Universitat Politècnica de Catalunya

Facultad de Informática de Barcelona

Malware i Arquitectures Emergents: El Cas de RISC-V

Sistemes Operatius 2

Autors

Nicolas Llorens

21/11/2024

Índex

1 Introducció **2**

2 Les noves arquitectures **2**
2.1 Context històric 2
2.2 RISC-V 3

3 Anàlisi de l'afirmació **3**
3.1 Arguments a favor 3
3.2 Arguments en contra 4
3.3 Evidències de malware en RISC-V 4

4 Implicacions per la seguretat **5**

5 Podria existir una arquitectura lliure de malware? **5**

6 Conclusions **6**

1 Introducció

En l'era digital actual, la seguretat informàtica ha esdevingut una prioritat fonamental tant per a les institucions públiques com per a les empreses privades. El desenvolupament d'arquitectures més segures ha estat una resposta a l'augment de les amenaces cibernètiques, entre les quals destaquen el malware, el ransomware i altres formes de programari maligne. En aquest context, l'arquitectura RISC-V ha emergit com una opció prometedora pel seu disseny obert, flexible i altament personalitzable.

RISC-V s'ha posicionat com una alternativa viable a les arquitectures propietàries, com x86 i ARM, proporcionant una base per al desenvolupament de processadors oberts i adaptables a necessitats específiques. No obstant això, aquest caràcter obert també planteja preguntes crítiques sobre la seva seguretat. Una de les afirmacions que ha generat debat és la idea que

L'objectiu d'aquest treball és avaluar la veracitat de l'afirmació: "el malware no existeix per a arquitectures noves com RISC-V". Per assolir aquest objectiu, es proporcionarà un context general sobre les noves arquitectures noves més enllà de x86, es prendrà RISC-V com a referència d'aquestes arquitectures per tal d'explorarar les característiques de seguretat i examinar les evidències existents sobre la presència de malware en aquesta arquitectura. A més, s'analitzaran les implicacions potencials d'aquestes evidències per a la seguretat de sistemes futurs.

El treball està estructurat de la següent manera: primer, es proporcionarà una visió general de les noves arquitectures, el perquè de la seva creació i les seves característiques clau. Es farà una petita introducció a RISC-V en concret. Seguidament, s'examinarà l'afirmació sobre la inexistència de malware en aquesta arquitectura, analitzant els arguments a favor i en contra. Posteriorment, es presentaran evidències i estudis de cas que puguin validar o refutar l'afirmació. Finalment, es discutiran les implicacions per a la seguretat i es presentaran les conclusions generals del treball.

2 Les noves arquitectures

2.1 Context històric

Les arquitectures de processadors han evolucionat al llarg dels anys amb l'objectiu de millorar el rendiment, l'eficència, la compatibilitat i la seguretat dels sistemes computacionals. Entre les arquitectures més destacades es troben x86 i ARM, que han dominat el mercat des de fa dècades.

L'arquitectura x86, desenvolupada per Intel a finals dels anys 70, es va convertir en un estàndard per als PCs i servidors. La seva compatibilitat retroactiva amb versions anteriors i el gran ecosistema de programari desenvolupat per a aquesta arquitectura van ser claus per al seu èxit. No obstant això, la seva complexitat creixent i l'augment de vulnerabilitats de seguretat, com ara *Spectre* i *Meltdown* Kocher et al., 2019; Lipp et al., 2018, han portat a la recerca d'alternatives més segures.

Per la seva banda, ARM es va popularitzar principalment en dispositius mòbils com gràcies a la seva eficiència energètica. A diferència de x86, ARM es basa en un model

de llicència, on les empreses poden dissenyar els seus propis processadors a partir de la seva arquitectura bàsica. Això ha permès la creació de processadors personalitzats per a telèfons, tauletes i dispositius IoT, el gran exemple d'éxit d'aquesta arquitectura ha estat el canvi que va fer Apple amb els seus processadors M (per ordinadors i tauletes) trencant la seva relació amb intel i l'ús de x86 a dissenyar els seus propis processadors fent ús de l'arquitectura ARM . Malgrat els seus avantatges, també s'han identificat vulnerabilitats de seguretat crítiques en aquests dispositius.

Aquest context posa en relleu la necessitat d'explorar noves arquitectures com RISC-V, que ofereixen una alternativa oberta, flexible i potencialment més segura, ja que el seu codi font és accessible per a tothom i permet auditories independents. L'història d'aquestes arquitectures servirà com a punt de partida per avaluar la presència de malware en plataformes emergents com RISC-V.

2.2 RISC-V

Reduced Instruction Set Computing V (RISC-V) és una arquitectura de conjunt d'instruccions (ISA) oberta i lliure que permet a qualsevol persona dissenyar, implementar i fabricar processadors personalitzats. Creada el 2010 a la Universitat de Califòrnia, Berkeley, RISC-V es va concebre amb l'objectiu de proporcionar una alternativa simplificada, eficient i flexible a les arquitectures tancades de les que s'han introduit abans.

