CS 155: Real-World Security

April 14, 2016

Alex Stamos
CSO, Facebook

Why are you here?

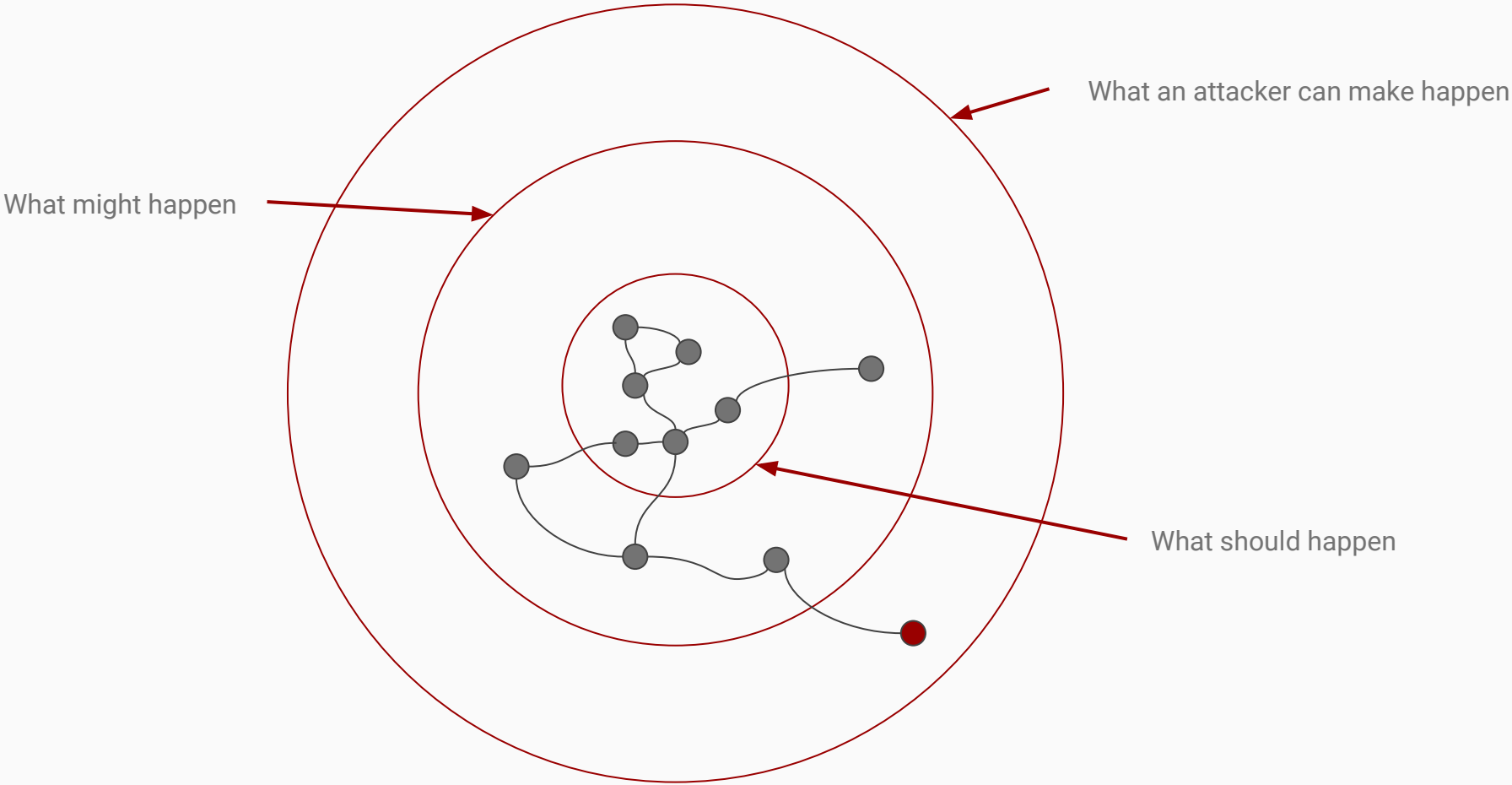
Agenda

- How bugs are found
- How defense works in the real world

- Real bugs
- Real impacts

- Interesting problems for you to solve
- Five basic tips for career success

How are bugs found?

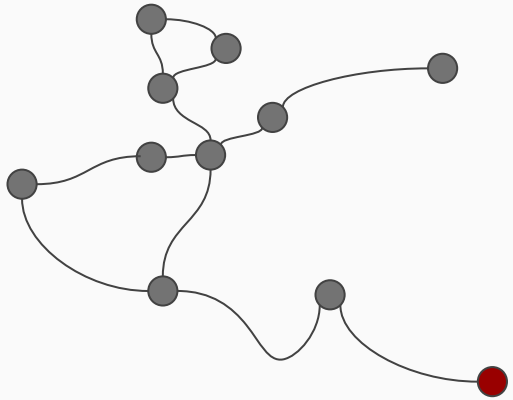

What an attacker can make happen
What might happen
What should happen

Vulnerability Discovery is the art of...

- Pushing software into exploitable states
- Predicting the kinds of mistakes engineers will make and QA/security teams will miss
- Making the impossible possible

