APPLIED COMPUTER SCIENCE

Applied Computer Science, vol. 18, no. 2, pp. 86–100
doi: 10.35784/acs-2022-15

Submitted: 2022-04-24 | Revised: 2022-06-08 | Accepted: 2022-06-08

Keywords: RowHammer, Cyber Security, DRAM

Hakan AYDIN [0000-0002-0122-8512]*, *Ahmet SERTBAŞ* [0000-0001-8166-1211]**

CYBER SECURITY IN INDUSTRIAL CONTROL SYSTEMS (ICS): A SURVEY OF ROWHAMMER VULNERABILITY

Abstract

Increasing dependence on Information and Communication Technologies (ICT) and especially on the Internet in Industrial Control Systems (ICS) has made these systems the primary target of cyber-attacks. As ICS are extensively used in Critical Infrastructures (CI), this makes CI more vulnerable to cyber-attacks and their protection becomes an important issue. On the other hand, cyberattacks can exploit not only software but also physics; that is, they can target the fundamental physical aspects of computation. The newly discovered RowHammer (RH) fault injection attack is a serious vulnerability targeting hardware on reliability and security of DRAM (Dynamic Random Access Memory). Studies on this vulnerability issue raise serious security concerns. The purpose of this study was to overview the RH phenomenon in DRAMs and its possible security risks on ICSs and to discuss a few possible realistic RH attack scenarios for ICSs. The results of the study revealed that RH is a serious security threat to any computer-based system having DRAMs, and this also applies to ICS.

1. INTRODUCTION

The industry 4.0 concept represents the new industrial revolution, which aims to bring together Information Technologies (IT) and Industry. This concept has enabled the inclusion of Cyber-Physical Systems (CPSs) in production systems. CPS is defined as integrations of computation, communication, and control to achieve the desired performance from physical processes (Mahmoud & Hamdan, 2019). Examples of CPSs include smart grids, autonomous car systems, medical monitoring, Industrial Control Systems (ICSs), robotic systems, and autopilot avionics projects (Khaitan & McCalley, 2014). CPS is often associated with the Industry 4.0 perspective (Carvajal, Rojas & Chacón, 2018; Johari et al., 2022; Lieu et al., 2019) and it is one of the underlying forces of Industry 4.0. Today, CPS, and thus Industry 4.0, seems to be promising in terms of producing new solutions, improving resource usage, and increasing efficiency. The most common example of CPSs is ICS, which is widely used in almost every Critical Infrastructure (CI) (Lu et al., 2014). Cyber security incidents that may occur in ICSs involve risks of causing large scale economic damage, loss of life,

[*] Istanbul Topkapı University, Faculty of Engineering, Istanbul, Turkey, hakanaydin@topkapi.edu.tr
[**] Istanbul University-Cerrahpasa, Faculty of Engineering, Istanbul, Turkey, asertbas@iuc.edu.tr

and even damage to national security. The integration of CI into public networks exposes the underlying ICS to a various attack vector (Zimba, Wang & Chen, 2018). According to Kaspersky ICS CERT (Industrial control systems threat medley: spyware and malicious scripts on the rise in H1 2021, 2021), almost one in three industrial computers is subject to malicious activity as shown in Figure 1.

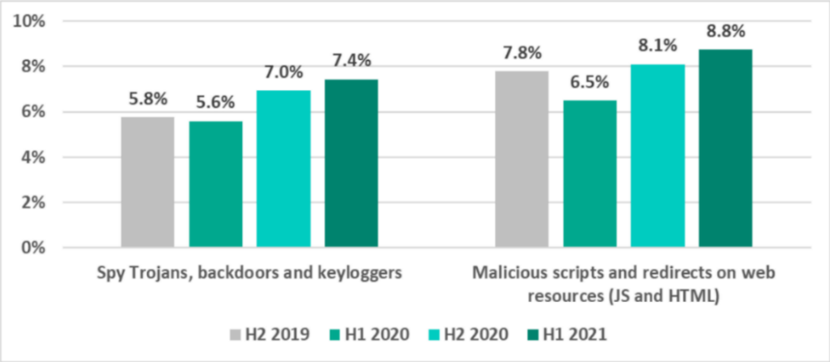

Fig. 1. Percentage of ICS computers on which malicious objects were blocked

However, cyber-attacks target not only software but also hardware. That is, such attacks also target the fundamental physical aspects of computing. Rowhammer (RH) is a fault injection attack targeting hardware on reliability and security of Dynamic Random Access Memory (DRAM). This security exploit targets DRAM, in which memory cells interact among themselves, by changing the contents of adjacent memory rows that are not addressed in the original memory access. RH was first introduced at the ISCA 2014 conference (Kim et al., 2014). RH bug occurs in most of today's memory modules and has destructive consequences for the security of all affected systems (e.g., privilege escalation attacks) (Gruss, Maurice & Mangard, 2016). It is stated that 85% of the DDR3 memories are vulnerable to RH (Kim et al., 2014). Today's DRAMs, including DDR4, are also vulnerable to RH (Cojocar et al., 2014; Gruss et al., 2018).

The purpose of this study is to provide an overview of RH, highlight the security risks that this vulnerability can pose to ICSs, and present a few realistic RH attack scenarios for ICSs. The scenarios described in this study are presented for the first time. For the purpose of the study, two basic questions are tried to be answered:

1. How can the RH cyber threat be evaluated within the scope of cyber security of ICSs?
2. What is the possible RH cyberattacking scenarios? The descriptive method was used in the research.

The contributions of this study to the literature can be expressed as follows:

- A comprehensive cybersecurity analysis of the RH problem is investigated within the scope of ICS cybersecurity.
- For the first time, several realistic RH attack scenarios and countermeasures for cybersecurity of ICSs are presented.

In the remaining of this article, a literature review on the related studies is presented in the 2nd section, while CPS & ICS and RH are overviewed in the 3rd section. RH attack scenarios are presented in the 4th section. Finally, in the 5th section, the study is concluded, and some ideas for future studies are explained.