El seu disseny modular permet afegir extensions personalitzades al conjunt d'instruccions bàsic, fet que la fa adequada per a una àmplia gamma d'aplicacions, des de dispositius IoT fins a supercomputadors. L'obertura d'aquesta arquitectura permet auditar-ne el codi font i millorar-ne la seguretat, ja que les vulnerabilitats poden ser detectades i corregides per la comunitat.

El caràcter obert de RISC-V ha generat interès tant en la indústria com en la comunitat acadèmica. Grans empreses tecnològiques, com Google, NVIDIA i Western Digital, han adoptat aquesta arquitectura en alguns dels seus projectes. Tot i això, la seva adopció massiva també pot atraure l'interès d'actors maliciosos, ja que, lógicament, la popularitat sovint està correlacionada amb l'augment d'atacs de malware.

3 Anàlisi de l'afirmació

L'afirmació que "el malware no existeix per a arquitectures noves com RISC-V"és, en certa manera, una afirmació controvertida i discutible. Si bé és cert que les arquitectures menys populars tenen menys atacs de malware reportats, això no implica la seva invulnerabilitat. De fet, la seguretat d'una arquitectura depèn de molts factors, incloent-hi el seu disseny, la seva implementació i el seu ecosistema de programari.

3.1 Arguments a favor

Baixa popularitat: Una de les raons per les quals podria semblar que no existeix malware per a RISC-V és la seva menor popularitat en comparació amb arquitectures com x86

o ARM. Com que menys dispositius utilitzen RISC-V, els atacants poden preferir centrar els seus esforços en objectius més comuns.

Seguretat per transparència: Ser una arquitectura de codi obert també pot ser un avantatge significatiu per a la seguretat. La comunitat global pot auditar el codi de manera oberta, identificant i solucionant vulnerabilitats abans que siguin explotades. A diferència de les arquitectures propietàries, on els errors poden romandre ocults fins que són explotats per atacants, el model obert de RISC-V promou la col·laboració i la millora contínua.

Modularitat i personalització: La capacitat d'adaptar l'arquitectura a necessitats específiques permet implementar mecanismes de seguretat personalitzats que poden dificultar la propagació de malware estàndard. Això redueix la superfície del atac.

3.2 Arguments en contra

Arquitectura oberta: Tot i que el codi obert pot ser un avantatge, també proporciona als atacants la mateixa capacitat per analitzar-lo i trobar vulnerabilitats explotables. Això pot suposar un risc si les vulnerabilitats no són detectades i corregides a temps.

Codi personalitzat: Les empreses que implementen extensions personalitzades poden introduir vulnerabilitats no detectades inicialment, que podrien ser explotades per atacants amb coneixement suficient de l'arquitectura.

Malware multiplataforma: Ja existeixen exemples de malware dissenyat per executar-se en diverses arquitectures, com es el cas de *Meltdown* Lipp et al., 2018 que es afectava tant a x86 com a ARM.

Increment de popularitat: Amb l'adopció creixent de RISC-V per part de grans empreses tecnològiques, és només qüestió de temps abans que aquesta arquitectura esdevingui un objectiu atractiu per a actors maliciosos.

3.3 Evidències de malware en RISC-V

Tot i la relativa novetat de RISC-V, ja s'han publicat estudis que demostren la possibilitat d'atacs de malware en aquesta arquitectura. Per exemple, *GhostWrite* Thomas et al., 2024 afirma:LLa vulnerabilitat de GhostWrite afecta les CPU T-Head XuanTie C910 i C920 RISC-V. Aquesta vulnerabilitat permet als atacants sense privilegis, fins i tot als que tenen un accés limitat, llegir i escriure qualsevol part de la memòria de l'ordinador i controlar dispositius perifèrics com targetes de xarxa. GhostWrite fa que les funcions de seguretat de la CPU siguin ineficaces i no es poden arreglar sense desactivar al voltant de la meitat de la funcionalitat de la CPU."

Aquesta vulnerabilitat és l'exemple de l'argument en contra de la afirmació mencionat a la secció 3.2 *Codi personalitzat*, les extensions personalitzades poden introduir vulnerabilitats potencials. A més, tot i ser una vulnerabilitat causada per l'extensió que ha fet l'empresa chinesa T-Head, les CPU que mencionen són les dues CPU més rapides disponibles al mercat en arquitectura RISC-V, és a dir, no es una vulnerabilitat d'una branca de RISC-V feta per qualsevol, sinó d'una empresa consolidad i amb un equip tècnic capaç. Això doncs, posa en vista que RISC-V no és una arquitectura invulnerable.

4 Implicacions per la seguretat

Les implicacions de les vulnerabilitats detectades en RISC-V són significatives per a la seguretat. En primer lloc, la flexibilitat de l'arquitectura, un dels seus punts forts, també pot esdevenir un desavantatge si no s'implementen mecanismes rigorosos per verificar i auditar extensions personalitzades. Les empreses que dissenyen modificacions específiques poden crear punts d'entrada per a atacants, com es va demostrar amb GhostWrite.

