An Overview of Reverse Engineering

Nuri Çilengir

Content

- Approaches
- Engineering
- Reverse Engineering
- Example Projects
- Application of Reverse Engineering

Different Approaches

- Top-down and Bottom-up strategies of information processing, knowledge ordering.
- Top-down approach
- breaking down of a system to gain insight into its compositional sub-systems in a reverse engineering fashion.
- Each subsystem is then refined in yet greater detail
- Top down approach starts with the big picture. It breaks down from there into smaller segments.

- https://en.wikipedia.org/wiki/Top-down_and_bottom-up_design#Computer_science

Manufacture

- Manufacture is the process of changing nature in order to meet the necessity of people to develop and sustain their existence. This effort is also the process of changing man's nature while he is changing nature.

Engineering ?

- The creative application of scientific principles to design or develop structures, machines, apparatus, or manufacturing processes, or works utilizing them singly or in combination; or to construct or operate the same with full cognizance of their design; or to forecast their behavior under specific operating conditions; all as respects an intended function, economics of operation and safety to life and property.(Britannica)
- Application and practical knowledge
- Invent, innovate, build, improve, maintain etc
- https://en.wikipedia.org/wiki/Outline_of_academic_disciplines

Reverse Engineering

- *Extraction of **knowledge** methodology,structure or design etc.*
- **Reverse engineering, also called back engineering, is the process of analyzing a subject system to create representations of the system at a higher level of abstraction.**
- **“going backwards through the development cycle”**
- *https://en.wikipedia.org/wiki/Reverse_engineering*

Reverse Engineering

- Kısaca, Mühendislik olgu veya ürünün diyalektik bakış ile ortaya çıkışı ise olgu ürün veya sürece karşı diyalektik bir bakış açısı da tersine mühendisliktir.
- Reverse Engineering is the foundation of Engineering. NAPOLEON BONAPARTE (1453)

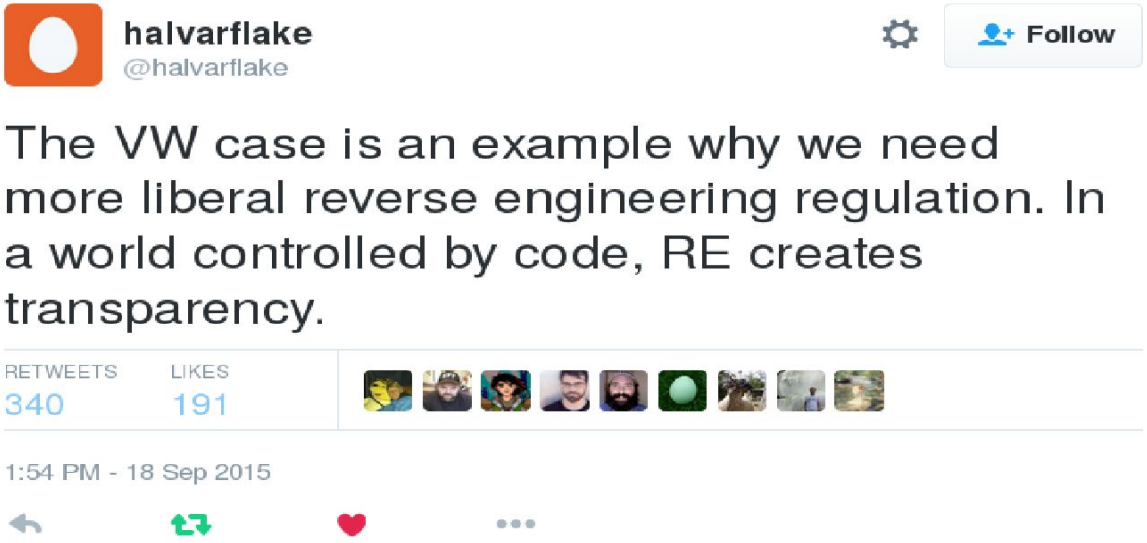
Motivation

- Espionage ?
- Outdated software/hardware that nobody knows ?
- Remove restrictions on software/hardware.
- Security
- Bug fixing
- Examine viruses and malware
- Open-Source ?