2. LITERATURE REVIEW

The RH problem was first raised by Kim et al. (2014). By conducting experimental studies on Intel (Sandy Bridge, Ivy Bridge, and Haswell) and AMD (Piledriver) systems using 2GB DDR3 modules, they showed that activating the same row in DRAM repeatedly corrupted the data in rows near this row. In addition, they proved in their study that up to 139K accesses were required to cause RH vulnerability and that up to one in every 1.7K cell was prone to errors. The authors proposed a low-cost solution to the RH problem they identified in their study. In the study conducted by Razavi et al. (2016), Flip Feng Shui (FFS) was presented as a new exploit vector that allowed an attacker to initiate random bit flips on physical memory in a completely controlled manner. By implementing an instance using the RH bug and memory deduplication, the authors showed that FFS was possible with very few constraints on the target data. They showed that FFS is extremely powerful; that is, a malicious VM in a practical cloud setting can gain unauthorized access to a co-hosted victim VM running OpenSSH. Using FFS, they exemplified end-to-end attacks breaking OpenSSH public-key authentication and forging GPG signatures from trusted keys, thereby compromising the Ubuntu/Debian update mechanism. Bosman et al. (2016) showed that a JavaScript-enabled attacker could use it to generate the RH exploit. The authors demonstrated in their study that random memory read/write access is possible with a modern Microsoft Edge browser. Gruss et al. (2016) showed that a fully automated attack through a website containing Javascript triggers failures on remote hardware. They showed that caches could be forced into fast cache eviction to trigger the RH bug with only regular memory accesses. Tatar et al. (2016) revealed that an attacker could trigger and exploit RH bitflips directly from a remote machine by only sending network packets. This is made possible by RDMA-enabled networks, which are widely used in clouds and data centers and are becoming increasingly fast. To demonstrate the threat, they showed how a malicious client could exploit RH bit flips to gain code execution on a remote key value server application. To counter this threat, they proposed protecting unmodified applications with a new buffer allocator that could achieve fine-grained memory isolation in the DRAM address space. Aweke et al. (2016) presented a software-based defense, ANVIL, which can block all known RH attacks on existing systems. ANVIL detects RH attacks by tracking the locality of DRAM accesses using existing hardware performance counters. The detector identifies the rows that are frequently accessed (i.e., the aggressors) and then selectively refreshes the nearby victim rows to prevent hammering. Experiments conducted on real hardware with the SPEC2006 benchmarks have shown that ANVIL has less than a 1% false-positive rate and an average slowdown of 1%. Aweke et al. (2016) also claimed that ANVIL is an effective approach for protecting existing and future systems from even advanced RH attacks. In a study conducted by Aga et al. (2017), a virtual-memory-based cache-flush free attack was enabled by the Cache Allocation Technology, a mechanism designed in part to protect virtual machines from denial-of-service (DOS) attacks. In the study of Bhattacharya & Mukhopadhyay (2018), a methodology combining timing analysis to perform hammering in a controlled manner for the purpose of creating bitflips in cryptographic keys stored in memory was presented. Barenghi et al. (2018) proposed a methodology to reverse engineer such maps without direct physical probing of the DRAM bus of the target platform. In a study con-ducted by Gruss et al. (2018), a new technique, named opcode flipping, that bypassed recent isolation mechanisms by flipping bits in a predictable and targeted way in user space binaries was proposed. The scholars replaced conspicuous and memory-exhausting spraying and grooming techniques with a novel reliable technique called memory waylaying. They abused Intel SGX to hide the attack entirely from the user and the operating system, making any inspection or detection of the attack infeasible. Cojocar et al. (2020) presented an end-to-end methodology to determine if cloud servers were susceptible to RH. They applied their methodology to three classes of servers from a major cloud provider. Their findings showed that none of the CPU instruction sequences used in previous studies to initiate RH attacks create worst-case DRAM testing conditions. To address this limitation, they developed an instruction sequence that leveraged microarchitectural side effects to hammer DRAM at a near-optimal rate on modern Intel Skylake and Cascade Lake platforms. They also designed a DDR4 fault injector that can reverse engineer row adjacency for any DDR4 DIMM. When applied to their cloud provider's DIMMs, they found that DRAM rows did not always follow a linear map. Hassan et al. (2021) proposed U-TRR, a novel experimental methodology for reverse-engineering Target RowRefresh (TRR), to implement in modern DRAM chips. Farmani et al. (2021) proposed an efficient test framework, called RHAT, to address the detection of RH vulnerable cells, which was very difficult, time-consuming, and expensive. It was stated that RHAT could be used for both manufacturing tests and in-field (deployment) tests. Kim et.al (2020) conducted experimental studies on 1580 DRAM chips (408× DDR3, 652× DDR4, and 520× LPDDR4) out of 300 DRAM modules (60× DDR3, 110× DDR4, and 130× LPDDR4) to reveal how RH affected modern and future devices at the circuit level. Zhang et al. (2022) systematized RH attacks and defenses by focusing on DRAM. Chekole et al. (2017) investigated the applicability of strong counter-measures against memory-safety attacks in the context of realistic ICS. They designed an experimental setup based on Programmable Logic Controller (PLC). Their results showed the security measure was highly effective in detecting memory-safety violations. Peng et al. (2015) presented an ICS-CPS operation dual-loop analysis model (ICONDAM) to be able to analyse human-cyber-physical interdependences of ICSs. According to the ICONDAM, a unified and fusion view for ICS is presented in Figure 2.

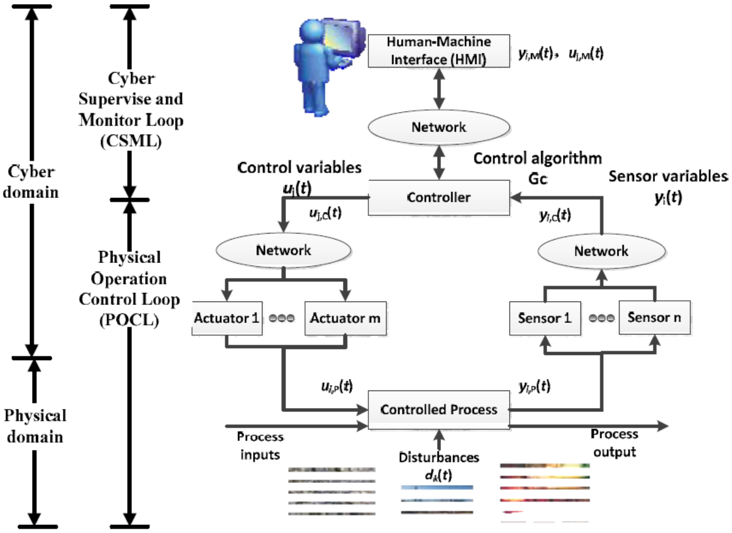

Fig. 2. ICS-CPS operation dual-loop analysis model (Peng et al., 2015)

A summary of the studies reviewed above is presented in Table 1.

