Developing cybersecurity curriculum for the general public

Why cybersecurity is too important to be left to experts

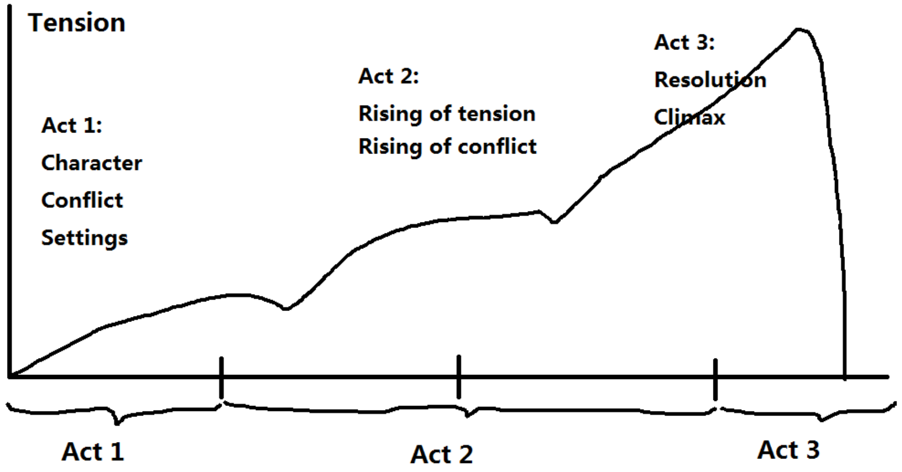
Allison Bishop

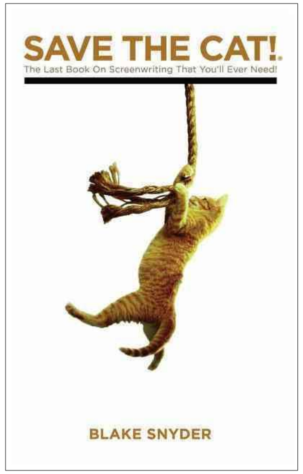
Proof Trading

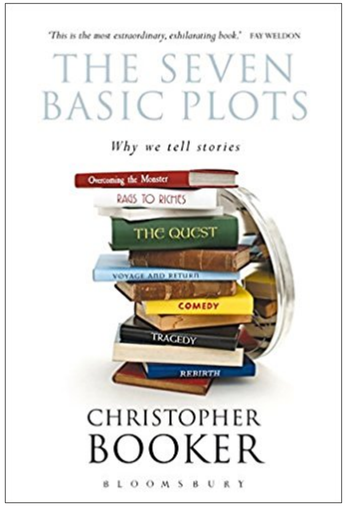
The science of writing

There is a method to the madness.

There is common structure underlying stories



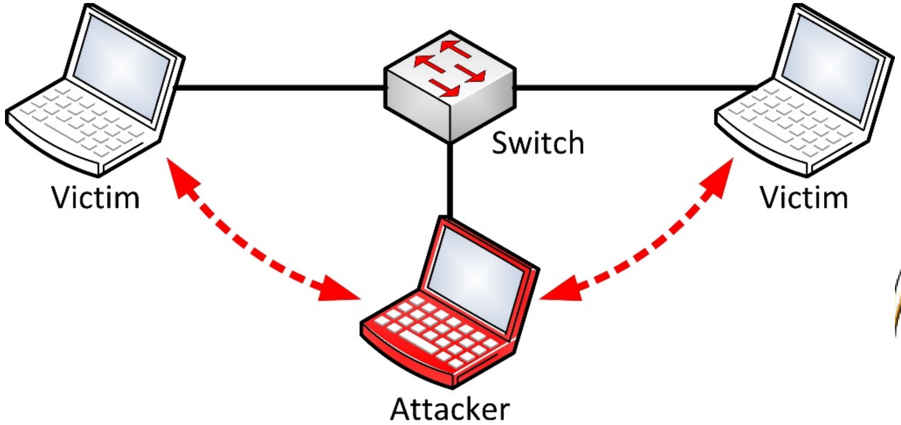




There are heroes and villains, and their behaviors are driven by their goals, as well as the tools they are given to achieve those goals.

The way we create and make sense of complex story worlds (e.g. Game of Thrones) is not a bad start for how to create and make sense of complex systems.

cryptography, we are pretty good at character development for villai



The many faces of Eve

We consider several types of adversaries

Let me stalk you on facebook until I accidently like a post you made six months ago.

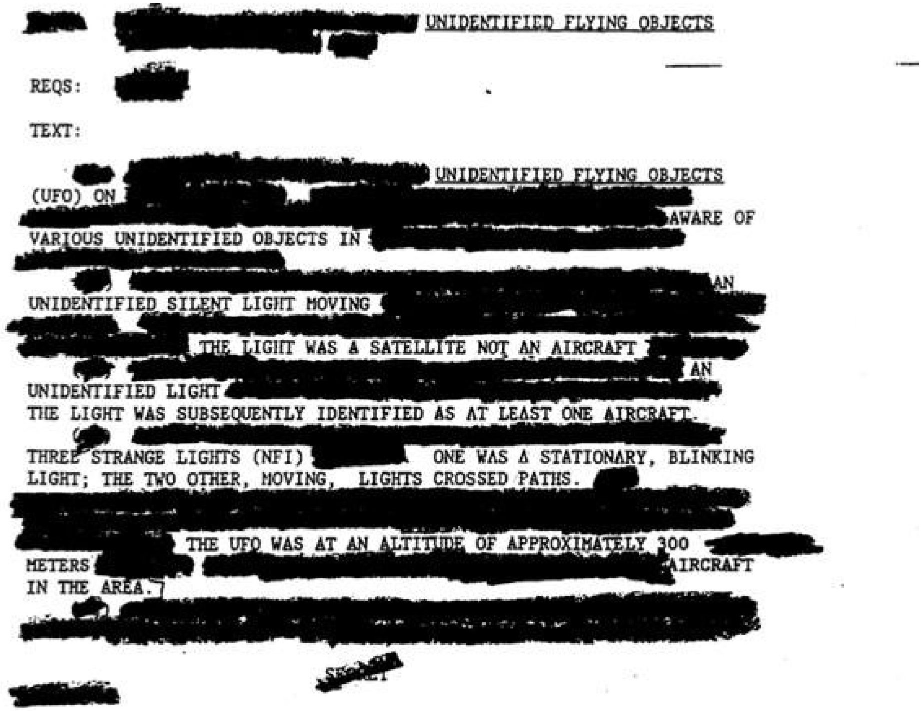
- State-level
- Corporate
- Individual

Adversaries vary in terms of *Resources* and *Access*

- How much time do your adversaries have?
- What computational resources are at their disposable?
- What kinds of access might they achieve?

