# AI for Security (AI4Sec)

## Security Overview

COMP-5370/6370

BRIAN OBLIVION
TAN
KINGPIN
MUDGE
WELD POND
SPACE ROGUE

# Failures Come in Many Forms

- Tacoma Narrows
  - Design Failure

# Failures Come in Many Forms

- Tacoma Narrows
  - Design Failure
- Hard Rock Hotel
  - Process Failure

# Failures Come in Many Forms

- Tacoma Narrows
  - Design Failure
- Hard Rock Hotel
  - Process Failure
- Therac-25
  - Implementation Failure

# Failures Come in Many Forms

- Tacoma Narrows
  - Design Failure
- Hard Rock Hotel
  - Process Failure
- Therac-25
  - Implementation Failure
- World Trade Center
  - Intentional Failure

# Adversary

- Intelligent Actor
  - Person, Group, or Organization
- Have own:
  - Capabilities
  - Motivations
  - Intentions
- Are **NOT** restricted by expectations

# Security Mindset

A way of thinking about scenarios in order to identify and mitigate possible failures.

- Come in many form and applicable outside of computers/networks

# Security Mindset

A way of thinking about scenarios in order to identify and mitigate possible failures.

- Come in many form and applicable outside of computers/networks
- Have to think like an attacker

# Security Mindset

A way of thinking about scenarios in order to identify and mitigate possible failures.

- Come in many form and applicable outside of computers/networks
- Have to think like an attacker
  - Comprehend abilities and behavior patterns
  - Understand how search for/exploit weaknesses

# Thinking Like an Attacker

- What is the **easiest/simplest** way to win?
  - “weakest link”, “low-hanging fruit”

# Thinking Like an Attacker

- What is the **easiest/simplest** way to win?
  - “weakest link”, “low-hanging fruit”
- What are the **explicit assumptions** built into the system?
  - What are the creator’s expectations?
  - Who else does the creator rely on?

# Thinking Like an Attacker

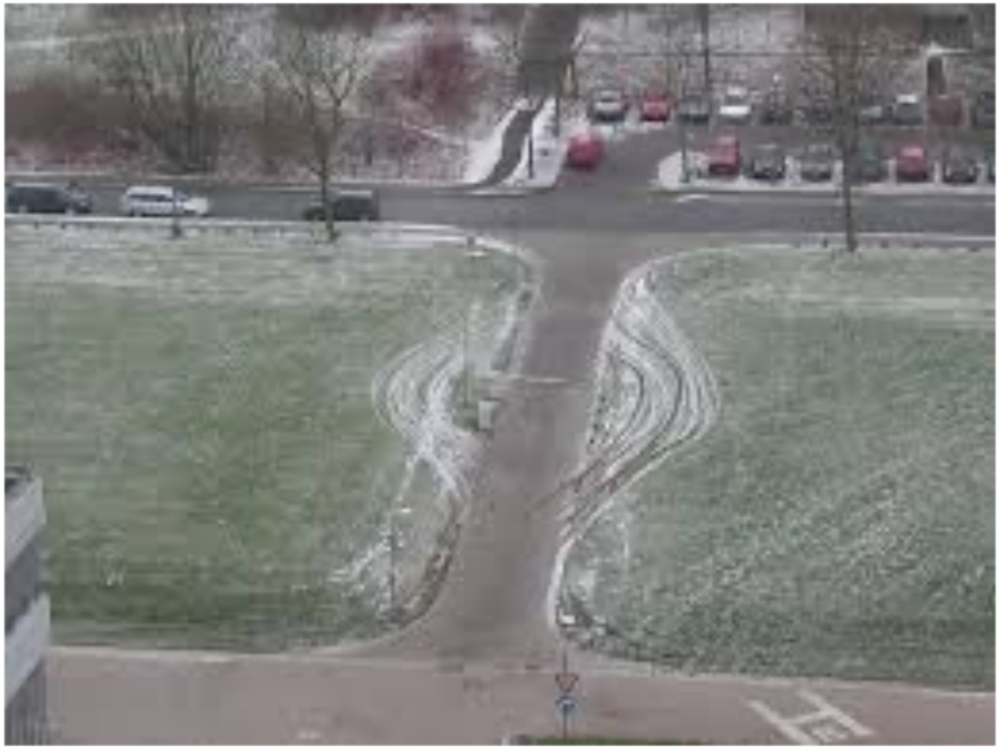
- What are the **explicit assumptions** built into the system?

# Thinking Like an Attacker

- What is the **easiest/simplest** way to win?
  - “weakest link”, “low-hanging fruit”
- What are the **explicit assumptions** built into the system?
  - What are the creator’s expectations?
  - Who else does the creator rely on?
- What are the **implicit assumptions** which the aren’t always true/strong?
  - “outside the box” solutions

# Thinking Like an Attacker

- What are the **implicit assumptions** which the aren’t always true/strong?



# Security Mindset

A way of thinking about scenarios in order to identify and mitigate possible failures.