Fuzzing

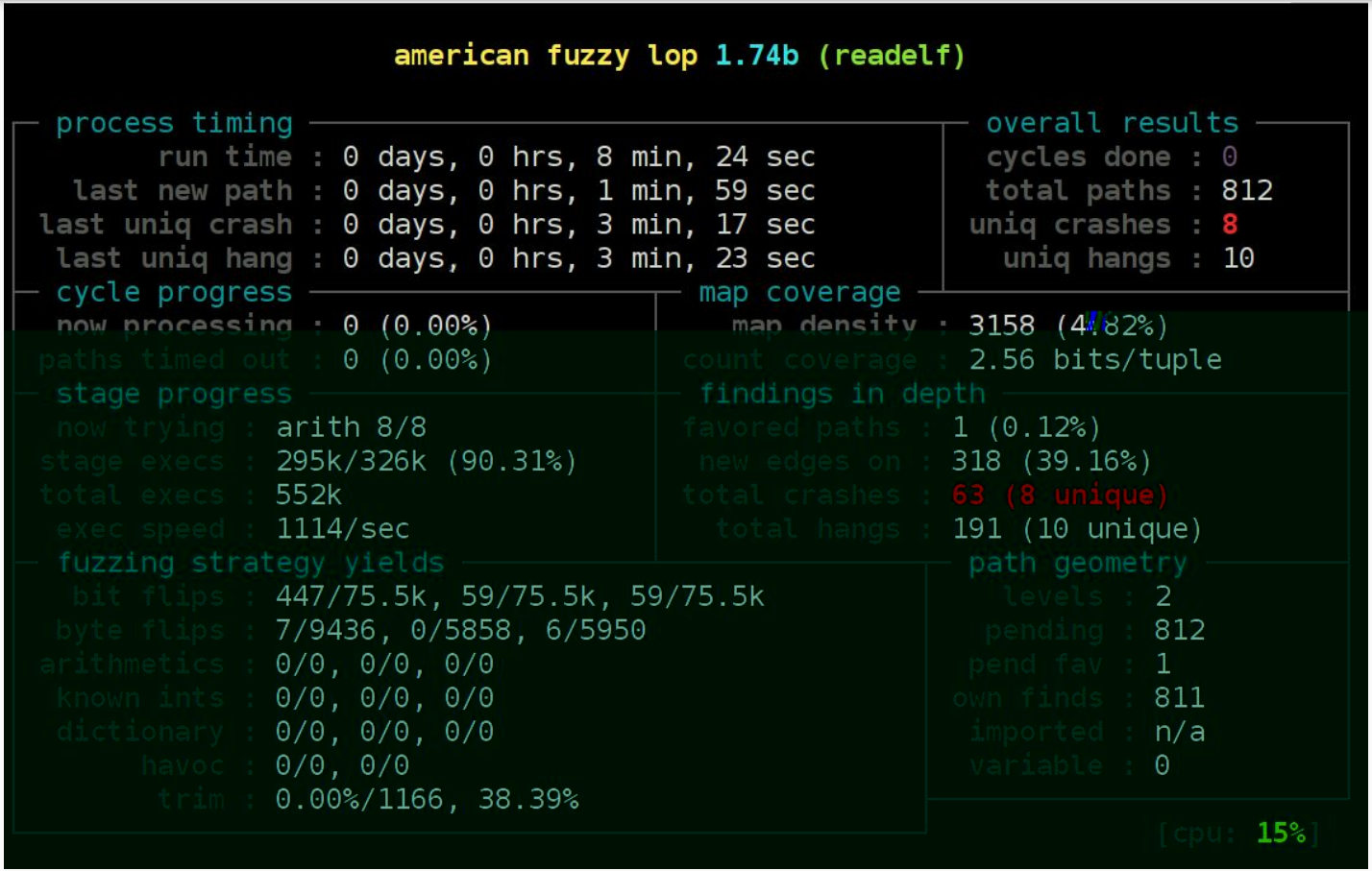
Using automation to mutate input into a system and look for exploitable states



Enhanced by:

- Intelligently unpacking, mutating, and re-packing formats
- Instrumenting the binary to accelerate input and look for caught exceptions
- Studying control-flow and intentionally hitting corner cases

Fuzzing

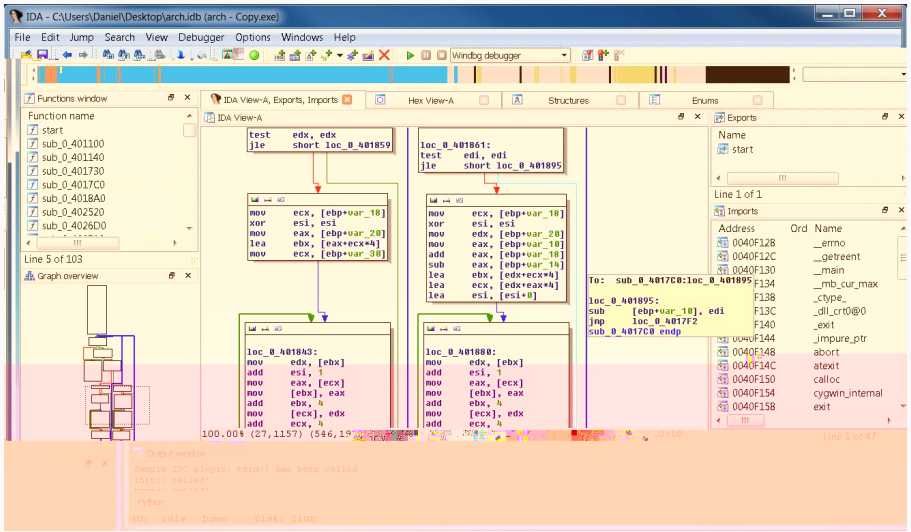


http://lcamtuf.coredump.cx/afl/

Reverse Engineering

Reverse engineering allows the researcher to:

- Find exploitable states and work backward
- Look for common antipatterns
- Understand and bypass sanity checks and protections



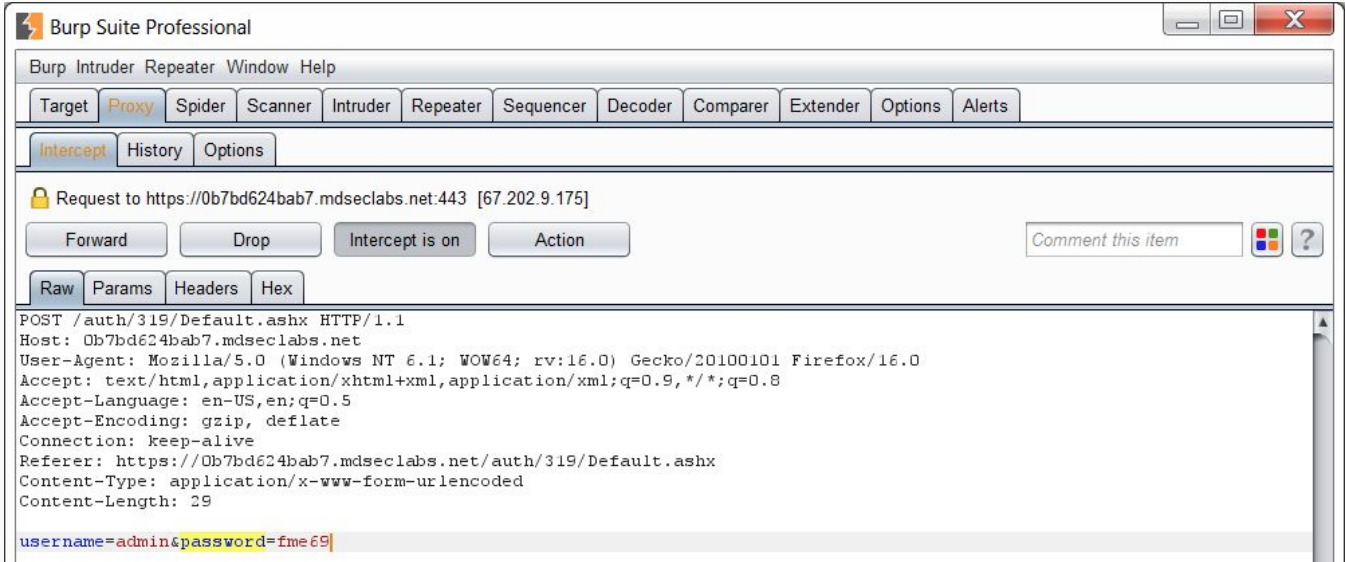
Includes:

