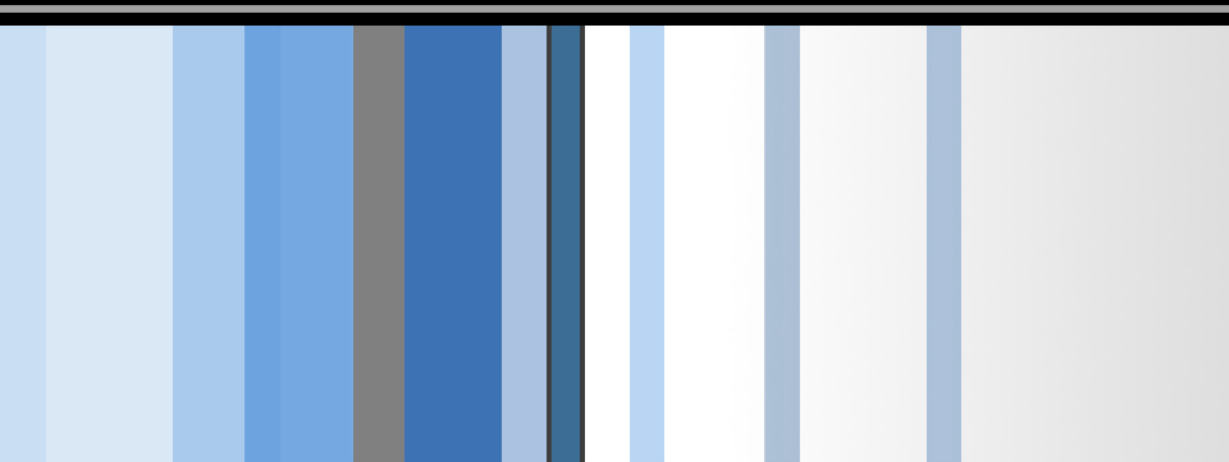


CSC 471/583

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
 - ...

- **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

```
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_
```

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

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.

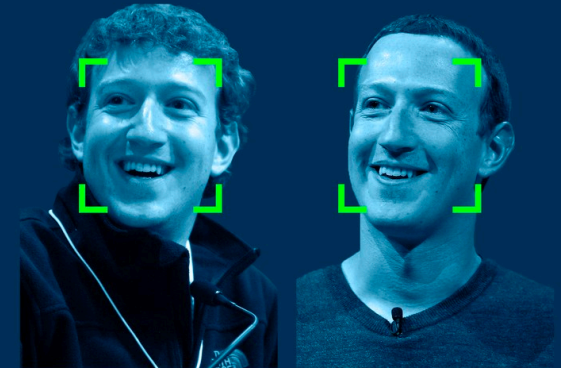
Why do people write malware?

