AMD – The Obituary

Viceroy analyze CTS Labs' report exposing fatal security vulnerabilities across AMD products

CTS Labs, a cyber-security research firm, released its findings on www.amdflaws.com. These findings demonstrate that AMD's key products, and it basis for profitability and growth, the EPYC and Ryzen processors, contain severe and pervasive security flaws that put users and organizations at an unacceptable and damaging risk. We understand that these flaws are difficult, some practically impossible, to patch.

We believe that AMD was compelled to release products as quickly and cheaply as possible as it was falling behind its competitors. This has led to what appears to be complete oversight or negligence of security **fundamentals** of AMD's products, which promote an evidently misguided competitive advantage – particularly with its Secure Processor (a.k.a. Platform Security Processor or PSP) – of providing "the greatest peace of mind on every AMD product."[1]. **Nothing could be further from the truth.**

Viceroy, in consultation with experts, have evaluated CTS's report. We believe **the issues identified by CTS are fatal to AMD on a commercial level, and *outright dangerous* at an international level**.

In light of CTS's discoveries, the meteoric rise of AMD's stock price now appears to be totally unjustified and entirely unsustainable. **We believe AMD is worth $0.00 and will have no choice but to file for Chapter 11 (Bankruptcy) in order to effectively deal with the repercussions of recent discoveries.**

- **AMD must immediately stop selling its Ryzen and EPYC processors –**The identified vulnerabilities in AMD's EPYC and Ryzen processors give hackers the ability to entrench malware at the hardware level, making them **virtually *undetectable and untouchable*** by security products. By abusing these vulnerabilities at the Secure Processor level, malware characteristics **can give hackers *unlimited control* over entire networks.** None of the vulnerabilities identified by CTS, both firmware and hardware, require physical access to computers to be exploited. The continued sale of these processors puts customers at significant risk. AMD must cease the sale of Ryzen and EPYC chips in the interest of public safety.
  - **The security protocols that AMD has been promoting to server customers are rendered useless in light of vulnerabilities identified by CTS** – We expect AMD cloud customers including Microsoft Azure, Baidu, DellEMC and TenCent will flee in the short term given the serious nature of chip flaws. AMD is unlikely to be trusted in this space again. We understand that one user could essentially compromise entire cloud networks **(i.e. all data from all customers).**
  - **Just one Ryzen chip could endanger an entire enterprise network –** Vulnerabilities identified in the Ryzen chip allow hackers to perform credential dumps on infected Ryzen work stations even if latest security mitigations are employed. Malware can quickly spread to other work stations throughout enterprise networks, regardless of whether they use a Ryzen chip or Intel. No prudent CISO or CTO will risk their network or their security by buying a Ryzen chip over more secure competitors.
  - **AMD's flawed chips are components in government and defense products –** AMD is pushing Embedded Ryzen and EPYC chips into government and defense industries – from aerospace through to enterprise servers and laptops – through promotion of "advanced security" of its Secure Processor – the very Secure Processor which CTS has found to be fundamentally flawed and open to hacking.

- **Negligent outsourcing in quest for superior margins** – In an apparently desperate attempt to compete with Intel, AMD has outsourced its Chipset, a central system component, to ASMedia and integrated it into its Ryzen PC, white-labeling it as AMD. According to CTS, a perfunctory security audit of the chipset would have discovered manufacturer backdoors. Manufacturer backdoors are extremely dangerous and for that reason not found within any competitor's products. ASMedia's parent company, AsusTek (TPE:2357), recently settled FTC charges alleging its home routers and cloud services were insecure and put customers at risk. The settlement requires AsusTek's security program be subject to independent audits for the next 20 years. It is astounding that AMD would even consider engaging AsusTek to produce vital security components.

[1] https://www.amd.com/en/technologies/security

Either **AMD failed to perform a satisfactory audit of its outsourced product, or simply ignored warnings and potential repercussions to its customers.**

- **Vulnerabilities are difficult to patch if patching is possible at all. Product recalls are warranted –** CTS identified a number of vulnerabilities at the hardware level (“logic gates[2]”) which may be not patchable. From discussions with experts: in the most optimistic of scenario it will take AMD many months to patch vulnerabilities on its devices. If AMD fails to find a workaround almost instantly, we believe a full recall in the interest of public safety would be necessary and enforced if need be. The Product Safety Commission has the power to force cessation of sale and obtain orders for product recall if the product if deemed to “present a substantial product hazard”.
  - **AMD appears to have lied about its patches before –** In December 2017, AMD reluctantly provided a patch to disable the Secure Processor following severe pressure from the cyber-security community, who were suspicious of locked-down closed source software. Contrary to AMD’s description of the patch, CTS found the patch only partially disables the Secure Processor: it remains vulnerable to attackers even when “disabled”.

- **Extended investigations –** We expect a litany of negative news, as additional vulnerabilities emerge through further scrutinization of AMD products. CTS’s report shows some of these vulnerabilities to be elementary failures. Now that CTS has sent their findings to major cyber-security firms, including AMD customers, **it is likely that additional vulnerabilities will be identified which AMD will also have to address**. Given AMD’s apparent total lack of fundamental security capabilities, **we expect that vulnerabilities will extend across AMD’s GPU product lines.**

- **Regulatory and legal issues may exacerbate problems for AMD –** While cybersecurity regulation is still in its nascent stages, it is becoming an increasingly important issue for company boards and management teams. This includes heightened scrutiny by the SEC, who recently released guidelines on timely cybersecurity disclosure following Spectre and Meltdown issues. Homeland security have also recently outlined proposals to integrate vetting of cyber-risks to the Government supply chains. We believe that AMD’s misleading representation of the security of its products have a wide host of potential regulatory and legal repercussions, including but not limited to product liability issues, warranty protections, and false advertising, which may all lead to various fines and lawsuits.

- **The CTS report is fatal to AMD growth story** – Ceasing sales and recalls would lead to unprecedented losses and limited cash to service debt and fund the research and development. AMD investments in research and development are already significantly lower than both Intel and Nvidia, and also spread across both CPUs and GPUs.

- **Management have been cashing out –** Since November 2016, AMD’s CEO has sold over 2.8 million shares of AMD, amounting to ~US$30 million, on the open market. In total, the management team has sold over 9 million shares of AMD since November 2016. Not one member of AMD’s management acquired one stock in the open market for over a year. Viceroy perceive this as a red flag, where management do not think AMD’s prospects are as rosy as portrayed to investors.

We believe AMD’s numerous vulnerabilities and seeming general disregard for basic security protocols make their products beyond unpurchaseable and outright dangerous. **Viceroy’s consultants advise that it would be blatantly irresponsible for any Chief Information Security Officer (“CISO”) or Chief Technology Officer (“CTO”) to justify the purchase of AMD’s products.**

As the product lifecycle of AMD’s older products wind down, AMD’s profitability is entirely reliant on the success of Ryzen and EPYC, particularly in light of the volatility of the crypto-currency mining market which we believe to be the major driver of AMD’s GPUs. We believe that demand for Ryzen, EPYC and other AMD’s products will be non-existent, AMD will no longer be profitable and riddled with massive liquidity issues and we do not believe there is hope for recovery.

[2] https://www.coursera.org/learn/build-a-computer/lecture/Aqrh6/unit-1-3-logic-gates

*AMD's CEO, Lisa Su, in a recent interview with CNBC, commented that "when we have high performance processors, security is job one". **AMD has evidently failed job one.***

In light of CTS's discoveries, the meteoric rise of AMD's stock price now appears to be totally unjustified and entirely unsustainable. **We believe AMD is worth $0.00 and will have no choice but to file for Chapter 11 (Bankruptcy) in order to effectively deal with the repercussions of recent discoveries.**

Important Disclaimer – Please read before continuing

This report has been prepared for educational purposes only and expresses our opinions. This report and any statements made in connection with it are the authors' opinions, which have been based upon publicly available facts, field research, information, and analysis through our due diligence process, and are not statements of fact. All expressions of opinion are subject to change without notice, and we do not undertake to update or supplement any reports or any of the information, analysis and opinion contained in them. We believe that the publication of our opinions about public companies that we research is in the public interest. We are entitled to our opinions and to the right to express such opinions in a public forum. You can access any information or evidence cited in this report or that we relied on to write this report from information in the public domain.

To the best of our ability and belief, all information contained herein is accurate and reliable, and has been obtained from public sources we believe to be accurate and reliable, and who are not insiders or connected persons of the stock covered herein or who may otherwise owe any fiduciary duty or duty of confidentiality to the issuer. We have a good-faith belief in everything we write; however, all such information is presented "as is," without warranty of any kind – whether express or implied.

In no event will we be liable for any direct or indirect trading losses caused by any information available on this report. Think critically about our opinions and do your own research and analysis before making any investment decisions. We are not registered as an investment advisor in any jurisdiction. By downloading, reading or otherwise using this report, you agree to do your own research and due diligence before making any investment decision with respect to securities discussed herein, and by doing so, you represent to us that you have sufficient investment sophistication to critically assess the information, analysis and opinions in this report. You should seek the advice of a security professional regarding your stock transactions.

This document or any information herein should not be interpreted as an offer, a solicitation of an offer, invitation, marketing of services or products, advertisement, inducement, or representation of any kind, nor as investment advice or a recommendation to buy or sell any investment products or to make any type of investment, or as an opinion on the merits or otherwise of any particular investment or investment strategy.

Any examples or interpretations of investments and investment strategies or trade ideas are intended for illustrative and educational purposes only and are not indicative of the historical or future performance or the chances of success of any particular investment and/or strategy.

As of the publication date of this report, you should assume that the authors have a direct or indirect interest/position in all stocks (and/or options, swaps, and other derivative securities related to the stock) and bonds covered herein, and therefore stand to realize monetary gains in the event that the price of either declines.

The authors may continue transacting directly and/or indirectly in the securities of issuers covered on this report for an indefinite period and may be long, short, or neutral at any time hereafter regardless of their initial recommendation.

Introduction

This report is a financial analysis as to the impact these vulnerabilities will have on AMD as a company and as such will rely heavily on the contents of CTS' report.

We understand that CTS are not at liberty to disclose certain information about the technical vulnerabilities in full detail for security purposes. Such disclosure would risk providing hackers with the information needed to exploit AMD's customers, potentially causing irreparable damage and risking threats to national security. We note again that all of CTS' findings, including those details not published here, have been validated by independent third parties provided to government agencies and major security experts, including Microsoft.

We note that it is possible that hackers have already identified these vulnerabilities and as such may already be sitting undetected and unreachable on systems that have a Ryzen or EPYC CPU.

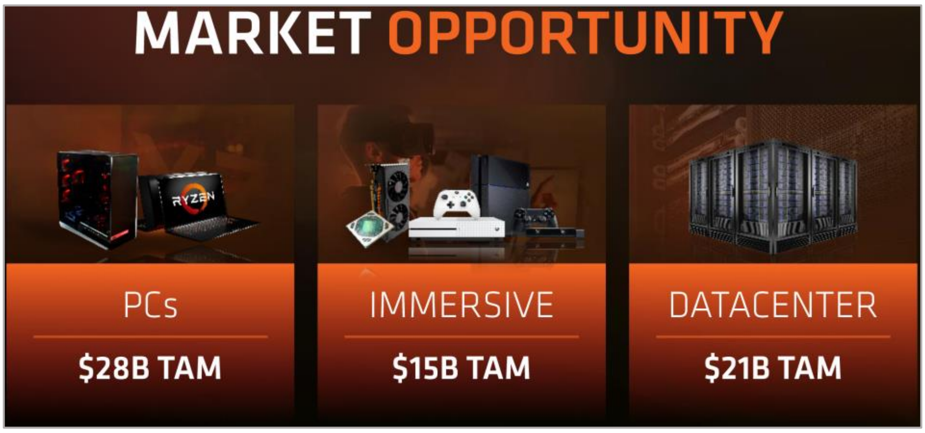
Through consultation with cyber security experts, we understand that many aspects of the findings in CTS' report were shocking, including:

- The sheer number of vulnerabilities that CTS discovered in such a short time;
- The scope of security issues associated with the vulnerabilities in the products;
- The fact that a number of the vulnerabilities would not exist had AMD followed basic cybersecurity principles; and
- The existence of vulnerabilities which should have been caught by even a cursory security audit.