- Debugging
- Disassembly
- Binary diffing
- Decompilation

Manual Manipulation

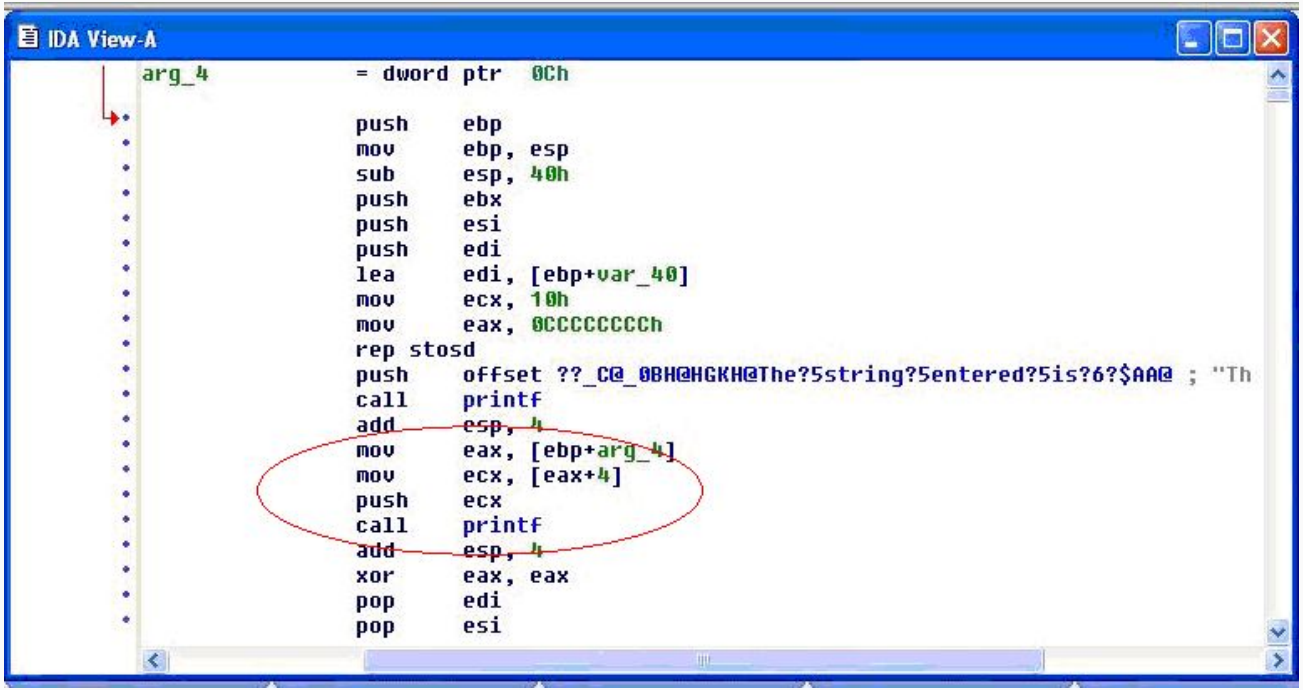
- Many interesting flaws boil down to asking the software to do something
- Due to:
  - Confused deputy problems
  - Missing access control checks
  - Lack of data consistency checks

