
# HUSHCON 2016 KEYNOTE TEST FOR ECHO

Adam Cecchetti
Deja vu Security

# Hello!

- Adam Cecchetti
- Deja vu Security : Founder, CEO
- Peach Fuzzer : Founder, Chairman

# Time: #3 Person of the Year

TIME

NO. 3 | THE DISRUPTERS

## THE HACKERS

*THEY MADE VULNERABILITY THE NEW NORMAL AND TOOK AIM AT DEMOCRACY ITSELF*

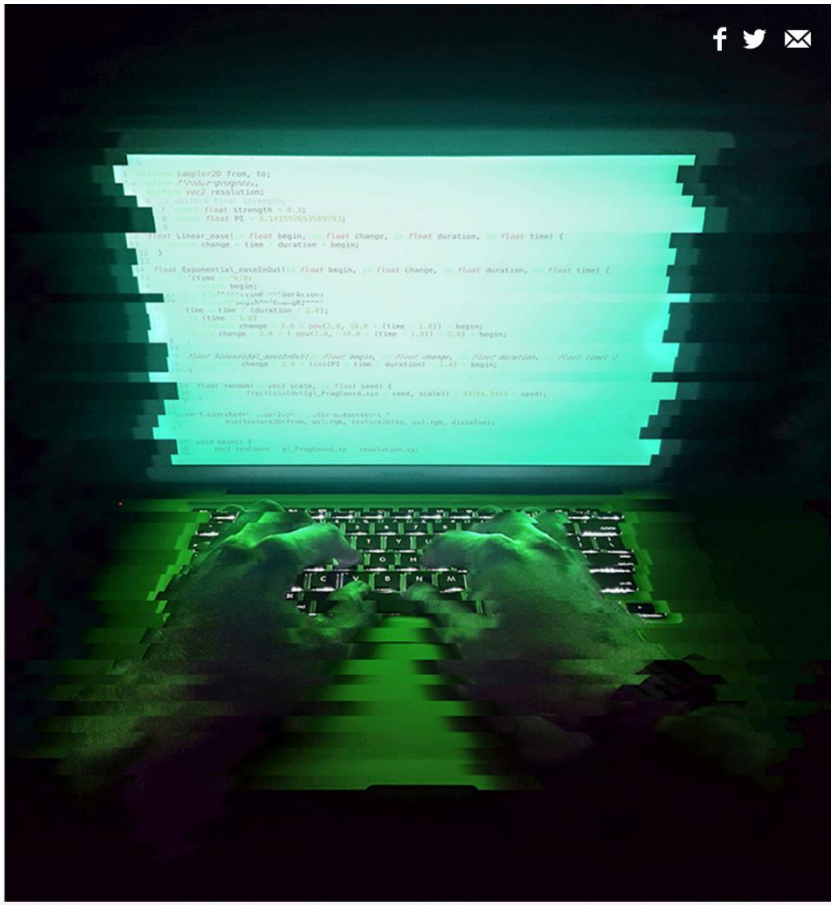
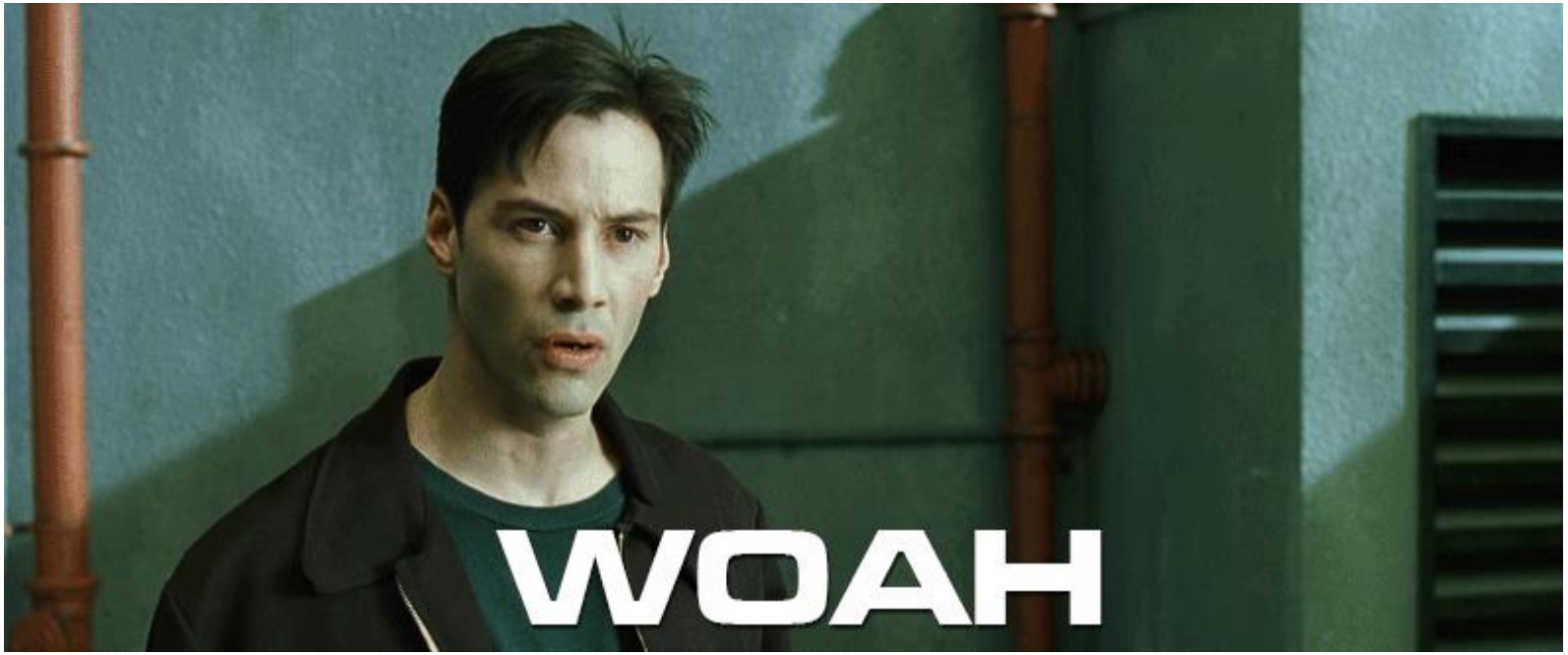


