Outro

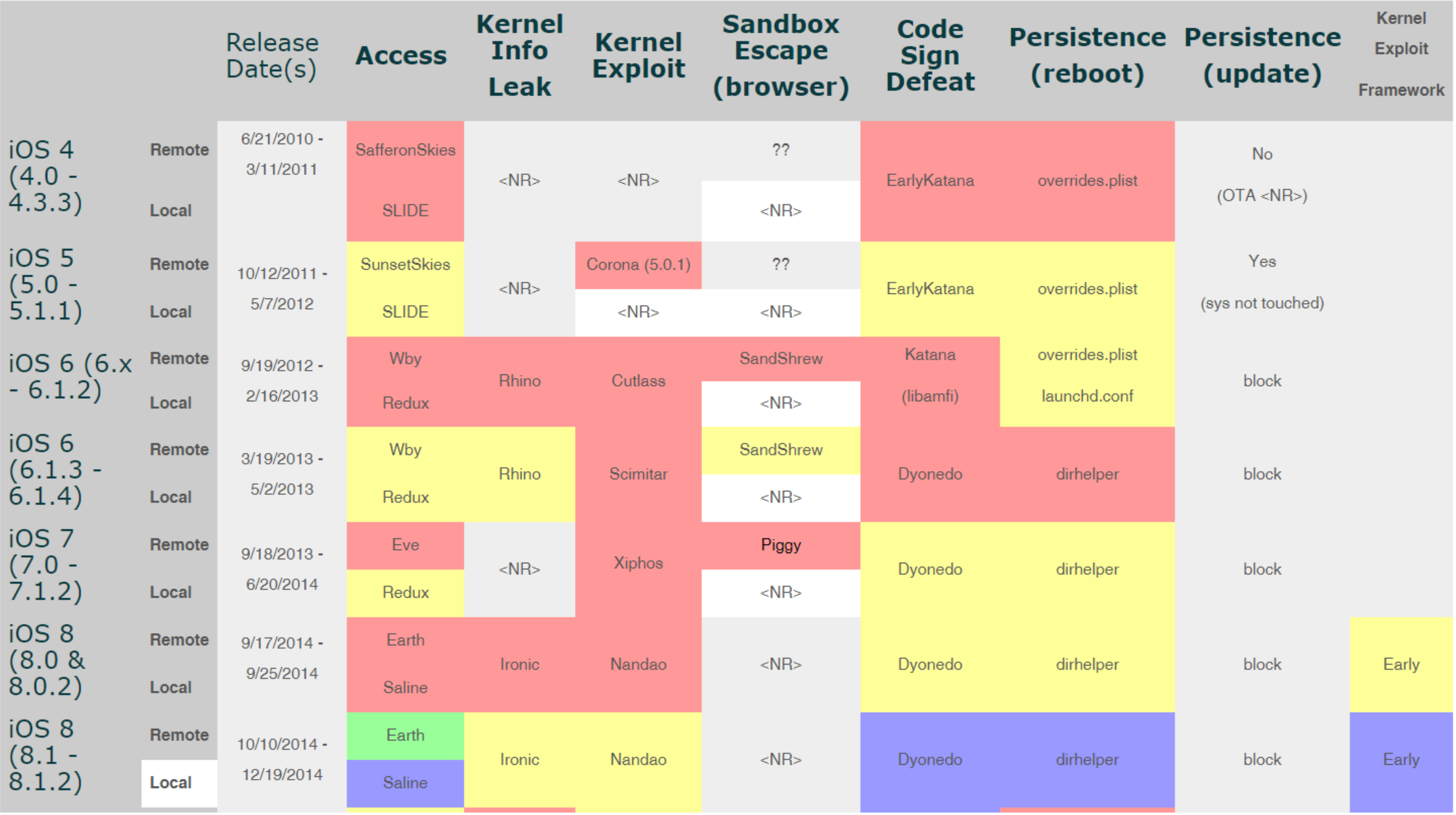
Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

High level overview

CIA Wikileak

CIA iOS Exploits



		Release Date(s)	Access	Kernel Info Leak	Kernel Exploit	Sandbox Escape (browser)	Code Sign Defeat	Persistence (reboot)	Persistence (update)	Kernel Exploit Framework
iOS 4 (4.0 - 4.3.3)	Remote	6/21/2010 - 3/11/2011	SafferonSkies	<NR>	<NR>	??	EarlyKatana	overrides.plist	No (OTA <NR>)	
	Local		SLIDE			<NR>				
iOS 5 (5.0 - 5.1.1)	Remote	10/12/2011 - 5/7/2012	SunsetSkies	<NR>	Corona (5.0.1)	??	EarlyKatana	overrides.plist	Yes (sys not touched)	
	Local		SLIDE		<NR>	<NR>				
iOS 6 (6.x - 6.1.2)	Remote	9/19/2012 - 2/16/2013	Wby	Rhino	Cutlass	SandShrew	Katana (libamfi)	overrides.plist launchd.conf	block	
	Local		Redux			<NR>				
iOS 6 (6.1.3 - 6.1.4)	Remote	3/19/2013 - 5/2/2013	Wby	Rhino	Scimitar	SandShrew	Dyonedo	dirhelper	block	
	Local		Redux			<NR>				
iOS 7 (7.0 - 7.1.2)	Remote	9/18/2013 - 6/20/2014	Eve	<NR>	Xiphos	Piggy	Dyonedo	dirhelper	block	
	Local		Redux			<NR>				
iOS 8 (8.0 & 8.0.2)	Remote	9/17/2014 - 9/25/2014	Earth	Ironic	Nandao	<NR>	Dyonedo	dirhelper	block	Early
	Local		Saline							
iOS 8 (8.1 - 8.1.2)	Remote	10/10/2014 - 12/19/2014	Earth	Ironic	Nandao	<NR>	Dyonedo	dirhelper	block	Early
	Local		Saline							