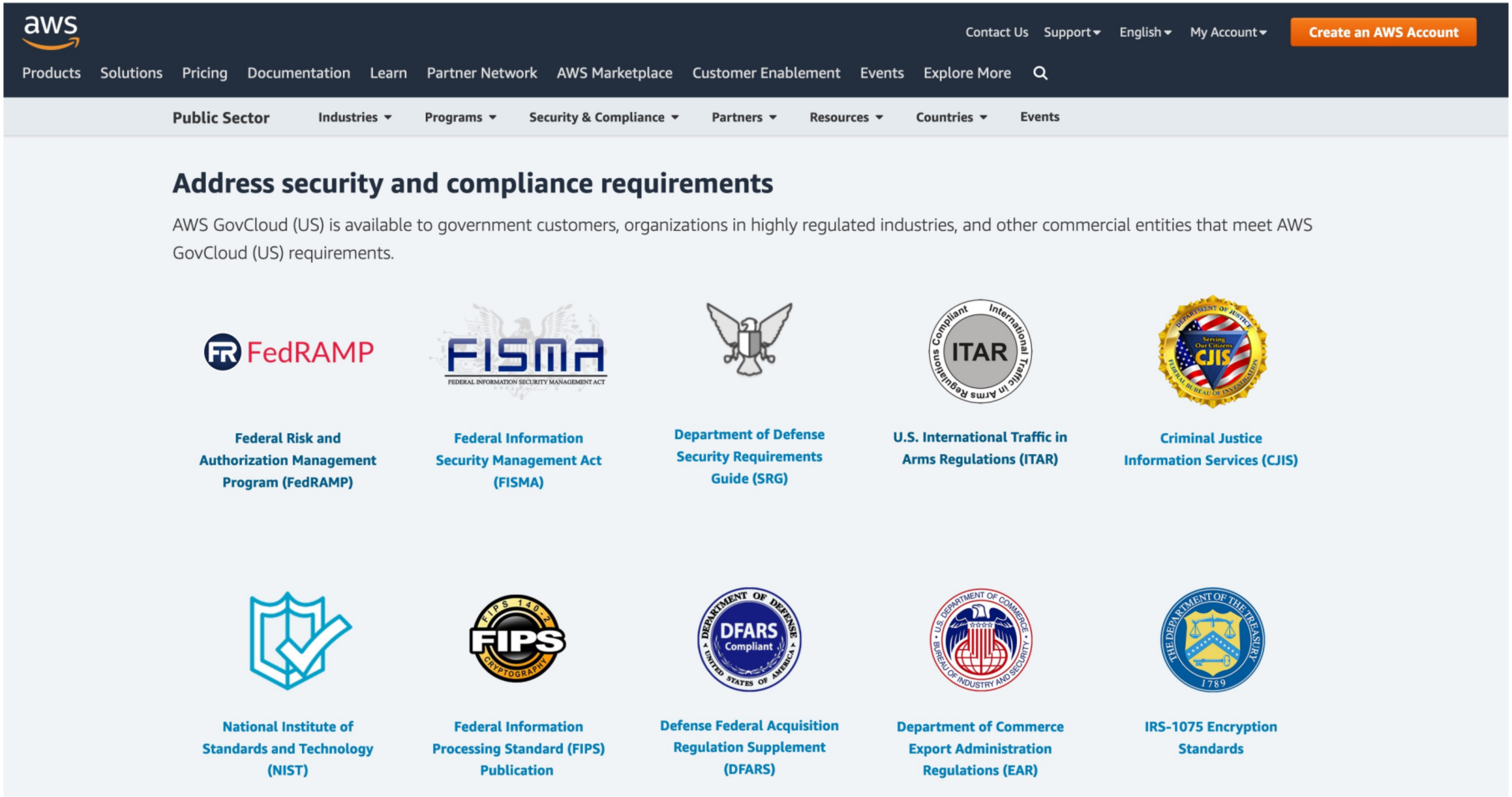
- Come in many form and applicable outside of computers/networks
- Have to think like an attacker
  - Comprehend abilities and behavior patterns
  - Understand how search for/exploit weaknesses
- Have to think like a defender
  - Identify what is being protected against who
  - Analyze/Evaluate cost-benefit trade-offs

# Thinking Like a Defender

- What **assets** are you trying to protect?
  - What about those assets is important?
- Who are you trying to **defend against**? Who are you willing to **let succeed**?
  - Nothing is ever 100% secure against all actors

# …a little practice…

# Certified != Secure



## Address security and compliance requirements

AWS GovCloud (US) is available to government customers, organizations in highly regulated industries, and other commercial entities that meet AWS GovCloud (US) requirements.

- Federal Risk and Authorization Management Program (FedRAMP)
- Federal Information Security Management Act (FISMA)
- Department of Defense Security Requirements Guide (SRG)
- U.S. International Traffic in Arms Regulations (ITAR)
- Criminal Justice Information Services (CJIS)
- National Institute of Standards and Technology (NIST)
- Federal Information Processing Standard (FIPS) Publication
- Defense Federal Acquisition Regulation Supplement (DFARS)
- Department of Commerce Export Administration Regulations (EAR)
- IRS-1075 Encryption Standards

# Improving Security

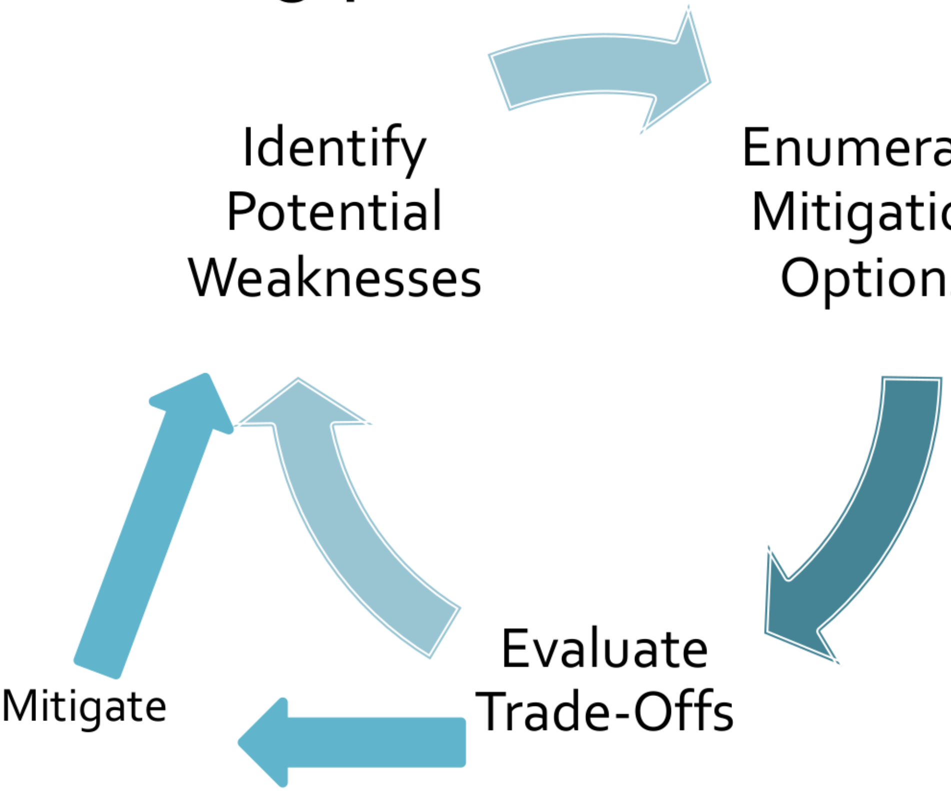
- Security is **not a checkbox** to hit on the way to releasing a product
  - “HIPAA Compliant” =!= safe/secure/private
  - “Used cipher X” =!= “Used cipher X correctly”