- Often using tools to intercept and manipulate inputs



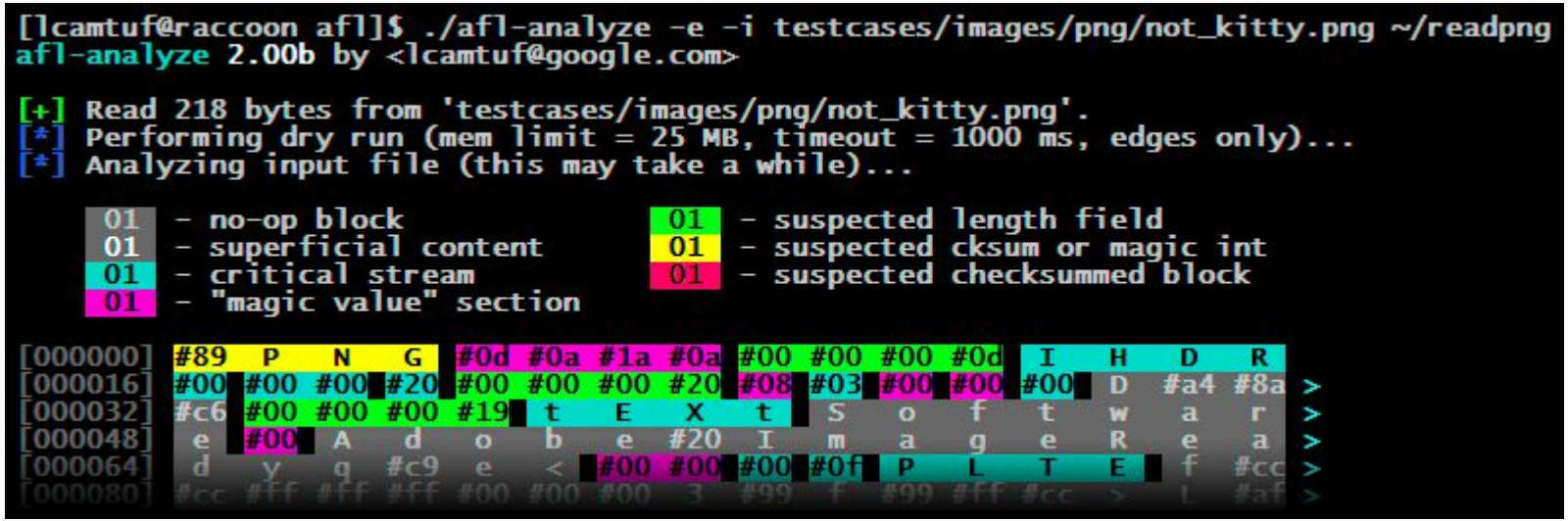
Pulling it Together

1. Disassemble a binary to discover:



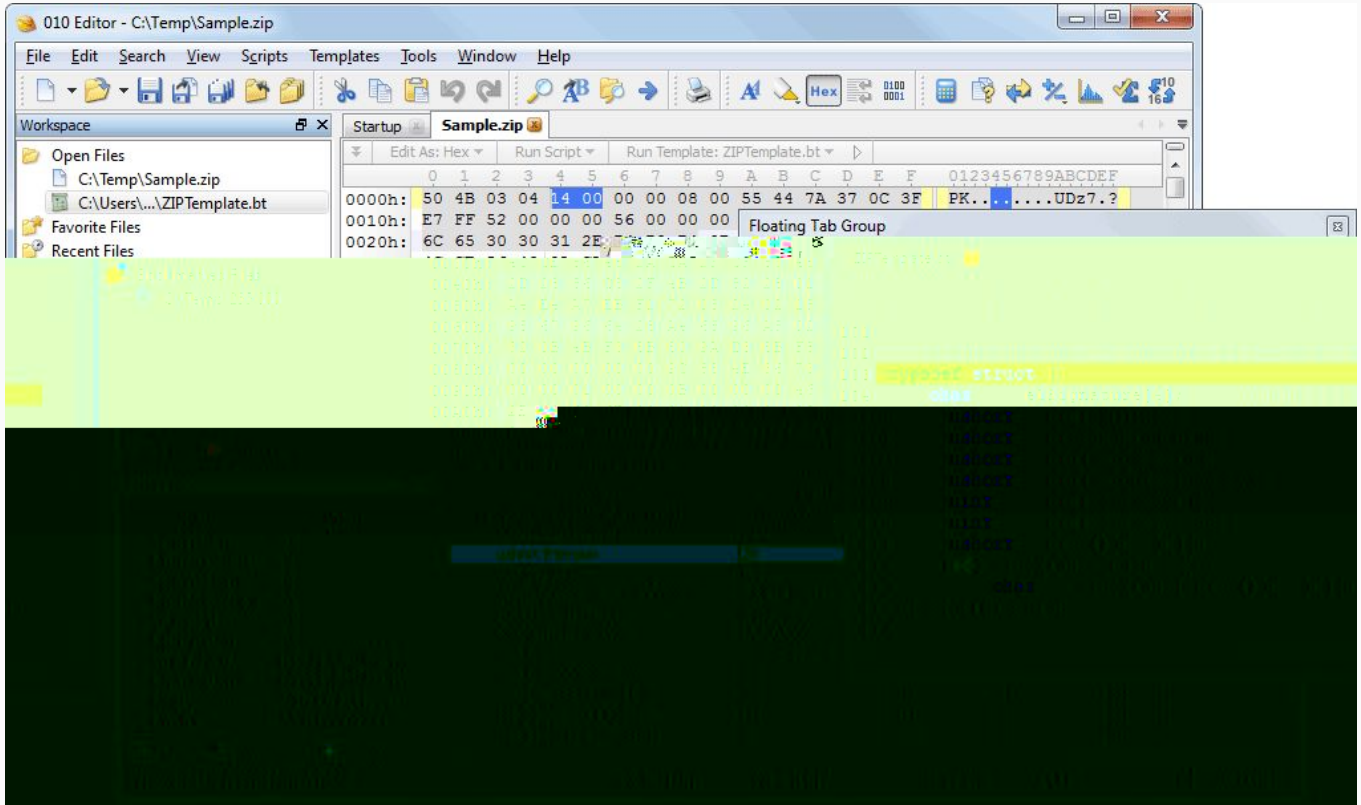
Pulling it Together

2. Use format-aware fuzzing to try to find entry points that lead to format string

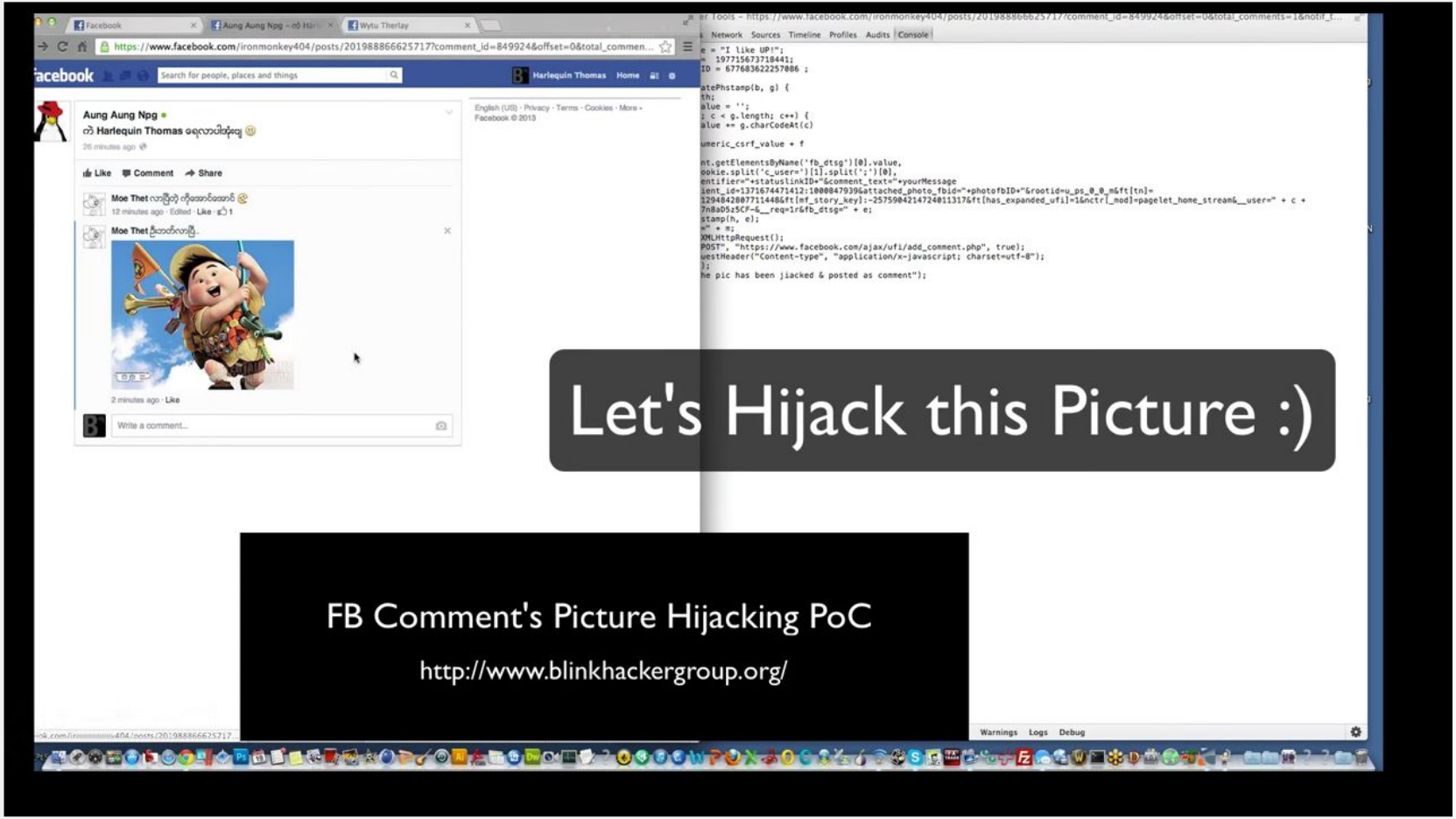


Pulling it Together

3. Researcher carefully modifies crash-creating documents by the fuzzer to obtain execution



Real World Bugs



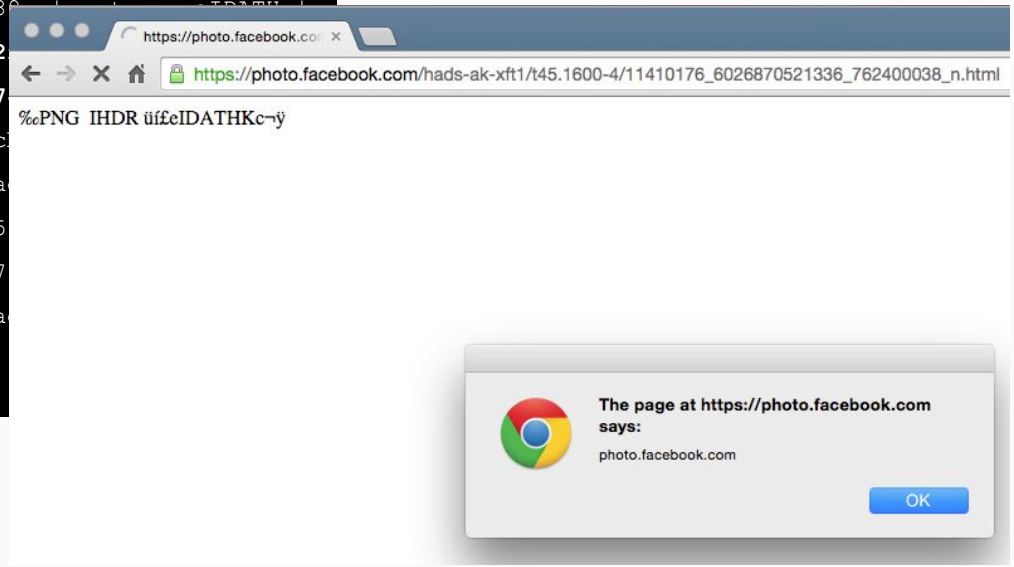
Facebook Picture Sharing on Comment Exploit

Apple's TLS Code

```
hashOut.data = hashes + SSL_MD5_DIGEST_LEN;
hashOut.length = SSL_SHA1_DIGEST_LEN;
if ((err = SSLFreeBuffer(&hashCtx)) != 0)
 goto fail;
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
 goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
 goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
 goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
 goto fail;
 goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
 goto fail;
err = sslRawVerify(...);
```

Embedding Script in Images

```
fin1te@mbp /tmp » hexdump -C xss-fnt-pe-png.png
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG........IHDR|
00000010  00 00 00 20 00 00 00 20  08 02 00 00 00 fc 18 ed  |... ... ........|
00000020  a3 00 00 00 09 70 48 59  73 00 00 0e c4 00 00 0e  |.....pHYs.......|
