

Softwareschutz nach Kerckhoffs' Prinzip

- ┌ Dr. Peer Wichmann
- ┌ IT-Sicherheitsbeauftragter

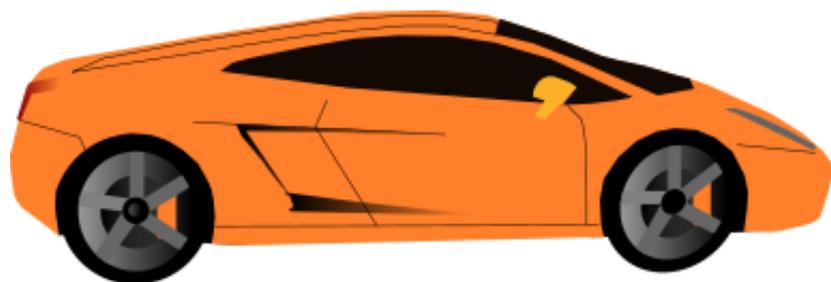
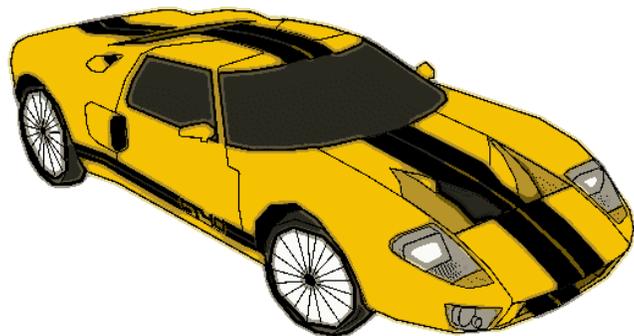










