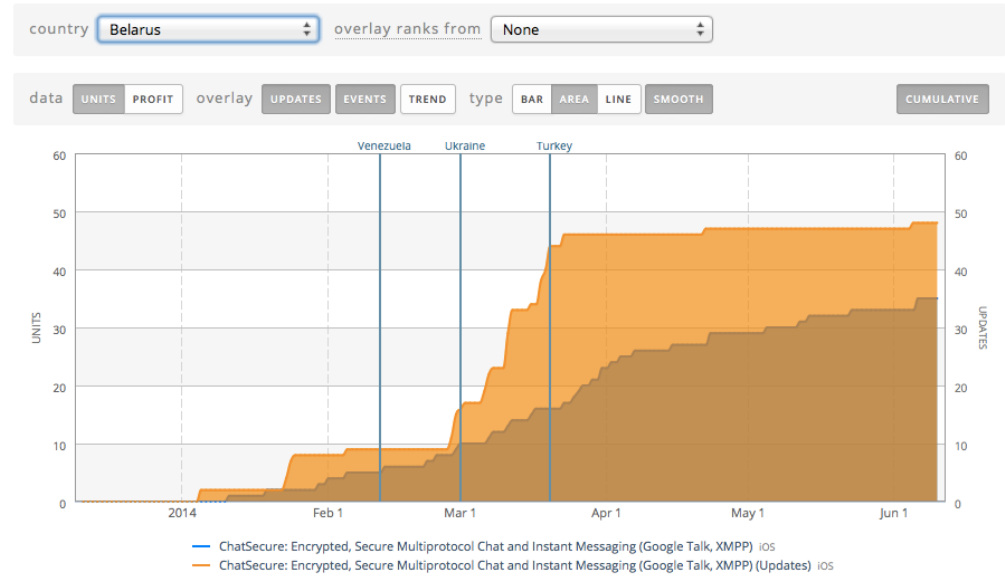
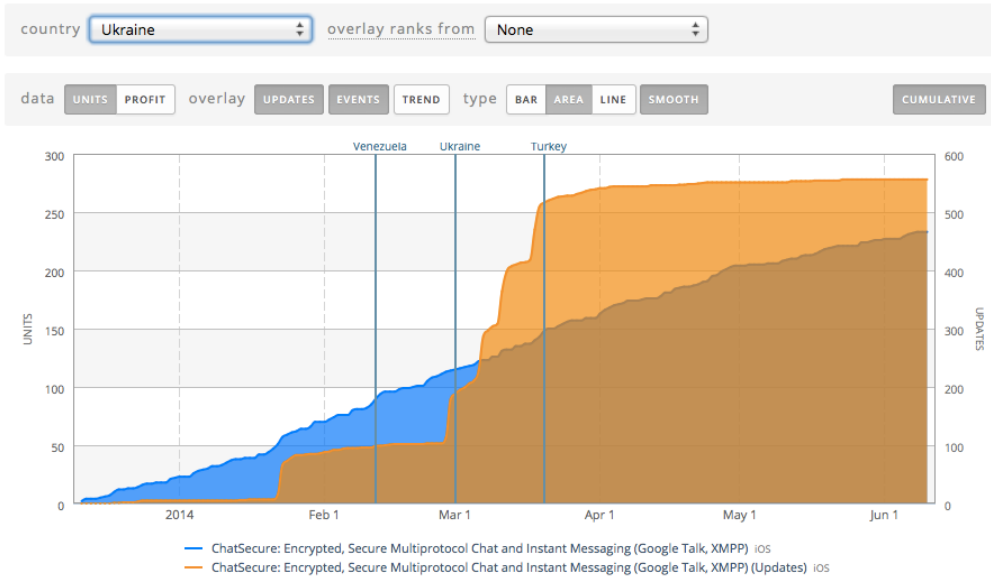