Photo-Illustration by Adam Ferriss for TIME

# A Sense of Deja vu

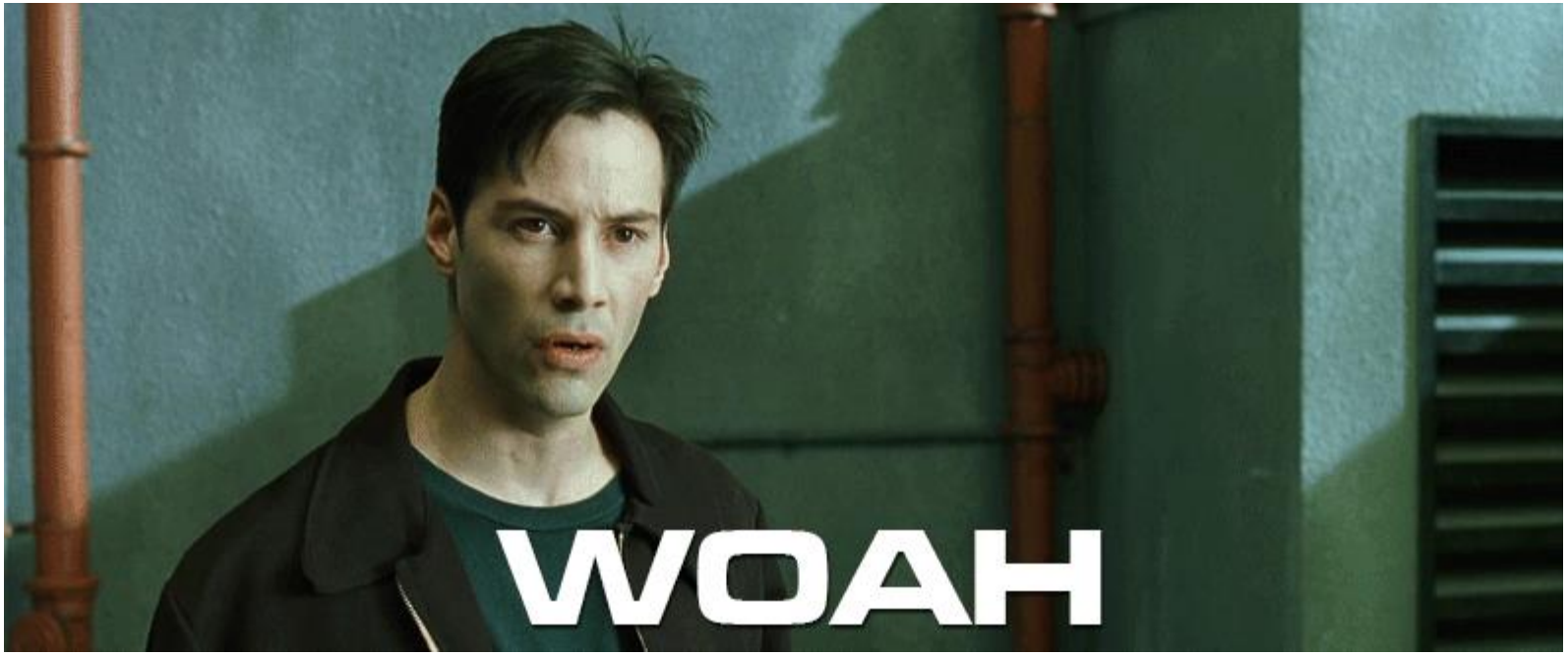



déjà vu SECURITY

# Deja vu. Deja vu. Deja vu. Deja vu.

| | |
|---|---|
| Networks | *"The tubes are on fire!"* |
| Applications | *"The desktop is on fire!"* |
| Web | *"The world is on fire!"* |
| Cloud | *"The sky is on fire!"* |
| Internet of Things (IoT) | *"Your pants are on fire!"* |

# Marketing!

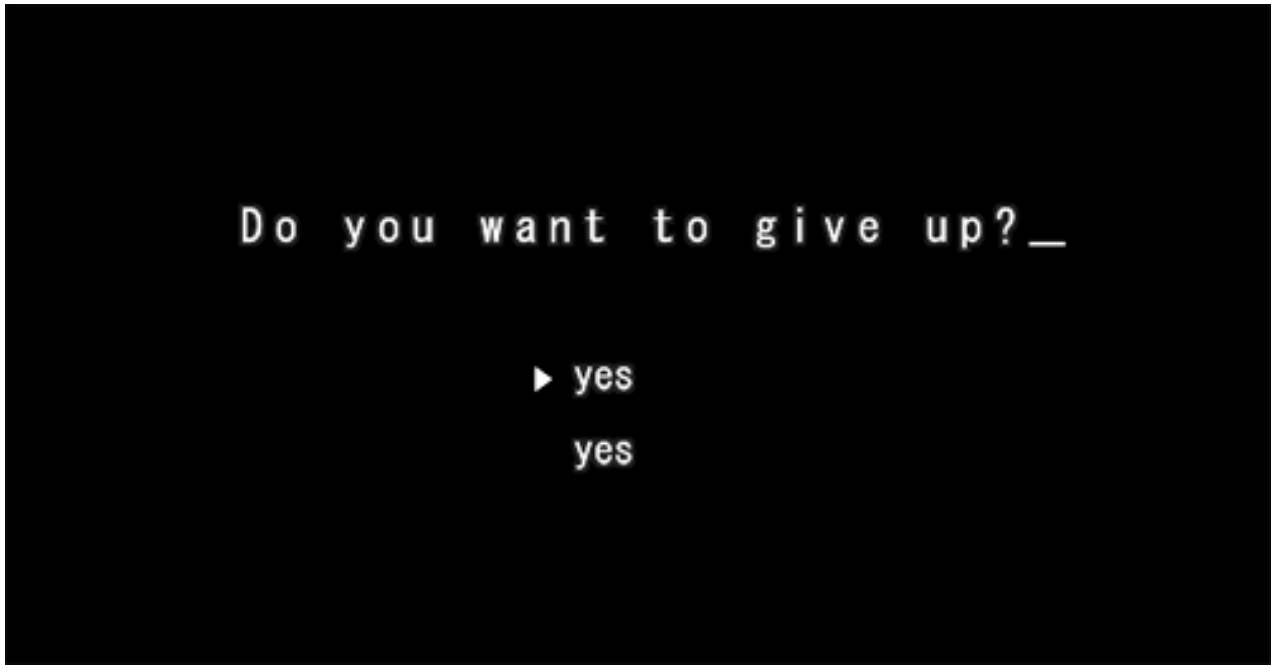



déjà vu SECURITY

# The Problem is Big

- The first step to recovery is the hardest.
  - Awareness is good, but it doesn't cure cancer.
- Security issues must be **found** they can't be created.
  - Inherited, *passed down the software genepool.*
  - Plentiful, *defense helps but we kick over more rocks.*
  - Random, *the future is asymmetrically secured.*
  - Polymorphic, *the tools we use to build systems are security issues.*
- We are going to have to start thinking differently.

