Memory Encryption: A Survey of Existing Techniques

MICHAEL HENSON and[1] STEPHEN TAYLOR, Dartmouth College

DARTMOUTH TECH REPORT: TR13-001
(submitted to ACM computing surveys)

Abstract

Memory Encryption (ME) has yet to be used at the core of operating system designs to provide confidentiality of code and data. As a result, numerous vulnerabilities exist at every level of the software stack. Three general approaches have evolved to rectify this problem. The most popular approach is based on complex *hardware enhancements*; this allows all encryption and decryption to be conducted within a well-defined trusted boundary. Unfortunately, these designs have not been integrated within commodity processors and have primarily been explored through simulation with very few prototypes. An alternative approach has been to augment existing hardware with *operating system enhancements* for manipulating keys, providing improved trust. This approach has provided insights into the use of encryption but has involved unacceptable overheads and has not been adopted in commercial operating systems. Finally, *specialized industrial devices* have evolved, potentially adding coprocessors, to increase security of particular operations in specific operating environments. However, this approach lacks generality and has introduced unexpected vulnerabilities of its own. Recently, memory encryption primitives have been integrated within commodity processors such as the Intel i7, AMD bulldozer, and multiple ARM variants. This opens the door for new operating system designs that provide confidentiality across the entire software stack outside the CPU. To date, little practical experimentation has been conducted and the improvements in security and associated performance degradation has yet to be quantified. This article surveys the current memory encryption literature from the viewpoint of these central issues.

Categories and Subject Descriptors: B.3.m [Hardware]: Memory Structures-*Miscellaneous*; C.1.0 [Processor Architectures]: *General*; C.4 [Computer Systems Organization]: Performance of Systems-*Reliability, availability, and serviceability*; D.4.2 [Operating Systems]: Storage Management-*Main memory*

General Terms: Design, Experimentation, Performance, Security

Additional Key Words and Phrases: Secure processors, memory encryption, confidentiality, protection, hardware attacks, software attacks

Background and Motivation

[1] This material is based on research sponsored by the Defense Advanced Research Projects Agency (DARPA) under agreement number FA8750-09-1-0213.

Encryption has been an important part of secure computing for decades, first in the DoD and national agencies and then publicly beginning with DES and public-key encryption in 1977 [Mel et al. 2001]. As public use of computers continued to grow, so did the need to secure sensitive information. In 1991, Phil Zimmerman released the first version of Pretty Good Privacy (PGP) allowing anyone to encrypt e-mail and files. In 1995, Netscape developed the secure sockets layer (SSL) protocol combining public and private-key encryption to protect online financial transactions.

Full disk encryption (FDE) in commodity computer systems is a more recent innovation that provides confidentiality of all data stored on disk. Recent advances to the overall speed of processors, thanks to the march of Moore's law, and hardware-based encryption have resulted in several commercially viable FDE implementations. Software approaches to FDE include TrueCrypt, PGPDisk, FileVault, and Bitlocker. In addition, multiple hard drive manufacturers offer self-encrypting drives (SED) in which encryption is handled entirely by the hard drive microcontroller. Several factors have resulted in increasing adoption of FDE technologies [Brink 2009]. Regulations, such as Sarbanes-Oxley and the Health Insurance Portability and Accountability Act (HIPAA), have increased the requirement for privacy. The advent of mobile computing and widespread movement of information over the Internet have raised concerns regarding physical access to data. Finally, numerous data breaches have been publicized raising awareness of vulnerabilities.

Unfortunately, even with FDE, systems exhibit a major weakness in that data and code stored in memory are unencrypted (i.e. stored in the clear) as shown in Figure 1. This weakness has been exploited to gather encryption keys, passwords, passphrases, and other personal information from memory, thereby diminishing, or in some cases nullifying, the value of FDE [Halderman et al. 2008]. Since code is also stored in memory, it is possible to inject a wide variety of malicious implants into both user process and operating system kernels. Even applications designed specifically with security in mind have been shown to be vulnerable. For example, cryptographic libraries have been designed to prevent access to keys by zeroizing (or overwriting with zeros) a key after it has been used. This zeroizing of code is sometimes removed by compiler optimization because it appears superfluous, re-introducing the vulnerability [Chow et al. 2004].

To exploit memory vulnerabilities, numerous attack vectors have been developed. In a cold boot attack, for example, memory is frozen using a refrigerant and then removed from the computer. It is then quickly placed into a specially designed system that reads out its content, targeting encryption keys and other sensitive information. While this approach is novel, the idea of recovering encryption keys from memory has been described as early as 1998 [Kaplan 2007]. Even without cooling, some information persists in RAM for several minutes [Halderman et al. 2008]. However, cooling slows down the rate of data loss, reducing recovery errors [Chhabra 2011b]. Some approaches, such as the DMA-firewire attack, deliberately bypass full disk encryption to enable forensic analysis. Unfortunately, these techniques are equally accessible to criminal organizations and other attackers as well as legitimate law enforcement. Similar results

are available via simple software attacks involving buffer overflows [Rabaiotti et al. 2010]. One particularly effective attack, bus-snooping and injecting, allows information to be captured or inserted via the bus lines between system components [Boileau 2006]. This exploitation method has been used to undermine the Xbox gaming system. This system was specifically designed to provide a secure chain of trust for enforcing digital rights management (DRM). Bus-snooping was used to capture keys as they transited between read-only-memory and the CPU. These keys were then used to decrypt the secure boot loader undermining the entire chain of trust. Subsequently, low-cost "mod" chips were developed that can be soldered into the gaming system bus, allowing a user to bypass DRM restrictions and play pirated games [Steil 2005]. Alternatively, the same chips can be used to run various operating systems on the gaming system allowing it to be used for illicit purposes [Rabaiotti et al. 2010].

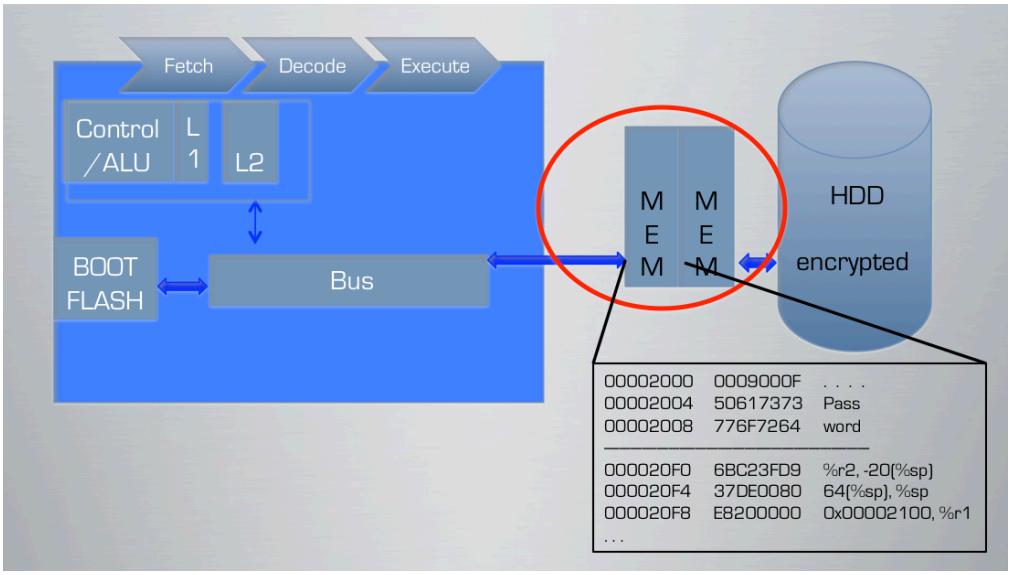

Figure 1: System with Full Disk Encryption but Vulnerable Code and Data.

Fortunately, access to information in conventional dynamic RAM presents an adversary with only a *fleeting* opportunity to obtain sensitive information between power cycles. However, dynamic RAM is being augmented or replaced with new non-volatile alternatives -- flash memory, magnetic RAM, and ferro-electric RAM -- which provide several benefits including energy efficiency and tolerance of power failure. Flash memory has been used to augment traditional RAM in the Vista and Windows 7 "ready boost" feature, whereas the other two technologies are potential RAM replacements. Unfortunately, these non-volatile memories allow information and attacks to *persist* indefinitely [Enck et al. 2008]. Interestingly, Microsoft has anticipated the security issues associated with persistent memory and designed the ready boost feature to encrypt all contents of flash making it difficult for forensics investigators to recover useful data [Hayes et al. 2009]. If these memories are adopted in future architectures, without adequate attention to encryption, there is the potential that memory based attacks will become more prevalent.

In effect, FDE has pushed the vulnerabilities associated with persistent data stored on disk down into the next level of the memory hierarchy, which has proven equally

vulnerable. The key concept by which vulnerabilities were mitigated on disk was encryption: encrypting the disk provided confidentiality preventing access to sensitive information. By migrating the same solution down into RAM, it will be possible to circumvent similar attacks at this lower level of the memory hierarchy.

The typical *threat model* assumed in the memory encryption literature involves hardware and/or software attack. Attackers are often assumed to have physical access to the vulnerable system where sensitive information can be captured in various ways. The primary goal of attackers is to steal secret information or code. Memory modification is sometimes discussed but usually as a means to force a system to leak confidential information. Examples of these attackers range from those motivated by financial gain such as bank employees capturing ATM pin numbers, criminals copying and distributing software (digital rights management), to those motivated by more nefarious goals such as reverse engineering or stealing intelligence from autonomous military vehicles.

Software attacks involve corrupt processes or the operating system itself. Since the OS typically controls memory arbitration, it must either be trusted and considered part of the trusted computing base (TCB) or dealt with in another way. This is handled in different ways in the literature with many adding a secure, trusted kernel to the list of assumptions of the work. Other approaches include only hardware in the TCB, treating the OS as any other untrusted process. A hybrid approach includes some portion of a trusted kernel or a trusted hypervisor along with hardware support.

One of the main assumptions in the ME literature is that the processor provides a natural boundary within which sensitive information can reside—it is a fundamental component of the TCB in most approaches. All components outside of the processor are assumed to be vulnerable to include RAM and its interconnections (data and address bus), other I/O devices, etc. Most schemes attempt to protect RAM and the data bus, and several also target the address bus [Duc and Keryell 2006], [Dallas 1997] while other external components are not normally considered. A subset of the memory encryption literature additionally adds the cache-to-cache connections as a consideration when protecting multiprocessor systems.