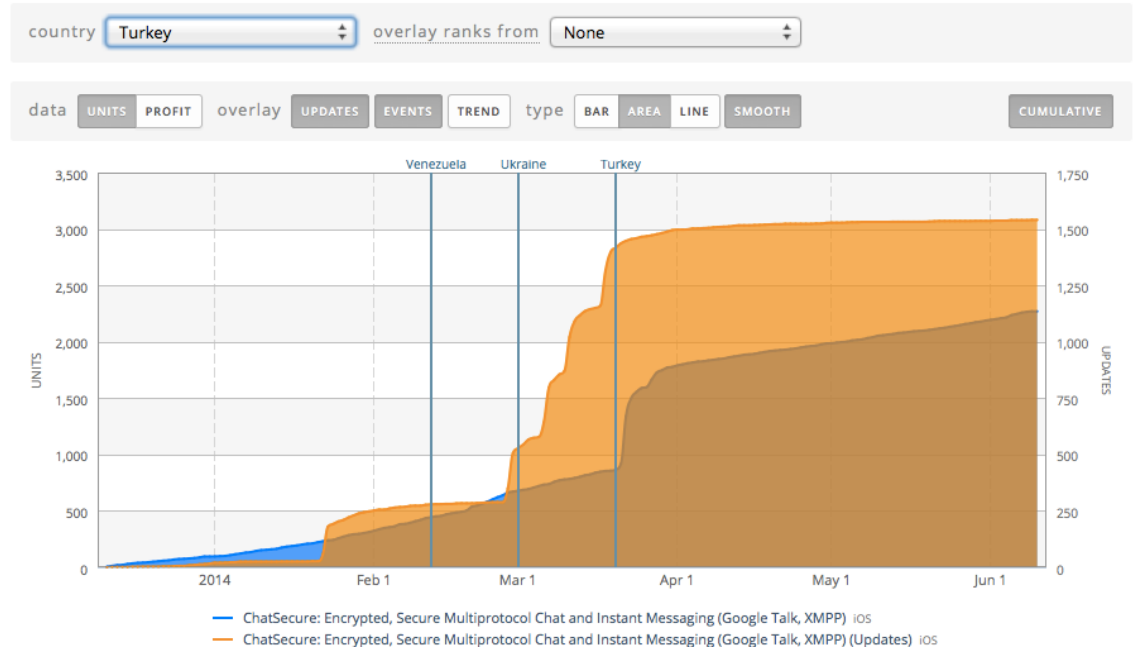
---

