SoK: 20 Years of Power, Privilege & Peril in x86 System Management Mode



Antonis Louka · **Jo Van Bulck**

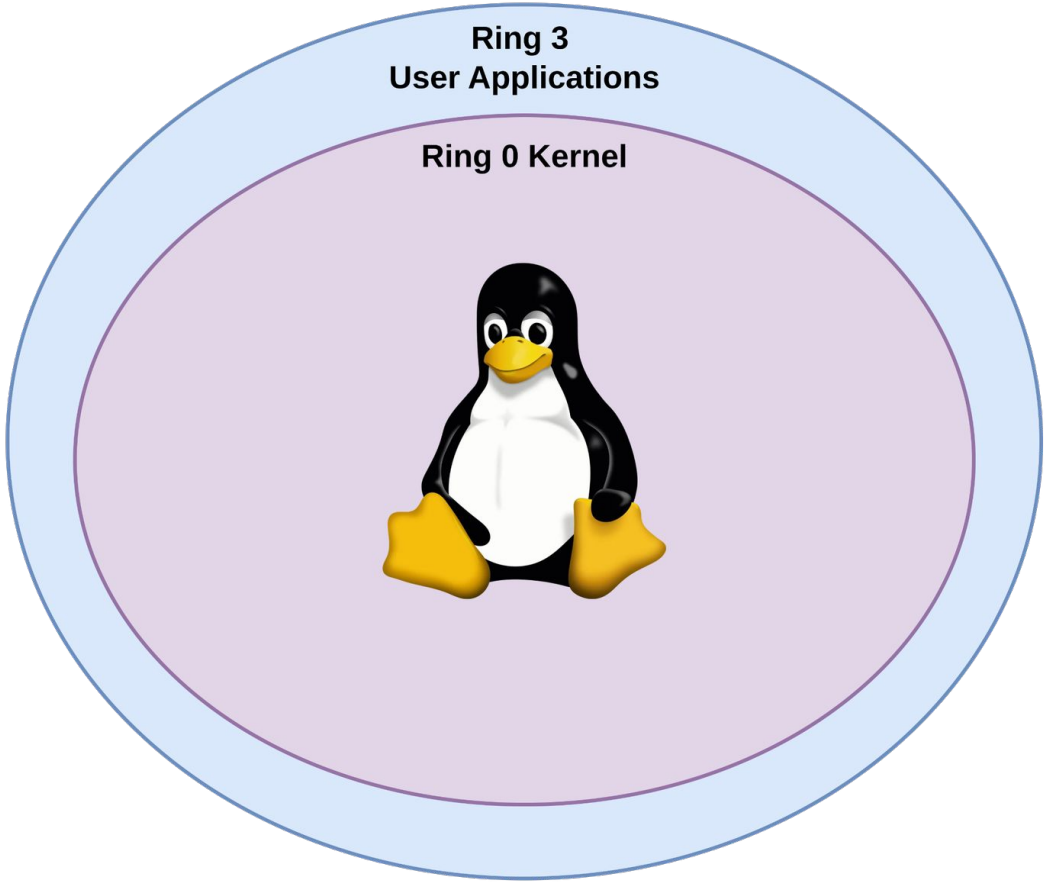
DistriNet, KU Leuven

WOOT '26 | August 2026

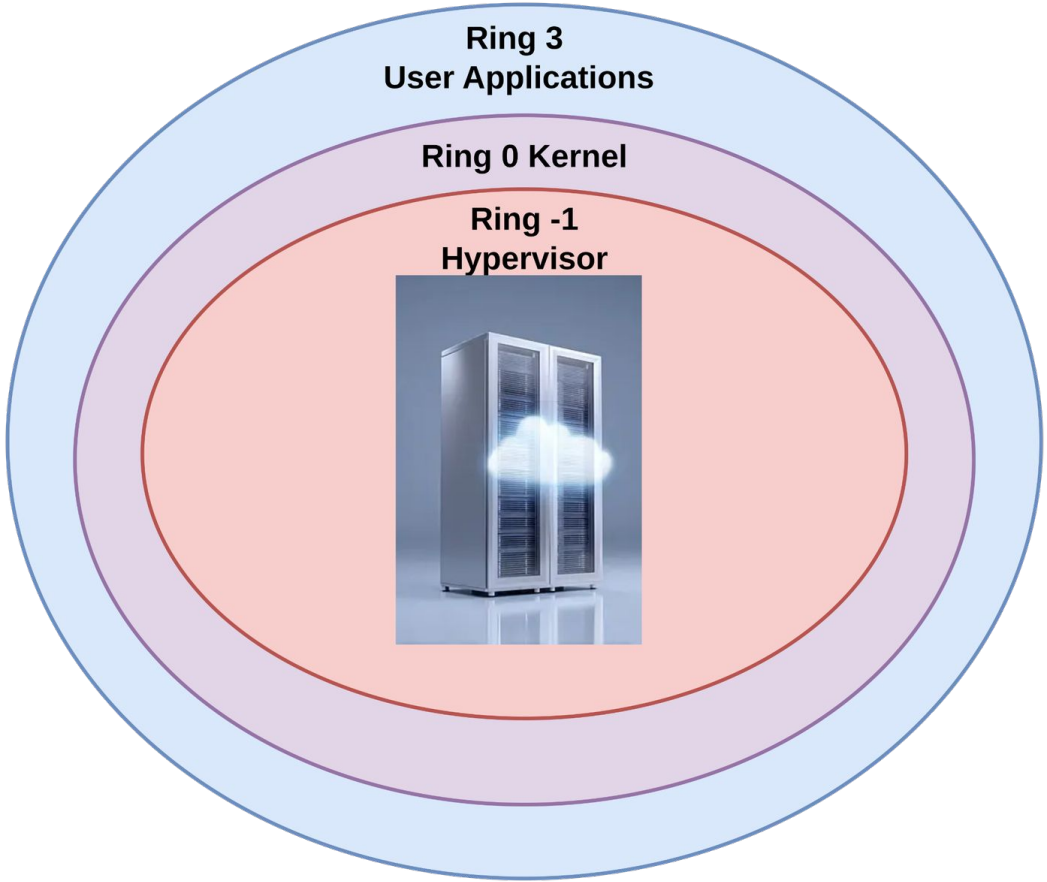
DistriNet KU LEUVEN


RINGS
AND
CPUS?

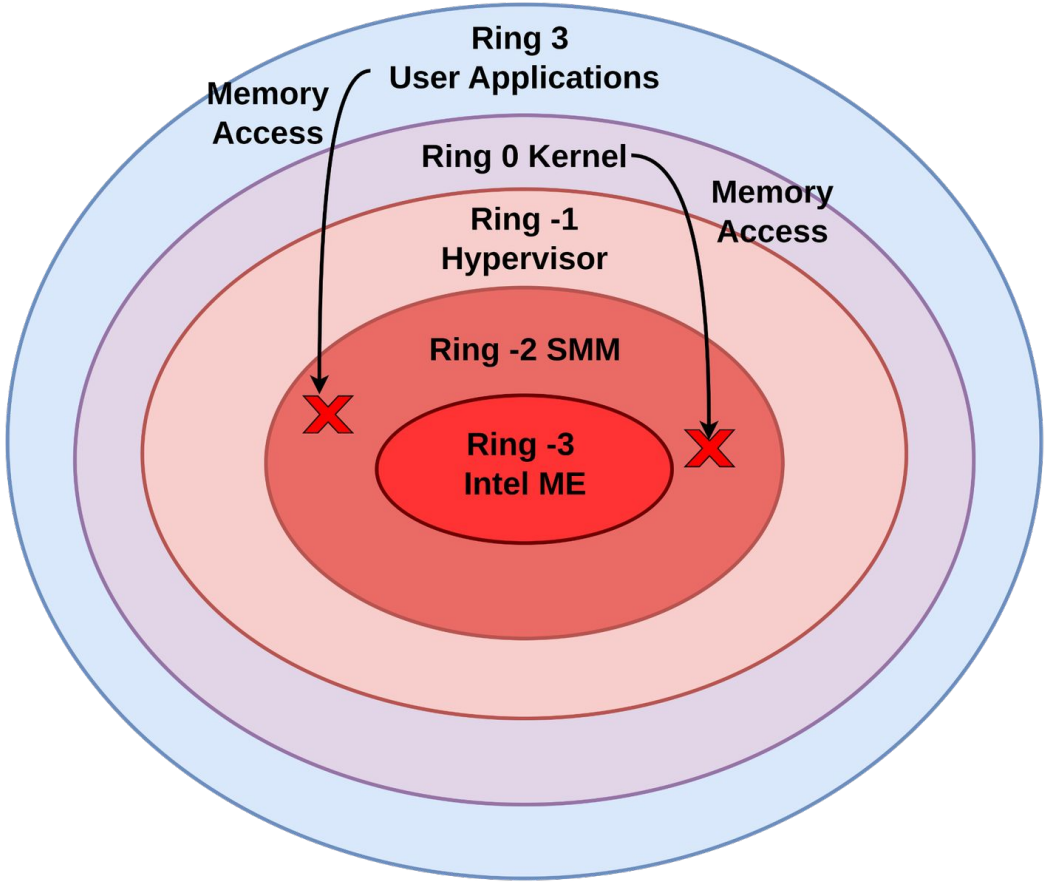
Privilege Rings on x86



Privilege Rings on x86: Ring −1

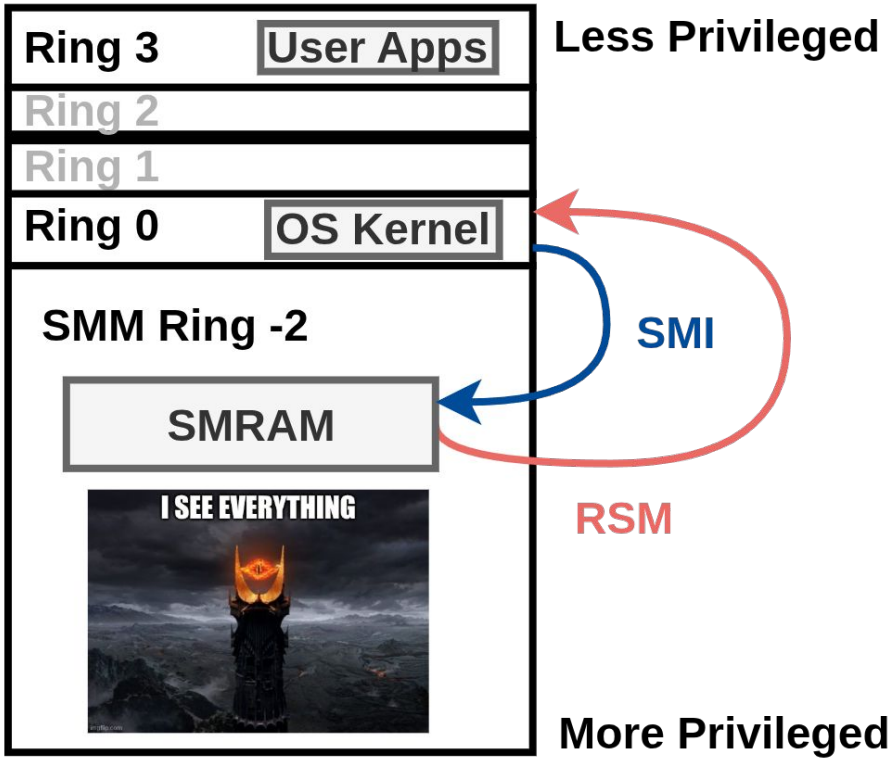


Privilege Rings on x86: Ring −2: SMM




I SEE EVERYTHING
imgflip.com

Interrupt-driven Mode Transparent to the OS



- Entered exclusively via an interrupt (SMI)
- Exit via a dedicated instruction (RSM)
- Dedicated SMRAM region

SMM in Real-World Applications



BIOS variables

Data for critical functions and platform configuration



Suspend to memory

The S3 resume path restores platform state



Secure boot

Enforcing that only trusted software runs



Capsule updates

The secure firmware update flow

SMM in the Wild

The SMM Rootkit Revisited: Fun with USB

Attacking Intel® BIOS

(TS//SI//REL) BERSERKR is a persistent backdoor that is implanted into the BIOS and runs from SMM. Although the core of the code is stable, there are always new requirements against which to develop. This includes new

[edit] (U//FOUO) GOPHERRAGE

(TS//SI//REL) GOPHERRAGE is a project that seeks to develop a hypervisor implant that would leverage both AMD and Intel's virtualization technology in order to provide both DNT implant persistence capabilities and a persistent back door.

(TS//SI//REL) Develop a hypervisor implant that would leverage both Intel's and AMDs virtualization technology in order to provide both DNT implant persistence capabilities and a persistent back door access. The idea would be similar to what BERSERKR can do from SMM in that it should be able to use

SECRET//COMINT//REL TO USA, FVEY

DEITYBOUNCE

ANT Product Data

(TS//SI//REL) DEITYBOUNCE provides software application persistence on Dell PowerEdge servers by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to gain periodic execution while the Operating System loads.

06/20/08

IRONCHEF

ANT Product Data

(TS//SI//REL) IRONCHEF provides access persistence to target systems by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to communicate with a hardware implant that provides two-way RF communication.

07/14/08

SMM Rootkits:

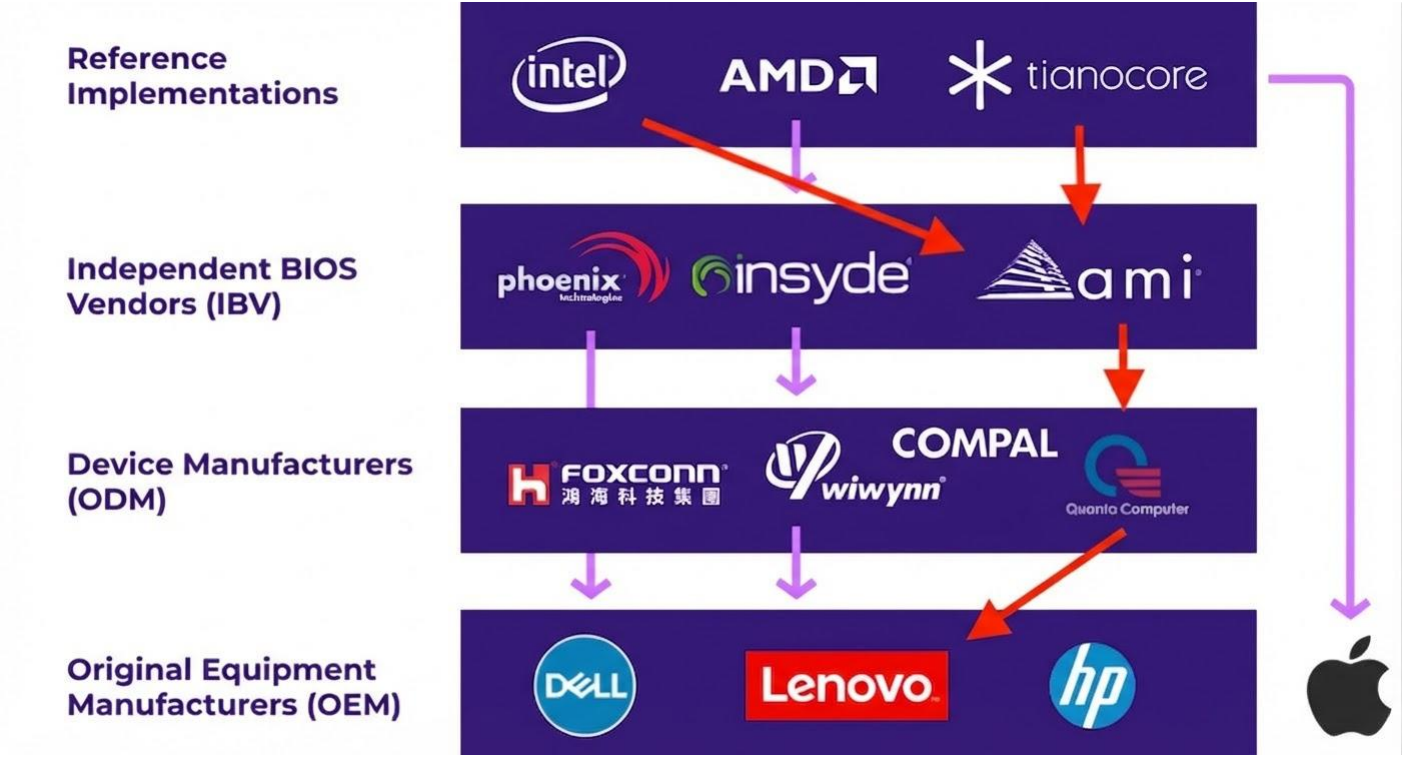
A New Breed of OS Independent Malware

Using CPU System Management Mode to Circumvent Operating System Security Functions

Attacking Intel® Trusted Execution Technology

Firmware and SMM Ecosystem

Source: [Binarly — Firmware supply chain security is broken: can we fix it?]



