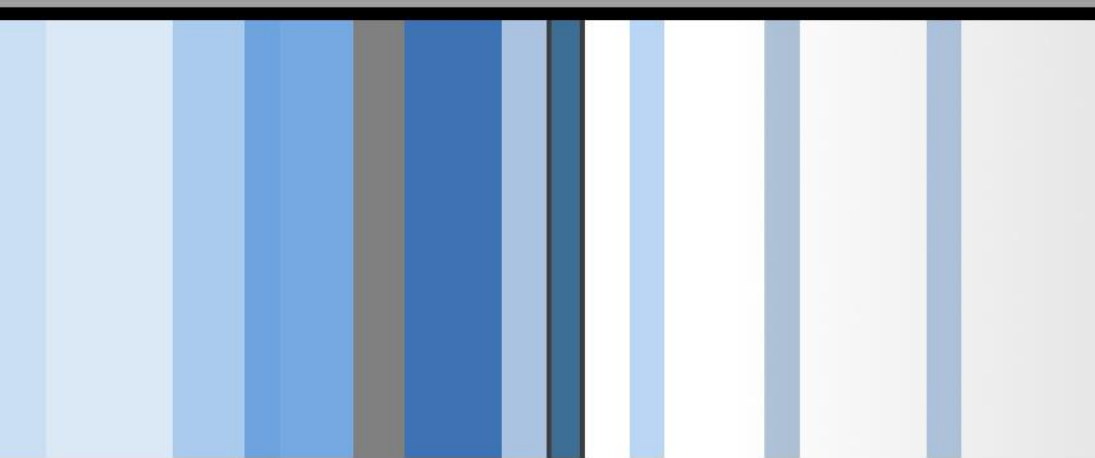


# CSC 600 Advanced Seminar Introduction

Si Chen (schen@wcupa.edu)



# What is computer security?

- Most developers and operators are concerned with **correctness**: achieving desired behavior
  - A working banking web site, word processor, blog, ...
- Security is concerned with **preventing undesired behavior**
  - Considers an enemy/opponent/hacker/adversary who is *actively and maliciously* trying to *circumvent* any protective measures you put in place

# Security Expectations

---

- **Confidentiality**: requires that information be kept private
- **Integrity**: the trustworthiness and correctness of data.
- **Availability**: the capability to use information and resources.

# Kinds of undesired behavior

- Stealing information: ~~confidentiality~~
  - Corporate secrets (product plans, source code, ...)
  - Personal information (credit card numbers, SSNs, ...)
- Modifying information or functionality: ~~integrity~~
  - Installing unwanted software (spyware, botnet client, ...)
  - Destroying records (accounts, logs, plans, ...)
- Denying access: ~~availability~~
  - Unable to purchase products
  - Unable to access banking information

# General perspectives and attack research

```
File View Debug Trace Plugins Options Windows Help
[Icons] [L] [E] [M] [W] [T] [C] [R] [K] [B] [M] [H] [Icons]
00401000 EB 10 JMP SHORT 00401012
00401002 66 DB 66
00401003 62 DB 62
00401004 3A DB 3A
00401005 43 DB 43
00401006 2B DB 2B
00401007 2B DB 2B
00401008 48 DB 48
00401009 4F DB 4F
0040100A 4F DB 4F
0040100B 4B DB 4B
0040100C 90 NOP
0040100D E9 DB E9
0040100E CC 614100 DD OFFSET CPPdebugHook
00401012 A1 BF614100 MOV EAX,DWORD PTR DS:[4161BF]
00401017 C1E0 02 SHL EAX,2
0040101A A3 C3614100 MOV DWORD PTR DS:[4161C3],EAX
0040101F 52 PUSH EDX
00401020 6A 00 PUSH 0
00401022 E8 65410100 CALL <JMP.&KERNEL32.GetModuleHandleA>
00401027 8BD0 MOV EDX,EAX
00401029 E8 BA980000 CALL 0040A8E8
0040102E 5A POP EDX
0040102F E8 18980000 CALL 0040A84C
00401034 E8 EF980000 CALL 0040A928
00401039 6A 00 PUSH 0
0040103B E8 3CAB0000 CALL 0040BB7C
00401040 59 POP ECX
00401041 68 68614100 PUSH OFFSET 00416168
00401046 6A 00 PUSH 0
00401048 E8 3F410100 CALL <JMP.&KERNEL32.GetModuleHandleA>
0040104D A3 C7614100 MOV DWORD PTR DS:[4161C7],EAX
00401052 6A 00 PUSH 0
00401054 E9 5FFB0000 JMP 00410BB8
00401059 E9 6AAB0000 JMP 0040BBC8
0040105E 33C0 XOR EAX,EAX
00401060 A0 B1614100 MOV AL,BYTE PTR DS:[4161B1]
00401065 C3 RETN
00401066 A1 C7614100 MOV EAX,DWORD PTR DS:[4161C7]
0040106B C3 RETN
0040106C 60 PUSHAD
0040106D BB 0050B0BC MOV EBX,BCB05000
00401072 53 PUSH EBX
00401073 68 AD0B0000 PUSH 0BAD
00401078 C3 RETN
00401079 B9 AC000000 MOV ECX,0AC
0040107E 0BC9 OR ECX,ECX
00401080 74 4D JZ SHORT 004010CF
00401082 833D BF614100 CMP DWORD PTR DS:[4161BF],0
00401089 73 0A JAE SHORT 00401095
0040108B B8 FE000000 MOV EAX,0FE
00401090 E8 D7FFFFF CALL 0040106C
00401095 B9 AC000000 MOV ECX,0AC
0040109A 51 PUSH ECX
0040109B 6A 08 PUSH 8
0040109D E8 FC400100 CALL <JMP.&KERNEL32.GetProcessHeap>
004010A2 50 PUSH EAX
004010A3 E8 2C410100 CALL <JMP.&KERNEL32.HeapAlloc>
Dest:=Test.00401012
```



**DIRTY COW**

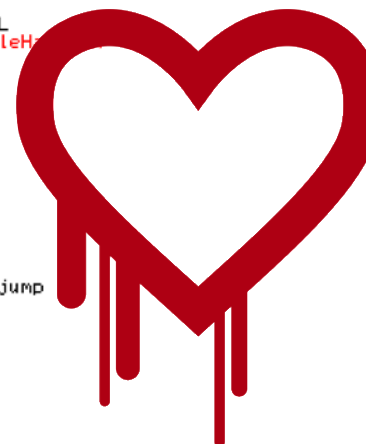
```
[Module Name = NULL
KERNEL32.GetModuleHandleA
```

```
[Test.0040A928
Arg1 = 0
Test.0040BB7C
```

```
[Module Name = NULL
KERNEL32.GetModuleH
```