While the security of systems employing memory encryption is enhanced, attacks on the devices are still possible, by etching away the chip walls with acid to reveal internal bus lines for microprobing, or electromagnetic and power analyses among other side channels [Ravi et al. 2004]; [Kocher et al. 1999]. For systems relying on *software based encryption*, key expansion tables (e.g. AES) are subject to cache attacks; a malicious process tracks and times cache accesses [Osvik et al. 2005], [Mowery et al. 2012]. The typical target of all of these attacks is the encryption key hidden within the chip boundary. Most of these approaches increase the attacker workload by an order of magnitude, require expert knowledge, and cannot be exploited remotely over a network [Suh et al. 2007]. Moreover, while tamper resistant mechanisms are already available that significantly increase the barrier to entry [Chari et al. 1999], protecting circuits from invasive and side-channel attacks is an open research area that is not addressed in the main body of memory encryption literature. Protections such as FDE are equally

available to criminals and well-intentioned users [Casey et al. 2011]. Disk encryption has been used to protect information on criminal activity and prevent successful prosecution. Some of the techniques identified to aid law enforcement (e.g. DMA-firewire attack) in the capture of key material on suspect machines would be thwarted by memory encryption—memory encryption could be used to further protect criminal activity. This paper explores efforts to realize protection of confidentiality through memory encryption in the context of next generation operating systems.

Full Memory Encryption in Operating Systems Design

In general, encryption is used to provide four basic properties of protection: *confidentiality*, *integrity*, *authentication*, and *non-repudiation*. In trusted computing and operating system security these properties are realized through *authenticated booting*, ensuring that program code is not changed before it is loaded into memory, *memory authentication*, ensuring that program code is not changed during use, and *attestation*, ensuring that hardware and software have not been altered. Trusted software components, which make up part of the trusted computing base (TCB), are booted and verified producing a *chain of trust*, without which the security mechanisms could be compromised before the system is initialized. While a few of the works discuss the implementation of these other mechanisms, most assume that these components are functional and focus on the overhead of ME in the steady-state. Other important assumptions often include mechanisms for secure code delivery, key creation and escrow, inter-process communication, and I/O protection among others. Memory authentication is often closely associated with memory encryption solutions; however, a thorough survey of memory authentication mechanisms is available [Elbaz et al. 2009].

Memory encryption is solely concerned with the *confidentiality* of data and code during execution, with the express purpose of increasing attacker workload associated with crafting exploits and stealing sensitive information. It is interesting to note, however, that memory encryption would also hamper attempts to inject code, generally assumed to require memory authentication. An adversary lacking an encryption key would be unable to successfully change an encrypted binary, as decryption would result in corrupt code and likely program termination [Barrantes et al. 2003]. Early work associated with full memory encryption (FME) was dominated by the desire to provide digital rights management and in particular to prevent the theft of intellectual property associated with program source code. This is still the primary purpose in some systems (e.g. gaming systems), but more recently these techniques have become recognized as a method for removing vulnerabilities and protecting system users.

There are two general approaches to providing confidentiality with encryption that are commonly used in computer architectures based on *symmetric* or *public* key encryption techniques. Symmetric key encryption, based on a shared secret (key), is generally held to be more efficient (i.e. on the order of 1,000 times faster) but does not provide non-repudiation and requires a non-trivial trusted key distribution scheme [Kaplan 2007]. Three common algorithms are typically used to realize this approach based on DES, Triple-DES, and AES. Public-key encryption involves the use of two interlocking keys,

one held privately and the other published, from which all four properties of protection, including non-repudiation, can be realized. This scheme has the advantage that public keys can be distributed across open networks. A broad variety of books are available that describe these core ideas, [Mel et al. 2001] is particularly accessible. In light of the speed and complexity involved in public key encryption, it is unsurprising that the memory encryption literature typically uses symmetric key cryptography. However, delivery of encrypted code over the network may be facilitated using the public key model [Kgil et al. 2005].

Unfortunately, computer users have consistently demonstrated an aversion to any form of increased response time, even when associated with increased security. Studies suggest that delays of longer than 150 ms are perceptible to users [Muller et al. 2011]. Full disk encryption has only become viable because overheads have been reduced to acceptable levels. Achieving similar levels of acceptable performance for memory encryption offers a far more significant challenge: there is an existing, growing, and well-documented speed-gap between processors and memory – improvements in processor speed are outpacing improvements in memory speed by an average of 18% per year [Hennessy et al. 2006]. Adding encryption latency to this already strained interface may require an overhaul of the basic fetch-decode-execute cycle employed by processors.

Added to the complexities of any memory encryption solution is the fact that, unlike the hard disk where data is sequentially stored for access, memory is used in a broad variety of dynamic access patterns. Numerous decisions must be made concerning the granularity of encryption in operating systems. For example, a running program will utilize RAM during execution for both stacks and heap space. The stack is accessed so frequently that adding encryption/decryption overhead to stack operations might prove prohibitive. Unfortunately, during context switches, registers containing sensitive information are normally saved to the stack in external memory. Additionally, the heap size, for any given program, is not normally known a-priori. The complexities of memory mapped input-output peripherals result in an inability to cache mapped regions. This naturally presents a challenge, if the overarching concept involves decrypting memory only after it is brought onto to the processor chip. It is not clear if the entire memory should be encrypted with a single key, or if shared libraries, individual programs, and/or data should be encrypted independently using separate keys. Alternatively should individual functions or cache blocks be used as the unit of encryption? All of these decisions incur a tradeoff between the number of keys that must be securely stored, verses the degree of protection and overlapping in operations that can be realized.

The literature on memory encryption is largely concerned with three core approaches based on hardware enhancements, operating system enhancements, and specialized industrial applications. These approaches are explored in the sections that follow. Unfortunately, almost all of the hardware and operating system enhancements have only been implemented through simulation or emulation, and as a result, the claims have yet to be validated and quantified on practical systems.

Monolithic Processor Enhancements

The general scope of hardware enhancements includes a number of approaches that have added specialized encryption units and/or key storage mechanisms to existing processor designs. In addition, several efforts have proposed inserting hardware into the system bus to leverage legacy code and hardware. Although the first patents detailing memory encryption were executed in 1979 [Best 1979; Best 1981; Best 1984], and the first paper detailing their use was published in 1980 [Best 1980], the body of in-depth academic research related to general-purpose memory encryption has occurred primarily in the past decade.

One of the earliest papers, often referenced by others of this genre, highlights an *execute-only memory* (XOM) architecture [Lie et al. 2000]. This architecture was designed to combat software piracy and combines aspects of both public and symmetric key encryption. Public key encryption is used to deliver binary code to the XOM chip, which maintains a unique private key. This allows vendors to encrypt the code for a particular system and ensures that it cannot be reused on another system. The header associated with the code includes a symmetric key embedded within it, used to segment memory into unique compartments at the granularity of a process. In order to map compartments to encryption keys, each compartment is tagged. A single null compartment is created to hold all unencrypted processes and libraries. This compartment enables communication between encrypted processes while allowing all processes to use shared libraries.

The XOM architecture assumes several hardware enhancements to existing processors. Special microcode is required to store the unique private key in a private on-chip memory. A symmetric-key encryption unit is added to the processor, together with a special privileged mode of operation for encryption. A hardware trap on instruction cache misses provides a segue into this encryption mode for encrypted code. When a cache miss occurs, the instruction is decrypted before being loaded into the processors instruction register. Although the authors state encryption could be accomplished in software they acknowledge that this would be very expensive in terms of overhead. Since many of the papers that follow XOM include similar hardware, only the differences or unique contributions of the other systems will be discussed.

XOM encrypts memory in a straightforward manner commonly known by the encryption community as *electronic codebook mode* but referred to in the literature as *direct encryption*. Each code block is decrypted after it is read from memory, by the encryption unit, and encrypted before it is written back to memory. Kgil et al. [2005] propose an additional chip enhancement targeted at improving the security of direct encryption, called ChipLock. This involves storing a small trusted part of an operating system kernel, called TrustCode, in a read-only memory (ROM), termed TrustROM. Additional instructions are added to enable secure communication between the trusted and untrusted parts of the operating system. The TrustCode intercepts all system calls for memory access and performs encryption without the knowledge of the untrusted portion of the

operating system. Symmetric keys are assigned at the granularity of the process as in XOM, with additional keys for shared libraries and the concept of a null bit for applications that are not encrypted.

Rogers et al. [2005] attempt to improve on direct encryption using an alternative mechanism, *prefetching*, which had already been improving the CPU-memory performance gap for decades. Prefetching uses stream buffers to capture *spatial locality* in programs by copying additional contiguous blocks of memory into local cache after each miss. These buffers are especially good at speeding up programs that exhibit *spatial locality* and *contiguous access*, such as scientific applications [Hennessy et al. 2006]. An alternative prefetching technique is also used that involves correlation tables to capture and reuse *temporal locality,* i.e. complex and/or non-contiguous sequences of memory access.

In another direct encryption scheme, Hong et al. [2011] perform a tradeoff analysis on the use of sensitive (encrypted) versus frequently accessed (unencrypted) data in embedded scratch pad memories (SPM). Scratch pad memories are software controlled SRAMs, as opposed to caches, which are typically controlled by hardware. There are numerous papers discussing both static and dynamic policies for SPM utilization to reduce power consumption and memory access latency. DynaPoMP was the first to consider partitioning the SPM into distinct areas with an area dedicated to sensitive code and data. The authors vary the size of the two partitions in an attempt to find the most efficient ratio. There is a common assumption that an encryption unit and special instructions are available in hardware.

Unfortunately, direct encryption schemes involve a one-to-one mapping between blocks of unencrypted and encrypted code. As a result, encrypted code portrays a similar statistical distribution as the unencrypted code, allowing a significant amount of information to be gleaned from frequency analysis [Chhabra 2010]. Based on the typical AES encryption block size of 128 bits, programs tend to exhibit multiple redundancies that would lead to information leakage as shown in Figure 2.

After XOM, a number of papers attempt to mitigate this statistical weakness using a one-time pad (OTP) [Suh et al. 2003; Shi et al. 2004; Yang et al. 2005; Yan et al. 2006; Suh et al. 2007; Duc et al. 2006]. A traditional one-time pad is simply a source of random data that is used exactly once to encrypt a particular communication. This is a form of symmetric-key cryptography since both the sender and receiver require the pad. Although variously referred to as “pseudo one time pads” (POTP) in the literature, this is more commonly known in the encryption community as counter-mode (CTR) encryption. In computing, OTP’s are created by encrypting a unique seed, typically producing a pad of 128 bits in length (i.e. the size of an AES encryption block) as shown in Figure 3. A fixed initialization vector (Nonce) is concatenated with a counter producing a unique seed. The seed is encrypted with a unique key generating the pad, which is then exclusively or’ed (XOR) with the plaintext to produce the cipher text. In memory encryption schemes, the counter is stored either internally, in a cached table that maps to a memory address, or unencrypted within the encrypted memory itself (i.e. RAM) since

counter secrecy is not required [Yan et al. 2006]. When a memory reference occurs, the pad is regenerated, using the counter (and optionally some other component such as the virtual address) and initialization vector, then exclusively or'ed with the encrypted data to produce the original plaintext. Since the encryption operation is no longer dependent upon the data in memory, this regeneration can be overlapped with the memory read, decreasing the performance impact of decryption.