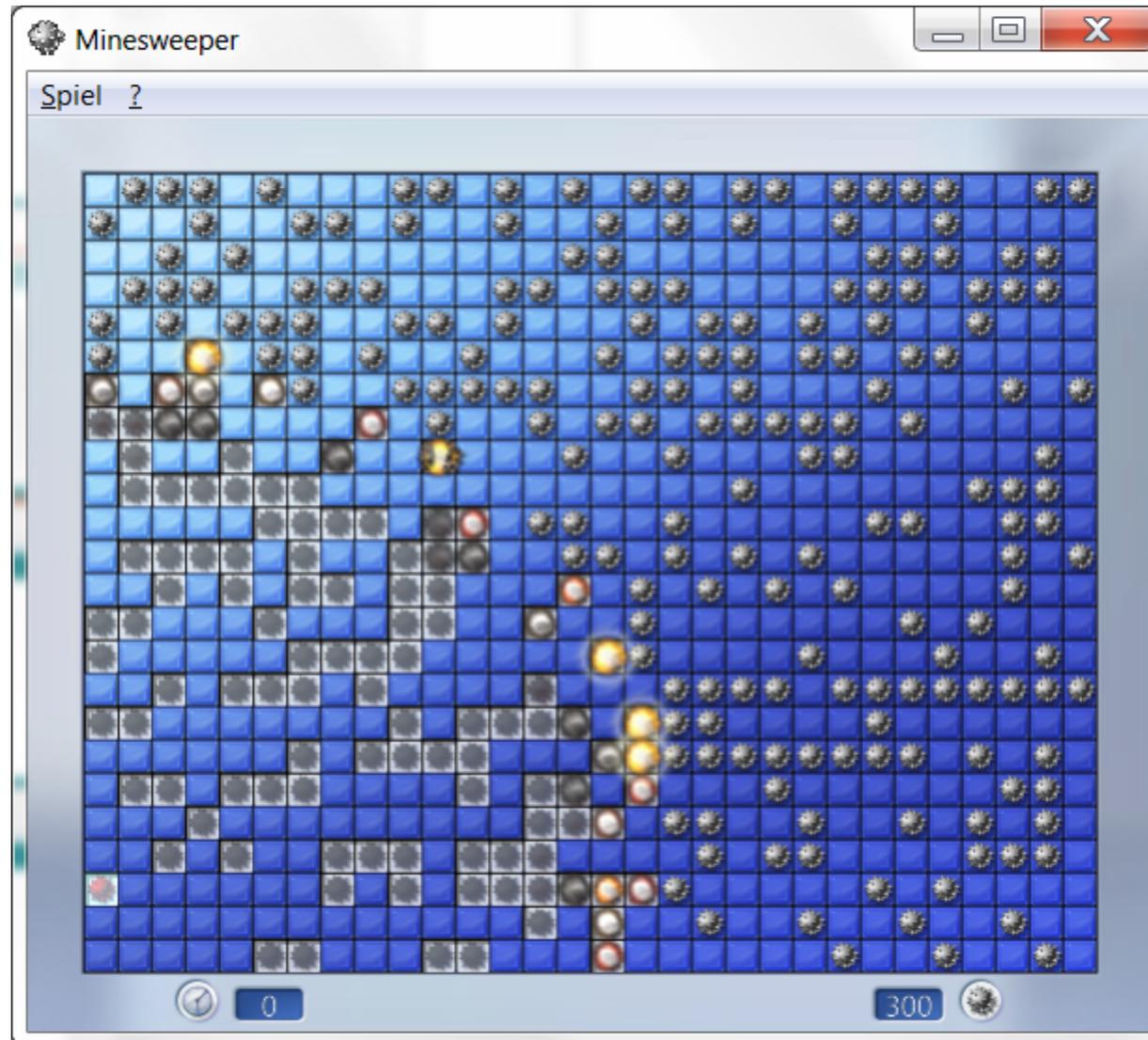






Profed dl. Kerckhoffs August,
difikel kadema vya.





The image shows two overlapping software windows. The background window is FormatFactory 4.0.0, a media conversion application. The foreground window is WinAPIOverride64, a hooking utility.

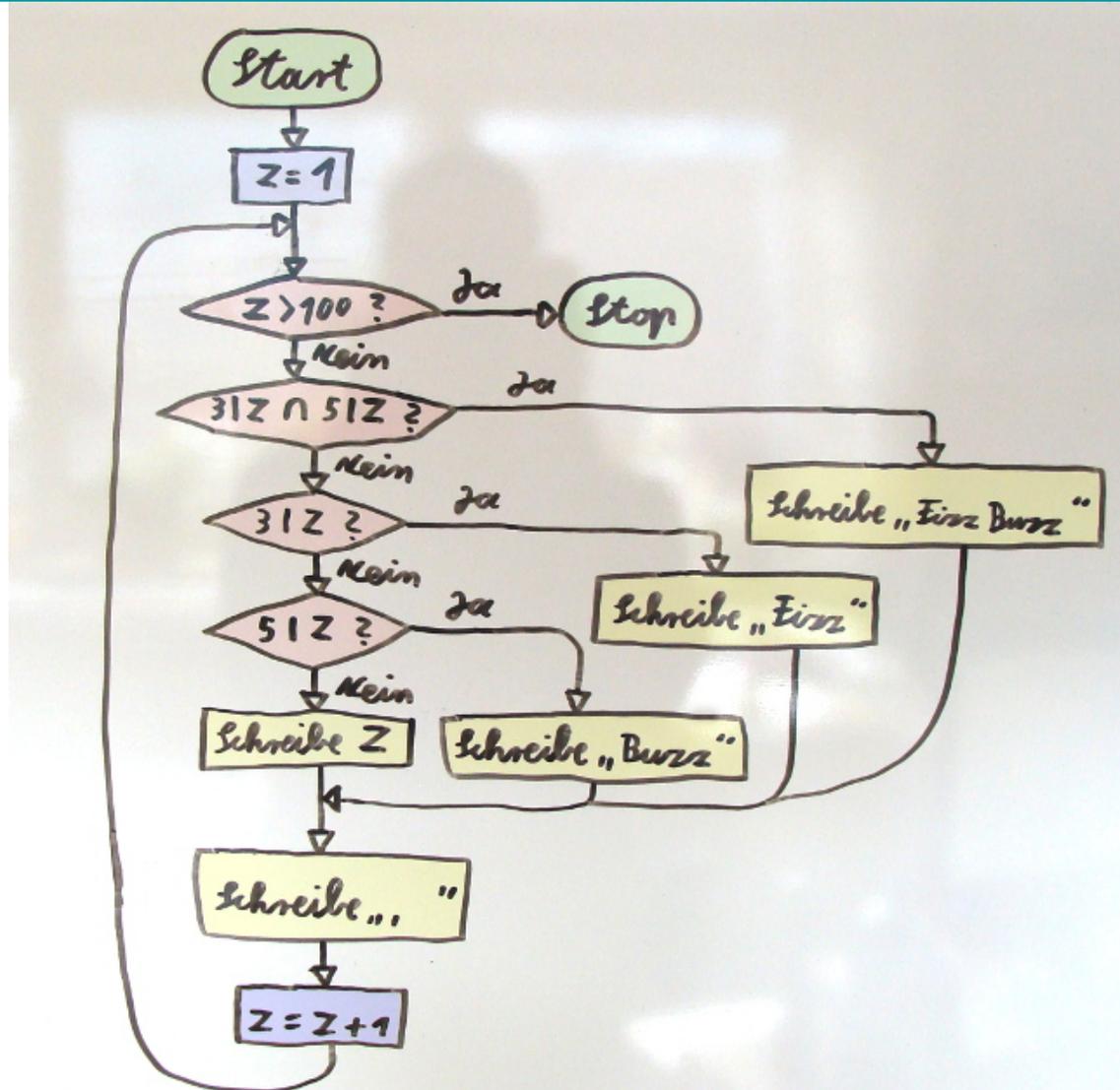
FormatFactory 4.0.0 interface includes:

- Menu: AUFGABE, OBERFLÄCHE, SPRACHE, HILFE
- Buttons: Zielverzeichnis, Optionen, Entfernen, Liste löschen, Stoppen, Starten, Picosmos Picture Tools
- Source: Quelldatei, Größe, Konvertierungsstatus, Ziel [F2]
- Video conversion options:
 - Mobiles Gerät, MP4
 - MKV, AVI, WebM
 - 3GP, GIF, WMV
 - MPEG, VOB, MOV
 - FLV, SWF
- Audio, Bilder, Document, ROM-Gerät\DVD\CD\ISO, Dienstprogramme
- Status: C:\FFOutput, Use Multi-Threads

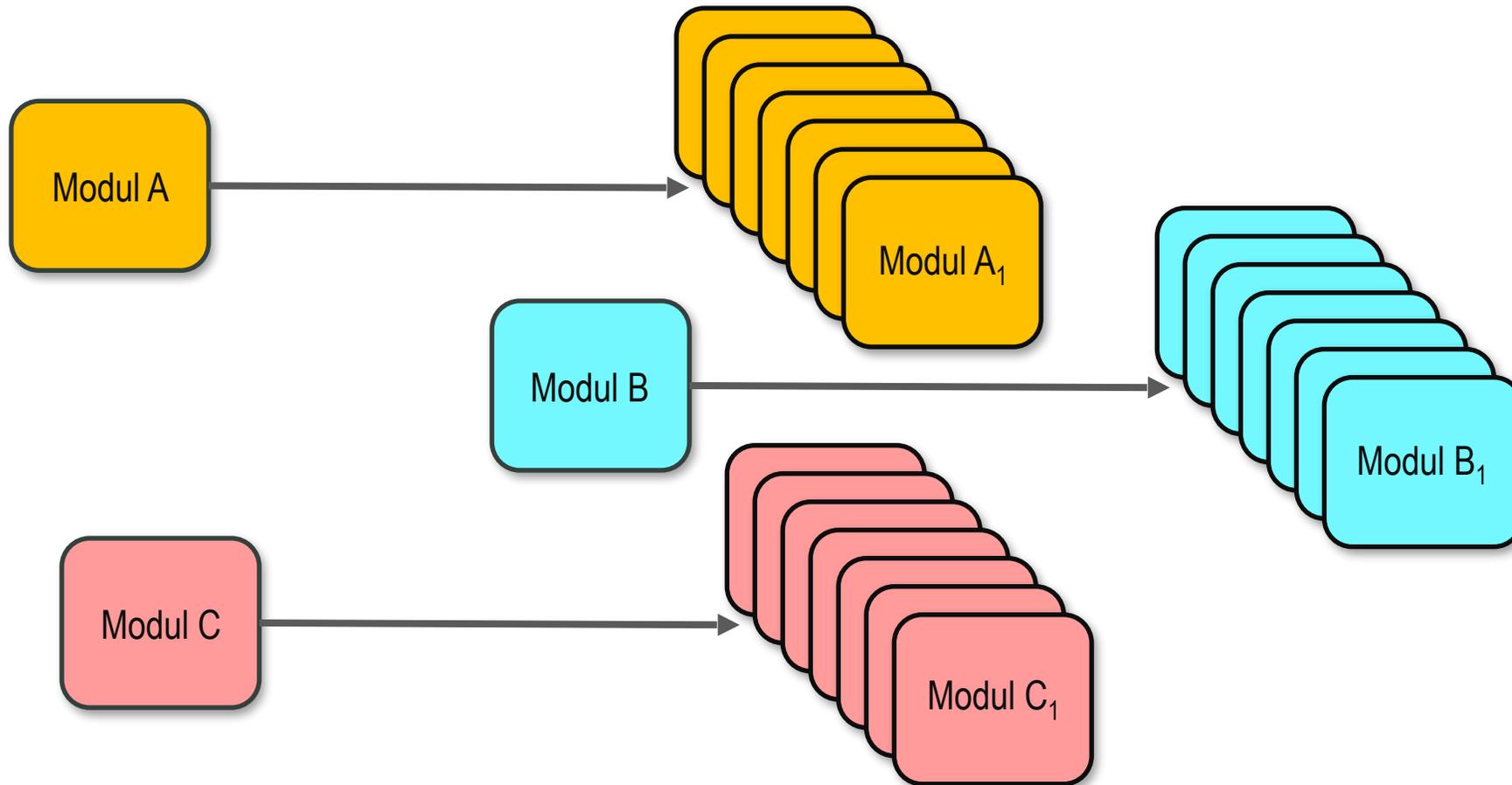
WinAPIOverride64 interface includes:

- Choose Application to Hook:
 - Attach to running process(es) : Enter Process ID, or Drag and Drop the Cross, or use processes list
 - Process ID: []
 - Attach at application startup
 - Application Path: []
 - Command: []
 - Run as: Administrator, Password: []
 - Inject before statically linked dll execution:
 - Inject Only after: 100 ms
 - Stop logging and kill application after: 5000 ms
 - Attach to all new processes
 - Inject into new processes only after: 100 ms
- Modules Filters:
 - Apply to Monitoring, Apply to Overriding
 - Modules Filters: []
 - Use list, Exclusion list (NotHookedModuleList.txt), Inclusion list
 - Only base module
- Table:

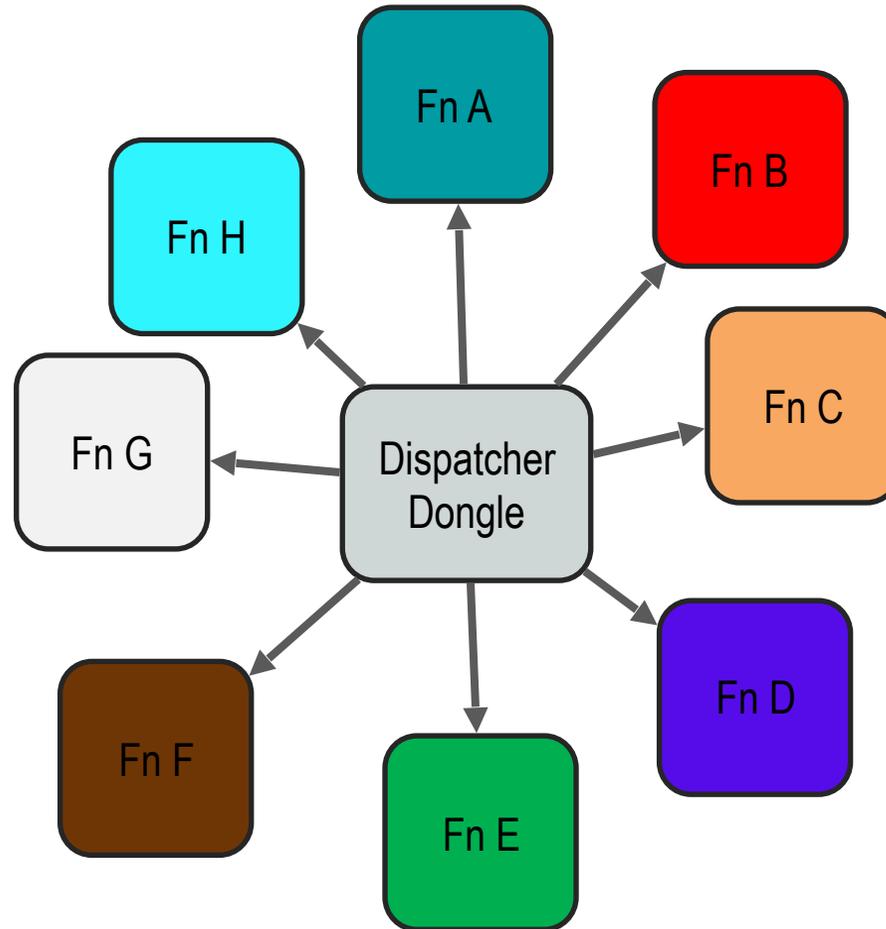
Id	Dir	Call	Ret Value	Caller Addr	Caller Relative Addr	ProcessID	ThreadID	Last Error	Registers Before Call