I'm a Virgin

[but this is an old t shirt]

Outro

My vision:

Detailed Basics

But also

Overview of current situation / State of the Art Exploitation

Outro

Detailed vs. Completeness

Free Speaking vs. Slides as Documentation

Understanding of Details vs. Understanding of Concepts

Self-Thinking vs. Step-by-Step description

Hands-On practice vs. Theory

Incremental Building Steps vs. Goal-Driven Explanation

Outro

Detailed vs. Completeness

Free Speaking vs. Slides as Documentation

Understanding of Details vs. Understanding of Concepts

Self-Thinking vs. Step-by-Step description

Hands-On practice vs. Theory

Incremental Building Steps vs. Goal-Driven Explanation

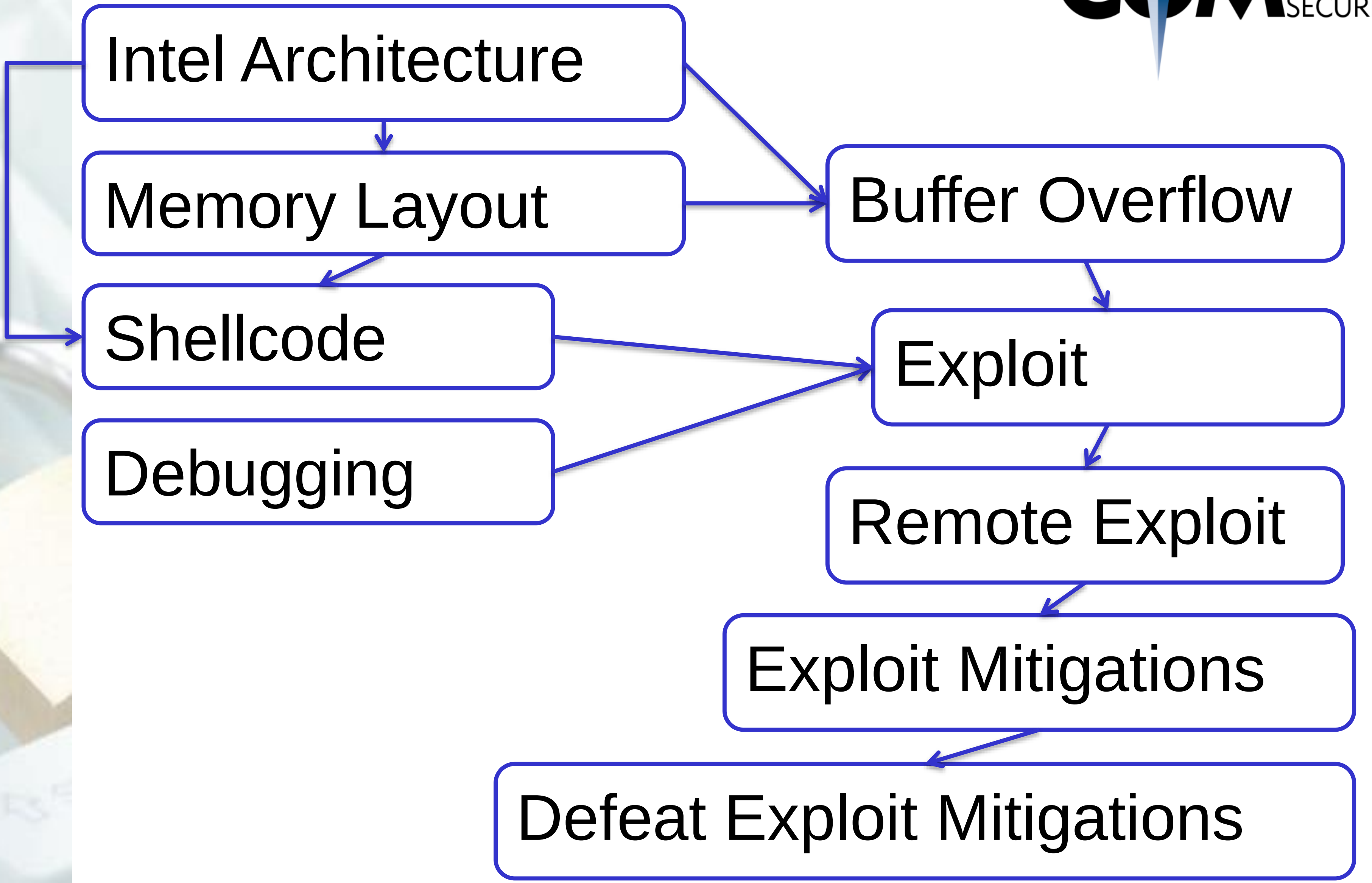
Getting lost in slides... Not enough time