Tab. 1. A summary of the studies reviewed

Research	Year	Summary
Kim et al.	2014	RH was first introduced as a failure mechanism in DRAM at the ISCA 2014 conference.
Gruss et al.	2016	It is demonstrated that a remote takeover of a server was vulnerable to RH via JavaScript code execution.
Razavi et al.	2016	It was shown that the victim virtual machine (VM) was hijacked by another attacker VM running on the same system.
Van Der Veen et al.	2016	This study shows that existing mobile systems are widely vulnerable to RH attacks.
Aga et al.	2017	A virtual memory-based non-cache attack, which was fast enough for RH with a double-speed refresh, was presented.
Jang et al.	2017	The Intel Software Guard Extensions (SGX)-Bomb attack that launches the RH attack against enclave memory to trigger the processor lockdown was introduced.
Frigo et al.	2018	Hijacking a mobile system by triggering RH using the WebGL interface on a mobile GPU was studied.
Lipp et al.	2018	The takeover over a remote system by triggering RH through the Remote Direct Memory Access (RDMA) protocol was presented.
Cojocar et al.	2020	In the study, an end-to-end methodology was proposed to determine if cloud servers were susceptible to RH.
Kim et al.	2020	Experimental studies on 1580 DRAM chips (408× DDR3, 652× DDR4, and 520× LPDDR4) out of 300 DRAM modules (60× DDR3, 110× DDR4, and 130× LPDDR4) were conducted. It was definitively shown that new DRAM chips were more vulnerable to RH.
Hassan et al.	2021	U-TRR, which is a novel experimental methodology for the reverse-engineering main RH mitigation mechanism was proposed.
Yağlikçi et al.	2021	BlockHammer, a low-cost, effective, and easy-to-adopt RH mitigation mechanism that prevents all RH bit-flips while overcoming the two key challenges was proposed. The proposed throttling technique selectively throttles memory accesses that could potentially cause RH bit flips.
Farmani et al.	2021	An efficient test framework, called RHAT, which can be employed for both manufacturing tests and in-field (deployment) tests was proposed.
Lee & Kwak	2021	A new attack detection technique, which extracts common features of RH attack files by performing static analysis of the attack codes, was proposed.
Zhang et al.	2022	The authors systematized RH attacks and defenses by focusing on DRAM.

The literature review presented in this study shows that RH is identified as a security threat to any computer-based system with DRAM.

3. BACKGROUND

3.1. An Overview of Industrial Control Systems (ICSs)

CPS refer to a modern system that integrates real-time data and modern Information and Communications Technologies (ICT) into the physical world (Carvajal, Rojas, & Chacón, 2018). In general, a CPS consists of the following elements: Plants, Sensors, PLCs, Actuators, Communication networks, and SCADA (Chekole et al., 2017). CIs, such as the power grid or water distribution network, are CPSs (Friedberg et al., 2017). CPS, which is an integration of computation, networking, and physical processes, plays an increasingly important role in critical infrastructure, government, and everyday life (Ding et al., 2018). ICT is increasingly becoming embedded and pervasive, which leads to CPSs (Chekole et al., 2017). CPS is the basis for the development of the areas such as smart manufacturing, smart medicine, smart buildings and infrastructures, smart city, smart vehicles, wearable devices, mobile systems, defense systems, meteorology, etc. (Figure 3).

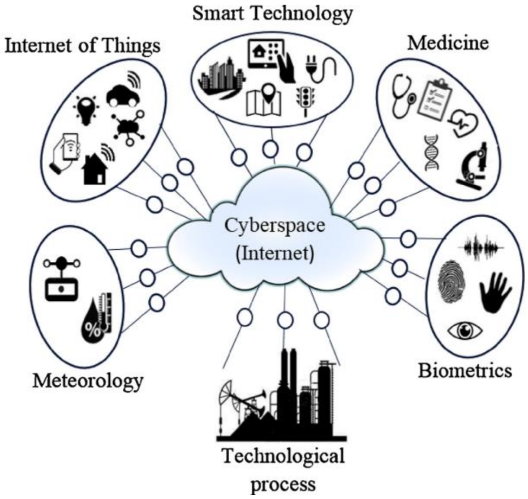

Fig. 3. Cyber-physical systems (Alguliyev, Imamverdiyev & Sukhostat, 2018)

CPS includes ICS (Khaitan & McCalley, 2014). According to Peng et al. (2015), ICSs are CPSs, and they affect the physical world directly. ICSs are used in industry to monitor and control processes related to industrial areas such as water, oil, gas, chemistry, paper, food, beverage, pharmaceutical, petroleum, natural gas pipelines, electrical networks, transportation, and railways. ICSs serve as the basic infrastructure to control or operate any type of industrial system, including those used in CI. ICS is the central nervous system of national critical infrastructures such as power plants, power grids, oil refineries, oil and gas pipelines, chemical plants, urban transport, railways, shipbuilding, and defense (Lu et al., 2014). Moreover, ICS is an all-encompassing term used for various automation systems and their de-vices, such as PLC, Human Machine Interface (HMI), Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Safety Instrumented Systems (SIS), and many others (Figure 4).

