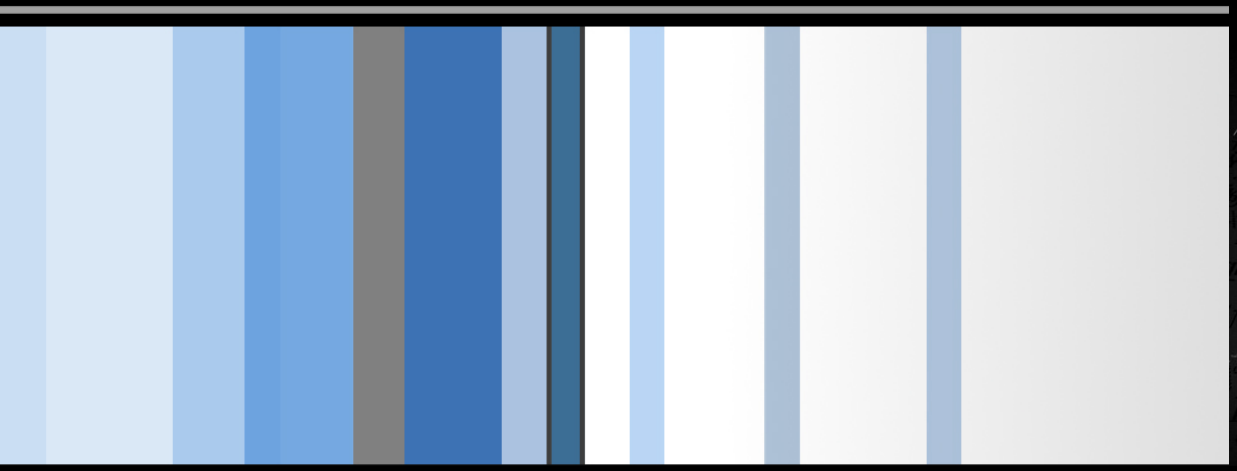
Class 1

CSC 471/583
Malware Analysis

Si Chen (schen@wcupa.edu)



Course Roadmap

- Basic Analysis
  - Debugging
  - Reverse Engineering
  - Malware Behavior
- Modern malware threats
  - APTs (Advanced Persistent threats)
  - Mobile malware
  - Web browser malware
  - IoT malware
  - Blockchain/smart contract malware
  - …

Our approach

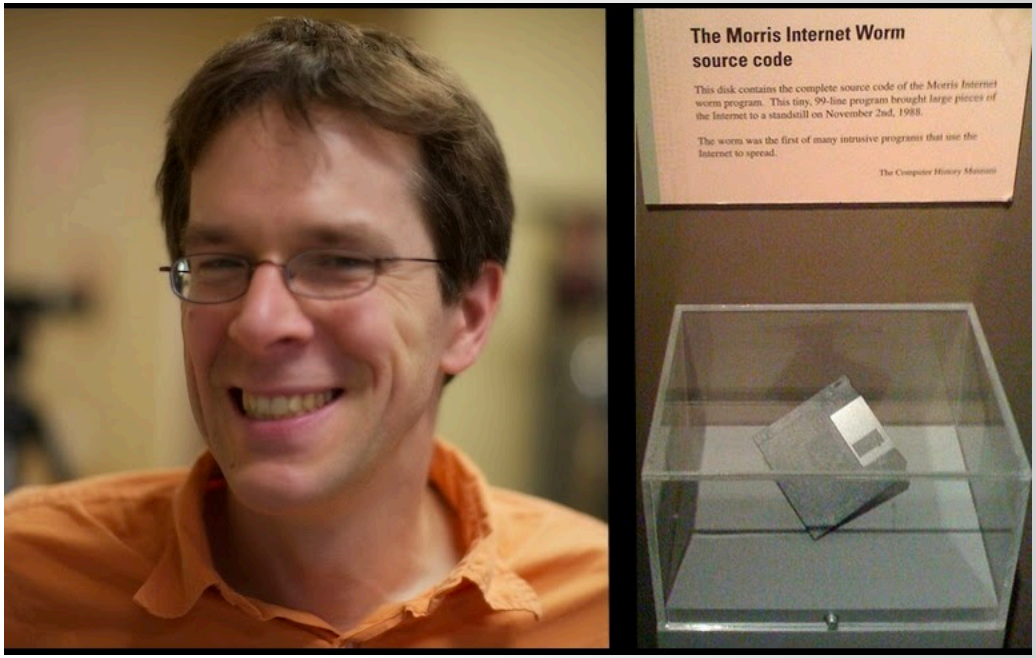
- **Breakdown each topic into two parts:**
  - **Part I: Malware Analysis Foundations**
    - Lecture
    - Lab
  - **Part II: Research Area Case Studies**
    - Reading paper and answer some questions (Reading Homework)
    - Group Project

What is malware?