RET is used as a jump

```
[Size => 172.
Flags = HEAP_ZERO_MEMORY
cKERNEL32.GetProcessHeap
Heap
NTDLL.BrIAI LocateHeap
```



**MELTDOWN**

# General perspectives and attack research

## Were you affected by the Xfinity data breach? Here's what you should do

Data breach underscores the importance of password protection, cybersecurity experts say

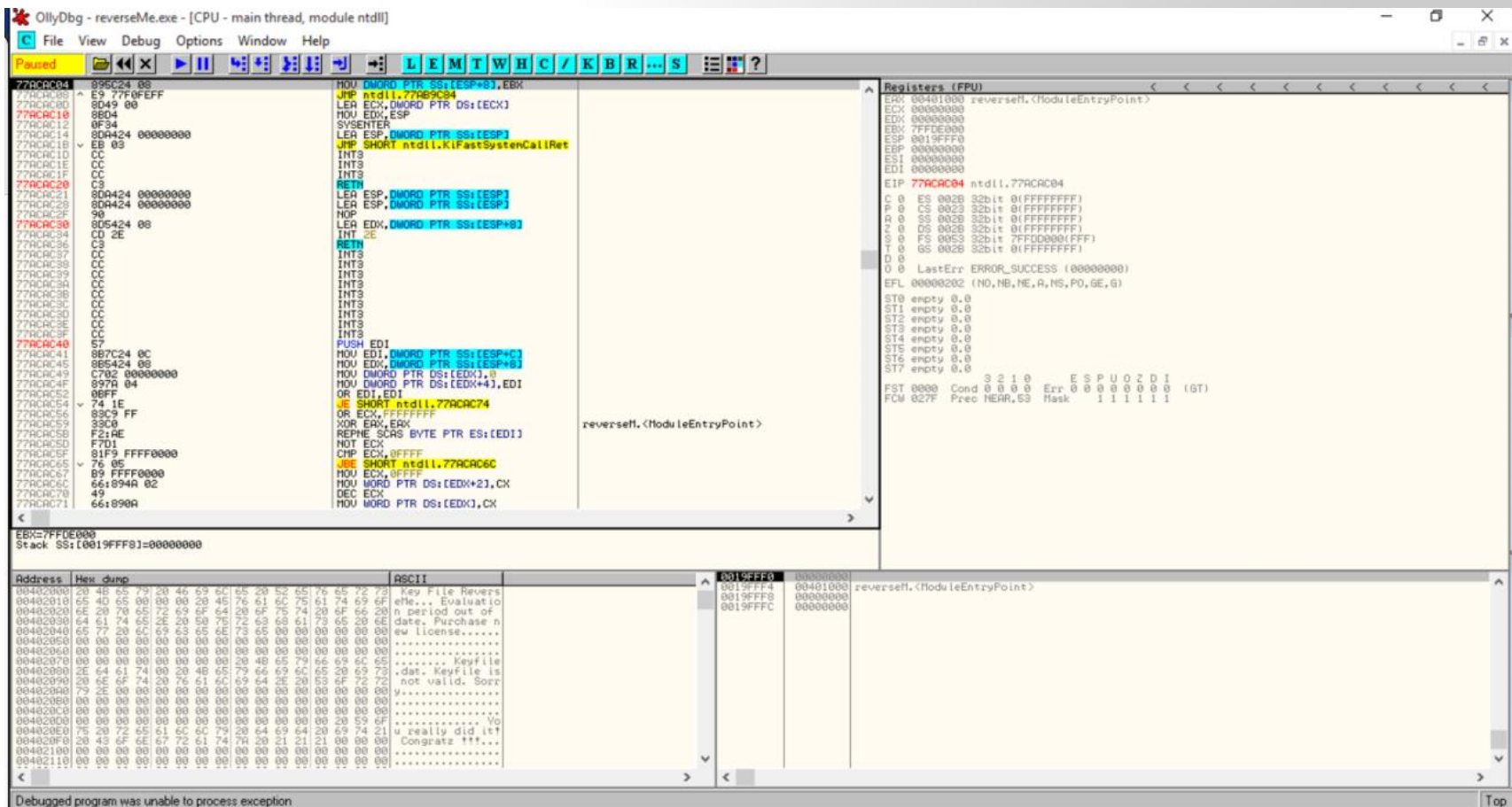


**CVE-2023-4966 “Citrix Bleed”**

Dr. Si Chen, associate computer science professor at West Chester University, thinks Comcast should be more transparent with customers and publish exactly what happened.

“They don’t have to be a technical guru to understand the details, but as a company, you need to publish that information so the people will have a clear message of what’s actually going on,” he said.