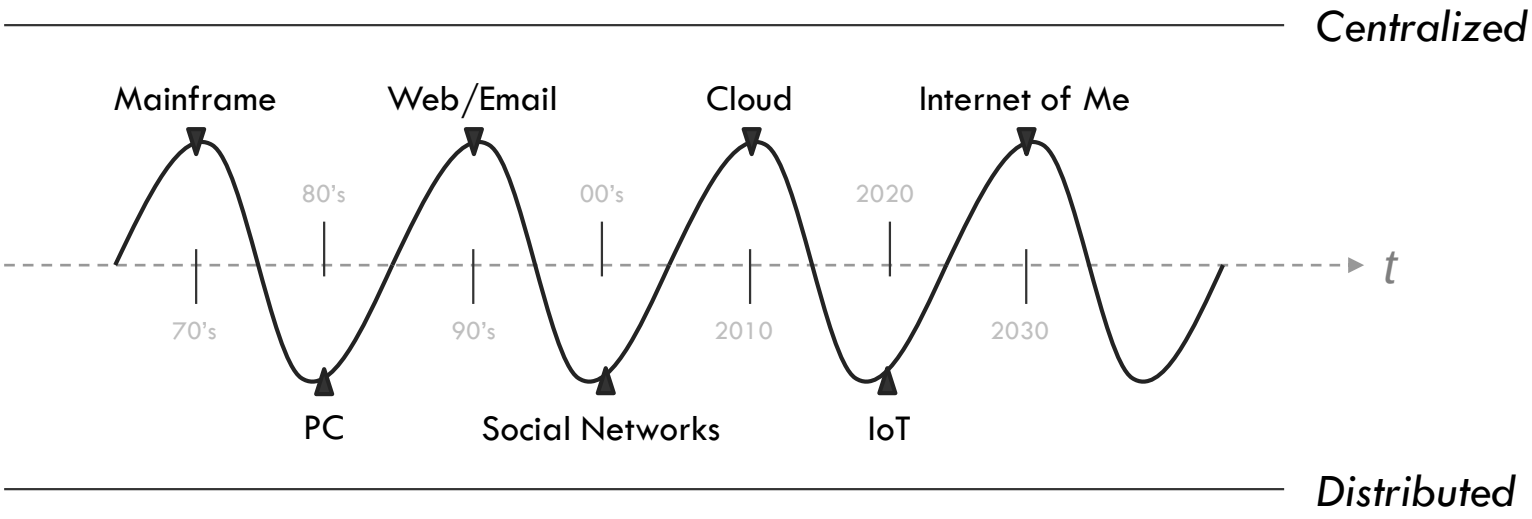
# Not That Differently




déjà vu SECURITY

# Tick, Tock.

- Data movement is a cadence to how we've built things.
- Echoes, the ghosts of usage models past.
- We leave data and code everywhere users go.
- User data replicates every decade or so.



# Security is a Snapshot in Time

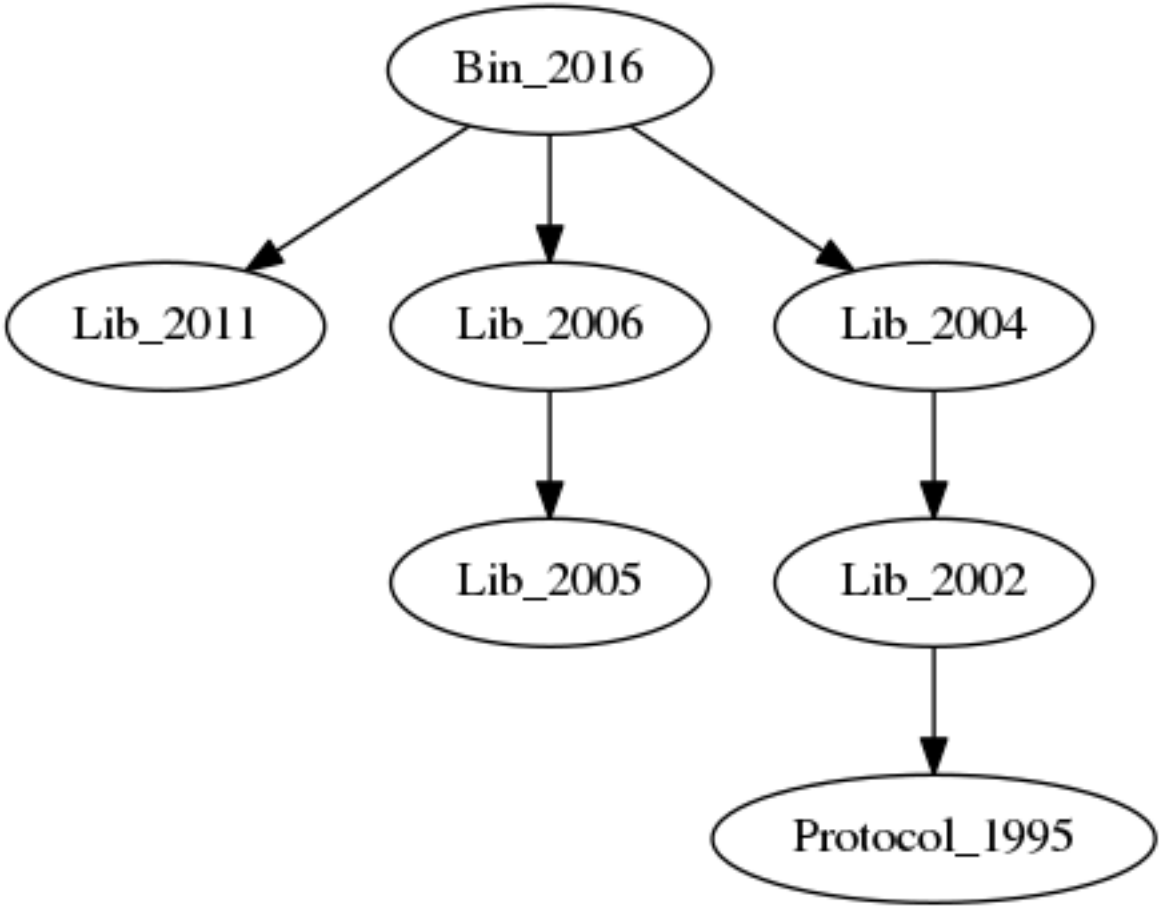
- Security is a snapshot in time.
  - Tomorrow is a new day full of drama on Twitter!
  - Today is a great day to deprecate a system.
  - Move user data to a safer and better place.
- Hackers are unstoppable in 1995.
  - The closer the temporal snapshot to 1995 the better for hackers.
- The person building the system decides the snapshot that is taken.
  - Protocols from 1995
  - Libraries from 2006
  - Binaries from 2014
  - A Linux build from 2016