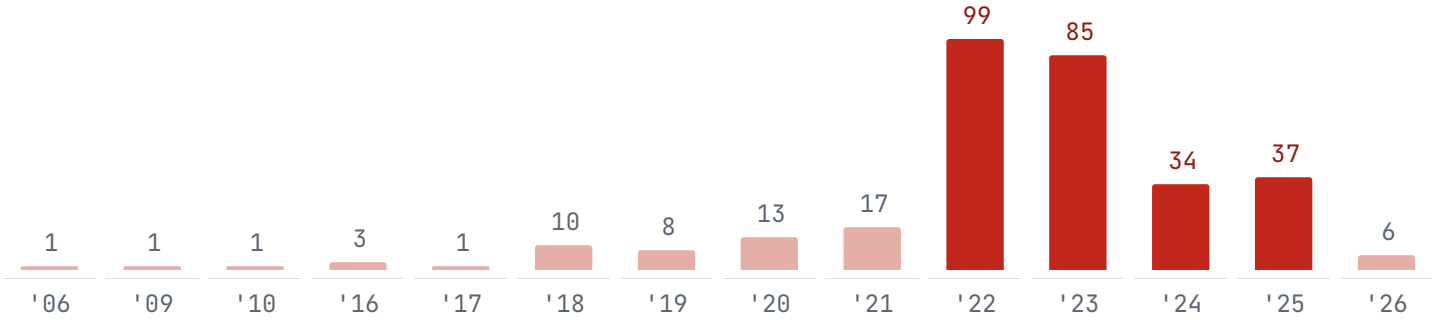
Need for Systematization of the SMM Landscape

Scattered across papers, talks, blogs and advisories

THIRTY YEARS OF SMM EVOLUTION

SMM Change	Era	Description	HW	FW
Baseline SMM	1990s (Intel i386SL)	SMI/RSM, SMRAM, and state save/restore	●	○
SMRAMC & SMM locking	Mid—late 1990s (i486)	Chipset-controlled SMRAM & relocatable SMBASE	●	○
CPU SMRAM isolation	Early—mid 2000s	SMRR SMRAM protection (CPU-enforced)	●	○
Expanded state save map	Mid-2000s (x86—64 era)	Extended SMRAM save-state formats for 64-bit CPUs	●	○
SMM-SMEP	2014 (Haswell)	Mitigations against SMM callouts	●	○
Intel STM	~2015	Deprivilege SMI handlers	●	●
SMM paging in EDK II	2016	Static SMM page tables with defensive memory attributes	○	●
Runtime BIOS Resilience	2018 (Intel 8th Gen)	Paging setup, long mode and lockdown	○	●
System Security Report	2019 (Intel 9th Gen)	OS-visible reporting of below-the-OS security properties	○	●
System Resources Defense	2020 (Intel 10th Gen)	Policy-based containment and deprivileging SMI handlers	●	●
AMD SMM Supervisor	2022	Deprivileging and policy mediation for SMI handlers	●	●

CVE INSTANCES BY YEAR PUBLISHED



69
STUDIES REVIEWED

57
SECURITY ADVISORIES

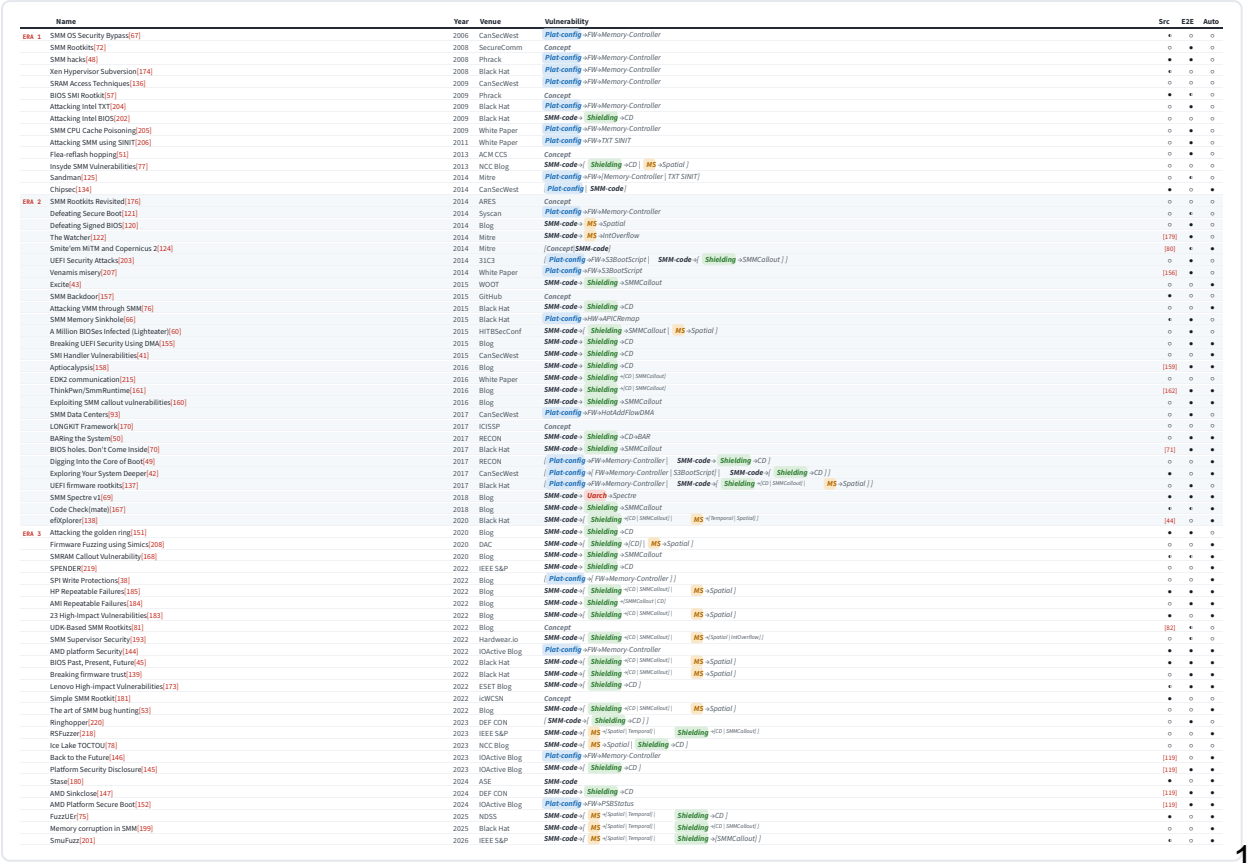
319
CVE INSTANCES

2006–26
COVERAGE


ATTACKERS
YOU SHALL NOT PASS
CPU VENDORS

Two-fold Systematization

- AXIS 1 · VULNERABILITY ANALYSIS
- AXIS 2 · LONGITUDINAL ANALYSIS



	Name	Year	Venue	Vulnerability	Src	E2E	Auto
ERA 1	SMM OS Security Bypass[67]	2006	CanSecWest	Plat-config ⇒FW⇒Memory-Controller	◐	○	○
	SMM Rootkits[72]	2008	SecureComm	Concept	○	●	○
	SMM hacks[48]	2008	Phrack	Plat-config ⇒FW⇒Memory-Controller	●	●	○
	Xen Hypervisor Subversion[174]	2008	Black Hat	Plat-config ⇒FW⇒Memory-Controller	◐	○	○
	SRAM Access Techniques[136]	2009	CanSecWest	Plat-config ⇒FW⇒Memory-Controller	○	○	○
	BIOS SMI Rootkit[57]	2009	Phrack	Concept	●	◐	○
	Attacking Intel TXT[204]	2009	Black Hat	Plat-config ⇒FW⇒Memory-Controller	○	●	○
	Attacking Intel BIOS[202]	2009	Black Hat	SMM-code ⇒ Shielding ⇒CD	○	○	○
	SMM CPU Cache Poisoning[205]	2009	White Paper	Plat-config ⇒FW⇒Memory-Controller	○	●	○
	Attacking SMM using SINIT[206]	2011	White Paper	Plat-config ⇒FW⇒TXT SINIT	○	●	○
	Flea-reflash hopping[51]	2013	ACM CCS	Concept	○	●	○
	Insyde SMM Vulnerabilities[77]	2013	NCC Blog	SMM-code ⇒[Shielding ⇒CD | MS ⇒Spatial]	○	○	○
	Sandman[125]	2014	Mitre	Plat-config ⇒FW⇒[Memory-Controller | TXT SINIT]	○	◐	○
	Chipsec[134]	2014	CanSecWest	Plat-config | SMM-code]	●	○	●
ERA 2	SMM Rootkits Revisited[176]	2014	ARES	Concept	○	○	○
	Defeating Secure Boot[121]	2014	Syscan	Plat-config ⇒FW⇒Memory-Controller	○	◐	○
	Defeating Signed BIOS[120]	2014	Blog	SMM-code ⇒ MS ⇒Spatial	○	●	○
	The Watcher[122]	2014	Mitre	SMM-code ⇒ MS ⇒IntOverflow	[179]	●	○
	Smite'em MiTM and Copernicus 2[124]	2014	Mitre	[Concept;SMM-code]	[80]	◐	●
	UEFI Security Attacks[203]	2014	31C3	[Plat-config ⇒FW⇒S3BootScript | SMM-code ⇒[Shielding ⇒SMMCallout]]	○	●	○
	Venamis misery[207]	2014	White Paper	Plat-config ⇒FW⇒S3BootScript	[156]	●	○
	Excite[43]	2015	WOOT	SMM-code ⇒ Shielding ⇒SMMCallout	○	○	●
	SMM Backdoor[157]	2015	GitHub	Concept	●	○	○
	Attacking VMM through SMM[76]	2015	Black Hat	SMM-code ⇒ Shielding ⇒CD	○	○	●
	SMM Memory Sinkhole[66]	2015	Black Hat	Plat-config ⇒HW⇒APICRemap	◐	●	○
	A Million BIOSes Infected (Lighteater)[60]	2015	HITBSecConf	SMM-code ⇒[Shielding ⇒SMMCallout | MS ⇒Spatial]	○	●	○
	Breaking UEFI Security Using DMA[155]	2015	Blog	SMM-code ⇒ Shielding ⇒CD	○	●	●
	SMI Handler Vulnerabilities[41]	2015	CanSecWest	SMM-code ⇒ Shielding ⇒CD	○	○	●
	Aptiocalypsis[158]	2016	Blog	SMM-code ⇒ Shielding ⇒CD	[159]	●	●
	EDK2 communication[215]	2016	White Paper	SMM-code ⇒ Shielding ⇒[CD | SMMCallout]	○	○	○
	ThinkPwn/SmmRuntime[161]	2016	Blog	SMM-code ⇒ Shielding ⇒[CD | SMMCallout]	[162]	●	●
	Exploiting SMM callout vulnerabilities[160]	2016	Blog	SMM-code ⇒ Shielding ⇒SMMCallout	○	●	●
	SMM Data Centers[93]	2017	CanSecWest	Plat-config ⇒FW⇒HotAddFlowDMA	○	●	○
	LONGKIT Framework[170]	2017	ICISSP	Concept	○	○	○
	BARing the System[50]	2017	RECON	SMM-code ⇒ Shielding ⇒CD⇒BAR	○	●	●
	BIOS holes. Don't Come Inside[70]	2017	Black Hat	SMM-code ⇒ Shielding ⇒SMMCallout	[71]	●	●
	Digging Into the Core of Boot[49]	2017	RECON	[Plat-config ⇒FW⇒Memory-Controller | SMM-code ⇒ Shielding ⇒CD]	○	○	●
	Exploring Your System Deeper[42]	2017	CanSecWest	[Plat-config ⇒[FW⇒Memory-Controller | S3BootScript] | SMM-code ⇒[Shielding ⇒CD]]	●	○	●
	UEFI firmware rootkits[137]	2017	Black Hat	[Plat-config ⇒FW⇒Memory-Controller | SMM-code ⇒[Shielding ⇒[CD | SMMCallout] | MS ⇒Spatial]]	○	●	○
	SMM Spectre v1[69]	2018	Blog	SMM-code ⇒ Uarch ⇒Spectre	●	●	●
	Code Check(mate)[167]	2018	Blog	SMM-code ⇒ Shielding ⇒SMMCallout	◐	◐	●
	efiXplorer[138]	2020	Black Hat	SMM-code ⇒[Shielding ⇒[CD | SMMCallout] | MS ⇒[Temporal | Spatial]]	[44]	○	●
ERA 3	Attacking the golden ring[151]	2020	Blog	SMM-code ⇒ Shielding ⇒CD	●	●	○
	Firmware Fuzzing using Simics[208]	2020	DAC	SMM-code ⇒[Shielding ⇒[CD] | MS ⇒Spatial]	○	○	●
	SMRAM Callout Vulnerability[168]	2020	Blog	SMM-code ⇒ Shielding ⇒SMMCallout	◐	◐	●
	SPENDER[219]	2022	IEEE S&P	SMM-code ⇒ Shielding ⇒CD	○	○	●
	SPI Write Protections[38]	2022	Blog	[Plat-config ⇒[FW⇒Memory-Controller]]	○	○	●
	HP Repeatable Failures[185]	2022	Blog	SMM-code ⇒[Shielding ⇒[CD | SMMCallout] | MS ⇒Spatial]	●	●	●
	AMI Repeatable Failures[184]	2022	Blog	SMM-code ⇒[Shielding ⇒[SMMCallout | CD]]	○	●	●
	23 High-Impact Vulnerabilities[183]	2022	Blog	SMM-code ⇒[Shielding ⇒[CD | SMMCallout] | MS ⇒Spatial]	●	○	●
	UDK-Based SMM Rootkits[81]	2022	Blog	Concept	[82]	◐	○
	SMM Supervisor Security[193]	2022	Hardwear.io	SMM-code ⇒[Shielding ⇒[CD | SMMCallout] | MS ⇒[Spatial | IntOverflow]]	○	◐	○
	AMD platform Security[144]	2022	IOActive Blog	Plat-config ⇒FW⇒Memory-Controller	●	●	●
	BIOS Past, Present, Future[45]	2022	Black Hat	SMM-code ⇒[Shielding ⇒[CD | SMMCallout] | MS ⇒Spatial]	●	●	●
	Breaking firmware trust[139]	2022	Black Hat	SMM-code ⇒[Shielding ⇒[CD | SMMCallout] | MS ⇒Spatial]	○	●	●
	Lenovo High-impact Vulnerabilities[173]	2022	ESET Blog	SMM-code ⇒[Shielding ⇒CD]	●	●	●
	Simple SMM Rootkit[181]	2022	icWCSN	Concept	●	○	○
	The art of SMM bug hunting[53]	2022	Blog	SMM-code ⇒[Shielding ⇒[CD | SMMCallout] | MS ⇒Spatial]	○	○	●
	Ringhopper[220]	2023	DEF CON	[SMM-code ⇒[Shielding ⇒CD]]	○	●	○
	RSFuzzer[218]	2023	IEEE S&P	SMM-code ⇒[MS ⇒[Spatial | Temporal] | Shielding ⇒[CD | SMMCallout]]	○	○	●
	Ice Lake TOCTOU[78]	2023	NCC Blog	SMM-code ⇒[MS ⇒Spatial | Shielding ⇒CD]	○	○	○
	Back to the Future[146]	2023	IOActive Blog	Plat-config ⇒FW⇒Memory-Controller	[119]	●	●
	Platform Security Disclosure[145]	2023	IOActive Blog	SMM-code ⇒[Shielding ⇒CD]	[119]	●	●
	Stase[180]	2024	ASE	SMM-code	●	○	●
	AMD Sinkclose[147]	2024	DEF CON	SMM-code ⇒ Shielding ⇒CD	[119]	●	●
	AMD Platform Secure Boot[152]	2024	IOActive Blog	Plat-config ⇒FW⇒PSBStatus	[119]	●	●
	FuzzUEr[75]	2025	NDSS	SMM-code ⇒[MS ⇒[Spatial | Temporal] | Shielding ⇒CD]	●	○	●
	Memory corruption in SMM[199]	2025	Black Hat	SMM-code ⇒[MS ⇒[Spatial | Temporal] | Shielding ⇒[CD | SMMCallout]]	○	○	●
	SmuFuzz[201]	2026	IEEE S&P	SMM-code ⇒[MS ⇒[Spatial | Temporal] | Shielding ⇒[SMMCallout]]	◐	○	●