- Some common names…
  - Trojan, virus, worm, RAT, rootkit
  - A piece of software that is intended to perform unwanted activities on a machine
- Some examples of malicious behavior...
  - Serving ads, stealing data, consuming resources
  - Others?

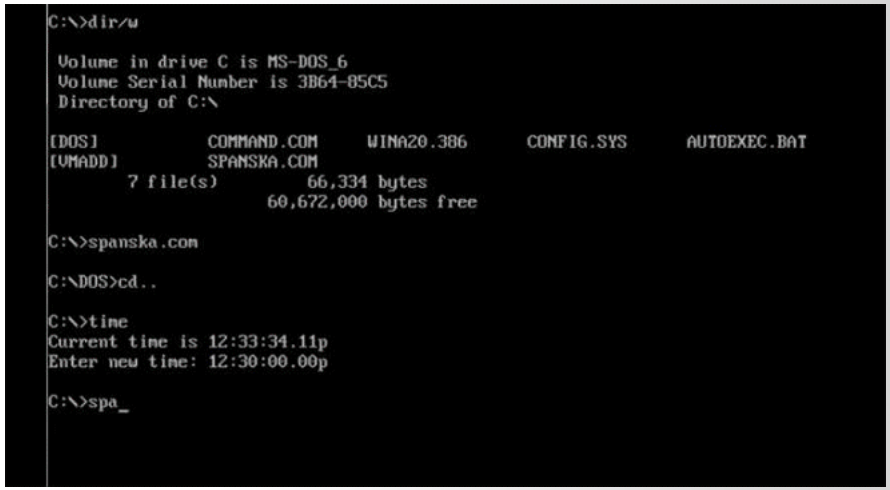
Why do people write malware?

- Morris Worm
  - On accident
  - Purpose: “gauge the size of the internet”
  - What happened: Fork bomb



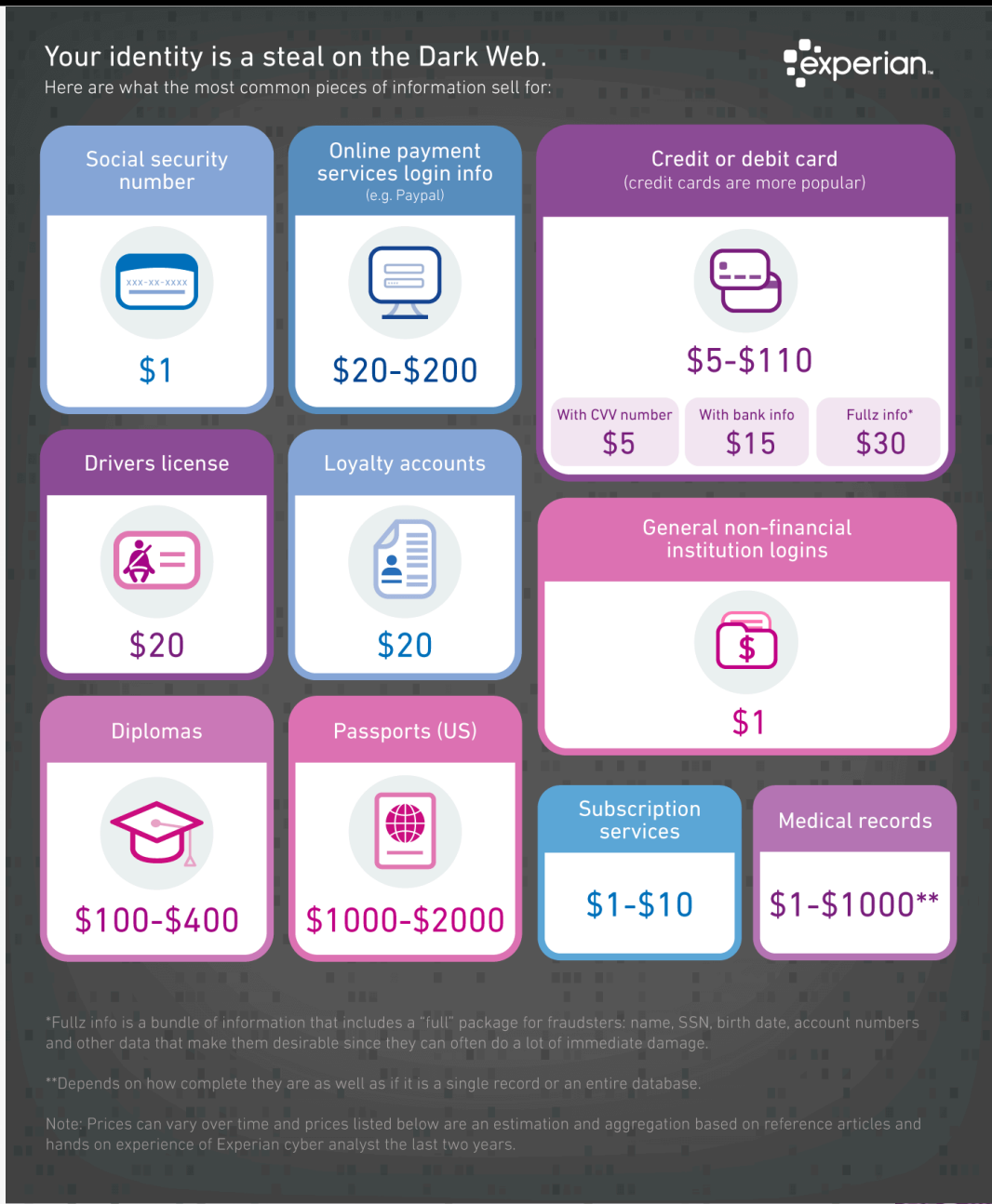
Why do people write malware?