The vulnerabilities that CTS identified have major repercussions for the following AMD product lines:

- Ryzen Workstation
- Ryzen Pro
- Ryzen Mobile
- EPYC Server

Together, the Ryzen and EPYC chips have total addressable markets of US$49 billion. This is far greater than AMD's graphics and semi-custom segment, with a total addressable market of US$15 billion. This is represented in Figure 1 below as the combined PC and datacenter segments, contrasted with the Immersive segment



MARKET OPPORTUNITY

PCs
$28B TAM

IMMERSIVE
$15B TAM

DATACENTER
$21B TAM

Figure 1 Extract from AMD FY2017 Investor Presentation[3]

These product lines compromised by the newly revealed are AMD's most important product with the largest total addressable markets.

[3] http://ir.amd.com/static-files/bdd95d7a-a689-487b-8da5-8bc3cdbacf5c

Product Overview

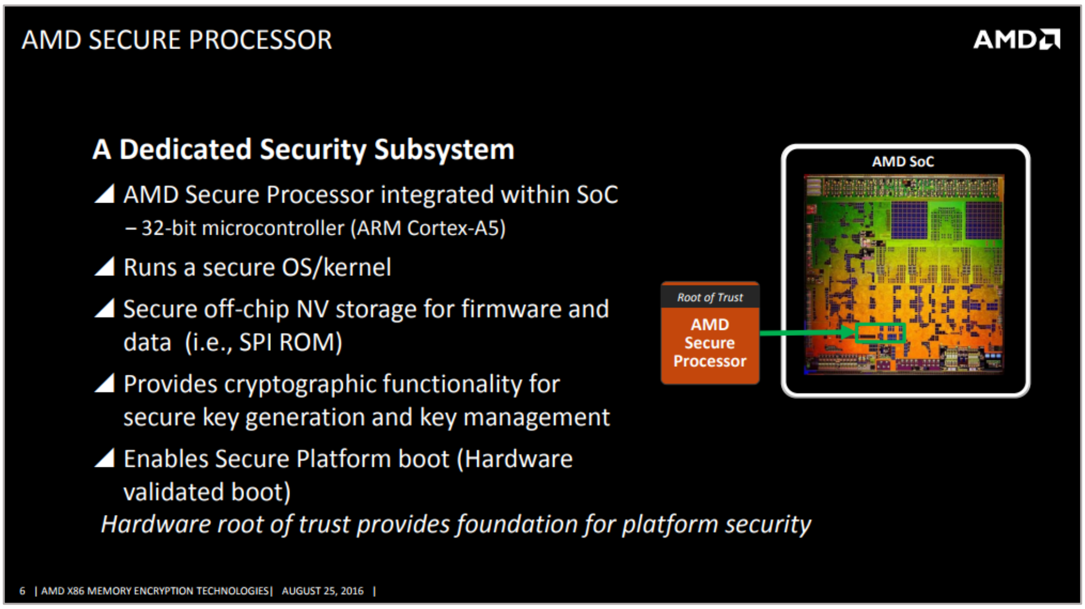
Viceroy believes much of the current positive market sentiment around AMD is due to the rapid growth and implied future performance of their Ryzen and EPYC product lines. We believe that the CTS revelations will kneecap AMD's acceptance in these markets.

The (un)Secure Processor

AMD's Secure Processor is the foundation of its promotional drive claiming state-of-the-art security, and a major selling point for its EPYC and Ryzen products. **A flawed Secure Processor means a completely flawed security system, which will be unacceptable to customers.**

The CTS report identifies a number of vulnerabilities on AMD's Secure Processor itself that give an attacker full control of the Secure Processor, and therefore, full control of the entire security system.

Even more worrying is that the inclusion AMD's Secure Processor is not limited to Ryzen and EPYC. AMD has already introduced – and continues to introduce – its highly flawed Secure Processor into other products, substantially increasing the potential for additional hacking attacks.



AMD SECURE PROCESSOR

AMD

A Dedicated Security Subsystem

- AMD Secure Processor integrated within SoC
  – 32-bit microcontroller (ARM Cortex-A5)
- Runs a secure OS/kernel
- Secure off-chip NV storage for firmware and data (i.e., SPI ROM)
- Provides cryptographic functionality for secure key generation and key management
- Enables Secure Platform boot (Hardware validated boot)

Hardware root of trust provides foundation for platform security

6 | AMD X86 MEMORY ENCRYPTION TECHNOLOGIES| AUGUST 25, 2016 |

Figure 2 Extract from AMD Secure Processor release announcement

Simply put: AMD's poor execution of its most important hardware has given hackers ability to exploit all of its customers' systems and networks.

Hardware security has become a top priority for customers due to the increasing sophistication of cyber-attackers' arsenals. This Secure Processor has become a key selling point for both EPYC and Ryzen.

Following the Spectre and Meltdown attacks, many saw an opportunity for AMD to assert itself as the industry leader in providing the most secure chips. AMD's Secure Processor was seen as the "knight in shining armor".

Hackers attempted to manipulate Intel's Management Engine, the equivalent to AMD's Secure Processor, for 11 years, and were only able to finally disable the engine in December 2017, and over the past 12 years, they only found one vulnerability and only through physical access to the hardware. CTS were able to *remotely* take full control of AMD's Secure Processor in less than 7 months[4].

[4] https://www.blackhat.com/docs/eu-17/materials/eu-17-Goryachy-How-To-Hack-A-Turned-Off-Computer-Or-Running-Unsigned-Code-In-Intel-Management-Engine.pdf

Ryzen

AMD's Ryzen product is key to an AMD strategic goal of relevant in the PC market, as it represents a far higher quality offering than the AMD 7th Generation APU.

The Ryzen release was among the most significant drivers of increasing sales and gross margins for AMD in FY2017, and is expected to continue to be a significant driver in FY2018, particularly with the ramp up Ryzen Mobile, which should push up ASPs and the winding down in sales of the old generation products.

As can be seen below, the Ryzen desktop and Ryzen Mobile are geared towards the premium market.

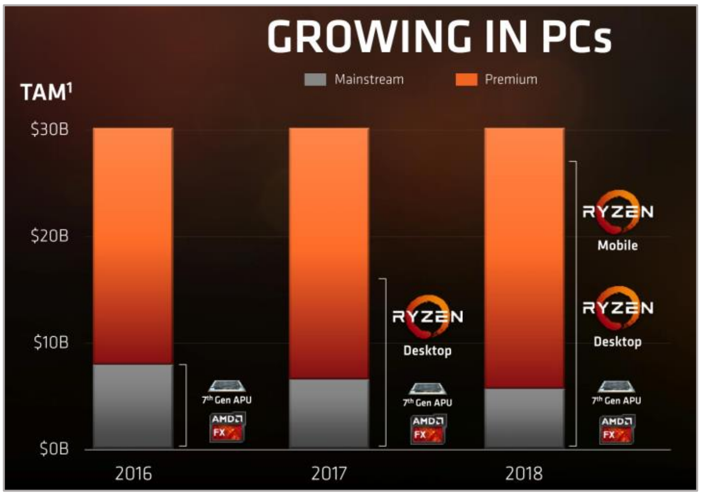
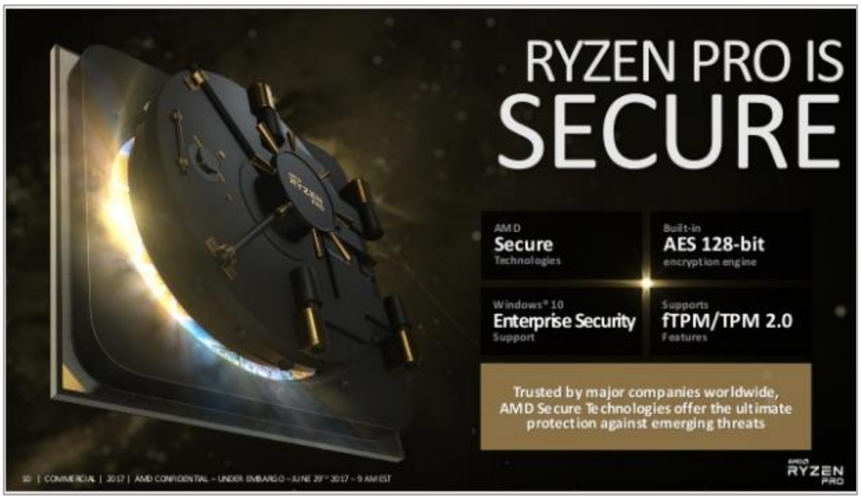


Figure 3 Extract from AMD FY2017 Investor Presentation[5]

Marketing materials for the Ryzen PRO heavily emphasize its security; particularly to the high-margin enterprise market:



RYZEN PRO IS SECURE

AMD **Secure** Technologies

Built-in **AES 128-bit** encryption engine

Windows® 10 **Enterprise Security** Support

Supports **fTPM/TPM 2.0** Features

Trusted by major companies worldwide, AMD Secure Technologies offer the ultimate protection against emerging threats

10 | COMMERCIAL | 2017 | AMD CONFIDENTIAL – UNDER EMBARGO – JUNE 29th 2017 – 9 AM EST

AMD RYZEN PRO

Figure 4 Extract from AMD Ryzen Pro presentation [6]

EPYC

The EPYC chip was launched with great fanfare in June 2017 and heralded AMD's re-entry to the server market after a decade. The launch included presentations from AMD's new server customers, including HP, Microsoft Azure, Baidu, Tencent and Dell EMC.

[5] http://ir.amd.com/static-files/bdd95d7a-a689-487b-8da5-8bc3cdbacf5c

[6] https://www.slideshare.net/pertonas/amd-ryzen-pro

AN EPYC BEGINNING

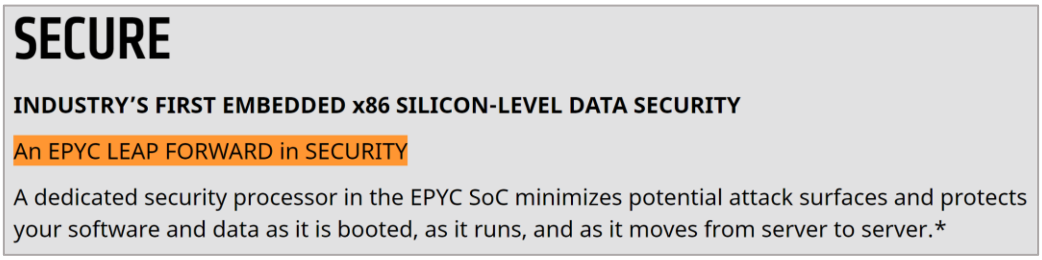
DR. LISA SU

PRESIDENT AND CEO

Figure 5 Extract from AMD EPYC release announcement[7]

The total addressable market for servers is huge and growing, and also has the highest potential gross margins of any of AMD's business segments. AMD recently announced the launch of EPYC Embedded and Ryzen Embedded, which it hopes to bring to networking, storage and industrial solutions markets, with AMD stressing that these include the on-chip security.[8] This is very worrying, considering the ultra-sensitive nature of these targeted markets and industries, includes defense and aerospace.

