MALWARE:
CASE STUDIES

CMSC 414

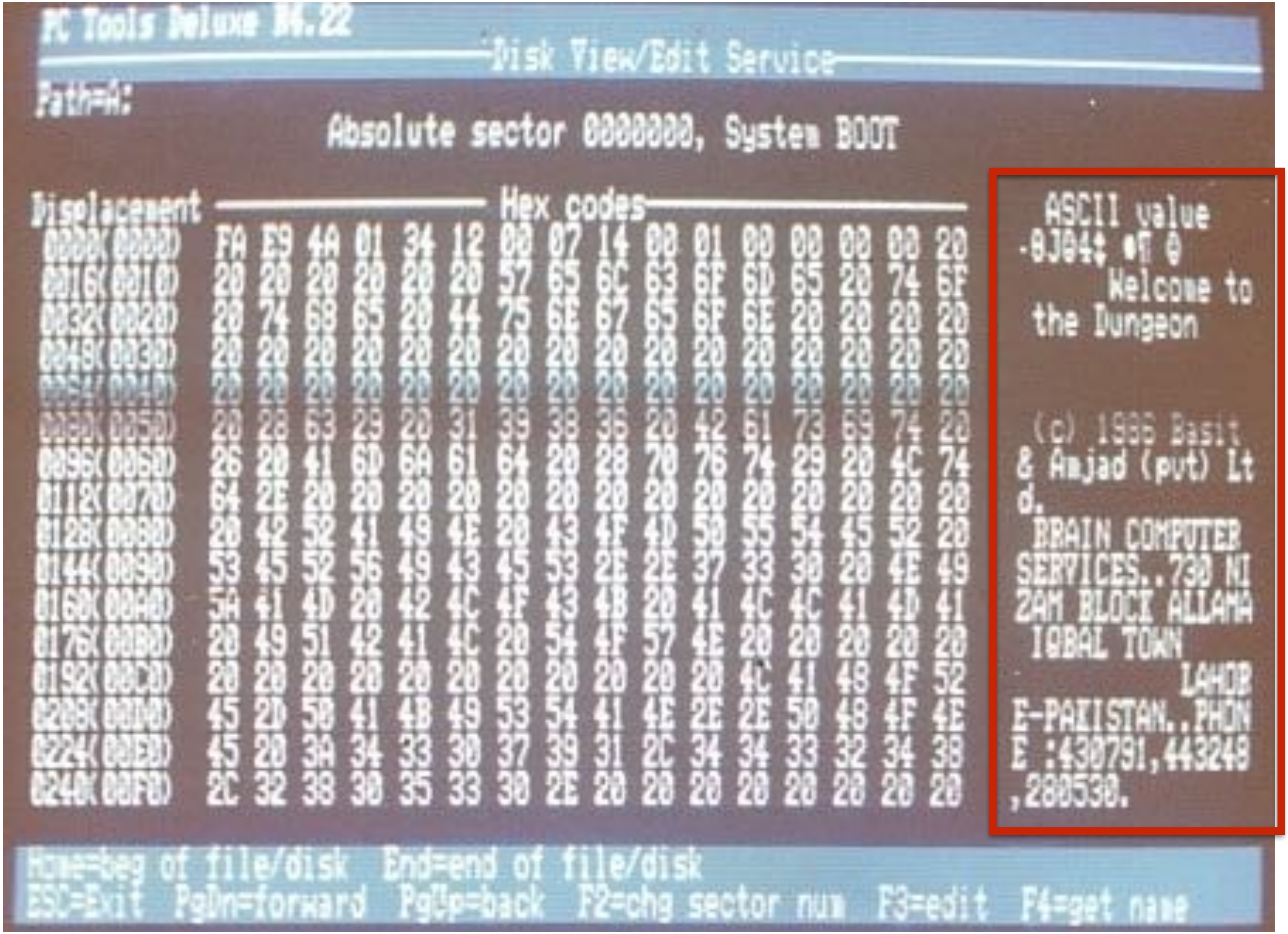
FEB 13 2018

BRAIN

First IBM PC virus (1987)

- Propagation method
  - Copies itself into the boot sector
  - Tells the OS that all of the boot sector is “faulty” (so that it won’t list contents to the user)
    - Thus also one of the first examples of a **stealth** virus
  - Intercepts disk read requests for 5.25” floppy drives
    - Sees if the 5th and 6th bytes of the boot sector are 0x1234
    - If so, then it’s already infected, otherwise, infect it

- Payload:
  - Nothing really; goal was just to spread (to show off?)