A Few Examples

- Longterm government secrets



[redacted] UNIDENTIFIED FLYING OBJECTS

REQS: [redacted]

TEXT:

[redacted] UNIDENTIFIED FLYING OBJECTS
(UFO) ON [redacted] AWARE OF
VARIOUS UNIDENTIFIED OBJECTS IN [redacted] AN
UNIDENTIFIED SILENT LIGHT MOVING [redacted]
THE LIGHT WAS A SATELLITE NOT AN AIRCRAFT [redacted] AN
UNIDENTIFIED LIGHT [redacted]
THE LIGHT WAS SUBSEQUENTLY IDENTIFIED AS AT LEAST ONE AIRCRAFT.

THREE STRANGE LIGHTS (NFI) [redacted] ONE WAS A STATIONARY, BLINKING
LIGHT; THE TWO OTHER, MOVING, LIGHTS CROSSED PATHS. [redacted]
THE UFO WAS AT AN ALTITUDE OF APPROXIMATELY 300
METERS [redacted] AIRCRAFT
IN THE AREA. [redacted]

[redacted]

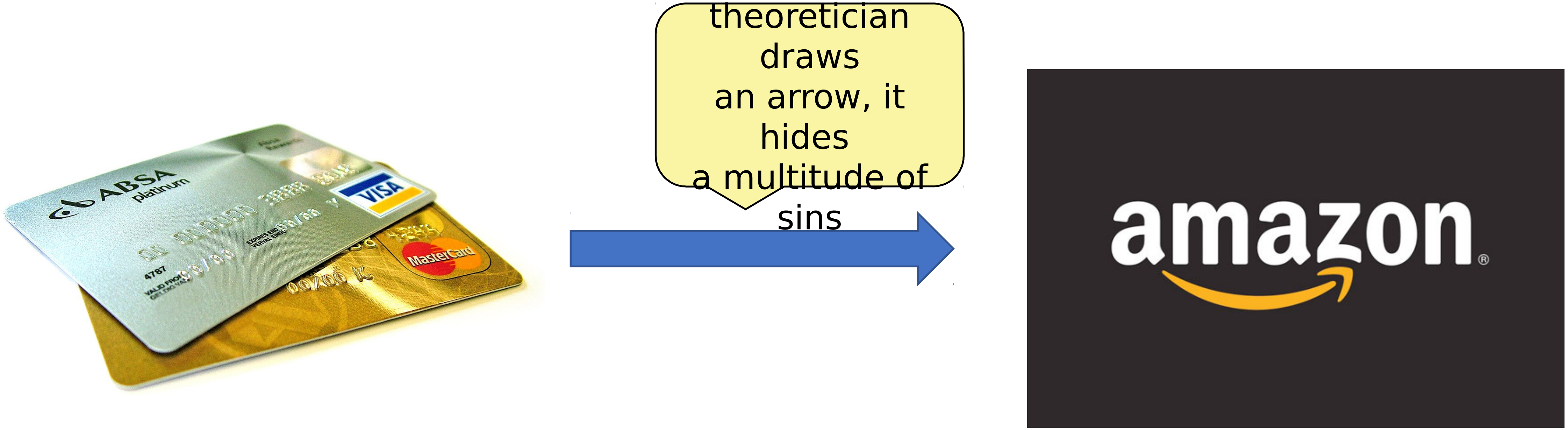
Expected Adversary Characteristics:

Goal is to be secure against nation-state level attacks over decades,
Lots of computational resources invested
Access to messages in flight likely,
Access to stored secrets hopefully not

This kind of
scenario
has driven much of
theoretical
cryptography
research since
1980s

A Few Examples

- Online Financial Transactions



Whenever a theoretician draws an arrow, it hides a multitude of sins

Expected Adversary Characteristics:

Goal is to be secure against credit card thieves over years,
Plenty of computational resources invested (since profitable).
Access to messages in flight likely,
Some database breaches to be expected,
Reuse of cards over many different websites/services
creates a rich attack surface.
Fraud detection and mitigation mechanisms deploye
by banks and credit card companies attempt to
limit profitability and increase resources required fo
successful attack.

This kind of
scenario
Is theoretically a
good fit for crypto,
but suffers
from a lot of
engineering
challenges/failures.

A Few Examples

- Your real-time location data

Raise your hand if you think you have a clue what entities have access to your location at any given moment.

Come on. I dare you.

Expected Adversary Characteristics?

One possible goal is to be secure today against an individual stalker who may ha
had past access to your phone.

Need to consider corporate actors you interact with through apps, etc. that may access your location data in the clear

Computational resources of attacker may be limited, as well as level of technical sophistication

This kind of scenario has been relatively neglected by theoreticians. Something now starting to change.

But what about character development for cryptography’s heroes and heroines?

Alice and Bob in the 80s:

Hey.

Hey.

We can use encryption to talk so our parents can’t spy on us.

Radical.

Alice and Bob in the 90s:

??

And I can like totally use daddy’s credit card
on the internet now, and it’s like, it’s like way cooler
Than even the mall, but I still have to go to the mall,
you know, to be seen and stuff, but that’s becoming
like *so as if*, you know?