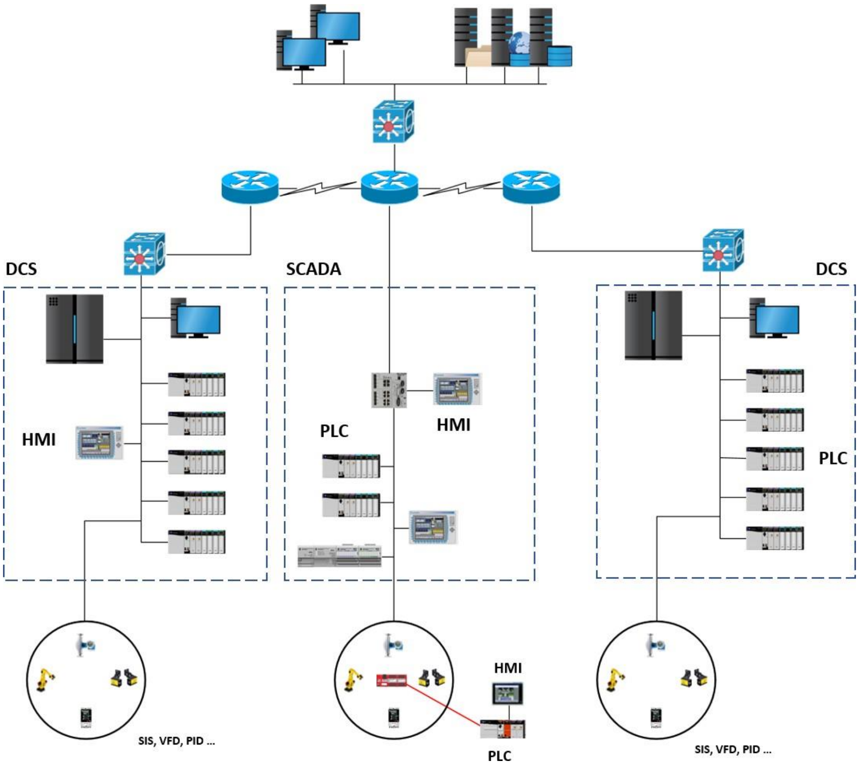

Fig. 4. Industrial Control System (ICS) Components (Ackerman, 2017)

The largest subgroup of ICS is SCADA systems (Stouffer, Falco & Scarfone, 2011). SCADA systems are a type of ICS that provides surveillance and control of a system and is designed to control, manage and monitor systems remotely and automatically. Control systems include SCADA systems that are used to monitor and control various decentralized operations; this actually means that the person who runs it is not physically right next to you (Teixeira et al., 2018). ICS and CI operated via SCADA systems can be shown as examples of operating CPSs through IT infrastructures that ensure timely data transmission between system components (Mahmoud & Hamdan, 2019).

PLC can be defined as automation devices that are generally used in production departments in factories or in the control of processes such as the control of machines. In general, a PLC consists of a Central Processing Unit (CPU), a Memory Unit, an Input Unit, and an Output Unit. A PLC Memory Unit (RAM, ROM, PROM, etc.) is the unit where the specific program used by the PLC is stored. PLC can use RAM, ROM PROM, EPROM, or EEPROM type memories. PLC memories, which are important and inseparable parts of PLC, are Internal and External Memories. The internal memory in the PLC is a type of burner in the user-accessible RAM structure. External memory, on the other hand, is the memory out-side the PLC and is usually of the EPROM or EEPROM type. However, the memory element used more often in PLCs is EPROM. As the name suggests, EPROM stands for erasable programmable read-only memory. On the other hand, DCSs are used to control production systems for industries such as oil refineries, water, and wastewater treatment, electrical power generation plants, and pharmaceutical processing plants.

Today, the increasing dependency of ICS on ICT and especially on the Internet has exposed these systems to cyber-attacks and threats. The interconnection of SCADA systems to various networks has exposed them to network security problems (Igure, Laughter & Williams, 2006). Since ICS is responsible for monitoring and controlling many CIs, a security vulnerability in these systems can cause not only economic damage but also the inability of people to receive critical services that are necessary for their lives and perhaps even loss of life. Cyber-attacks that may occur in ICS systems can cause some problems such as fire and explosion by stopping industrial production facilities in cyberspace, causing system crashes, and making wrong manoeuvres on the systems. As a vital part of CI infrastructure, protecting ICS from cyber threats has become a high priority (Barrère et al., 2020).

Cyber terrorism uses computer systems to shut down or damage critical national infrastructures such as energy, transportation, and state operations and to coerce or intimidate a government or civilian population. Currently, the most famous cyber-attack targeting ICSs is Stuxnet (Yampolskiy et al., 2013). Considering the sectoral distribution of cyber-attacks, it is seen that attacks against the energy sector are in the first place, and these CI hosting ICS/SCADA systems are among the sectors most exposed to cyber-attacks (Ackerman, 2017). ICS typically involve a large spectrum of overlapping cyber-physical security measures used to protect their operational components (Barrère et al., 2020). SCADA and other ICSs continue to present several challenges that make protection of them particularly difficult against determined attackers (Loukas, 2015). Cyberattacks exploiting memory-safety vulnerabilities constitute a major attack vector against CPSs (Chekole et al., 2017). The National Institute of Standards and Technology (NIST) states that possible events an ICS may encounter will include Blocked or delayed flow of information through ICS networks (Bhattacharya & Mukhopadhyay, 2018).

3.2. Rowhammer (RH) Vulnerability

Memory is the key component in computer systems and it is important for short-term data access within a computer. It is the central storage unit of the computer system made up of RAM and ROM, which communicate directly within the CPU, Auxiliary memory, and Cache memory. Computer systems use different memories, and the amount of memory that a computer system uses affects and determines the speed and performance of that system. That is, speed and cost are the two most important parameters of the memory of a computer system. The fastest memory circuits need adding a considerable number of circuits to the main memory, which makes the memory expensive. DRAM and SRAM are fast-speed and volatile memories, while ROM, PROM, EPROM, and EEPROM are non-volatile memories. DRAM capacity has been increased by downsizing it in size, and this scaling has brought more capacity, reasonable energy savings, and lower cost, but has not helped with latency that much. A modern DRAM cell consists of an access transistor and a capacitor (Figure 5).