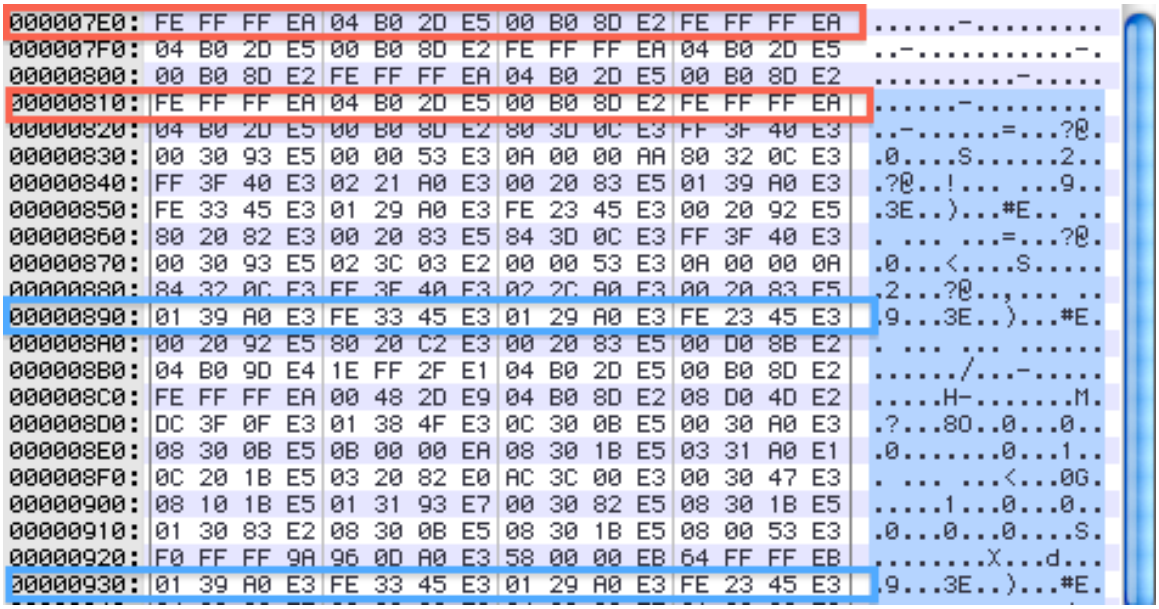

Figure 2: Redundancies in 128 Bit Sections of a Small Selection of Program Binary Code

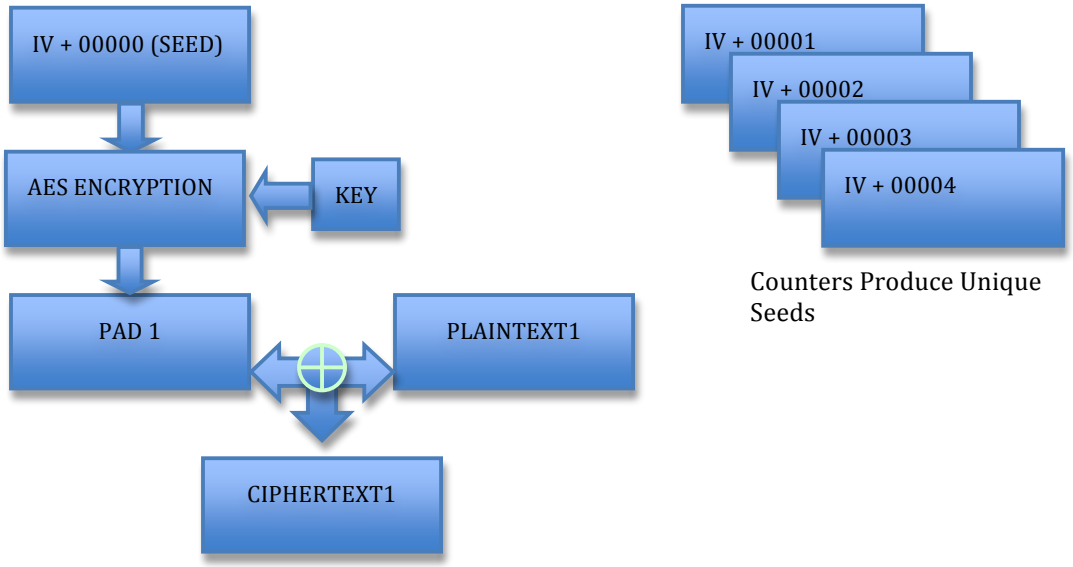

Figure 3: Pseudo-One Time Pad or Counter Mode Encryption

While Aegis is a OTP approach, it was originally proposed as a direct encryption scheme in 2003. Suh et al. propose the one-time pad approach in [2003b], perhaps illustrating the

shift away from direct encryption in the community. One interesting contribution from this paper is the method of creating the unique key. The chip-specific encryption key is created by *physically unclonable functions* (PUF) [Suh et al. 2003a]. These functions make use of unique timing characteristics of "identical" models of the hardware to create the unique keys. Aegis is one of several approaches to include the idea of a small, protected security kernel that is separate from the rest of the untrusted operating system. Unfortunately, this kernel measures 74K lines of code for virtual memory management alone [Chhabra et al. 2011].

In [Yang et al. 2005], the authors look to reduce the execution overhead of using one-time pads by adding a *sequence number cache* (SNC) onto the chip below the L2 cache. Sequence numbers, in this paper, correspond to the counters used in Figure 3. However, the initialization vector is unique per cache block and corresponds to the virtual address. Since the addresses are unique across memory, the pads (and thus the ciphertext) will be *spatially* unique. The counters are updated upon each write to memory ensuring *temporal* uniqueness (i.e. pads used for a single location will not be the same over time). The authors suggest that a reasonable addition to a chip would be a SNC of 64 KB. Based on this limitation, two policies for using the SNC are described. In the first, only the portion of memory corresponding to the number of available sequence numbers stored in the SNC can be encrypted. The amount of protected memory is therefore limited by the SNC size. In the second method, additional memory lines are encrypted and sequence numbers that do not fit in the cache are stored in plaintext in memory. Level two cache is increased in both methods by four percent in order to store the virtual memory addresses used to index into the SNC since only physical addresses are typically available above the level one cache.

In [2006], Yan et al. present *split counter mode* encryption, in which they introduce major and minor page counters. In this scheme, a 4 KB page has one 64 bit major counter and 64 7-bit minor counters (one per 64 Byte cache line). Concatenating the page major counter with the cache line minor counter forms the overall counter. This counter is further concatenated with the memory block's virtual address, and an initialization vector to form the unique seed. The vector can be unique per process, group of processes or system based on security requirements.

In CryptoPage [Duc et al. 2006], the authors again attempt to enhance the OTP encryption scheme. In this case, they modify the translation look-aside buffer (TLB) and page table structures, adding information for pad computation. Since the TLB and/or page table structures are always accessed before a memory read, the authors claim that the pad generation latency can be almost completely removed. This scheme is implemented on top of the *HIDE* memory obfuscation technique whereby access patterns are permuted in memory at designated times [Zhuang et al. 2004].

In *address independent seed encryption* (AISE) [Rogers et al. 2007], the authors propose to use a *logical* identifier, rather than the virtual or physical block address, as the major counter portion of the seed. This scheme closely resembles split mode counters [Yan et al. 2006]. It is claimed that using an address independent seed enables common memory

management techniques, such as virtual addressing, paging, and inter-process sharing. In [2011], Chhabra et al. propose to build a secure hypervisor upon the AISE substrate. The hypervisor implements *memory cloaking,* whereby the operating system only has access to the encrypted pages of applications. The authors suggest that this cloaking will protect processes from vulnerabilities in the insecure underlying operating system, with an order of magnitude fewer lines of code than in Aegis.

In [2007], Nagarajan et al. propose compiler-assisted memory encryption for embedded processors assuming some limited hardware support. They claim that the current counter mode solutions require too much silicon space for small and medium size embedded processors. The compiler supports memory encryption by introducing special instructions to calculate OTP's prior to loads and stores, and assumes the existence of additional process-unique registers used to store the counters. Space for the unique key and global counter is also provided inside the CPU and the availability of a crypto unit is assumed. The compiler attempts to ensure that the counter used for a store is still available for successive loads from the same memory location. A global counter must be available for those loads and stores that do not match one of the process-unique counter registers. The authors claim that since frequently executed loads and stores exhibit highly accurate counter matching, 8 special hardware registers with 32 counters are sufficient for reasonable performance.

Multiprocessor Enhancements

Chhabra et al. [2010] compare a symmetric multiprocessor (SMP) and a distributed shared memory (DSM) design; they also provide a quick look at monolithic memory encryption. Whereas the efficiency of memory-to-cache confidentiality is the primary concern for monolithic processors, multiprocessor systems must also protect cache-to-cache traffic. In symmetric multiprocessors, the shared bus between caches and memory can be used as a way to coordinate messages between processors. This sharing is not available in distributed shared memory systems, which must use message passing. Additionally, DSM systems can be observed more easily than monolithic chips via interconnect wires that are exposed at the back of server racks [Rogers et al. 2008].

In [2004], Shi et al. use OTP encryption both for memory-to-cache and cache-to-cache transfers as shown in Figure 4. In this approach sequence numbers (counters) are incremented in lockstep in each separate processor resulting in a claim of "very low" overhead for cache-to-cache encryption. A hardware mechanism in the processors ensures that the sequence numbers begin differently after each reboot. Besides the typical crypto-engines placed within each processor core, a separate crypto-unit is embedded in the north bridge memory controller for memory-to-cache transfers. For these transfers, 64-bit sequence numbers are stored in RAM reducing the available memory by 25 percent.