Two-fold Systematization

AXIS 1 · VULNERABILITY ANALYSIS

Every entry carries a label/path through a classification tree

AXIS 2 · LONGITUDINAL ANALYSIS

	Name	Year	Venue	Vulnerability	Src	E2E	Auto
ERA 1	SMM OS Security Bypass[67]	2006	CanSecWest	Plat-config ▫FW▫Memory-Controller	●	○	○
	SMM Rootkits[72]	2008	SecureComm	Concept	○	●	○
	SMM hacks[48]	2008	Phrack	Plat-config ▫FW▫Memory-Controller	●	●	○
	Xen Hypervisor Subversion[174]	2008	Black Hat	Plat-config ▫FW▫Memory-Controller	●	○	○
	SRAM Access Techniques[136]	2009	CanSecWest	Plat-config ▫FW▫Memory-Controller	○	○	○
	BIOS SMI Rootkit[57]	2009	Phrack	Concept	●	◐	○
	Attacking Intel TXT[204]	2009	Black Hat	Plat-config ▫FW▫Memory-Controller	○	●	○
	Attacking Intel BIOS[202]	2009	Black Hat	SMM-code ▫ Shielding ▫CD	○	○	○
	SMM CPU Cache Poisoning[205]	2009	White Paper	Plat-config ▫FW▫Memory-Controller	○	●	○
	Attacking SMM using SINIT[206]	2011	White Paper	Plat-config ▫FW▫TXT SINIT	○	●	○
	Flea-reflash hopping[51]	2013	ACM CCS	Concept	○	●	○
	Insyde SMM Vulnerabilities[77]	2013	NCC Blog	SMM-code ▫[Shielding ▫CD | MS ▫Spatial]	○	○	○
	Sandman[125]	2014	Mitre	Plat-config ▫FW▫[Memory-Controller | TXT SINIT]	○	◐	○
	Chipsec[134]	2014	CanSecWest	Plat-config | SMM-code]	●	○	●
ERA 2	SMM Rootkits Revisited[176]	2014	ARES	Concept	○	○	○
	Defeating Secure Boot[121]	2014	Syscan	Plat-config ▫FW▫Memory-Controller	○	◐	○
	Defeating Signed BIOS[120]	2014	Blog	SMM-code ▫ MS ▫Spatial	○	●	○
	The Watcher[122]	2014	Mitre	SMM-code ▫ MS ▫IntOverflow	[179]	●	○
	Smite'em MiTM and Copernicus 2[124]	2014	Mitre	[Concept|SMM-code]	[80]	◐	●
	UEFI Security Attacks[203]	2014	31C3	[Plat-config ▫FW▫S3BootScript | SMM-code ▫[Shielding ▫SMMCallout]]	○	●	○
	Venamis misery[207]	2014	White Paper	Plat-config ▫FW▫S3BootScript	[156]	●	○
	Excite[43]	2015	WOOT	SMM-code ▫ Shielding ▫SMMCallout	○	○	●
	SMM Backdoor[157]	2015	GitHub	Concept	●	○	○
	Attacking VMM through SMM[76]	2015	Black Hat	SMM-code ▫ Shielding ▫CD	○	○	●
	SMM Memory Sinkhole[66]	2015	Black Hat	Plat-config ▫HW▫APICRemap	◐	●	○
	A Million BIOSes Infected (Lighteater)[60]	2015	HITBSecConf	SMM-code ▫[Shielding ▫SMMCallout | MS ▫Spatial]	○	●	○
	Breaking UEFI Security Using DMA[155]	2015	Blog	SMM-code ▫ Shielding ▫CD	○	●	●
	SMI Handler Vulnerabilities[41]	2015	CanSecWest	SMM-code ▫ Shielding ▫CD	○	○	●
	Aptiocalypsis[158]	2016	Blog	SMM-code ▫ Shielding ▫CD	[159]	●	●
	EDK2 communication[215]	2016	White Paper	SMM-code ▫[Shielding ▫[CD | SMMCallout]	○	○	○
	ThinkPwn/SmmRuntime[161]	2016	Blog	SMM-code ▫ Shielding ▫[CD | SMMCallout]	[162]	●	●
	Exploiting SMM callout vulnerabilities[160]	2016	Blog	SMM-code ▫ Shielding ▫SMMCallout	○	●	●
	SMM Data Centers[93]	2017	CanSecWest	Plat-config ▫FW▫HotAddFlowDMA	○	●	○
	LONGKIT Framework[170]	2017	ICISSP	Concept	○	○	○
	BARing the System[50]	2017	RECON	SMM-code ▫ Shielding ▫CD▫BAR	○	●	●
	BIOS holes. Don't Come Inside[70]	2017	Black Hat	SMM-code ▫ Shielding ▫SMMCallout	[71]	●	●
	Digging Into the Core of Boot[49]	2017	RECON	[Plat-config ▫FW▫Memory-Controller | SMM-code ▫ Shielding ▫CD]	○	○	●
	Exploring Your System Deeper[42]	2017	CanSecWest	[Plat-config ▫[FW▫Memory-Controller | S3BootScript] | SMM-code ▫[Shielding ▫CD]]	●	○	●
	UEFI firmware rootkits[137]	2017	Black Hat	[Plat-config ▫FW▫Memory-Controller | SMM-code ▫[Shielding ▫[CD | SMMCallout] | MS ▫Spatial]]	○	●	○
	SMM Spectre v1[69]	2018	Blog	SMM-code ▫ Uarch ▫Spectre	●	●	●
	Code Check(mate)[167]	2018	Blog	SMM-code ▫ Shielding ▫SMMCallout	◐	◐	●
	efiXplorer[138]	2020	Black Hat	SMM-code ▫[Shielding ▫[CD | SMMCallout] | MS ▫[Temporal | Spatial]]	[44]	○	●
ERA 3	Attacking the golden ring[151]	2020	Blog	SMM-code ▫ Shielding ▫CD	●	●	○
	Firmware Fuzzing using Simics[208]	2020	DAC	SMM-code ▫[Shielding ▫[CD] | MS ▫Spatial]	○	○	●
	SMRAM Callout Vulnerability[168]	2020	Blog	SMM-code ▫ Shielding ▫SMMCallout	◐	◐	●
	SPENDER[219]	2022	IEEE S&P	SMM-code ▫ Shielding ▫CD	○	○	●
	SPI Write Protections[38]	2022	Blog	[Plat-config ▫[FW▫Memory-Controller]]	○	○	●
	HP Repeatable Failures[185]	2022	Blog	SMM-code ▫[Shielding ▫[CD | SMMCallout] | MS ▫Spatial]	●	●	●
	AMI Repeatable Failures[184]	2022	Blog	SMM-code ▫[Shielding ▫[SMMCallout | CD]	○	●	●
	23 High-Impact Vulnerabilities[183]	2022	Blog	SMM-code ▫[Shielding ▫[CD | SMMCallout] | MS ▫Spatial]	●	○	●
	UDK-Based SMM Rootkits[81]	2022	Blog	Concept	[82]	◐	○
	SMM Supervisor Security[193]	2022	Hardwear.io	SMM-code ▫[Shielding ▫[CD | SMMCallout] | MS ▫[Spatial | IntOverflow]]	○	◐	○
	AMD platform Security[144]	2022	IOActive Blog	Plat-config ▫FW▫Memory-Controller	●	●	●
	BIOS Past, Present, Future[45]	2022	Black Hat	SMM-code ▫[Shielding ▫[CD | SMMCallout] | MS ▫Spatial]	●	●	●
	Breaking firmware trust[139]	2022	Black Hat	SMM-code ▫[Shielding ▫[CD | SMMCallout] | MS ▫Spatial]	○	●	●
	Lenovo High-impact Vulnerabilities[173]	2022	ESET Blog	SMM-code ▫[Shielding ▫CD]	●	●	●
	Simple SMM Rootkit[181]	2022	icWCSN	Concept	●	○	○
	The art of SMM bug hunting[53]	2022	Blog	SMM-code ▫[Shielding ▫[CD | SMMCallout] | MS ▫Spatial]	○	○	●
	Ringhopper[220]	2023	DEF CON	[SMM-code ▫[Shielding ▫CD]]	○	●	○
	RSFuzzer[218]	2023	IEEE S&P	SMM-code ▫[MS ▫[Spatial | Temporal] | Shielding ▫[CD | SMMCallout]]	○	○	●
	Ice Lake TOCTOU[78]	2023	NCC Blog	SMM-code ▫[MS ▫Spatial | Shielding ▫CD]	○	○	○
	Back to the Future[146]	2023	IOActive Blog	Plat-config ▫FW▫Memory-Controller	[119]	●	●
	Platform Security Disclosure[145]	2023	IOActive Blog	SMM-code ▫[Shielding ▫CD]	[119]	●	●
	Stase[180]	2024	ASE	SMM-code	●	○	●
	AMD Sinkclose[147]	2024	DEF CON	SMM-code ▫ Shielding ▫CD	[119]	●	●
	AMD Platform Secure Boot[152]	2024	IOActive Blog	Plat-config ▫FW▫PSBStatus	[119]	●	●
	FuzzUEr[75]	2025	NDSS	SMM-code ▫[MS ▫[Spatial | Temporal] | Shielding ▫CD]	●	○	●
	Memory corruption in SMM[199]	2025	Black Hat	SMM-code ▫[MS ▫[Spatial | Temporal] | Shielding ▫[CD | SMMCallout]]	○	○	●
	SmuFuzz[202]	2026	IEEE S&P	SMM-code ▫[MS ▫[Spatial | Temporal] | Shielding ▫[SMMCallout]]	●	○	●

Two-fold Systematization

AXIS 1 · VULNERABILITY ANALYSIS

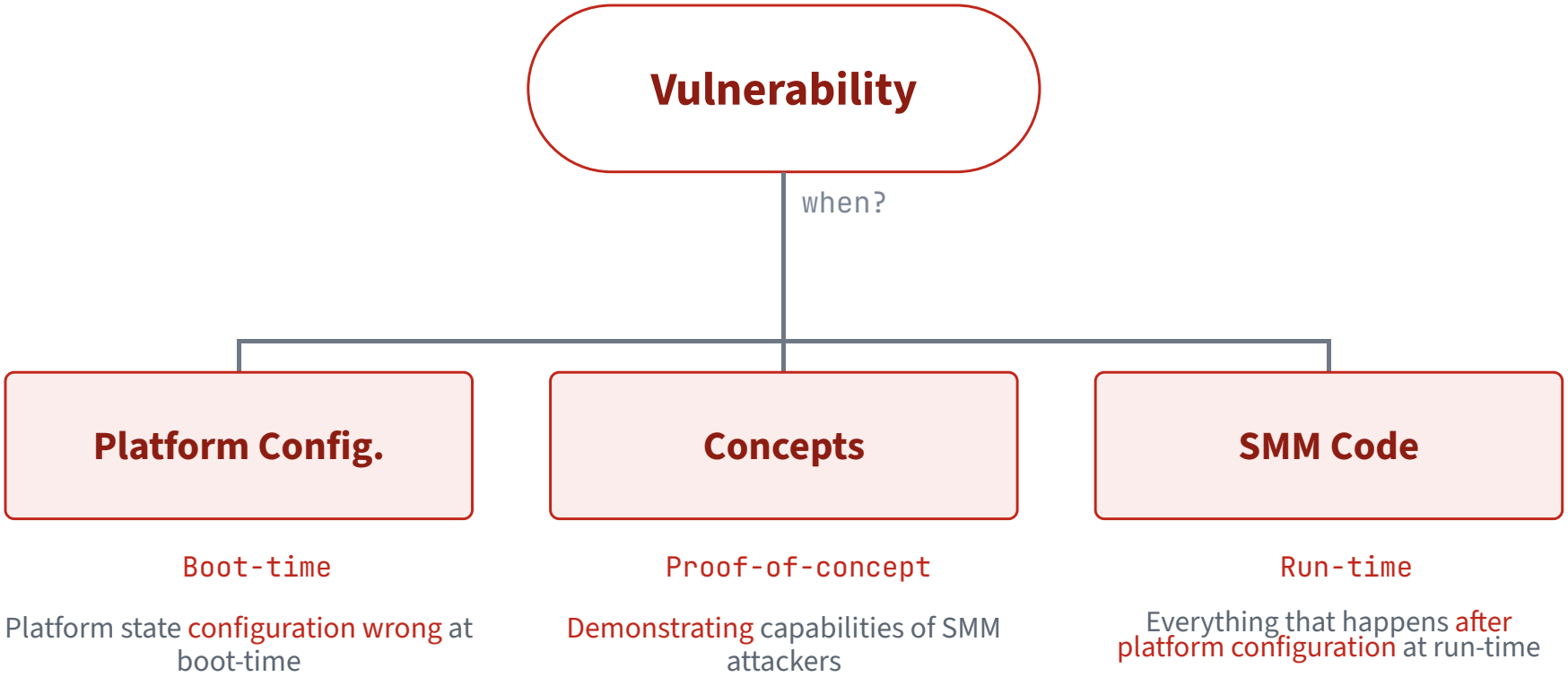
AXIS 2 · LONGITUDINAL ANALYSIS

Three distinct eras, set by shifts in the dominant vulnerability class

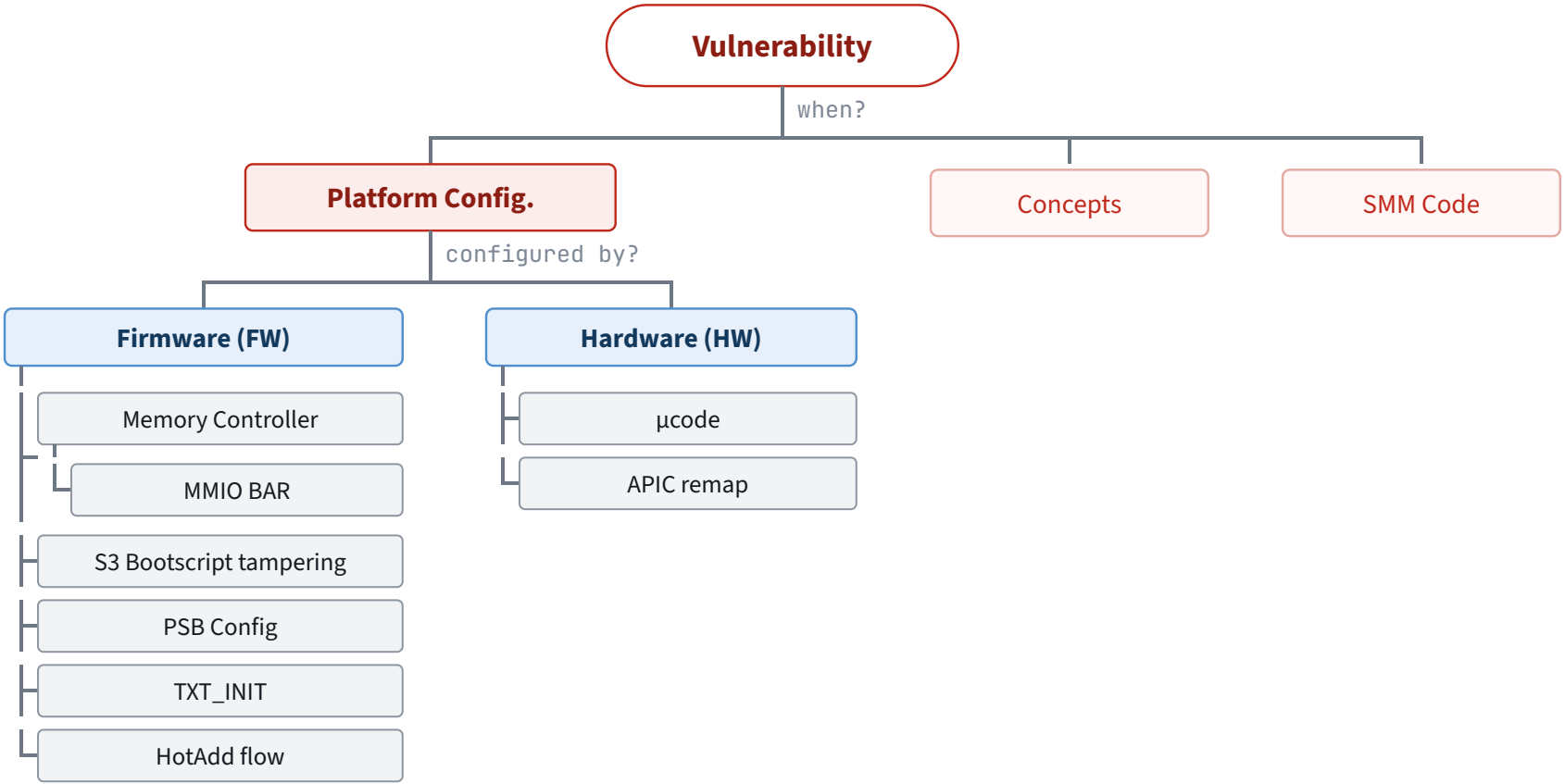
ERA 1	2006–2014
ERA 2	2014–2020
ERA 3	2020–2026