  - However, it served as the template for future viruses



```
PC Tools Deluxe R4.22
─────────────────────────Disk View/Edit Service──────────────────────────
Path=A:
                  Absolute sector 0000000, System BOOT

Displacement ─────────────── Hex codes ────────────────────    ASCII value
 0000(0000)  FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20   ·ΘJ☺4↕ •¶ ☺
 0016(0010)  20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F         Welcome to
 0032(0020)  20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20    the Dungeon
 0048(0030)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0064(0040)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0080(0050)  20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20    (c) 1986 Basit
 0096(0060)  26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74   & Amjad (pvt) Lt
 0112(0070)  64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20   d.
 0128(0080)  20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20    BRAIN COMPUTER
 0144(0090)  53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49   SERVICES..730 NI
 0160(00A0)  5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41   ZAM BLOCK ALLAMA
 0176(00B0)  20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20    IQBAL TOWN
 0192(00C0)  20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52              LAHOR
 0208(00D0)  45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E   E-PAKISTAN..PHON
 0224(00E0)  45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38   E :430791,443248
 0240(00F0)  2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20   ,280530.

Home=beg of file/disk  End=end of file/disk
ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Downloaded from wikipedia.org

ROOTKITS

Malicious code that hides from discovery

- Ways to hide:
  - By intercepting system calls, patching the kernel, etc.
  - Often effectively done by a man in the middle attack

- Rootkit revealer: analyzes the disk offline and through the online system calls, and compares

- Mark Russinovich ran a rootkit revealer and found a rootkit in 2005…

SONY XCP ROOTKIT

Detected 2005

SONY XCP ROOTKIT

Detected 2005

- Goal: keep users from copying copyrighted material

SONY XCP ROOTKIT

Detected 2005

- Goal: keep users from copying copyrighted material
- How it worked:
  - Loaded thanks to autorun.exe on the CD
  - Intercepted read requests for its music files
  - If anyone but Sony’s music player is accessing them, then garble the data
  - Hid itself from the user (to avoid deletion)

SONY XCP ROOTKIT

Detected 2005

- Goal: keep users from copying copyrighted material
- How it worked:
  - Loaded thanks to autorun.exe on the CD
  - Intercepted read requests for its music files
  - If anyone but Sony's music player is accessing them, then garble the data
  - Hid itself from the user (to avoid deletion)
- How it messed up
  - Morally: violated trust
  - Technically: Hid ***all files*** that started with "sys"
  - Seriously?: The uninstaller did not check the integrity of the code it downloaded, and would not delete it afterwords.