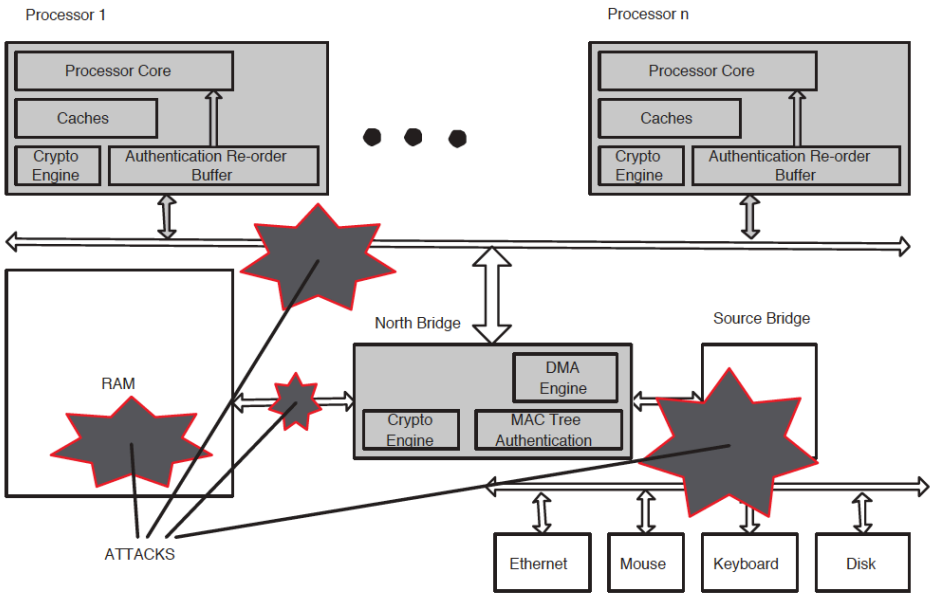

Figure 4: SMP Architecture With Memory Encryption Support

In SENSS [2005], Zhang et al. utilize OTP's for memory-to-cache transfers and AES cipher block-chaining mode for cache-to-cache transfers. This alternative to direct encryption divides the clear text into blocks and encrypts the first block with an initialization vector; subsequent blocks are chained together such that the output of the previous block is XOR'd with the input of the next before being encrypted. Cipher block chaining implies sequential access since each block depends upon each previous block. RAM is typically accessed in a fairly random pattern, so this mode of operation is impractical except on a very small scale (per cache block for example). Cipher block chaining is acceptable for cache-to-cache transfers as only one previous encrypted block must be stored at each processor (i.e. there is no requirement for access to previously encrypted blocks). The authors propose a secure hardware unit (SHU), located at each processor, comprising an encryption unit with associated storage for keeping track of communication. This storage includes memory for a group processor matrix and group information table. The group processor matrix is used by each SHU to determine if broadcast messages should be read. The matrix is only 640 bytes in size, assuming a maximum of 32 processors. The information table contains the secret information for communicating between groups, such as the symmetric key and pads, and is estimated at 149 KB. An additional 11 bus lines are used for control signals and to pass group id numbers. In [Jannepally et al. 2009], the SENSS scheme is improved using Galois Counter-Mode (GCM) AES, which provides both encryption and authentication simultaneously.

In I2SEMS [2007], Lee et al. create a scheme that is claimed to be applicable to both SMP and DSM systems. They propose a global counter cache (GCC) that assigns different sections of the overall counter space to processors (akin to assigning blocks of IP addresses to groups of computers). The blocks of counters are also broadcast to all

processors so that they can begin pre-computation of pads. Each processor has a keystream (pad) queue, keystream cache and keystream pool. The queue and cache both contain pads for encryption. The queue has new pads while the cache contains pads that have been used previously. The authors claim that pads may be reused as long as the plaintext has not been modified and that their scheme scales well to large numbers of processors since over 25% of pads are reused. The keystream pool holds pads for incoming data; the pads are chosen based on prediction with the aid of the broadcast scheme.

The first paper to exclusively address DSM systems [2006] was by Rogers et al., who again make use of counter mode encryption. Since the memory-to-cache scheme is similar to those already discussed, we only focus on the cache-to-cache scheme. The authors propose three methods for managing the pad counters: *private, shared,* and *cached* counter stream. In the first *private* method, tables are kept within each processor with separate counters for send and receive operations to/from every other processor in the system. While this technique allows for nearly perfect pad hit rates, and therefore very low overhead, it suffers from large storage needs (180KB in each processor for a 1024-processor DSM). The second *shared* scheme, aims to reduce the storage requirement by eliminating half of the table: Instead of keeping track of send counters for each processor, only one counter is kept for sending pads. This results in increased execution overhead since messages are less likely to arrive contiguously and therefore must be recomputed. The final *cached* scheme takes advantage of the intuition that processors in DSM systems often communicate in cliques [Lee et al. 2007]. The overall table size is thus reduced to a quarter of the private scheme's memory with minimal impact on execution overhead. In a subsequent paper [2008], Rogers et al. identify the previous scheme as a two level approach since remote memory requests will first be decrypted by the owning processor and then re-encrypted for cache-to-cache transmission to another processor. In the new scheme, a single mechanism is used for both memory-to-cache and cache-to-cache transfers bypassing the unnecessary decryption and re-encryption. The associated hardware includes a 32-entry buffer (1 KB) for counter prediction and a 32-entry mask buffer that stores a bit vector of recent data block accesses (512 bytes).

Bus Inserts

Another area of active research involves placing specialized encryption hardware outside of the CPU. The locations include the memory bus (i.e. externally between system memory and the CPU) and within RAM. The primary goal of this approach is to increase the likelihood that this solution will be adopted since re-engineering of commodity processors is not required. One such approach, SecBus [Su et al. 2009] shown in Figure 5, can be located at the frontend of the memory controller. The authors state that this method of modification is required in many user markets when embedding new functionality into systems with legacy CPUs. SecBus is essentially a cryptographic coprocessor with internal storage and bus manager. The page security parameters entry (PSPE) includes information to map pages to corresponding security policy (SP), which includes a confidentiality mode, integrity mode and secret key. SecBus includes the

ability to choose between multiple encryption modes based on the type of memory (i.e. code or data).

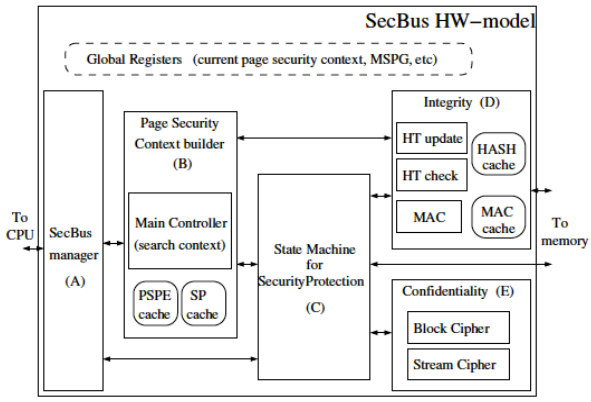

Figure 5: SecBus Hardware Augmentation Model

In [2008], Enck et al. design a memory encryption control unit (MECU) to again be placed on the memory bus between the processor and RAM. The goal of MECU is to provide the same guarantees of security provided by the volatility of traditional RAM when utilizing non-volatile main memory. MECU uses a OTP scheme with internal storage for the array of counter seeds and the encryption engine. A secret key and master counter, which tracks the greatest overall counter, are stored on a removable smart card. In order to reduce the storage requirement, the encryption chunk granularity is increased from one cache line to *n*, where *n* is 256 in the common case but can grow to the entire memory for experimentation.

With the same goal as [Enck et al. 2008], Chhabra et al. [2011] propose placing the cryptographic engine and other required hardware in non-volatile RAM modules. Their scheme keeps most of the RAM encrypted with a smaller group of frequently accessed pages in plaintext in a similar fashion to [Hong et al. 2011]. The authors claim that by doing this, the remainder of the RAM can be encrypted at power-down within 5 seconds, paralleling traditional RAM volatility.

Operating System Enhancements

Similar to the bus insert method for enabling memory encryption, software-only approaches seek to provide solutions that can be implemented without major changes to applications or commodity hardware to increase the likelihood of adoption.

In [2008], Chen et al. propose an operating system controlled memory bus encryption technique for systems that offer scratch pad memory (SPM) or cache locking that is software controllable. Both types of memory are available in some embedded processors including the Intel XScale series. A new symmetric key is generated each time the system is booted and random vectors (32 bits generated using /dev/urandom and padded with 0's) are used to initialize AES encryption at the granularity of a page. The vectors are then placed in memory with the pages. This scheme requires a 0.4% space overhead when used with 1 KB pages. When a page fault occurs for a secure process, a specially

crafted handler moves the encrypted page into the chip boundary and decrypts it there placing it into the cache, which is then locked to prevent leakage of sensitive data. The locked region holds several pages of data and encryption variables. In order to facilitate this special handling, a boolean status variable is added to each process descriptor residing in kernel address space. The authors note the scheme is appropriate when embedded systems designers can tolerate a significant performance overhead for protected processes.

In Cryptkeeper [2010], Peterson modifies the virtual memory manager and partitions RAM into two parts; the plaintext *Clear* and the encrypted *Crypt*. Essentially, this technique aims to reduce the amount of sensitive data available at any time in memory. All pages initially start in the clear and the number of Free Clear Pages (FCP) is reduced with each allocation. The least recently used pages are encrypted and moved to the Crypt when the limit of FCP runs low. This operates under the assumption that the number of high use pages will be small, and therefore most infrequently used pages will be encrypted. This has the unfortunate side effect of maintaining all the important pages in the clear. A prototype Cryptkeeper system was designed based on the Linux 2.6.24 kernel. The kernel page structure was extended to include information indicating whether a page is in the Clear or Crypt portions of memory.

Specialized Industrial Devices

Industry offers several solutions for memory encryption including low frequency specialized processors for ATM use, expensive tamper resistant coprocessors for financial transactions, proprietary gaming systems and, more recently, enabling technologies in commodity processors to enhance trust.

The Dallas Semiconductor 5002FP secure processor is an 8051 compliant processor and runs at a maximum frequency of 16 MHz [Dallas 1997]. The processor encrypts memory addresses to prevent traffic analysis on the memory bus in addition to data. The device uses spare processor cycles to place dummy memory accesses on the bus since analysis of memory access patterns can reveal useful information (e.g. encryption keys or sensitive algorithms) to attackers [Gao et al. 2006]. All external memory is encrypted via a proprietary encryption algorithm with a 64-bit secret key that is stored in a tamper-protected, battery-maintained static RAM. Plaintext code is uploaded via serial port and a firmware monitor encrypts it and stores it in external RAM. The 5002FP is commonly used in credit card (i.e. point of sale) terminals, automated teller machines, and pay-TV decoders [Yang et al. 2005]. A newer version (DS5250) includes a larger 1 KB instruction cache, which, according to Dallas Semiconductor, reduces the effect of memory encryption on execution speed providing a 2.5X performance improvement. The newer processor runs at a maximum frequency of 25 MHz.

Another active area of secure hardware used in industry is the cryptographic coprocessor. Primary examples include the IBM PCI-4758, PCI-XCC shown in Figure 6, and the latest

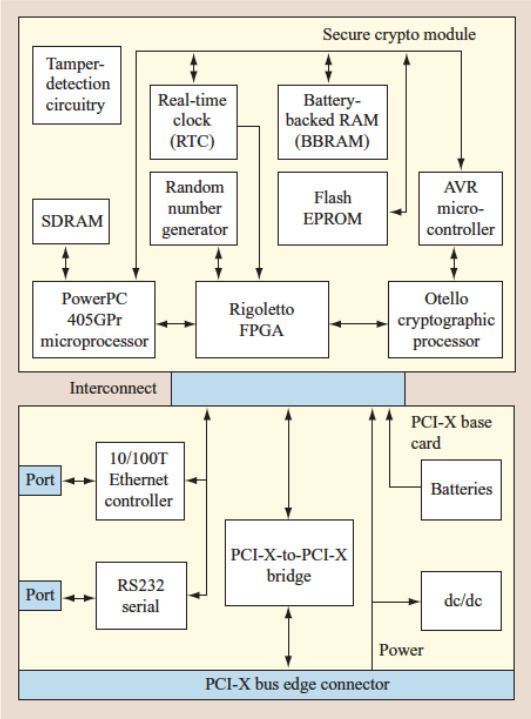

Figure 6: IBM PCIXCC Hardware Model

PCI-e. These coprocessors include an impressive array of technology but are generally limited to IBM server platforms under customized contracts and tend to be used for financial and banking systems. The PCI-XCC is an adapter card including an IBM PowerPC 405GPr microprocessor (266 MHz), 64 MB of DRAM, 16 MB of flash EEPROM, 128 KB of CMOS RAM backed up by battery, tamper-detection circuitry, cryptographic processor and FPGA. It is certified at the FIPS 140-2 tamper resistance standard level 4 [Arnold and Doorn 2004]. The packaging around the unit is designed to detect or prevent all known physical attacks such as acid etching or probing. A modified version of embedded Linux runs on the system providing a subset of typical features. The previous version (4758) used the IBM developed CP/Q message-passing microkernel. The secure module is encased in a flexible mesh of overlapping conductive lines meant to prevent any physical intrusion. If such intrusion is detected the system responds by zeroizing the internal RAM which holds the 168 bit Triple-DES secret key. The cryptographic processor performs at a throughput of 67 MB/s for Triple DES and 185 MB/s for AES-128. The stated purpose of the IBM secure coprocessor is to offload computationally intensive cryptographic processes (e.g. specialized financial transactions) from the host server.