00000030  c4 01 95 2b 0e 1b 00 00  00 65 49 44 41 54 48 80  |...+.....eIDATH.|
00000040  63 ac ff 3c 53 43 52 49  50 54 20 53 52 43 3d 2  |c..<SCRIPT SRC=|
00000050  2f 46 4e 54 2e 50 45 3e  3c 2f 73 63 72 69 70 7  |/FNT.PE><script|
00000060  3e c3 ea c0 46 8d 17 f3  af de 3d 73 d3 fd 15 c  |>...F.....=s....|
00000070  43 2f 0f b5 ab a7 af ca  7e 7d 2d ea e2 90 22 a  |C/......~}-...".|
00000080  73 85 45 60 7a 90 d1 8c  3f 0c a3 60 14 8c 82 5  |s.E`z...?..`....|
00000090  30 0a 46 c1 28 18 05 a3  60 14 8c 82 61 00 00 7  |0.F.(...`...a..|
000000a0  32 1c 02 78 65 1f 48 00  00 00 00 49 45 4e 44 a  |2..xe.H....IEND.|
000000b0  42 60 82                                        |B`.|
```



https://whitton.io/articles/xss-on-facebook-via-png-content-types/

Bug or feature?

FFmpeg Protocols Documentation

Table of Con

3.4 concat

Physical concatenation protocol.

Read and seek from many resources in sequence as if they were a unique resource.

A URL accepted by this protocol has the syntax:

```
concat:URL1|URL2|...|URLN
```

where *URL1*, *URL2*, ..., *URLN* are the urls of the resource to be concatenated, each one possibly specifying a distinct protocol.

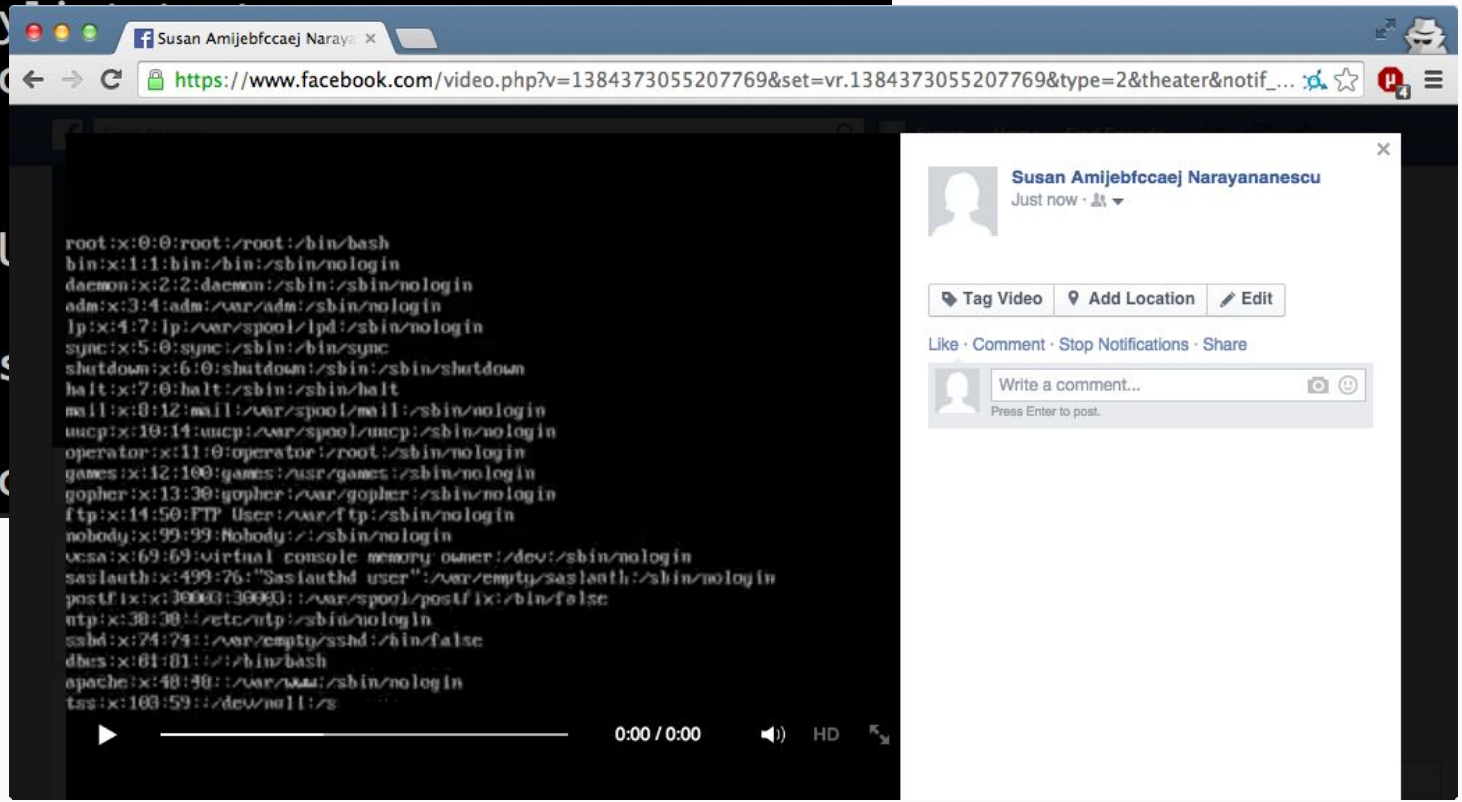
For example to read a sequence of files `split1.mpeg`, `split2.mpeg`, `split3.mpeg` with `ffplay` use the command:

```
ffplay concat:split1.mpeg\|split2.mpeg\|split3.mpeg
```