Account Number:

Password:  Use your mouse to enter your password on the keyboard below.  
(Password is not case sensitive.)



# Gathering metrics vs. protecting privacy

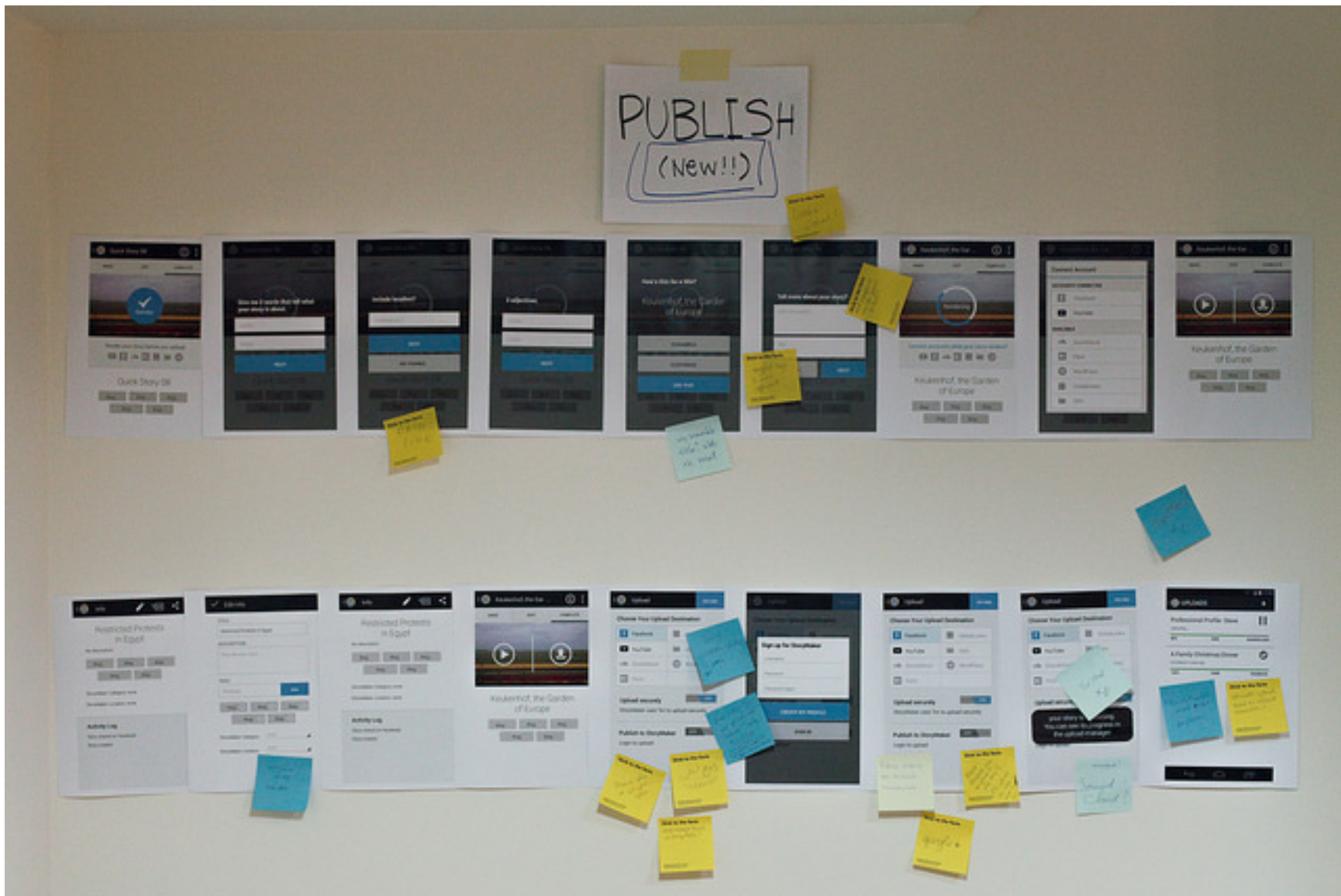


Which projects build  
usable tools?

# ~~Good projects have big teams?~~

<whine>But we're not Goooooooooooooogle</whine>  
(still: 1-2 people is not optimal)