STUXNET

June 2010

- Virus in that it initially spread by infected USB stick
  - Once inside a network, it acted as a worm, spreading quickly
- Exploited **four** zero-day exploits
  - Zero-day: Known to only the attacker until the attack
  - Typically, one zero-day is enough to profit
  - Four was unprecedented
    - Immense cost and sophistication on behalf of the attacker
- Rootkit: installed *signed* device drivers
  - Thereby avoiding user alert when installing
  - Signed with certificates stolen from two Taiwanese CAs

STUXNET: PAYLOAD

STUXNET: PAYLOAD

- Do nothing

STUXNET: PAYLOAD

- Do nothing
- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz

STUXNET: PAYLOAD

- Do nothing
- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
    - You know, like those in Iran and Finland

STUXNET: PAYLOAD

- Do nothing
- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
  - You know, like those in Iran and Finland
  - .. those ones that are used to operate centrifuges

STUXNET: PAYLOAD

- Do nothing
- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
    - You know, like those in Iran and Finland
    - .. those ones that are used to operate centrifuges
    - .. for producing enriched uranium for nuclear weapons

STUXNET: PAYLOAD

- Do nothing

- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
    - You know, like those in Iran and Finland
    - .. those ones that are used to operate centrifuges
    - .. for producing enriched uranium for nuclear weapons

- In which case, slowly increase the freq to 1410Hz