# Improving Security

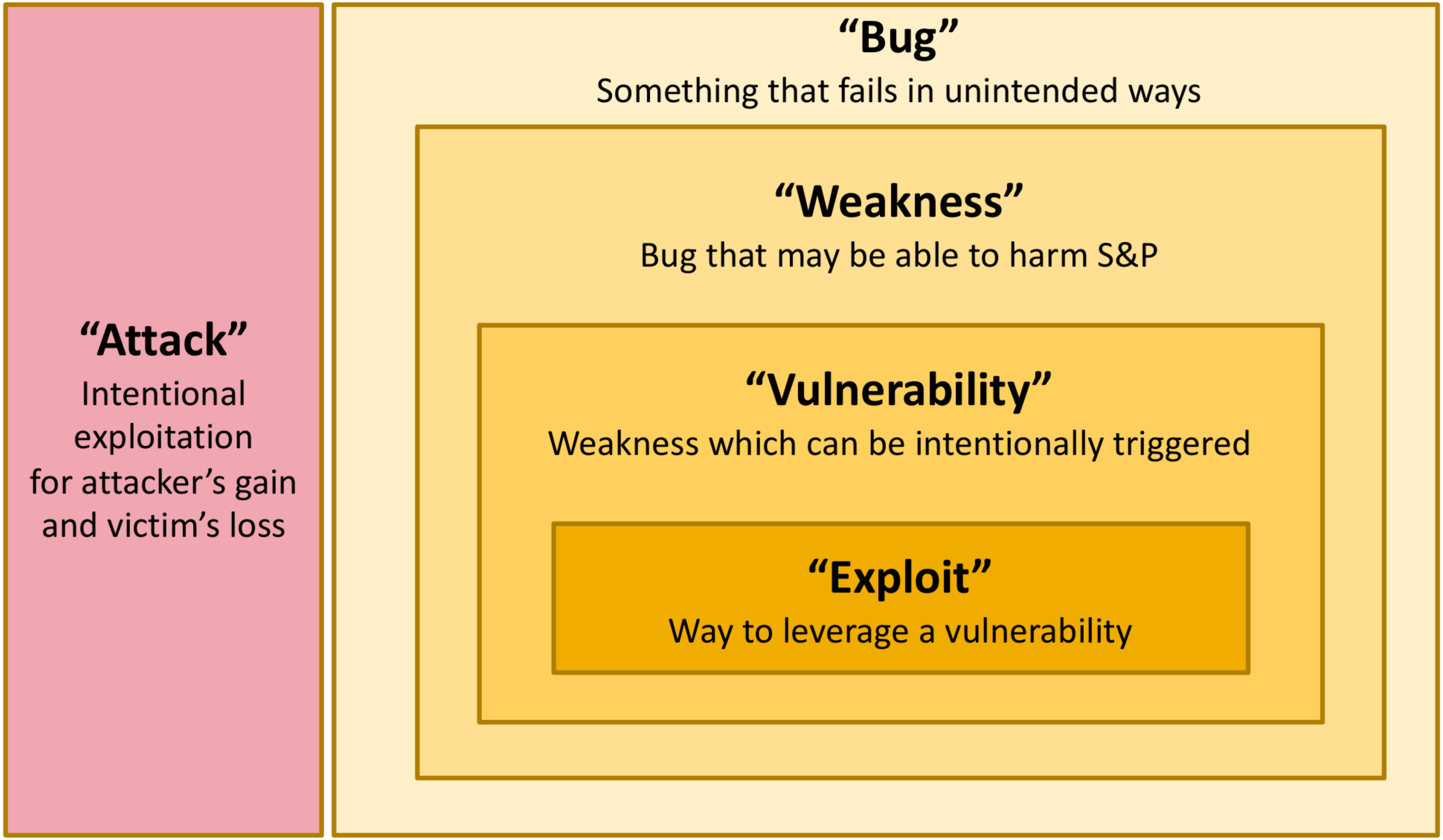
- Security is **not a checkbox** to hit on the way to releasing a product
  - “HIPAA Compliant” =!= safe/secure/private
  - “Used cipher X” =!= “Used cipher X correctly”
- Security is the outcome of a **process** and is not a *product* by itself
  - It is extremely hard to add-to design later
  - Is an on-going effort throughout the lifecycle

# Threat Modeling

A systematic approach to analyzing and understanding potential weaknesses.