# You Wouldn't March This Army Today

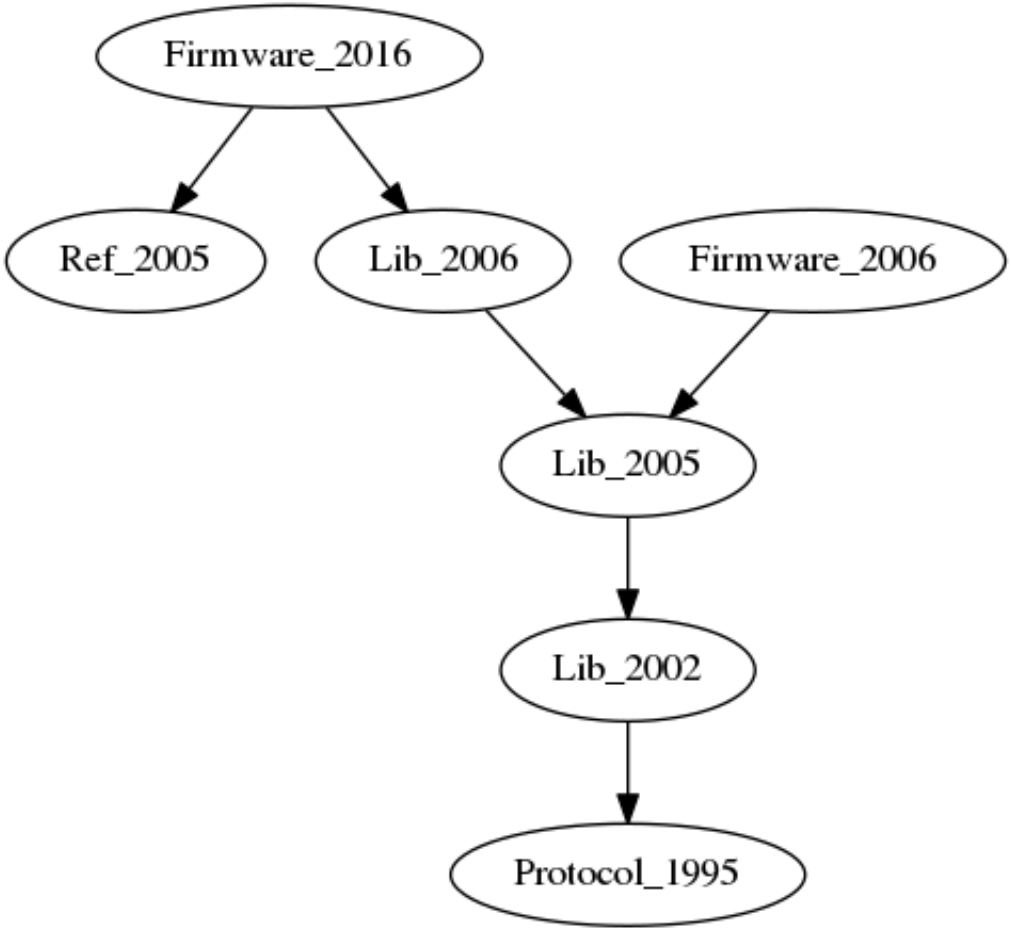
# You Wouldn't March This Army in 2116


déjà vu SECURITY

# Snapshot 1: 2002 vs 2016 Hackers



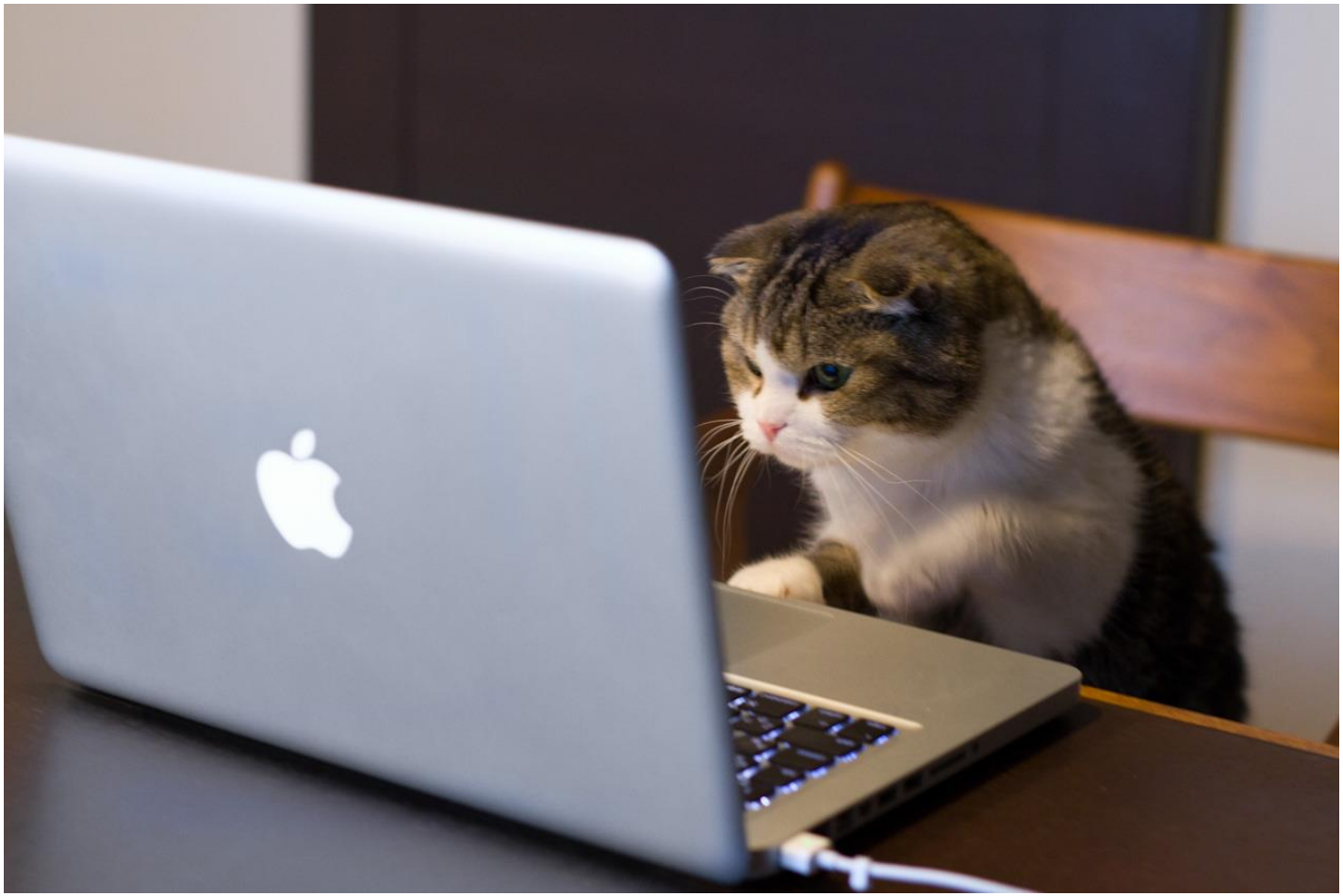
# Snapshot 2 : 1995 vs 2016 Hackers



# Computers are Awesome!

- They don't LET you do anything.
- They DO anything!
  - And only things you tell them
- CPU: AMMA that's about Machine code to Microcode
    - Good luck with the rest! That's not what I do!
- General computation is good however it means:
  - No reliability, no availability, no security.
- This includes anything we build.
  - Complexity leads to side effects and exploitation is programing with side effects.

# Memory Leak in /dev/litterbox?!



déjà vu SECURITY

# We Are at an Odd Juncture

- Mobile is eating all markets just like the PC did.
- User habits are changing, again.
  - Web ate the rest of the world.
- User data flows in new directions
  - And lingers in the eddies.
- And for those of us left that still care about general computation we have to run unknown kernel and firmware exploits to program our phones.

# Jail Broken

# The Internet Finally Showed Up!

- The amount of air gap between our lives and the Internet is shrinking daily.
  - Soon it will be gone. Good Riddance! Plug me in!
  - Unless you have decided to live in a cave.
    - And in another tick tock there's still a chance it will have IP enabled bat guano.
- Technology is awesome!
  - In 5 years my self driving car will live stream.
  - Localized live traffic video broadcasting and viewing is going to be a thing.