While mostly constrained for use in playing games and other entertainment media (unless compromised) gaming systems are some of the most capable (e.g. fast processor speed and relatively large storage) to incorporate memory encryption techniques. As an example of these systems, the Xbox 360 provides encrypted/signed bootup and

executables, partially encrypted RAM, and an encrypted hypervisor [Steil and Domke 2008]. These mechanisms are provided via a Microsoft proprietary processor with 64 KB of internal RAM, random number generation and encryption as opposed to the "off the shelf" processor used in the original Xbox. While it is possible to use the Xbox as a general-purpose platform, this requires compromising the system's security measures first. Alternatively, the Sony Playstation 3 includes many of the same security mechanisms of the Xbox 360, but allows the end user to partition the hard drive for use with a chosen (e.g. Linux) operating system. However, the proprietary security mechanisms of the Playstation 3 are not available to the additional operating system [Conrad et al. 2010].

Most of the approaches in the ME literature assume that several components are necessary for secure, efficient performance: a way to generate and securely store encryption keys (i.e. not in RAM); and hardware to accelerate encryption performance. Although not targeted specifically at memory encryption, nascent technology could be used to form the basis of an encrypted memory solution for general-purpose systems. One of the developers of IBM's 4758 cryptographic coprocessor has suggested, for example, that a general-purpose system with hardware support (such as a trusted platform module) could theoretically be turned into a somewhat less secure but more pervasive and less expensive version of the 4758 [Smith 2004]. Encryption engines have been added to Intel's core i5 and i7, AMD's bulldozer and various embedded processors [Muller et al. 2011]. Intel's advanced encryption standard - new instructions (AES-NI) include six instructions to speed up key expansion and encryption. Intel states that the new instructions can provide a two to three time performance improvement over software-only approaches for non-parallel modes of operation such as cipher-block-chaining (CBC) encryption [Gueron 2010]. Further, a 10-fold improvement can be realized for parallelizable modes including CBC-decrypt and counter-mode encryption (CTR). As an example of the performance improvements possible, the authors ran TrueCrypt's encryption algorithm benchmark test on a MacBook Pro with an Intel i7 dual-core, 266 GHz CPU. Using a 5 MB buffer in RAM, the throughput averages 202 MB/s without AES-NI support, and 1 GB/s with it – approaching the speed required to overcome encryption overheads on general-purpose systems.

The trusted computing group (TCG) designed the Trusted Platform Module (TPM) based on the IBM 4758 secure coprocessor [Vandana 2008]. The TPM provides secure key storage and the capability for platform measurements for chain-of-trust booting. The current specification for the TPM calls for it to be attached to a typical motherboard via the low pin count (LPC) bus. The TPM provides non-volatile storage for encryption keys and an encryption engine including support for RSA, SHA-1 hashing, and random number generation. The LPC bus is limited in speed and the cryptographic engine on the TPM is not meant to be a cryptographic accelerator. Over 350 million TPMs were deployed as of 2010 and can be found in many laptops and general-purpose computers (disabled by default) [Dunn et al. 2011]. On its own, the TPM would not be powerful enough to provide general memory encryption with acceptable overhead. However, the TPM may be used to provide secure key storage between power cycles. Unfortunately, a small weakness still exists in that keys must be sent in the clear over the LPC bus to the

CPU, allowing a bus snooping attack to capture them [Simmons 2011]. Other interesting methods to store encryption keys have been described recently in schemes targeted at preventing cold-boot attacks on full disk encryption. For example, Muller et al. describe TRESOR, a technique for utilizing CPU debug registers for encryption key storage [2011]. In order to protect against memory attacks on the key, the decryption routines are carefully written in assembly to avoid using the stack, heap or data segment during decryption. By utilizing AES-NI, TRESOR was shown to perform better than software based full disk encryption (17.04 MB/s vs. 14.67 MB/s) with the additional protection. A similar approach is taken in [Simmons 2011] except that registers used for performance counting are targeted for master key storage with multiple encrypted keys being stored in RAM.

Intel has recently filed several patents for processors incorporating memory encryption, perhaps indicating a move toward support in commodity processors [Gueron 2012], [Gueron 2013]. The patents describe a new processor with hardware including a memory encryption engine (MEE) and on-chip storage for counters. The hardware described in the application modifies the AES-XTS *tweak* mode of operation. XTS stands for XEX based tweaked codebook mode with ciphertext stealing and this mode is typically used for disk encryption [Martin 2010]. A tweak is similar to an initialization vector and is an additional input to a cipher designed to protect against similarities in ciphertext. For disk encryption, the tweak tends to be the sector number. In Intel's patents, the tweak is extended to include a time stamp or counter value along with the memory address. The counter is updated each time a cache line is written, providing protection against a replay attack where a chunk of memory is copied and inserted back into memory at a later time.

Analysis

Although the primary goal of memory encryption architectures is security, the work tends to focus on the overheads involved, both in chip area and performance degradation. This is unfortunate though unsurprising given that most of the work is simulated and it is within the intricacies of implementation that security vulnerabilities tend to be found. The analysis here focuses on the data available including encryption latencies, performance degradation, simulation environments, operating system assumptions, overall space requirements, user requirements and general observations regarding security.

Since the performance degradation of memory encryption results in less likelihood of its use, it is an extremely important factor in the comparison of different schemes. One of the major issues with the body of literature is the lack of a common set of measurement standards, with explicit assumptions regarding memory access latency, encryption latency etc. This makes it difficult to directly compare approaches and draw valid conclusions. Encryption latencies are typically given as the number of cycles required to encrypt/decrypt a cache line that varies from 16 to 128 bytes, typically using a value of 64 bytes. The latencies range from 11 to 160 cycles with 80 being the most common value (especially in the multiprocessor work). The authors in [Rogers et al. 2006] state that 80-cycle latency is assumed in order not to penalize the direct encryption scheme

(upon which they are trying to improve) since a recent (circa 2006) hardware implementation required over 300 ns. Cycles and nanoseconds are often used interchangeably since many of the systems modeled are based on 1 GHz processors. Low encryption latencies are possible but at the cost of large die area making them appropriate for powerful processors. For example, it is claimed in [Suh et al. 2003] that 40 cycle-latency is achievable with four AES units chained together requiring 300,000 gates. In AEGIS [Suh et al. 2007], a single AES unit is estimated at 86,655 gates, which the authors claim is modest when compared to the size of commercial cores. Unfortunately, the OR1200 soft core used to demonstrate Aegis is only approximately 60,000 gates (meaning one AES unit is 144% of the original core size).

The methods used for determining performance include mathematical models, simulation, kernel prototypes and FPGA prototypes with various benchmarking suites used in the latter three. Simulation is performed with (in order of decreasing usage) SimpleScalar, Simics, SESC, GEMS, SOC designer, RSIM, and M5. Benchmark suites used include SPEC2000, SPLASH2, Mediabench, EEMBC and several user developed varieties such as one entitled "memeater". A group of the simulations utilize SimpleScalar and [Duc and Keyell 2006] notes that this simulator neglects the impact of the operating system and other running processes. Besides these limitations, some authors admit a lack of model fidelity with significant differences between systems modeled and those targeted. For example, in [Chen et al. 2008] an x86 architecture is modeled since it happens to be better supported by the simulation tool (Simics) even though the scheme is actually targeted for embedded-ARM systems. Unfortunately, even if a system under test were to be modeled perfectly, the simulation tools themselves have been shown to sometimes exhibit behavior unlike real systems. In [Muller et al. 2011], the behavior of CPU registers is interrogated under simulation in QEMU with the contents surviving soft-boot. This behavior would circumvent the protections afforded in that work, however, real hardware behaves differently and zeroes out the registers.

A summary of the featured techniques is presented in Table I to provide an overview of memory encryption. The table includes basic characteristics of each approach such as complexity information including execution and storage overheads. In order to fairly compare the different schemes, several assumptions were made. For example, the size of internal storage required is sometimes dependent on the size of RAM, and where possible an assumption of 1 GB is made. Similarly, an assumption of 32 processors is made where possible for the multiprocessor approaches. When there is no data available, an element of the table is left blank. Two values are commonly reported in the literature with regard to execution overhead: worst case (max) and the average (based on some suite of benchmark tests) percentage slowdown when compared to non-protected execution. Storage overheads typically break down into internal (cache) and external (RAM) usage (and one example of the increase to overall code size). Operating system approach indicates whether the authors assumed the existence of a secure kernel (A), described hardware to protect the processes from an insecure kernel (H), or ignored the operating system (I) (further discussion of this requirement below). Finally, slightly fewer than two-thirds of the authors included memory integrity (I) along with memory confidentiality (C) mechanisms. Where possible, results (e.g. execution overhead and