# Security Vocab



**“Attack”**

Intentional exploitation for attacker’s gain and victim’s loss

**“Bug”**

Something that fails in unintended ways

**“Weakness”**

Bug that may be able to harm S&P

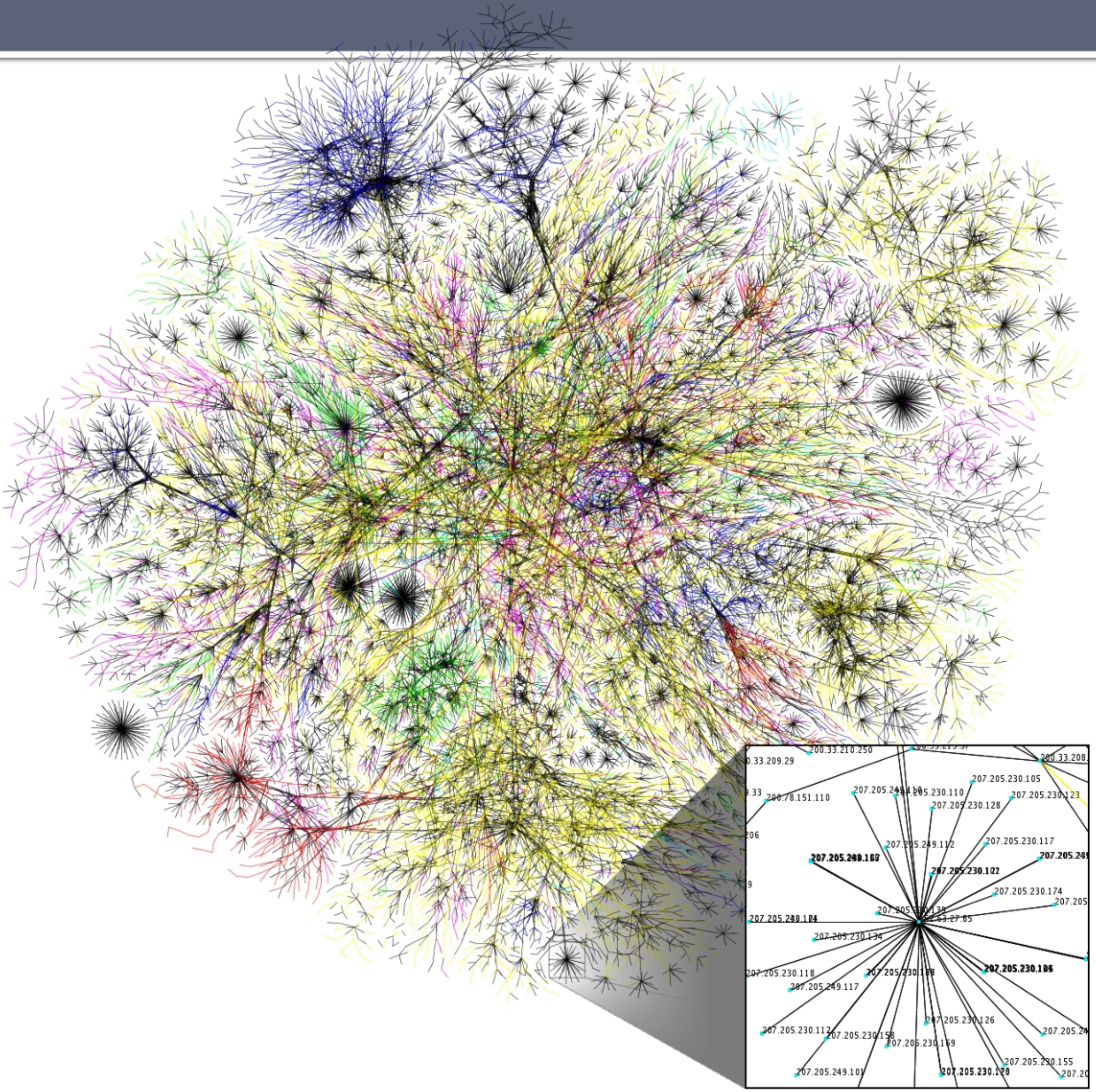
**“Vulnerability”**

Weakness which can be intentionally triggered

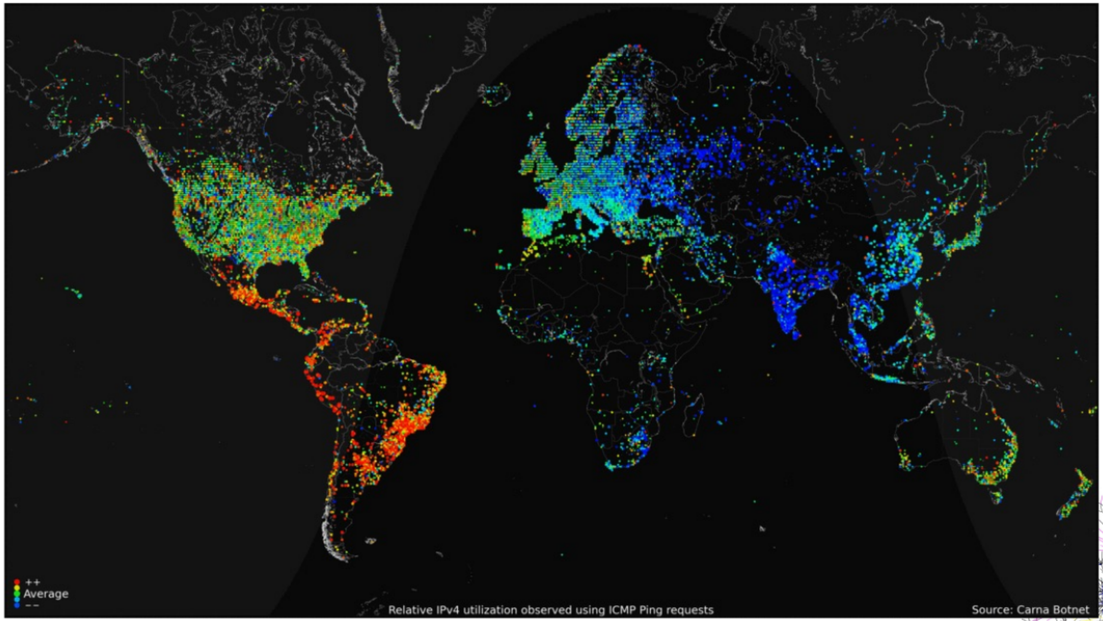
**“Exploit”**

Way to leverage a vulnerability

# The Internet

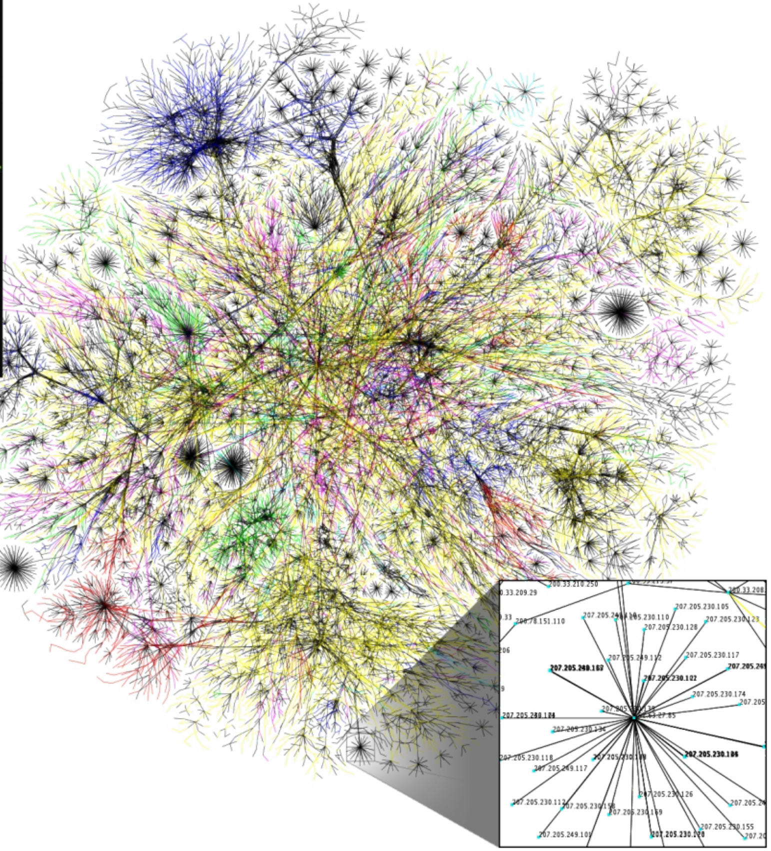


# The Internet is Complicated

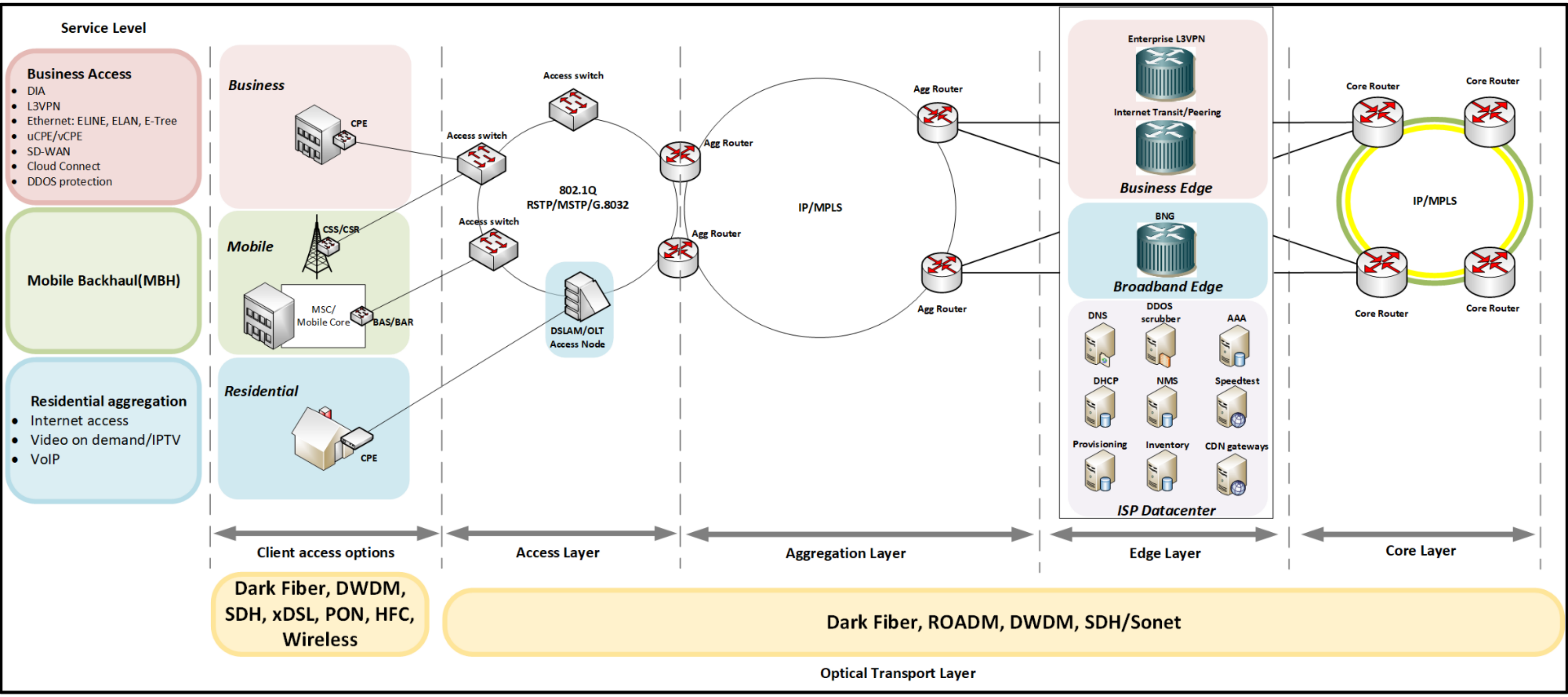


Relative IPv4 utilization observed using ICMP Ping requests

Source: Carna Botnet



# Simplified is Complicated



Service Level

**Business Access**

- DIA
- L3VPN
- Ethernet: ELINE, ELAN, E-Tree
- uCPE/vCPE
- SD-WAN
- Cloud Connect