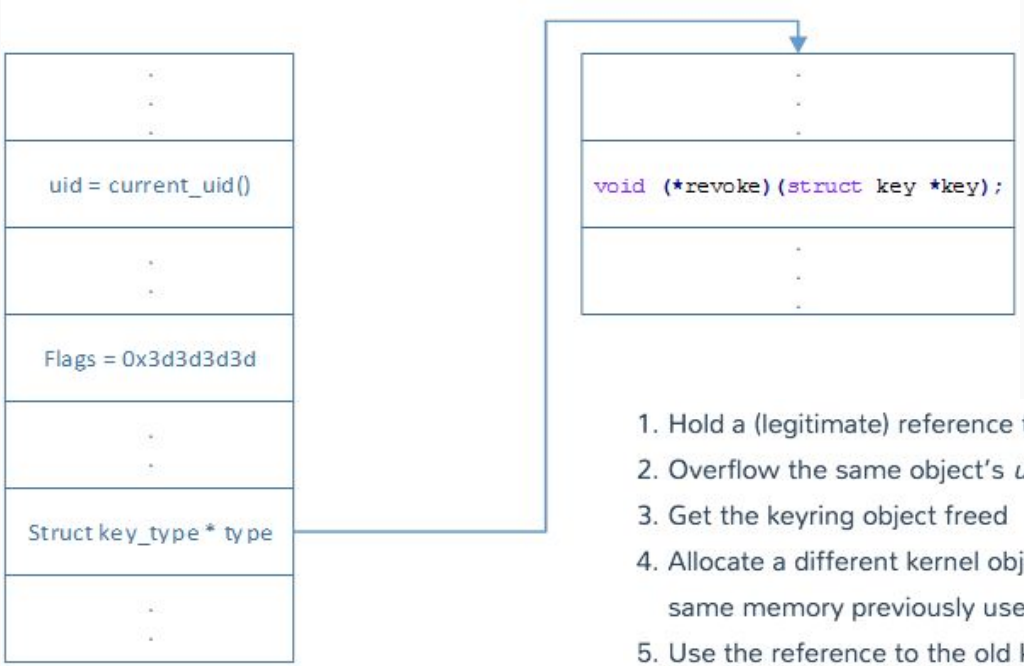
Note that you may need to escape the character "|" which is special for many shells.

Bug or feature?

```
alexstamos-mbp:Downloads alexstamos$ file hax.mp4
hax.mp4: M3U play
alexstamos-mbp:Do
#EXTM3U
#EXT-X-VERSION:4
#EXT-X-MEDIA-SEQU
#EXTINF:10,
concat://etc/pass
#EXT-X-ENDLIST
alexstamos-mbp:Do
```



Memory Management



1. Hold a (legitimate) reference to a key object
2. Overflow the same object's *usage*
3. Get the keyring object freed
4. Allocate a different kernel object from user-space, with a user-controlled content, over the same memory previously used by the freed keyring object
5. Use the reference to the old key object and trigger code execution

http://perception-point.io/2016/01/14/analysis-and-exploitation-of-a-linux-kernel-vulnerability-cve-2016-0728/

Who Finds Bugs?

Who Looks for Bugs?

- Have benefit of source code, access to engineers
- Target 100% coverage, so broad-and-shallow testing is common
- Generally need automation to assist

- Have less information, not a huge problem with shipped code
- Only need a handful of flaws to chain them together
- Need to find and explore issues without alerting defenders

- Various motivations. Money? Fame?
- Lots of ethical reporting options via bug bounties
- Generally want to stay on right side of the law

Real World Defense

Real World Defense Should Focus on...

... (for securing people)

Three biggest problems for most people:

1. Compromised reused passwords
2. Phishing credentials
3. Common, n-day malware

... (for securing enterprises)

Namely, capabilities, tools, techniques and procedures for the intrusion kill chain:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. Actions on Objectives

http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Security research often misses the point

The incentives for private and academic research point the wrong way:

The World's Address: An App That's Worn

Anatomization and Protection of Mobile Apps' Location Privacy Threats .....
Kassem Fawaz, Huan Feng, and Kang G. Shin, *University of Michigan*

LinkDroid: Reducing Unregulated Aggregation of App Usage Behaviors .....
Huan Feng, Kassem Fawaz, and Kang G. Shin, *University of Michigan*

PowerSpy: Location Tracking using Mobile Device Power Analysis .....
Yan Michalevsky, Aaron Schulman, Gunaa Arumugam Veerapandian, and Dan Boneh,
Gabi Nakibly, *National Research and Simulation Center/Rafael Ltd.*

ADDioS!

In the Compression Hornet's Nest: A Security Study of Data Compression in Netwo
Giancarlo Pellegrino, *Saarland University;* Davide Balzarotti, *Eurecom;* Stefan Winter
Technische Universität Darmstadt

Bohatei: Flexible and Elastic DDoS Defense .....
Seyed K. Fayaz, Yoshiaki Tobioka, and Vyas Sekar, *Carnegie Mellon University;* Micha
of Illinois at Urbana-Champaign

Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge....
Bradley Reaves, *University of Florida;* Ethan Shernan, *Georgia Institute of Technology;*
University of Florida; Henry Carter, *Georgia Institute of Technology;* Patrick Traynor,

Attacks: I Won't Let You Down

GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies ..
Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval
University of the Negev

Thermal Covert Channels on Multi-core Platforms .....
Ramya Jayaram Masti, Devendra Rai, Aanjhan Ranganathan, Christian Müller, Lothar
SrdjanČapkun, *ETH Zürich*

Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors.....
Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Ch
and Yongdae Kim, *Korea Advanced Institute of Science and Technology (KAIST)*

How Do You Secure a Cloud and Pin it Down?