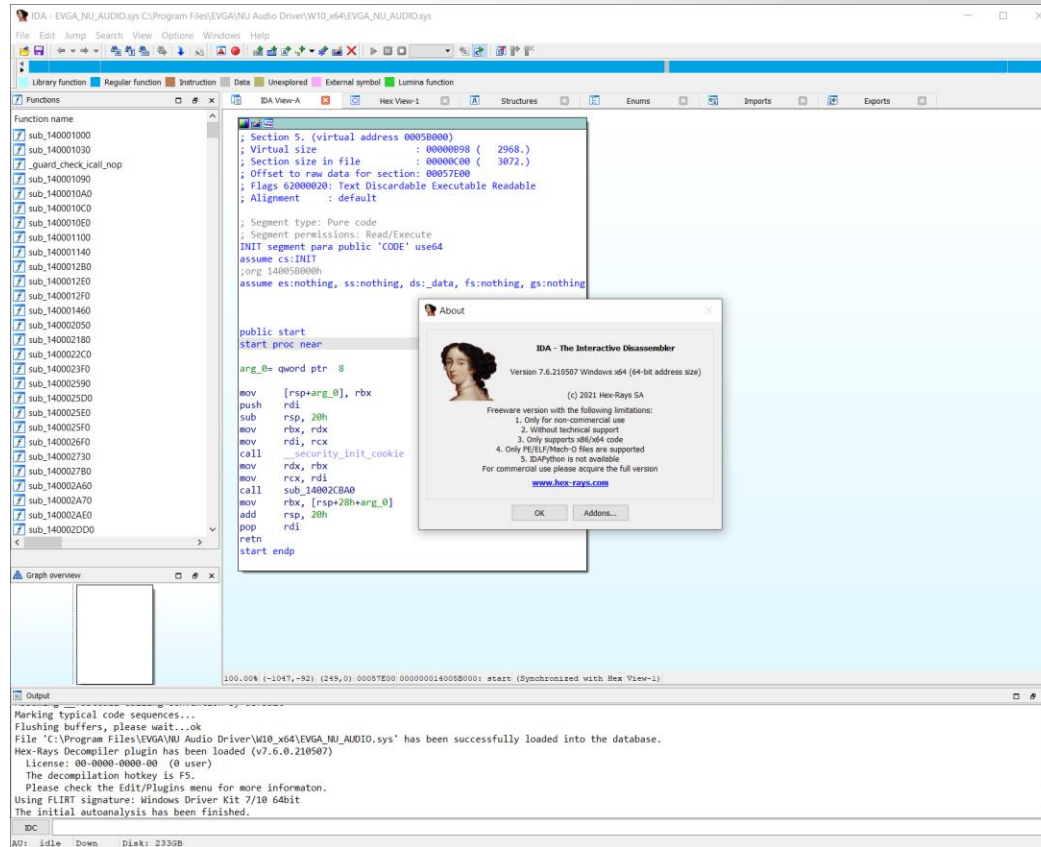
# Debugging Software



**Ollydbg:** OllyDbg was an x86 debugger that emphasizes binary code analysis, which is useful when source code is not available. It traces registers, recognizes procedures, API calls, switches, tables, constants and strings, as well as locates routines from object files and libraries. Wikipedia



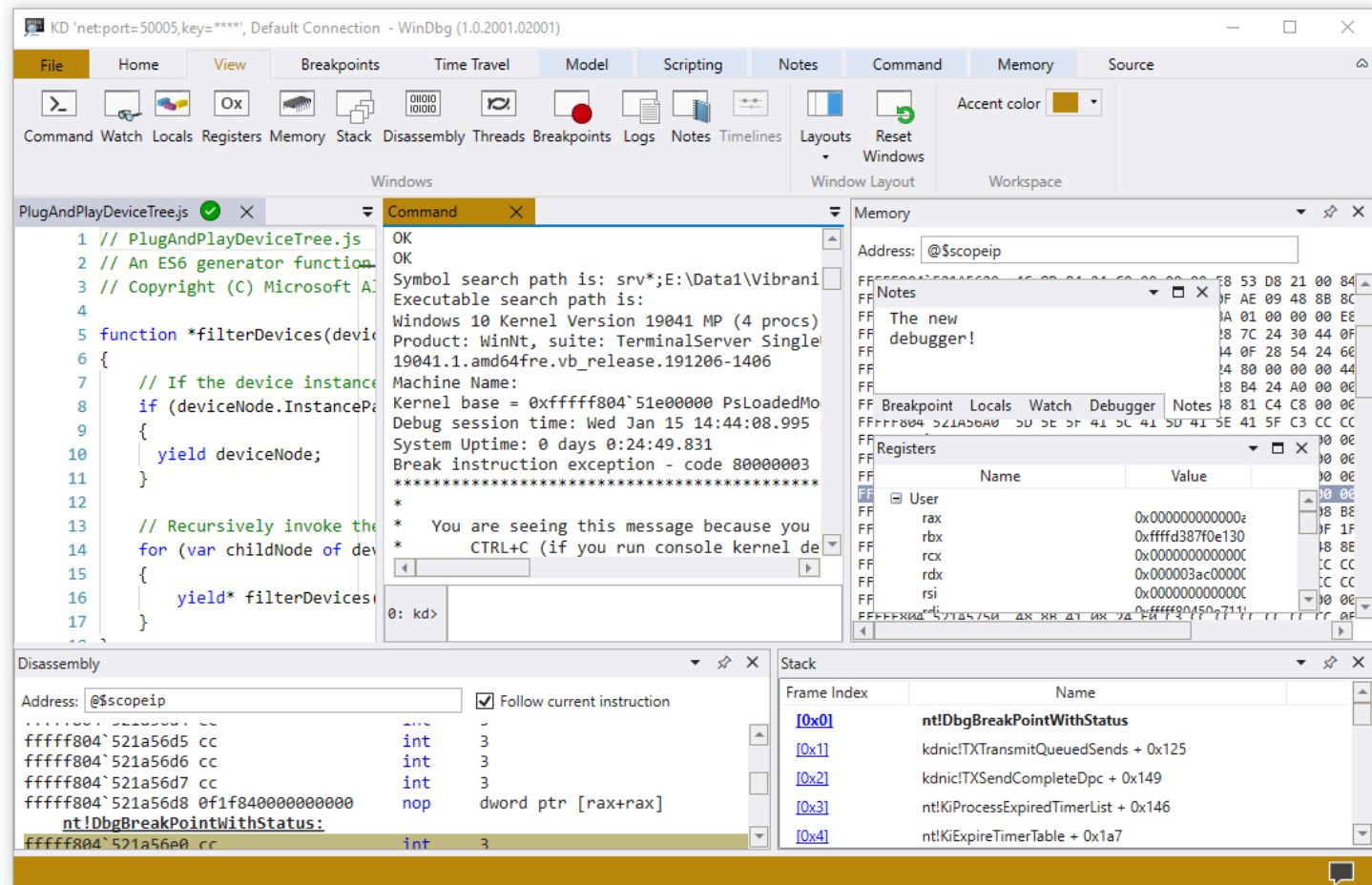
# Debugging Software



**IDA free:** This free version of IDA offers a privilege opportunity to see IDA in action. This light but powerful tool can quickly analyze the binary code samples and users can save and look closer at the analysis results.