- DDOS protection

**Mobile Backhaul(MBH)**

**Residential aggregation**

- Internet access
- Video on demand/IPTV
- VoIP

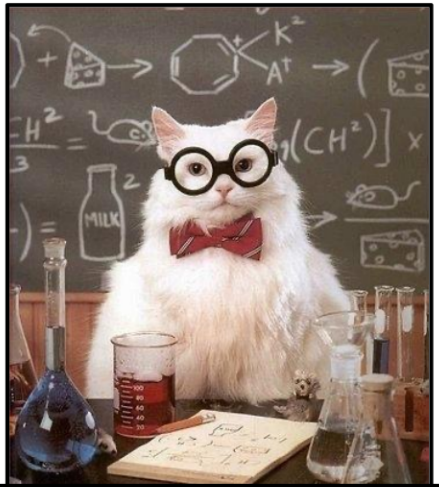
Client access options | Access Layer | Aggregation Layer | Edge Layer | Core Layer

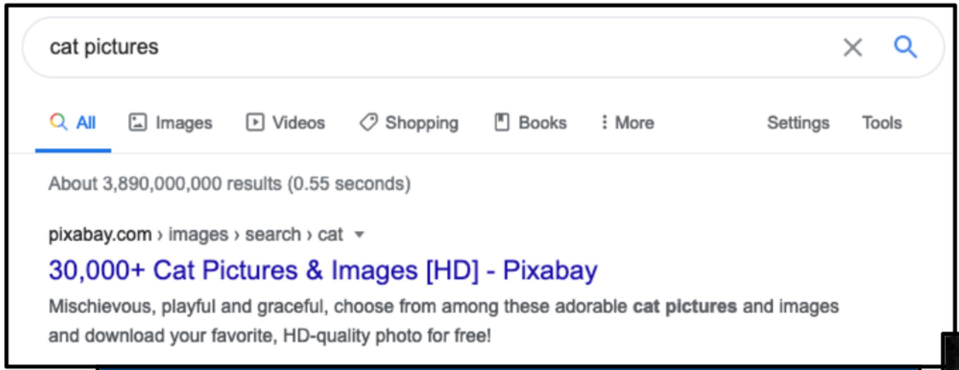
Dark Fiber, DWDM, SDH, xDSL, PON, HFC, Wireless

Dark Fiber, ROADM, DWDM, SDH/Sonet

Optical Transport Layer

# The “web” was built to serve cat pictures.





cat pictures

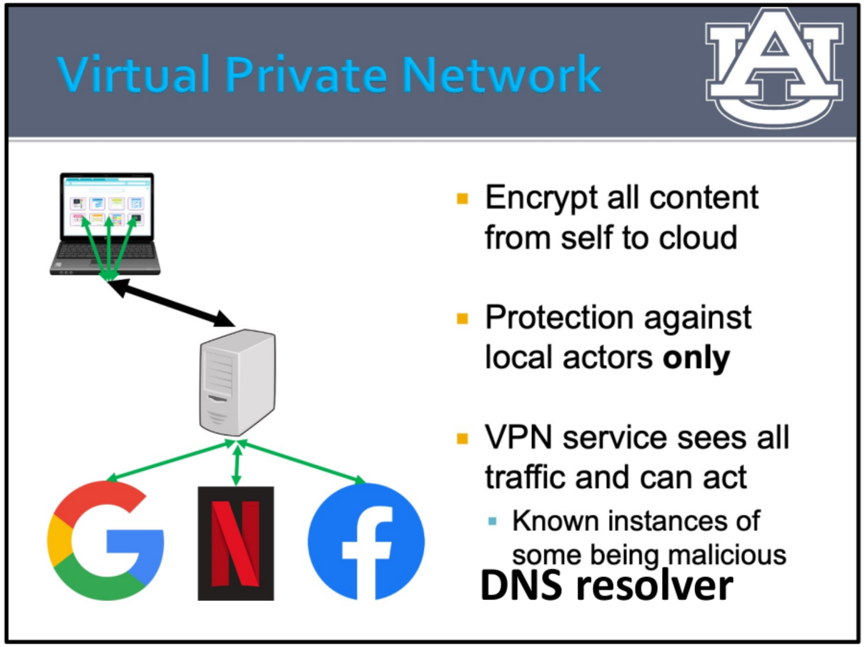
About 3,890,000,000 results (0.55 seconds)

pixabay.com › images › search › cat

30,000+ Cat Pictures & Images [HD] - Pixabay

Mischievous, playful and graceful, choose from among these adorable **cat pictures** and images and download your favorite, HD-quality photo for free!