- Once upon a time… (25 Years Ago)
  - Just for fun
  - Spread to other machines & display a message



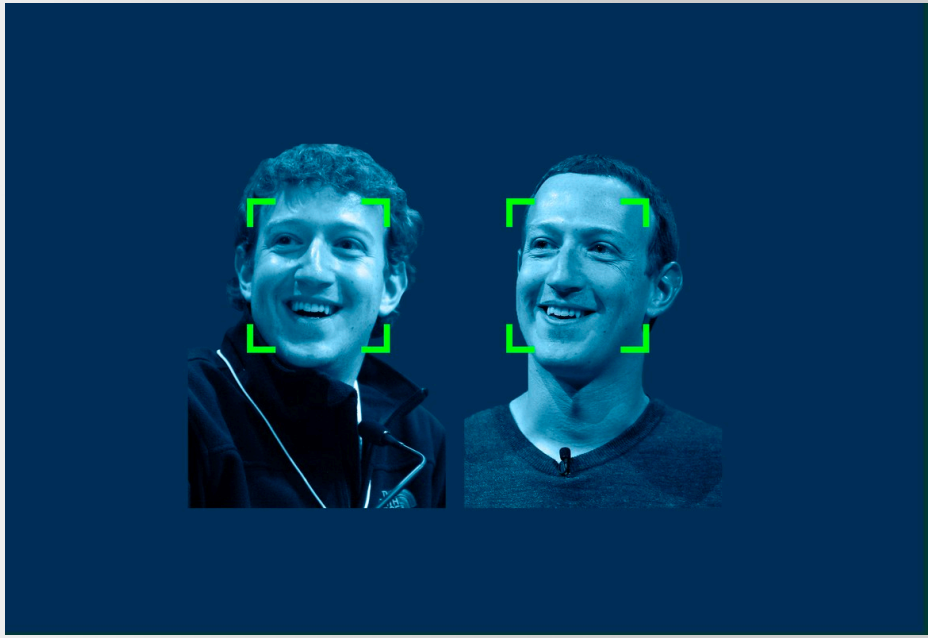
Why do people write malware?

- Today
  - — $$$
- Organizations buy malware
  - Steal passwords, credit cards, bank info, ransoms, intellectual property, trade secrets
  - They can use this info or sell it



Why do people write malware?

- Future…
  - Gathering (more) Information



Why Facebook's '10-Year Challenge' Is A Disaster For Big Data Surveillance

Zak Doffman Contributor ⓘ
Cybersecurity
I write about security and surveillance technologies

Kate O'Neill ✔ 
@kateo

Me 10 years ago: probably would have played along with the profile picture aging meme going around on Facebook and Instagram
Me now: ponders how all this data could be mined to train facial recognition algorithms on age progression and age recognition

♡ 24.8K 4:25 PM - Jan 12, 2019 ⓘ

Why do people write malware?