	Name	Year	Venue	Vulnerability	Src	E2E	Auto
ERA 1	SMM OS Security Bypass[67]	2006	CanSecWest	*Plat-config* →FW→*Memory-Controller*	◐	○	○
	SMM Rootkits[72]	2008	SecureComm	*Concept*	○	●	○
	SMM hacks[48]	2008	Phrack	*Plat-config* →FW→*Memory-Controller*	●	●	○
	Xen Hypervisor Subversion[174]	2008	Black Hat	*Plat-config* →FW→*Memory-Controller*	◐	○	○
	SRAM Access Techniques[136]	2009	CanSecWest	*Plat-config* →FW→*Memory-Controller*	○	○	○
	BIOS SMI Rootkit[57]	2009	Phrack	*Concept*	●	◐	○
	Attacking Intel TXT[204]	2009	Black Hat	*Plat-config* →FW→*Memory-Controller*	○	●	○
	Attacking Intel BIOS[202]	2009	Black Hat	*SMM-code* → *Shielding* →CD	○	○	○
	SMM CPU Cache Poisoning[205]	2009	White Paper	*Plat-config* →FW→*Memory-Controller*	○	●	○
	Attacking SMM using SINIT[206]	2011	White Paper	*Plat-config* →FW→*TXT SINIT*	○	●	○
	Flea-reflash hopping[51]	2013	ACM CCS	*Concept*	○	◐	○
	Insyde SMM Vulnerabilities[77]	2013	NCC Blog	*SMM-code* →[*Shielding* →CD | *MS* →*Spatial*]	○	○	○
	Sandman[125]	2014	Mitre	*Plat-config* →FW→[*Memory-Controller* | *TXT SINIT*]	○	◐	○
	Chipsec[134]	2014	CanSecWest	[*Plat-config* | *SMM-code*]	●	○	●
ERA 2	SMM Rootkits Revisited[176]	2014	ARES	*Concept*	○	○	○
	Defeating Secure Boot[121]	2014	Syscan	*Plat-config* →FW→*Memory-Controller*	○	◐	○
	Defeating Signed BIOS[120]	2014	Blog	*SMM-code* → *MS* →*Spatial*	○	●	○
	The Watcher[122]	2014	Mitre	*SMM-code* → *MS* →*IntOverflow*	[179]	●	○
	Smite'em MiTM and Copernicus 2[124]	2014	Mitre	[*Concept*;*SMM-code*]	[80]	◐	●
	UEFI Security Attacks[203]	2014	31C3	[*Plat-config* →FW→*S3BootScript* | *SMM-code* →[*Shielding* →*SMMCallout*]]	○	●	○
	Venamis misery[207]	2014	White Paper	*Plat-config* →FW→*S3BootScript*	[156]	●	○
	Excite[43]	2015	WOOT	*SMM-code* → *Shielding* →*SMMCallout*	○	○	●
	SMM Backdoor[157]	2015	GitHub	*Concept*	●	○	○
	Attacking VMM through SMM[76]	2015	Black Hat	*SMM-code* → *Shielding* →CD	○	○	●
	SMM Memory Sinkhole[66]	2015	Black Hat	*Plat-config* →HW→*APICRemap*	◐	●	○
	A Million BIOSes Infected (Lighteater)[60]	2015	HITBSecConf	*SMM-code* →[*Shielding* →*SMMCallout* | *MS* →*Spatial*]	○	●	○
	Breaking UEFI Security Using DMA[155]	2015	Blog	*SMM-code* → *Shielding* →CD	○	●	●
	SMI Handler Vulnerabilities[41]	2015	CanSecWest	*SMM-code* → *Shielding* →CD	○	○	●
	Aptiocalypsis[158]	2016	Blog	*SMM-code* → *Shielding* →CD	[159]	●	●
	EDK2 communication[215]	2016	White Paper	*SMM-code* → *Shielding* →[CD | *SMMCallout*]	○	○	○
	ThinkPwn/SmmRuntime[161]	2016	Blog	*SMM-code* → *Shielding* →[CD | *SMMCallout*]	[162]	●	●
	Exploiting SMM callout vulnerabilities[160]	2016	Blog	*SMM-code* → *Shielding* →*SMMCallout*	○	●	●
	SMM Data Centers[93]	2017	CanSecWest	*Plat-config* →FW→*HotAddFlowDMA*	○	●	○
	LONGKIT Framework[170]	2017	ICISSP	*Concept*	○	○	○
	BARing the System[50]	2017	RECON	*SMM-code* → *Shielding* →CD→*BAR*	○	●	●
	BIOS holes. Don't Come Inside[70]	2017	Black Hat	*SMM-code* → *Shielding* →*SMMCallout*	[71]	●	●
	Digging Into the Core of Boot[49]	2017	RECON	[*Plat-config* →FW→*Memory-Controller* | *SMM-code* → *Shielding* →CD]	○	○	●
	Exploring Your System Deeper[42]	2017	CanSecWest	[*Plat-config* →[FW→*Memory-Controller* | *S3BootScript*] | *SMM-code* →[*Shielding* →CD]]	●	○	●
	UEFI firmware rootkits[137]	2017	Black Hat	[*Plat-config* →FW→*Memory-Controller* | *SMM-code* →[*Shielding* →[CD | *SMMCallout*] | *MS* →*Spatial*]]	○	●	○
	SMM Spectre v1[69]	2018	Blog	*SMM-code* → *Uarch* →*Spectre*	●	●	●
	Code Check(mate)[167]	2018	Blog	*SMM-code* → *Shielding* →*SMMCallout*	◐	◐	●
	efiXplorer[138]	2020	Black Hat	*SMM-code* →[*Shielding* →[CD | *SMMCallout*] | *MS* →[*Temporal*| *Spatial*]]	[44]	○	●
ERA 3	Attacking the golden ring[151]	2020	Blog	*SMM-code* → *Shielding* →CD	●	●	○
	Firmware Fuzzing using Simics[208]	2020	DAC	*SMM-code* →[*Shielding* →[CD] | *MS* →*Spatial*]	○	○	●
	SMRAM Callout Vulnerability[168]	2020	Blog	*SMM-code* → *Shielding* →*SMMCallout*	◐	◐	●
	SPENDER[219]	2022	IEEE S&P	*SMM-code* → *Shielding* →CD	○	○	●
	SPI Write Protections[38]	2022	Blog	[*Plat-config* →[FW→*Memory-Controller*]]	○	○	●
	HP Repeatable Failures[185]	2022	Blog	*SMM-code* →[*Shielding* →[CD] | *SMMCallout*] | *MS* →*Spatial*]	●	●	●
	AMI Repeatable Failures[184]	2022	Blog	*SMM-code* →[*Shielding* →[*SMMCallout* | CD]	○	●	●
	23 High-Impact Vulnerabilities[183]	2022	Blog	*SMM-code* →[*Shielding* →[CD | *SMMCallout*] | *MS* →*Spatial*]	●	○	●
	UDK-Based SMM Rootkits[81]	2022	Blog	*Concept*	[82]	◐	○
	SMM Supervisor Security[193]	2022	Hardwear.io	*SMM-code* →[*Shielding* →[CD | *SMMCallout*] | *MS* →[*Spatial*| *IntOverflow*]]	○	◐	○
	AMD platform Security[144]	2022	IOActive Blog	*Plat-config* →FW→*Memory-Controller*	●	●	●
	BIOS Past, Present, Future[45]	2022	Black Hat	*SMM-code* →[*Shielding* →[CD | *SMMCallout*] | *MS* →*Spatial*]	●	●	●
	Breaking firmware trust[139]	2022	Black Hat	*SMM-code* →[*Shielding* →[CD | *SMMCallout*] | *MS* →*Spatial*]	○	●	●
	Lenovo High-impact Vulnerabilities[173]	2022	ESET Blog	*SMM-code* →[*Shielding* →CD]	●	●	●
	Simple SMM Rootkit[181]	2022	icWCSN	*Concept*	●	○	○
	The art of SMM bug hunting[53]	2022	Blog	*SMM-code* →[*Shielding* →[CD | *SMMCallout*] | *MS* →*Spatial*]	○	○	●
	Ringhopper[220]	2023	DEF CON	[*SMM-code* →[*Shielding* →CD]]	○	●	●
	RSFuzzer[218]	2023	IEEE S&P	*SMM-code* →[*MS* →[*Spatial*| *Temporal*] | *Shielding* →[CD | *SMMCallout*]]	○	○	●
	Ice Lake TOCTOU[78]	2023	NCC Blog	*SMM-code* →[*MS* →*Spatial*| *Shielding* →CD]	○	○	○
	Back to the Future[146]	2023	IOActive Blog	*Plat-config* →FW→*Memory-Controller*	[119]	●	●
	Platform Security Disclosure[145]	2023	IOActive Blog	*SMM-code* →[*Shielding* →CD]	[119]	●	●
	Stase[180]	2024	ASE	*SMM-code*	●	○	●
	AMD Sinkclose[147]	2024	DEF CON	*SMM-code* → *Shielding* →CD	[119]	●	●
	AMD Platform Secure Boot[152]	2024	IOActive Blog	*Plat-config* →FW→*PSBStatus*	[119]	●	●
	FuzzUEr[75]	2025	NDSS	*SMM-code* →[*MS* →[*Spatial*| *Temporal*] | *Shielding* →CD]	●	○	●
	Memory corruption in SMM[199]	2025	Black Hat	*SMM-code* →[*MS* →[*Spatial*| *Temporal*] | *Shielding* →[CD | *SMMCallout*]]	○	○	●
	SmuFuzz[202]	2026	IEEE S&P	*SMM-code* →[*MS* →[*Spatial*| *Temporal*] | *Shielding* →[*SMMCallout*]]	●	○	●

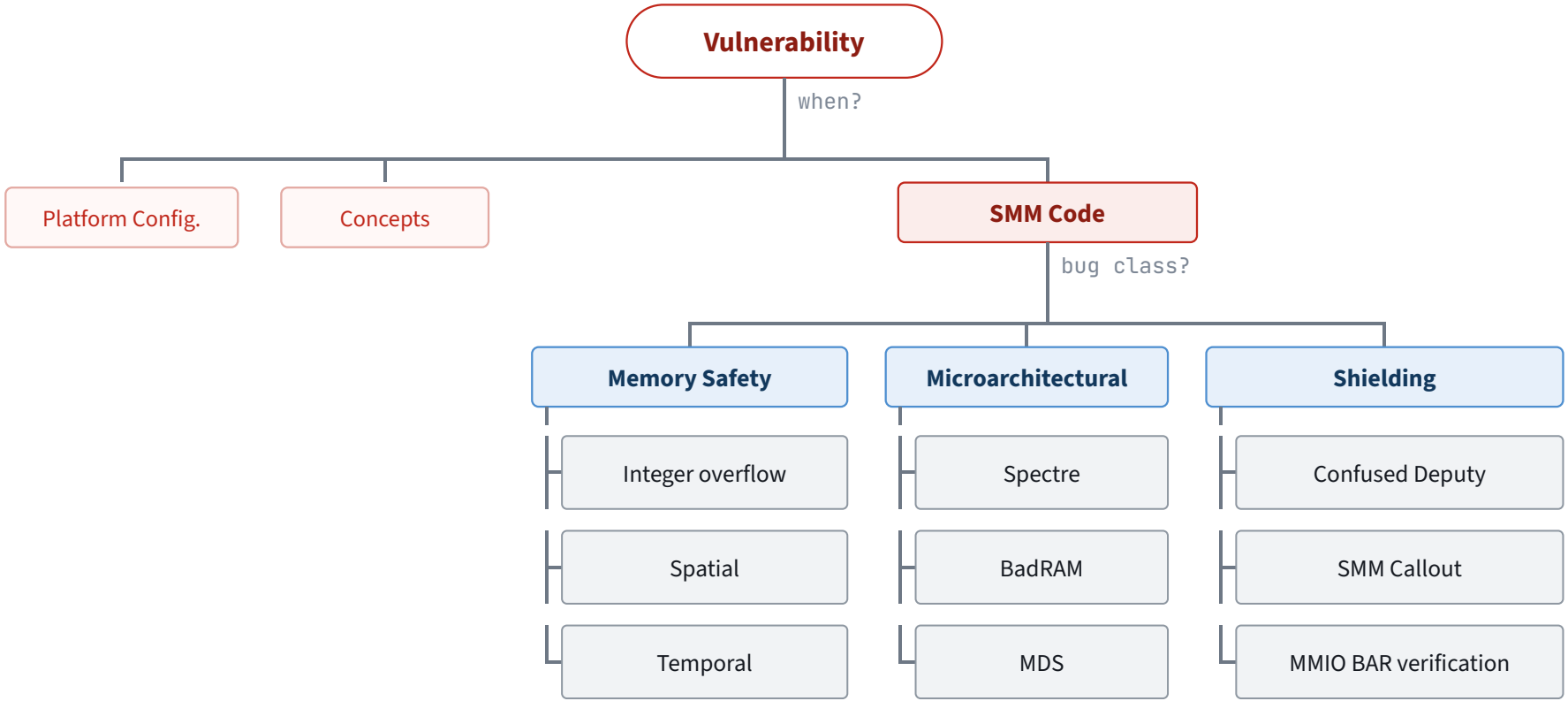
Vulnerability Analysis – Classification Tree



Vulnerability Analysis – Classification Tree – Boot time



Vulnerability Analysis – Classification Tree – Run time



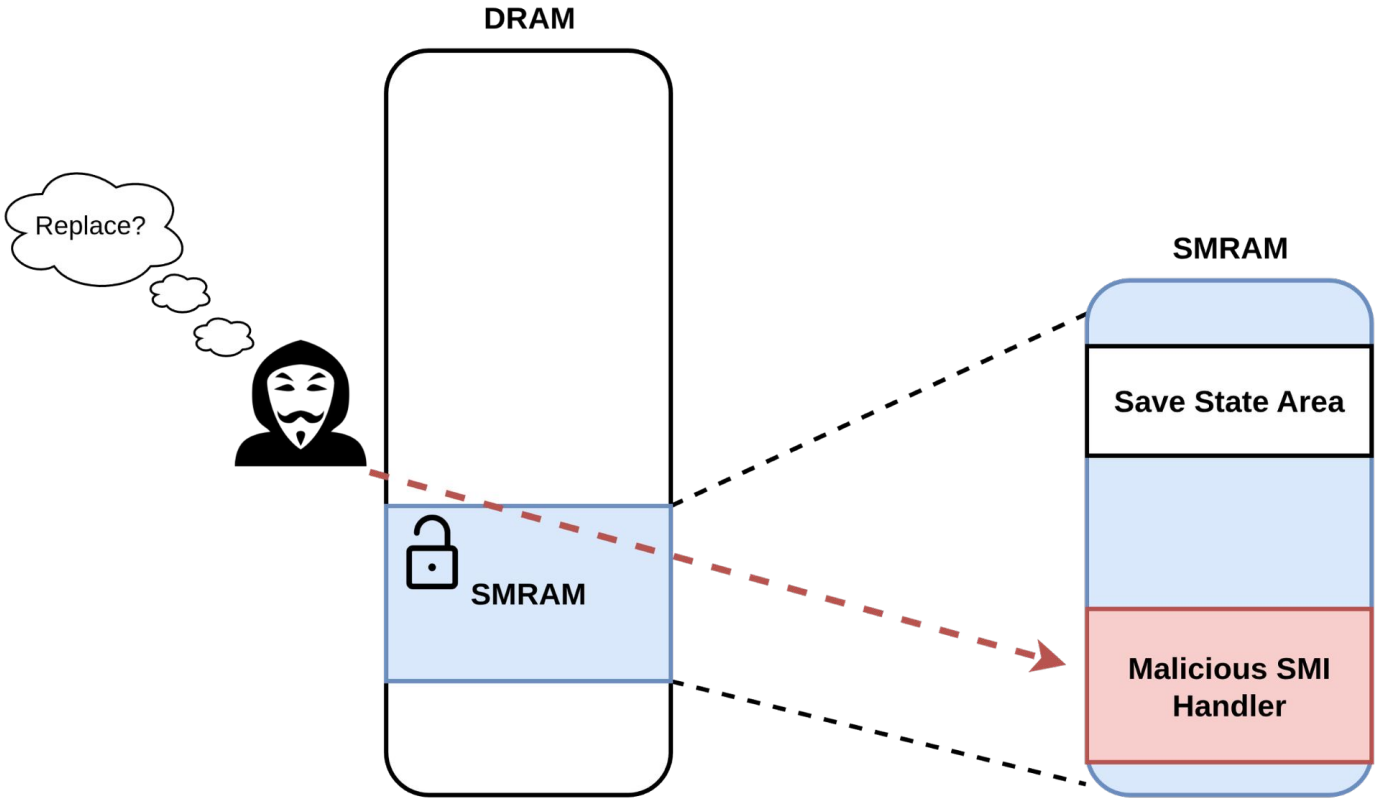
Era 1 – Platform Configuration Vulnerabilities