Example Projects

- **Wine**
- Samba
- **OpenOffice & LibreOffice**
- **ReactOS**
- Windows Internals

Tansparency ?



https://en.wikipedia.org/wiki/Volkswagen_emissions_scandal

Application Fiels of RE

- Bus analyzer
- Clone (computing)
- Connectix Virtual Game Station
- Cryptanalysis
- Forensic engineering
- Decompile
- Software cracking
- Software archaeology
- etc.

Application Fiels of RE

- Reverse engineering of software
- Reverse engineering of integrated circuits/smart cards
- Reverse engineering of protocols
- Reverse engineering of machines

Reverse engineering of software

- Institute of Electrical and Electronics Engineers (IEEE) defined reverse engineering as "the process of analyzing a subject system to identify the system's components and their interrelationships and to create representations of the system in another form or at a higher level of abstraction", where the "subject system" is the end product of software development.
-

How ?


#include<stdio.h>
int add(int prm1, int prm2)
{
int result;
result = prm1 + prm2;
return result;
}
int main()
{
int i = 10;
int j = 20;
int sonuc;
sonuc = add(i, j);
printf("Sonuc = %d", sonuc);
getchar();
}
DERLEME
LİNKLEME
push ebp
mov ebp,esp
sub esp,0C
mov dword ptr ss:[ebp-8],0A
mov dword ptr ss:[ebp-4],14
mov eax,dword ptr ss:[ebp-4]
push eax
mov ecx,dword ptr ss:[ebp-8]
push ecx
call PE-x86-0.add
add esp,8
mov dword ptr ss:[ebp-C],eax
mov edx,dword ptr ss:[ebp-C]
push edx
push PE-x86-0.00403000
call PE-x86-0.printf
add esp,8
TERSİNE MÜHENDİSLİK

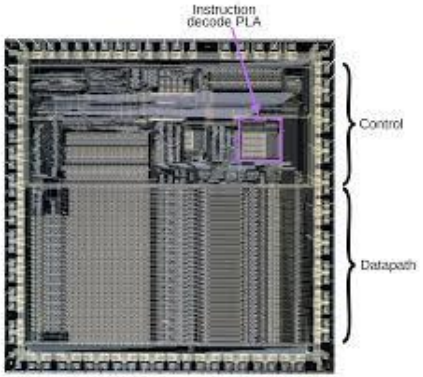
Enviroment Variable

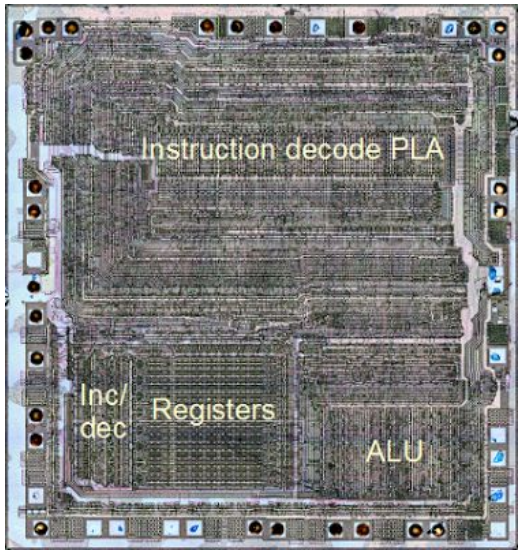
- Mimari: Intel x86, PowerPC, ARM vs.
- İşletim Sistemi: GNU+Linux, FreeBSD, Windows vs.
- Sanal Ortam: Java, .NET vs.
- Çalıştırılabilir Dosya: PE, ELF vs.