- Future…
  - Spread False Information

Cougar Football | Cougars | Pac-12 | Sports

WSU coach Mike Leach tweets fake Barack Obama video, stirs up a Twitter storm

Originally published June 18, 2018 at 10:41 am | *Updated June 18, 2018 at 11:08 am*

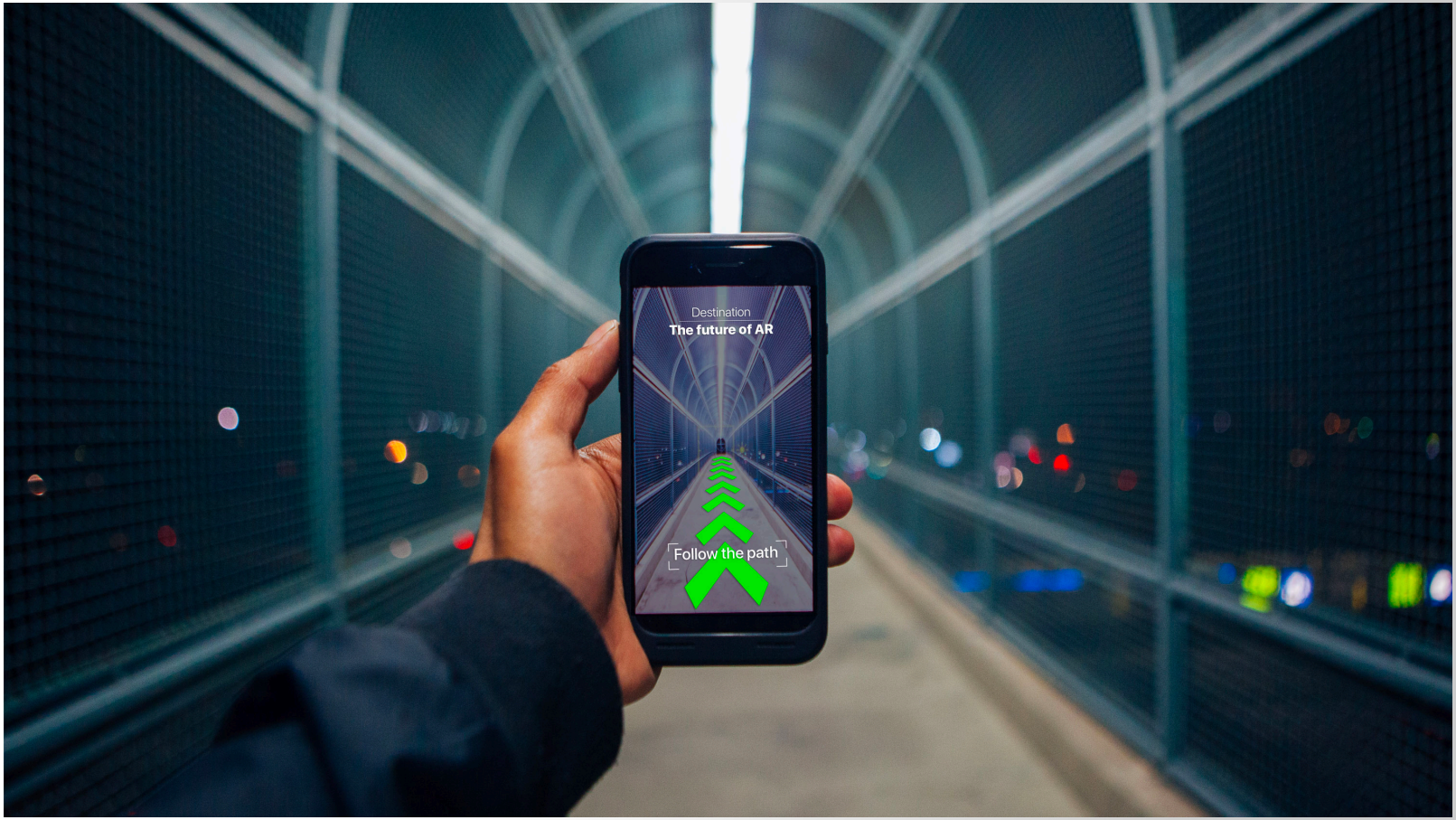
https://www.youtube.com/watch?v=cQ54GDm1eL0