AMD described the Secure Processor's role for the EPYC chip as "An EPYC LEAP FORWARD in Security":



SECURE

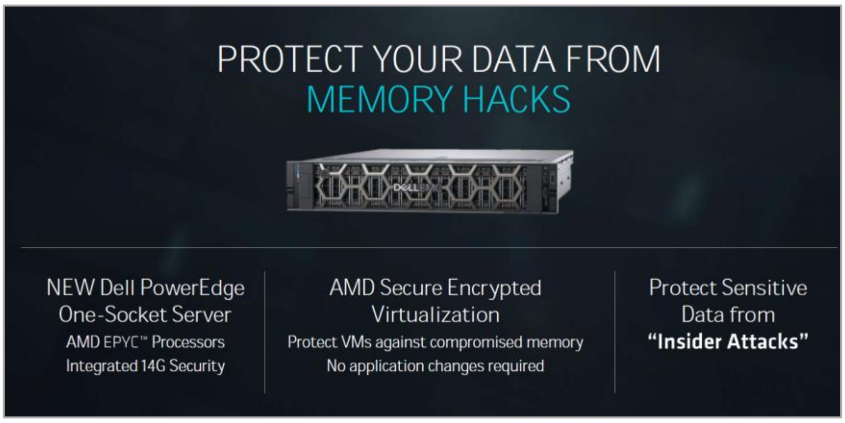
INDUSTRY'S FIRST EMBEDDED x86 SILICON-LEVEL DATA SECURITY

An EPYC LEAP FORWARD in SECURITY

A dedicated security processor in the EPYC SoC minimizes potential attack surfaces and protects your software and data as it is booted, as it runs, and as it moves from server to server.*

Figure 6 Extract from AMD webpage "Datacenter workloads"

The importance of this security to EPYC customers is evident from this slide presented by Dell at the EPYC launch and from white papers published by AMD customers including as Dell.



PROTECT YOUR DATA FROM MEMORY HACKS

NEW Dell PowerEdge One-Socket Server

AMD EPYC™ Processors

Integrated 14G Security

AMD Secure Encrypted Virtualization

Protect VMs against compromised memory

No application changes required

Protect Sensitive Data from **"Insider Attacks"**

Figure 7 Extract from AMD EPYC release announcement[9]

Security is the largest concern for the server market and for cloud providers in particular.

[7] http://ir.amd.com/static-files/3fc34d2c-ec46-4dd0-8db7-74389fb72779

[8] https://www.amd.com/en-us/press-releases/Pages/amd-launches-EPYC-embedded-2018feb21.aspx

[9] http://ir.amd.com/static-files/3fc34d2c-ec46-4dd0-8db7-74389fb72779

Vulnerabilities

Due to the security risk of publishing execution details of the vulnerabilities, the descriptions contained in CTS's report of AMD are limited to their findings. The full vulnerabilities have been validated by independent third-parties with extensive experience in the cyber-security industry. Below is a list of the vulnerabilities and a brief description of their mechanism of action.

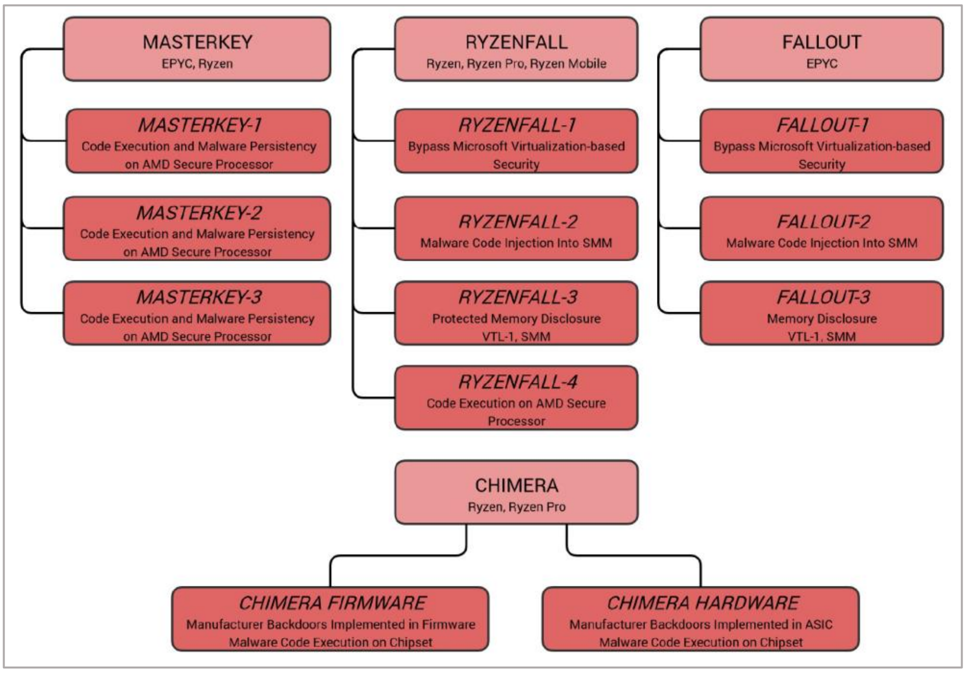

MASTERKEY
EPYC, Ryzen
MASTERKEY-1
Code Execution and Malware Persistency on AMD Secure Processor
MASTERKEY-2
Code Execution and Malware Persistency on AMD Secure Processor
MASTERKEY-3
Code Execution and Malware Persistency on AMD Secure Processor
RYZENFALL
Ryzen, Ryzen Pro, Ryzen Mobile
RYZENFALL-1
Bypass Microsoft Virtualization-based Security
RYZENFALL-2
Malware Code Injection Into SMM
RYZENFALL-3
Protected Memory Disclosure VTL-1, SMM
RYZENFALL-4
Code Execution on AMD Secure Processor
FALLOUT
EPYC
FALLOUT-1
Bypass Microsoft Virtualization-based Security
FALLOUT-2
Malware Code Injection Into SMM
FALLOUT-3
Memory Disclosure VTL-1, SMM
CHIMERA
Ryzen, Ryzen Pro
CHIMERA FIRMWARE
Manufacturer Backdoors Implemented in Firmware Malware Code Execution on Chipset
CHIMERA HARDWARE
Manufacturer Backdoors Implemented in ASIC Malware Code Execution on Chipset

Figure 8 Extract of CTS report

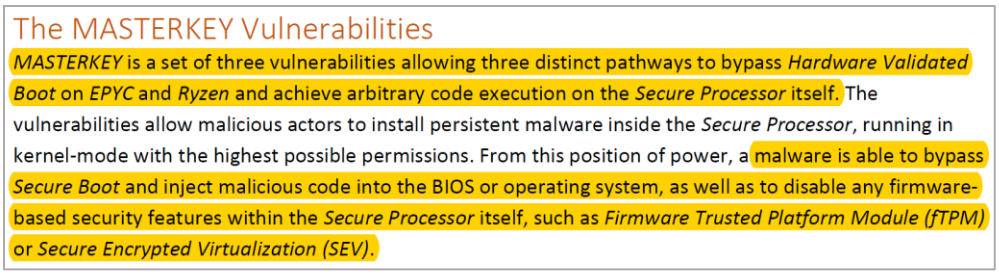
Note that three of the vulnerabilities; Masterkey, Ryzenfall and Fallout, are associated with the AMD processors. The fourth vulnerability, Chimera, is a result of a glaring oversight in the manufacture of the Ryzen chipset.

Viceroy's commentary on AMD will be more specific to the impact of CTS's findings on a commercial level. Please see CTS's report for greate detail on the specifics of the vulnerabilities:

www.amdflaws.com

We have annexed the summary segment of the above flaws highlighted by CTS in this report.

Masterkey



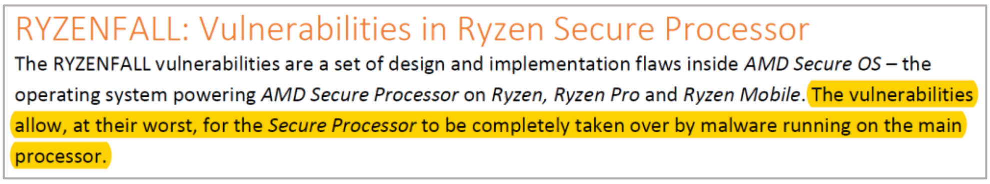
The MASTERKEY Vulnerabilities

MASTERKEY is a set of three vulnerabilities allowing three distinct pathways to bypass *Hardware Validated Boot* on *EPYC* and *Ryzen* and achieve arbitrary code execution on the *Secure Processor* itself. The vulnerabilities allow malicious actors to install persistent malware inside the *Secure Processor*, running in kernel-mode with the highest possible permissions. From this position of power, a malware is able to bypass *Secure Boot* and inject malicious code into the BIOS or operating system, as well as to disable any firmware-based security features within the *Secure Processor* itself, such as *Firmware Trusted Platform Module (fTPM)* or *Secure Encrypted Virtualization (SEV)*.

Figure 9 Extract of CTS report

The Masterkey fault consists of three vulnerabilities which allow attackers to bypass the AMD-specific Hardware Validated Boot (HVB) mechanism, through which the Secure Processor first boots up the computer. Masterkey leverages the Secure Processor's privileges to wreak havoc on target computers.

Ryzenfall

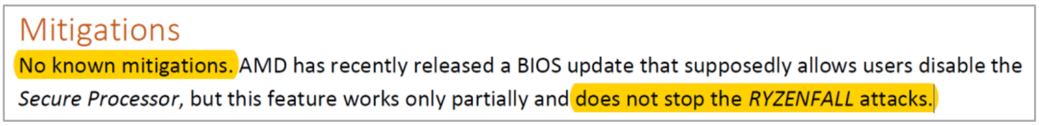


RYZENFALL: Vulnerabilities in Ryzen Secure Processor

The RYZENFALL vulnerabilities are a set of design and implementation flaws inside *AMD Secure OS* – the operating system powering *AMD Secure Processor* on *Ryzen, Ryzen Pro* and *Ryzen Mobile*. The vulnerabilities allow, at their worst, for the *Secure Processor* to be completely taken over by malware running on the main processor.

Figure 10 Extract of CTS report

Ryzenfall's most concerning impact is its weakness in allowing hackers to engage in **arbitrary code execution on the Secure Processor**, essentially allowing an attacker to execute **any command of their choice** on a target Ryzen or Ryzen Pro Secure Processor.

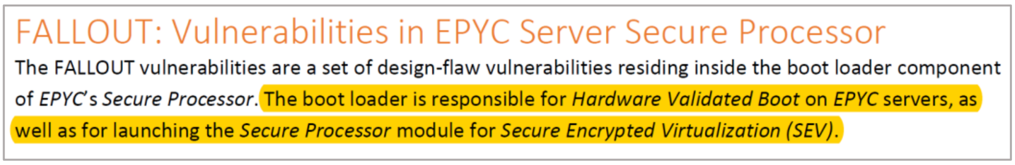


Mitigations

No known mitigations. AMD has recently released a BIOS update that supposedly allows users disable the *Secure Processor*, but this feature works only partially and does not stop the *RYZENFALL* attacks.

Figure 11 Extract of CTS report

Fallout

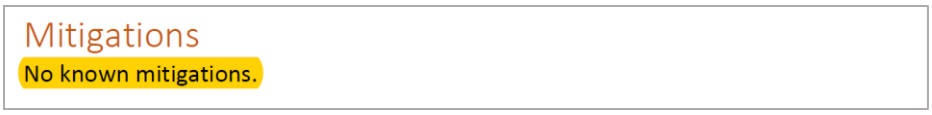


FALLOUT: Vulnerabilities in EPYC Server Secure Processor

The FALLOUT vulnerabilities are a set of design-flaw vulnerabilities residing inside the boot loader component of *EPYC*'s *Secure Processor*. The boot loader is responsible for *Hardware Validated Boot* on *EPYC* servers, as well as for launching the *Secure Processor* module for *Secure Encrypted Virtualization (SEV)*.

Figure 12 Extract of CTS report

We have detailed the nature and impact of the vulnerabilities in the HVB under the *Masterkey* section above, however the boot loader Fallout vulnerabilities further highlight the crippling security oversights in the design and implementation of AMD's EPYC server processors.

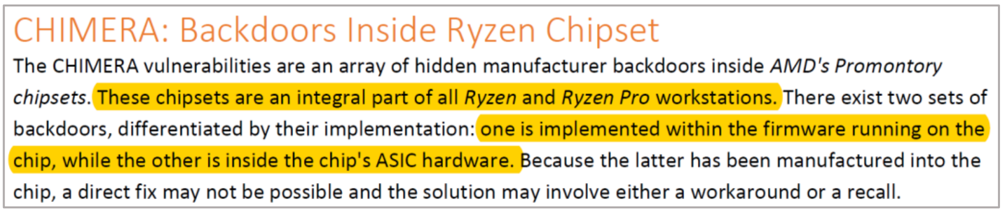


Mitigations

No known mitigations.