	Name	Year	Venue	Vulnerability	Src	E2E	Auto
ERA 1	SMM OS Security Bypass[67]	2006	CanSecWest	*Plat-config* ⇒FW⇒*Memory-Controller*	◐	○	○
	SMM Rootkits[72]	2008	SecureComm	*Concept*	○	●	○
	SMM hacks[48]	2008	Phrack	*Plat-config* ⇒FW⇒*Memory-Controller*	●	●	○
	Xen Hypervisor Subversion[174]	2008	Black Hat	*Plat-config* ⇒FW⇒*Memory-Controller*	◐	○	○
	SRAM Access Techniques[136]	2009	CanSecWest	*Plat-config* ⇒FW⇒*Memory-Controller*	○	○	○
	BIOS SMI Rootkit[57]	2009	Phrack	*Concept*	●	◐	○
	Attacking Intel TXT[204]	2009	Black Hat	*Plat-config* ⇒FW⇒*Memory-Controller*	○	●	○
	Attacking Intel BIOS[202]	2009	Black Hat	*SMM-code* ⇒ *Shielding* ⇒*CD*	○	○	○
	SMM CPU Cache Poisoning[205]	2009	White Paper	*Plat-config* ⇒FW⇒*Memory-Controller*	○	●	○
	Attacking SMM using SINIT[206]	2011	White Paper	*Plat-config* ⇒FW⇒*TXT SINIT*	○	●	○
	Flea-reflash hopping[51]	2013	ACM CCS	*Concept*	○	●	○
	Insyde SMM Vulnerabilities[77]	2013	NCC Blog	*SMM-code* ⇒[*Shielding* ⇒*CD*] *MS* ⇒*Spatial*]	○	○	○
	Sandman[125]	2014	Mitre	*Plat-config* ⇒FW⇒[*Memory-Controller*	*TXT SINIT*]	○	◐	○
	Chipsec[134]	2014	CanSecWest	[*Plat-config*	*SMM-code*]	●	○	●
ERA 2	SMM Rootkits Revisited[176]	2014	ARES	*Concept*	○	○	○
	Defeating Secure Boot[121]	2014	Syscan	*Plat-config* ⇒FW⇒*Memory-Controller*	○	◐	○
	Defeating Signed BIOS[120]	2014	Blog	*SMM-code* ⇒ *MS* ⇒*Spatial*	○	●	○
	The Watcher[122]	2014	Mitre	*SMM-code* ⇒ *MS* ⇒*IntOverflow*	○	●	○
	Smite'em MiTM and Copernicus 2[124]	2014	Mitre	[*Concept*|*SMM-code*]	○	◐	●
	UEFI Security Attacks[203]	2014	31C3	[*Plat-config* ⇒FW⇒*S3BootScript*	*SMM-code* ⇒[*Shielding* ⇒*SMMCallout*]]	○	●	○
	Venamis misery[207]	2014	White Paper	*Plat-config* ⇒FW⇒*S3BootScript*	[156]	●	○
	Excite[43]	2015	WOOT	*SMM-code* ⇒ *Shielding* ⇒*SMMCallout*	○	○	●
	SMM Backdoor[157]	2015	GitHub	*Concept*	●	○	○
	Attacking VMM through SMM[76]	2015	Black Hat	*SMM-code* ⇒ *Shielding* ⇒*CD*	○	○	●
	SMM Memory Sinkhole[66]	2015	Black Hat	*Plat-config* ⇒HW⇒*APICRemap*	◐	●	○
	A Million BIOSes Infected (Lighteater)[60]	2015	HITBSecConf	*SMM-code* ⇒[*Shielding* ⇒*SMMCallout*] *MS* ⇒*Spatial*]	○	●	○
	Breaking UEFI Security Using DMA[155]	2015	Blog	*SMM-code* ⇒ *Shielding* ⇒*CD*	○	●	●
	SMI Handler Vulnerabilities[41]	2015	CanSecWest	*SMM-code* ⇒ *Shielding* ⇒*CD*	○	○	●
	Aptiocalypsis[158]	2016	Blog	*SMM-code* ⇒ *Shielding* ⇒*CD*	[159]	●	●
	EDK2 communication[215]	2016	White Paper	*SMM-code* ⇒ *Shielding* ⇒[*CD*|*SMMCallout*]	○	○	○
	ThinkPwn/SmmRuntime[161]	2016	Blog	*SMM-code* ⇒ *Shielding* ⇒[*CD*|*SMMCallout*]	[162]	●	●
	Exploiting SMM callout vulnerabilities[160]	2016	Blog	*SMM-code* ⇒ *Shielding* ⇒*SMMCallout*	○	●	●
	SMM Data Centers[93]	2017	CanSecWest	*Plat-config* ⇒FW⇒*HotAddFlowDMA*	○	●	○
	LONGKIT Framework[170]	2017	ICISSP	*Concept*	○	○	○
	BARing the System[50]	2017	RECON	*SMM-code* ⇒ *Shielding* ⇒*CD*⇒*BAR*	○	●	●
	BIOS holes. Don't Come Inside[70]	2017	Black Hat	*SMM-code* ⇒ *Shielding* ⇒*SMMCallout*	[71]	●	●
	Digging Into the Core of Boot[49]	2017	RECON	[*Plat-config* ⇒FW⇒*Memory-Controller*] *SMM-code* ⇒ *Shielding* ⇒*CD*]	○	○	●
	Exploring Your System Deeper[42]	2017	CanSecWest	[*Plat-config* ⇒[FW⇒*Memory-Controller*	*S3BootScript*]	*SMM-code* ⇒[*Shielding* ⇒*CD*]]	●	○	●
	UEFI firmware rootkits[137]	2017	Black Hat	[*Plat-config* ⇒FW⇒*Memory-Controller*] *SMM-code* ⇒[*Shielding* ⇒[*CD*|*SMMCallout*] *MS* ⇒*Spatial*]]	○	●	○
	SMM Spectre v1[69]	2018	Blog	*SMM-code* ⇒ *Uarch* ⇒*Spectre*	●	●	●
	Code Check(mate)[167]	2018	Blog	*SMM-code* ⇒ *Shielding* ⇒*SMMCallout*	◐	◐	●
	efiXplorer[138]	2020	Black Hat	*SMM-code* ⇒[*Shielding* ⇒[*CD*|*SMMCallout*] *MS* ⇒[*Temporal*|*Spatial*]]	[44]	○	●
ERA 3	Attacking the golden ring[151]	2020	Blog	*SMM-code* ⇒ *Shielding* ⇒*CD*	●	●	○
	Firmware Fuzzing using Simics[208]	2020	DAC	*SMM-code* ⇒[*Shielding* ⇒[*CD*]] *MS* ⇒*Spatial*]	○	○	●
	SMRAM Callout Vulnerability[168]	2020	Blog	*SMM-code* ⇒ *Shielding* ⇒*SMMCallout*	◐	◐	●
	SPENDER[219]	2022	IEEE S&P	*SMM-code* ⇒ *Shielding* ⇒*CD*	○	○	●
	SPI Write Protections[38]	2022	Blog	[*Plat-config* ⇒[FW⇒*Memory-Controller*]]	○	○	●
	HP Repeatable Failures[185]	2022	Blog	*SMM-code* ⇒[*Shielding* ⇒[*CD*|*SMMCallout*] *MS* ⇒*Spatial*]	●	●	●
	AMI Repeatable Failures[184]	2022	Blog	*SMM-code* ⇒ *Shielding* ⇒[*SMMCallout*|*CD*]	○	●	●
	23 High-Impact Vulnerabilities[183]	2022	Blog	*SMM-code* ⇒[*Shielding* ⇒[*CD*|*SMMCallout*] *MS* ⇒*Spatial*]	●	○	●
	UDK-Based SMM Rootkits[81]	2022	Blog	*Concept*	[82]	◐	○
	SMM Supervisor Security[193]	2022	Hardwear.io	*SMM-code* ⇒[*Shielding* ⇒[*CD*|*SMMCallout*] *MS* ⇒[*Spatial*|*IntOverflow*]]	○	◐	○
	AMD platform Security[144]	2022	IOActive Blog	*Plat-config* ⇒FW⇒*Memory-Controller*	●	●	●
	BIOS Past, Present, Future[45]	2022	Black Hat	*SMM-code* ⇒[*Shielding* ⇒[*CD*|*SMMCallout*] *MS* ⇒*Spatial*]	●	●	●
	Breaking firmware trust[139]	2022	Black Hat	*SMM-code* ⇒[*Shielding* ⇒[*CD*|*SMMCallout*] *MS* ⇒*Spatial*]	○	●	●
	Lenovo High-impact Vulnerabilities[173]	2022	ESET Blog	*SMM-code* ⇒[*Shielding* ⇒*CD*]	◐	●	●
	Simple SMM Rootkit[181]	2022	icWCSN	*Concept*	●	○	○
	The art of SMM bug hunting[53]	2022	Blog	*SMM-code* ⇒[*Shielding* ⇒[*CD*|*SMMCallout*] *MS* ⇒*Spatial*]	○	○	●
	Ringhopper[220]	2023	DEF CON	[*SMM-code* ⇒[*Shielding* ⇒*CD*]]	○	●	○
	RSFuzzer[218]	2023	IEEE S&P	*SMM-code* ⇒[*MS* ⇒[*Spatial*|*Temporal*] *Shielding* ⇒[*CD*|*SMMCallout*]]	○	○	●
	Ice Lake TOCTOU[78]	2023	NCC Blog	*SMM-code* ⇒[*MS* ⇒*Spatial*	*Shielding* ⇒*CD*]	○	○	○
	Back to the Future[146]	2023	IOActive Blog	*Plat-config* ⇒FW⇒*Memory-Controller*	[119]	○	●
	Platform Security Disclosure[145]	2023	IOActive Blog	*SMM-code* ⇒[*Shielding* ⇒*CD*]	[119]	●	●
	Stase[180]	2024	ASE	*SMM-code*	●	○	●
	AMD Sinkclose[147]	2024	DEF CON	*SMM-code* ⇒ *Shielding* ⇒*CD*	[119]	●	●
	AMD Platform Secure Boot[152]	2024	IOActive Blog	*Plat-config* ⇒FW⇒*PSBStatus*	[119]	●	●
	FuzzUEr[75]	2025	NDSS	*SMM-code* ⇒[*MS* ⇒[*Spatial*|*Temporal*] *Shielding* ⇒*CD*]	●	○	●
	Memory corruption in SMM[199]	2025	Black Hat	*SMM-code* ⇒[*MS* ⇒[*Spatial*|*Temporal*] *Shielding* ⇒[*CD*|*SMMCallout*]]	○	○	●
	SmuFuzz[201]	2026	IEEE S&P	*SMM-code* ⇒[*MS* ⇒[*Spatial*|*Temporal*] *Shielding* ⇒[*SMMCallout*]]	◐	○	●

Era 1 – Platform Configuration Vulnerabilities

SMM OS Security Bypass [67]	2006	***Plat-config*** →*FW*→*Memory-Controller*
SMM Rootkits [72]	2008	***Concept***
SMM hacks [48]	2008	***Plat-config*** →*FW*→*Memory-Controller*
Xen Hypervisor Subversion [174]	2008	***Plat-config*** →*FW*→*Memory-Controller*
SRAM Access Techniques [136]	2009	***Plat-config*** →*FW*→*Memory-Controller*
BIOS SMI Rootkit [57]	2009	***Concept***
Attacking Intel TXT [204]	2009	***Plat-config*** →*FW*→*Memory-Controller*
Attacking Intel BIOS [202]	2009	***SMM-code***→***Shielding***→*CD*
SMM CPU Cache Poisoning [205]	2009	***Plat-config*** →*FW*→*Memory-Controller*
Attacking SMM using SINIT [206]	2011	***Plat-config*** →*FW*→*TXT SINIT*
Flea-reflash hopping [51]	2013	***Concept***
Insyde SMM Vulnerabilities [77]	2013	***SMM-code***→*[****Shielding***→*CD* |***MS***→*Spatial]*
Sandman [125]	2014	***Plat-config*** →*FW*→*[Memory-Controller* | *TXT SINIT]*
Chipsec [134]	2014	*[* ***Plat-config*** | ***SMM-code*** *]*

Era 1 – Platform Configuration Vulnerabilities – Unlocked Platform State



Era 2 – Shift from Boot-time to Run-time Vulnerabilities

	Name	Year	Venue	Vulnerability	Src	E2E	Auto
ERA 1	SMM OS Security Bypass[67]	2006	CanSecWest	*Plat-config* ⇒FW⇒*Memory-Controller*	◐	○	○
	SMM Rootkits[72]	2008	SecureComm	*Concept*	○	●	○
	SMM hacks[48]	2008	Phrack	*Plat-config* ⇒FW⇒*Memory-Controller*	●	●	○
	Xen Hypervisor Subversion[174]	2008	Black Hat	*Plat-config* ⇒FW⇒*Memory-Controller*	◐	○	○
	SRAM Access Techniques[136]	2009	CanSecWest	*Plat-config* ⇒FW⇒*Memory-Controller*	○	○	○
	BIOS SMI Rootkit[57]	2009	Phrack	*Concept*	●	◐	○
	Attacking Intel TXT[204]	2009	Black Hat	*Plat-config* ⇒FW⇒*Memory-Controller*	○	●	○
	Attacking Intel BIOS[202]	2009	Black Hat	*SMM-code* ⇒ *Shielding* ⇒*CD*	○	○	○
	SMM CPU Cache Poisoning[205]	2009	White Paper	*Plat-config* ⇒FW⇒*Memory-Controller*	○	●	○
	Attacking SMM using SINIT[206]	2011	White Paper	*Plat-config* ⇒FW⇒*TXT SINIT*	○	●	○
	Flea-reflash hopping[51]	2013	ACM CCS	*Concept*	○	●	○
	Insyde SMM Vulnerabilities[77]	2013	NCC Blog	*SMM-code* ⇒[*Shielding* ⇒*CD*] *MS* ⇒*Spatial*]	○	○	○
	Sandman[125]	2014	Mitre	*Plat-config* ⇒FW⇒*Memory-Controller* [*TXT SINIT*]	○	◐	○
	Chipsec[134]	2014	CanSecWest	[*Plat-config*] *SMM-code*]	◐	○	◐
ERA 2	SMM Rootkits Revisited[176]	2014	ARES	*Concept*	○	○	○
	Defeating Secure Boot[121]	2014	Syscan	*Plat-config* ⇒FW⇒*Memory-Controller*	○	◐	○
	Defeating Signed BIOS[120]	2014	Blog	*SMM-code* ⇒ *MS* ⇒*Spatial*	○	●	○
	The Watcher[122]	2014	Mitre	*SMM-code* ⇒ *MS* ⇒*IntOverflow*	[179]	●	○
	Smite'em MiTM and Copernicus 2[124]	2014	Mitre	[*Concept*]*SMM-code*]	[80]	◐	●
	UEFI Security Attacks[203]	2014	31C3	[*Plat-config* ⇒FW⇒*S3BootScript* [*SMM-code* ⇒[*Shielding* ⇒*SMMCallout*]]	○	●	○
	Venamis misery[207]	2014	White Paper	*Plat-config* ⇒FW⇒*S3BootScript*	[156]	●	○
	Excite[43]	2015	WOOT	*SMM-code* ⇒ *Shielding* ⇒*SMMCallout*	○	○	●
	SMM Backdoor[157]	2015	GitHub	*Concept*	●	○	○
	Attacking VMM through SMM[76]	2015	Black Hat	*SMM-code* ⇒ *Shielding* ⇒*CD*	○	○	●
	SMM Memory Sinkhole[66]	2015	Black Hat	*Plat-config* ⇒HW⇒*APICRemap*	◐	●	○
	A Million BIOSes Infected (Lighteater)[60]	2015	HITBSecConf	*SMM-code* ⇒[*Shielding* ⇒*SMMCallout*] *MS* ⇒*Spatial*]	○	●	○
	Breaking UEFI Security Using DMA[155]	2015	Blog	*SMM-code* ⇒ *Shielding* ⇒*CD*	○	●	●
	SMI Handler Vulnerabilities[41]	2015	CanSecWest	*SMM-code* ⇒ *Shielding* ⇒*CD*	○	○	●
	Aptiocalypsis[158]	2016	Blog	*SMM-code* ⇒ *Shielding* ⇒*CD*	[159]	●	●
	EDK2 communication[215]	2016	White Paper	*SMM-code* ⇒ *Shielding* ⇒[*CD*	*SMMCallout*]	○	○	○
	ThinkPwn/SmmRuntime[161]	2016	Blog	*SMM-code* ⇒ *Shielding* ⇒[*CD*	*SMMCallout*]	[162]	●	●
	Exploiting SMM callout vulnerabilities[160]	2016	Blog	*SMM-code* ⇒ *Shielding* ⇒*SMMCallout*	○	●	●
	SMM Data Centers[93]	2017	CanSecWest	*Plat-config* ⇒FW⇒*HotAddFlowDMA*	○	●	○
	LONGKIT Framework[170]	2017	ICISSP	*Concept*	○	○	○
	BARing the System[50]	2017	RECON	*SMM-code* ⇒ *Shielding* ⇒*CD*⇒*BAR*	○	●	●
	BIOS holes. Don't Come Inside[70]	2017	Black Hat	*SMM-code* ⇒ *Shielding* ⇒*SMMCallout*	[71]	●	●
	Digging Into the Core of Boot[49]	2017	RECON	[*Plat-config* ⇒FW⇒*Memory-Controller*] *SMM-code* ⇒ *Shielding* ⇒*CD*]	○	○	●
	Exploring Your System Deeper[42]	2017	CanSecWest	[*Plat-config* ⇒[*FW⇒Memory-Controller* [*S3BootScript*] [*SMM-code* ⇒[*Shielding* ⇒*CD*]]	●	○	●
	UEFI firmware rootkits[137]	2017	Black Hat	[*Plat-config* ⇒FW⇒*Memory-Controller* [*SMM-code* ⇒[*Shielding* ⇒[*CD*	*SMMCallout*] *MS* ⇒*Spatial*]]	○	●	○
	SMM Spectre v1[69]	2018	Blog	*SMM-code* ⇒ *Uarch* ⇒*Spectre*	●	●	●
	Code Check(mate)[167]	2018	Blog	*SMM-code* ⇒ *Shielding* ⇒*SMMCallout*	◐	◐	●
	efiXplorer[138]	2020	Black Hat	*SMM-code* ⇒[*Shielding* ⇒[*CD*	*SMMCallout*] *MS* ⇒[*Temporal*	*Spatial*]]	[44]	○	●
ERA 3	Attacking the golden ring[151]	2020	Blog	*SMM-code* ⇒ *Shielding* ⇒*CD*	●	●	○
	Firmware Fuzzing using Simics[208]	2020	DAC	*SMM-code* ⇒[*Shielding* ⇒[*CD*]] *MS* ⇒*Spatial*]	○	○	●
	SMRAM Callout Vulnerability[168]	2020	Blog	*SMM-code* ⇒ *Shielding* ⇒*SMMCallout*	◐	◐	●
	SPENDER[219]	2022	IEEE S&P	*SMM-code* ⇒ *Shielding* ⇒*CD*	○	○	●
	SPI Write Protections[38]	2022	Blog	[*Plat-config* ⇒[*FW⇒Memory-Controller*]]	○	○	●
	HP Repeatable Failures[185]	2022	Blog	*SMM-code* ⇒[*Shielding* ⇒[*CD*	*SMMCallout*] *MS* ⇒*Spatial*]	●	●	●
	AMI Repeatable Failures[184]	2022	Blog	*SMM-code* ⇒ *Shielding* ⇒[*SMMCallout*	*CD*]	○	●	●
	23 High-Impact Vulnerabilities[183]	2022	Blog	*SMM-code* ⇒[*Shielding* ⇒[*CD*	*SMMCallout*] *MS* ⇒*Spatial*]	●	○	●
	UDK-Based SMM Rootkits[81]	2022	Blog	*Concept*	[82]	◐	○
	SMM Supervisor Security[193]	2022	Hardwear.io	*SMM-code* ⇒[*Shielding* ⇒[*CD*	*SMMCallout*] *MS* ⇒[*Spatial*	*IntOverflow*]]	○	◐	○
	AMD platform Security[144]	2022	IOActive Blog	*Plat-config* ⇒FW⇒*Memory-Controller*	●	●	●
	BIOS Past, Present, Future[45]	2022	Black Hat	*SMM-code* ⇒[*Shielding* ⇒[*CD*	*SMMCallout*] *MS* ⇒*Spatial*]	●	●	●
	Breaking firmware trust[139]	2022	Black Hat	*SMM-code* ⇒[*Shielding* ⇒[*CD*	*SMMCallout*] *MS* ⇒*Spatial*]	○	●	●
	Lenovo High-impact Vulnerabilities[173]	2022	ESET Blog	*SMM-code* ⇒[*Shielding* ⇒*CD*]	◐	●	●
	Simple SMM Rootkit[181]	2022	icWCSN	*Concept*	●	○	○
	The art of SMM bug hunting[53]	2022	Blog	*SMM-code* ⇒[*Shielding* ⇒[*CD*	*SMMCallout*] *MS* ⇒*Spatial*]	○	○	●
	Ringhopper[220]	2023	DEF CON	[*SMM-code* ⇒[*Shielding* ⇒*CD*]]	○	●	○
	RSFuzzer[218]	2023	IEEE S&P	*SMM-code* ⇒[*MS* ⇒[*Spatial*	*Temporal*]	*Shielding* ⇒[*CD*	*SMMCallout*]]	○	○	●
	Ice Lake TOCTOU[78]	2023	NCC Blog	*SMM-code* ⇒[*MS* ⇒*Spatial*	*Shielding* ⇒*CD*]	○	○	○
	Back to the Future[146]	2023	IOActive Blog	*Plat-config* ⇒FW⇒*Memory-Controller*	[119]	○	●
	Platform Security Disclosure[145]	2023	IOActive Blog	*SMM-code* ⇒[*Shielding* ⇒*CD*]	[119]	●	●
	Stase[180]	2024	ASE	*SMM-code*	●	○	●
	AMD Sinkclose[147]	2024	DEF CON	*SMM-code* ⇒ *Shielding* ⇒*CD*	[119]	●	●
	AMD Platform Secure Boot[152]	2024	IOActive Blog	*Plat-config* ⇒FW⇒*PSBStatus*	[119]	●	●
	FuzzUEr[75]	2025	NDSS	*SMM-code* ⇒[*MS* ⇒[*Spatial*	*Temporal*]	*Shielding* ⇒*CD*]	●	○	●
	Memory corruption in SMM[199]	2025	Black Hat	*SMM-code* ⇒[*MS* ⇒[*Spatial*	*Temporal*]	*Shielding* ⇒[*CD*	*SMMCallout*]]	○	○	●
	SmuFuzz[201]	2026	IEEE S&P	*SMM-code* ⇒[*MS* ⇒[*Spatial*	*Temporal*]	*Shielding* ⇒[*SMMCallout*]]	◐	○	●