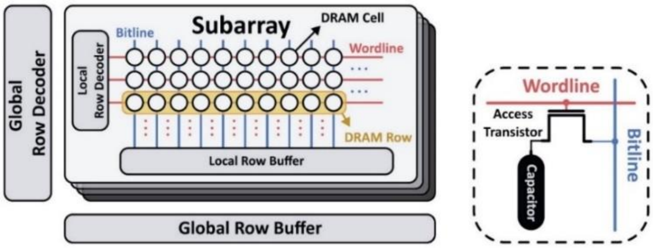

Fig. 5. DRAM bank and cell (Kim et al., 2020)

DRAM failure mode is now popularly called RH (Mutlu & Kim, 2019). A DRAM cell stores a single bit of data based on the charge level of the cell capacitor. But over time, charge leaks appear from the storage capacitor. Repeatedly opening (activating) and closing (pre-charging) a DRAM row causes RH bitflips in nearby cells. To access data on a DRAM row, the memory controller must first activate the DRAM row it wants to reach. Then, to be able to begin accessing data from another DRAM row, the memory controller must close or pre-charge the previous DRAM row. Rapidly activating and pre-charging a DRAM bank may cause bit flips on nearby rows. This phenomenon is known as RH. Shortly, RH is a problem related to some recent DRAM devices in which repeatedly accessing (i.e., hammering) a row of memory can cause bit flips in adjacent rows (Kim et al., 2014; Seaborn & Dullien, 2015; Orosa et al., 2021). It has been demonstrated in the literature that parasitic effects in DRAM can alter the contents of a memory cell without accessing it, but by accessing other memory lo-cations at a high frequency (Gruss et al., 2016). RH has emerged as a vulnerability where repeated ac-cess to a DRAM row could speed up the unloading of neighbouring bits (Aga, Aweke & Austin, 2017). The RH problem enables powerful privilege-escalation attacks by allowing unauthorized changing of bits in DRAM cells (Gruss et al., 2018). This is a classic example of how layered abstractions and trust (in this case, virtual memory) can be broken from a hardware level (Qiao & Seaborn, 2016). In the RH problem, the same address in DRAM is read over and over again and the data at the addresses close to this address is corrupted. Circuit-level charge leakage mechanisms that are exacerbated by certain memory access patterns cause RH bitflips (Cojocar et al., 2020). RH is a prime (and perhaps the first) example of how a circuit-level failure mechanism can cause a practical and widespread system security vulnerability (Mutlu & Kim, 2019).

The potential vulnerabilities of all DRAM types to RH attacks are published by studies related to the security issue. These attacks are a problem that has arisen as a result of DRAM scaling and threaten hardware reliability and security. By a RH attack, it is possible to change the data on the attacked hardware, such as altering existing data or elevating the attacker's privileges. These attacks have become a problem as a result of the gradually shrinking of modern memory cards known as RAM. A study showed that given the number of cores increasing faster than DRAM capacity, the expected memory capacity per core would decrease by 30% every two years (Mutlu & Subramanian, 2015). When scaling the size of the computing system, memory also must be scaled, but this makes the maintenance and enhancement of its capacity, energy efficiency, and reliability significantly costlier than conventional techniques (Mutlu, 2015). RH attacks are about the idea that hardware is not so vulnerable and one can attack hardware by exploiting its vulnerabilities. Hardware-related attacks, such as RH, prompted some researchers to examine hardware issues and focus on other hardware-related issues. An RH attack can control user access and compromise the integrity of sensitive data with attacks such as a privilege escalation and an alteration of the encryption keys (Lee & Kwak, 2021). Kim at al. (2014) showed that a very simple user-level program can also reliably and consistently induce RH errors in AMD and Intel systems that use vulnerable DRAM modules.

3.3. Countermeasures for Rowhammer Vulnerability

As a defense against cyberattacks caused by exploiting the RH vulnerability, manufacturers attempt to improve the hardware's DRAM chips or fix errors using an error-correcting code (ECC). Studies are carried out on efforts for increasing the refresh rate, which is among these defenses. Since DRAMs affected by RH are currently used in the market, it is evaluated that RH attacks should be detected before they occur, and studies are carried out on defense measures against this vulnerability. In their study, Kim et al. (2014) examined seven solutions (Table 2) to tolerate, prevent, or reduce corruption errors. They stated that among these solutions, the seventh and final solution, called PARA, was the most efficient and cost-effective.

Tab. 2. Seven Solutions to Rowhammer (RH) Problem (Kim et al., 2014)

No.	Solution	Summary
1.	Make better chips	The problem can be fixed by manufacturers at the chip level.
2.	Correct errors	It is about employing ECC modules that have extra DRAM chips in server-grade systems. Due to their high cost, ECC modules are rarely used in consumer-grade systems.
3.	Refresh all rows frequently	For sufficiently short refresh intervals, corruption errors can be eliminated.
4.	Retire cells (manufacturer)	Victim cells can be identified and remapped to spare cells by manufacturers before DRAM chips are sold.
5.	Retire cells (end-user)	Modules can be tested by end-users, and system-level methods can be applied by them to struggle with problems
6.	Identify “hot” rows and refresh neighbors.	Refreshing neighbors of frequently opened rows only.
7.	PARA (Probabilistic Adjacent Row Activation) Solution	Refreshing of a given adjacent row with a probability when the row is closed.

Deployed defenses employ two strategies (Aweke et al., 2016): (1) doubling the system DRAM refresh rate and (2) restricting access to the CLFLUSH instruction that attackers use to bypass the cache to in-crease memory access frequency. To address the RH problem, computer and software vendors have: i) doubled DRAM refresh rates, ii) restricted access to virtual-to-physical page mappings, and iii) disabled access to cache-flush operations in sandboxed environments (Aga, Aweke & Austin, 2017). RH is a critical vulnerability and it is important to address and provide solutions to the issues identified in the potential RH scenarios suggested above. Enforcing Error Correction Codes (ECC) protection, increasing the refresh rate of DRAM cells, abolishing the use of DRAM cells that the DRAM manufacturers identify as victim cells, and refreshing vulnerable rows can be shown among the solutions to the RH problem (Kim et al., 2014). Regarding this problem, in their critical security release, Apple has publicly mentioned that they increased the memory refresh rates (Mutlu & Kim, 2019). ANVIL, which ended up as another solution proposal, proposes software-based detection of RH attacks. In this method hardware, performance counters, and selective explicit refreshing of victim rows that are determined to be under attack are monitored (Aweke et al., 2016).

4. CYBER ATTACK SCENARIOS

Considering the RH vulnerability issue as a security threat to ICSs, this section describes the RH exploit attempts against ICSs in five different scenarios as shown in Figure 6.