Figure 13 Extract of CTS report

Chimera



CHIMERA: Backdoors Inside Ryzen Chipset

The CHIMERA vulnerabilities are an array of hidden manufacturer backdoors inside *AMD's Promontory chipsets*. These chipsets are an integral part of all *Ryzen* and *Ryzen Pro* workstations. There exist two sets of backdoors, differentiated by their implementation: one is implemented within the firmware running on the chip, while the other is inside the chip's ASIC hardware. Because the latter has been manufactured into the chip, a direct fix may not be possible and the solution may involve either a workaround or a recall.

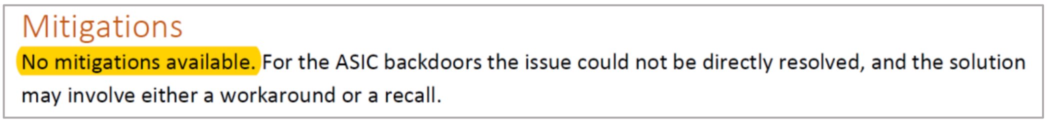
Figure 14 Extract of CTS report

Chimera differs from the other three vulnerabilities discovered by CTS as its involves the use of a manufacturer backdoor. CTS's report claims that this is due to AMD's use of ASMedia-manufactured chipsets all of which have displayed the same glaring inclusion of manufacturer backdoors.

Readers will note that hardware manufacturers **such as Apple have historically objected to the introduction of backdoors in a finished product even under pressure from the FBI**[10].

AMD's Ryzen and EPYC appear to have backdoors **built in**.

[10] https://www.apple.com/customer-letter/



Mitigations

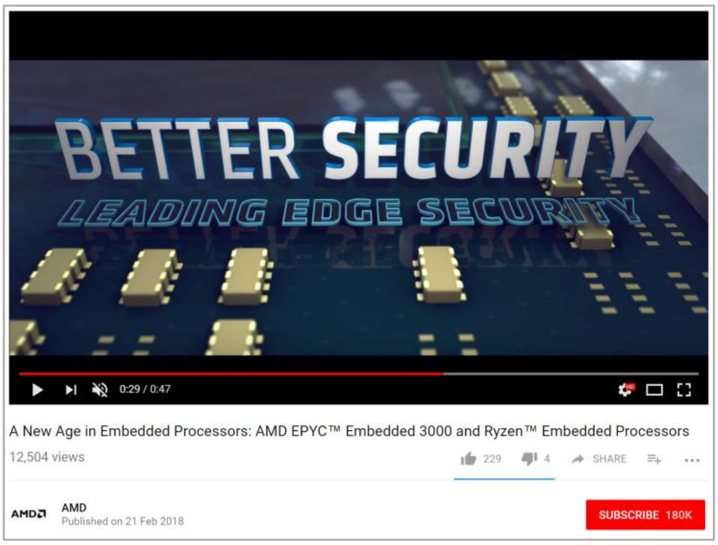
No mitigations available. For the ASIC backdoors the issue could not be directly resolved, and the solution may involve either a workaround or a recall.

Figure 15 Extract of CTS report

Practical implications from identified flaws

As the three vulnerabilities named Masterkey, Ryzen and Fallout all affect the Secure Processor, the possible implications for customers can be devastating.

We note the following slides from a recent AMD video advertising their embedded processors, which stresses AMD's security capabilities again and again[11]:



A New Age in Embedded Processors: AMD EPYC™ Embedded 3000 and Ryzen™ Embedded Processors

12,504 views

AMD

Published on 21 Feb 2018

Figure 16 Extract from AMD YouTube video[12]

Attackers can access data for every customer on a cloud provider's server

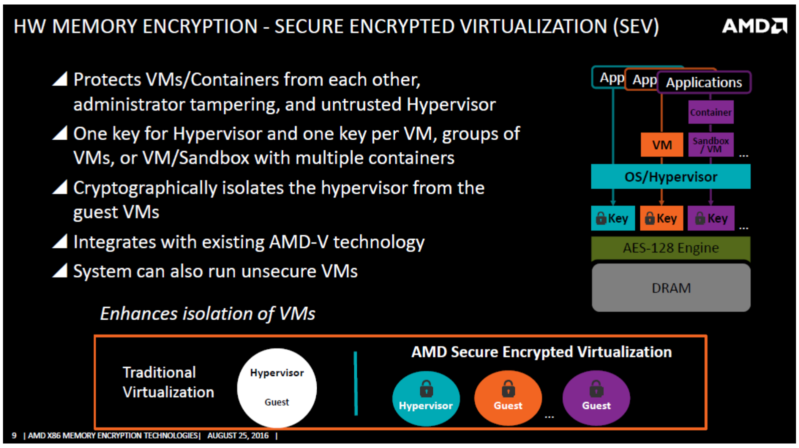
One of the key attractions of AMD's EPYC chip for cloud providers is AMD's Secured Encrypted Virtualization (SEV).

By encrypting the customer's virtual machines to which an administrator or hacker does not have access, the goal of the SEV is to protect customers by ensuring that a hacker, untrusted Hypervisor, or even a rogue administrator would not be able to read the actual underlying data. In essence, access to data is segregated and gated in order to prevent unauthorized access.

Customers of cloud providers are extremely concerned about the security of their customers' data and the risk of their data being accessed or manipulated by an unauthorized party. AMD created the SEV to allay these fears.

[11] https://www.amd.com/en

[12] https://www.youtube.com/watch?v=kwERyyABKdY



HW MEMORY ENCRYPTION - SECURE ENCRYPTED VIRTUALIZATION (SEV)

- Protects VMs/Containers from each other, administrator tampering, and untrusted Hypervisor
- One key for Hypervisor and one key per VM, groups of VMs, or VM/Sandbox with multiple containers
- Cryptographically isolates the hypervisor from the guest VMs
- Integrates with existing AMD-V technology
- System can also run unsecure VMs

Enhances isolation of VMs

Figure 17 Extract from AMD Virtual Memory Encryption presentation[13]

AMD's SEV is entirely managed by the Secure Processor. As a result, the promoted security features of AMD's SEV is compromised and useless, giving hackers access and total control over every customer's data that is stored by the cloud provider.

The vulnerability of AMD's Secure Processor to Masterkey, Ryzenfall and Fallout vulnerabilities renders SEV useless

Attackers can easily spread throughout the network

Generally speaking, the first computer hacked in a network is regarded as a "low-value target". A key objective for an attacker is to move within the network to a "high-value target" (i.e. CEO's).

Microsoft developed Windows Credential Guard to stop "credential dumping", a key mechanism used by attackers to spread through a network through credential theft.

The vulnerabilities in the Secure Processor allow hackers to perform credential dumps regardless of Windows Credential Guard. Once these credentials have been obtained, attackers are free to move about the entire enterprise network.

This also means that just one workstation with a Ryzen or EPYC chip within an enterprise network is potentially at risk, even if they remainder of users are on more secure Intel chips.

The vulnerability of AMD's Secure Processor to Masterkey, Ryzenfall and Fallout vulnerabilities renders Windows Credential Guard useless.

Attackers achieve persistency and full control

A key attack vector is the first few moments after the processor has started up, during which many security protocols are not yet active. AMD's Secure Processor verifies itself upon startup essentially giving it the highest level of privilege in the system. Any malware present on the Secure Processor is nigh-untouchable by the majority of security protocols. This ability to install malware that can remain undetected and out of the reach of anti-virus software is known as "persistency"[14].

[13] http://www.linux-kvm.org/images/7/74/02x08A-Thomas_Lendacky-AMDs_Virtualizatoin_Memory_Encryption_Technology.pdf

[14] https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf

According to CTS the Masterkey and Ryzenfall vulnerability allows hackers arbitrary code execution on the Secure Processor, essentially hijacking the security center of the processor.

AMD has essentially given hackers the keys to the kingdom, giving them unfettered control over a workstation and/or network. The AMD user would not even know that they have been hacked.

The vulnerability of AMD’s Secure Processor to Masterkey, Ryzenfall and Fallout vulnerabilities renders AMD’s Secure Boot process useless.

Attackers are free to engage in ransomware and hardware Destruction

Once a hacker sits on the Secure Processor, the hacker can introduce any code it wants, and can hijack the system at will and ransom it.

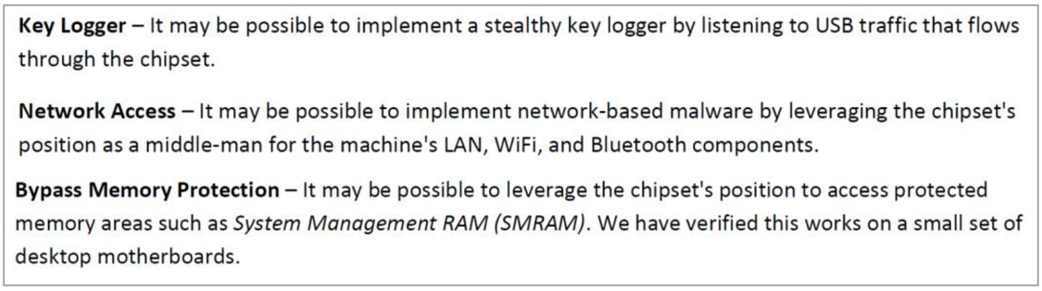
AMD Secure Processor’s vulnerabilities mean that hackers could compromise a large number of systems that have the Ryzen or EPYC chips and hold them for ransom.

Victims would be under incredible pressure to pay a ransom if they find that a large number of their workstations are being hijacked. Readers will be familiar with ransomware from the recent attacks using Wannacry[15]. Once in control, a hacker is also able to “brick” the machine by introducing bad code that can physically destroys the machine.

Implications of Chimera

According to CTS, the effects of Chimera are fairly different to those of the Masterkey, Ryzenfall and Fallout vulnerabilities. This is due to the role of the chipset and the role in the connection of a computer’s peripherals including USB host controllers, SATA and PCI Express as well as its links to the computers access to LAN, WIFI and Bluetooth.

CTS suggests Chimera vulnerabilities would allow an attacker to:



Key Logger – It may be possible to implement a stealthy key logger by listening to USB traffic that flows through the chipset.

Network Access – It may be possible to implement network-based malware by leveraging the chipset's position as a middle-man for the machine's LAN, WiFi, and Bluetooth components.

Bypass Memory Protection – It may be possible to leverage the chipset's position to access protected memory areas such as *System Management RAM (SMRAM)*. We have verified this works on a small set of desktop motherboards.

Figure 18 Composite extract from CTS Report

AMD has failed to detect and fix deeply flawed code from ASMedia which contained manufacturer backdoors in hardware (ASIC) and backdoors in firmware which **allow a hacker to read and write memory to the chip**.

Experts were shocked to find that the AMD chipset integrated with Ryzen PCs contained all the manufacturer backdoors in hardware (ASIC) and in firmware that had been present on previous ASMedia chips dating back to 2012.

[15] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

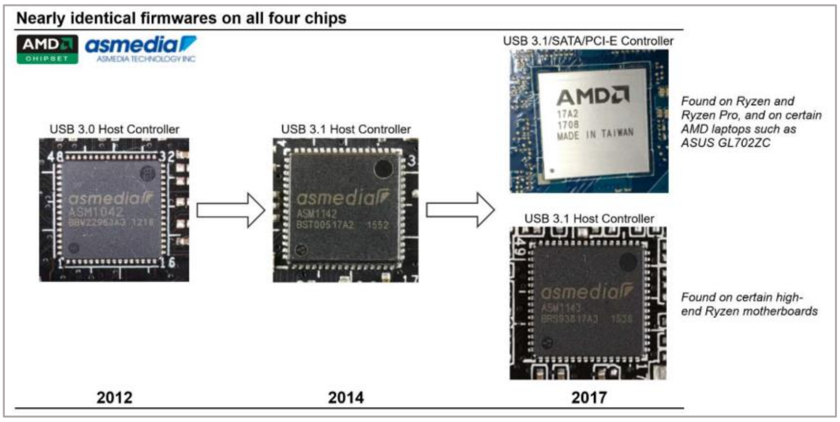

Nearly identical firmwares on all four chips
AMD CHIPSET
asmedia
ASMEDIA TECHNOLOGY INC
USB 3.0 Host Controller
USB 3.1 Host Controller
USB 3.1/SATA/PCI-E Controller
Found on Ryzen and Ryzen Pro, and on certain AMD laptops such as ASUS GL702ZC
USB 3.1 Host Controller
Found on certain high-end Ryzen motherboards
2012
2014
2017

Figure 19 Extract of CTS report

Viceroy believes that AMD outsourced this component to ASMedia because only ASMedia and Intel have the intellectual property to design USB 3.1 controllers, which are in high demand due to a large increase in speed compared to the USB 3.0 controllers.