Deepfakes are just the beginning for cybersecurity's Faceswap nightmare

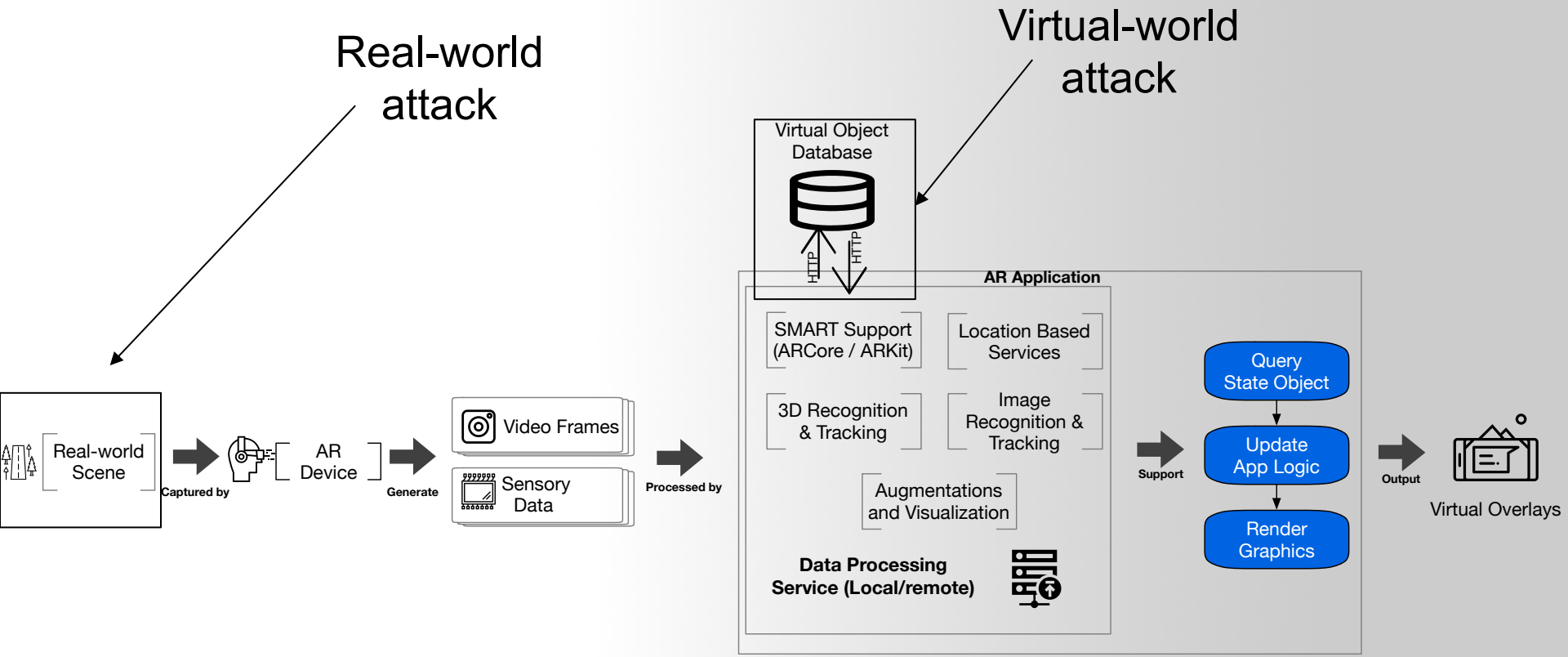
Fergus Halliday (PC World) on 04 April, 2018 14:44

Why do people write malware?