Technique	Reference	Category	Execution Overhead Max/Average %	Storage Overhead (I)nternal, (R)AM, (C)ode	Operating System Approach	Maturity	(C)onf (I)ntegrity	Encryption Algorithm	Full/Partial Memory Encryption	*Security Level*
XOM	[Lie et al. 2000]	Mono/Direct	50 /	I – Private Mem & XVMM	H + Virt Machine	Math	C + I	3 DES	PME	*MEDIUM*
ChipLock	[Kgil et al. 2005]	Mono/Direct	/ 3	I – Key Table	H + Part of Kernel	Sim	C + I	AES	FME	*HIGH*
Predecryption	[Rogers et al. 2005]	Mono/Direct	/ 1	1.5 MB-I	I	Sim	C	UNK	FME	*LOW*
Aegis	Suh et al. 2003]	Mono/Counter	32 / 4.5	12 KB-I 6%-R	H + Part of Kernel	P-FPGA	C + I	AES	FME	*HIGH*
SNC	[Yang et al. 2005]	Mono/Counter	/ 3.9	64 KB-I 1.5%-R	H	Sim	C	AES	FME	*MEDIUM*
Split Counter	[Yan et al. 2006]	Mono/Counter	9 / 2	32 KB-I 1.5%-R	A	Sim	C + I	AES-GCM	FME	*MEDIUM*
CryptoPage	[Duc and Keryell 2006]	Mono/Counter	7.4 / 3		H	Sim	C + I	AES	PME	*HIGH*
Compiler	[Nagarajan et al. 2007]	Mono/Counter	/ 2.3	32 B-I 12.5%-R 3%-C	I	Sim	C	AES	FME	*LOW*
SecureME	[Chhabra et al. 2011]	Multi/Counter	13 / 5.2	32 KB-I 1.6%-R	H	Sim	C + I	AES	FME	*HIGH*
AISE	[Rogers et al. 2007]	Multi/Counter	13 / 1.6	32 KB-I 1.6%-R	I	Sim	C + I	AES	FME	*MEDIUM*
Arch Supt	[Shi et al. 2004]	Multi/Counter	55 /	32 KB-I 25%-R	A	Sim	C + I	AES	FME	*HIGH*
SENSS	[Zhang et al. 2005]	Multi/Counter	/ 12	149 KB-I	H	Sim	C + I	AES-CBC	FME	*HIGH*
FE and Auth	[Jannepally et al. 2009]	Multi/Counter	/ 5.2	4.8 KB-I	I	Sim	C + I	AES-GCM	FME	*LOW*
I2SEMS	[Lee et al. 2007]	Multi/Counter	10 / 4	608 KB-I	I	Sim	C + I	AES-GCM	FME	*MEDIUM*
EDP-DSM	[Rogers et al. 2006]	Multi/Counter	/ 6	4.5 KB-I	I	Sim	C + I	AES	FME	*MEDIUM*
SLICP	[Rogers et al. 2008]	Multi/Counter	7 / 1.6	33.5 KB-I	I	Sim	C + I	AES	FME	*MEDIUM*
SecBus	[Su et al. 2009]	Insert/Direct	23,753/ 100		A	Sim	C + I	UNK	FME	*LOW*
MECU	[Enck et al. 2008]	Insert/Counter	4.4 / 2.1	131 KB-I	H	Sim	C	UNK	FME	*LOW*
i-NVMM	[Chhabra and Solihin 2011]	Insert/Direct	20 / 7.2	78 MB-I	H	Sim	C	AES	PME	*LOW*
OS Controlled	[Chen et al. 2008]	Soft/Direct	78 / 37	0.4%-R	A	Sim	C	AES-CBC	PME	*LOW*
Cryptkeeper	[Peterson 2010]	Soft/Direct	800 / 9		I	P-Soft	C	AES-ECB	PME	*LOW*
DynaPoMP	[Hong et al. 2010]				I	Sim	C	AES	PME	*LOW*

storage) are provided for memory encryption only. Maturity indicates how the technique was evaluated if not a commercial product. Methods appear in the table as they are presented in the survey and detailed in the approach column: monolithic processor, multiprocessor, bus insert, or software/direct or counter mode encryption.

We will consider partial/full memory encryption and security level in more detail. While partial memory encryption schemes are typically used to decrease both space and execution overheads, they place the onus for identifying secure components, a non-trivial task, on application or system designers. Today, an analog can be observed in the adoption of hard disk encryption technologies, whereby administrators struggling to identify which files (or parts of files) require encryption are opting instead for full disk encryption [Brink 2009]. *Security level* refers to the overall security of the ME approach with multiple factors from the table taken into consideration: operating system approach, addition of integrity mechanisms, encryption algorithm, and partial vs. full ME. Additional factors include consideration of implementation details outside of the "steady state" such as key escrow, delivery of secure code, inter-process communication, etc. Each approach is qualitatively classified into one of three levels—low, medium, and high based on these factors. The Aegis approach [Suh et al. 2003] has the highest security level of the works surveyed: the operating system approach includes both hardware and a small, trusted kernel; integrity mechanisms are included; the AES encryption algorithm is used; full memory encryption is provided; and much of the additional details required for a fully functional, secure implementation are discussed. It is unsurprising that the approach with the highest security evaluation is also the most mature (implemented as an FPGA prototype). In contrast, operating system controlled ME [Chen et al. 2008] is classified among the lowest security levels: this approach *assumes* the kernel is secure; does not provide integrity mechanisms; targets partial memory-encryption; lacks sufficient detail for a fully functional system; and assumes the attacker is a *clever outsider*.

For direct encryption, the performance overhead ranges from a claimed low of 1% in [Rogers et al. 2005] based on simulation of pre-decryption to a high of 50% for XOM [Lie et al. 2000] using mathematical analysis based on a worst-case scenario. Rogers et al. find an average slowdown for a model of XOM of 21% based on the same 18 SPEC2000 benchmarks used in their own simulation work. In four particular benchmarks (applu, bt, ft, and mcf) the overall execution time for pre-decryption is similar to the direct encryption scheme because prefetching adds mis-predicted memory references to bus traffic increasing contention. Overhead for OTP based encryption, in monolithic chips, ranges from a claimed 1.6% for AISE (SESC and 21 CPU2000 benchmarks) [Rogers et al. 2007] to up to 50% for the basic model in CryptoPage (SimpleScalar and 10 CPU2000 benchmarks) [Duc and Keryell 2006]. The authors of CryptoPage claim only 1% of this overhead is attributable to the memory encryption.

For multiprocessor systems, the reported overheads range from a low of 4% in I2SEMS (Simics + GEMS and 4 SPLASH2 benchmarks) [Lee et al. 2007] to a high of 55% in [Shi et al. 2004] (RSIM and 6 SPLASH2 benchmarks). I2SEMS is claimed to work equally well on both SMP and DSM systems but the simulation environment is limited to SMP.

Cache-to-cache overheads are very low (especially for SMP systems that use the shared bus for synchronization) in these multiprocessor schemes. All of the multiprocessor schemes build upon work in the monolithic memory encryption area and use the counter mode (OTP) model.

There are only two models surveyed for hardware insert and they exhibit very different performance characteristics. MECU [Enck et al. 2008] is based on the OTP scheme and exhibits 2.1% and 4.1% overhead based on block sizes of 256 and 4096 cache lines respectively and SimpleScalar simulation with 5 SPEC2000 benchmarks. SecBus [Su et al. 2009] is based on direct encryption and exhibits worst case slowdowns of 472% based on various EEMBC benchmarks and SoC designer. Besides the method of encryption, the architectures modeled add to the significant differences in overhead. While SecBus is simulated on an embedded system with 16KB L1 cache and no L2 cache, MECU is modeled after an x86 system with 32KB L1 and 256KB unified L2. Clearly, the amount of cache available has a huge impact on performance. If complete working sets fit into a system's cache, the penalty for memory encryption includes only the initial decryption time, which is amortized across the entire duration of the process.

As might be expected, the software-only approaches suffer from impractical overheads. In [2008], Chen et al. simulate operating system controlled memory encryption and report from 137% to 850% overhead based on Simics and Mediabench benchmarks. In Cryptkeeper [Peterson 2010], the overhead to read a page when compared to an unprotected system is 6015%. As far as commercial hardware, there is no literature available reporting the performance degradation of either the Dallas Semiconductor chips or the IBM cryptographic coprocessors (e.g. PCIXCC). However, these solutions run at slow overall frequencies (25 MHz and 266 MHz respectively) and are not particularly well suited for general-purpose systems. The IBM PCIXCC coprocessor has a reported AES-128 throughput of 185 MB/s.

In general, the counter mode methods exhibit less computational overhead than the direct encryption techniques and are resistant to direct encryption's statistical weaknesses. However, the choice of size for the counter is critical since a "wraparound", whereby the counter resets to zero, requires a change of key in order that each pad is only used once (a condition necessary to ensure protection from chosen plaintext attacks) [Lipman et al. 2000]. In the case where only one key is used the entire memory then requires re-encryption. This re-encryption can be costly depending on the size of memory and results in a temporary freezing of the system, which is unacceptable for real-time performance [Yan et al. 2006]. Choosing a value too small will result in too many re-encryptions but choosing one too large will require unacceptable amounts of storage space either in cache or memory. For example, in [Suh et al. 2003] the authors suggest 32 bits is an appropriate size for the counter. However, even at this size, and based on their simulations, a re-encryption is required every 5.35 hours on average and every 35 minutes for a particularly memory intensive program. In [Yang et al. 2005], the authors choose to disregard the problem since the provided security is assumed to be no weaker than that of the XOM scheme, whereas the wraparound issue is not considered at all in [Suh et al. 2007]. In [2006], Yan et al. attempt to address the counter size vs. re-

encryption problem with their split-counter encryption scheme. With larger page counters and multiple smaller per-memory block counters, overruns result in a much finer granularity of re-encryption (per page instead of per process). Since some pages are written back to memory more often than others, the overall necessity for re-encryption is reduced since the fastest incrementing counter would have controlled the entire memory space in previous schemes. Another critical decision involves where to store the counters.

Although using cache is obviously faster, it is also problematic as cache resources are typically limited and expensive. If pre-existing cache space is utilized instead, additional memory references occur since part of processes' working sets are forced out of cache (essentially reducing the size of the usable cache causing capacity misses). For example, in [Yang et al. 2005] the authors state that a 1 GB memory space would require over 8 million sequence numbers based on cache line granularity and a cache line size of 128 bytes. Adding a cache that large (~ 28 MB) is unreasonable so the authors suggest adding a much smaller 64 KB one. However, this design decision either limits the security of the system, since a large part of memory would be unencrypted, or some sequence numbers would be stored in memory. There are 32K numbers (2 Bytes each) stored in the SNC covering 32K L2 cache lines and 4 MB of memory. Although RAM is slower than cache, the seed (which is smaller than a cache line) is the first memory access and would arrive earlier than the rest of the reference. Although this does not hide as much latency as using cache, it is an improvement over the direct encryption scheme. This technique would also render part of RAM unusable, as it would be utilized for additional storage.

In address independent seed encryption (AISE) [Rogers et al. 2007], the authors suggest that all of the previous OTP schemes are flawed in their use of memory address as part of pad computation. Using virtual addresses as a component of the input to the pad seeds may lead to a vulnerability since separate processes will use the same address tweak as part of the seed (breaking the requirement for pad uniqueness). Additionally, using the virtual address for pad computation can cause problems for shared memory inter-process communication since the pads would be different for the various processes even though both need to access the plaintext. For schemes using the physical address as part of the pad computation there are other issues when swapping to the backing store. Since pages in memory that are swapped out are likely to reside at a new physical address when brought back in, there is a potential for pad reuse or the requirement for a decryption and re-encryption of a page loaded into a different address.

