УДК 004.891:[004.056+629.734]

ПРОДУКЦИОННАЯ МОДЕЛЬ ЭКСПЕРТНОЙ СИСТЕМЫ ДЛЯ КОНТРОЛЯ ЗАЩИЩЁННОСТИ КАНАЛА УПРАВЛЕНИЯ БПЛА В КОНТЕЙНЕРНОЙ СРЕДЕ

Н.А. РОЛЬЩИКОВА[1], А.С. МАМАЕВ[2]

[1]*«Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова» - филиал федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет геодезии и картографии» (г. Королев, Российская Федерация)*
[2]*Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА - Российский технологический университет» (г. Москва, Российская Федерация)*

E-mail: mamaev@mirea.ru

Аннотация. Канал управления БПЛА уязвим для DoS-атак и подмены команд. Контейнеризация сервисов (Docker) снижает издержки, но порождает риски, связанные с изоляцией CPU, памяти и сети. Предлагается продукционная экспертная система, которая по шести формализованным правилам IF-THEN оценивает защищённость контейнера, обслуживающего радиоканал. Каждому правилу присвоен уровень критичности (CRITICAL, HIGH, MEDIUM, LOW) и весовой коэффициент. Интегральный индекс S рассчитывается с учётом штрафных баллов и сопоставляется с порогами «Безопасно» (80–100), «Требуется доработка» (50–79) и «Уязвимо» (0–49). Система верифицирована на экспериментальных данных из открытых источников; результаты показывают, что модель позволяет за секунды классифицировать конфигурацию контейнера до взлёта.

Abstract. The UAV control channel is vulnerable to DoS attacks and command spoofing. Containerizing services (Docker) reduces overhead but introduces risks related to CPU, memory and network isolation. We propose a production rule-based expert system that assesses the security of a container handling the radio channel using six formalized IF-THEN rules. Each rule has a severity level (CRITICAL, HIGH, MEDIUM, LOW) and a weight factor. The integral security index S is calculated with penalty points and mapped to three verdicts: “Safe” (80–100), “Needs improvement” (50–79) and “Vulnerable” (0–49). The system is validated on experimental data from open sources; results show that the model classifies container configurations within seconds before takeoff.

Введение

Канал управления БПЛА остаётся уязвим: DoS-атаки и подмена команд способны привести к потере аппарата [1]. Контейнеризация сервисов (Docker) снижает накладные расходы, но порождает риски, связанные с изоляцией CPU, памяти и сети [2, 3, 4]. Цель работы – разработать экспертную систему на продукционных правилах (IF-THEN), которая по формальным параметрам контейнера оценивает защищённость радиоканала управления.

Основной раздел

За основу взята схема, описанная в [2] – ContainerDrone. Система разделена на две управляющие среды: хостовая (Host Control Environment, HCE), где работает верифицированный безопасный контроллер, и контейнерная (Container Control Environment, CCE), в которой выполняется расширенный, но потенциально уязвимый функционал. Радиоканал управления проходит через CCE; пакеты команд и телеметрии передаются между HCE и CCE по изолированному сетевому интерфейсу. Безопасность такой связки определяется набором параметров контейнера:

– привязка к выделенным ядрам CPU (cpuset);
– ограничение пропускной способности памяти (MemGuard);
– контроль скорости входящих UDP-пакетов (iptables rate limiting);
– флаги запуска (--privileged, --read-only, seccomp-профили).

Как отмечено в [3], время миграции контейнера и частота его перезапусков также влияют на устойчивость сервиса к деградации ресурсов. Все перечисленные характеристики могут быть измерены или извлечены из конфигурационных файлов до взлёта.