- Future...
 - 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

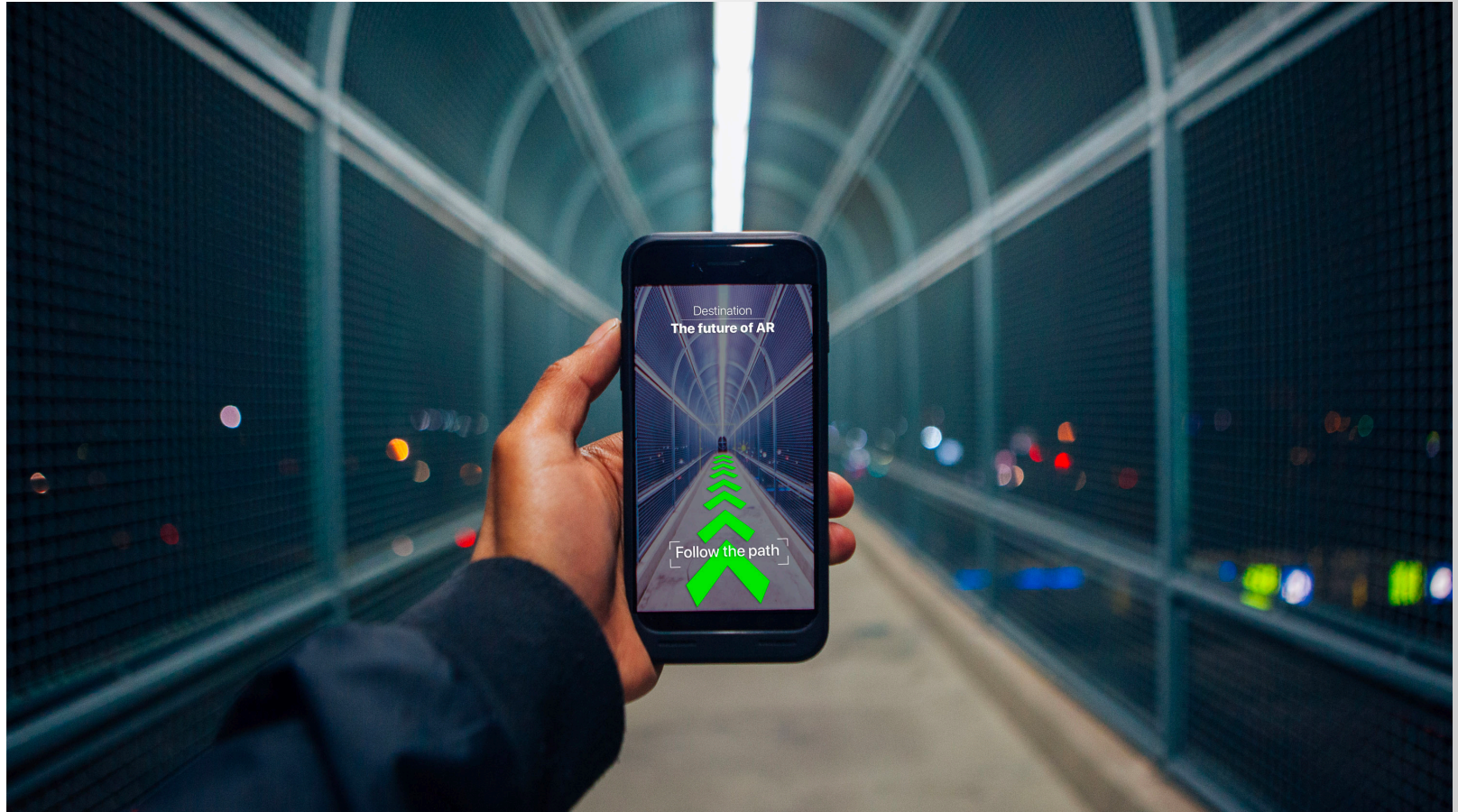
<https://www.youtube.com/watch?v=cQ54GDm1eL0>