- There are going to be people sitting in traffic watching other people sit in traffic around the world.

# Live From the 520 Parking Lot…

déjà vu SECURITY

# Be Still My Beating Heart

- The Internet of Me is coming soon.
  - I can't wait until my heart has an IP address.
  - And firmware updates
  - And an app store to monetize!
  - Cardio Trainer+ 4.0
    - Now with Twitter Integration!
  - Cardio Trainer+ 4.0.1
    - Pushed a patch as some users were excessively twitching while Tweeting.
- Move fast and break things is not what I want for addressable organs.

# Everybody Bugs

- Bugs happen.
  - They happen to the best.
  - They happen to the worst.
- Imperfection is the proof of life and existence.
  - Mistakes are proof you actually did something.

# How to Lose Normal People


déjà vu SECURITY

# Start with Details

- “The buffer can overflow causing a corruption of the pointer which in turn is referenced by the vtable to cause code to jump to a known location as a result of ASLR being not compiled into a supporting DLL”
- “The password is P@ssw0rd!”
- “User A can access the details of User B”

# CVE-2017 – Critical Bass Overflow

# How to Get Things Flowing

# Helping People Understand w/Impact

- The user's bank account can be drained.
  - One person cares.
- The company can no longer perform transactions.
  - The entire company cares.
- The car performs a J-turn at 60 mph during rush hour
  - 1 news cycle.
- The planes crashes
  - 2 news cycles, 4 if they can't find the plane.
- The pacemaker stops and kills the user.
  - 2 Federal Agencies + n pacemaker users care.
- The power plant explodes.
  - People care until the lights come back on.