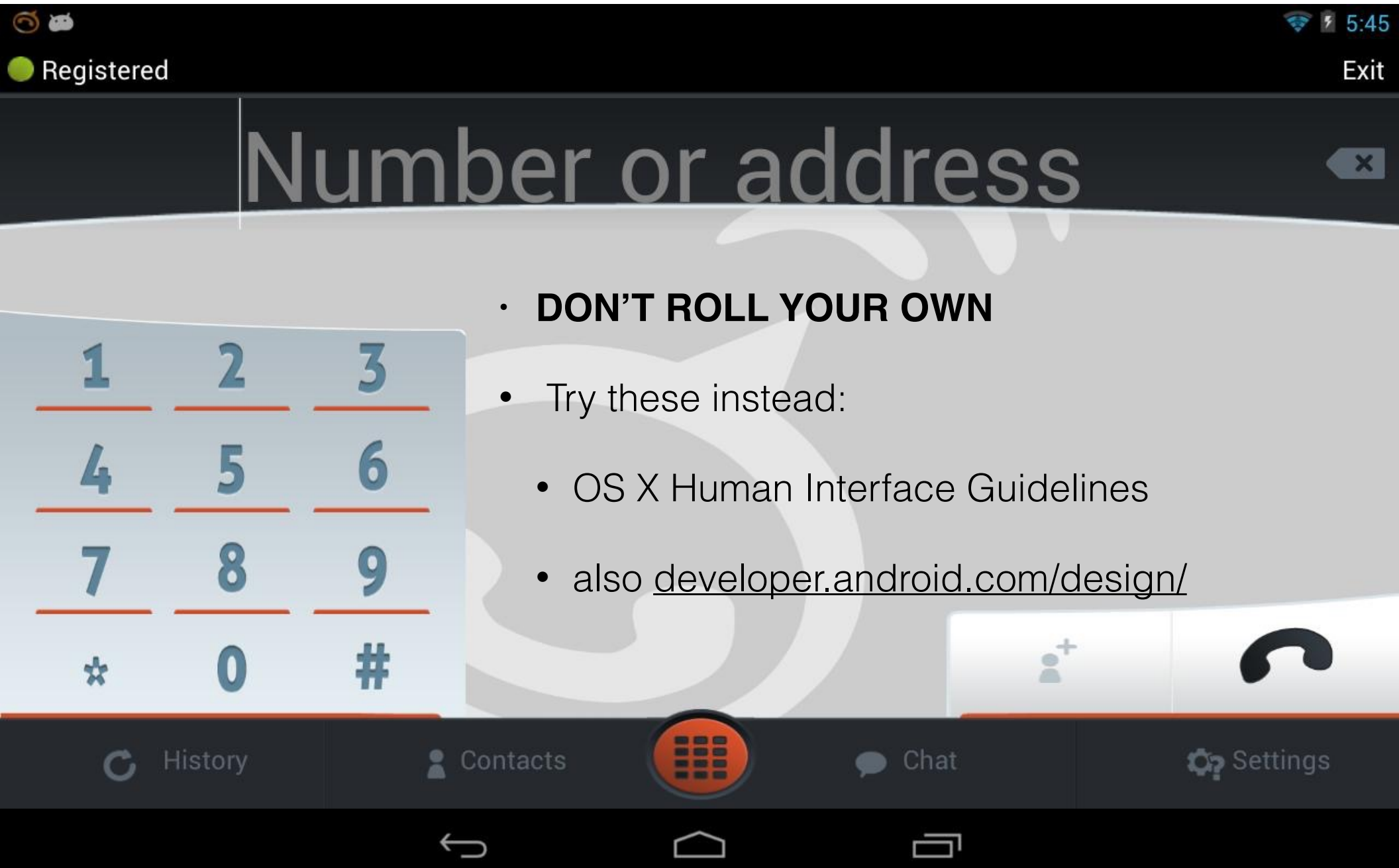


Good projects observe  
and listen to users  
early and often

# ~~Mailing lists~~

\*\$%# them right in the ear  
also: ~~only Github~~

# Reliance on standard patterns



OK, so what  
should I do?

~~Build a new tool~~

~~roll your own encryption~~

HAVE WE LEARNED NOTHING, PEOPLE



# Go out and find people who aren't like you

- OBSERVE
- Listen
- Don't interrupt



# Focus groups!

The reason you think “soft sciences” are “soft.”  
(see my 2014 talk at HOPE)

Why is Assange leading this focus group tho amirite?

# Where tho?

- Libraries
- NGOs
- Coffeehouses
- Newspapers?
- “Snowball sampling”
- ~~Your family/friends~~



# Avoid leading questions

## **DON'T**

- “How often do you encounter blocked websites?”
- “Do you encrypt?”
- “Do you face censorship?”

## **DO**

- “Do you think you are blocked from getting to some websites? Why?”
- “How do you protect your privacy?”
- not ask people from China this

# Move from general to specific

- “Are there factors that keep you from getting online? What are they?”
- “What do you do to stay safe online?”
- “Are you concerned about your government or other parties watching what you are doing? In what ways?”
- “What tools and technologies do you use?”

## Subscribing to the Enigmail Mailing List

Subscribe to enigmail-users by filling out the following form. You will be sent email requesting confirmation, to prevent others from gratuitously subscribing you. This is a hidden list, which means that the list of members is available only to the list administrator.

Your email address:

Your name (optional):

You may enter a privacy password below. This provides only mild security, but should prevent others from messing with your subscription. **Do not use a valuable password** as it will occasionally be emailed back to you in cleartext.

If you choose not to enter a password, one will be automatically generated for you, and it will be sent to you once you've confirmed your subscription. You can always request a mail-back of your password when you edit your personal options.