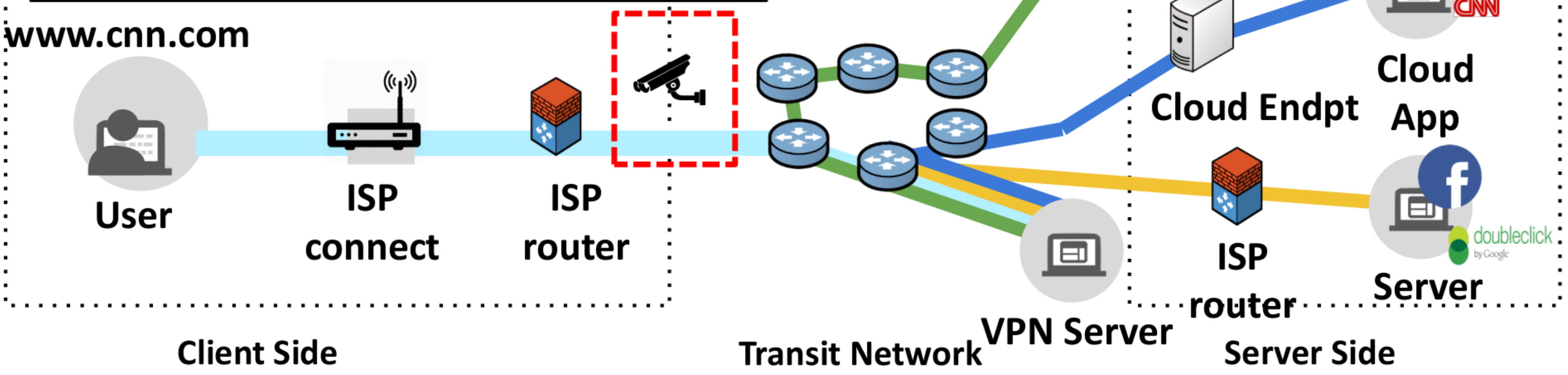
# Network Security



## Virtual Private Network

- Encrypt all content from self to cloud
- Protection against local actors **only**
- VPN service sees all traffic and can act
  - Known instances of some being malicious

- DPI much less useful w/ encrypted traffic
  - VPNs are the simplest

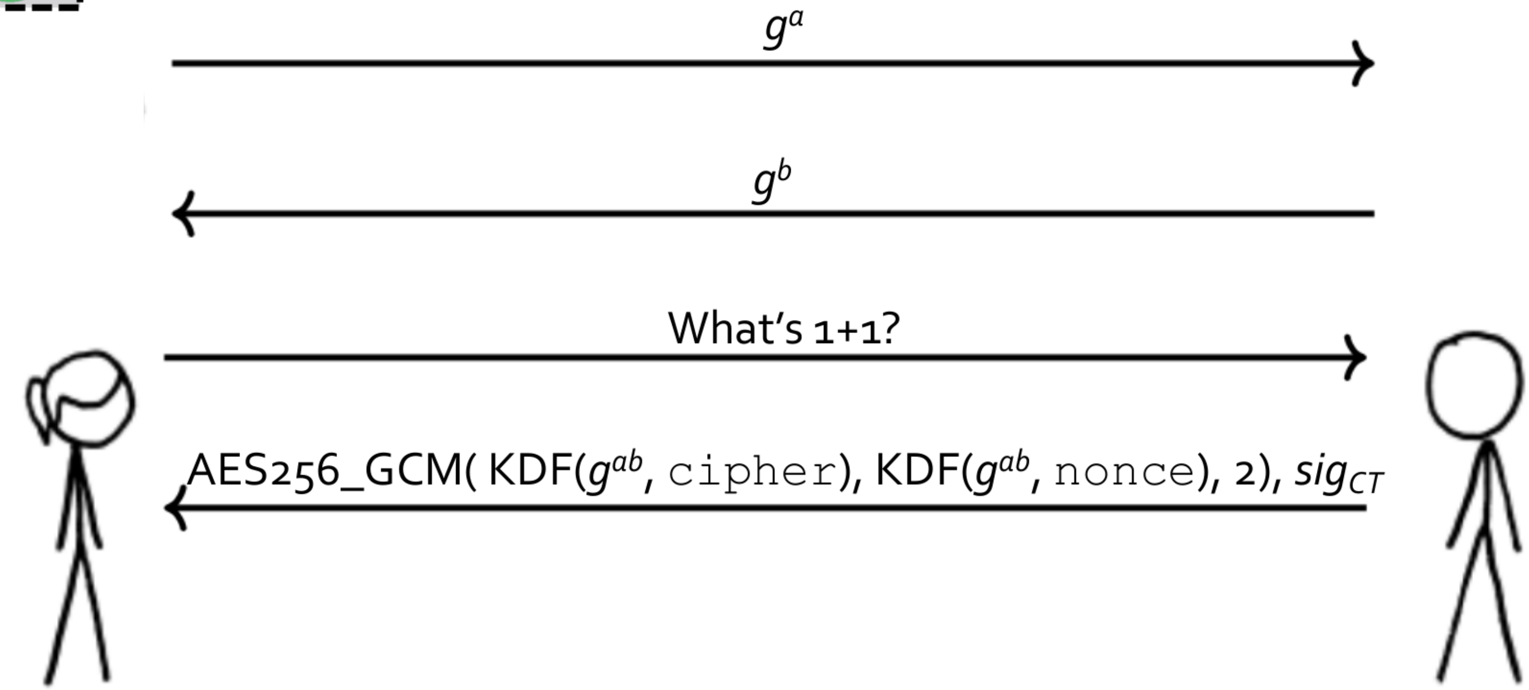


# Secure Channels + Crypto

☺ Confidentiality

☺ Message Integrity

☺ Sender Authenticity



$g^a$

$g^b$

What's 1+1?

AES256_GCM( KDF($g^{ab}$, `cipher`), KDF($g^{ab}$, `nonce`), 2), $sig_{CT}$

# Web Security

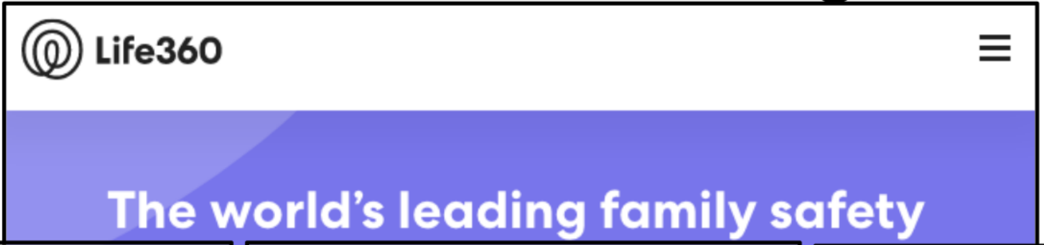
```
<div>
    Hello {get name from url}
</div>
```

https://example.com?name=Alice%0D%3Cimg%20src%3D%22https%3A%2F%2Fexample.com%2Fdog-picture.png%22%3E