# In an Age of Infinite Scroll

# “Hacked a what? Oh, right.”

ANDY GREENBERG SECURITY 03.08.16 7:00 AM

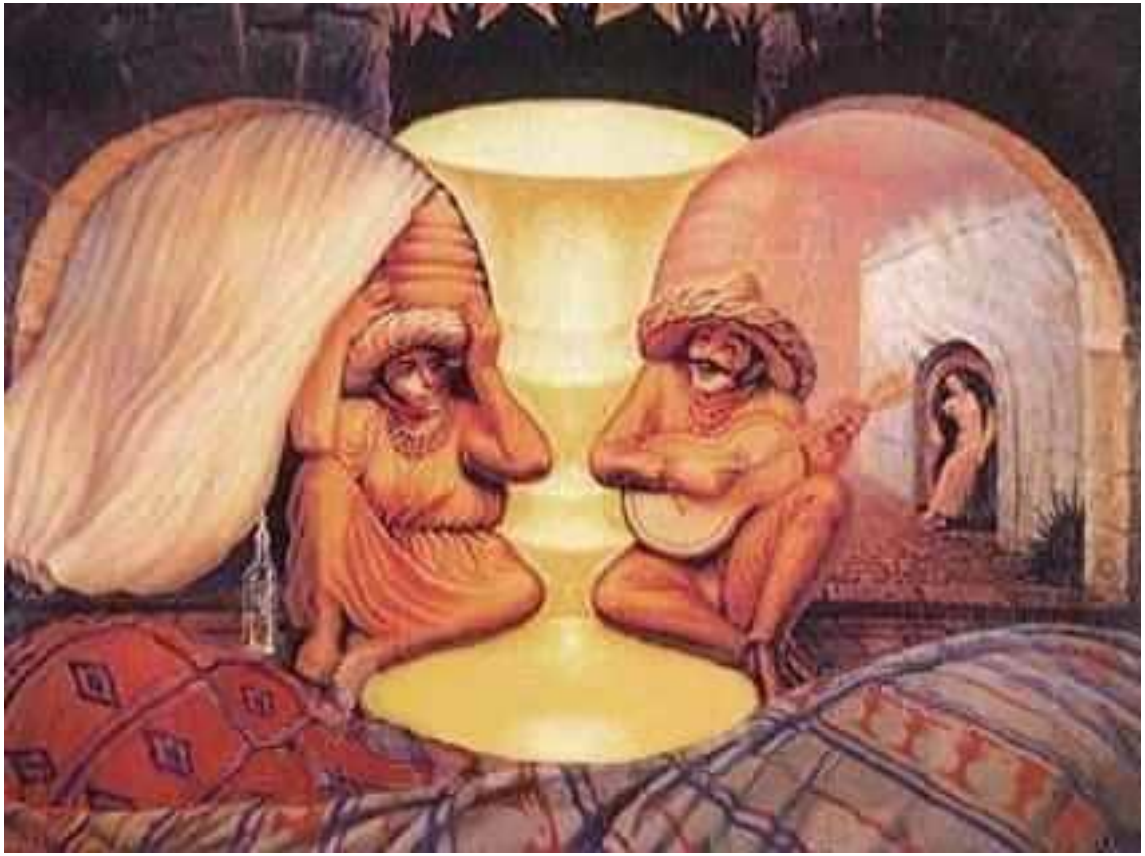
## ONLY ONE IN 4 AMERICANS REMEMBERS LAST YEAR’S EPIC JEEP HACK

déjà vu SECURITY

# Ken

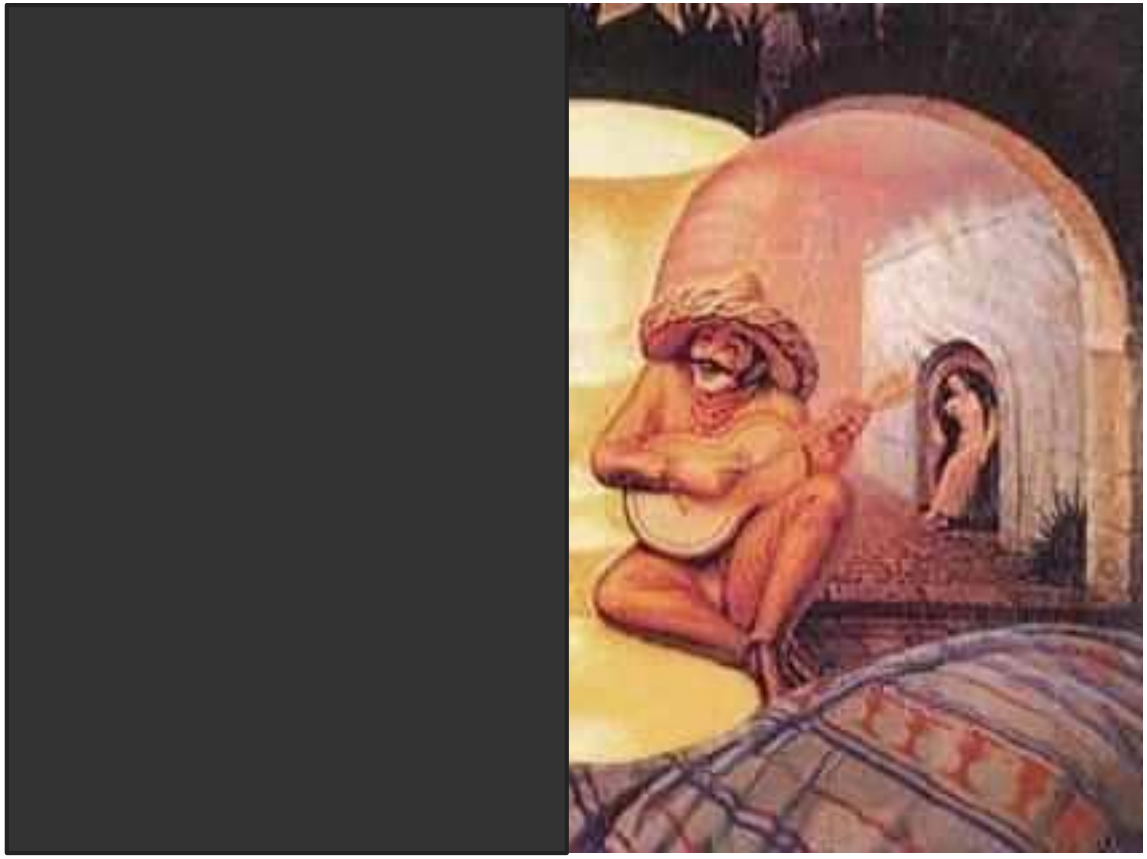
- Ken /ken/ *noun*
  - “one's range of knowledge or sight”
  - “know”
- How far you see.
- How wide or narrow are you focused.
- How much you understand.
- How far someone else can see, focus, and understand.