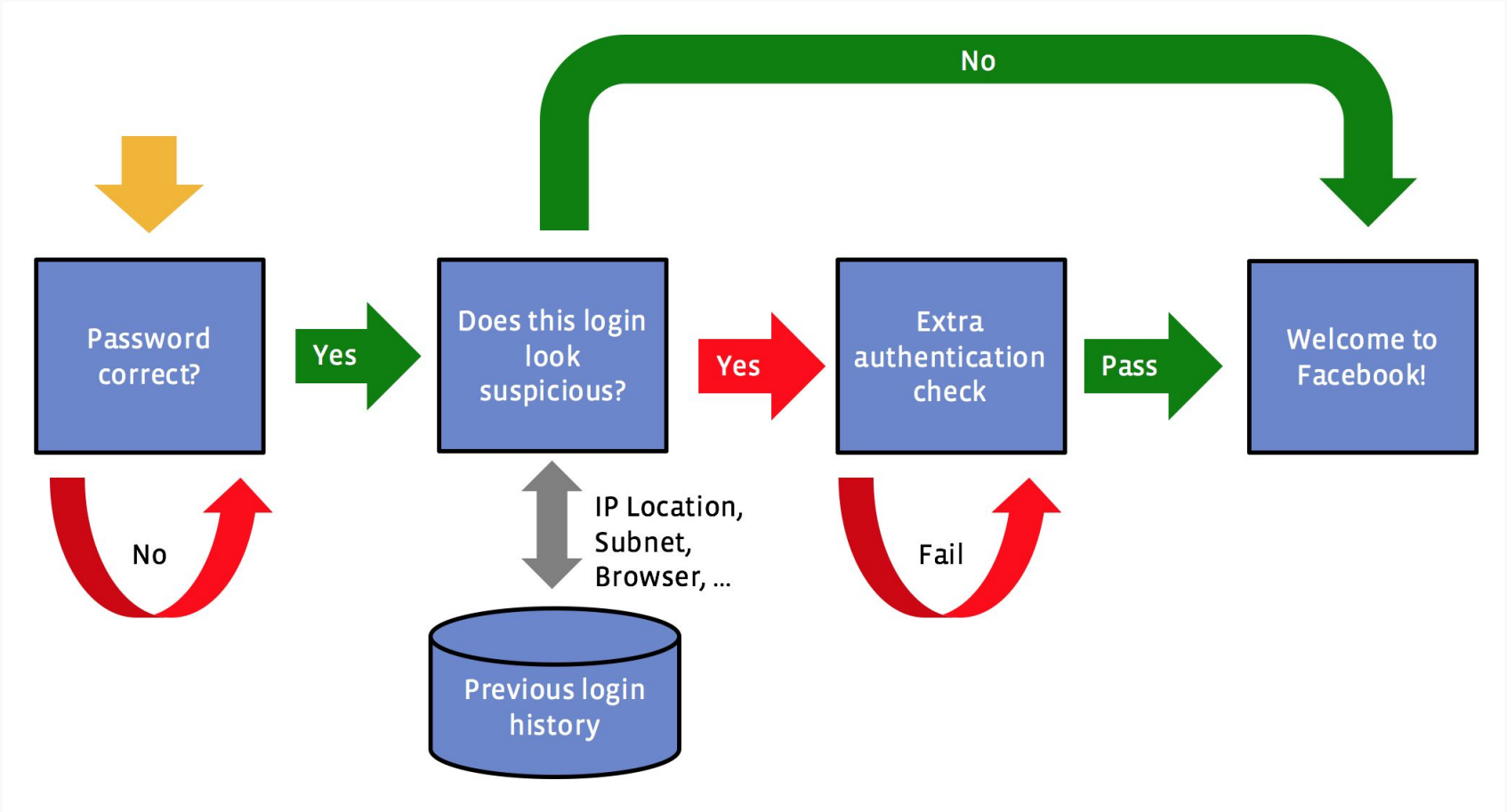
Cache Template Attacks: Automating Attacks on Inclusive Last-Level Caches.....
Daniel Gruss, Raphael Spreitzer, and Stefan Mangard, *Graz University of Technology*

A Placement Vulnerability Study in Multi-Tenant Public Clouds .....
Venkatanathan Varadarajan, *University of Wisconsin—Madison;* Yinqian Zhang, *The O*
Thomas Ristenpart, *Cornell Tech;* Michael Swift, *University of Wisconsin—Madison*

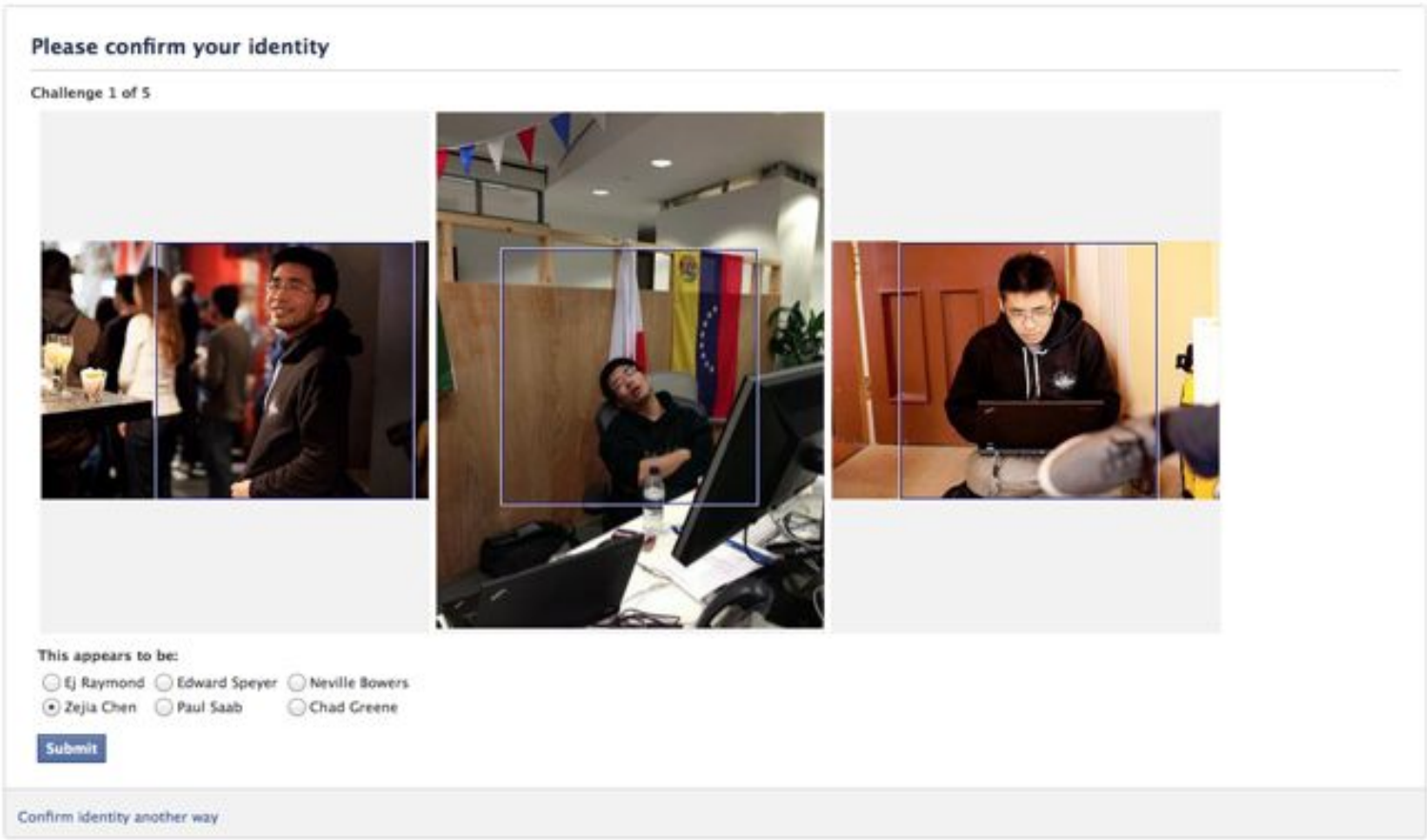
A Measurement Study on Co-residence Threat inside the Cloud.....
Zhang Xu, *College of William and Mary;* Haining Wang, *University of Delaware;* Zhen
NEC Laboratories America