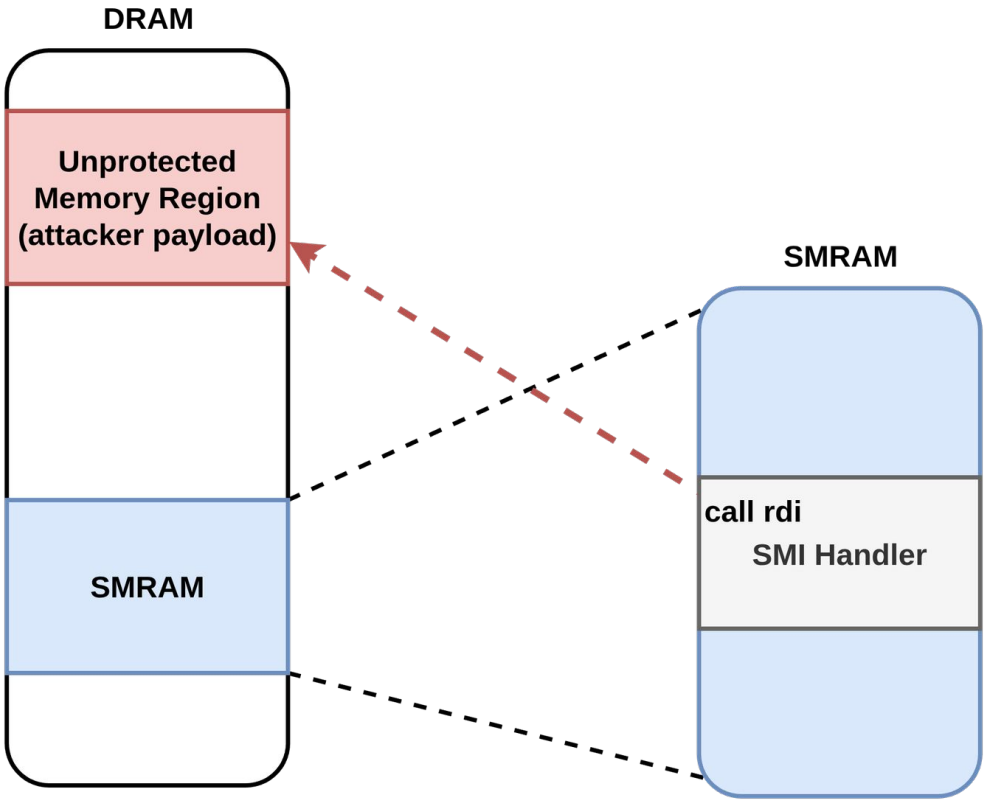


Era 2 – Shift from Boot-time to Run-time Vulnerabilities

2014	*Concept*
2014	*Plat-config →FW→Memory-Controller*
2014	*SMM-code → MS →Spatial*
2014	*SMM-code → MS →IntOverflow*
2014	*[Concept|SMM-code]*
2014	*[Plat-config →FW→S3BootScript | SMM-code →[Shielding →SMMCallout]]*
2014	*Plat-config →FW→S3BootScript*
2015	*SMM-code → Shielding →SMMCallout*
2015	*Concept*
2015	*SMM-code → Shielding →CD*
2015	*Plat-config →HW→APICRemap*
2015	*SMM-code →[Shielding →SMMCallout | MS →Spatial]*
2015	*SMM-code → Shielding →CD*
2015	*SMM-code → Shielding →CD*
2016	*SMM-code → Shielding →CD*
2016	*SMM-code → Shielding →[CD | SMMCallout]*
2016	*SMM-code → Shielding →[CD | SMMCallout]*
2016	*SMM-code → Shielding →SMMCallout*
2017	*Plat-config →FW→HotAddFlowDMA*
2017	*Concept*
2017	*SMM-code → Shielding →CD→BAR*
2017	*SMM-code → Shielding →SMMCallout*
2017	*[Plat-config →FW→Memory-Controller | SMM-code → Shielding →CD]*
2017	*[Plat-config →[FW→Memory-Controller | S3BootScript] | SMM-code →[Shielding →CD]]*
2017	*[Plat-config →FW→Memory-Controller | SMM-code →[Shielding MS →Spatial]]*
2018	*SMM-code→Uarch→Spectre*
2018	*SMM-code → Shielding →SMMCallout*
2020	*SMM-code →[Shielding →[CD | SMMCallout] | MS →[Temporal | Spatial]]*

- Shielding dominates — confused deputy, SMM callouts, memory safety
- Configuration bugs thin out

Era 2 – Confused Deputy Vulnerability



Era 3 – Persisting Vulnerabilities

	Name	Year	Venue	Vulnerability	Src	E2E	Auto
ERA 1	SMM OS Security Bypass[67]	2006	CanSecWest	*Plat-config* ↛*FW*↛*Memory-Controller*	◐	○	○
	SMM Rootkits[72]	2008	SecureComm	*Concept*	○	●	○
	SMM hacks[48]	2008	Phrack	*Plat-config* ↛*FW*↛*Memory-Controller*	●	●	○
	Xen Hypervisor Subversion[174]	2008	Black Hat	*Plat-config* ↛*FW*↛*Memory-Controller*	◐	○	○
	SRAM Access Techniques[136]	2009	CanSecWest	*Plat-config* ↛*FW*↛*Memory-Controller*	○	○	○
	BIOS SMI Rootkit[57]	2009	Phrack	*Concept*	●	◐	○
	Attacking Intel TXT[204]	2009	Black Hat	*Plat-config* ↛*FW*↛*Memory-Controller*	○	●	○
	Attacking Intel BIOS[202]	2009	Black Hat	*SMM-code* ↛ *Shielding* ↛*CD*	○	○	○
	SMM CPU Cache Poisoning[205]	2009	White Paper	*Plat-config* ↛*FW*↛*Memory-Controller*	○	●	○
	Attacking SMM using SINIT[206]	2011	White Paper	*Plat-config* ↛*FW*↛*TXT SINIT*	○	●	○
	Flea-reflash hopping[51]	2013	ACM CCS	*Concept*	○	●	○
	Insyde SMM Vulnerabilities[77]	2013	NCC Blog	*SMM-code* ↛[*Shielding* ↛*CD*] *MS* ↛*Spatial*]	○	○	○
	Sandman[125]	2014	Mitre	*Plat-config* ↛*FW*↛*Memory-Controller* [*TXT SINIT*]	○	◐	○
	Chipsec[134]	2014	CanSecWest	[*Plat-config*] *SMM-code*]	◐	○	◐
ERA 2	SMM Rootkits Revisited[176]	2014	ARES	*Concept*	○	○	○
	Defeating Secure Boot[121]	2014	Syscan	*Plat-config* ↛*FW*↛*Memory-Controller*	○	◐	○
	Defeating Signed BIOS[120]	2014	Blog	*SMM-code* ↛ *MS* ↛*Spatial*	○	●	○
	The Watcher[122]	2014	Mitre	*SMM-code* ↛ *MS* ↛*intOverflow*	[179]	●	○
	Smite'em MiTM and Copernicus 2[124]	2014	Mitre	[*Concept*]*SMM-code*]	[80]	◐	●
	UEFI Security Attacks[203]	2014	31C3	[*Plat-config* ↛*FW*↛*S3BootScript* [*SMM-code* ↛[*Shielding* ↛*SMMCallout*]]	○	●	○
	Venamis misery[207]	2014	White Paper	*Plat-config* ↛*FW*↛*S3BootScript*	[156]	●	○
	Excite[43]	2015	WOOT	*SMM-code* ↛ *Shielding* ↛*SMMCallout*	○	○	●
	SMM Backdoor[157]	2015	GitHub	*Concept*	●	○	○
	Attacking VMM through SMM[76]	2015	Black Hat	*SMM-code* ↛ *Shielding* ↛*CD*	○	○	●
	SMM Memory Sinkhole[66]	2015	Black Hat	*Plat-config* ↛*HW*↛*APICRemap*	◐	●	○
	A Million BIOSes Infected (Lighteater)[60]	2015	HITBSecConf	*SMM-code* ↛[*Shielding* ↛*SMMCallout*] *MS* ↛*Spatial*]	○	●	○
	Breaking UEFI Security Using DMA[155]	2015	Blog	*SMM-code* ↛ *Shielding* ↛*CD*	○	●	●
	SMI Handler Vulnerabilities[41]	2015	CanSecWest	*SMM-code* ↛ *Shielding* ↛*CD*	○	○	●
	Aptiocalypsis[158]	2016	Blog	*SMM-code* ↛ *Shielding* ↛*CD*	[159]	●	●
	EDK2 communication[215]	2016	White Paper	*SMM-code* ↛ *Shielding* ↛[*CD*| *SMMCallout*]	○	○	○
	ThinkPwn/SmmRuntime[161]	2016	Blog	*SMM-code* ↛ *Shielding* ↛[*CD*| *SMMCallout*]	[162]	●	●
	Exploiting SMM callout vulnerabilities[160]	2016	Blog	*SMM-code* ↛ *Shielding* ↛*SMMCallout*	○	●	●
	SMM Data Centers[93]	2017	CanSecWest	*Plat-config* ↛*FW*↛*HotAddFlowDMA*	○	●	○
	LONGKIT Framework[170]	2017	ICISSP	*Concept*	○	○	○
	BARing the System[50]	2017	RECON	*SMM-code* ↛ *Shielding* ↛*CD*↛*BAR*	○	●	●
	BIOS holes. Don't Come Inside[70]	2017	Black Hat	*SMM-code* ↛ *Shielding* ↛*SMMCallout*	[71]	●	●
	Digging Into the Core of Boot[49]	2017	RECON	[*Plat-config* ↛[*FW*↛*Memory-Controller*] *SMM-code* ↛ *Shielding* ↛*CD*]	○	○	●
	Exploring Your System Deeper[42]	2017	CanSecWest	[*Plat-config* ↛[*FW*↛*Memory-Controller* [*S3BootScript*] [*SMM-code* ↛[*Shielding* ↛*CD*]]	●	○	●
	UEFI firmware rootkits[137]	2017	Black Hat	[*Plat-config* ↛*FW*↛*Memory-Controller* [*SMM-code* ↛[*Shielding* ↛[*CD*| *SMMCallout*] *MS* ↛*Spatial*]]	○	●	○
	SMM Spectre v1[69]	2018	Blog	*SMM-code* ↛ *Uarch* ↛*Spectre*	●	●	●
	Code Check(mate)[167]	2018	Blog	*SMM-code* ↛ *Shielding* ↛*SMMCallout*	◐	◐	●
	efiXplorer[138]	2020	Black Hat	*SMM-code* ↛[*Shielding* ↛[*CD*| *SMMCallout*] *MS* ↛[*Temporal*| *Spatial*]]	[44]	○	●
ERA 3	Attacking the golden ring[151]	2020	Blog	*SMM-code* ↛ *Shielding* ↛*CD*	●	●	○
	Firmware Fuzzing using Simics[208]	2020	DAC	*SMM-code* ↛[*Shielding* ↛[*CD*] *MS* ↛*Spatial*]	○	○	●
	SMRAM Callout Vulnerability[168]	2020	Blog	*SMM-code* ↛ *Shielding* ↛*SMMCallout*	◐	◐	●
	SPENDER[219]	2022	IEEE S&P	*SMM-code* ↛ *Shielding* ↛*CD*	○	○	●
	SPI Write Protections[38]	2022	Blog	[*Plat-config* ↛[*FW*↛*Memory-Controller*]]	○	○	●
	HP Repeatable Failures[185]	2022	Blog	*SMM-code* ↛[*Shielding* ↛[*CD*| *SMMCallout*] *MS* ↛*Spatial*]	●	●	●
	AMI Repeatable Failures[184]	2022	Blog	*SMM-code* ↛ *Shielding* ↛[*SMMCallout*| *CD*]	○	●	●
	23 High-Impact Vulnerabilities[183]	2022	Blog	*SMM-code* ↛[*Shielding* ↛[*CD*| *SMMCallout*] *MS* ↛*Spatial*]	●	○	●
	UDK-Based SMM Rootkits[81]	2022	Blog	*Concept*	[82]	◐	○
	SMM Supervisor Security[193]	2022	Hardwear.io	*SMM-code* ↛[*Shielding* ↛[*CD*| *SMMCallout*] *MS* ↛[*Spatial*| *intOverflow*]]	○	◐	○
	AMD platform Security[144]	2022	IOActive Blog	*Plat-config* ↛*FW*↛*Memory-Controller*	●	●	●
	BIOS Past, Present, Future[45]	2022	Black Hat	*SMM-code* ↛[*Shielding* ↛[*CD*| *SMMCallout*] *MS* ↛*Spatial*]	●	●	●
	Breaking firmware trust[139]	2022	Black Hat	*SMM-code* ↛[*Shielding* ↛[*CD*| *SMMCallout*] *MS* ↛*Spatial*]	○	●	●
	Lenovo High-impact Vulnerabilities[173]	2022	ESET Blog	*SMM-code* ↛[*Shielding* ↛*CD*]	◐	●	●
	Simple SMM Rootkit[181]	2022	icWCSN	*Concept*	●	○	○
	The art of SMM bug hunting[53]	2022	Blog	*SMM-code* ↛[*Shielding* ↛[*CD*| *SMMCallout*] *MS* ↛*Spatial*]	○	○	●
	Ringhopper[220]	2023	DEF CON	[*SMM-code* ↛[*Shielding* ↛*CD*]]	○	◐	○
	RSFuzzer[218]	2023	IEEE S&P	*SMM-code* ↛[*MS* ↛[*Spatial*| *Temporal*] *Shielding* ↛[*CD*| *SMMCallout*]]	○	○	●
	Ice Lake TOCTOU[78]	2023	NCC Blog	*SMM-code* ↛[*MS* ↛*Spatial* *Shielding* ↛*CD*]	○	○	○
	Back to the Future[146]	2023	IOActive Blog	*Plat-config* ↛*FW*↛*Memory-Controller*	[119]	○	●
	Platform Security Disclosure[145]	2023	IOActive Blog	*SMM-code* ↛[*Shielding* ↛*CD*]	[119]	●	●
	Stase[180]	2024	ASE	*SMM-code*	●	○	●
	AMD Sinkclose[147]	2024	DEF CON	*SMM-code* ↛ *Shielding* ↛*CD*	[119]	●	●
	AMD Platform Secure Boot[152]	2024	IOActive Blog	*Plat-config* ↛*FW*↛*PSBStatus*	[119]	●	●
	FuzzUEr[75]	2025	NDSS	*SMM-code* ↛[*MS* ↛[*Spatial*| *Temporal*] *Shielding* ↛*CD*]	●	○	●
	Memory corruption in SMM[199]	2025	Black Hat	*SMM-code* ↛[*MS* ↛[*Spatial*| *Temporal*] *Shielding* ↛[*CD*| *SMMCallout*]]	○	○	●
	SmuFuzz[201]	2026	IEEE S&P	*SMM-code* ↛[*MS* ↛[*Spatial*| *Temporal*] *Shielding* ↛[*SMMCallout*]]	◐	○	●



Era 3 – Persisting Vulnerabilities

2020 **SMM-code** → **Shielding** →CD

2020 **SMM-code** →[**Shielding** →[CD] | **MS** →Spatial]

2020 **SMM-code** → **Shielding** →SMMCallout

2022 **SMM-code** → **Shielding** →CD

2022 [**Plat-config** →[FW→Memory-Controller]]

2022 **SMM-code** →[**Shielding** →[CD | SMMCallout] | **MS** →Spatial]

2022 **SMM-code** → **Shielding** →[SMMCallout | CD]

2022 **SMM-code** →[**Shielding** →[CD | SMMCallout] | **MS** →Spatial]

2022 **Concept**

2022 **SMM-code** →[**Shielding** →[CD | SMMCallout] | **MS**

2022 **Plat-config** →FW→Memory-Controller

2022 **SMM-code** →[**Shielding** →[CD | SMMCallout] | **MS** →Spatial]

2022 **SMM-code** →[**Shielding** →[CD | SMMCallout] | **MS** →Spatial]

2022 **SMM-code** →[**Shielding** →CD]

2022 **Concept**

2022 **SMM-code** →[**Shielding** →[CD | SMMCallout] | **MS** →Spatial]

2023 [**SMM-code** →[**Shielding** →CD]]

2023 **SMM-code** →[**MS** →[Spatial | Temporal] | **Shielding** →[CD | SMMCallout]]

2023 **SMM-code** →[**MS** →Spatial | **Shielding** →CD]

2023 **Plat-config** →FW→Memory-Controller

2023 **SMM-code** →[**Shielding** →CD]

2024 **SMM-code**

2024 **SMM-code** → **Shielding** →CD

2024 **Plat-config** →FW→PSBStatus

2025 **SMM-code** →[**MS** →[Spatial | Temporal] | **Shielding** →CD]

2025 **SMM-code** →[**MS** →[Spatial | Temporal] | **Shielding** →[CD | SMMCallout]]

2026 **SMM-code** →[**MS** →[Spatial | Temporal] | **Shielding** →[SMMCallout]]

- Fuzzers and static analysis tools
- Plat-config reappears, this time on AMD

Eras × Taxonomy

Category	Era 1 Platform config	Era 2 Breaking SMM code	Era 3 Automated validation
Plat-config	**8**	9	4
Shielding	**2**	**18**	**19**
Memory safety	1	4	12
Microarchitectural	0	1	0
Automated tools	1	**15**	**21**
Total	**13**	**30**	**26**





Hardening and Isolation

SMM Vulnerabilities Inspire Hardening



SMM Hardening

SMM code in memory-safe languages



SMM Containment

Deprivilege SMI handlers — Intel STM, AMD SMM Supervisor, Samsung knox.