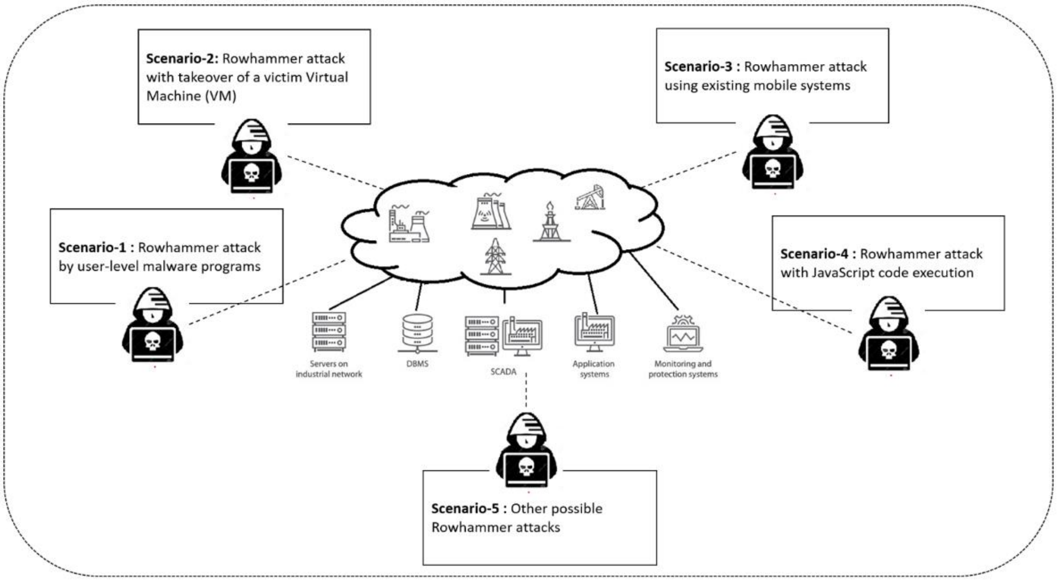
Scenario-2: Rowhammer attack with takeover of a victim Virtual Machine (VM)
Scenario-3 : Rowhammer attack using existing mobile systems
Scenario-1 : Rowhammer attack by user-level malware programs
Scenario-4 : Rowhammer attack with JavaScript code execution
Servers on industrial network
DBMS
SCADA
Application systems
Monitoring and protection systems
Scenario-5 : Other possible Rowhammer attacks

Fig. 6. Row Hammer Attack Scenarios for ICS Security

The first scenario is based on attacking ICS hardware by user-level malware programs. Using malware in cyber-attacks is one of the most typical incidents in practice. RH can be exploited by a user-level malicious program to breach memory protection and compromise the ICS system. The cyber-attacks in this scenario can be carried out by triggering the RH threat with spy trojans, backdoors and keyloggers, malicious scripts, and redirects on web resources (JS and HTML). In the scenario, it is assumed that with some engineering effort, a program is developed that triggers the RH problem, crashing the system or taking control of the system. This scenario is one of the most likely in ICSs since malware programs are designed specifically to target ICSs. The malicious codes can be injected into programs or used to intercept the system control by utilizing a bit flip attack.

The second scenario, a victim virtual machine (VM) is hijacked by another attacker VM running on the same system. Virtualization is one of the most important technology catalysts for the new industrial revolution. Virtualized solutions require fewer physical servers because multiple virtual control functions can be combined on industry-standard hardware along with information technology (IT) and operational technology (OT) functions, rather than deploying each function as a dedicated device. Virtualization enables CI companies to reduce operating costs with secure, robust, flexible software-based solutions as an alternative to legacy, fixed-function hardware. In the case of such an attack, since RH attacks modify memory without writes, the modification cannot be detected, and the victim VM continues to use the corrupted page.

The third scenario is based on the idea that existing mobile systems used in ICSs are widely vulnerable to RH attacks. In this scenario, there is an attack that exploits RH on a mobile device using a malicious user-level application that requires no permissions. This third scenario of our study takes advantage of the deterministic memory allocation patterns in the Android Linux Operating System. In this RH attack scenario, which is not based on software vulnerability and does not require user permission, an Android-based root exploit is used.

The fourth scenario is based on the idea that an RH attack can be launched by a website to gain root privileges on an ICS that uses or visits the website. In this scenario, the RH attack is initiated by a website to gain root privileges on an ICS system that uses or visits the website via JavaScript. In the scenario, a server vulnerable to RH is taken over remotely via JavaScript code execution. Since JavaScript is available and enabled by default in every modern browser, this fourth attack can be launched by a web-site to gain root privileges on a system that visits the website. Since this type of attack, which can be done through a website, can be carried out simultaneously and secretly on ICSs, it creates a huge security threat. In this scenario, the fully automated attack runs in JavaScript through a remote website and can gain unrestricted access to systems. As a result of this attack, unlimited access to the systems of website visitors can be achieved.

The fifth scenario is based on the idea that different types of RH attacks can be carried out by cyber attackers, especially on ICS components. Many studies in the literature show other practical hacks using this fault injection attack. In this context, it can be said that new types of RH attacks targeting ICSs can be carried out by cyber attackers, except for the attack scenarios specifically mentioned above.

5. CONCLUSION

In this study, after an overview of the phenomenon of RowHammer (RH) in DRAMs, RH induced security risks to ICSs, and scenarios for possible RH attacks targeting ICSs were discussed. In this context, the RH security exploits that take advantage of an unintended and undesirable side effect in DRAM were presented as a security threat to ICSs. The overview of the RH problem in DRAMs, ways to induce it, countermeasure techniques against it, and the possible attack scenarios discussed in the paper were adopted from the studies published in the literature. It is seen in this study that the RH problem is identified as a security threat to any computer-based system with DRAMs. This is also important in terms of computer architecture because modern computer architecture also aims to design secure computer hardware that can prevent and be immune to cyber-attacks. It is an inevitable fact that even a simple hardware failure mechanism at the circuit level will endanger the security of the entire system. Even though ICSs generally use industry-standard computers, today they have begun to resemble classical computer systems in terms of operating systems, network protocols, remote access capabilities, wireless networking, etc. Different units of ICSs, such as SCADA, HMI, and PLC, contain DRAM. In this respect, RH vulnerability also arises as a security threat to ICSs, as in any other cyber-physical system with DRAMs. This study can inspire many researchers to take RH into account in studies to be conducted to identify new attacks that may be carried out against CPSs.