All new Ryzen and Ryzen Pro PCs will be bundled with a compromised chipset that controls the peripherals.

ASMedia: a history of vulnerabilities

ASMedia is 41% owned by ASUSTek Computer (ASUS), a publicly-listed company in Taiwan, which produces computers under the ASUS brand. In February 2016, ASUS settled FTC charges that alleged its home routers and cloud services were insecure and put customers at risk. The settlement required ASUS to establish and maintain a comprehensive security program subject to independent audits for the next 20 years[16]. The FTC commented that they weren't just unhappy about ASUS's bogus security claims, but it's also unhappy with the company's response time[17].

It is astounding that AMD would even consider outsourcing such an integral component of their security features from ASUSTek.

In light of the FTC's imposed audits and the poor reputation around security practices at ASMedia, customers should expect that AMD had conducted extensive security audits of ASMedia's chipset and code before integrating with Ryzen to ensure that no vulnerabilities exist, particularly considering that AMD slaps its own name on the chipset, using ASMedia as a private label supplier.

Through consultation with experts, Viceroy understand that the manufacturer backdoors were so glaring that any cursory security audit would have identified the vulnerabilities within hours. CTS was able to identify these flaws from the machine code.

[16] https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put

[17] https://thehackernews.com/2016/02/asus-router-security-hack.html

All this leads us to question the presence of the backdoors:

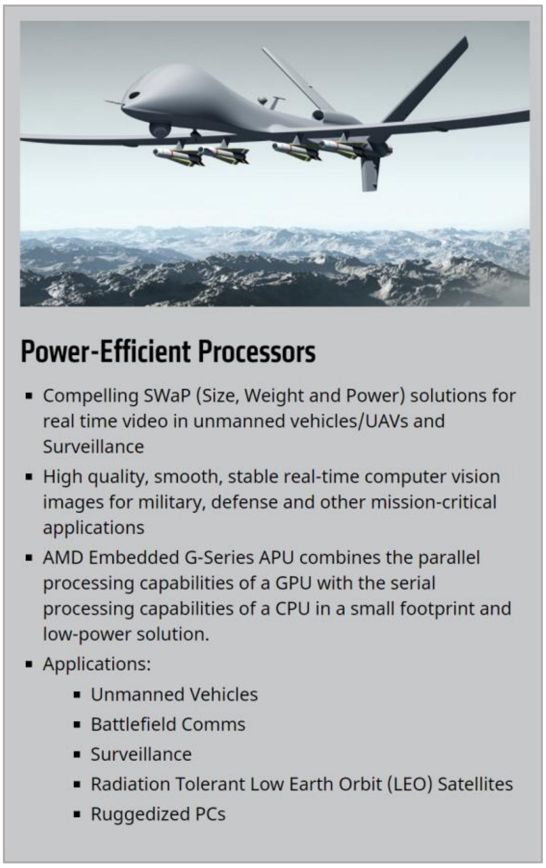
1. Does the presence of these obvious flaws mean that AMD did not conduct sufficient security audits?
2. If a security audit was even conducted, was the inclusion of the vulnerabilities a result of pure negligence by AMD's security auditors? and;
3. If AMD were aware of the vulnerabilities: did they look the other way out of a rush to release their product?

Regardless of the answer, AMD's Ryzen chipset is riddled with security vulnerabilities, failing Security 101.

Key takeaways

These products were AMD's chance to regain a foothold in high margin PCs and the server market. But in its rush to reinvent itself, AMD shot itself in the foot. Intel's security issues could have been a boon for AMD, but AMD's security flaws are far, far greater.

Viceroy believes the Masterkey, Ryzenfall and Fallout vulnerabilities will make AMD's product non-functioning and fatally erode consumer trust in the short and long term. Frighteningly, AMD claims that its main benefit to the Aerospace and Defense sector is the fundamentally flawed Secure Processor.



Power-Efficient Processors

- Compelling SWaP (Size, Weight and Power) solutions for real time video in unmanned vehicles/UAVs and Surveillance
- High quality, smooth, stable real-time computer vision images for military, defense and other mission-critical applications
- AMD Embedded G-Series APU combines the parallel processing capabilities of a GPU with the serial processing capabilities of a CPU in a small footprint and low-power solution.
- Applications:
    - Unmanned Vehicles
    - Battlefield Comms
    - Surveillance
    - Radiation Tolerant Low Earth Orbit (LEO) Satellites
    - Ruggedized PCs

Figure 20 Extract from AMD webpage "Embedded Aerospace and Defence"[18]

[18] https://www.amd.com/en/products/embedded-aero-defense-solutions

Patching - Can't AMD just patch the problem?

From consultations with experts, Viceroy understand that the collective fundamental vulnerabilities with AMD's Ryzen and EPYC product lines are practically **un-patchable**. There are at least three parts to the patching process:

1. **Programming the patch –** Programming a patch could take as little as a few days, although complex workarounds for hardware vulnerabilities are far more complex and could take months. While it is hard to anticipate the impact the patch and workarounds will have on the performance of the chip and system, a significant slowdown or loss of features and functionality, this will cause the chips to be unattractive to customers.

2. **Quality assurance –** Once a patch has been programmed it will have to go through quality assurance, which could take more than 3 months. The reason for the long delay is that if the patch has an error, it could destroy the customer's hardware.

3. **Distribution –** Once the patch has passed through quality assurance, it will then be distributed to AMD's OEM partners through AGESA (reference). The OEMs will then need to ensure that this patch is compatible with its products and will need to go through another round of quality assurance to ensure that it does not corrupt its customers' products. Once this is complete, they can then distribute the patch. The BIOS update may need a full reboot of the system and most importantly, it would need IT administrators and individuals to actually update the BIOS themselves if not done so automatically.

Within distribution, experts communicated that original equipment manufacturers (OEMs) would need to perform these three steps again in order for the patch to be fully implemented. During this time AMD's devices would be completely vulnerable.

For reference, a security researcher from Google's cloud security team identified what we understand should have been an easily patchable vulnerability in the fTPM (Firmware Trusted Platform Module) of AMD Secure Processor which required physical access to execute and reported this to AMD in late September 2017[19]. The patch was only distributed in mid-January (exact dates are OEM specific).

Patching the chipset's hardware backdoors will be very difficult because there is a design flaw in the logic gates. Before potentially being forced into a recall, AMD will attempt to create a workaround, but this could be very difficult, as blocking access to hardware backdoors could break access to USB ports or other peripherals. **There is really no simple solution to this and a recall is highly possible, although totally impractical.**

The biggest hurdle Viceroy perceive is time. From discussions with experts: in the most optimistic of scenario it will take AMD many months to patch vulnerabilities on its devices.

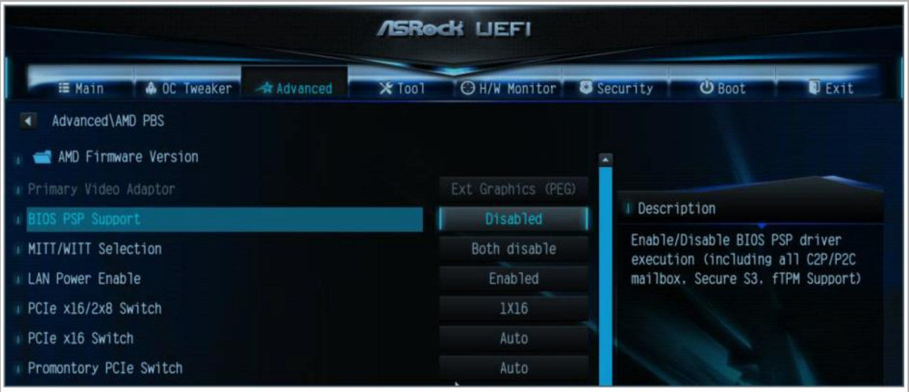
If AMD fails to find a workaround almost instantly, we believe a full recall in the interest of public safety would be necessary. The Product Safety Commission has the power to force cessation of sale and obtain orders for product recall if the product if deemed to "present a substantial product hazard".

[19] https://www.theregister.co.uk/2018/01/06/amd_cpu_psp_flaw/

AMD patches don’t always work

In December 2017, AMD reluctantly provided a patch to disable the Secure Processor following severe pressure from the cyber-security community who were suspicious of locked-down closed source software.

In their report CTS states that contrary to AMD’s description of the patch, the patch **only partially disables the** Secure Processor. Essentially even “disabling” the Secure Processor and leaves Ryzenfall vulnerabilities in the CTS report open to attackers.



Advanced\AMD PBS

AMD Firmware Version

Primary Video Adaptor	Ext Graphics (PEG)
BIOS PSP Support	Disabled
MITT/WITT Selection	Both disable
LAN Power Enable	Enabled
PCIe x16/2x8 Switch	1X16
PCIe x16 Switch	Auto
Promontory PCIe Switch	Auto

Description

Enable/Disable BIOS PSP driver execution (including all C2P/P2C mailbox, Secure S3, fTPM Support)

Disable PSP support has no effect on RYZENFALL

Figure 21 Extract of CTS report

AMD’s patch to disable the Secure Processor was evidently completely ineffective by design or by negligence. Regardless of which, this is just another example showing that AMD does not have the skills to operate in a market that requires state-of-the-art security and cannot be trusted to follow through.

The impact: an AMD autopsy

Regulation

AMD’s release of products with security vulnerabilities introduces a wide range of potential regulatory and legal issues. While cyber-security regulation is still in its nascent stages, it is becoming an increasingly important issue in light of various high-profile security breaches, including Spectre and Meltdown.

As such, regulators are introducing and implementing new pieces of cybersecurity regulation and requirements designed to protect consumers’ private data. The implicit goal of this new regulation is to increase the security within systematically important institutions and to hold companies accountable for their cybersecurity requirements. There have been two notable pieces of cybersecurity regulation released recently:

1. **Department of Financial Services Cybersecurity Regulation (US) –** regulation implemented by the Financial Services Superintendent in the US and designed to protect financial institutions. Banks, insurance companies and other financial services institutions regulated by the DFS are required to have a cybersecurity program designed to protect consumers’ private data; a written policy or policies that are approved by the board or a senior officer; a Chief Information Security Officer to help protect data and systems; and controls and plans in place to help ensure safety and soundness of the financial services industry. The first compliance date for this regulation was effective August 28, 2017.[20]

2. **Global Data Protection Regulation (EU) (GDPR)** – this is regulation implemented by EU Parliament to protect EU citizens from privacy and data breaches. The regulation introduces penalties for non-compliance including fines (4% of annual global turnover or €20M) for serious infringements such as violating the core **of “Privacy by Design” concepts.** This regulation comes into effect on May 25, 2018.[21]

[20] http://www.dfs.ny.gov/about/press/pr1708281.htm

[21] https://www.eugdpr.org/key-changes.html

Further to this regulation, shareholder derivative lawsuits have emerged targeting a number of companies who are alleged to have failed to maintain proper internal controls related to data security and misleading affected consumers regarding breaches that had occurred[22]. We would not be surprised if numerous class action claims arise on the back of CTS's research.