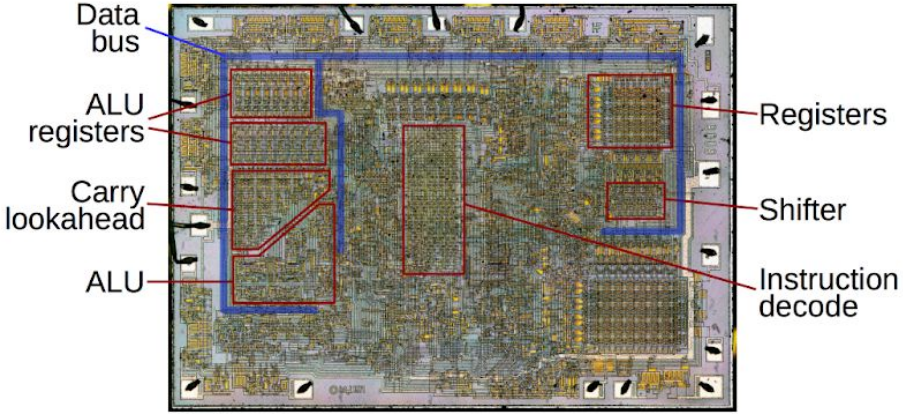
Reverse engineering of integrated circuits/smart cards

- Reverse engineering is an invasive and destructive form of analyzing a smart card. The attacker grinds away layer after layer of the smart card and takes pictures with an electron microscope. With this technique, it is possible to reveal the complete hardware and software part of the smart card. The major problem for the attacker is to bring everything into the right order to find out how everything works. The makers of the card try to hide keys and operations by mixing up memory positions, for example, bus scrambling.
- https://twitter.com/i/status/1112642788439588864

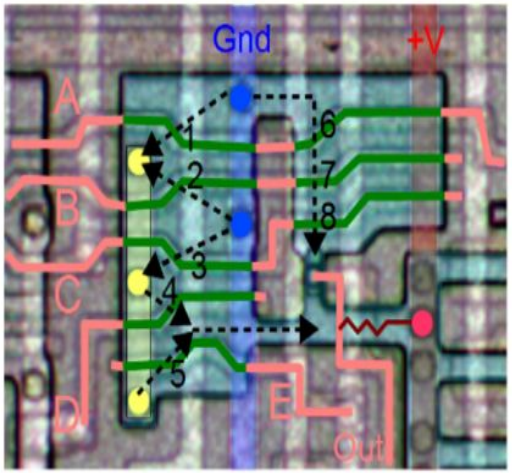
https://twitter.com/reivilo_t/status/1112642788439588864?s=19