# Debugging Software



**WinDbg:** WinDbg is a multipurpose debugger for the Microsoft Windows computer operating system, distributed by Microsoft. Debugging is the process of finding and resolving errors in a system; in computing it also includes exploring the internal operation of software as a help to development. [Wikipedia](#)

# Volatility

```
CSI Linux (clean Install of CSI Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
csi@csi-analyst:~/Desktop/memdumps$ volatility -f cridex.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address      Remote Address      Pid
-----
0x02087620 172.16.112.128:1038    41.168.5.140:8080    1484
0x023a8008 172.16.112.128:1037    125.19.103.198:8080  1484
csi@csi-analyst:~/Desktop/memdumps$ volatility -f cridex.vmem --profile=WinXPSP2x86 sockets
Volatility Foundation Volatility Framework 2.6
Offset(V)  PID  Port  Proto Protocol  Address      Create Time
-----
0x81ddb780 664  500   17 UDP        0.0.0.0      2012-07-22 02:42:53 UTC+0000
0x82240d08 1484 1038  6 TCP        0.0.0.0      2012-07-22 02:44:45 UTC+0000
0x81dd7618 1220 1900  17 UDP       172.16.112.128 2012-07-22 02:43:01 UTC+0000
0x82125610 788  1028  6 TCP        127.0.0.1     2012-07-22 02:43:01 UTC+0000
0x8219cc08 4  445   6 TCP        0.0.0.0      2012-07-22 02:42:31 UTC+0000
0x81ec23b0 908  135   6 TCP        0.0.0.0      2012-07-22 02:42:33 UTC+0000
0x82276878 4  139   6 TCP       172.16.112.128 2012-07-22 02:42:38 UTC+0000
0x82277460 4  137   17 UDP       172.16.112.128 2012-07-22 02:42:38 UTC+0000
0x81e76620 1004 123  17 UDP       127.0.0.1     2012-07-22 02:43:01 UTC+0000
0x82172808 664  0     255 Reserved 0.0.0.0      2012-07-22 02:42:53 UTC+0000
0x81e3f460 4  138   17 UDP       172.16.112.128 2012-07-22 02:42:38 UTC+0000
0x821f0630 1004 123  17 UDP       172.16.112.128 2012-07-22 02:43:01 UTC+0000
0x822cd2b0 1220 1900  17 UDP       127.0.0.1     2012-07-22 02:43:01 UTC+0000
0x82172c50 664  4500  17 UDP       0.0.0.0      2012-07-22 02:42:53 UTC+0000
0x821f0d00 4  445   17 UDP       0.0.0.0      2012-07-22 02:42:31 UTC+0000
```

**Volatility:** Volatility is an open-source memory forensics framework for incident response and malware analysis. It is written in Python and supports Microsoft Windows, Mac OS X, and Linux. Volatility was created by Aaron Walters, drawing on academic research he did in memory forensics. [Wikipedia](#)

# First-gen Hacker

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



# First-gen Hacker

- Once upon a time... (30 Years Ago)
  - Just for fun
  - Spread to other machines & display a message

```
C:\>dir/w

Volume in drive C is MS-DOS_6
Volume Serial Number is 3B64-85C5
Directory of C:\

[DOS]          COMMAND.COM      WINA20.386      CONFIG.SYS      AUTOEXEC.BAT
[UMADD]        SPANSKA.COM
               7 file(s)         66,334 bytes
                               60,672,000 bytes free

C:\>spanska.com

C:\DOS>cd..

C:\>time
Current time is 12:33:34.11p
Enter new time: 12:30:00.00p

C:\>spa_
```

- Today

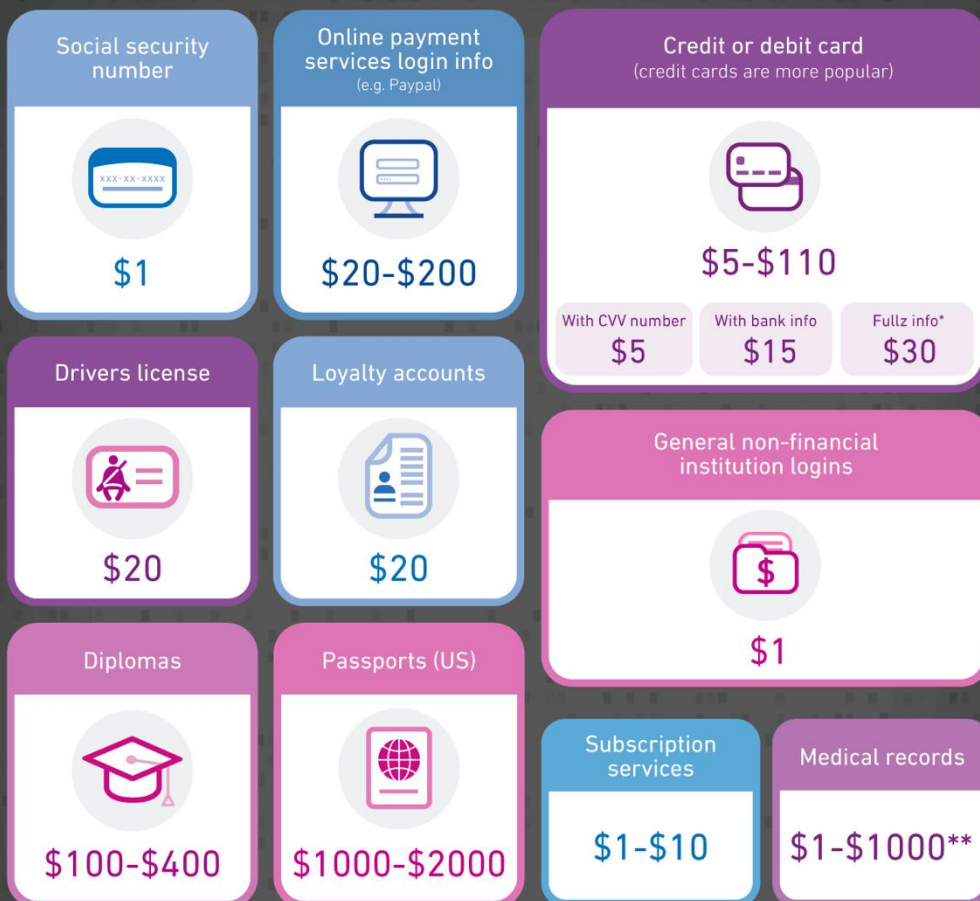
- \$\$\$

- Organizations buy malware

- Steal passwords, credit cards, bank info, ransoms, intellectual property, trade secrets
  - They can use this info or sell it

## Your identity is a steal on the Dark Web.

Here are what the most common pieces of information sell for:



\*Fullz info is a bundle of information that includes a "full" package for fraudsters: name, SSN, birth date, account numbers and other data that make them desirable since they can often do a lot of immediate damage.

\*\*Depends on how complete they are as well as if it is a single record or an entire database.

Note: Prices can vary over time and prices listed below are an estimation and aggregation based on reference articles and hands on experience of Experian cyber analyst the last two years.

# Why do people write malware?

- ~~Future...~~ Today
  - Gathering more information about a person.