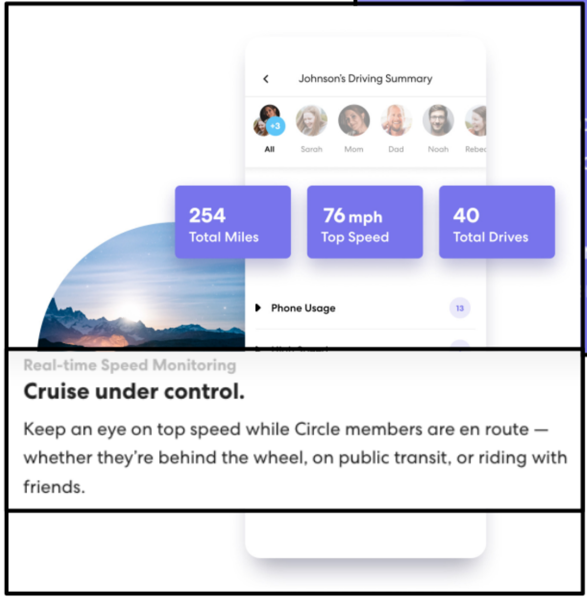
```
<div>
    Hello Alice
<img src=‘https://example.com/dog-
picture.png’>
</div>
```

# Application Security

- Some instances are significantly less obvious due to their branding


Life360

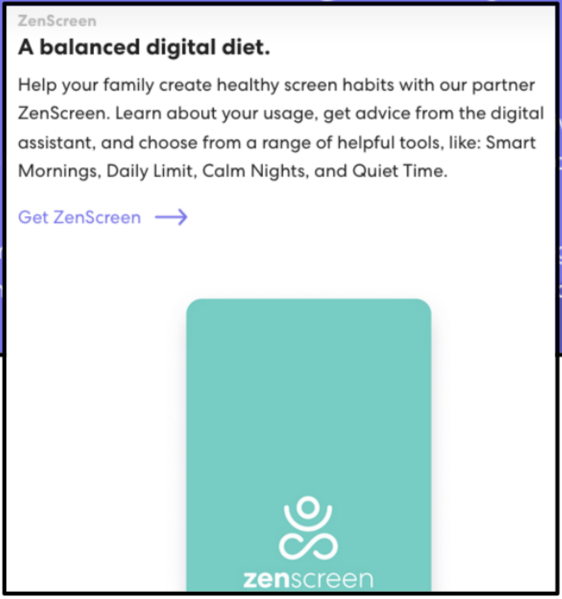
The world's leading family safety



Real-time Speed Monitoring

**Cruise under control.**

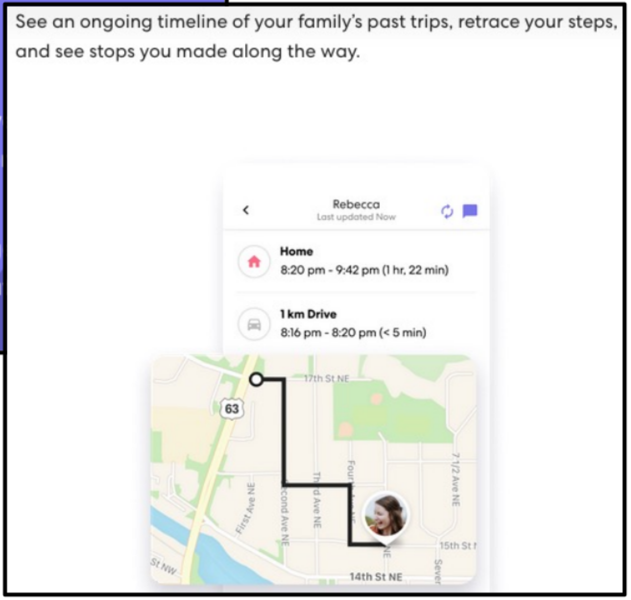
Keep an eye on top speed while Circle members are en route — whether they're behind the wheel, on public transit, or riding with friends.


ZenScreen

**A balanced digital diet.**

Help your family create healthy screen habits with our partner ZenScreen. Learn about your usage, get advice from the digital assistant, and choose from a range of helpful tools, like: Smart Mornings, Daily Limit, Calm Nights, and Quiet Time.

Get ZenScreen →


See an ongoing timeline of your family's past trips, retrace your steps, and see stops you made along the way.

# Human Security

**Humans reuse passwords due to relatively small storage capacity**

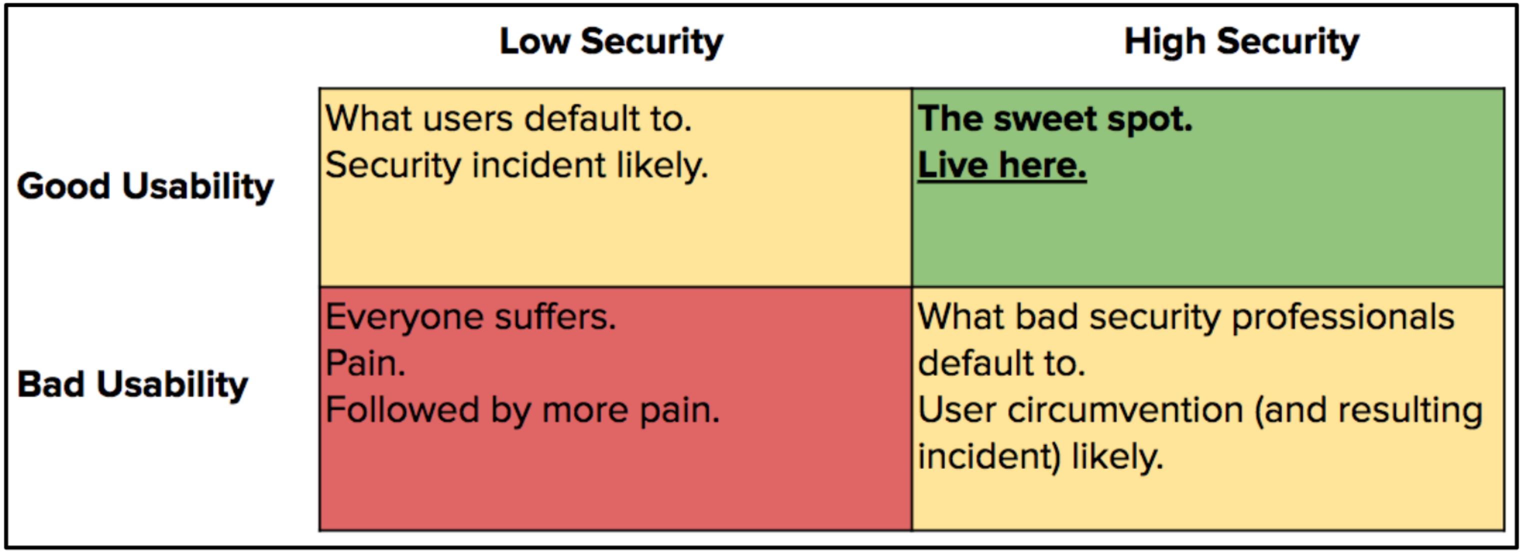
- Nearly everything requires a login
  - Important and unimportant services
- Passwords used passwords (~48 hours)