Pick a password:

Reenter password to confirm:

Which language do you prefer to display your messages? English (USA)

Would you like to receive list mail batched in a daily digest?  No  Yes

# VS.





TRONG



MAMUN



SARAH



LILLY



SHURA



JOSEFA



MARY



FATIMA



JAY



FETLEH



CARLOS

is.gd/securitypersonas  
( [medium.com/@gusandrews](https://medium.com/@gusandrews) )



*UNDERSTANDING  
INTERNET  
FREEDOM:  
THE TIBETAN  
EXILE COMMUNITY*



*UNDERSTANDING  
INTERNET  
FREEDOM:  
VIETNAM'S  
DIGITAL  
ACTIVISTS*

# To-do list

- Before you build tools, ask people: what do you need?
- Test early, test often
- Find others to work with — including designers
- Put settings in a menu nobody wants to see that
- Put “Help” in-app, not on web
- Use graphics/icons to give instructions
- Metrics?
  - Don’t assume users are as paranoid about data as you are. (Ask them.)
- If you can’t do user research yourself... come talk to Simply Secure!

# Steal From Capitalists



# Startup Techniques





# Don't Scratch Itches



# Build Stuff People Use



# Lean Startup Shit

## CUSTOMER RESEARCH & VALIDATION

### EXERCISE 1:

- Who, specifically, do you think your customer is?
- What problem, specifically, do you think they have?

PROBLEM HYPOTHESIS	Parents	CUSTOMER
Learn chinese:	Banks	Red workers
Custom flower essence	Parents of children with difficulties	
Let co-workers know	Hungry people	
Boutique Univ.	Online customers	back to stores
Licence - commoditize law	Architects - Low corp records	
Credit Cards	Bit managers	
Learn English	International businesspeople	
Greater happiness in Biz environment	Biz people	
Platform for learning	Teachers	
Risk Assessment		
Pick right hair color	Women	
Biz management	Small non profit	
Mi Dr - Single platform entertainment	Consumers	
Connection at last minute	Urban Proff	24-40
Blend therapy	Self-help	
Virtual social environment	Med professionals	
Virtual private servers	Web dev's	Comp.Sci. Depts
Break cadenters patterns	workers at desks	worried about health
Curated travel content	Bit travellers	
Therapy Medicom	Phy. therapy patients	
Reduce neg effects of social patterns	general population	18-70
Find funding via crowdsourcing	Small biz owners	
Deal w/trauma in Public Schools - via incentive model	Students who are trauma	(innercity)
Denko site usage feedback & impact	URBAN RESIDENTS	
HEALTHY FOOD DRIVE THRU	URBAN CUSTOMERS	

## LEAN UX

- CONTEXT FIRST
- HYPOTHESES, NOT REQUIREMENTS
- OPINIONS = GUESSES
- VISUALIZE YOUR WORK
- REDUCE CYCLE TIMES
- LAST RESPONSIBLE MOMENT



## EMPATHY

## INTERVIEW QUESTIONS:

TELL ME ABOUT... HOW SO? WHAT ARE YOUR THOUGHTS ON... GIVE ME SOME EXAMPLES TELL ME ABOUT THE LAST TIME...

## ETHNOGRAPHY

- PRIVATE AND PUBLIC DISPLAYS OF RITUAL
- SPEAK IN THE LANGUAGE PEOPLE USE
- DIVE DEEPLY
- LEARN CONTEXT
- PRACTICE "ACTIVE SEEING" & "ACTIVE LISTENING"

"DIGITAL ETHNOGRAPHER'S TOOLKIT" BY CHRIS KHAIL

## SURVEYS

- AVOID SUBJECTIVITY... i.e. "FREQUENTLY/SOMETIMES"
- QUESTIONS MUST MEAN THE SAME THING TO EVERYONE
- USE CLEAR ANCHORS OF MENTAL MODELS:

ALWAYS ← → NEVER

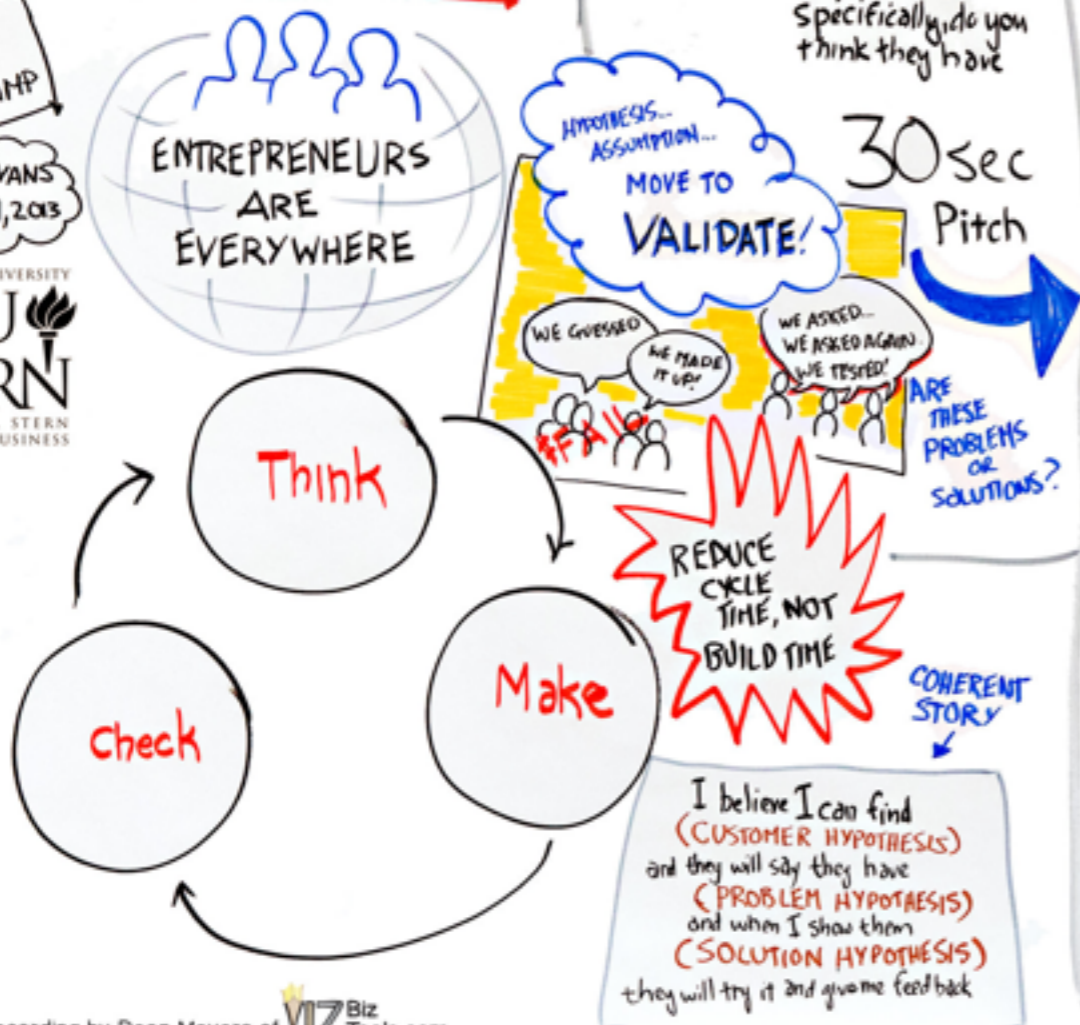
## PERSONAS

- FACTUAL INFO
- BEHAVIORS
- PAIN
- GOAL



LEAN SUMMER BOOT CAMP  
WILL EVANS  
JULY 19, 2013

NEW YORK UNIVERSITY  
NYU STERN  