We believe AMD's numerous vulnerabilities and apparent lack of care for basic security protocols make their products unpurchaseable from the perspective of both the pieces of regulation outlined above. **Simply, any Chief Information Security Officer ("CISO") would be completely irresponsible if they recommended the purchase of AMD's products.**

Legal liabilities

Existing regulation would serve to augment existing laws and regulation in place that would protect consumers of AMD's products. While it is currently unclear which specific pieces of regulation or legislation would apply to the vulnerabilities associated with AMD's products, we believe the Company will face a number of issues surrounding:

1. **Product liability –** A consumer's cause of action is usually based on common law as no federal product liability law exists. This cause of action revolves around three types of claims:
    a. Breach of warranty: the ability to seek remedy when a product fails to satisfy express representations, is not merchantable, or is unfit for its particular purpose.[23]
    b. Negligence: the ability to seek remedy from the defendant for failing to use due care[24]
    c. Strict liability: the ability to seek remedy for product defect regardless of steps the manufacturer has taken[25]

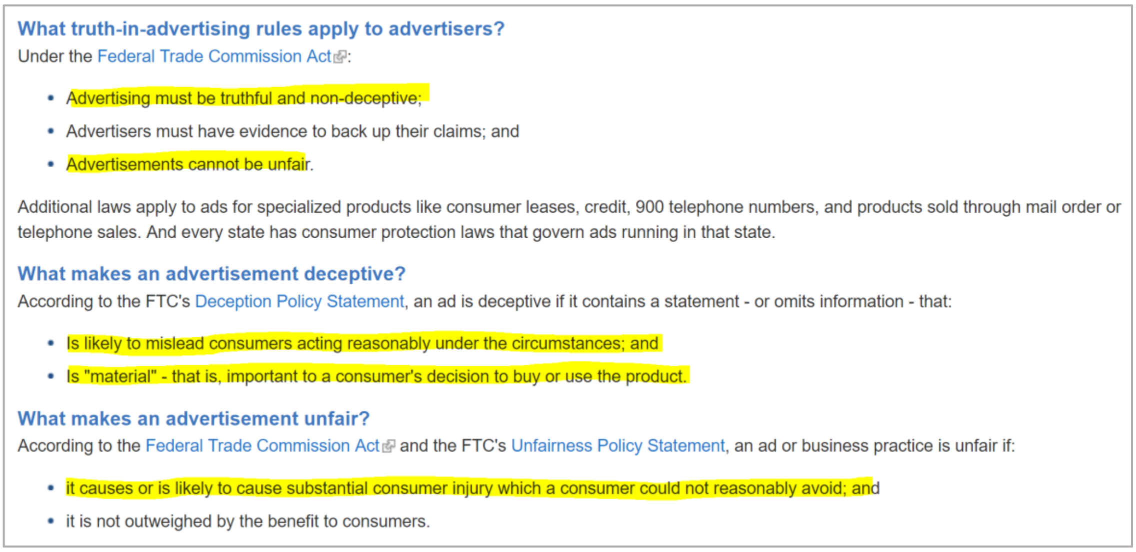
    AMD passed on ASMedia's flawed technology to customers with little in the way of due diligence or effective security review[26,27]

2. **Warranties[28] –** Implied warranties are unspoken and unwritten promises created by state law between a seller or merchant, to their customers. There are two types of implied warranties that occur in consumer product transactions; the implied warranty of merchantability and the implied warranty of fitness for a particular purpose.
    a. The implied warranty of merchantability is a merchant's basic promise that the goods sold will do what they are supposed to do and that there is nothing significantly wrong with them. In other words, it is an implied promise that the goods are fit to be sold.
    b. The implied warranty of fitness for a particular purpose is a promise sellers make when their customers rely on their advice that a product can be used for some specific purpose.

    Based on the ease with which the vulnerabilities in AMD's products are exploitable, we do not believe these products conform with the basic promise of a safe, secure product fit for use.

[22] https://iapp.org/news/a/cybersecurity-in-the-boardroom-the-new-reality-for-directors/
[23] https://www.law.cornell.edu/wex/breach_of_warranty
[24] http://www.courts.state.ny.us/reporter/archives/macpherson_buick.htm
[25] https://www.cozen.com/admin/files/publications/kiernan1954533.pdf?embed
[26] http://www.mondaq.com/unitedstates/x/89684/Product+Liability+Safety/Developments+In+US+Product+Liability+Law+And+The+Issues+Relevant+To+Foreign+Manufacturers
[27] https://www.kreamlaw.com/Frequently-Asked-Questions-Products-Liability.shtml
[28] https://www.ftc.gov/tips-advice/business-center/guidance/businesspersons-guide-federal-warranty-law

4. **False advertising**[29] **–** The FTC has responsibility for enforcing the nation's competition laws including protecting consumers from unfair or deceptive practices.



What truth-in-advertising rules apply to advertisers?
Under the Federal Trade Commission Act:

- Advertising must be truthful and non-deceptive;
- Advertisers must have evidence to back up their claims; and
- Advertisements cannot be unfair.

Additional laws apply to ads for specialized products like consumer leases, credit, 900 telephone numbers, and products sold through mail order or telephone sales. And every state has consumer protection laws that govern ads running in that state.

What makes an advertisement deceptive?
According to the FTC's Deception Policy Statement, an ad is deceptive if it contains a statement - or omits information - that:

- Is likely to mislead consumers acting reasonably under the circumstances; and
- Is "material" - that is, important to a consumer's decision to buy or use the product.

What makes an advertisement unfair?
According to the Federal Trade Commission Act and the FTC's Unfairness Policy Statement, an ad or business practice is unfair if:

- it causes or is likely to cause substantial consumer injury which a consumer could not reasonably avoid; and
- it is not outweighed by the benefit to consumers.

Figure 22 Extract from FTC webpage "Advertising FAQ's: A Guide for Small Business[30]

As outlined in this report, AMD has been misrepresenting itself as a leader in security in the chipset industry with state-of-the-art security. Based on the sheer amount of vulnerabilities and the potential risks it exposes users to we believe it is clear that AMD has falsely been advertising itself as a "more secure" solution.

Risk of recall

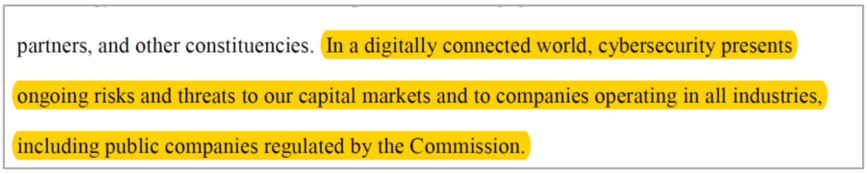
A duty to recall could be imposed by a governmental directive issued pursuant to a state or regulation. One such entity is the Consumer Product Safety Commission, which is generally focused on children's toys but has case-by-case power to force cessation of sale of a product if deemed to "present a substantial product hazard".

Voluntary recalls by semiconductor companies are not without precedent. Intel has recalled the Pentium FDIV (1994) and Cougar Point (2011)[31] at significant cost (US$475M and US$700M respectively). While a deep analysis of these two recalls is beyond the scope of this research report, the security flaws in AMD's products far exceed the defects identified in Intel's processors which necessitated a recall.

We believe that AMD will likely have to recall its Ryzen chips given the scope and severity of the vulnerabilities, the lengthy period to provide patches and work-arounds, and the prospect of more vulnerabilities being discovered.

The SEC

The SEC has taken particular interest in cybersecurity recently including the release of a statement to provide guidance for Public Company Cybersecurity Disclosures. In the introduction, the SEC succinctly summarizes cybersecurity risks and their implications and explicitly highlights that:



partners, and other constituencies. In a digitally connected world, cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies regulated by the Commission.

Figure 23 Extract from SEC Statement and Guidance on Public Company Cybersecurity Disclosures[32]

[29] https://www.ftc.gov/public-statements/1997/04/role-advertising-and-advertising-regulation-free-market#N_13_

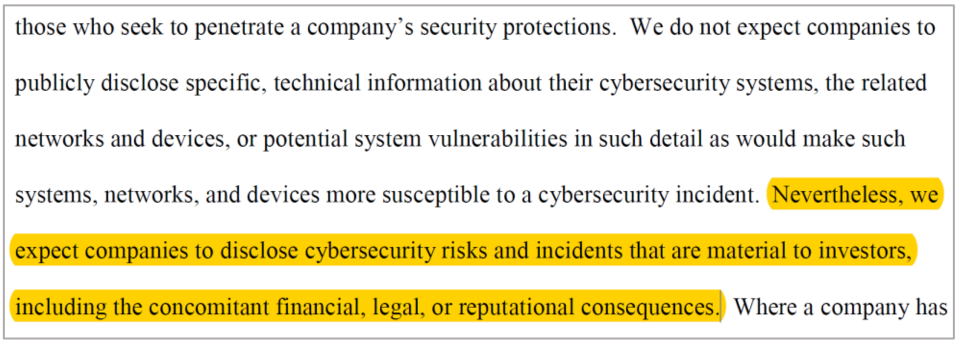
[30] https://www.ftc.gov/tips-advice/business-center/guidance/advertising-faqs-guide-small-business

[31] http://www.tomshardware.com/reviews/cougar-point-recall-sata-6gbps,2896.html

[32] https://www.sec.gov/rules/interp/2018/33-10459.pdf

These SEC guidelines are speculated to come amid scrutiny of a massive stock by sale Intel CEO Brian Krzanich made last fall after his company found out about – but before it publicly disclosed -- the Meltdown and Spectre vulnerabilities[33]. The SEC advised companies to disclose such incidents to investors in a "timely" manner:

"Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.



those who seek to penetrate a company's security protections. We do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident. Nevertheless, we expect companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences. Where a company has

Figure 24 Extract from SEC Statement and Guidance on Public Company Cybersecurity Disclosures

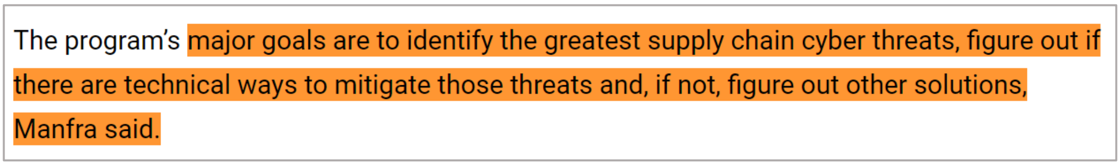
We believe this language is very strong and explicitly highlights AMD's duty to publicize these vulnerabilities as soon as they are made aware of them. We would also note that AMD's management has also been heavily selling stock over the last year, as discussed.

Intel's handling of the disclosure of the exploits is now the subject of some 35 lawsuits, including a number of shareholder derivative lawsuits related to the CEO's stock sales[34]. Some of these law suits charge that the disclosure of the attacks show that statements Intel made about its products or business were false or misleading.

Viceroy believes AMD's disclosures regarding its superior security are far more misleading and will attract similar levels of scrutiny and attack.

Homeland Security Department – the implications for AMD / ASMedia Customers

The Department of Homeland Security's (DHS) Assistant Secretary for Cybersecurity and Communications Jeanette Manfra on February 18, 2018 outlined proposals to integrate vetting of cyber-risks to the Government supply chains[35].

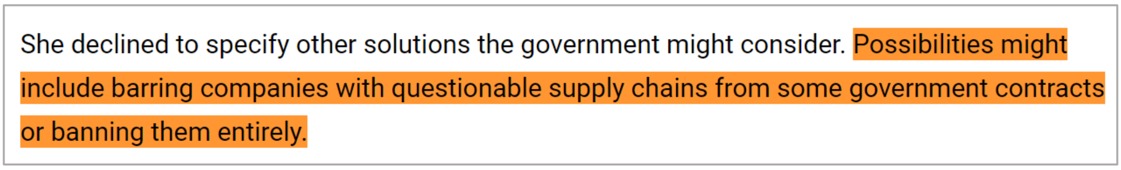


The program's major goals are to identify the greatest supply chain cyber threats, figure out if there are technical ways to mitigate those threats and, if not, figure out other solutions, Manfra said.

Figure 25 Extract of nextgov.com article "DHS to Scrutinize Government Supply Chain for Cyber Risks"

The consequences are likely to be significant for customers of AMD and ASMedia, especially those using the Ryzen and EPYC product lines.