# Why do people write malware?

- ~~Future...~~ Today
  - 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



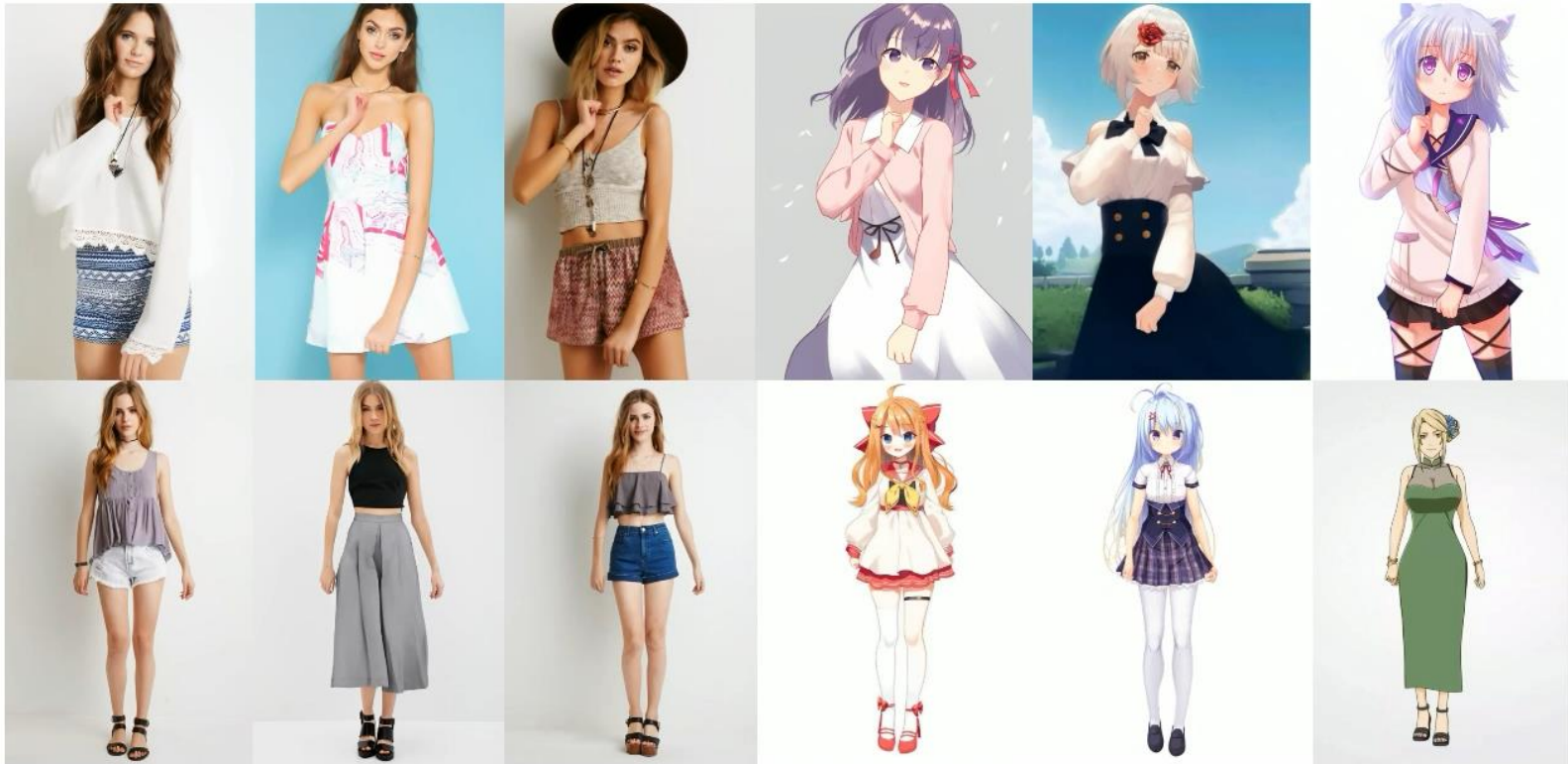
# Why do people write malware?

## VividTalk: One-Shot Audio-Driven Talking Head Generation Based on 3D Hybrid Prior



# Why do people write malware?

## Animate Anyone: Consistent and Controllable Image-to-Video Synthesis for Character Animation



- 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>

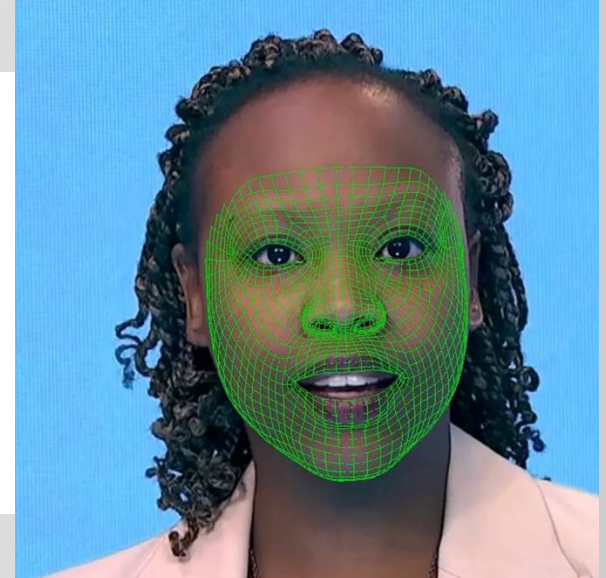
## Deepfakes are just the beginning for cybersecurity's Faceswap nightmare