LEONARD N. STERN SCHOOL OF BUSINESS




# Growth Hacking



# Learn Quickly

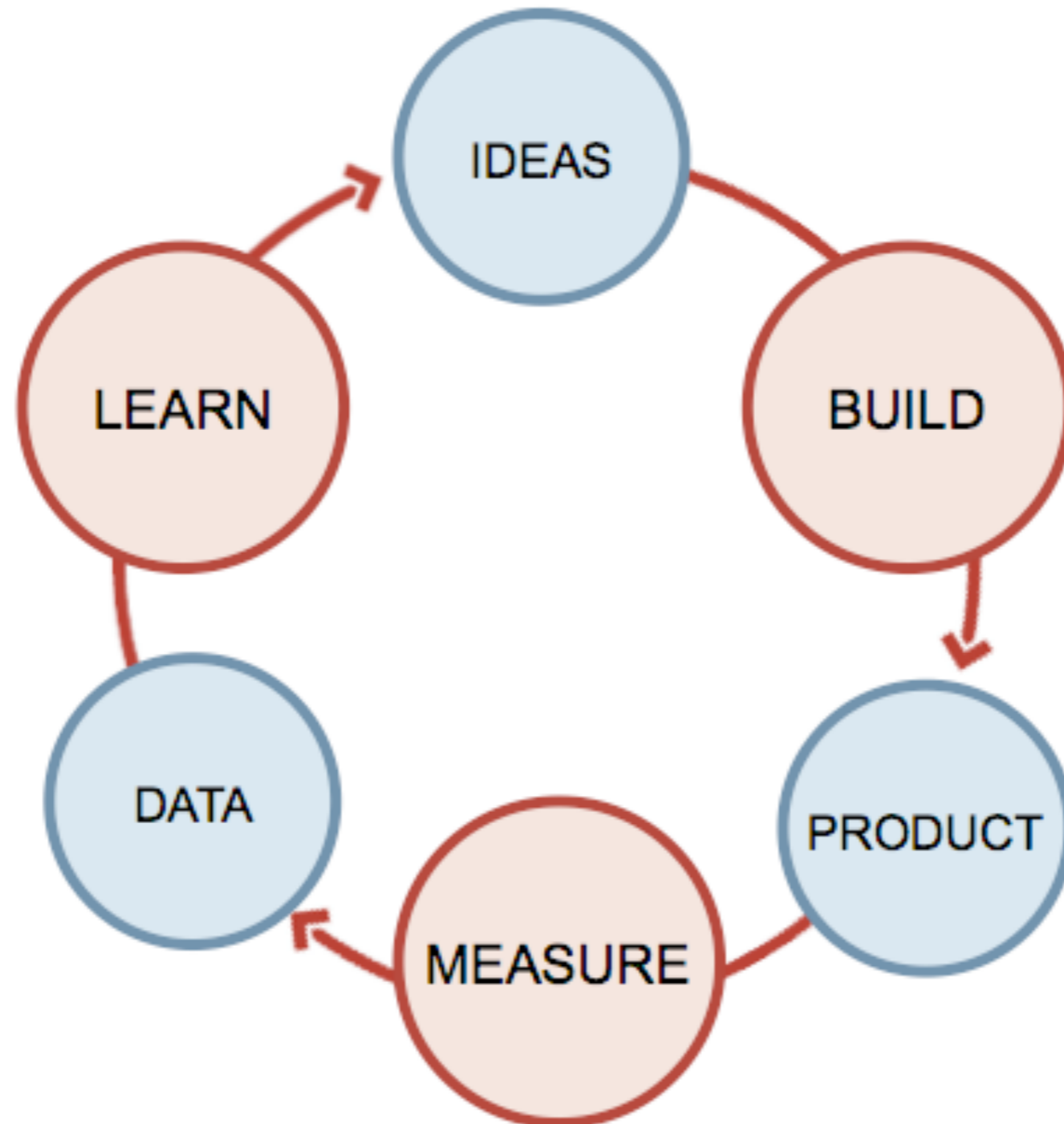
**I have not failed.  
I've just found  
10,000 ways  
that won't work.**

