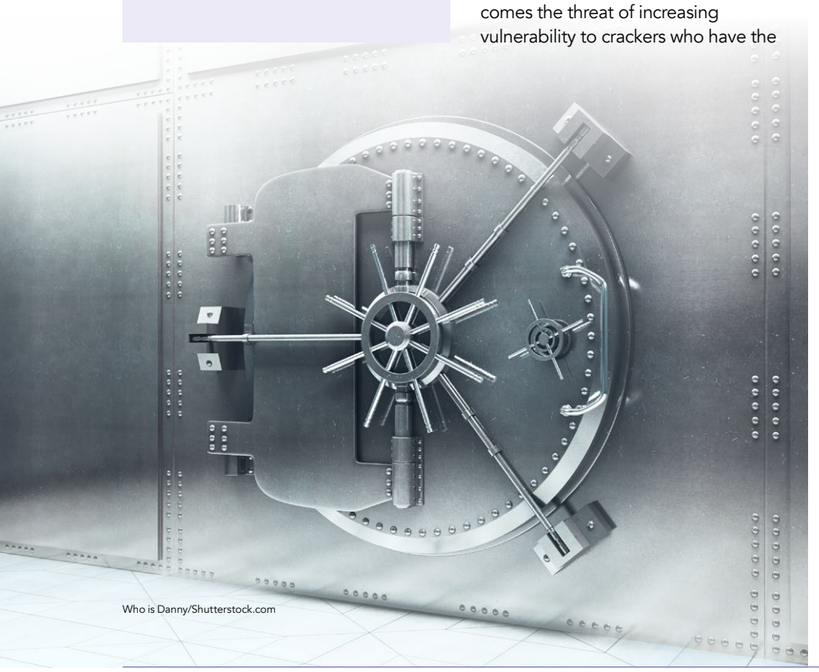
Bunker jails

Providing application level firewall protection for Bank IT infrastructure security

The increase in cyber-attacks on leading financial institutions highlights the need for secure Bank IT infrastructures. Dr Alin-Adrian Anton and Dr Razvan-Dorel Cioarga, Lecturers at the Department of Computer and Information Technology, Politehnica University of Timisoara in Romania, have developed Bunker jails that provide application level firewall protection for Bank IT infrastructure security. Bunkers operate as prison level firewalls, enabling the security jails and networked services to eliminate threats and surprises.

Information technology (IT) infrastructures underpin the financial industry. For many decades, these infrastructures were confined to the institution's back office, fulfilling key tasks such as storaging data on mainframe computers. Today, a bank's IT infrastructure is made up of a wide assortment of hardware and software. This includes their employees' laptops and desktops, networks linking offices and data centres around the world, and Internet of Things (IoT) devices. The development of the internet and the subsequent mobile revolution mean that banks' IT infrastructures are now enablers of business as well as being part of their consumers' daily life.

Together with these advancements comes the threat of increasing vulnerability to crackers who have the capability to dismantle a bank's critical infrastructure. The need for secure IT infrastructures has never been more prominent. Dr Alin-Adrian Anton and Dr Razvan-Dorel Cioarga, Lecturers at the Department of Computer and Information Technology, Politehnica University of Timisoara in Romania, have developed Bunker jails that provide application level firewall protection for Bank IT infrastructure security.



Who is Danny/Shutterstock.com

BUNKER JAILS

The researchers explain that these innovative Bunkers are network isolated HardenedBSD jails that will only permit the execution of bit-exact validated software. HardenedBSD is a security enhanced branch of FreeBSD, a free, open-source operating system, similar to Unix. System administrators can partition a FreeBSD system into a number of independent security systems known as jails. These jails are effectively security prisons; each running as a lightweight (in terms of system overheads) operating system where a critical service, such as a database, server or antivirus engine, can be located.

Jails offer three main advantages in terms of their virtualisation, security and ease of delegation. Each individual jail provides a virtual environment with its own files and processes that runs on the host machine with a copy of the same kernel, so it can have its own user and superuser accounts. A jail is isolated from other jails in order to provide an additional level of security, but overlapped jails are possible. Each jail performs only a few specific tasks so system administrators can delegate tasks and permit superuser access to a particular jail rather than the complete system. A non-privileged user level can also be enforced jail-wide.

whiteMoccai/Shutterstock.com

This research realises a novel paradigm in cybersecurity - networked services are statically compiled and secured in sealed environments that are isolated and protected within virtual Bunkers.

A NOVEL PARADIGM IN CYBERSECURITY

Dr Anton's and Dr Cioarga's research realises a novel paradigm in cybersecurity where networked services are statically compiled and secured in sealed environments that are isolated and protected within virtual Bunkers. A specific bit-exact validated list of binaries and services can operate from within each Bunker that contains only the binary files required to operate the particular service it houses.

If malicious exploits succeed in penetrating a Bunker, whether due to software vulnerabilities, user authentication or configuration errors, the foreign shellcode will be unable to load and execute a new process or run any command outside of the permitted service already running on the target system. The researchers disable the internet stack within Bunkers, so that the critical services residing in the Bunkers have to communicate with the external world via local files instead of using internet sockets. This is particularly appropriate for database systems and antivirus engines.

ANTIVIRUS BUNKER OBJECTIVES

The researchers' primary objective is to ensure that remote exploits and payloads are rendered unresponsive within the Bunker. This is achieved by isolating the remote attacker and ensuring that it does not connect with the vulnerable system.

Their secondary objective is to provide intrusion detection for the HardenedBSD jail system using the global system log to record any attempt to execute the socket() function with AF_INET networking capability. The socket() function allows the exchange of information between either processes on the same machine or across a network. AF_INET is used to designate the internet type for the addresses that your socket can communicate with.