Questions

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Content



Intel Architecture

Memory Layout

Shellcode

Debugging

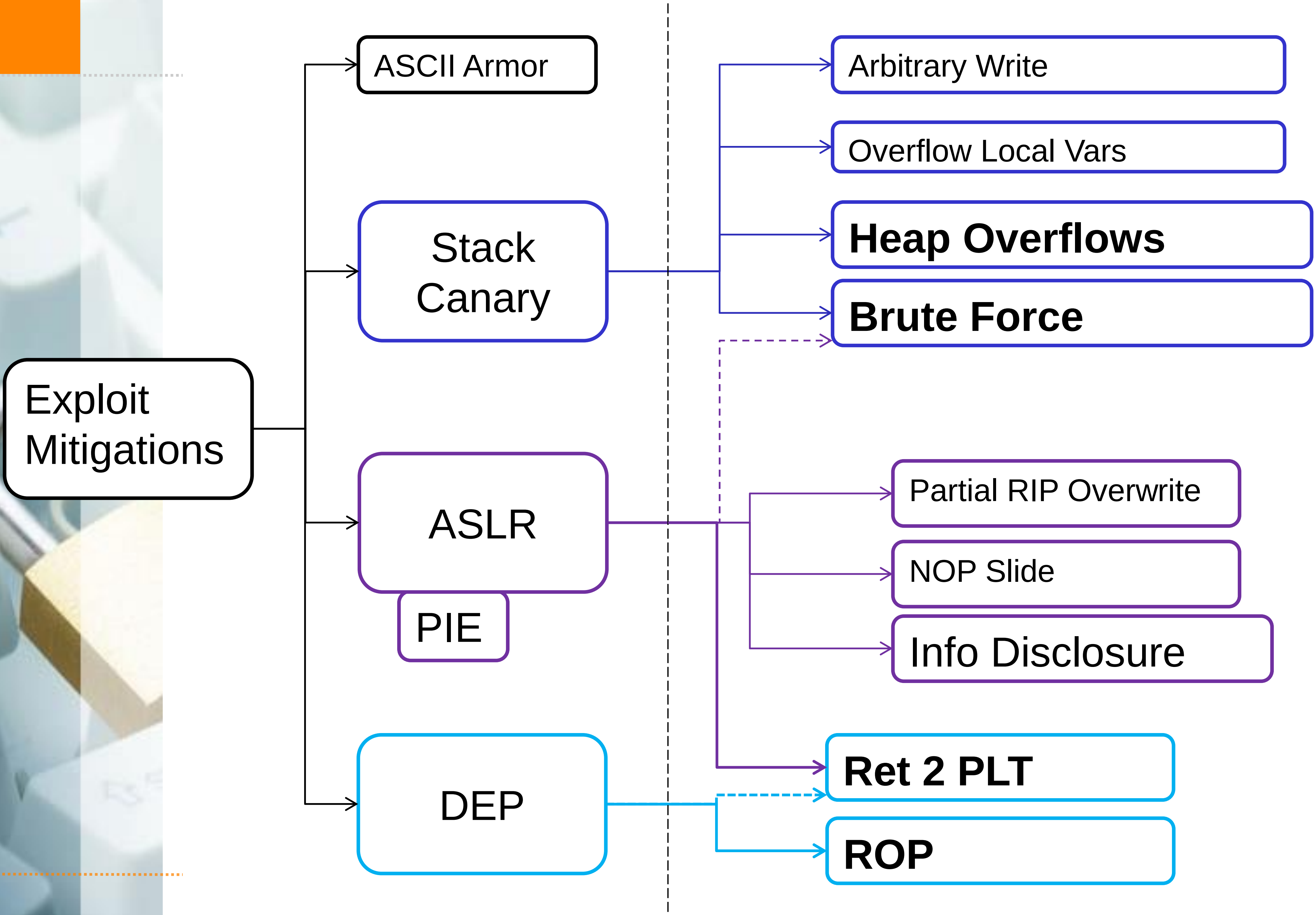
Buffer Overflow

Exploit

Remote Exploit

Exploit Mitigations

Defeat Exploit Mitigations



Exploit Mitigations

ASCII Armor

Stack Canary

ASLR

PIE

DEP

Arbitrary Write

Overflow Local Vars

Heap Overflows

Brute Force

Partial RIP Overwrite

NOP Slide

Info Disclosure

Ret 2 PLT

ROP

Questions

Was gibt es für Anti-Exploit Mechanismen?

- DEP
- ASLR
- Stack Canary

Erzähl mir was über Anti-Exploit Mechanism [X]

- Gegen welchen Teil eines Exploits schützt es?
- Wie funktioniert er?
- Ist der Mechanismus effektiv?
  - Wann nicht?
  - Warum nicht?
- Wird der Mechanismus eingesetzt (Default, Linux, Windows)?