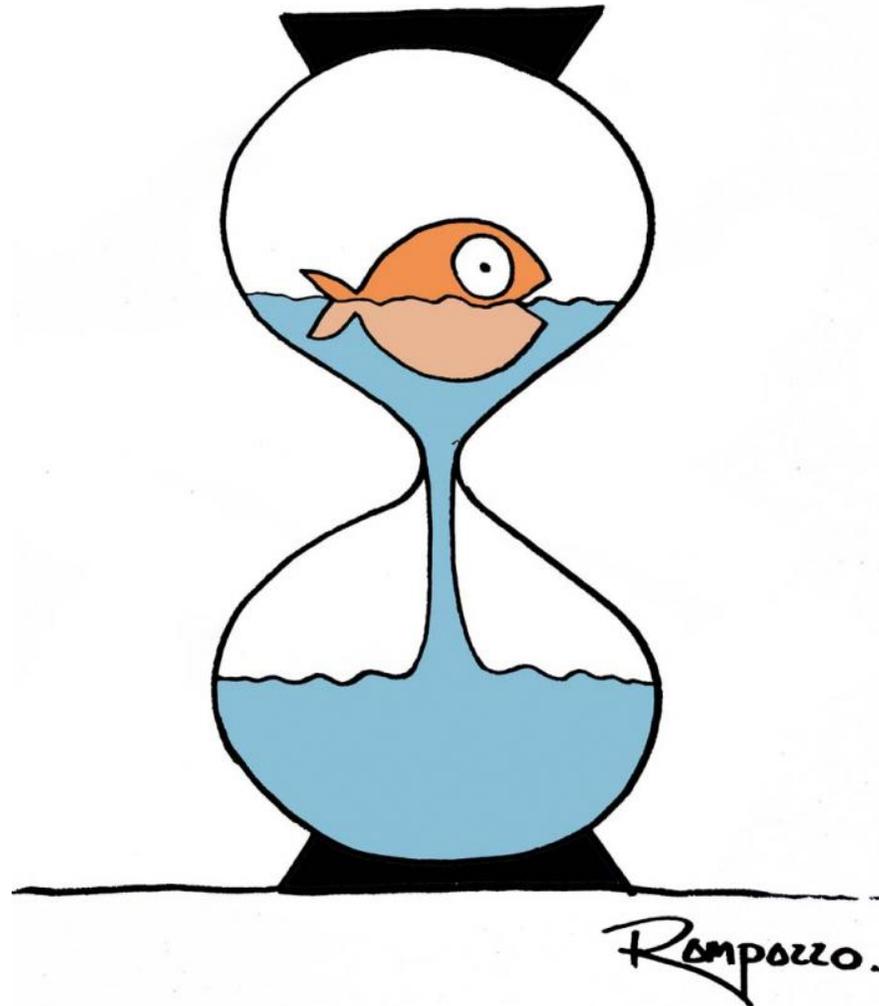
- Sicherheitsanker verwaltet den aktuellen Programmstatus
- Jeder Aufruf an den Anker gibt an von wo nach wo sich der Status ändern darf / muss
- Wildcards möglich
- Wird ein ungültiger Zustandsübergang erkannt, so wird die Lizenz gesperrt



- Ersetzen von Modulen durch eine Vielzahl von Varianten
- Auswahl der Variante über Sicherheitsanker
- Funktional ist die Variante nur lokal gültig
- Die Variante überprüft ob gültige Parameter gegeben







#hackBB