For future studies, we plan to perform some of the RH attack scenarios described in this study in a real ICS simulation test environment and evaluate their results.

REFERENCES

Ackerman, P. (2017). *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*. Packt Publishing Ltd.

Aga, M. T., Aweke, Z. B., & Austin, T. (2017). When good protections go bad: Exploiting anti-DoS measures to accelerate Rowhammer attacks. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* (pp. 8–13). IEEE. https://doi.org/10.1109/HST.2017.7951730

Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security is-sues. *Computers in Industry*, *100*, 212-223. https://doi.org/10.1016/j.compind.2018.04.017

Aweke, Z. B., Yitbarek, S. F., Qiao, R., Das, R., Hicks, M., Oren, Y., & Austin, T. (2016). ANVIL: Soft-ware-based protection against next-generation Rowhammer attacks. *ACM SIGPLAN Notices*, *51*(4), 743–755. https://doi.org/10.1145/2954679.2872390

Barenghi, A., Breveglieri, L., Izzo, N., & Pelosi, G. (2018). Software-only reverse engineering of physical DRAM mappings for RowHammer attacks. In *2018 IEEE 3rd International Verification and Security Workshop (IVSW)* (pp. 19–24). IEEE. https://doi.org/10.1109/IVSW.2018.8494868

Barrère, M., Hankin, C., Nicolaou, N., Eliades, D. G., & Parisini, T. (2020). Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies. *Journal of information security and applications, 52,* 102471. https://doi.org/10.1016/j.jisa.2020.102471

Bhattacharya, S., & Mukhopadhyay, D. (2018). Advanced fault attacks in software: Exploiting the RowHammer bug. In *Fault Tolerant Architectures for Cryptography and Hardware Security* (pp. 111–135). Springer. https://doi.org/10.1007/978-981-10-1387-4_6

Bosman, E., Razavi, K., Bos, H., & Giuffrida, C. (2016). Dedup est machina: Memory deduplication as an advanced exploitation vector. In *2016 IEEE symposium on security and privacy* (SP) (pp. 987–1004). IEEE. https://doi.org/10.1109/SP.2016.63

Carvajal, J. H., Rojas, O. A., & Chacón, E. (2018). Cyber-physical system for industrial control automation based on the holonic approach and the IEC 61499 standard. In *2018 Forum on Specification & Design Languages (FDL)* (pp. 5–16). IEEE. https://doi.org/10.1109/FDL.2018.8524082

Chekole, E. G., Castellanos, J. H., Ochoa, M., & Yau, D. K. (2017). Enforcing memory safety in cyber-physical systems. *In Computer security* (pp. 127–144). Springer. https://doi.org/10.1007/978-3-319-72817-9_18

Cojocar, L., Kim, J., Patel, M., Tsai, L., Saroiu, S., Wolman, A., & Mutlu, O. (2020). Are we susceptible to Rowhammer? An end-to-end methodology for cloud providers. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 712–728). IEEE. https://doi.org/10.1109/SP40000.2020.00085

Ding, D., Han, Q. L., Xiang, Y., Ge, X., & Zhang, X. M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, *275,* 1674–1683. https://doi.org/10.1016/j.neucom.2017.10.009

Farmani, M., Tehranipoor, M., & Rahman, F. (2021). RHAT: Efficient RowHammer-Aware Test for Modern DRAM Modules. In *2021 IEEE European Test Symposium (ETS)* (pp. 1–6). IEEE. https://doi.org/10.1109/ETS50041.2021.9465436

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2017). STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of information security and applications, 34,* 183–196. https://doi.org/10.1016/j.jisa.2016.05.008

Frigo, P., Giuffrida, C., Bos, H., & Razavi, K. (2018). Grand pawning unit: Accelerating microarchitectural attacks with the GPU. In *2018 IEEE Symposium on Security and Privacy* (sp) (pp. 195–210). IEEE. https://doi.org/10.1109/SP.2018.00022

Gruss, D., Lipp, M., Schwarz, M., Genkin, D., Juffinger, J., O'Connell, S., Yarom, Y. (2018). An-other flip in the wall of Rowhammer defenses. In *2018 IEEE Symposium on Security and Privacy* (SP) (pp. 245–261). IEEE. https://doi.org/10.1109/SP.2018.00031

Gruss, D., Maurice, C., & Mangard, S. (2016). Rowhammer. js: A remote software-induced fault attack in JavaScript. In *International conference on detection of intrusions and malware, and vulnerability assessment* (pp. 300–321). Springer. https://doi.org/10.1007/978-3-319-40667-1_15

Hassan, H., Tugrul, Y. C., Kim, J. S., Van der Veen, V., Razavi, K., & Mutlu, O. (2021). Uncovering In-DRAM RowHammer Protection Mechanisms: A New Methodology, Custom RowHammer Patterns, and Implications. In *MICRO-54: 54th Annual IEEE/ACM International Symposium on Microarchitecture* (pp. 1198–1213). https://doi.org/10.1145/3466752.3480110

Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security*, *25*(7), 498–506. https://doi.org/10.1016/j.cose.2006.03.001

Industrial control systems threat medley: spyware and malicious scripts on the rise in H1 2021. (2021). *Kaspersky*. Retrieved April 8, 2022 from https://www.kaspersky.com/about/press-releases/2021_industrial-control-systems-threat-medley-spyware-and-malicious-scripts-on-the-rise-in-h1-2021

Jang, Y., Lee, J., Lee, S., & Kim, T. (2017). SGX-Bomb: Locking down the processor via Row-hammer attack. In *Proceedings of the 2nd Workshop on System Software for Trusted Execution* (pp. 1–6). https://doi.org/10.1145/3152701.3152709

Johari, R., Kaur, A., Hashim, M., Rai, P. K., & Gupta, K. (2022). SEVA: Secure E-Voting Application in Cyber Physical System. *Cyber-Physical Systems*, *8*(1), 1–31. https://doi.org/10.1080/23335777.2020.1837250

Khaitan, S. K., & McCalley, J. D. (2014). Design techniques and applications of cyberphysical systems: A survey. *IEEE Systems Journal*, *9*(2), 350-365. https://doi.org/10.1109/JSYST.2014.2322503

Kim, J. S., Patel, M., Yağlıkçı, A. G., Hassan, H., Azizi, R., Orosa, L., & Mutlu, O. (2020). Revisiting Rowhammer: An experimental analysis of modern dram devices and mitigation techniques. In *2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)* (pp. 638–651). IEEE. https://doi.org/10.1109/ISCA45697.2020.00059

Kim, Y., Daly, R., Kim, J., Fallin, C., Lee, J. H., Lee, D., Mutlu, O. (2014). Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors. *ACM SIGARCH Computer Architecture News*, *42*(3), 361–372. https://doi.org/10.1145/2678373.2665726

Lee, M., & Kwak, J. (2021). Detection Technique of Software-Induced Rowhammer Attacks. *CMC-Computers Materials & Continua*, *67*(1), 349–367.