STUXNET: PAYLOAD

- Do nothing
- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
  - You know, like those in Iran and Finland
  - .. those ones that are used to operate centrifuges
  - .. for producing enriched uranium for nuclear weapons
- In which case, slowly increase the freq to 1410Hz
  - You know, enough to break the centrifuge

STUXNET: PAYLOAD

- Do nothing
- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
  - You know, like those in Iran and Finland
  - .. those ones that are used to operate centrifuges
  - .. for producing enriched uranium for nuclear weapons
- In which case, slowly increase the freq to 1410Hz
  - You know, enough to break the centrifuge
  - .. all the while sending “looks good to me” readings to the user

STUXNET: PAYLOAD

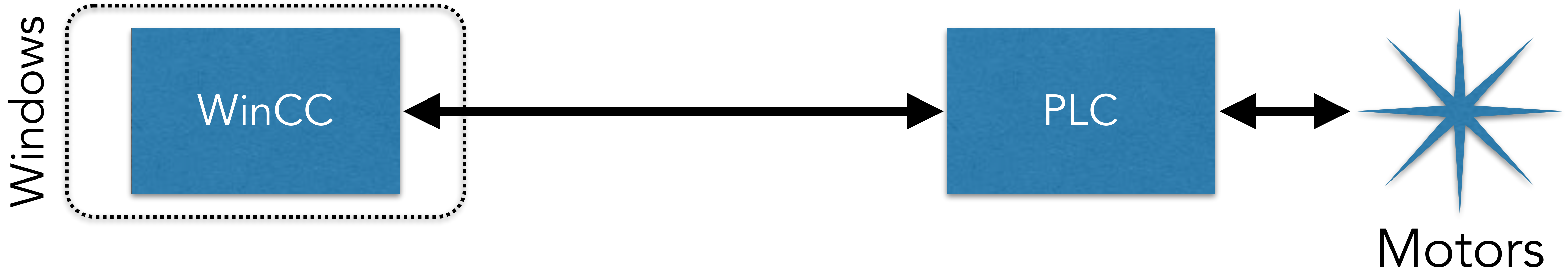
- Do nothing

- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
  - You know, like those in Iran and Finland
  - .. those ones that are used to operate centrifuges
  - .. for producing enriched uranium for nuclear weapons

- In which case, slowly increase the freq to 1410Hz
  - You know, enough to break the centrifuge
  - .. all the while sending “looks good to me” readings to the user
  - .. then drop back to normal range

STUXNET: PAYLOAD

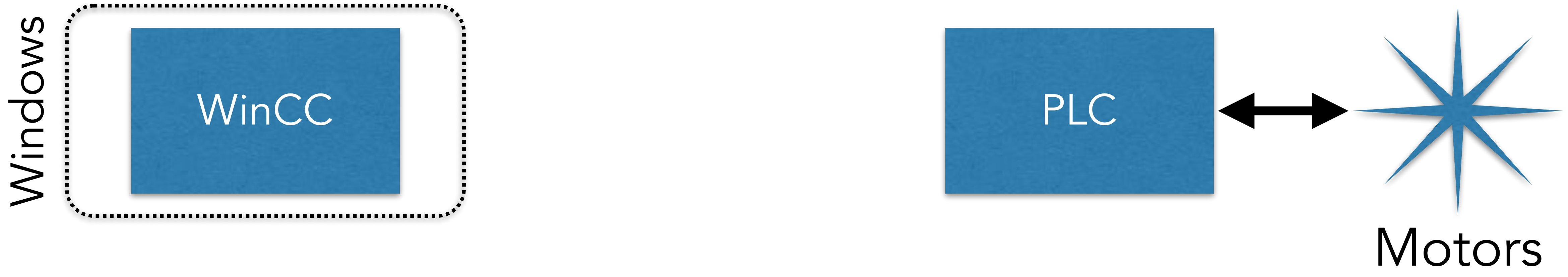
- Targets industrial control systems by overwriting programmable logic boards
- Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator



- In reality, it sped up and slowed down the motors