Open-source concerns

Closed source firmware code — months of reverse engineering



Open Evaluation Tooling

Available Firmware/SMM Tooling





Firmware ecosystems





Firmware Parsing and Modification





Assess Platform Configuration



Firmware Code Analysis



Industry, Academia and Practice

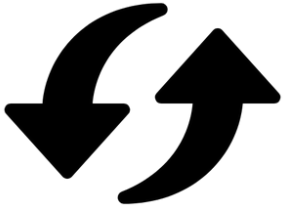
Gap Between Industry, Academia and Practice



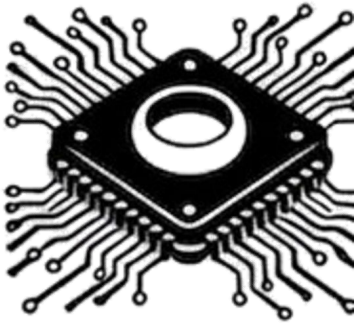
Systematic evaluation workflows



Open-source frameworks



Reusable datasets



Microarchitectural Security

Assessment of µarch Leakage Across SMM Transitions





Name	Year	Advisory	Vulnerability
Mobile boards privilege escalation [87]	2008	Intel	*Plat-config*→FW→Memory-Controller
Server boards privilege escalation [88]	2009	Intel	*Plat-config*→FW→Memory-Controller
Desktop boards privilege escalation [89]	2010	Intel	*Plat-config*→FW→Memory-Controller
SINIT Buffer Overflow [90]	2011	Intel	*SMM-code*→*MS*→Spatial
SINIT ACM privilege escalation [91]	2013	Intel	*SMM-code*→*Shielding*→CD
Local APIC privilege elevation [92]	2015	Intel	*Plat-config*→HW→APICRemap
Memory corruption [104]	2016	Intel	*SMM-code*→*Shielding*→CD
SmmRuntime privilege escalation [105]	2016	Intel	*SMM-code*→*Shielding*→SMMCallout
NUC SMM callout [106]	2017	Intel	*SMM-code*→*Shielding*→SMMCallout
Intel NUC BIOS security updates [94]	2017	Intel	*SMM-code*→*Shielding*→CD
Foreshadow [95]	2018	Intel	*SMM-code* → *Uarch*→MDS
NUC SW SMI Callout [108]	2018	Intel	*SMM-code*→*Shielding*→SMMCallout
EDK2 SMM page protection [107]	2018	Intel	*Plat-config*→FW→Memory-Controller
MDS [112]	2019	Intel	*SMM-code* → *Uarch*→MDS
Intel graphics advisory [110]	2019	Intel	*Plat-config*→FW→Memory-Controller
Intel processor security [96]	2019	Intel	*Plat-config*→FW→Memory-Controller
Trust asynchronous abort [111]	2019	Intel	*SMM-code* → *Uarch*→MDS
AMD race-condition in ASP [2]	2021	AMD	*SMM-code*→*Shielding*→Race-condition
Spectre V1/V2 [113]	2021	Intel	*SMM-code* → *Uarch*→Spectre
MMIO stale data [115]	2022	Intel	*SMM-code* → *Uarch*→MDS
AMD client CPUs vulnerabilities May [3]	2022	AMD	*SMM-code*→*Shielding*→CD
Branch history injection [114]	2022	Intel	*SMM-code* → *Uarch*→Spectre
Snoop assisted L1DS [116]	2022	Intel	*SMM-code* → *Uarch*→MDS
AMD supervisor [9]	2023	AMD	*SMM-code*→*Shielding*→SMMCallout
AMD memory corruption [11]	2023	AMD	*SMM-code*→*Shielding*→SMMCallout
SMU input corrupts SMRAM [7]	2023	AMD	*SMM-code*→*Shielding*→CD
AMD client CPUs vulnerabilities Jan [4]	2023	AMD	*SMM-code*→*Shielding*→CD
AMD client CPUs vulnerabilities Nov [5]	2023	AMD	*SMM-code*→*Shielding*→CD
AMD server CPUs vulnerabilities Jan [6]	2023	AMD	*SMM-code*→*Shielding*→CD
AMD server CPUs vulnerabilities Nov [8]	2023	AMD	*SMM-code*→*Shielding*→CD
Insufficient input validation in ASP [10]	2023	AMD	*SMM-code*→*Shielding*→CD
SPI lock bypass [19]	2024	AMD	*Plat-config*→FW→Memory-Controller
AMD SMM lock bypass [18]	2024	AMD	*Plat-config*→FW→Memory-Controller
STM privilege escalation [117]	2024	Intel	*Plat-config*→HW→ucode
AMD server CPUs — SMM TOCTOU [15]	2024	AMD	*SMM-code*→*Shielding*→CD
AMD client CPUs — SMM TOCTOU [17]	2024	AMD	*SMM-code*→*Shielding*→CD
AMD embedded CPUs — SMM TOCTOU [12]	2024	AMD	*SMM-code*→*Shielding*→CD
AMD Embedded CPUs vulnerabilites Feb [13]	2024	AMD	[*Plat-config*→FW→Memory-Controller |*SMM-code*→*Shielding*→CD]
SMM heap-overflow and access-control [14]	2024	AMD	[*Plat-config*→FW→Memory-Controller |*SMM-code*→*MS*→Spatial]
AMD SMM callout [27]	2025	AMD	*SMM-code*→*Shielding*→SMMCallout
SMM MCE on SMI entry [29]	2025	AMD	*SMM-code*→*Shielding*→Race-condition
SPD input validation [26]	2025	AMD	*SMM-code* → *Uarch*→BadRAM
AMD SMM vulnerabilities [28]	2025	AMD	*SMM-code*→*Shielding*→SMMCallout
Intel slim bootloader [100]	2025	Intel	*Plat-config*→FW→Memory-Controller
AMD client CPUs — input validation [20]	2025	AMD	*SMM-code*→*Shielding*→CD
AMD client CPUs vulnerabilites Aug [21]	2025	AMD	*SMM-code*→*Shielding*→CD
AMD embedded CPUs — input validation [23]	2025	AMD	*SMM-code*→*Shielding*→CD
AMD embedded CPUs [24]	2025	AMD	*SMM-code*→*Shielding*→CD
AMD microcode signature verification [22]	2025	AMD	*Plat-config*→HW→ucode
AMD server CPUs — input validation [25]	2025	AMD	*SMM-code*→*Shielding*→CD
AMD Ryzen & Athlon [30]	2025	AMD	*SMM-code*→*Shielding*→CD
Intel firmware advisory [102]	2026	Intel	*SMM-code*→*Shielding*→CD
AMD embedded CPUs — input validation [31]	2026	AMD	*SMM-code*→[*MS*→[Spatial] |*Shielding*→[CD | SMMCallout]]
AMD embedded CPUs vulnerabilities May [33]	2026	AMD	*SMM-code*→[*MS*→[Spatial] |*Shielding*→[CD | SMMCallout]]
AMD EPYC CPUs — input validation [32]	2026	AMD	*SMM-code*→*Shielding*→CD
Incorrect user of LocateProtocol [34]	2026	AMD	*SMM-code*→*Shielding*→CD
UEFI Reference Firmware Advisory [101]	2026	Intel	*SMM-code*→*Shielding*→CD





Assessment of µarch Leakage Across SMM Transitions





Name	Year	Vulnerability
Foreshadow [95]	2018	*SMM-code* → *Uarch* →*MDS*
MDS [112]	2019	*SMM-code* → *Uarch* →*MDS*
Trust asynchronous abort [111]	2019	*SMM-code* → *Uarch* →*MDS*
Spectre V1/V2 [113]	2021	*SMM-code* → *Uarch* →*Spectre*
MMIO stale data [115]	2022	*SMM-code* → *Uarch* →*MDS*
Branch history injection [114]	2022	*SMM-code* → *Uarch* →*Spectre*
Snoop assisted L1DS [116]	2022	*SMM-code* → *Uarch* →*MDS*
SPD input validation [26]	2025	*SMM-code* → *Uarch* →*BadRAM*





8/57 advisories mention impact on SMM



SMM as a Defensive Substrate

Integration with Confidential VMs, GPU-cc



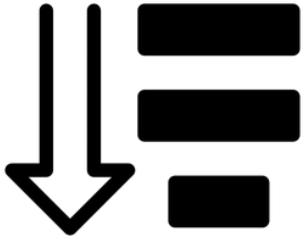
Transparent monitoring

Invisible introspection of the OS and hypervisor



Security services

Secure kernel patching and secure I/O paths for enclaves and confidential VMs



Isolated designs

Reduce dependency on OS or hypervisor



Lessons Beyond x86 Firmware

Lessons Beyond x86 Firmware





Platform configuration

Locking and privilege modes — on every platform





Code vulnerabilities

Memory-safe implementations and SMI handler validation tools



Beyond Intel/AMD

Other x86 vendors ship SMM as well

Takeaways

DATASET & LIVE TABLE



Need for automated tooling

Discovery scales with tooling



Open-source – vague ecosystem

Firmware and defences are closed source



Join forces: industry, academia, hacker community

Joint expertise



HELD IN RESERVE

Backup Slides

Vulnerability column



	Name	Year	Venue
Era 1	SMM OS Security Bypass [62]	2006	CanSecW
	SMM Rootkits [67]	2008	SecureCo
	SMM hacks [45]	2008	Phrack
	Xen Hypervisor Subversion [169]	2008	Black Hat
	SMRAM Access Techniques [132]	2009	CanSecW
	BIOS SMI Rootkit [53]	2009	Phrack
	Attacking Intel TXT [193]	2009	Black Hat
	Attacking Intel BIOS [191]	2009	Black Hat
	SMM CPU Cache Poisoning [194]	2009	White Pap
	Attacking SMM using SINIT [195]	2011	White Pap
	Flea-reflash hopping [48]	2013	ACM CCS
	Insyde SMM Vulnerabilities [72]	2013	NCC Blog
	Sandman [122]	2014	Mitre
	Chipsec [131]	2014	CanSecW
Era 2	SMM Rootkits Revisited [170]	2014	ARES
	Defeating Secure Boot [118]	2014	Syscan
	Defeating Signed BIOS [117]	2014	Blog
	The Watcher [119]	2014	Mitre
	Smite'em MiTM and Copernicus 2 [121]	2014	Mitre
	UEFI Security Attacks [192]	2014	31C3
	Venamis misery [196]	2014	White Pap
	Excite [39]	2015	WOOT
	SMM Backdoor [153]	2015	GitHub
	Attacking VMM through SMM [71]	2015	Black Hat
	SMM Memory Sinkhole [61]	2015	Black Hat
	A Million BIOSes Infected (Lighteater) [55]	2015	HITBSec
	Breaking UEFI Security Using DMA [151]	2015	Blog
	SMI Handler Vulnerabilities [37]	2015	CanSecW
	Aptiocalypsis [154]	2016	Blog
	EDK2 communication [204]	2016	White Pap

2006 Plat-config →FW→Memory-Controller

2008 Concept

2008 Plat-config →FW→Memory-Controller

2008 Plat-config →FW→Memory-Controller

2009 Plat-config →FW→Memory-Controller

2009 Concept

2009 Plat-config →FW→Memory-Controller

2009 SMM-code → Shielding →CD

2009 Plat-config →FW→Memory-Controller

2011 Plat-config →FW→TXT SINIT

2013 Concept

2013 SMM-code →[Shielding →CD | MS →Spatial]

2014 Plat-config →FW→[Memory-Controller | TXT SINIT]

2014 [Plat-config | SMM-code]

2014 Concept

2014 Plat-config →FW→Memory-Controller

2014 SMM-code → MS →Spatial

2014 SMM-code → MS →IntOverflow

2014 [Concept|SMM-code]

2014 [Plat-config →FW→S3BootScript | SMM-code →[Shielding →SMMCallout]]

2014 Plat-config →FW→S3BootScript

2015 SMM-code → Shielding →SMMCallout

2015 Concept

2015 SMM-code → Shielding →CD

2015 Plat-config →HW→APICRemap

2015 SMM-code →[Shielding →SMMCallout | MS →Spatial]

2015 SMM-code → Shielding →CD

2015 SMM-code → Shielding →CD

2016 SMM-code → Shielding →CD

2016 SMM-code → Shielding →[CD | SMMCallout]

2016 SMM-code → Shielding →[CD | SMMCallout]

2016 SMM-code → Shielding →SMMCallout

2017 Plat-config →FW→HotAddFlowDMA

2017 Concept

2017 SMM-code → Shielding →CD→BAR

2017 SMM-code → Shielding →SMMCallout

2017 [Plat-config →FW→Memory-Controller | SMM-code → Shielding →CD]

2017 [Plat-config →[FW→Memory-Controller | S3BootScript] | SMM-code →[Shielding

2017 [Plat-config →FW→Memory-Controller | SMM-code →[Shielding →[CD | SMMCallout] | MS →Spatial]]

2018 SMM-code → Uarch →Spectre

2018 SMM-code → Shielding →SMMCallout

2020 SMM-code →[Shielding →[CD | SMMCallout] | MS →[Temporal | Spatial]]

2020 SMM-code → Shielding →CD

2020 SMM-code →[Shielding →[CD] | MS →Spatial]

2020 SMM-code → Shielding →SMMCallout

2022 SMM-code → Shielding →CD

2022 [Plat-config →[FW→Memory-Controller]]

2022 SMM-code →[Shielding →[CD | SMMCallout] | MS →Spatial]

2022 SMM-code → Shielding →[SMMCallout | CD]

2022 SMM-code →[Shielding →[CD | SMMCallout] | MS →Spatial]

2022 Concept

2022 SMM-code →[Shielding →[CD | SMMCallout] | MS →[Spatial | IntOverflow]]

2022 Plat-config →FW→Memory-Controller

2022 SMM-code →[Shielding →[CD | SMMCallout] | MS →Spatial]

2022 SMM-code →[Shielding →[CD | SMMCallout] | MS →Spatial]

2022 SMM-code →[Shielding →CD]

2022 Concept

2022 SMM-code →[Shielding →[CD | SMMCallout] | MS →Spatial]

2023 [SMM-code →[Shielding →CD]]