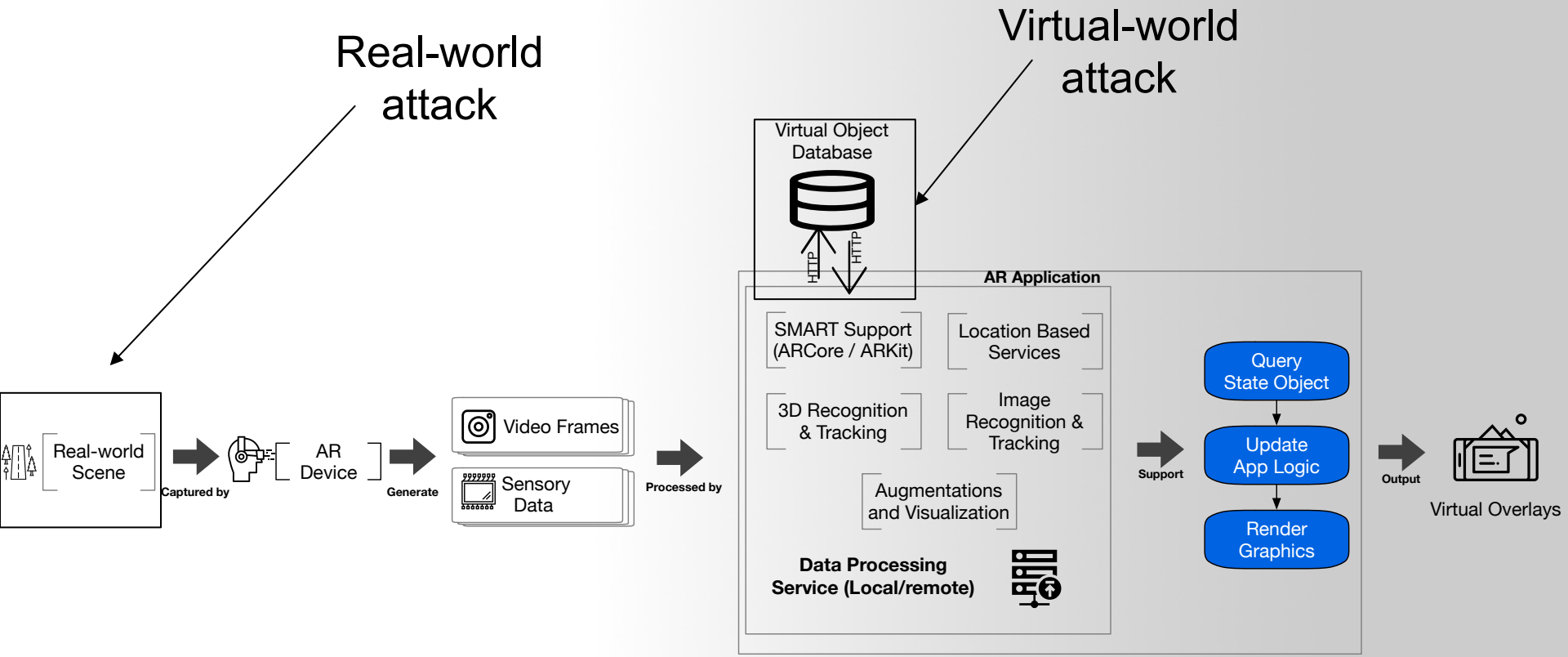
- Future…
  - Control your Life



Our project – Disinformation in AR



Our project – Disinformation in AR



Why analyze malware?

- Detect and respond to intrusions
  - Threat analysis
    - Host & Network signatures
    - What's the damage?
      - Who/What is infected?
  - Threat prevention
  - Threat removal

General perspectives and attack research

Top computer security conference --- The Big 4

Top computer security conference

ACM Conference on Computer and Communications Security (CCS)

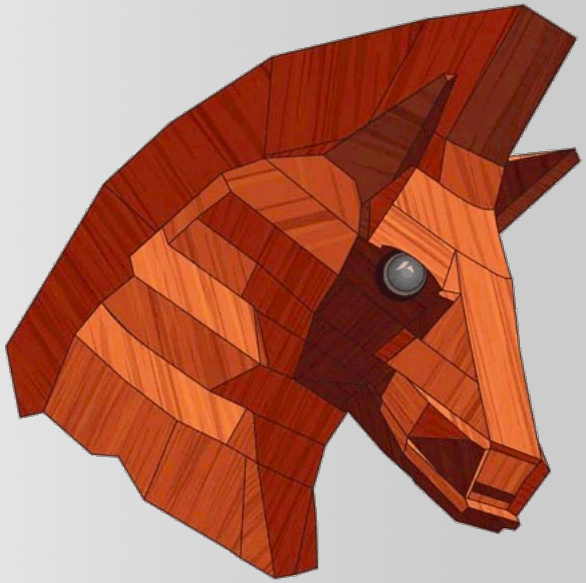
About CCS

The ACM Conference on Computer and Communications Security (CCS) is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM). The conference brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results. It provides an environment to conduct intellectual discussions. From its inception, CCS has established itself as a high-standard research conference in its area.

Top computer security conference

IEEE Symposium on Security and Privacy (S&P)

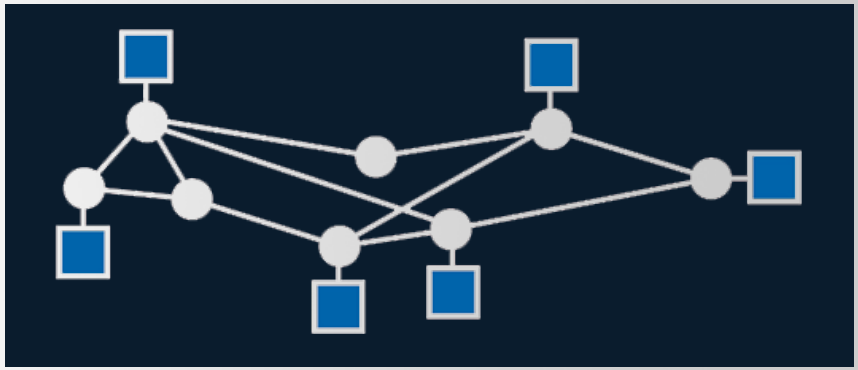
Since 1980, the IEEE Symposium on Security and Privacy (S&P)has been the premier forum for the presentation of developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field.



Top computer security conference

ISOC Network and Distributed System Security Symposium (NDSS)

The Network and Distributed System Security Symposium (NDSS) fosters information exchange among researchers and practitioners of network and distributed system security. The target audience includes those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation. A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of available security technologies.