- Result: Destroy (or at least decrease the productivity of) nuclear centrifuges

STUXNET: PAYLOAD

- Targets industrial control systems by overwriting programmable logic boards
- Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator

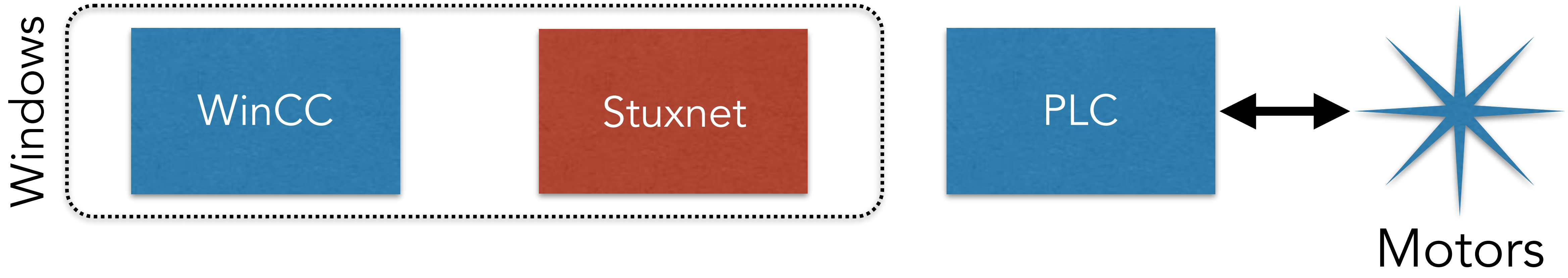


- In reality, it sped up and slowed down the motors
- Result: Destroy (or at least decrease the productivity of) nuclear centrifuges

STUXNET: PAYLOAD

- Targets industrial control systems by overwriting programmable logic boards

- Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator



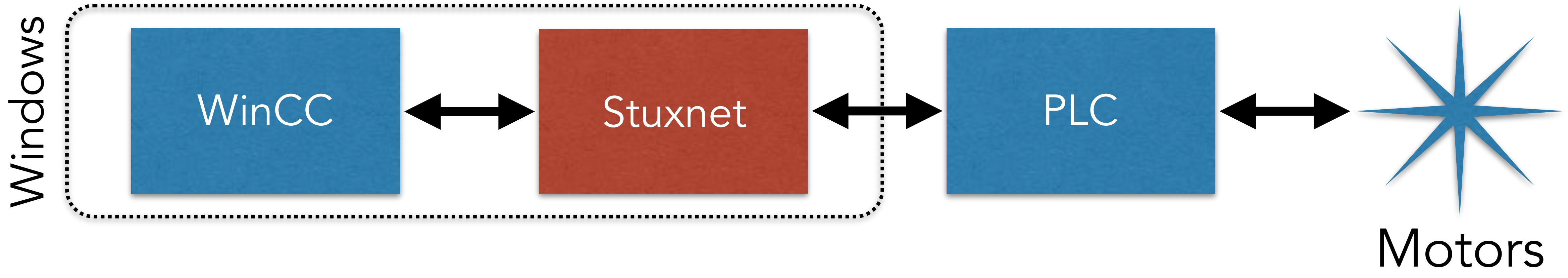
- In reality, it sped up and slowed down the motors

- Result: Destroy (or at least decrease the productivity of) nuclear centrifuges

STUXNET: PAYLOAD

- Targets industrial control systems by overwriting programmable logic boards

- Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator



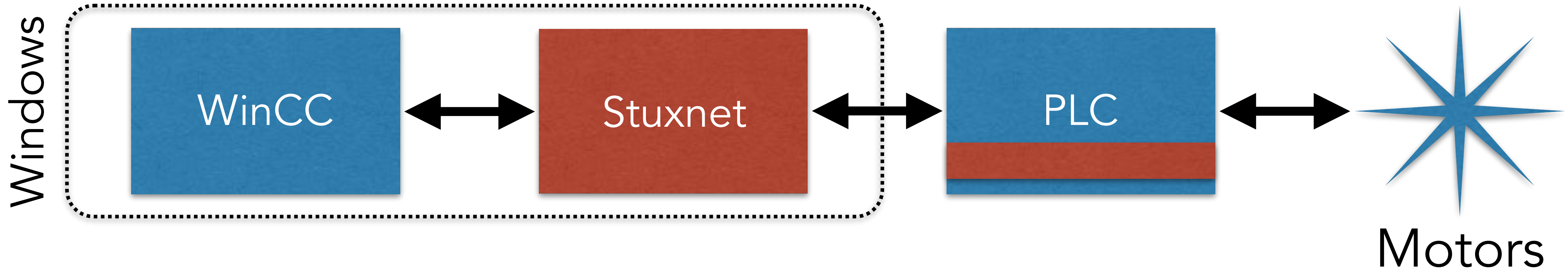
- In reality, it sped up and slowed down the motors

- Result: Destroy (or at least decrease the productivity of) nuclear centrifuges

STUXNET: PAYLOAD

- Targets industrial control systems by overwriting programmable logic boards

- Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator



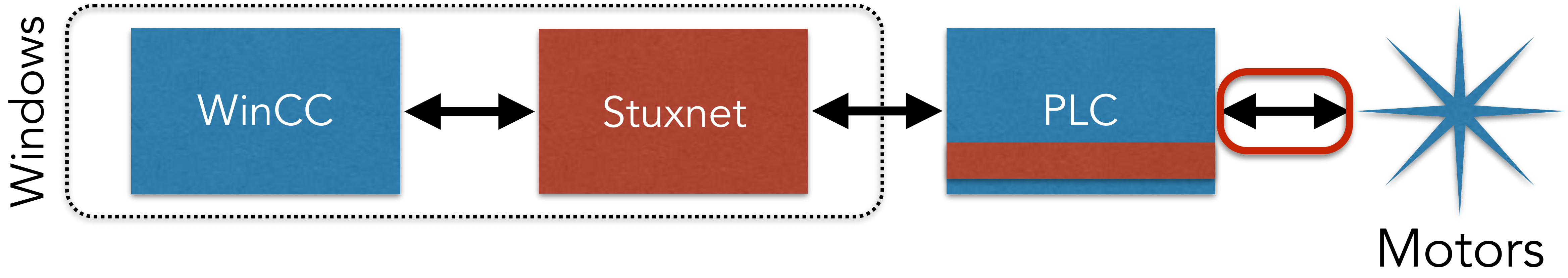
- In reality, it sped up and slowed down the motors

- Result: Destroy (or at least decrease the productivity of) nuclear centrifuges

STUXNET: PAYLOAD

- Targets industrial control systems by overwriting programmable logic boards

- Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator



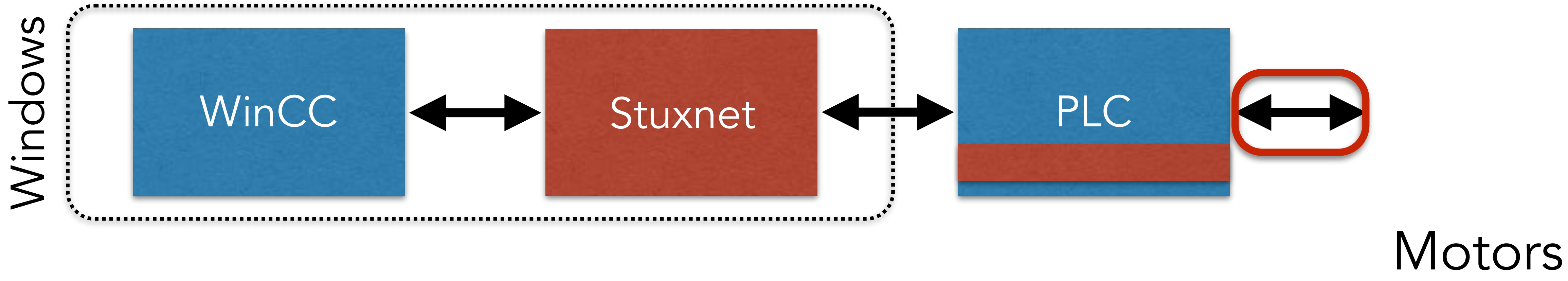
- In reality, it sped up and slowed down the motors

- Result: Destroy (or at least decrease the productivity of) nuclear centrifuges

STUXNET: PAYLOAD

- Targets industrial control systems by overwriting programmable logic boards

- Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator



- In reality, it sped up and slowed down the motors

- Result: Destroy (or at least decrease the productivity of) nuclear centrifuges

STUXNET FALLOUT

- Iran denied they had been hit by Stuxnet
- Then claimed they were, but had contained it
- Understood now that it took out 1k of Iran’s 5k centrifuges
- Security experts believe the U.S. did it (possibly along with Israel) due to its sophistication and cost
- **Legitimized cyber warfare**

VIRUSES: SUMMARY

- Technological arms race between those who wish to detect and those who wish to evade detection

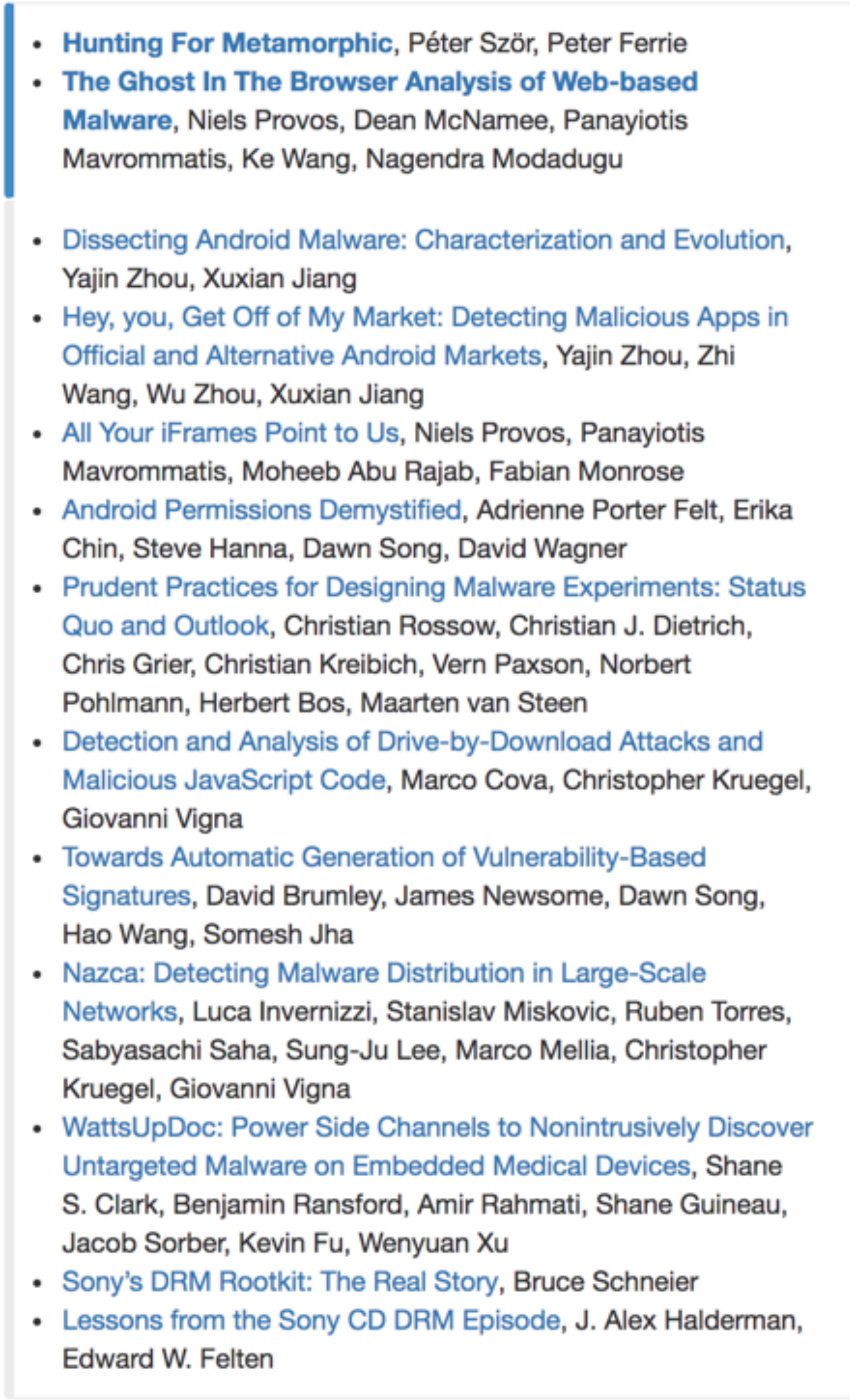
- Started off innocuously, capable by only a few very clever people

- But viruses have become commoditized; any scriptkiddy can launch one (creation remains hard)

- No longer purely of academic interest
  - Economic pursuits (zero-day markets)
  - Cyber warfare

OTHER WORK

- Detecting malware in the Android app store
- Lots of drive-by-download work
- Malware distribution networks: use enterprise-wide network traces to detect malware downloads
- Side-channel defenses: Measure, e.g., power consumption of benign vs. malicious code
- Metamorphic arms race