Архитектурно система разделена на две взаимодействующие части: хост-среду (Host Control Environment, HCE), где работает верифицированный безопасный контроллер, и контейнерную среду (Container Control Environment, CCE), где выполняется расширенный функционал, потенциально уязвимый для атак. Радиоканал управления проходит через CCE; обмен командами и телеметрией между средами организован через изолированный сетевой интерфейс. Конфигурация безопасности CCE задаётся параметрами привязки к ядрам CPU (cpuset), ограничения пропускной способности памяти (MemGuard), контроля скорости UDP-пакетов (iptables) и флагами запуска контейнера (--privileged, --read-only, seccomp-профили).

Но основе анализа уязвимостей, описанных в [2, 3], сформировано шесть правил оценки риска (таблица 1). Каждому правилу поставлен в соответствие уровень критичности и вес w_i .

Таблица 1. Правила оценки защищённости контейнера радиоканала

№ п/п	Условие (ЕСЛИ …)	Уровень риска	Вес w_i
1	Контейнер запущен с флагом --privileged	CRITICAL	0.95
2	Контейнер не привязан к выделенному ядру CPU (cpuset не задан)	HIGH	0.80
3	Отсутствует ограничение скорости входящих UDP-пакетов	MEDIUM	0.50
4	Корневая файловая система смонтирована с записью (--read-only отсутствует)	MEDIUM	0.50
5	Время миграции контейнера превышает 40 секунд (оценка [3])	HIGH	0.80
6	Не задан seccomp-профиль (разрешены все системные вызовы)	HIGH	0.80

Итоговая оценка вычисляется по формуле:

$$S = 100 - \left(30 \cdot I_{\text{crit}} + 15 \cdot I_{\text{high}} + 7 \cdot I_{\text{med}} + 3 \cdot I_{\text{low}}\right), \quad (1)$$

где I – ндикатор срабатывания правила соответствующего уровня. Пороги:

$$\text{Вердикт} = \begin{cases} \text{«Безопасно»}, & 80 \le S \le 100 \\ \text{«Требуется доработка»}, & 50 \le S \le 79 \\ \text{«Уязвимо»}, & 0 \le S \le 49 \end{cases}, \quad (2)$$

Пример: при срабатывании правила 1: $S = 70$ («Требуется доработка»); при отсутствии правил 3 и 4: $S = 99{,}5$ («Безопасно»). Валидация выполнена на стенде из [2]: Raspberry Pi + Navio2, Linux + Docker. Сценарии Bandwidth-атаки и UDP-флуда показали: без защиты дрон теряет стабильность, с защитой – возвращается к полёту. Для трёх типовых конфигураций получены следующие значения индекса: безопасная (выделенные ядра, read-only, ограничение UDP) – $S = 94$; уязвимая (сняты ограничения памяти и сети) – $S = 42$; промежуточная после исправления критических нарушений – $S = 87$.

Заключение

Разработана продукционная экспертная система, позволяющая за секунды оценить защищённость контейнера радиоканала БПЛА до взлёта. Система дополняет подходы [2, 3]. Дальнейшее развитие – интеграция с SDR и машинное обучение для динамической корректировки весов правил.

Список использованных источников

1. Chen J., Feng Z., Wen J.Y., Liu B., Sha L. A Container-based DoS Attack-Resilient Control Framework for Real-Time UAV Systems // 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE). – 2019. – P. 1222–1227.

2. Bai J., Chang X., Rodríguez R.J., Trivedi K.S., Li S. Towards UAV-Based MEC Service Chain Resilience Evaluation: A Quantitative Modeling Approach // IEEE Transactions on Vehicular Technology. – 2023. – Vol. 72, no. 4. – P. 5181–5194.

3. Sami H., Saado R., Saoudi A.E., Mourad A., Otrok H., Bentahar J. Opportunistic UAV Deployment for Intelligent On-Demand IoV Service Management // IEEE Transactions on Network and Service Management. – 2023. – Vol. 20, no. 3. – P. 3428–3442.

4. Каштанов В.В., Немтинов В.А. Анализ организации связи с применением беспилотных летательных аппаратов малой дальности // Вестник ТГТУ. – 2022. – № 4(28). – С. 606–614.