Alice and Bob in the 2000s:

“Hey Bob, isn’t social networking more fun than thinking about data security?

I’ve completely lost track of
who can see my pics,
and I’m weirdly ok with it!”

“Let’s be serious, Alice.
Leakage-resilient, simulation-secure
MPC for formula-based ABE policies
is a *real world* problem. “

“Also, does this hoodie and glasses
combo make me look like
a plausible dot.com founder?”

Alice and Bob in the 2010s:

Hey Alice, did you know whats app has end-to-end encryption?

Whatevs.

Don’t you think that’s cool?

I feel like we have nothing left to say to each other.

I am Satoshi.

No you’re not, Bob. Just no.

Alice and Bob’s Marriage Plot…

(a lesson in how *not* to explain key exchange, perhaps?)

- Bob wants to send an engagement ring to Alice through the mail
- But the mailman may try to open packages and steal valuables
- Bob puts his lock on the package, sends to Alice
- Alice adds her lock to the package, sends to Bob
- Bob removes his lock, sends back to Alice

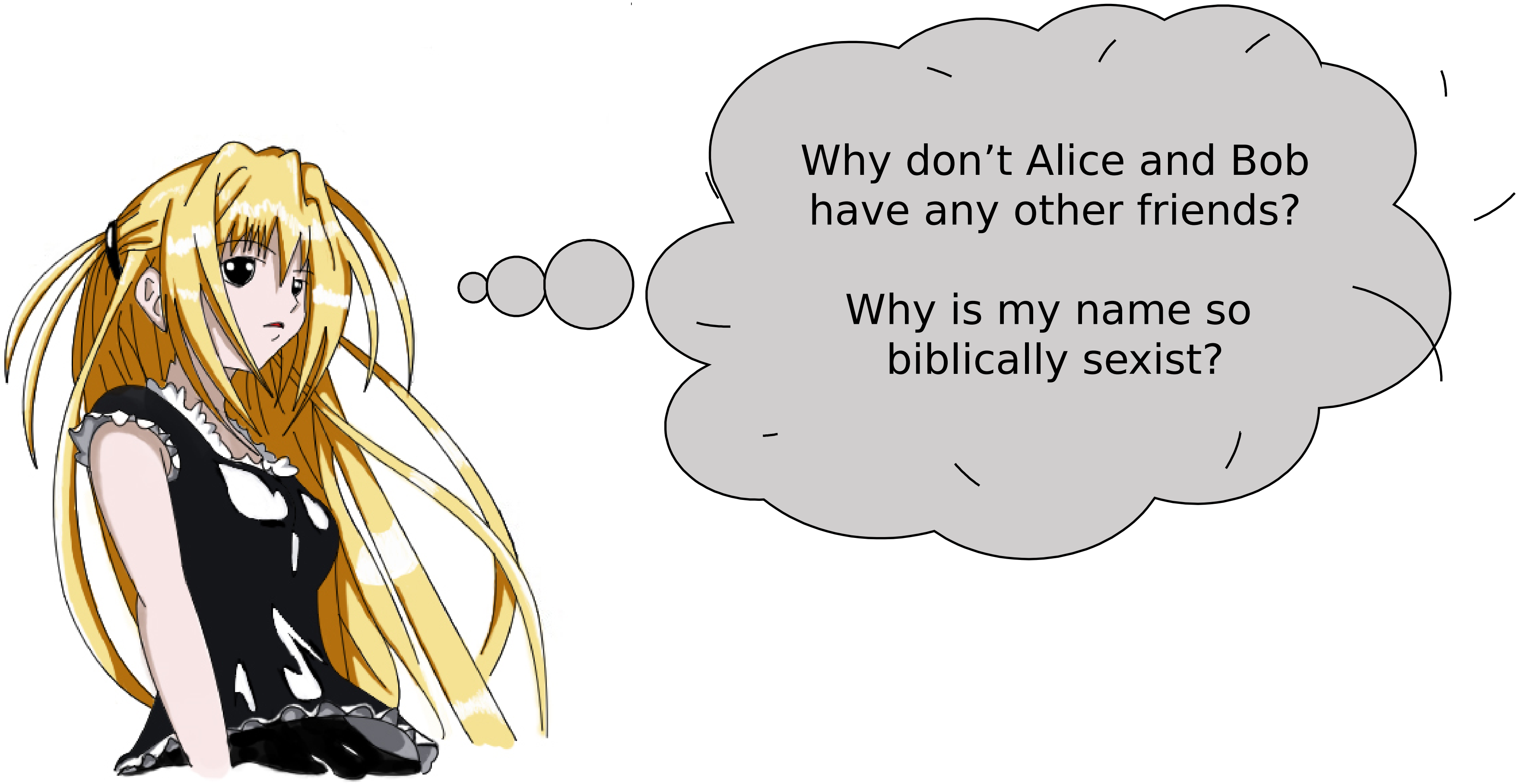
This just raises so many questions.

1. What about man in the middle attacks?

2. Why doesn’t the mailman invest in bolt cutters?

3. Why is Bob sending an engagement ring in the mail in the first place?

What Eve Really Wants to Know…



Why don’t Alice and Bob have any other friends?