- **Hunting For Metamorphic**, Péter Ször, Peter Ferrie
- **The Ghost In The Browser Analysis of Web-based Malware**, Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, Nagendra Modadugu

- Dissecting Android Malware: Characterization and Evolution, Yajin Zhou, Xuxian Jiang
- Hey, you, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets, Yajin Zhou, Zhi Wang, Wu Zhou, Xuxian Jiang
- All Your iFrames Point to Us, Niels Provos, Panayiotis Mavrommatis, Moheeb Abu Rajab, Fabian Monrose
- Android Permissions Demystified, Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, David Wagner
- Prudent Practices for Designing Malware Experiments: Status Quo and Outlook, Christian Rossow, Christian J. Dietrich, Chris Grier, Christian Kreibich, Vern Paxson, Norbert Pohlmann, Herbert Bos, Maarten van Steen
- Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code, Marco Cova, Christopher Kruegel, Giovanni Vigna
- Towards Automatic Generation of Vulnerability-Based Signatures, David Brumley, James Newsome, Dawn Song, Hao Wang, Somesh Jha
- Nazca: Detecting Malware Distribution in Large-Scale Networks, Luca Invernizzi, Stanislav Miskovic, Ruben Torres, Sabyasachi Saha, Sung-Ju Lee, Marco Mellia, Christopher Kruegel, Giovanni Vigna
- WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices, Shane S. Clark, Benjamin Ransford, Amir Rahmati, Shane Guineau, Jacob Sorber, Kevin Fu, Wenyuan Xu
- Sony's DRM Rootkit: The Real Story, Bruce Schneier
- Lessons from the Sony CD DRM Episode, J. Alex Halderman, Edward W. Felten