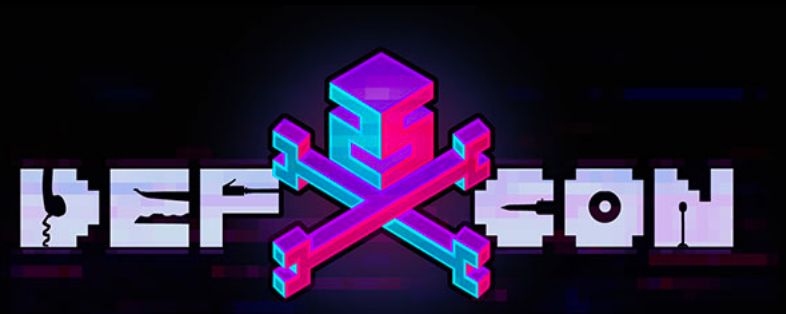


Top computer security conference

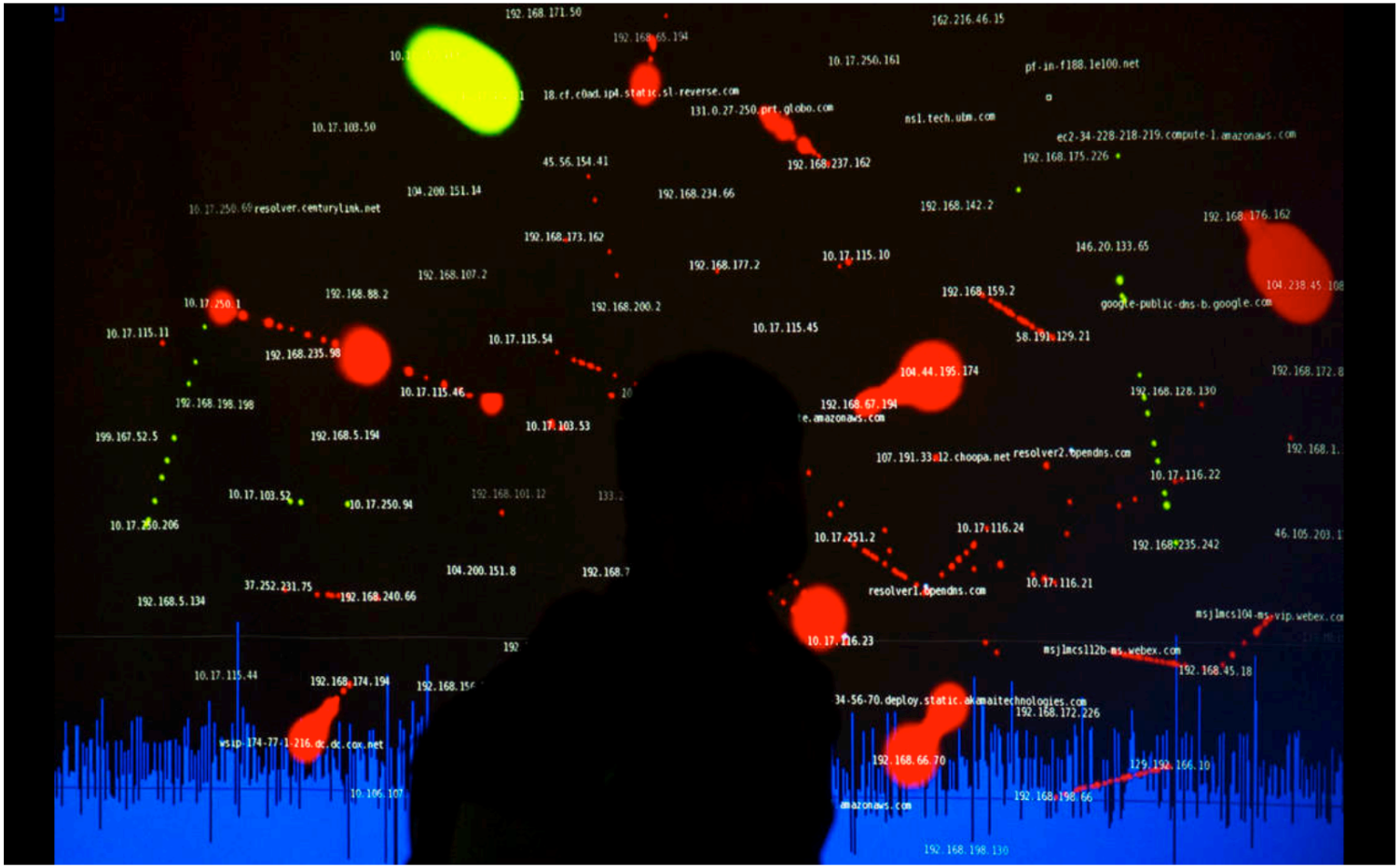
Usenix Security Symposium (USENIX)

The USENIX Security Symposium brings together researchers, practitioners, system administrators, system programmers, and others interested in the latest advances in the security and privacy of computer systems and networks.