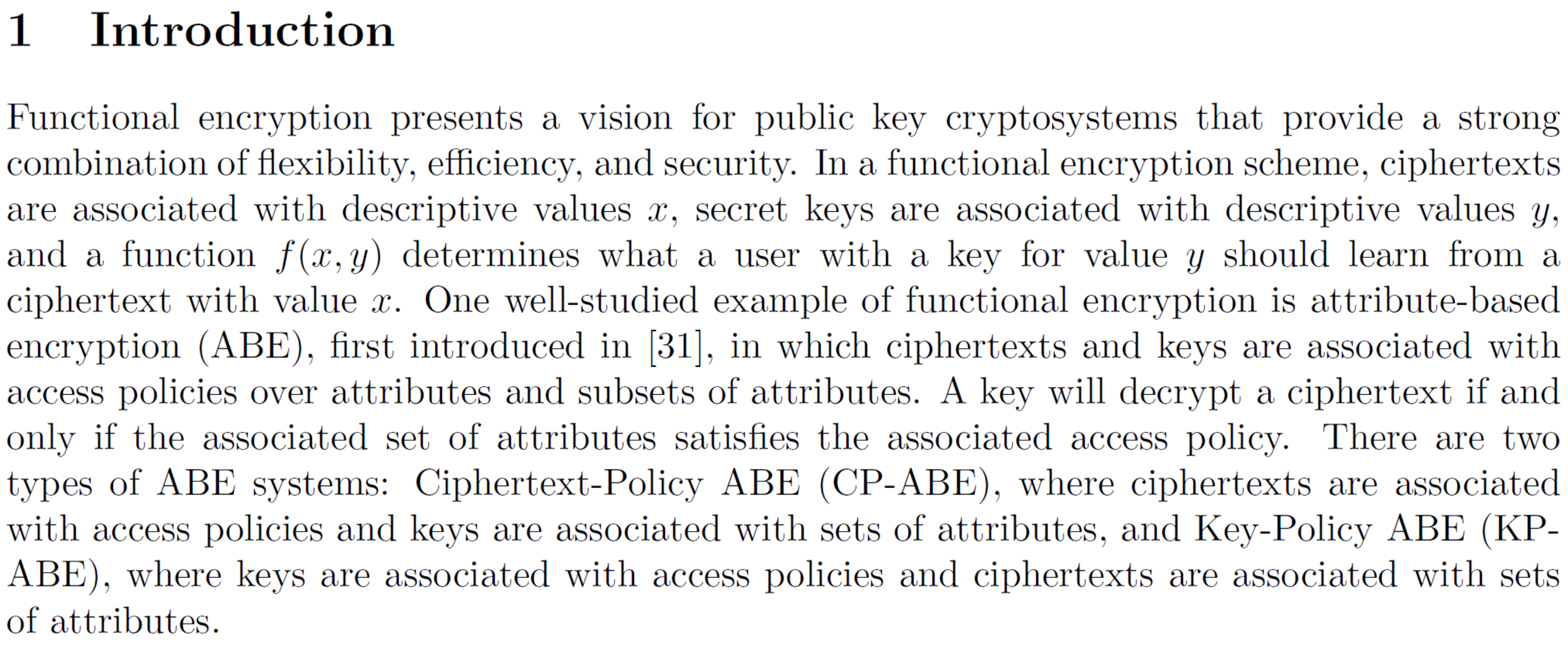
Why is my name so biblically sexist?

Cryptography has really dropped the ball on defining the goals for its heroes/heroines in resonating and compelling ways.

Too often we often lazily treat cryptography’s tools as goals in themselves.

Me writing a research paper in graduate school…

Advice to my former, grad student self:
Saying a vision exists and actually laying out a vision are different things!



1 Introduction

Functional encryption presents a vision for public key cryptosystems that provide a strong combination of flexibility, efficiency, and security. In a functional encryption scheme, ciphertexts are associated with descriptive values x, secret keys are associated with descriptive values y, and a function $f(x, y)$ determines what a user with a key for value y should learn from a ciphertext with value x. One well-studied example of functional encryption is attribute-based encryption (ABE), first introduced in [31], in which ciphertexts and keys are associated with access policies over attributes and subsets of attributes. A key will decrypt a ciphertext if and only if the associated set of attributes satisfies the associated access policy. There are two types of ABE systems: Ciphertext-Policy ABE (CP-ABE), where ciphertexts are associated with access policies and keys are associated with sets of attributes, and Key-Policy ABE (KP-ABE), where keys are associated with access policies and ciphertexts are associated with sets of attributes.

Goal or Tool?

- “Encrypt the data at rest”
- “Get a PhD”
- “Put it on the blockchain”
- “Use AI”
- “User Privacy”
- “Diversity” – we’ll come back to this one

“Privacy” and “security” are not really good goals.

- They’re vague.

- They don’t resonate as well with younger generations.

- They are seen as reactionary and holding back “progress”

Goals for cybersecurity outreach

- Define security-related goals that are more resonate, more clear, and more adaptable:

Neutral access to information
You may not care about your “private” data being “known,”
But you may care about it being used to filter the news you read.
The active goal of controlling information access may resonate better than
The passive goal of avoiding data leakage.

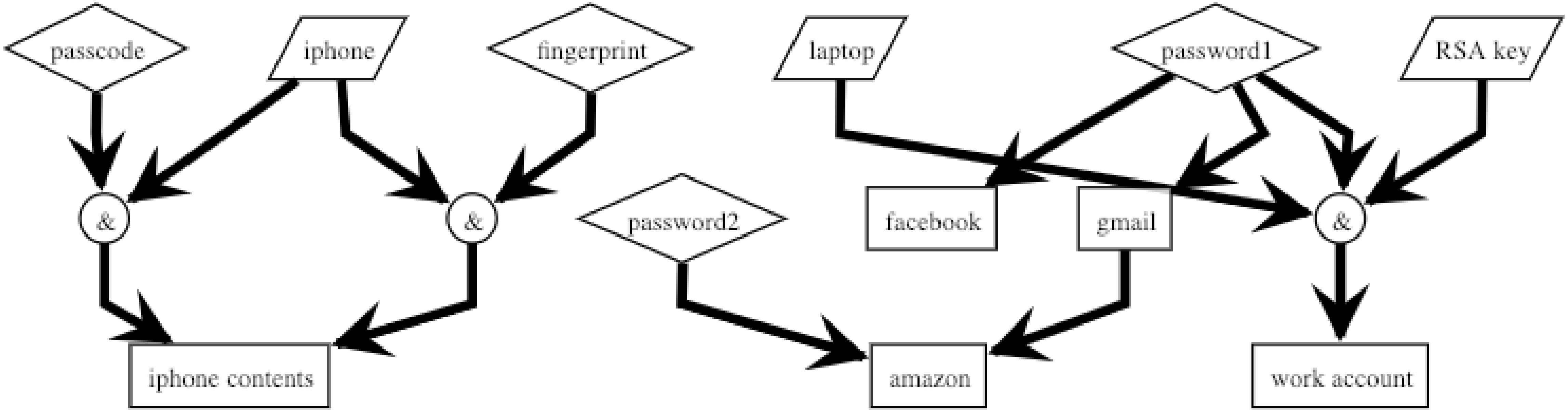
- Empower people with the tools and knowledge to work towards these goal.