A més, l'obertura de RISC-V, tot i facilitar auditories públiques, també proporciona als atacants accés al disseny complet de l'arquitectura, cosa que pot accelerar el descobriment de vulnerabilitats. Això posa en relleu la necessitat de protocols de desenvolupament robustos, amb controls rigorosos per validar tant el maquinari com el programari associat.

Per garantir una seguretat òptima, cal promoure la col·laboració entre desenvolupadors, la comunitat acadèmica i la indústria per identificar i mitigar proactivament els riscos. Això inclou la creació d'estàndards globals i frameworks de seguretat que integrin eines per avaluar la resistència d'extensions personalitzades a atacs potencials.

5 Podria existir una arquitectura lliure de malware?

Tot i que en teoria es podria imaginar una arquitectura lliure de malware, en la pràctica és un objectiu gairebé impossible d'assolir. Les vulnerabilitats poden sorgir per diverses raons: errors humans durant el disseny i implementació, limitacions intrínseques en la verificació de seguretat, o la contínua evolució de tècniques d'atac.

Per exemple, arquitectures totalment tancades podrien reduir la superfície d'atac, però sacrificarien la flexibilitat i la innovació. D'altra banda, arquitectures obertes, com RISC-V, permeten auditories externes però també ofereixen més informació als atacants.

La clau, potser, no rau en crear una arquitectura completament invulnerable, sinó en dissenyar sistemes resilients que puguin detectar, mitigar i recuperar-se d'atacs. Això inclou implementar mecanismes proactius com:

- Monitoratge constant i actualitzacions de seguretat.
- Sandboxing i aïllament de processos.
- Verificació formal per identificar vulnerabilitats abans del desplegament.

6 Conclusions

Aquest treball ha explorat l'afirmació sobre la inexistència de malware en arquitectures emergents com RISC-V, aportant evidències que demostren que, tot i la seva menor popularitat i disseny obert, aquesta arquitectura no és invulnerable. La vulnerabilitat *GhostWrite* posa de manifest que les extensions personalitzades poden introduir riscos significatius, i que l'obertura de RISC-V, si bé afavoreix l'auditoria i la innovació, també ofereix oportunitats per a atacants.

En un context on la seguretat és una prioritat creixent, RISC-V representa un punt d'inflexió en la manera de concebre i implementar arquitectures de processadors. La seva flexibilitat i el suport de la comunitat la converteixen en una opció prometedora, però només amb estàndards rigorosos i col·laboració internacional es podrà garantir una seguretat robusta.

Finalment, s'ha destacat que, si bé una arquitectura totalment lliure de malware pot ser una utopia, és essencial centrar els esforços en el desenvolupament de sistemes resilients capaços de resistir, detectar i mitigar atacs de manera eficient. Per tant, el que es busca d'una arquitectura es una seguretat óptima, més que la útopia de la seguretat completa. RISC-V ofereix una oportunitat única per avançar en aquesta direcció, establint les bases d'un futur més segur i colaboratiu en el món de la computació.

Referències

Computerphile. (2023). *How Branch Prediction Works in CPUs*. Consultat el 14 de desembre de 2024, a partir de https://www.youtube.com/watch?v=nczJ58WvtYo

Harris, S. L. (2023). RISC-V System-on-Chip Design: Wally Open-Source RISC-V Core & SoC with Accompanying Textbook [Consultat el 14 de desembre de 2024]. https://web.fdi.ucm.es/posgrado/conferencias/SarahHarris-slides.pdf

Kocher, P., Horn, M., Daniel Genkin, Fogh, M., Moritz Lipp, Gruss, D., Yarom, Y., & Hamburg, Y. (2019). Spectre Attacks: Exploiting Speculative Execution. *Proceedings of the IEEE Symposium on Security and Privacy*, 1 - 19. https://doi.org/10.1109/SP.2019.00002

Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Fogh, A., & Mangard, S. (2018). Meltdown: Reading Kernel Memory from User Space. *Proceedings of the 27th USENIX Security Symposium*, 973 - 990. https://www.usenix.org/conference/usenixsecurity18/presentation/lipp

Thomas, F., Hetterich, L., Zhang, R., Weber, D., Gerlach, L., & Schwarz, M. (2024). RISCVuzz: Discovering Architectural CPU Vulnerabilities via Differential Hardware Fuzzing.

Xataka. (2024). *A RISC-V le ha salido un aliado inesperado: NVIDIA ha producido 1.000 millones de núcleos de este tipo*. Consultat el 15 de desembre de 2024, a partir de https://www.xataka.com/empresas-y-economia/a-risc-v-le-ha-salido-aliado-inesperado-nvidia-ha-producido-1-000-millones-nucleos-este-tipo-2024