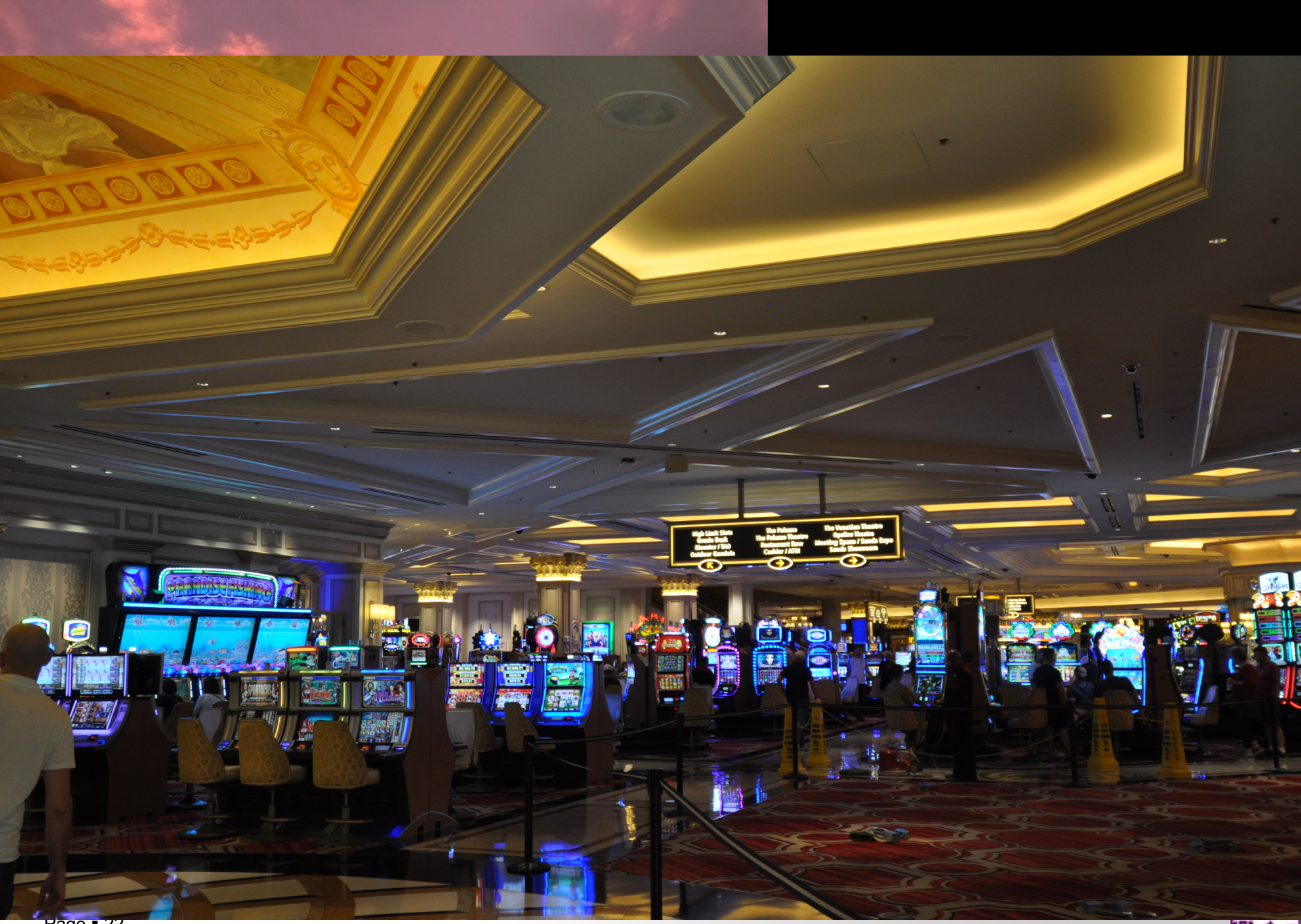
- **Top Security Conference for Hacking**
  - **Black hat USA**
  - **DEFCON**



DefCon, Black Hat bring extra cybersecurity concerns to Las Vegas



A Black Hat tech associate works in the network operating center (NOC) during the Black Hat information security conference at Mandalay Bay, Wednesday, July 26, 2017, In Las Vegas. Richard Brian Las Vegas Review-Journal


PARADISE FISHING

Q & A