Tools for cybersecurity outreach

Threat modeling 101 for the general public: a 2 hr workshop (April 20
understanding and controlling the attack surface
you create through everyday interactions with technology

Collaboration with awesome students: Justin Whitehouse, Yogi Koppo
Michael Paciullo (and several others who beta-tested workshop mate

Mapping out our digital universe:



Imagining a specific attacker.

I imagine an attacker named Jamie who is a stalker/bully.

Her goal is to get embarrassing personal data to humiliate me in front of my friends.

She is nothing exactly like the girl who bullied me in middle sch

Exercise people really like to do:

Imagine an attacker.

What do they want?

What opportunities do they have?

What resources/knowledge do they have?

For each thing in your digital universe, set a difficulty score for your attacker to *directly* acquire it:

Laptop 8

Facebook account 10

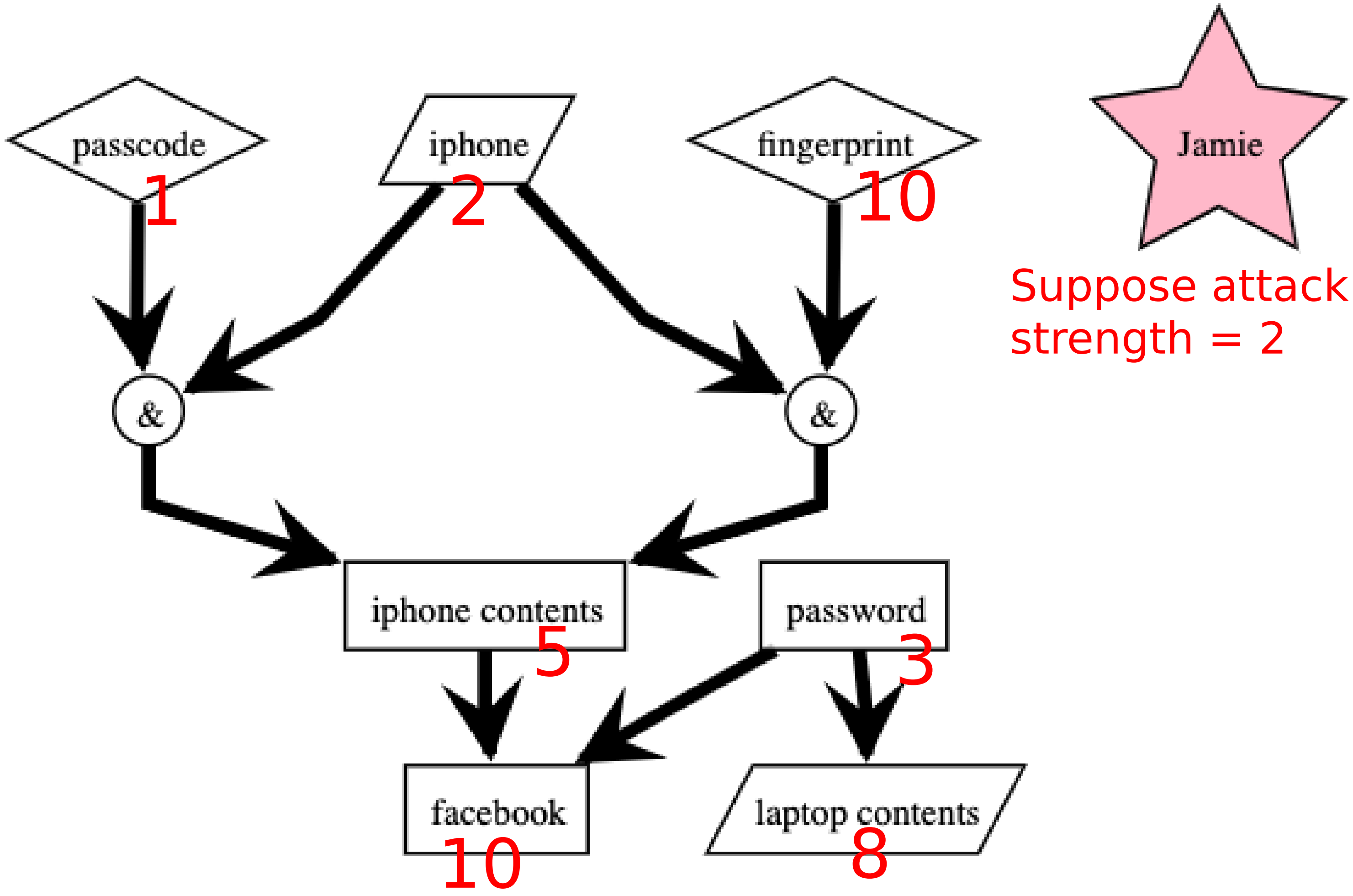
iphone 2

password 3

passcode 1

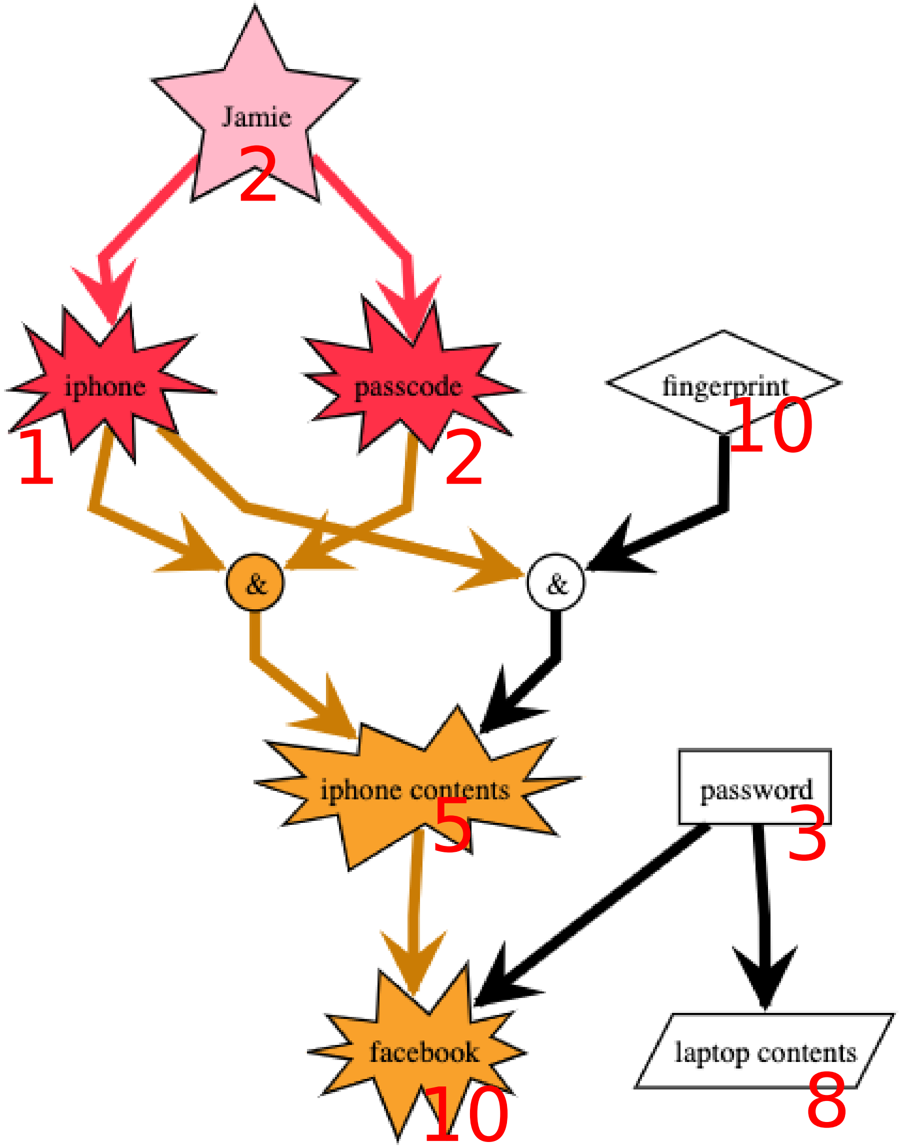
= easy --> 10 = very hard

Now simulate an attack and follow its consequences:



Suppose attack strength = 2

We can simulate an attack and follow its consequences:



3eyond threat modeling for personal devices:

Basic structure of networks/internet communication

Ad-targeting and how (if?) you can control your exposure

Anything else we think of that could be interesting to non-experts without too much background or time-commitment required to lea

Back to diversity – a test case for threat modeling

Diversity in tech/cybersecurity has been stated as a “goal”
by universities, companies, funding agencies, etc. for decades now

Tools have been/ are being deployed to work towards this goal:
funding, events like this, corporate donations and participation, etc.