2023 SMM-code →[MS →[Spatial | Temporal] | Shielding →[CD | SMMCallout]]

2023 SMM-code →[MS →Spatial | Shielding →CD]

2023 Plat-config →FW→Memory-Controller

2023 SMM-code →[Shielding →CD]

2024 SMM-code

2024 SMM-code → Shielding →CD

2024 Plat-config →FW→PSBStatus

2025 SMM-code →[MS →[Spatial | Temporal] | Shielding →CD]

2025 SMM-code →[MS →[Spatial | Temporal] | Shielding →[CD | SMMCallout]]

2026 SMM-code →[MS →[Spatial | Temporal] | Shielding →[SMMCallout]]

	Name	Year	Venue	Vulnerability	Src	E2E	Auto
ERA 1	SMM OS Security Bypass[67]	2006	CanSecWest	Plat-config →FW→Memory-Controller	◐	○	○
	SMM Rootkits[72]	2008	SecureComm	Concept	○	●	○
	SMM hacks[48]	2008	Phrack	Plat-config →FW→Memory-Controller	●	●	○
	Xen Hypervisor Subversion[174]	2008	Black Hat	Plat-config →FW→Memory-Controller	◐	○	○
	SRAM Access Techniques[136]	2009	CanSecWest	Plat-config →FW→Memory-Controller	○	○	○
	BIOS SMI Rootkit[57]	2009	Phrack	Concept	●	◐	○
	Attacking Intel TXT[204]	2009	Black Hat	Plat-config →FW→Memory-Controller	○	●	○
	Attacking Intel BIOS[202]	2009	Black Hat	SMM-code → Shielding →CD	○	○	○
	SMM CPU Cache Poisoning[205]	2009	White Paper	Plat-config →FW→Memory-Controller	○	●	○
	Attacking SMM using SINIT[206]	2011	White Paper	Plat-config →FW→TXT SINIT	○	●	○
	Flea-reflash hopping[51]	2013	ACM CCS	Concept	○	●	○
	Insyde SMM Vulnerabilities[77]	2013	NCC Blog	SMM-code →[Shielding →CD | MS →Spatial]	○	○	○
	Sandman[125]	2014	Mitre	Plat-config →FW→[Memory-Controller | TXT SINIT]	○	◐	○
	Chipsec[134]	2014	CanSecWest	[Plat-config | SMM-code]	●	○	●
ERA 2	SMM Rootkits Revisited[176]	2014	ARES	Concept	○	○	○
	Defeating Secure Boot[121]	2014	Syscan	Plat-config →FW→Memory-Controller	○	◐	○
	Defeating Signed BIOS[120]	2014	Blog	SMM-code → MS →Spatial	○	●	○
	The Watcher[122]	2014	Mitre	SMM-code → MS →IntOverflow	[179]	●	○
	Smite'em MiTM and Copernicus 2[124]	2014	Mitre	[Concept | SMM-code]	[80]	◐	●
	UEFI Security Attacks[203]	2014	31C3	[Plat-config →FW→S3BootScript | SMM-code →[Shielding →SMMCallout]]	○	●	○
	Venamis misery[207]	2014	White Paper	Plat-config →FW→S3BootScript	[156]	●	○
	Excite[43]	2014	WOOT	SMM-code → Shielding →SMMCallout	○	○	●
	SMM Backdoor[157]	2015	GitHub	Concept	●	○	○
	Attacking VMM through SMM[76]	2015	Black Hat	SMM-code → Shielding →CD	○	○	●
	SMM Memory Sinkhole[66]	2015	Black Hat	Plat-config →HW→APICRemap	◐	●	○
	A Million BIOSes Infected (Lighteater)[60]	2015	HITBSecConf	SMM-code →[Shielding →SMMCallout | MS →Spatial]	○	●	○
	Breaking UEFI Security Using DMA[155]	2015	Blog	SMM-code → Shielding →CD	○	●	●
	SMI Handler Vulnerabilities[41]	2015	CanSecWest	SMM-code → Shielding →CD	○	○	●
	Aptiocalypsis[158]	2016	Blog	SMM-code → Shielding →CD	[159]	●	●
	EDK2 communication[215]	2016	White Paper	SMM-code → Shielding →[CD | SMMCallout]	○	○	○
	ThinkPwn/SmmRuntime[161]	2016	Blog	SMM-code → Shielding →[CD | SMMCallout]	[162]	●	●
	Exploiting SMM callout vulnerabilities[160]	2016	Blog	SMM-code → Shielding →SMMCallout	○	●	●
	SMM Data Centers[93]	2017	CanSecWest	Plat-config →FW→HotAddFlowDMA	○	●	○
	LONGKIT Framework[170]	2017	ICISSP	Concept	○	○	○
	BARing the System[50]	2017	RECON	SMM-code → Shielding →CD→BAR	○	●	●
	BIOS holes. Don't Come Inside[70]	2017	Black Hat	SMM-code → Shielding →SMMCallout	[71]	●	●
	Digging Into the Core of Boot[49]	2017	RECON	[Plat-config →FW→Memory-Controller | SMM-code → Shielding →CD]	○	○	●
	Exploring Your System Deeper[42]	2017	CanSecWest	[Plat-config →[FW→Memory-Controller | S3BootScript] | SMM-code →[Shielding →CD]]	●	○	●
	UEFI firmware rootkits[137]	2017	Black Hat	[Plat-config →FW→Memory-Controller | SMM-code →[Shielding →[CD | SMMCallout] | MS →Spatial]]	○	●	○
	SMM Spectre v1[69]	2018	Blog	SMM-code → Uarch →Spectre	●	●	●
	Code Check(mate)[167]	2018	Blog	SMM-code → Shielding →SMMCallout	◐	◐	●
	efiXplorer[138]	2020	Black Hat	SMM-code →[Shielding →[CD | SMMCallout] | MS →[Temporal | Spatial]]	[44]	○	●
ERA 3	Attacking the golden ring[151]	2020	Blog	SMM-code → Shielding →CD	●	●	○
	Firmware Fuzzing using Simics[208]	2020	DAC	SMM-code →[Shielding →[CD] | MS →Spatial]	○	○	●
	SMRAM Callout Vulnerability[168]	2020	Blog	SMM-code → Shielding →SMMCallout	◐	◐	●
	SPENDER[219]	2022	IEEE S&P	SMM-code → Shielding →CD	○	○	●
	SPI Write Protections[38]	2022	Blog	[Plat-config →[FW→Memory-Controller]]	○	○	●
	HP Repeatable Failures[185]	2022	Blog	SMM-code →[Shielding →[CD | SMMCallout] | MS →Spatial]	●	●	●
	AMI Repeatable Failures[184]	2022	Blog	SMM-code → Shielding →[SMMCallout | CD]	○	●	●
	23 High-Impact Vulnerabilities[183]	2022	Blog	SMM-code →[Shielding →[CD | SMMCallout] | MS →Spatial]	●	○	●
	UDK-Based SMM Rootkits[81]	2022	Blog	Concept	[82]	◐	○
	SMM Supervisor Security[193]	2022	Hardwear.io	SMM-code →[Shielding →[CD | SMMCallout] | MS →[Spatial | IntOverflow]]	○	◐	○
	AMD platform Security[144]	2022	IOActive Blog	Plat-config →FW→Memory-Controller	●	●	●
	BIOS Past, Present, Future[45]	2022	Black Hat	SMM-code →[Shielding →[CD | SMMCallout] | MS →Spatial]	●	●	●
	Breaking firmware trust[139]	2022	Black Hat	SMM-code →[Shielding →[CD | SMMCallout] | MS →Spatial]	○	●	●
	Lenovo High-impact Vulnerabilities[173]	2022	ESET Blog	SMM-code →[Shielding →CD]	◐	●	●
	Simple SMM Rootkit[181]	2022	icWCSN	Concept	●	○	○
	The art of SMM bug hunting[53]	2022	Blog	SMM-code →[Shielding →[CD | SMMCallout] | MS →Spatial]	○	○	●
	Ringhopper[220]	2023	DEF CON	[SMM-code →[Shielding →CD]]	○	●	○
	RSFuzzer[218]	2023	IEEE S&P	SMM-code →[MS →[Spatial | Temporal] | Shielding →[CD | SMMCallout]]	○	○	●
	Ice Lake TOCTOU[78]	2023	NCC Blog	SMM-code →[MS →Spatial | Shielding →CD]	○	○	○
	Back to the Future[146]	2023	IOActive Blog	Plat-config →FW→Memory-Controller	[119]	○	●
	Platform Security Disclosure[145]	2023	IOActive Blog	SMM-code →[Shielding →CD]	[119]	●	●
	Stase[180]	2024	ASE	SMM-code	●	○	●
	AMD Sinkclose[147]	2024	DEF CON	SMM-code → Shielding →CD	[119]	●	●
	AMD Platform Secure Boot[152]	2024	IOActive Blog	Plat-config →FW→PSBStatus	[119]	●	●
	FuzzUEr[75]	2025	NDSS	SMM-code →[MS →[Spatial | Temporal] | Shielding →CD]	●	○	●
	Memory corruption in SMM[199]	2025	Black Hat	SMM-code →[MS →[Spatial | Temporal] | Shielding →[CD | SMMCallout]]	○	○	●
	SmuFuzz[201]	2026	IEEE S&P	SMM-code →[MS →[Spatial | Temporal] | Shielding →[SMMCallout]]	◐	○	●

Vulnerability Analysis

`Plat-config`

FW / HW misconfiguration, before any handler runs

`SMM-code`

Memory safety, µarch and shielding bugs inside the handler

`Concepts`

Capability demonstrated, no concrete class assigned

Three Eras of SMM Offense

ERA 1

Platform configuration

2006

manual RE · platform-specific · few artifacts

↑ CHIPSEC 2014

ERA 2

SMM code

2014

reproducible PoCs · shielding bugs dominate

↑ efiXplorer 2020

ERA 3

Automated discovery

2020 2026

fuzzing · symbolic execution · same bug classes

The Shift from Boot-Time to Run-Time

Era 2	SMM Rootkits Revisited [170]	2014	ARES	*Concept*	○	○	○
	Defeating Secure Boot [118]	2014	Syscan	*Plat-config→FW→Memory-Controller*	○	◐	○
	Defeating Signed BIOS [117]	2014	Blog	*SMM-code→MS→Spatial*	○	●	○
	The Watcher [119]	2014	Mitre	*SMM-code→MS→IntOverflow*	[172]	●	○
	Smite'em MiTM and Copernicus 2 [121]	2014	Mitre	*[Concept ! SMM-code]*	[76]	◐	●
	UEFI Security Attacks [192]	2014	31C3	*[Plat-config→FW→S3BootScript ! SMM-code→[Shielding→SMMCallout]]*	○	●	○
	Venamis misery [196]	2014	White Paper	*Plat-config→FW→S3BootScript*	[152]	●	○
	Excite [39]	2015	WOOT	*SMM-code→Shielding→SMMCallout*	○	○	●
	SMM Backdoor [153]	2015	GitHub	*Concept*	●	○	○
	Attacking VMM through SMM [71]	2015	Black Hat	*SMM-code→Shielding→CD*	○	○	●
	SMM Memory Sinkhole [61]	2015	Black Hat	*Plat-config→HW→APICRemap*	◐	●	○
	A Million BIOSes Infected (Lighteater) [55]	2015	HITBSecConf	*SMM-code→[Shielding→SMMCallout ! MS→Spatial]*	○	○	○
	Breaking UEFI Security Using DMA [151]	2015	Blog	*SMM-code→Shielding→CD*	○	●	●
	SMI Handler Vulnerabilities [37]	2015	CanSecWest	*SMM-code→Shielding→CD*	○	○	●
	Aptiocalypsis [154]	2016	Blog	*SMM-code→Shielding→CD*	[155]	●	●
	EDK2 communication [204]	2016	White Paper	*SMM-code→Shielding→[CD ! SMMCallout]*	○	○	○
	ThinkPwn/SmmRuntime [157]	2016	Blog	*SMM-code→Shielding→[CD ! SMMCallout]*	[158]	●	●
	Exploiting SMM callout vulnerabilities [156]	2016	Blog	*SMM-code→Shielding→SMMCallout*	○	●	●
	SMM Data Centers [89]	2017	CanSecWest	*Plat-config→FW→HotAddFlowDMA*	○	●	○
	LONGKIT Framework [165]	2017	ICISSP	*Concept*	○	○	○
	BARing the System [47]	2017	RECON	*SMM-code→Shielding→CD→BAR*	○	●	●
	BIOS holes. Don't Come Inside [65]	2017	Black Hat	*SMM-code→Shielding→SMMCallout*	[66]	●	●
	Digging Into the Core of Boot [46]	2017	RECON	*[Plat-config→FW→Memory-Controller ! SMM-code→Shielding→CD]*	○	○	●
	Exploring Your System Deeper [38]	2017	CanSecWest	*[Plat-config→[FW→Memory-Controller ! S3BootScript] ! SMM-code→[Shielding→CD]]*	●	○	●
	UEFI firmware rootkits [133]	2017	Black Hat	*SMM-code→Shielding→CD*	○	●	○
	SMM Spectre v1 [64]	2018	Blog	*SMM-code→Uarch→Spectre*	●	●	●
	Code Check(mate) [162]	2018	Blog	*SMM-code→Shielding→SMMCallout*	◐	◐	●
	efiXplorer [134]	2020	Black Hat	*SMM-code→[Shielding→[CD ! SMMCallout] ! MS→[Temporal ! Spatial]]]*	[42]	○	●

KEY DISTINCTIONS

- **Shielding** becomes the dominant class — confused deputy and SMM callouts, over and over.
- **Memory safety** enters the record: spatial errors and integer overflows inside the handler.
- *Plat-config* (blue) thins out as platforms ship stricter initialisation.
- The root changes: *SMM-code* replaces *Plat-config* as the common prefix.
- efiXplorer (2020) automates callout discovery — the closing marker of the era.

Same Classes, Now Found by Tooling

Era 3	Attacking the golden ring [147]	2020	Blog	*SMM-code→Shielding→CD*	●	●	○
	Firmware Fuzzing using Simics [197]	2020	DAC	*SMM-code→[Shielding→[CD] | MS→Spatial]*	○	○	●
	SMRAM Callout Vulnerability [163]	2020	Blog	*SMM-code→Shielding→SMMCallout*	◐	◐	●
	SPENDER [208]	2022	IEEE S&P	*SMM-code→Shielding→CD*	○	○	●
	SPI Write Protections [34]	2022	Blog	*[Plat-config→[FW→Memory-Controller]]*	○	○	●
	HP Repeatable Failures [178]	2022	Blog	*SMM-code→[Shielding→[CD | SMMCallout] | MS→Spatial]*	●	●	●
	AMI Repeatable Failures [177]	2022	Blog	*SMM-code→Shielding→[SMMCallout | CD]*	○	●	○
	23 High-Impact Vulnerabilities [176]	2022	Blog	*SMM-code→[Shielding→[CD | SMMCallout] | MS→Spatial]*	●	○	●
	UDK-Based SMM Rootkits [77]	2022	Blog	*Concept*	[78]	◐	○
	SMM Supervisor Security [185]	2022	Hardwear.io	*SMM-code→[Shielding→[CD | SMMCallout] | MS→Spatial]*	○	◐	○
	AMD platform Security [140]	2022	IOActive Blog	*Plat-config→FW→Memory-Controller*	●	●	●
	BIOS Past, Present,Future [43]	2022	Black Hat	*SMM-code→[Shielding→[CD | SMMCallout] | MS→Spatial]*	●	●	●
	Breaking firmware trust [135]	2022	Black Hat	*SMM-code→[Shielding→[CD | SMMCallout] | MS→Spatial]*	○	●	●
	Lenovo High-impact Vulnerabilities [168]	2022	ESET Blog	*SMM-code→[Shielding→CD]*	◐	●	●
	Simple SMM Rootkit [174]	2022	icWCSN	*Concept*	●	○	○
	The art of SMM bug hunting [50]	2022	Blog	*SMM-code→[Shielding→[CD | SMMCallout] | MS→Spatial]*	○	○	●
	Ringhopper [209]	2023	DEF CON	*[SMM-code→[Shielding→CD]]*	○	●	○
	RSFuzzer [207]	2023	IEEE S&P	*SMM-code→[MS→[Spatial | Temporal] | Shielding→[CD | SMMCallout]]*	○	○	●
	Ice Lake TOCTOU [73]	2023	NCC Blog	*SMM-code→[MS→Spatial | Shielding→CD]*	○	○	○
	Back to the Future [142]	2023	IOActive Blog	*Plat-config→FW→Memory-Controller*	[114]	○	●
	Platform Security Disclosure [141]	2023	IOActive Blog	*SMM-code→[Shielding→CD]*	[114]	●	●
	Stase [173]	2024	ASE	*SMM-code*	●	○	●
	AMD Sinkclose [143]	2024	DEF CON	*SMM-code→Shielding→CD*	[114]	●	●
	AMD Platform Secure Boot [148]	2024	IOActive Blog	*Plat-config→FW→PSBStatus*	[114]	●	●
	FuzzUEr [70]	2025	NDSS	*SMM-code→[MS→[Spatial | Temporal] | Shielding→CD]*	●	○	●
	Memory corruption in SMM [190]	2025	Black Hat	*SMM-code→[MS→[Spatial | Temporal] | Shielding→[CD | SMMCallout]]*	○	○	●

KEY DISTINCTIONS

Shielding and **memory safety** repeat year after year with little variation — neither class is being retired.

— The automation column fills in: fuzzers and static analysis at scale (RSFuzzer, FuzzUEr, Stase).

— Discovery follows tooling, not new attacker capability.

— *Plat-config* reappears — on AMD, fifteen years after the same bugs on Intel.

BACKUP

What SMM Compromise Buys

CAPABILITY	CONSEQUENCE
OS & hypervisor subversion	invisible escalation, keylogging
SPI flash writes	survives reinstall and disk swap
Boot script manipulation	defeats measured launch
Authenticated variable tampering	signed settings rewritten from inside

BACKUP

Who Does What

COMMUNITY	CONTRIBUTES	PUBLISHES AS
Hackers	discovery, exploitation, disclosure	talks, blogs
Vendors	hardening, containment, tooling	closed firmware
Academia	program analysis for handlers	papers, tools often unreleased

> Open frameworks and shared datasets are the bridge.

BACKUP

SMM as a Defensive Substrate

Introspection

Integrity monitoring of OS and hypervisor from beneath them

Security services

Secure I/O to enclaves, live kernel patching

Pre-SGX TEE

Early Intel research used SMM as a trusted execution environment

Open question

How does this compose with confidential VMs and GPU CC?