Thomas Edison

Photo by Marius Brede  
 Symphony of Love



# They're Learning Faster

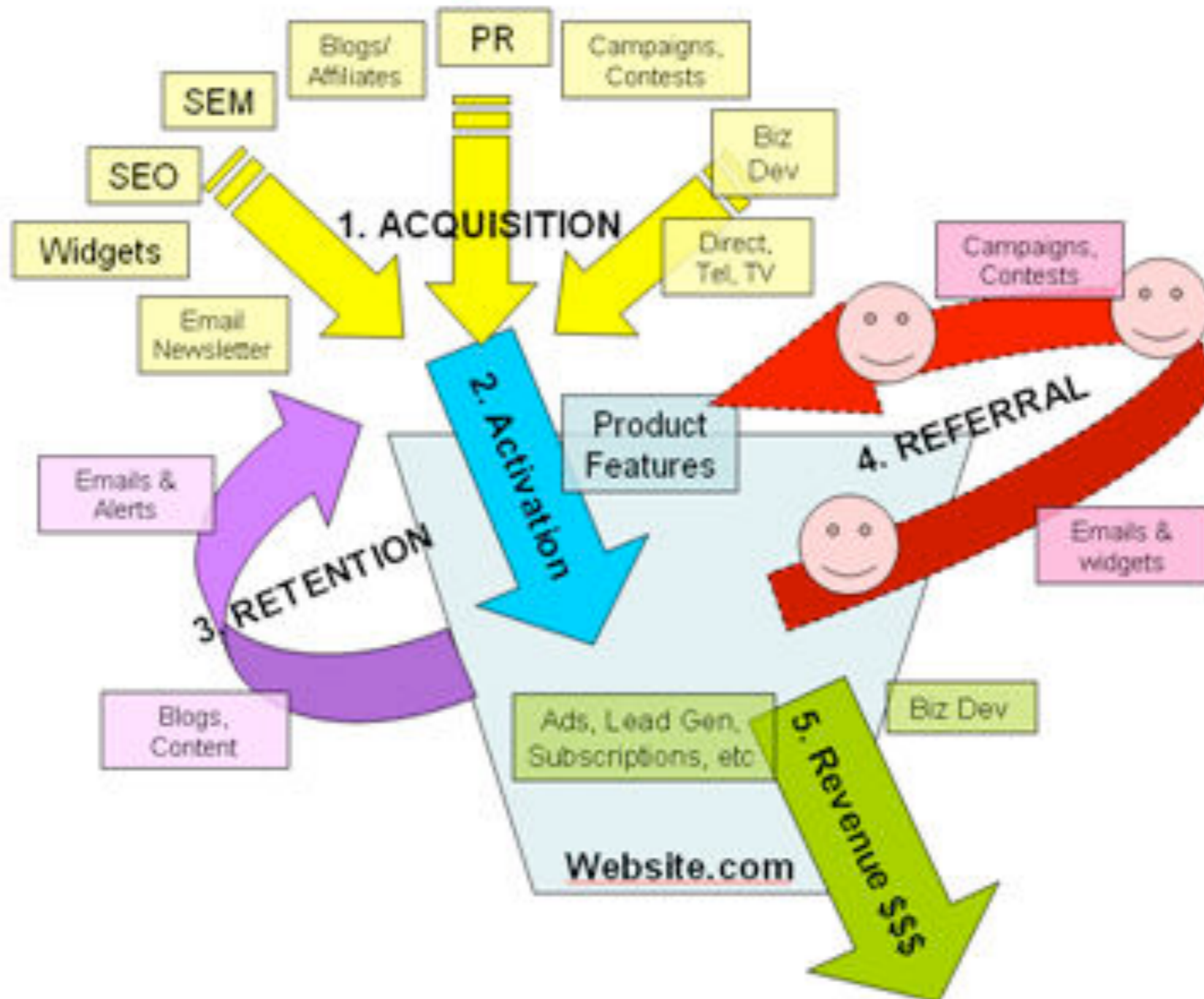


# Test All The Things



# Pirate Metrics

## Customer Lifecycle / Conversion Behavior





# Pirate Metrics



**Acquisition**

**Activation**

**Retention**

**Revenue**

**Referral**

# Pirate Metrics



**Acquisition**

**Activation**

**Retention**

**Use**

**Referral**

# It's a race



**It's a race**



# Easy Wins