So what might be going wrong?

The “Real” goal?

rporations and the organizations that cater to them often make
case that diversity is a tool to solve a workforce supply problem.
of course they care, they want to solve the problem as much as you

ey point to early stages in the pipeline (e.g. elementary school, middle school,
school, college) where diversity leaks out, and insist that this is what
ould be fixed. But don’t worry, they’ve donated some ipads to kids!
they’ve sponsored an event where people will talk about diversity.
d they pinky swear that once the pipeline issues are fixed, they’ll
ally hire lots of engineers from underrepresented groups.

I have a very nuanced and sophisticated response to this: 😝

Why this makes *no sense:*

Diversity is *not* a solution to technical workforce shortage projections. is is because while the universities and other traditional training resources e not gender/race/etc. balanced, they are operating at full capacity!

Many companies hire second career software engineers out of boot camps, etc. there is no need to wait for today’s kindergarteners to reach adulthood solve this problem.

ar of future technical workforce shortages belies a more real goal of corporations: stability.

ations that are doing well are risk-averse, and want as little change as possible, as slowly as pos

ate diversity initiatives can skeptically be viewed as tools to achieve this goal: placating people ations are doing something about the problem and putting off the day when the corporations o do anything that would require deeper changes to their day-to-day practices.

But there is a better case for diversity as a tool – just not for solving workforce shortages.

Why should we care about diversity in tech?

A common trap:

Women think differently than men

↓

Underrepresentation can be justified by merit

Women think the same as men

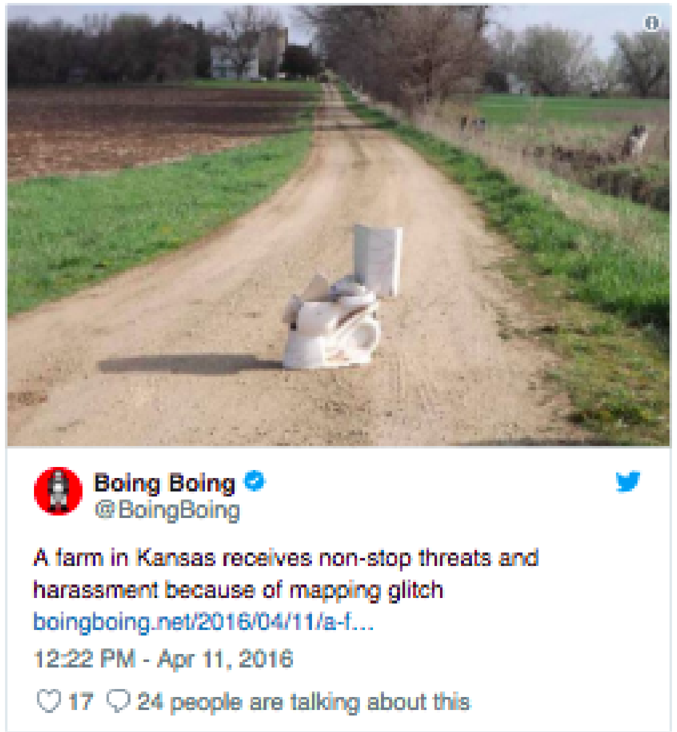
↓

Underrepresentation is not important

The illusions of merit

- Merit is a kind of quantum phenomena:
  to measure it is to change it
- Merit is not a static, objective target:
  most technology is about tradeoffs
- “diversity of thought” is not a substitute for diversity of experience
- A team that must work harder to communicate because
  of having less in common might actually produce better technology!

A modern parable

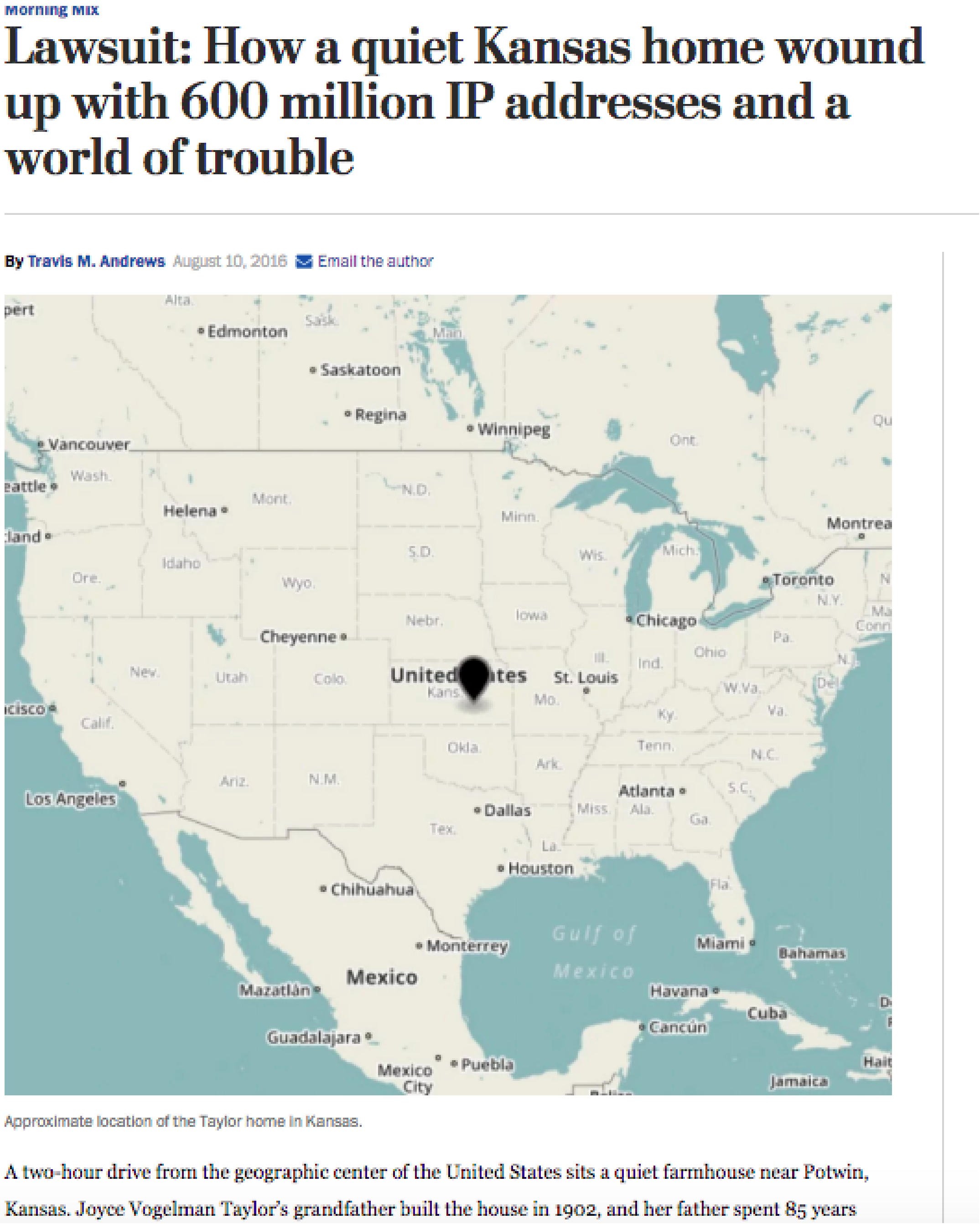


Boing Boing
@BoingBoing

A farm in Kansas receives non-stop threats and harassment because of mapping glitch boingboing.net/2016/04/11/a-f…