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

# Why do people write malware?

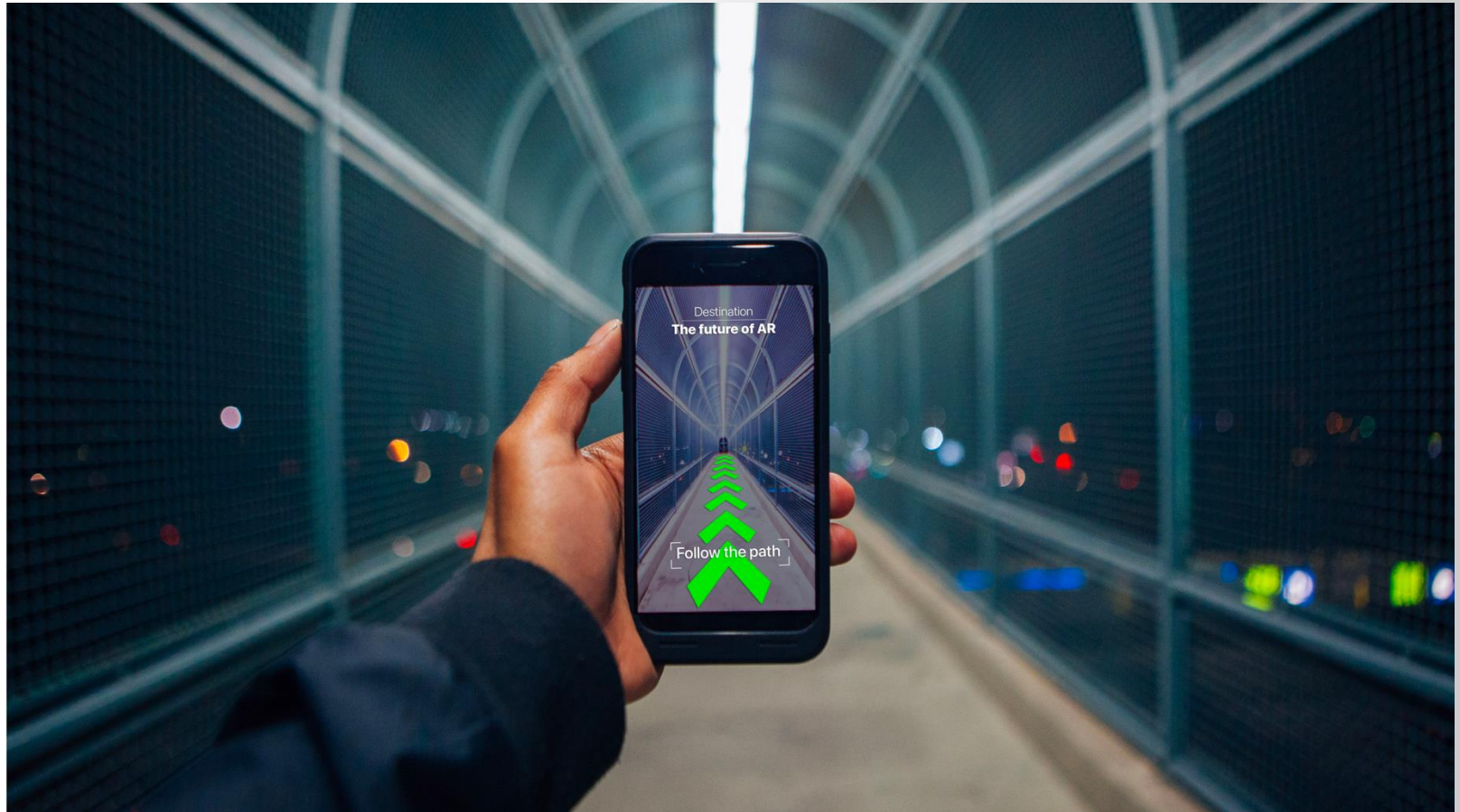
## *As Deepfakes Flourish, Countries Struggle With Response*

Few governments have approved regulations, often because of free-speech concerns. New mandates from China could change the tone of the debate on digital forgeries.