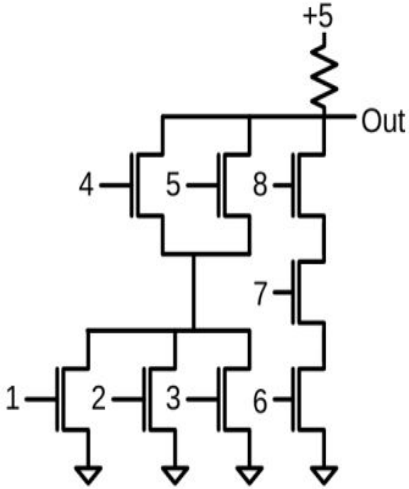


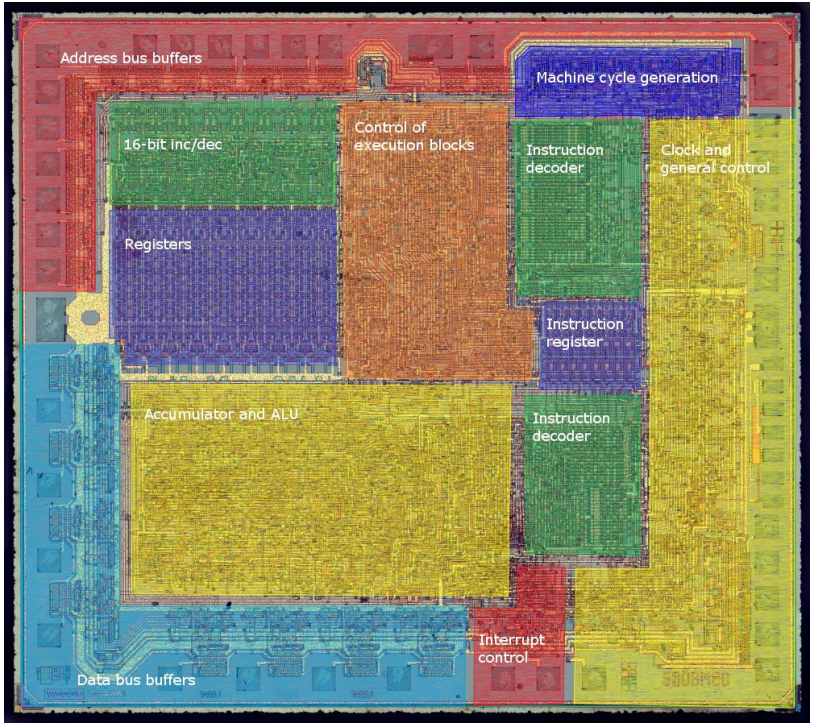

Instruction decode PLA
Inc/
dec
Registers
ALU


Data
bus
ALU
registers
Carry
lookahead
ALU
Registers
Shifter
Instruction
decode

Gates get weird in the ALU

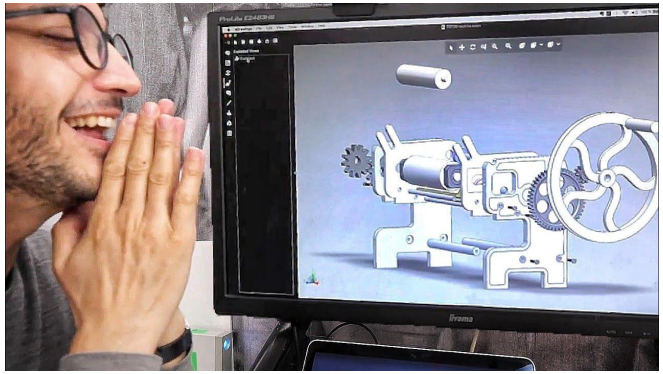






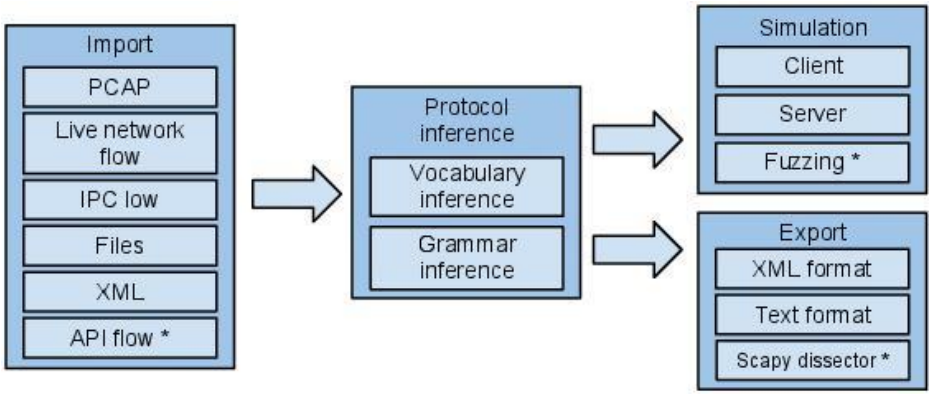
Reverse engineering of machines

- As computer-aided design (CAD) has become more popular, reverse engineering has become a viable method to create a 3D virtual model of an existing physical part for use in 3D CAD, CAM, CAE or other software.[10] The reverse-engineering process involves measuring an object and then reconstructing it as a 3D model. The physical object can be measured using 3D scanning technologies like CMMs, laser scanners, structured light digitizers, or Industrial CT Scanning (computed tomography).