What causes the most problems for normal users?

Real World Defense - Logins

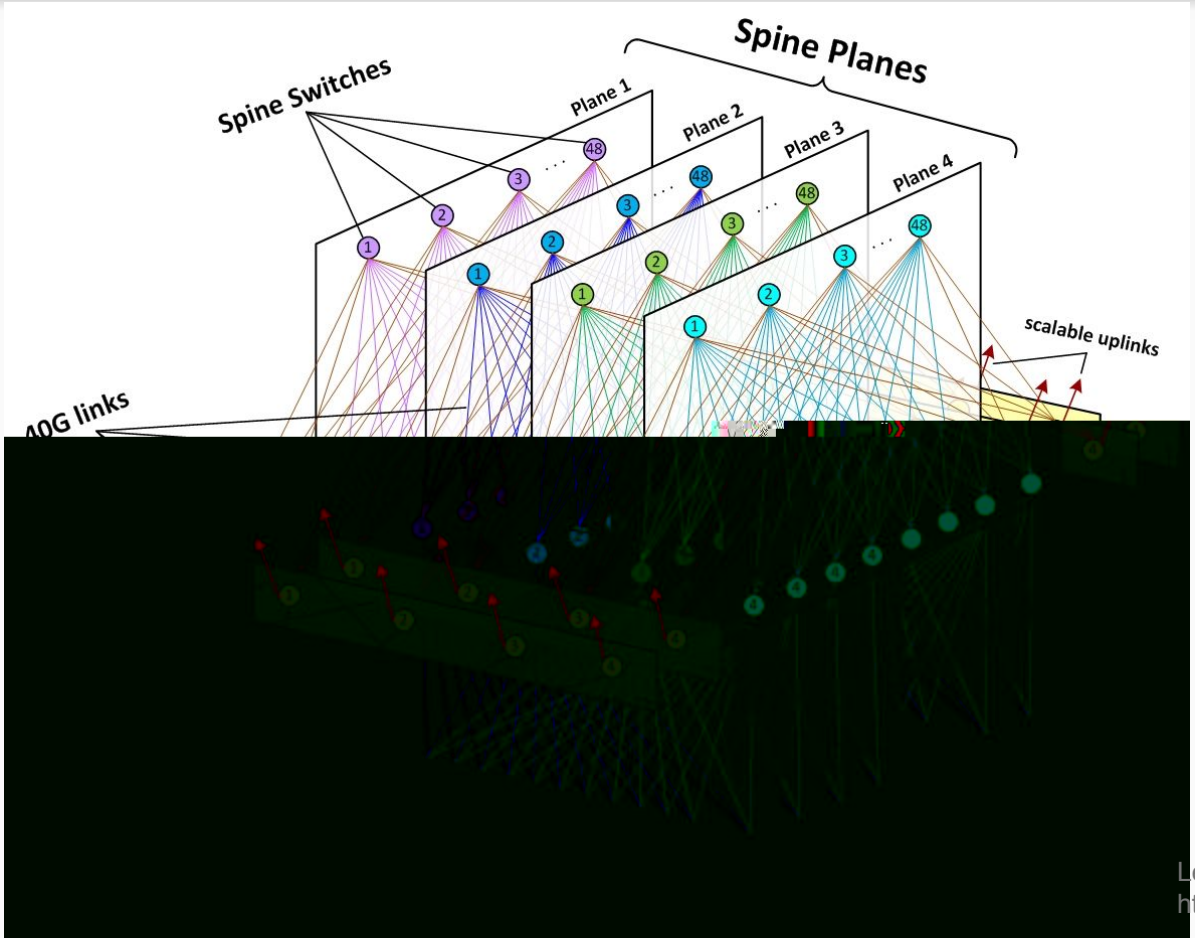


Supplemental Authentication



Open Real World Problems

Network Security at Scale



Learn More:
https://youtu.be/mLEawo6OzFM

Dumb sensors, smart (delayed) decisions

box

Google Apps

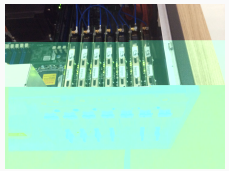
amazon web services

salesforce

Cloud Logs

CHEF

Host Instrumentation



NIDS

Exchange

SharePoint

ORACLE

IT Systems

Spark MLlib

hadoop

ThreatExchange

Microsoft Pinterest NETFLIX

bitly YAHOO! stripe tumblr.

https://threatexchange.fb.com/

Threat Feeds

Careers in Security

What impact do you want to have on the world?

InfoSec might be the most impactful engineering discipline of the 21st century.

You can choose to:

- Protect those who cannot protect themselves
- Bring voice to those who have never had it
- Secure the technologies that billions depend upon
- Stop those who wish to use technology to control and oppress millions

Participating in this industry makes you a moral actor.

Shape your career around your ethical choices, not vice versa.

Six Tips for a Successful Career

1. Always put yourself in a position to learn and grow. Comfort == decay
2. Be part of the product, not the plumbing
3. Your point of maximum leverage comes right after you get a job offer
4. Understand the Cap Table for any private company
5. Always go into a meeting knowing what you want the outcome to be
6. It’s a small industry. Be nice

Thank you and good luck!

alex@stamos.org