Lieu Tran, T. B., Törngren, M., Nguyen, H. D., Paulen, R., Gleason, N. W., & Duong, T. H. (2019). Trends in preparing cyber-physical systems engineers. *Cyber-Physical Systems*, *5*(2), 65–91. https://doi.org/10.1080/23335777.2019.1600034

Lipp, M., Schwarz, M., Raab, L., Lamster, L., Aga, M. T., Maurice, C., & Gruss, D. (2020). Nethammer: Inducing Rowhammer faults through network requests. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 710–719). IEEE. https://doi.org/10.1109/EuroSPW51379.2020.00102

Loukas, G. (2015). Cyber-physical attacks on industrial control systems. In *Cyber-Physical Attacks* (pp. 105–144). Elsevier.

Lu, T., Guo, X., Li, Y., Peng, Y., Zhang, X., Xie, F., & Gao, Y. (2014). Cyberphysical security for industrial control systems based on wireless sensor networks. *International Journal of Distributed Sensor Networks*, *10*(6), 438350. https://doi.org/10.1155/2014/438350

Mahmoud, M. S., & Hamdan, M. M. (2019). Improved control of cyber-physical systems subject to cyber and physical attacks. *Cyber-Physical Systems*, *5*(3), 173–190. https://doi.org/10.1080/23335777.2019.1631889

Mutlu, O. (2015). Main memory scaling: Challenges and solution directions. In *More than Moore technologies for next generation computer design* (pp. 127–153). Springer. https://doi.org/10.1007/978-1-4939-2163-8_6

Mutlu, O., & Kim, J. S. (2019). Rowhammer: A retrospective. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *39*(8), 1555–1571. https://doi.org/10.1109/TCAD.2019.2915318

Mutlu, O., & Subramanian, L. (2014). Research problems and opportunities in memory systems. *Supercomputing frontiers and innovations*, *1*(3), 19–55.

Orosa, L., Yaglikci, A. G., Luo, H., Olgun, A., Park, J., Hassan, H., & Mutlu, O. (2021). A Deeper Look into RowHammer's Sensitivities: Experimental Analysis of Real DRAM Chips and Implications on Future Attacks and Defenses. In *MICRO-54: 54th Annual IEEE/ACM International Symposium on Microarchitecture* (pp. 1182–1197). https://doi.org/10.1145/3466752.3480069

Peng, Y., Wang, Y., Xiang, C., Liu, X., Wen, Z., Chen, D., & Zhang, C. (2015). Cyber-physical attack-oriented Industrial Control Systems (ICS) modeling, analysis and experiment environment. In *2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)* (pp. 322–326). IEEE. https://doi.org/10.1109/IIH-MSP.2015.110

Qiao, R., & Seaborn, M. (2016). A new approach for Rowhammer attacks. In *2016 IEEE international symposium on hardware oriented security and trust (HOST)* (pp. 161–166). IEEE. https://doi.org/10.1109/HST.2016.7495576

Razavi, K., Gras, B., Bosman, E., Preneel, B., Giuffrida, C., & Bos, H. (2016). Flip feng shui: Hammering a needle in the software stack. In *25th USENIX Security Symposium (USENIX Security 16)* (pp. 1–18). USENIX Association.

Seaborn, M., & Dullien, T. (2015). Exploiting the DRAM Rowhammer bug to gain kernel privileges. *Black Hat*, *15*, 71.

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), 16–16.

Tatar, A., Konoth, R. K., Athanasopoulos, E., Giuffrida, C., Bos, H., & Razavi, K. (2018). Throwhammer: Rowhammer attacks over the network and defenses. In *2018 USENIX Annual Technical Conference (USENIX ATC 18)* (pp. 213–226). USENIX Association.

Teixeira, M. A., Salman, T., Zolanvari, M., Jain, R., Meskin, N., & Samaka, M. (2018). SCADA system testbed for cybersecurity research using machine learning approach. *Future Internet*, *10*(8), 76. https://doi.org/10.3390/fi10080076

Van Der Veen, V., Fratantonio, Y., Lindorfer, M., Gruss, D., Maurice, C., Vigna, G.& Giuffrida, C. (2016). Drammer: Deterministic rowhammer attacks on mobile platforms. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 1675–1689). https://doi.org/10.1145/2976749.2978406

Yağlikçi, A. G., Patel, M., Kim, J. S., Azizi, R., Olgun, A., Orosa, L., & Mutlu, O. (2021). Blockhammer: Preventing Rowhammer at low cost by blacklisting rapidly-accessed dram rows. In *2021 IEEE International Symposium on High-Performance Computer Architecture (HPCA)* (pp. 345–358). IEEE. https://doi.org/10.1109/HPCA51647.2021.00037

Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y., & Sztipanovits, J. (2013). Taxonomy for description of cross-domain attacks on CPS. In *Proceedings of the 2nd ACM international conference on High confidence networked systems* (pp. 135-142). ACM Digital Library https://doi.org/10.1145/2461446.2461465

Zhang, Z., Qi, J., Cheng, Y., Jiang, S., Lin, Y., Gao, Y., & Zou, Y. (2022). A Retrospective and Future-spective of Rowhammer Attacks and Defenses on DRAM. *arXiv preprint arXiv:2201.02986*. https://doi.org/10.48550/arXiv.2201.02986

Zimba, A., Wang, Z., & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *ICT Express*, *4*(1), 14–18. https://doi.org/10.1016/j.icte.2017.12.007