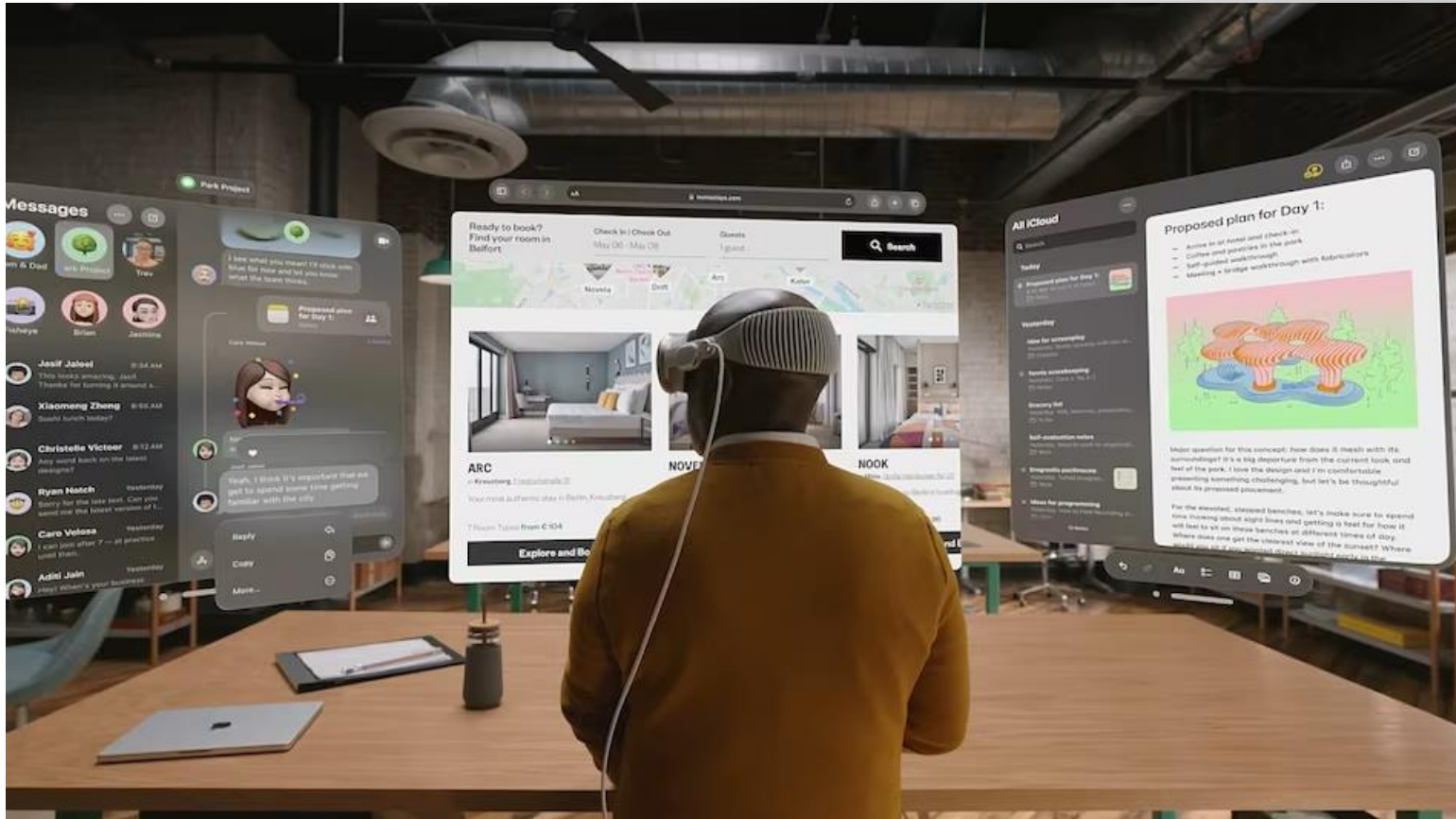


- Future...
  - Control your Life

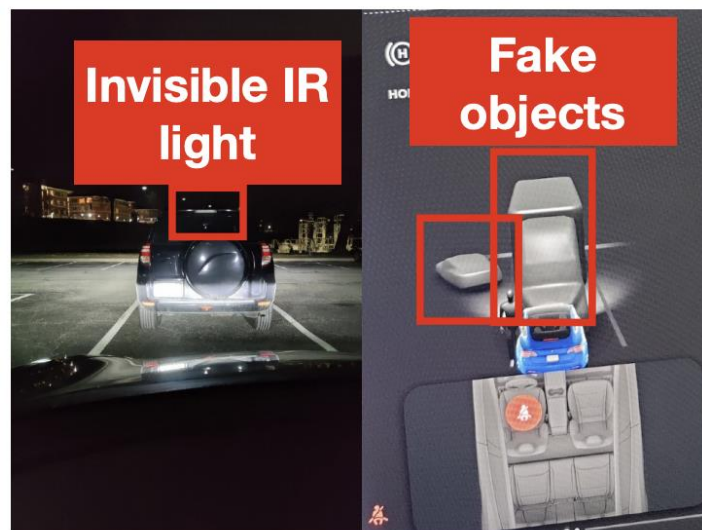
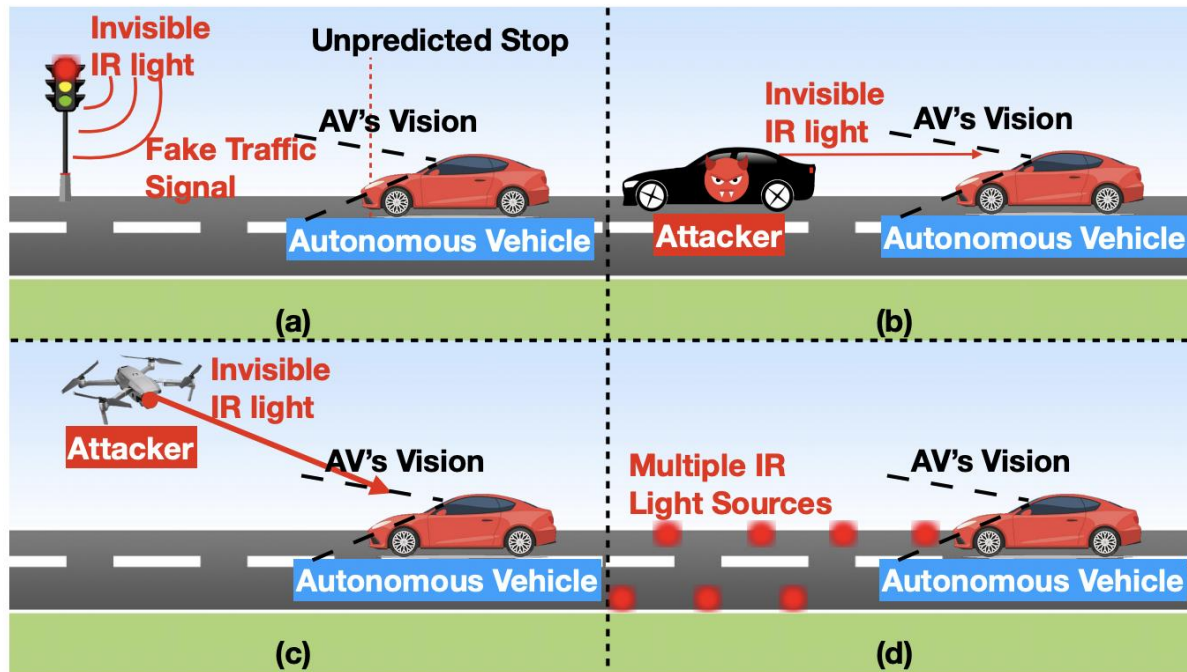