12:22 PM - Apr 11, 2016

♡ 17 24 people are talking about this



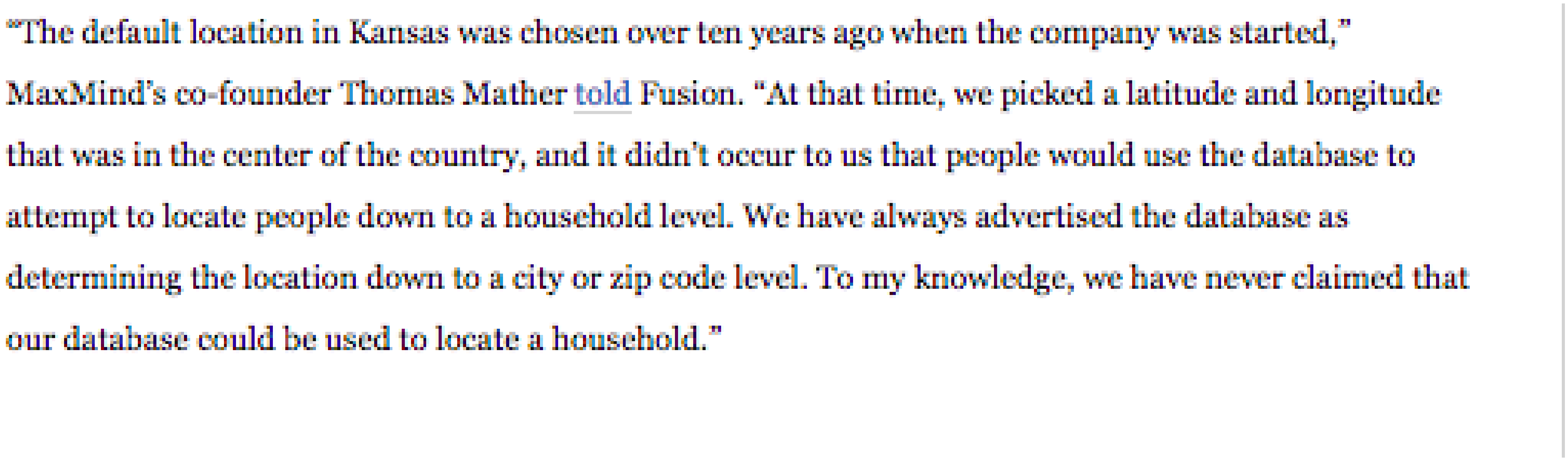
Morning Mix

Lawsuit: How a quiet Kansas home wound up with 600 million IP addresses and a world of trouble

By Travis M. Andrews August 10, 2016 Email the author

Approximate location of the Taylor home in Kansas.

A two-hour drive from the geographic center of the United States sits a quiet farmhouse near Potwin, Kansas. Joyce Vogelman Taylor's grandfather built the house in 1902, and her father spent 85 years



"The default location in Kansas was chosen over ten years ago when the company was started," MaxMind's co-founder Thomas Mather told Fusion. "At that time, we picked a latitude and longitude that was in the center of the country, and it didn't occur to us that people would use the database to attempt to locate people down to a household level. We have always advertised the database as determining the location down to a city or zip code level. To my knowledge, we have never claimed that our database could be used to locate a household."

Some estimated stats for the US
source: CDC 2010

- 1 in 6 women and 1 in 17 men will be stalked in their lifetime. (7.5 million each year)

- 1 in 4 women and 1 in 7 men will experience domestic abuse in their lifetime.

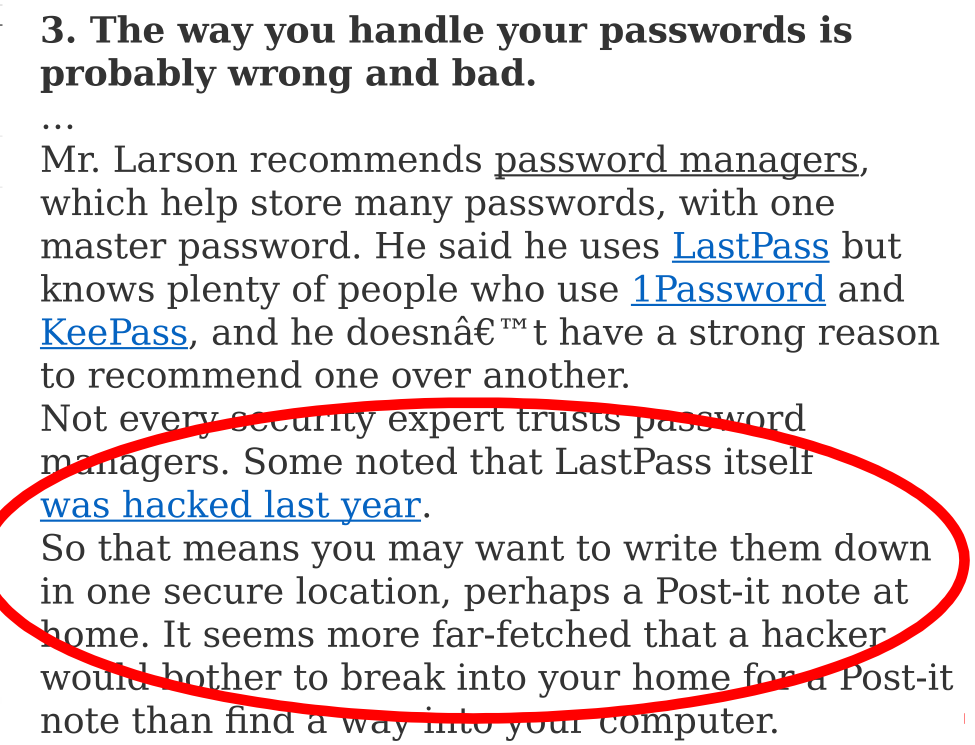
Cybersecurity “experts” often given advice not appropriate for everyone:

PERSONAL TECH

Protecting Your Digital Life in 8 Easy Steps

By JONAH ENGEL BROMWICH NOV. 16, 2016

George Etheredge for The New York Times



3. The way you handle your passwords is probably wrong and bad.

…

Mr. Larson recommends password managers, which help store many passwords, with one master password. He said he uses LastPass but knows plenty of people who use 1Password and KeePass, and he doesnâ€™t have a strong reason to recommend one over another.

Not every security expert trusts password managers. Some noted that LastPass itself was hacked last year.

So that means you may want to write them down in one secure location, perhaps a Post-it note at home. It seems more far-fetched that a hacker would bother to break into your home for a Post-it note than find a way into your computer.

Technology is about Magic Tradeoffs!

- Usability vs. Security
- Privacy vs. Personalization
- Information vs. Entertainment
- Public Health vs. Monetization

Whose interests will be served by emerging technologies?

Coming soon…

CFAIL

The first Conference for Failed Approaches and Insightful Losses in cryptology

At Columbia University in New York City, May 31-June 2 2019

www.cfail2019.com