Industrial implementations have been shown to be vulnerable to attack. In [1998], Kuhn demonstrates what is essentially a brute-force attack on the 5002FP. External hardware is used to control input to the processor and force it to power cycle. After each power-on, different encrypted "guesses" (possible instructions) are fed to the system and the output ports are observed. The 5002FP had been described as the most secure processor available for commercial users at the time of this successful attack, which required a personal computer, and a device built in a student laboratory for about $300. One of the reasons the 5002FP is vulnerable to brute force attack is the small size of the plaintext.

Kuhn notes that encryption performed over whole cache lines (of at least 8 bytes) instead of on single bytes would make the brute-force attack impractical. There is no known example of a successful attack against the IBM cryptographic coprocessors. However, these coprocessors are relatively expensive, used for highly specialized applications and difficult to upgrade [Suh et al. 2007], making them undesirable for general purpose computing environments. While the TPM chip has been included in various trusted computing schemes, it is potentially vulnerable to the same types of snooping and bus injection attacks used against systems with unencrypted memory [Shi et al. 2004; Suh et al. 2007; Simmons 2011]. In fact, when utilizing the TPM with bitlocker drive encryption, the secret key is copied into RAM making it vulnerable to capture via cold-boot and other attacks as demonstrated in [Halderman et al. 2008]. Since the key must be in RAM for bitlocker to function properly, the additional protection of the TPM is potentially nullified.

There are three basic approaches in the literature surveyed with regard to operating systems. The problem lies in the fact that without a secure (trusted) operating system extra protections must be placed in hardware to prevent a compromised system from breaking the confidentiality of other processes. For example, when processes are context switched by the operating system the registers and other internal memory will be in plaintext. The first approach is to explicitly assume the existence of a secure operating system [Chen et al. 2008; Shi et al. 2004; Yan et al. 2006; Suh et al. 2003; Su et al. 2009; Chen and Morris 2003]. Some of the papers taking this first approach discuss implementation requirements but none have been developed. In the second approach, the complexity of the hardware is increased in order to protect all processes (including the operating system) from each other [Kgil et al. 2005; Yang et al. 2005; Duc and Keryell 2006; Enck et al. 2008; Lie et al. 2000; Platte et al. 2006; Zhang et al. 2005; Chhabra et al. 2011]. One example of such hardware includes special instructions and extra registers which are called before context switches [Lie et al. 2000]. The internal registers are then encrypted strictly by the hardware before the kernel can intervene and complete the context switch as normal. Although several papers note the importance of working on a secure kernel to complement secure architectures we have found no work to date suggesting the completion of any such effort. In the third approach, the requirement for a secure operating system is simply not addressed [Nagarajan 2007; Rogers et al. 2005; Rogers et al. 2007; Hong et al. 2011; Lee et al. 2007; Jannepally et al. 2009; Rogers et al. 2006; Rogers et al. 2008].

Conclusion

This survey has considered the research challenges associated with full memory encryption and distinguished three primary groups of techniques that attempt to solve those challenges — hardware enhancements, operating system enhancements, and specialized industrial devices. While the concept of memory encryption has existed for over three decades, there are still no general-purpose, commercial-off-the-shelf (COTS) solutions integrated with secure operating systems. However, there is clearly a growing need for privacy and intellectual property protection on the Internet as evidenced by the increasing use of full disk encryption, recent policy directives such as the Federal Data

Breach Notification Act and components of the Health Insurance Portability and Accountability Act [Brink 2009]. Between 2002 and 2007, a reported 773 breaches of US organizations were reported with a total of 267 million private records lost. Over 42% of these breaches were a result of lost or stolen hardware including laptops, PDAs and portable memory devices [Romanosky et al. 2008]. Additionally, it is apparent that at least one major chip maker (Intel) has recognized this growing need as two recent patent applications for adding memory encrypting hardware to processors attests [Gueron et al. 2012], [Gueron et al. 2013].

The range of overheads reported in the literature is quite large (1% to 6015%). The results on the lower end of the spectrum are possibly overly optimistic given the lack of fidelity in the simulation frameworks and the lack of standards for comparison. If standardization could be injected into the validation methodologies through common AES decryption latency, benchmarks etc. it would enable more meaningful comparative analyses. Even with standardization, the number of assumptions make it difficult to be confident that simulation will provide anything more than high-level information: It ignores the more difficult and interesting implementation issues and associated security impact based on vulnerability and exploit analysis. Where, in the few cases available, the literature addresses these low-level issues, it tends to be with generalization since there is no chance for practical experimentation or empirical evidence [Lie et al. 2000; Shi et al. 2004; Chhabra et al. 2010]. While the security of the encryption algorithm or cipher mode is often pointed out, it is commonly the complexity of the system in which these algorithms run that presents vulnerabilities. The most developed, though not commercially available, general-purpose technologies are FPGA soft-core emulations [Suh et al. 2007] and the Linux prototype used in Cryptkeeper [Peterson 2010]. While the industrial devices are mature and practical, they are not general purpose, catering to highly specialized operations. Additionally, these devices are either low-frequency or expensive and difficult to upgrade [Dallas 1997; Arnold and Doorn 2004].

Several technologies have been incorporated into general-purpose systems recently and often without the knowledge of those buying them. These technologies include TPM chips for storing keys and encryption engines and instructions. Given a system with these components, it is now possible to experiment with memory encryption providing an opportunity to better understand the difficult implementation details and ultimately provide data on overhead and security enhancement. This data should prove invaluable for determining the feasibility of memory encryption in general-purpose systems and for comparing against (and perhaps validating) the results of previous simulation work.

Notice

REFERENCES

ANDERSON, R., and KUHN, M. Tamper resistance – a cautionary note. In *Proceedings of the Second USENIX Workshop on Electronic Commerce*. 2 (November 1996), 1-11.

ARNOLD, T., and DOORN, L. The IBM PCIXCC: a new cryptographic coprocessor for the IBM eserver. *The IBM Journal of Research and Development*. (2004), 120-126.

BARRANTES, E., ACKLEY, D., FORREST, S., PALMER, T., SEFANOVIC, D., and ZOVI, D. Randomized instruction set emulation to disrupt binary code injection attacks. In *Proceedings of the 10th ACM conference on Computer and communications security (CCS '03)*. (October 2003), 281-289.

BEST, R. Crypto microprocessor for executing enciphered programs. U.S. patent 4,278,837. (14 July 1981).

BEST, R. Crypto microprocessor that executes enciphered programs. U.S. patent 4,465,901. (14 August 1984).

BEST, R. Microprocessor for executing enciphered programs. U.S. patent 4,168,396. (18 September 1979).

BEST, R. Preventing software piracy with crypto-microprocessors. In *Proceedings of the IEEE Spring Compcon*. (February 1980), 466-469.

BOILEAU, A. Hit by a bus: physical access attacks with firewire. Presented at *Ruxcon*. (2006).

BRINK, D. Full-disk encryption on the rise. *Aberdeen Research Group Report*. (September 2009).

CASEY, E., FELLOWS, G., GEIGER, M., and STELLATOS, G. The growing impact of full disk encryption on digital forensics. in *Digital Investigation*. 8 (September 2011), 129-134.

CHAHAL, S., KAMHOUT, D., KOHLENBERG, T., KUMAR, M., MANCINI, S., MORGAN, D., PURCELL, S., ROSS, A., and SMITH, C. Evolution of integrity checking with Intel trusted execution technology: an Intel IT perspective. *Intel white paper*. (August 2010).

CHARI, S., JUTLA, C., RAO, J., and ROHATGI, P. Towards sound approaches to counteract power analysis attacks. In *Proceedings of the CRYPTO'99: 19th Annual International Cryptology Conference*. 1666 (1999), 398-412.

CHEN, B., and MORRIS, R. Certifying program execution with secure processors. In *Proceedings of the 9th Conference on Hot Topics in Operating Systems*. (2003), 23-29.

CHEN, X., DICK, R., and CHOUDHARY, A. Operating system controlled processor-memory bus encryption. In *Proceedings of DATE*. (2008).

CHHABRA, S., ROGERS, B., SOLIHIN, Y., and PRVULOVIC, M. SecureMe: a hardware-software approach to full system security. In *Proceedings of the International Conference on Supercomputing (ICS)*. (May 2011).

CHHABRA, S., and SOLIHIN, Y. i-NVMM: a secure non-volatile main memory system with incremental encryption. In *Proceedings of the International Symposium on Computer Architecture (ISCA)*. (June 2011).

CHHABRA, S., SOLIHIN, Y., LAL, R., and HOEKSTRA, M. An analysis of secure processor architectures. In *Transactions on Computational Science VII*. Marina L. Gavrilova and C. J. Kenneth Tan (Eds.). Lecture Notes In Computer Science. Springer-Verlag, Berlin. 5890, (2010), 101-121.

CHOW, J., PFAFF, B., GARFINKEL, T., CHRISTOPHER, K., and ROSENBLUM, M. Understanding data lifetime via whole system simulation. In *Proceedings of the USENIX Security Symposium*. (August 2004).

CONRAD, S., DORN, G., and CRAIGER, P. Forensic analysis of a sony playstation 3 gaming console. In Advances in Digital Forensics VI. K.P. Chow and S. Shenoi (Eds.). AICT 337, (2010), 65-76.

DALLAS SEMICONDUCTOR. Secure microcontroller data book. Dallas, (1997).

DUNN, A., HOFMANN, O., WATERS, B., and WITCHEL, E. Cloaking malware with the trusted platform module. In *Proceedings of the 29th USENIX Conference on Security*. (2011), 26.

DUC, G., and KERYELL, R. CryptoPage: an efficient secure architecture with memory encryption, integrity and information leakage protection. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*. (2006).

ELBAZ, R., CHAMPAGNE, D., GEBOTYS, C., LEE, R., POTLAPALLY, N., and TORRES, L. Hardware mechanisms for memory authentication: a survey of existing techniques and engines. In *Transactions on Computational Science*. 4, (2009), 1-22.

ELBAZ, R., TORRES, L., SASSATELLI, G., GUILLEMIN, P., ANGUILLE, C., BARDOUILLET, M., BUATOIS, C., and RIGAUD, J. Hardware engines for bus encryption: a survey of existing techniques. In *Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE)*. (2005).

ENCK, W., BUTLER, K., RICHARDSON, T., MCDANIEL, P., and SMITH, A. Defending against attacks on main memory persistence. In *Proceedings of the 24th Annual Computer Security Applications Conference*. (December 2011).

FRANTZEN, M., and SHUEY, M. StackGhost: hardware facilitated stack protection. In *Proceedings of the 10th USENIX Security Symposium*. (August 2001).

GAO, L., YANG, J., CHROBALL, M., ZHANG, Y., NGUYEN, S., and LEE, H. A low cost memory remapping scheme for address bus protection. In *Proceedings of the 15th International Conference on Parallel Architecture Compilation Techniques (PACT)*. (September 2006).

GARFINKEL, T., PFAFF, B., CHOW, J., ROSENBLUM, M., and BONEH, D. Terra: a virtual machine-based platform for trusted computing. In *Proceedings of the ACM Symposium on Operating Systems Principles (SOSP)*. (2003).