[33] https://www.businessinsider.sg/sec-issue-guidelines-regarding-disclosure-of-security-breaches-2018-2/
[34] http://www.businessinsider.com/35-lawsuits-have-been-filed-against-intel-over-spectre-and-meltdown-2018-2
[35] http://www.nextgov.com/cybersecurity/2018/02/dhs-scrutinize-government-supply-chain-cyber-risks/145998/



She declined to specify other solutions the government might consider. Possibilities might include barring companies with questionable supply chains from some government contracts or banning them entirely.

Figure 26 Extract of nextgov.com article "DHS to Scrutinize Government Supply Chain for Cyber Risks"

Considering the vast number and diversity of AMD's customers and the concerns relating to the backdoors, Viceroy believes AMD products, especially the Ryzen and EPYC product lines will be banned entirely from the government supply chain. The knock-on effect of this restriction to AMD customers will be significant, including HP, Microsoft Azure, Baidu and Dell EMC.

Readers will be familiar with the US government ban on Kaspersky Lab products based on the suspected influence of the Russian government of the company. On December 12, 2017 the use of all Kaspersky Lab products within the US government was banned. This followed a September 13, 2017 directive to remove any Kaspersky Lab software from government systems within 90 days was issued.

Viceroy believes a similar purge of AMD products from government systems will be imminent that adversaries of any government or entity using the AMD Ryzen or EPYC products will be open to attack by hostile entities.

Potential Financial Impacts

Due to the unprecedented nature of the Ryzen and EPYC vulnerabilities in scope as well as the recent nature of the CTS report Viceroy believes analysis of their financial impact with any resolution to be premature at this time. However Intel's legal problems following the far less severe Meltdown/Spectre attacks leads us to believe the costs legal and regulatory issues caused by vulnerabilities to AMD will be catastrophic.

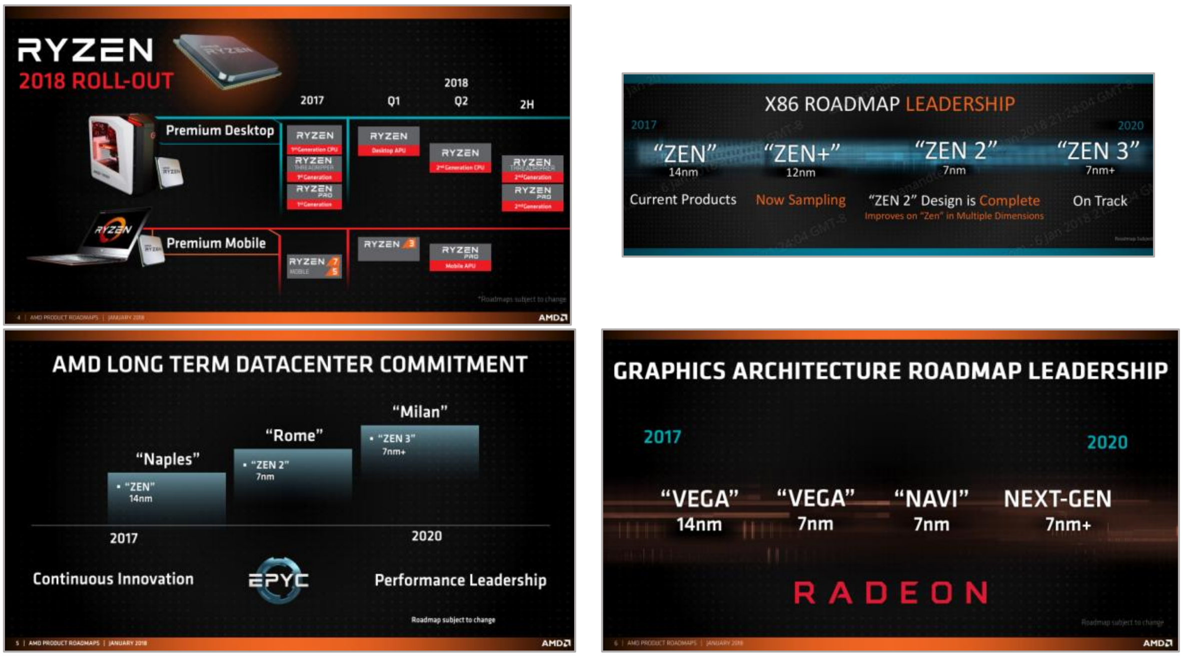
Below is a non-exhaustive list of potential financial impacts arising from the legal and regulatory issues stated above:

- Litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-U.S. authorities;
- Remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack;
- Increased cybersecurity protection costs, which may include the costs of making organizational changes, deploying additional personnel and protection technologies, training employees and engaging third party experts and consultants;
- Claims related to warranties, breach of contract, product recall / replacement, indemnification of counterparties;
- Increased insurance premiums;
- Reputation damage that adversely affects customer or investor confidence;
- Damage to the company's competitiveness, stock price, and long-term shareholder value; and
- Investigation of management's stock sales.

Management appears highly skeptical

AMD's stock has risen dramatically, from US$2 per share in January 2016 to US$11.52 today, due to increased expectations for Ryzen, EPYC and GPUs. Despite this, AMD management's actions appear to be highly cynical of the company's ability to perform.

As seen below, AMD has provided unusually clear product roadmaps for its major products, both on its website[36] and at CES 2018.[37]



RYZEN
2018 ROLL-OUT

2017 | 2018 Q1 | Q2 | 2H

Premium Desktop: RYZEN 1st Generation CPU; RYZEN THREADRIPPER 1st Generation; RYZEN PRO 1st Generation; RYZEN Desktop APU; RYZEN 2nd Generation CPU; RYZEN THREADRIPPER 2nd Generation; RYZEN PRO 2nd Generation

Premium Mobile: RYZEN 7 5 MOBILE; RYZEN 3; RYZEN PRO Mobile APU

*Roadmaps subject to change

4 | AMD PRODUCT ROADMAPS | JANUARY 2018

X86 ROADMAP LEADERSHIP

2017 — 2020

"ZEN" 14nm — Current Products
"ZEN+" 12nm — Now Sampling
"ZEN 2" 7nm — "ZEN 2" Design is Complete — Improves on "Zen" in Multiple Dimensions
"ZEN 3" 7nm+ — On Track

AMD LONG TERM DATACENTER COMMITMENT

"Naples" • "ZEN" 14nm
"Rome" • "ZEN 2" 7nm
"Milan" • "ZEN 3" 7nm+

2017 — 2020

Continuous Innovation — EPYC — Performance Leadership

Roadmap subject to change

5 | AMD PRODUCT ROADMAPS | JANUARY 2018

GRAPHICS ARCHITECTURE ROADMAP LEADERSHIP

2017 — 2020

"VEGA" 14nm
"VEGA" 7nm
"NAVI" 7nm
NEXT-GEN 7nm+

RADEON

Roadmap subject to change

6 | AMD PRODUCT ROADMAPS | JANUARY 2018

Figure 27 Extracts from AMD presentation "Roadmaps 2018 and Beyond"[38]

Strangely with such as supposedly exciting future ahead, AMD's management has been very actively dumping their stock. Since November 2016, AMD's CEO, Lisa Su, has sold over 2.8 million shares of AMD, amounting to US$30m. In total, the management team has sold over 9 million shares of AMD since November 2016.

Note on the graph below that the **completely absent green annotations indicate an insider buy**, compared to the red annotations denoting an insider sale.

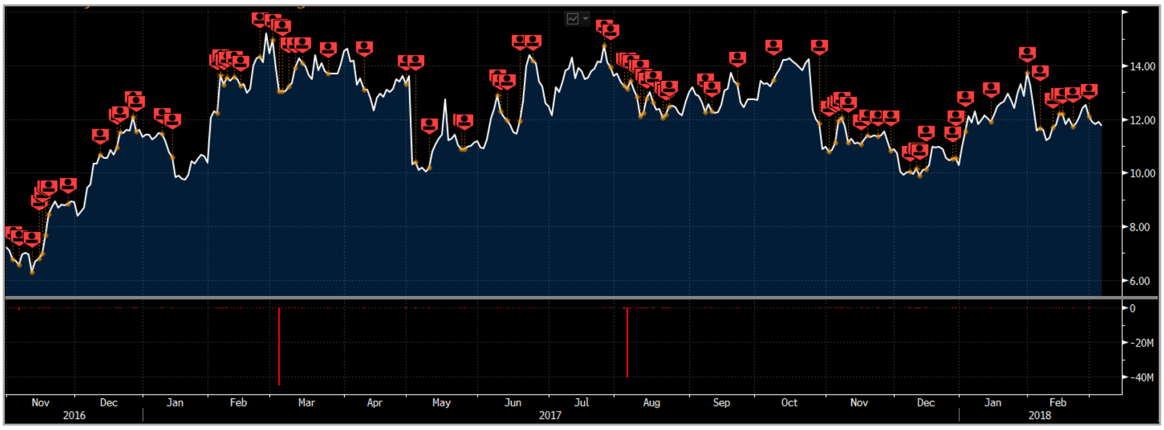


Figure 28 Graph of AMD insider trading activity

None of AMD's executives has acquired a single share in the open market in the 15 months to February 2018.

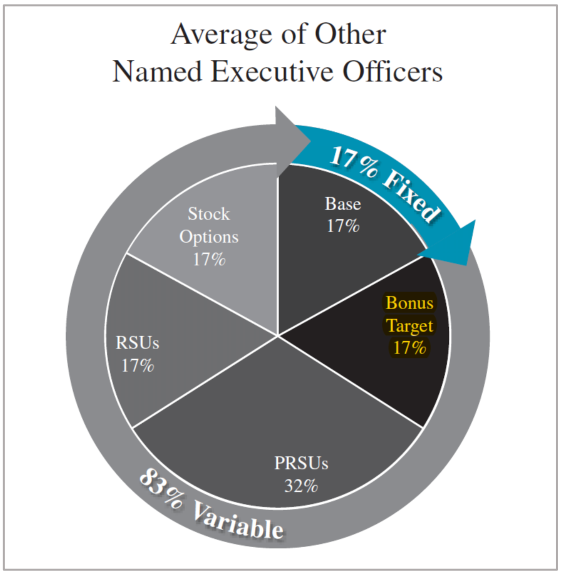
[36] http://ir.amd.com/static-files/a63127c4-569f-4fbe-9fcf-54c24dcfa808

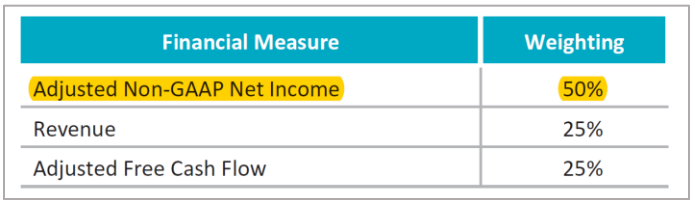
[37] https://www.anandtech.com/show/12233/amd-tech-day-at-ces-2018-roadmap-revealed-with-ryzen-apus-zen-on-12nm-vega-on-7nm

[38] http://ir.amd.com/static-files/a63127c4-569f-4fbe-9fcf-54c24dcfa808

Creative accounting to boost management compensation

As detailed in the FY2017 proxy statement, AMD management compensation is tied to financial performance and stock price. Management bonuses are based on the company's financial performance: with 50% of the target bonus which consists approximately 15% of total compensation, weighted towards adjusted Non-GAAP net income, and another 75% based on stock price appreciation.