# Ken

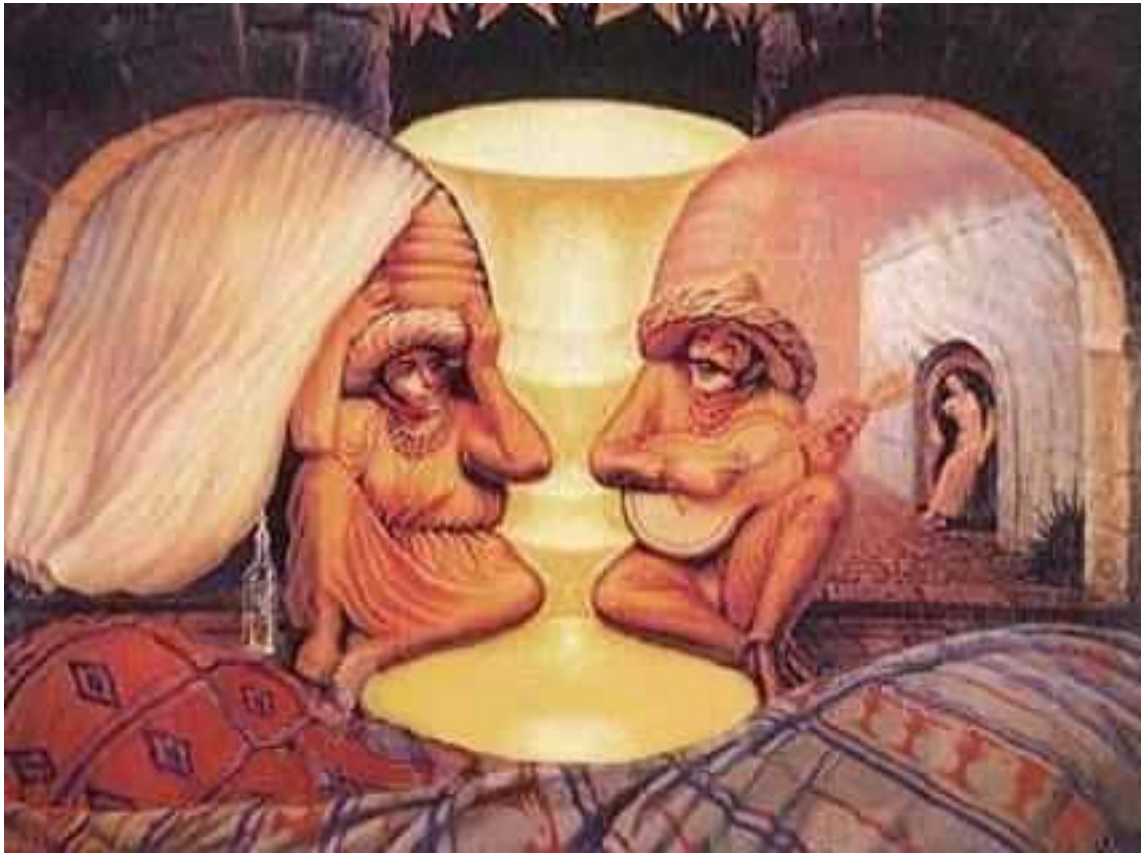


# Ken : My Ken

# Ken : Your Ken



# Ken : Our Ken



# Admitting Blindness is Beaten Out of Us

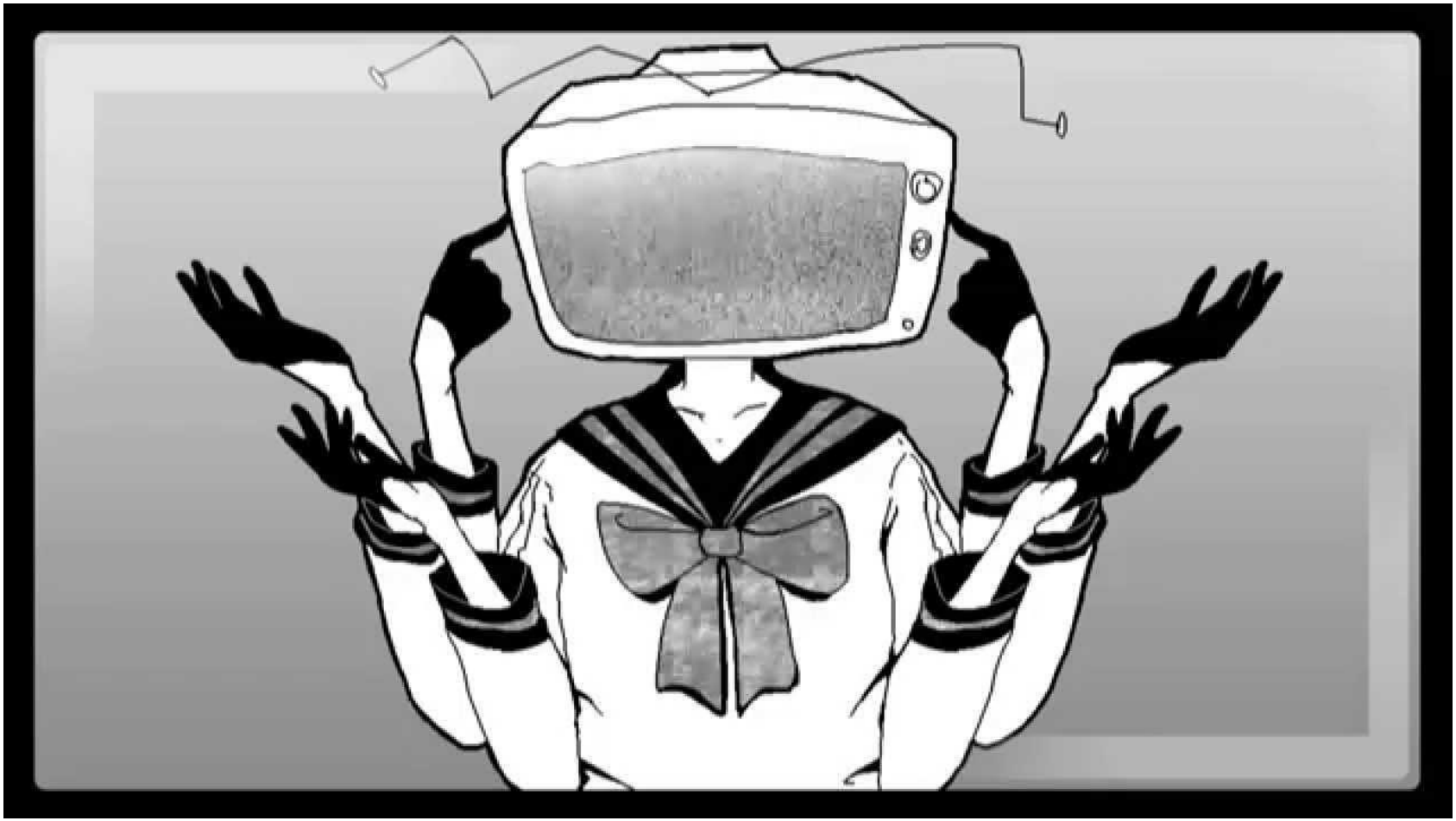
# Ken

- Their Ken: I need to move 14,000 planes a day with 300 people in them each or the global economy stops.
- My Ken: Planes can move in ways you don't intend if you connect them to the Internet, might even crash.
- Their Ken: Customers don't like to crash.
- My Ken: Less planes move if they crash.
- Our Ken: Let make new planes that are easier to move, safer, and crash less.

# Ken

- Accepting WE > I
- Knowing the range of my knowledge and vision enables me to spend our time better.
- Knowing how to better understand the range of another's vision helps us get to shared impact faster.
- Then we can start sharing details.
  - If we want to keep our place at the table it is our job to extend our ken with everyone seated.

# Testing for Echo



# Test for Echo

- You have lost if:
  - All you are hearing is your own words come back.
  - Things you already know.
- Shared exchange of ken is shared extension.
- Sustained echo is at best rapid construction of a chamber.
- On a more than decade time scale it is slow death.

# Details: Our Three Wins

- Firewalls
- Encryption
- Two Factor Authentication

# Impact: Three Extensions of Ken

- Firewalls
  - I don't want to run Ethernet cable in my house.
  - Wifi + Firewall = Win!
- Encryption
  - I can't make it to the bank or store today.
  - I need to work from home.
  - Commerce from home + encrypted tunnel = Win!
- Two Factor Authentication
  - I don't want to re-grind my character.
  - World of Warcraft = Win!