The primary objective is to ensure that remote exploits and payloads are rendered unresponsive within the Bunker.

The research team presents two use-cases that demonstrate how their Bunker jail application fulfils these objectives.

BANK E-MAIL ANTIVIRUS BUNKER

A real e-mail service was used to compare the performance of Bunker jails with that of regular jails. The email service, a store and forward system, stored and scanned file attachments before inserting them into an employee's inbox. Two test cases were deployed: the first comprising 10 threads with 500 emails per thread; and the second made up of 20 threads with 100 emails per thread. Both test cases were performed with and without the Bunker mode over a 2-hour period. The researchers analysed the test results from their Bunker mechanism with those from regular jails and a rival approach Integriforce. The Bunker jails produced similar


Bunkers can be deployed in any UNIX service that forms part of any Bank's critical infrastructure.

performance results, in terms of e-mail data rate capacity, to the other systems.

BANK WEB PROXY ANTIVIRUS BUNKER

Bank's employees' web traffic is usually routed through an outbound security proxy with antivirus capabilities by Bank IT security experts. The researchers used ClamAV a trusted open source antivirus engine frequently used on mail servers as an email virus scanner. This protects web users by scanning files from malicious web content traffic without interruption. Two test cases were implemented with and without the antivirus engine using Bunker jails, regular jails and Integriforce. Once again, Bunker jails displayed similar performance under real web browser heavy load conditions.

BIT-EXACT VALIDATION

The research team has established that the bit-exact validation of service binaries used by Bunker jails is comparable with the classic cryptographic checksum approaches in terms of performance impact. They have also demonstrated that it remains 100% secure against future collision attacks and vulnerabilities in modern cryptographic algorithms, including attack by a quantum computer.

BENCHMARKING

Extensive benchmarks with databases containing millions of entries revealed an impact of 10-20% percent in terms of CPU response time. In return for this negligible impact on the system, Bunkers provide a solid cyber security paradigm when running critical services. The researchers describe how, depending on the software packages being used, a dedicated CPU will already be operating at 10-20% capacity prior to the service starting. In terms of modern CPU hardware, this is more than adequate for critical systems.

It's like trapping the attacker inside a freezing vault and alerting the host operating system.

EXPLOIT MITIGATION TECHNIQUES

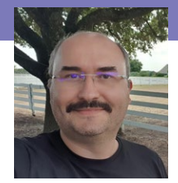
Bunkers can be deployed in any UNIX service that forms part of any Bank's critical infrastructure with the proviso that the service's binary executable file is statically compiled and that the service can communicate via local UNIX sockets. The research team chose to use HardenedBSD as the operating system to develop Bunker services, including the Bank e-mail antivirus Bunker and the bank web proxy antivirus Bunker described above, because it provides enhanced exploit mitigation techniques for unknown vulnerabilities and zeroday exploits, i.e. cyber-attacks occurring on the same day as the software weakness is discovered so that it can be exploited before a fix is available, that can affect critical financial services.

The Bunker services enable the security jails and the networked services to eliminate threats and surprises. If any of the other security mechanisms are defeated, the Bunkers operate as prison level firewalls, effectively freezing the virtual instances into a state whereby they cannot communicate with the attacker. The researchers explain "it's like trapping the attacker inside a freezing vault and alerting the host operating system where all system logs and whitelists are located, far away outside the Bunker, on the surface, outside the reach of the paralysed attacker." Any attempt to run foreign code inside the Bunker or communicate with the internet will be logged on the host system and the system administer is alerted.

Dr Anton and Dr Cioarga have made their source code available to readers upon request.

Behind the Research

Dr Alin-Adrian Anton



Dr Razvan-Dorel Cioarga

E: alin.anton@upt.ro **T:** +40256403261 **W:** www.cs.upt.ro, www.upt.ro, www.anton.doctor, www.cioarga.net, www.cioarga.ro

Detail

2nd Victory Square
300006 Timisoara
Timis, Romania

Bio

Dr Alin-Adrian Anton and Dr Razvan-Dorel Cioarga are Lecturers at the Department of Computer and Information Technology, Politehnica University of Timisoara. Dr Anton's research focus is on cybersecurity, privacy and computational fluid dynamics. Dr Cioarga's research interests include embedded systems, intelligent robotic environments, intelligent infrastructures and environments, web-based systems.

Collaborators

Authors acknowledge Dr Luca Verderame, Department of Informatics, Bioengineering, Robotics, and Systems Engineering, University of Genoa, for constructive recommendations.

References

Anton A., Cioargă R. (2020) Bunkers: Jail Application Level Firewall for the Mitigation and Identification of Service Takeover Attacks on HardenedBSD. In: Fournaris A. *et al.* (eds) *Computer Security. IOSEC 2019, MSTEC 2019, FINSEC 2019, in conjunction with the 24th European Symposium on Research in Computer Security (ESORICS 2019). Lecture Notes in Computer Science*, [online] 11981, 242-257. Springer, Cham. Available at: https://doi.org/10.1007/978-3-030-42051-2_17 [Accessed 9th September 2020]

Personal Response

What inspired you to develop Bunker jails?

"People talk about unwanted remote management microchips stealthily running entire operating systems inside consumer devices, however, when running services for critical financial infrastructures they just plug in the next best thing. Banks spend millions of dollars on firewalls, AI-based intrusion detection systems and cryptography. This approach doesn't solve the security problems. Bunker jails really should be the only way internet services should face the world. They are mandatory bit-exact border controls, freezing the security device in a state where only the expected job can be run. Given that all the native exploit mitigation techniques fail, Bunkers will seal the problem."


vs148/Shutterstock.com