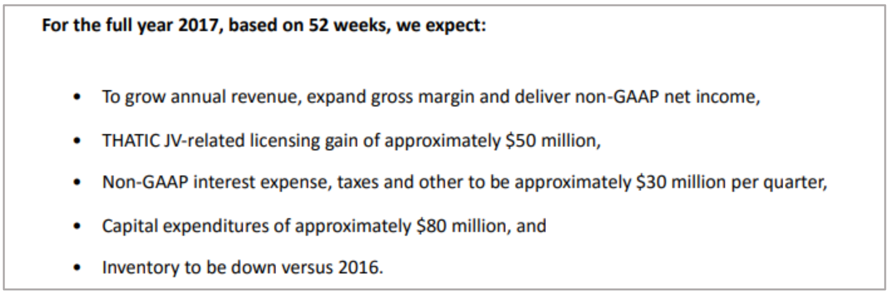


Financial Measure	Weighting
Adjusted Non-GAAP Net Income	50%
Revenue	25%
Adjusted Free Cash Flow	25%

Figures 29 & 30 Extracts from 2017 AMD Proxy Statement[39]

Common sense dictate stock prices move when there are positive earnings stories, and **what better way to flatter earnings and increase compensation than by excluding expenses?**

On January 31, 2017, AMD published its CFO commentary for its FY2016 final quarter results, including outlook and guidance for FY2017. As per the extract below, AMD had guided capital expenditures for the year of US$80 million:



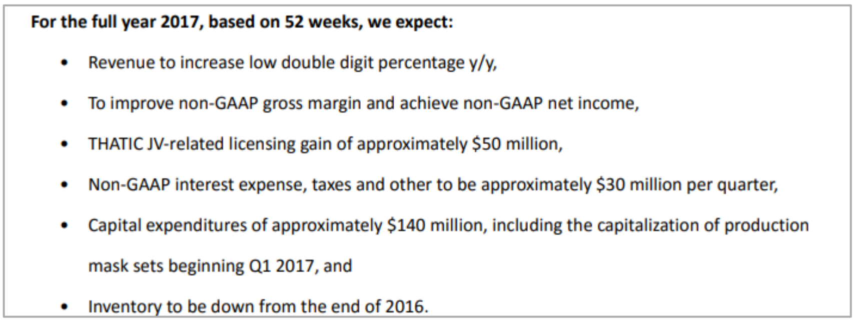
For the full year 2017, based on 52 weeks, we expect:

- To grow annual revenue, expand gross margin and deliver non-GAAP net income,
- THATIC JV-related licensing gain of approximately $50 million,
- Non-GAAP interest expense, taxes and other to be approximately $30 million per quarter,
- Capital expenditures of approximately $80 million, and
- Inventory to be down versus 2016.

Figure 31 Extract from AMD Q4 2016 CFO Commentary[40]

[39] http://ir.amd.com/static-files/83eeb3ba-5aed-4f7b-9a7a-0aa2e6e94bdd
[40] http://ir.amd.com/static-files/f1094ee0-ffd3-4179-ba98-f21c738f9463

Just a few months later, on May 1, 2017, guidance was raised to US$140 million, due to the capitalization of production photomask sets beginning in Q1 2017:

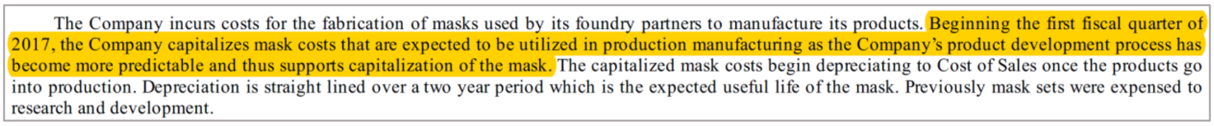


For the full year 2017, based on 52 weeks, we expect:

- Revenue to increase low double digit percentage y/y,
- To improve non-GAAP gross margin and achieve non-GAAP net income,
- THATIC JV-related licensing gain of approximately $50 million,
- Non-GAAP interest expense, taxes and other to be approximately $30 million per quarter,
- Capital expenditures of approximately $140 million, including the capitalization of production mask sets beginning Q1 2017, and
- Inventory to be down from the end of 2016.

Figure 32 Extract from AMD Q4 2016 CFO Commentary[41]

In its quarterly report for Q1 2017, AMD described its reasoning for capitalizing the mask costs:



The Company incurs costs for the fabrication of masks used by its foundry partners to manufacture its products. Beginning the first fiscal quarter of 2017, the Company capitalizes mask costs that are expected to be utilized in production manufacturing as the Company's product development process has become more predictable and thus supports capitalization of the mask. The capitalized mask costs begin depreciating to Cost of Sales once the products go into production. Depreciation is straight lined over a two year period which is the expected useful life of the mask. Previously mask sets were expensed to research and development.

Figure 33 Extract from AMD Q1 2017 10Q[42]

Photomasks are an essential part of the photolithographic manufacturing process.

For all intents and purposes AMD has stripped out US$60 million of expenses from the Income Statement and recategorized it as capital expenditure for FY2017. As AMD emphasized in its Q1 earnings call, there is no impact on free cash flow. The only impact it does have is on earnings.

The capitalization flatters AMD's earnings in two ways:

1. **Deferring expenses –** The items are only capitalized once the masks are put into production, and as such, any costs borne in the associated research and development will not be depreciated until the masks are put into production. In FY2017, AMD admitted that there is no depreciation or amortization charge associated with the capitalized costs. As such, AMD inflated its FY2017 earnings by US$60 million just from this simple change in accounting[43].
2. **Spreading out the expenses** – Based on the Company's statements above, the mask costs will be amortized over 2 years, instead of being expensed in the year incurred. This also helps inflate AMD's earnings.

As a Credit Suisse anaylst comments, the capitalization of the photomasks is an unusual practice[44], and as AMD itself states, it has no cash impact. The only real beneficiaries of inflating the bottom line are management.

Pre-tax income for FY2017 was US$69 million, and so without the US$60 million reduction in expenses from this accounting game, which had no impact on 2017 cash flow, AMD would have made less than US$10 million. Based on this being an unusual practice and AMD's opaque justification that "the Company's product development process has become more predictable and thus supports capitalization," we believe this was done solely so that AMD could report higher net income.

AMD's management has failed at securing its customers by sacrificing security for profit. It has inflated its earnings through accounting changes and has continued selling stock when it can. **Viceroy believes AMD's management decision to capitalize photomask costs was motivated by greed**

[41] http://ir.amd.com/static-files/7cdff8d0-4a47-49c6-890d-9e98bfc653a1

[42] https://www.sec.gov/Archives/edgar/data/2488/000000248817000227/amd0930201710q.htm

[43] AMD Analyst Day, 16 May 2017

[44] Credit Suisse research report, 29 January 2018

Conclusion

Make no mistake the AMD growth story is dead.

- **Dependence on Ryzen and EPYC to meet growth forecasts –** Analyst forecast growth from Ryzen and EPYC product lines to constitute a median 76% of AMD's revenue growth from FY2017 to FY2018, and a median 80% of the growth from FY2018 to FY2019. To fully illustrate the importance of this growth story, **the median CAGR from FY2017 to FY2019 excluding the growth from Ryzen or EPYC is just 2.25%.**

- **Loss of revenue from downtime and recalls –** If, as we believe, AMD is required to conduct a product recall and issue patches to fix the vulnerabilities detailed in the CTS report**. Some of the crippling vulnerabilities may be practically un-patchable.** Experts believe that development and distribution of limited-effectiveness patches will take more than 6 months, time during which Ryzen and EPYC product lines would be **completely vulnerable**. Viceroy does not believe AMD will be able to survive such a blow without extremely dilutive equity raises, or unreasonable levels of debt.

- **Legal and regulatory –** Given the endemic nature of the Masterkey, Ryzenfall, Fallout and Chimera vulnerabilities and the limited ability of patches to remedy them, Viceroy believes an involuntary product recall is imminent. AMD will likely face costly and lengthy legal action such as that currently levelled at Intel over the Meltdown/Spectre fiasco. Coupled with financial implications, we believe AMD would prudently file for Chapter 11 (Bankruptcy) in order to manage this issue.

- **Significant reputational harm –** The release of the CTS report has put an ignominious end to AMD's reputation as a secure hardware provider, especially in light of the negligent nature of the Chimera vulnerabilities. Customers are unlikely to trust AMD again in the short and medium term

If, as we expect, AMD fails to achieve any additional growth in Ryzen or EPYC, then AMD will be loss-making based on the majority of analyst models. Further we believe the financial damage caused makes AMD's long-term survival a rocky proposition.

Neither the bull nor the bear case envisions the scenario that AMD is currently facing. Viceroy believes CTS Labs has opened a Pandora's Box of vulnerabilities with AMD's Ryzen and EPYC product lines: the tone of the report indicates that **more vulnerabilities are likely to be discovered**.

In light of CTS's discoveries, the meteoric rise of AMD's stock price now appears to be totally unjustified and entirely unsustainable. ***We believe AMD is worth $0.00 and will have no choice but to file for Chapter 11 (Bankruptcy) in order to effectively deal with the repercussions of recent discoveries.***

Annexure – Impacts of AMD vulnerabilities

Vulnerabilities	Impact
MASTERKEY-1 ***MASTERKEY-2*** ***MASTERKEY-3***	▪ Persistent malware running inside AMD Secure Processor ▪ Bypass firmware-based security features such as *Secure Encrypted Virtualization* (SEV) and *Firmware Trusted Platform Module* (fTPM) ▪ Network credential theft. Bypass *Microsoft Virtualization-based Security* (VBS), including *Windows Credential Guard* ▪ Physical damage to hardware (SPI flash wear-out, etc.) ▪ Affects: *EPYC, Ryzen, Ryzen Pro, Ryzen Mobile*. Successfully exploited on *EPYC* and *Ryzen*
RYZENFALL-1 ***FALLOUT-1***	▪ Write to protected memory areas, including: o Windows Isolated User Mode and Isolated Kernel Mode (VTL1) o AMD Secure Processor Fenced DRAM – Allows direct tampering with trusted code running on AMD Secure Processor. Only applicable to select *Ryzen* motherboards ▪ Network credential theft. Bypass *Microsoft Virtualization-based Security (VBS)* including *Windows Credential Guard* ▪ Enables memory-resident *VTL1* malware that is resilient against most endpoint security solutions ▪ Affects: *EPYC, Ryzen, Ryzen Pro, Ryzen Mobile*. Successfully exploited on *EPYC, Ryzen*, *Ryzen Pro* and *Ryzen Mobile*
RYZENFALL-2 ***FALLOUT-2***	▪ Disable *Secure Management RAM (SMRAM)* read/write protection ▪ Enables memory-resident SMM malware, resilient against most endpoint security solutions ▪ Affects: *EPYC, Ryzen, Ryzen Pro*. Successfully exploited on *EPYC, Ryzen, Ryzen Pro*. *Ryzen Mobile* is not affected
RYZENFALL-3 ***FALLOUT-3***	▪ Read from protected memory areas, including: o Windows Isolated User Mode and Isolated Kernel Mode (VTL1) o Secure Management RAM (SMRAM) o AMD Secure Processor Fenced DRAM. Only applicable to select *Ryzen* motherboards ▪ Network credential theft. Bypass *Windows Credential Guard* by reading secrets from VTL1 memory ▪ Affects: *EPYC, Ryzen, Ryzen Pro*. Successfully exploited on *EPYC, Ryzen, Ryzen Pro*. *Ryzen Mobile* is not affected
RYZENFALL-4	▪ Arbitrary code execution on AMD Secure Processor ▪ Bypass firmware-based security features such as *Firmware Trusted Platform Module* (fTPM) ▪ Network credential theft. Bypass *Microsoft Virtualization-based Security* (VBS), including *Windows Credential Guard* ▪ Physical damage to hardware (SPI flash wear-out, etc.) ▪ Affects: *Ryzen, Ryzen Pro*. Successfully exploited on *Ryzen, Ryzen Pro*.
CHIMERA-FW ***CHIMERA-HW***	▪ Two sets of manufacturer backdoors: One implemented in firmware, the other in hardware (ASIC) ▪ Allows malware to inject itself into the chipset's internal *8051 architecture* processor ▪ The chipset links the CPU to USB, SATA, and PCI-E devices. Network, WiFi and Bluetooth traffic often flows through the chipset as well ▪ Malware running inside the chipset could take advantage of the chipset's unique position as a middleman for hardware peripherals ▪ Affects: *Ryzen, Ryzen Pro*. Successfully exploited on *Ryzen* and *Ryzen Pro*.