# Why do people write malware?

- Future...
  - Control your Life

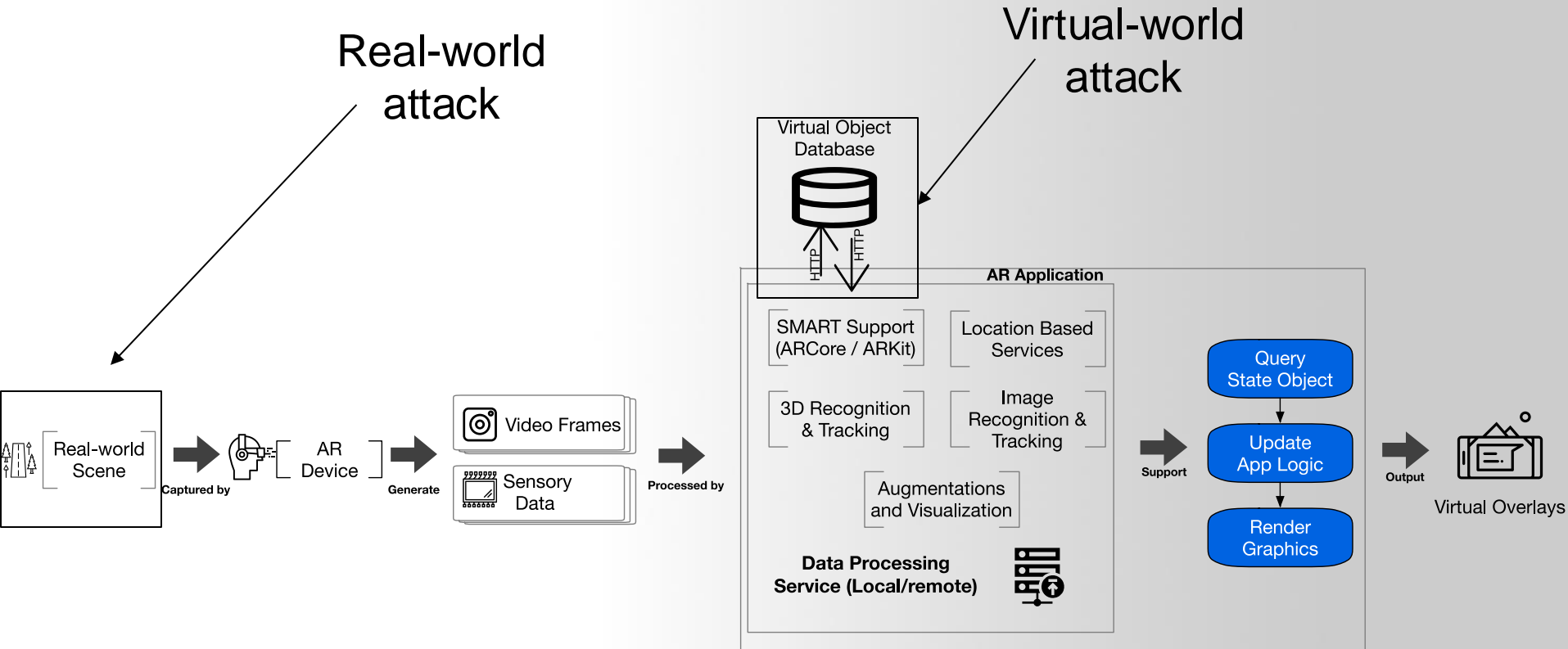


# I Can See the Light: Attacks on Autonomous Vehicles Using Invisible Lights





# Our project – AR Security



# Our approach

- **The content of the course is broken down into two sections:**
  - **Section 1: Foundations and Perspectives**
    - Lecture on the topic
    - Reading paper and answer some questions (Lab Homework)
  - **Section 2: In-depth Examination of Research Topics**
    - Group presentation and discussion on the research topics

# Top computer security conference

# 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.

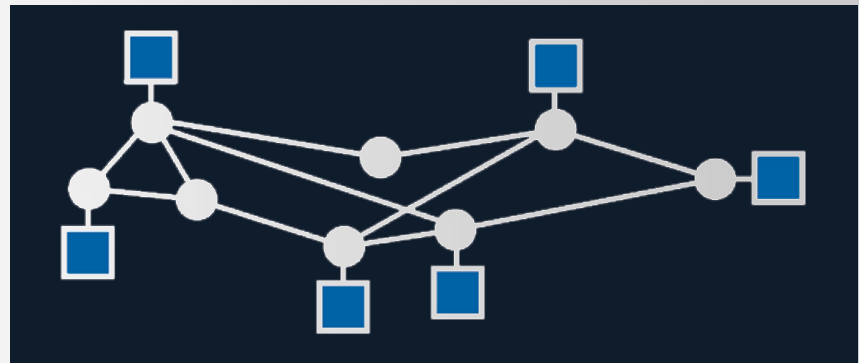
## IEEE Symposium on Security and Privacy (S&P)

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.



## 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.



## **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.

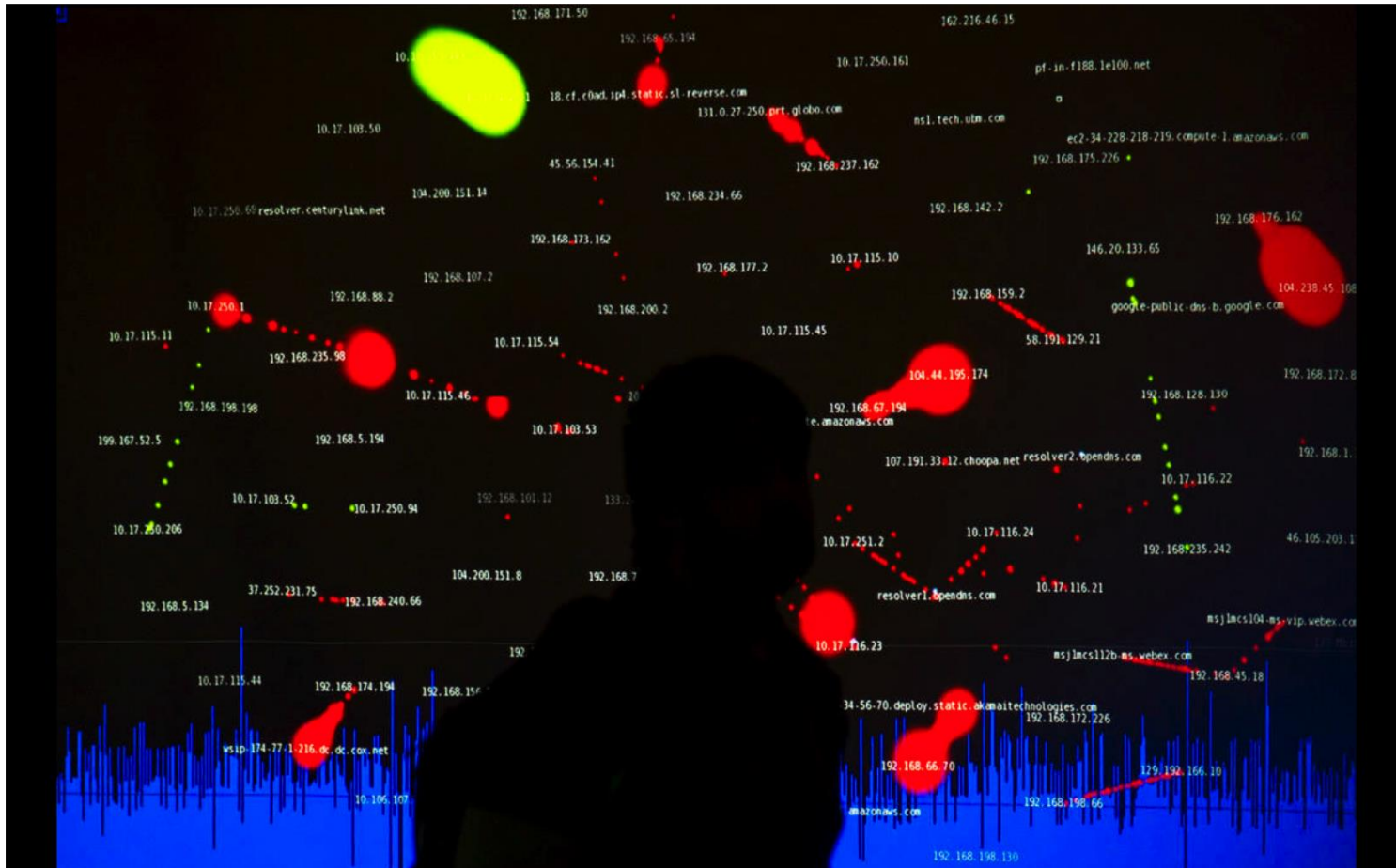


- **Top Security Conference for Hacking**

- **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





Q & A