# Ken: When Have We Won?

- We've won the same way everyone else has.
- When we've made someone's life better they adopted a technology.
  - It happen to be more secure because we spent years working on the details.
- If we want to get pedantic we used Trojan horses to backdoor security into people's lives.
- Applying security to a shift in user behavior.
  - This is better!
  - We defined that part of being better was more secure!

# Ken: The users

- Want to do the thing and will always want to do the thing.
- Help the user keep doing the thing they want to do.

# To Master Details

- Do your research
- Do not be afraid of the work
- Do not be afraid to fail and never stop.

- Hack fast, conserve bugs, never ever make a deal with a Blackhat.

# Get to Work


déjà vu SECURITY

# Details: Data as Code

- What do Cross Site Scripting, SQL Injection, and Buffer Overflows all have in common?
  - They are all data being interpreted as code.
  - Any place that user or machine controlled data is being used, interpreted, parsed; a security issue awaits.
- This is big enough to master that you can spend multiple lifetimes right here.
  - We've actually started to make steps towards fixing this problem in some places.

# Details: Gamers are Going to Game

- Logical Issues require someone to game the system
  - Must try and understand all the unexpected behavior of the logic of the system.
  - Few good ways of automated testing here
- The Meta Game
  - Attackers will continue to go for the weakest link
  - Unless the time vs. reward scenario is high
  - or the motivation .vs reward scenario is super high

# Details: We Rely on Secrets

- Password1!
  - Upper Lower, Numeric, Special!
  - Secure by most standards!
- " Or '1'='1'; --
  - Upper, Lower, Numeric, Special!
  - No key words!
  - 16 characters!
  - Secure!
- If not bad jumbles then bits generated by a machine given back to a machine!

# To Master Impact

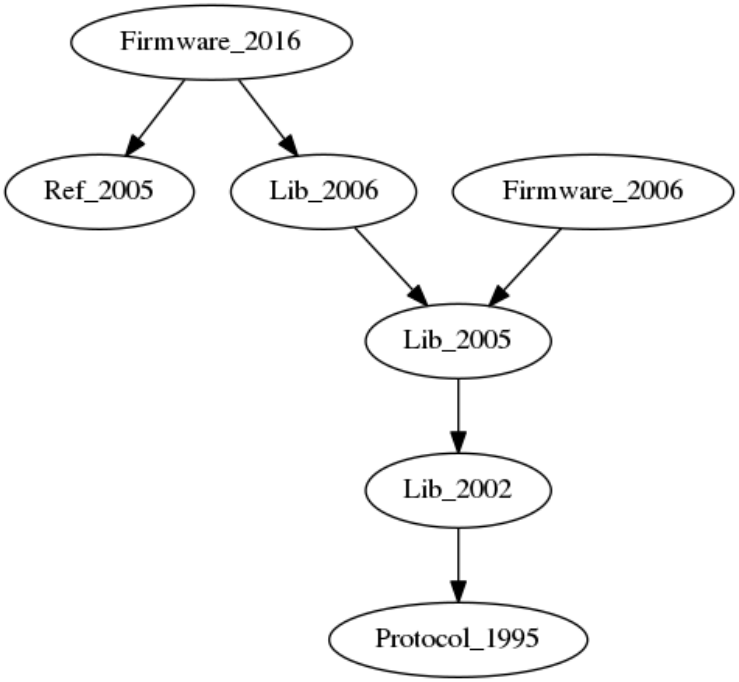
- See the system as a graph of lists of sorted by time.
- Know what matters in the system.
- Use the details to break the system.
- When the system will not break change the game.

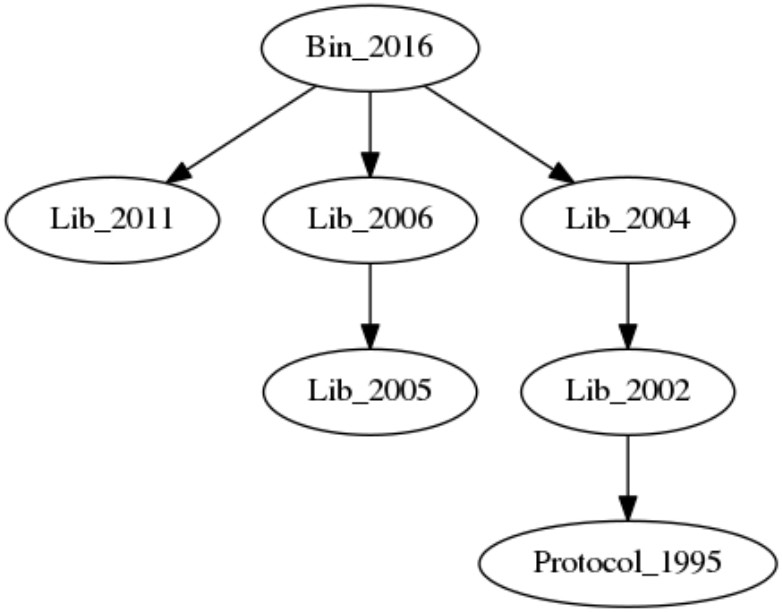
# Impact: Master The Graph

déjà vu SECURITY

# Impact: Master The Graph

- Seeing the system as a graph allows direct access to what is most impactful for the system.




déjà vu SECURITY

# Impact: Master the Clock


déjà vu SECURITY

# To Master Ken

- Know yourself and share ideas and creations.
  - Ask to know and understand others.
- Use impacts to connect yourself to others faster.
  - Seek the patterns that allow you to extend your vision and knowledge.

# To Master Ken

- In cooperation:
  - Use your ken to help others see what they cannot.
  - Ask to be shown what you cannot see.
- In conflict:
  - Find the blind spots.
  - Where someone is blind they cannot defend.

# Mastering Ken

# Ken: Test for Echo

- Step out of the echo chamber from time to time.
- Find people who have problems you'll never have.
- Listen to them.
- See how much you can share, but more importantly see what comes back when you do.

# Takeaways

- We have the ears of very important people.
  - It is easy to lose a voice at the table if we constantly echo the same message over focused on details.
- Building a better tomorrow requires more than details and impact.
- It requires understanding our own ken.
- I hope this talk has extended yours.

# Thank You



DÉJÀ VU SECURITY

@adamcecc