GASSEND, B., SUH, G., CLARKE, D., DIJK, M., and DEVADAS, S. Caches and hash trees for efficient memory integrity verification. In *Proceedings of the 9th International Symposium on High-Performance Computer Architecture*. (February 2003), 295.

GILMONT, T., LEGAT, J., and QUISQUATER, J. An architecture of security management unit for safe hosting of multiple agents. In *Proceedings of the International Workshop on Intelligent Communications and Multimedia Terminals*. (November 1998), 79-82.

GUERON, S. Intel advanced encryption standard (AES) instructions set. *Intel Technical Report*. (2010).

GUERON, S., GERZON, G., ANATI, I., DOWECK, J., MAOR, M., and CHO, L. A tweakable encryption mode for memory encryption with protection against replay attacks. WO patent number 2012040679. (29 March 2012).

GUERON, S., SAVAGAONKAR, U., MCKEEN, F., ROZAS, C., DURHAM, D., DOWECK, J., MULLA, O., ANATI, I., GREENFIELD, Z., and MAOR, M. Method and apparatus for memory encryption with integrity check and protection against replay attacks. WO patent number 2013002789. (3 January 2013).

HALDERMAN, J., SCHOEN, S., HENINGER, N., CLARKSON, W., PAUL, W., CALANDRINO, J., FELDMAN, A., APPELBAUM, J., and FELTEN, E. Lest we remember: cold boot attacks on encryption keys. In *Proceedings of the USENIX Security Symposium*. (February 2008).

HAYES, D., and QURESHI, S. Implications of Microsoft vista operating system for computer forensics investigations. In *Proceedings of the IEEE Systems, Applications and Technology Conference*. (May 2009), 1-9.

HENNESSY, J., and PATTERSON, D. *Computer Architecture, Fourth Edition: A Quantitative Approach*. Morgan Kaufmann Publishers Inc., San Francisco, (2006).

HONG, D., BATTEN, L., LIM, S., and DUTT, N. DynaPoMP: dynamic policy-driven memory protection for SPM-based embedded systems. In *Proceedings of the Workshop on Embedded Systems Security*. (2011).

HUNT, G., LARUS, J., ABADI, M., AIKEN, M., BARHAM, P., FAHNDRICH, M., HAWBLITZEL, C., HODSON, O., LEVI, S., MURPHY, N., STEENSGAARD, B., TARDITI, D., WOBBER, T., and ZILL, B. An overview of the singularity project. *Microsoft Research Technical Report MSR-TR-2005-135*. (2005).

JANNEPALLY, V., and SOHONI, S. Fast encryption and authentication for cache-to-cache transfers using GCM-AES. In *Proceedings of the International Conference on Sensors, Security, Software and Intelligent Systems*. (January 2009).

KAPLAN, B. RAM is key: extracting disk encryption keys from volatile memory. Master's thesis report. Carnegie Mellon University. (May 2007).

KENT, S. Protecting externally supplied software in small computers. PhD thesis, *MIT Laboratory for Computer Science, MIT-LCS-TR-255*. (March 1981).

KGIL, T., FALK, L., and MUDGE, T. ChipLock: support for secure microarchitectures. *ACM Sigarch*, 33, 1, (March 2005).

KOCHER, P., JAFFE, J., and JUN, B. Differential power analysis. In *Proceedings of the CRYPTO 19th Annual International Cryptology Conference*. 1666, (1999), 388-397.

KUHN, M. Cipher instruction search attack on the bus-encryption security microcontroller DS5002FP. In *IEEE Transactions on Computing*. 47, (October 1998), 1153-2257.

LEE, M., AHN, M., and KIM, E. I2SEMS: interconnects-independent security enhances shared memory multiprocessor systems. In *Proceedings of the International Conference on Parallel Architectures and Compilation Techniques (PACT)*. (2007).

LIE, D., THEKKATH, C., MITCHELL, M., LINCOLN, P., BONEH, D., MITCHELL, J., and HOROWITZ, M. Architectural support for copy and tamper resistant software. In *Proceedings of the 9th Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS*). (2000), 168-177.

LIPMAN, H., ROGAWAY, P., and WAGNER, D. Comments to NIST concerning AES modes of operations:ctr-mode encryption. (2000).

MARTIN, L. XTS: A mode of AES for encrypting hard disks," In *Security & Privacy, IEEE* , vol.8, no.3, May-June (2010), 68-69.

MCCLEAN, M., and MOORE, J. Securing FPGAs for red/black systems, FPGA-based single chip cryptographic solution. In the *Journal of Military Embedded Systems*. (2007).

MEL, H., and BAKER, D. *Cryptography Decrypted*. Addison-Wesley. Upper Saddle River, (2001).

MULLER, T., FREILING, F., and DEWALD, A. TRESOR runs encryption securely outside RAM. In *Proceedings of the 20th USENIX Conference on Security*. (2011).

NAGARAJAN, V., GUPTA, R., and KRISHNASWAMY, A. Compiler-assisted memory encryption for embedded processors. In *HiPPEAC*. (2007), 7-22.

OSVIK, D., SHAMIR, A., and TROMER, E. Cache attacks and countermeasures: the case of AES.

PETERSON, P. Cryptkeeper: improving security with encrypted RAM. In *Proceedings of the IEEE International Conference on Technologies for Homeland Security (HST)*. (November 2010), 120-126.

PLATTE, J., DIAZ, R., and NAROSKA, E. A new encryption and hashing scheme for the security architecture for microprocessors. In *Communications and Multimedia Security*. 4237, (October 2006), 120-129.

POLONSKY, S., KNEBEL, D., SANDA, P., MCMANUS, M., HUOTT, W., PELELLA, A., MANZER, D., STEEN, S., WILSON, S., and CHAN, Y. Non-invasive timing analysis of IBM G6 microprocessor L1 cache using backside time-resolved hot electron luminescence. In *Proceedings of the IEEE International Solid-State Circuits Conference*. (2000), 222-224.

PROVOS, N. Encrypting virtual memory. In *Proceedings of the 9th USENIX Security Symposium*. (2000).

RABAIOTTI, J., and HARGREAVES, C. Using a software exploit to image RAM on an embedded system. *Digital Investigation*. (February 2010).

RAMACHANDRAN, Z., and HUANG, D. Computing cryptographic algorithms in portable and embedded devices. *IEEE Portable*. (May 2007), 1-7.

RAVI, A., RAGHUNATHAN, A., and CHAKRADHAR, S. Tamper resistance mechanisms for secure embedded systems. *IEEE Intl. Conf. on VLSI Design*. (January 2004).

ROGERS, B., SOLIHIN, Y., and PRVULOVIC, M. Memory predecryption: hiding the latency overhead of memory encryption. in *ACM SIGARCH Computer Architecture News*, 33, 1, (March 2005), 27-33.

ROGERS, B., CHHABRA, S., SOLIHIN, Y., and PRVULOVIC, M. Using address independent seed encryption and bonsai merkle trees to make secure processors OS and performance friendly. In *Proceedings of the 40th International Symposium on Microarchitecture, IEEE Computer Society*. (2007), 183-196.

ROGERS, B., PRVULOVIC, M., and SOLIHIN, Y. Efficient data protection for distributed shared memory multiprocessors. In *Proceedings of the 15th International Conference on Parallel Architectures and Compilation Techniques (PACT)*. (September 2006).

ROGERS, B., CHENYU, Y., CHHABRA, S., PRVULOVIC, M., and SOLIHIN, Y. Single level integrity and confidentiality protection for distributed shared memory multiprocessors. In *Proceedings of the 14th International Symposium on High Performance Computer Architecture*. (2008), 161-172.

ROMANOSKY, S., TELANG, R., and ACQUISTI, A. Do data breach disclosure laws reduce identify theft. Carnegie Mellon Technical Report. (2008)

SHI, W., LEE, H., GHOSH, M., and LU, C. Architectural support for high speed protection of memory integrity and confidentiality in multiprocessor systems. In *Proceedings of the 13th International Conference on Parallel Architecture and Compilation Techniques (PACT)*. (2004).

SIMMONS, P. Security through amnesia: a software-based solution to the cold boot attack on disk encryption. In *Proceedings of the 27th Annual Computer Security Applications Conference*. (December 2011).

SMITH, S. Magic boxes and boots: security in hardware. In *IEEE Computer Software*. (October 2004), 106-109.

STEIL, M. 17 mistakes Microsoft made in the xbox security system. In *Proceedings of the 22nd Chaos Communication Congress*. (2005).

STEIL, M., and DOMKE, F. The Xbox 360 Security System and its Weaknesses. Google TechTalk available at http://www.youtube.com/watch?v=uxjpmc8ZIxM August (2008)

SU, L., COURCAMBICK, S., GUILLEMIN, P., SCHWARZ, C., and PASCALET, R. SecBus: operating system controlled hierarchical page-based memory bus protection. *EDAA*. (2009).

SU, L., MARTINEZ, A., GUILLEMIN, P., CERDAN, S., PACALET, R. Hardware mechanism and performance evaluation of hierarchical page-based memory bus protection. In *Proceedings of the Conference on Design, Automation and Test in Europe (DATE)*. (2009).

SUH, G., CLARKE, D., GASSEND, B., DIJK, M., and DEVADAS, S. Aegis: architecture for tamper-evident and tamper-resistant processing. In *Proceedings of the 17th International Conference on Supercomputing*. (June 2003).

SUH, G., CLARKE, D., GASSEND, B., DIJK, M., and DEVADAS, S. Efficient memory integrity verification and encryption for secure processors. In *Proceedings of the 36th International Symposium on Microarchitecture*. (2005).

SUH, G., O'DONELL, C., and DEVADAS, S. Aegis: a single-chip secure processor. In *IEEE Design and Test of Computers*. (2007).

VANDANA, G. Exploring trusted platform module capabilities: a theoretical experimental study. Doctor of Philosophy in Computer Science Dissertation. (May 2008).

WOLLINGER, T., GUAJARDO, J., and PAAR, C. Cryptography in embedded systems: an overvies. In *Proceedings of the Embedded World 2003 Conference*. (February 2003), 735-744.

YAN, C., ROGERS, B., ENGLENDER, D., SOLIHIN, Y., and PRVULOVIC, M. Improving cost performance and security of memory encryption and authentication. In *Proceedings of the 33rd International Symposium on Computer Architecture*. (June 2006).

YANG, J., GAO, L., and ZHANG, Y. Improving memory encryption performance in secure processors. In *IEEE Transactions on Computing*. (May 2005).

ZHANG, Y., GAO, L., YANG, J., ZHANG, X., and GUPTA, R. SENSS: security enhancement to symmetric shared memory multiprocessors. In *Proceedings of the 11th International Symposium on High-Performance Computer Architecture*. (February 2005).

ZHUANG, X., ZHANG, T., and PANDE, S. Hide: an infrastructure for efficiently protectiong information leakage on the address bus. In *Proceedings of the 11th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*. (October 2004). 72-84.