Deepfakes are just the beginning for cybersecurity's Faceswap nightmare

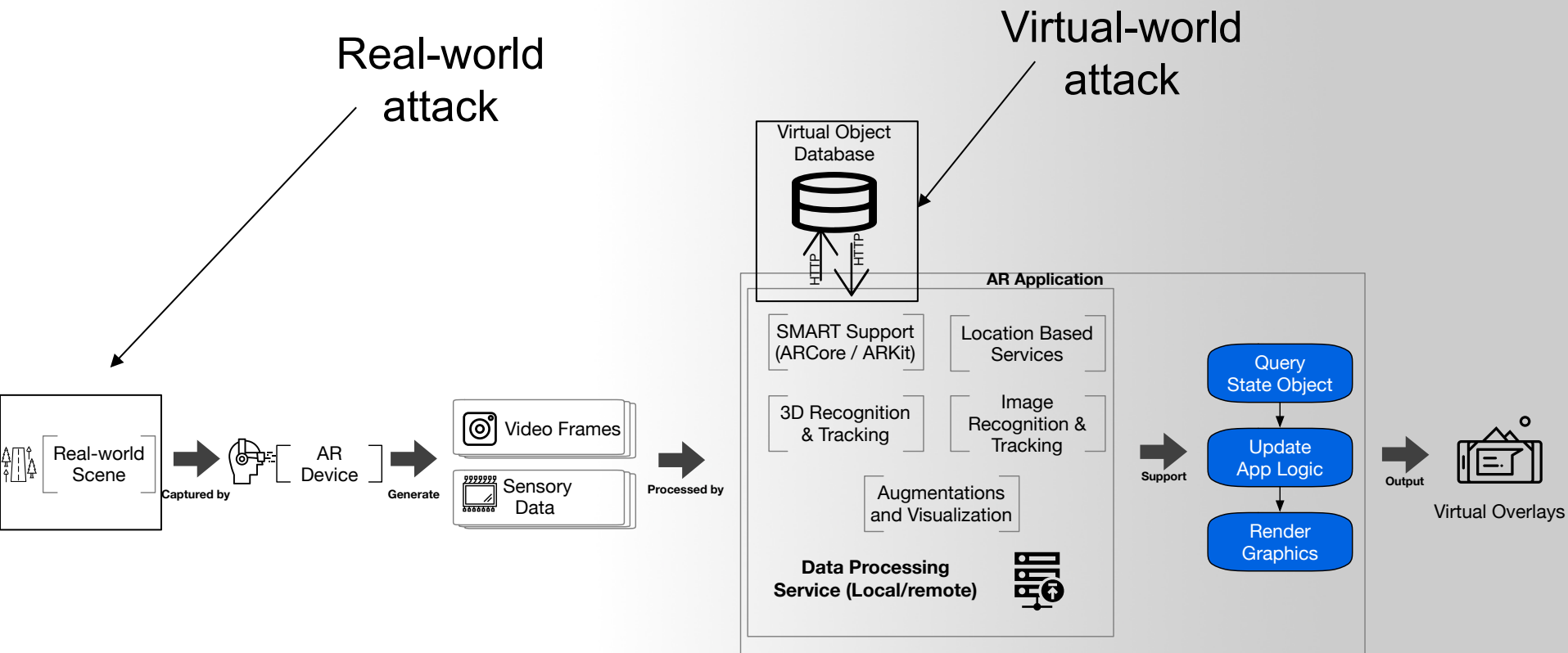
Fergus Halliday (PC World) on 04 April, 2018 14:44