Phone (x4)
BIOS (x2)
OS login (x9)
Disk encryption (x7)
Data Services (x3)

Gmail (x5)
AU SSO login (x1)
Amazon (x2)
File Encryption (many)
Banking (x5)

# Usable Security

Making things secure is hard.
Making secure things usable is **harder**.



| | **Low Security** | **High Security** |
|---|---|---|
| **Good Usability** | What users default to.<br>Security incident likely. | **The sweet spot.**<br>**Live here.** |
| **Bad Usability** | Everyone suffers.<br>Pain.<br>Followed by more pain. | What bad security professionals default to.<br>User circumvention (and resulting incident) likely. |

## Why (Special Agent) Johnny (Still) Can't Encrypt:
## A Security Analysis of the APCO Project 25 Two-Way Radio System

Sandy Clark Travis Goodspeed Perry Metzger Zachary Wasserman Kevin Xu
Matt Blaze
*University of Pennsylvania*

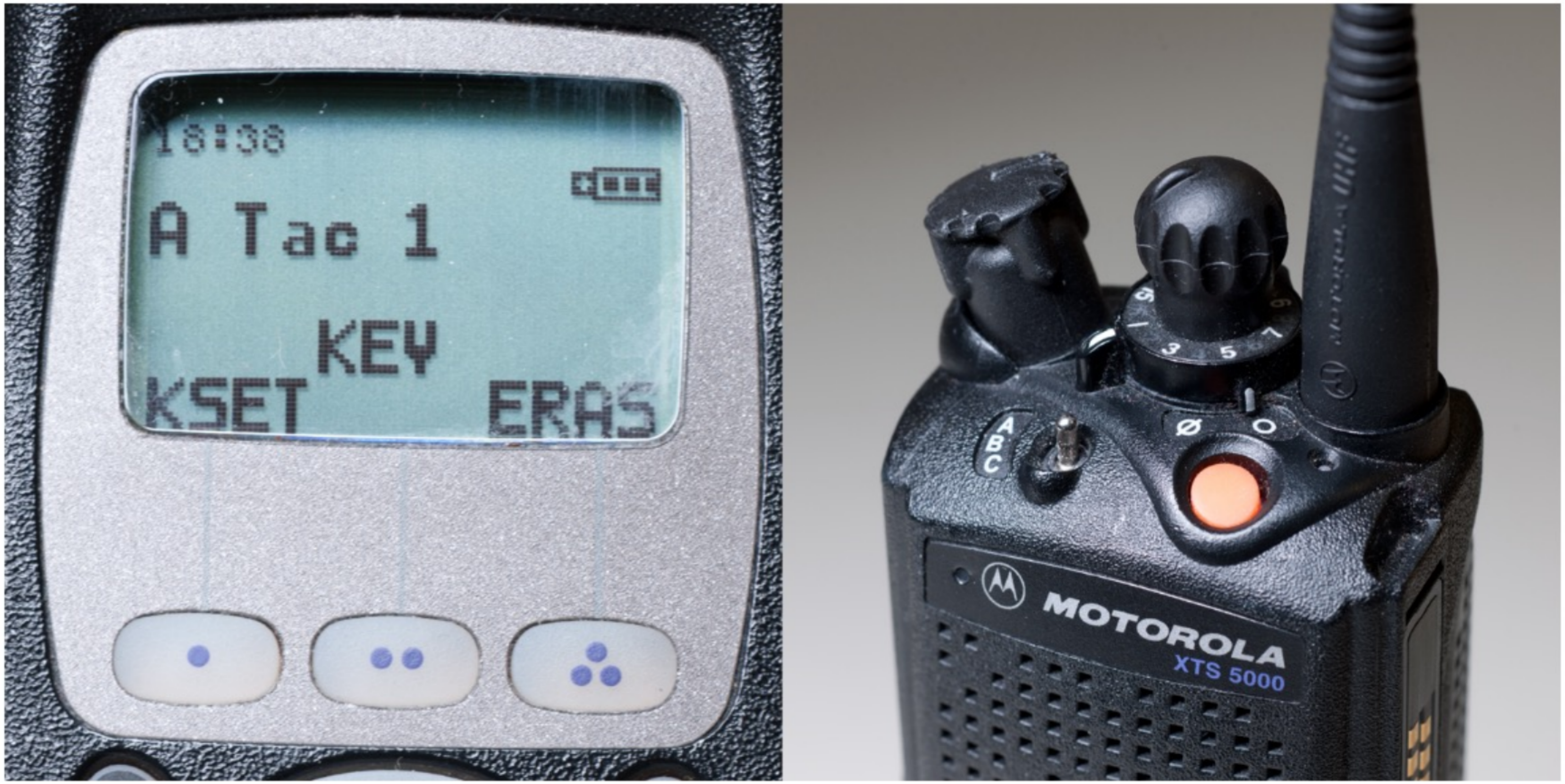
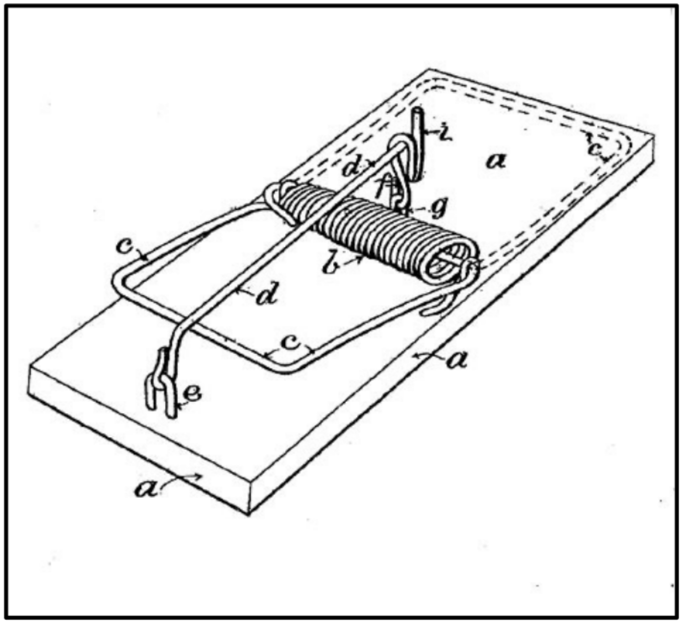


Figure 5: XTS5000 in "Clear" Mode

# Technical Solutions


i
a
c
d
f
g
c
b
d
c
a
e
a