Reverse engineering of protocols

- **Protocols are sets of rules that describe message formats and how messages are exchanged (i.e., the protocol state-machine). Accordingly, the problem of protocol reverse-engineering can be partitioned into two subproblems; message format and state-machine reverse-engineering.**

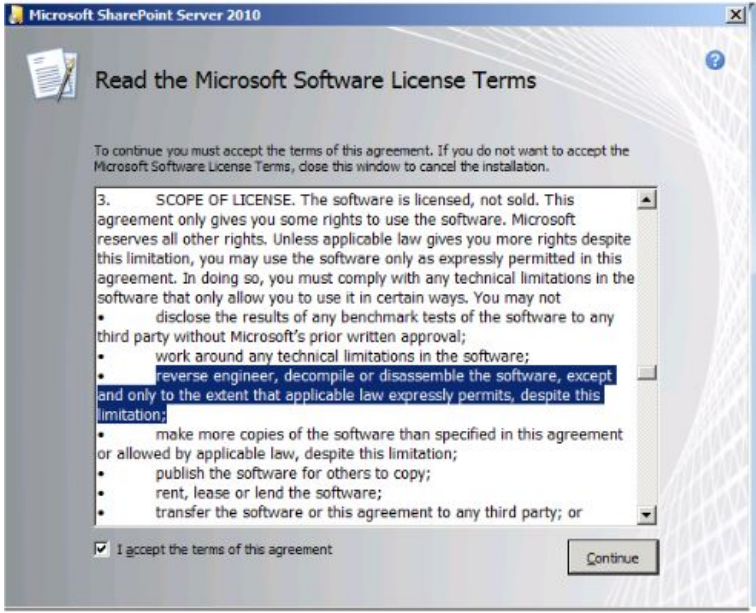


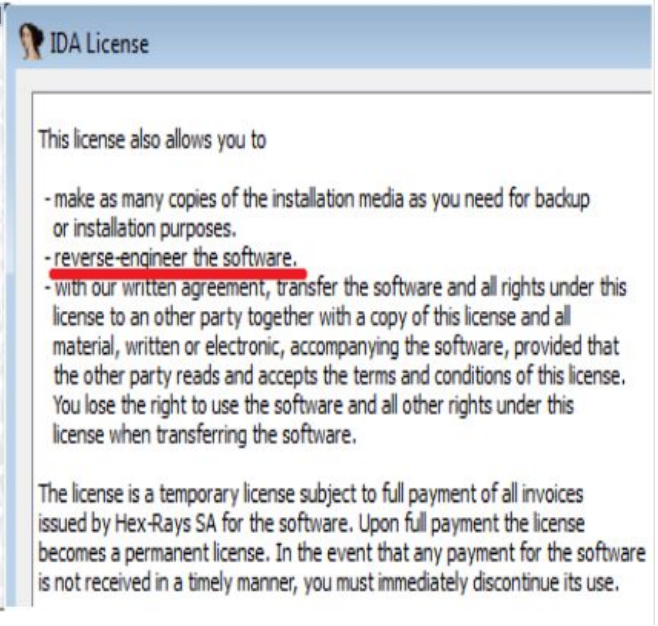
Reverse engineering for military applications

- Tupolev Tu-4
- V2 Roketi

Is it Legal?

- **Grey area**
- **EULA, Copyright, DMCA, Trade Secret Law**
- **https://www.eff.org/tr/issues/coders/reverse-engineering-faq**


Microsoft SharePoint Server 2010
Read the Microsoft Software License Terms
To continue you must accept the terms of this agreement. If you do not want to accept the Microsoft Software License Terms, close this window to cancel the installation.
3. SCOPE OF LICENSE. The software is licensed, not sold. This agreement only gives you some rights to use the software. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not
• disclose the results of any benchmark tests of the software to any third party without Microsoft's prior written approval;
• work around any technical limitations in the software;
• reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
• make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
• publish the software for others to copy;
• rent, lease or lend the software;
• transfer the software or this agreement to any third party; or
I accept the terms of this agreement
Continue


IDA License
This license also allows you to
- make as many copies of the installation media as you need for backup or installation purposes.
- reverse-engineer the software.
- with our written agreement, transfer the software and all rights under this license to an other party together with a copy of this license and all material, written or electronic, accompanying the software, provided that the other party reads and accepts the terms and conditions of this license. You lose the right to use the software and all other rights under this license when transferring the software.
The license is a temporary license subject to full payment of all invoices issued by Hex-Rays SA for the software. Upon full payment the license becomes a permanent license. In the event that any payment for the software is not received in a timely manner, you must immediately discontinue its use.