Why do people write malware?

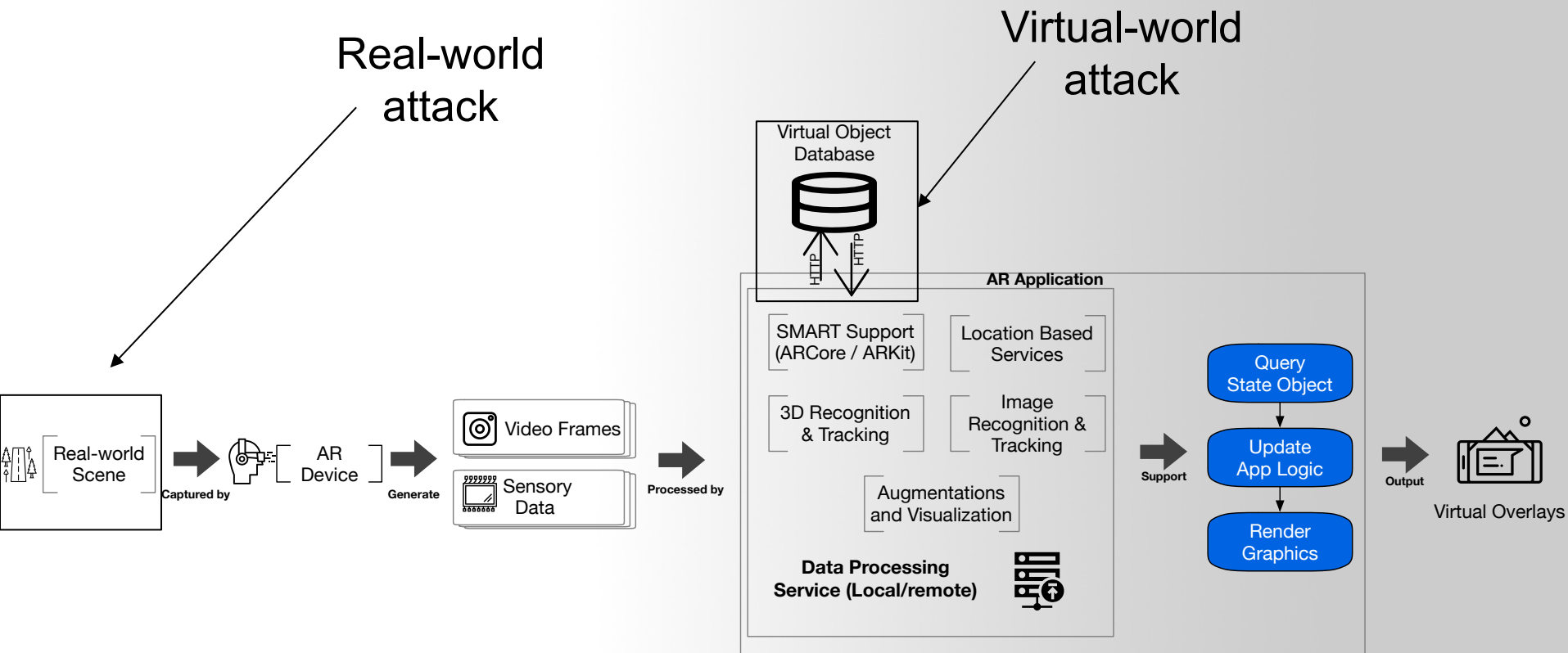
- Future...
 - Control your Life



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

```
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 CC614100 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 EDI,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
0040108D E8 07FFFFF 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
```



```
CHAR 'f'
CHAR 'b'
CHAR ':'
CHAR 'C'
CHAR '2'
CHAR '+'
CHAR 'H'
CHAR '0'
CHAR '0'
CHAR 'K'

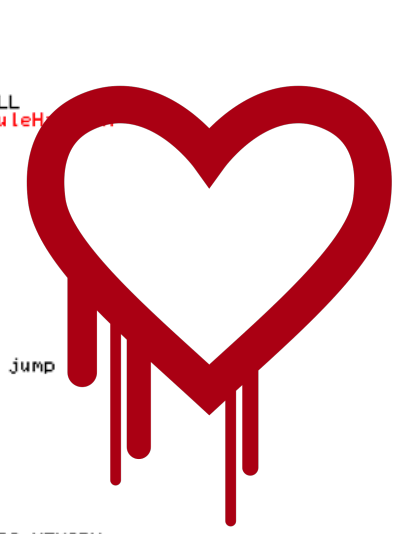
[Module Name = NULL
KERNEL32.GetModuleHandleA

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

[Module Name = NULL
KERNEL32.GetModuleHandleA

RET is used as a jump

[Size => 172.
Flags = HEAP_ZERO_MEMORY
KERNEL32.GetProcessHeap
Heap
NTDLL.Br.IALocateHeap
```



MELTDOWN

Top computer security conference --- The Big 4

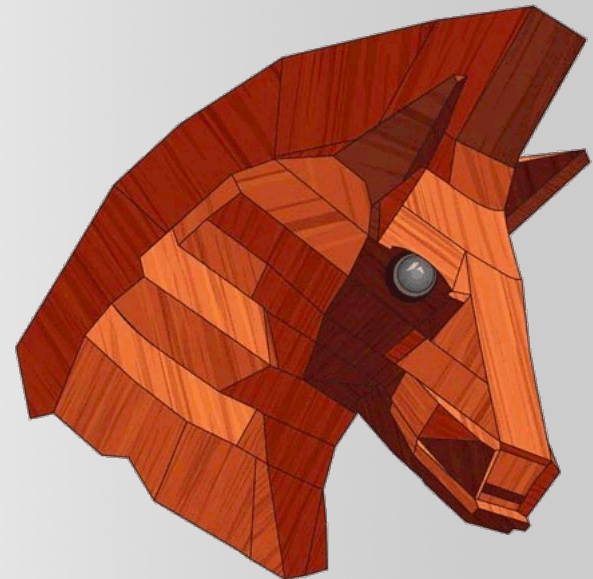
ACM Conference on Computer and Communications Security (CCS)

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.

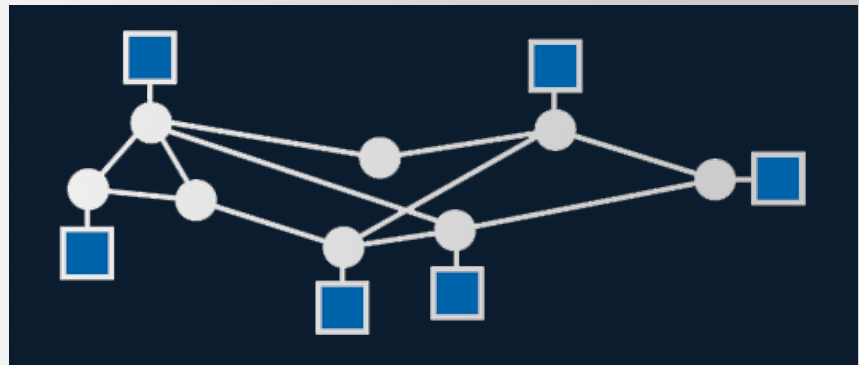
IEEE Symposium on Security and Privacy (S&P)

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**



Q & A

