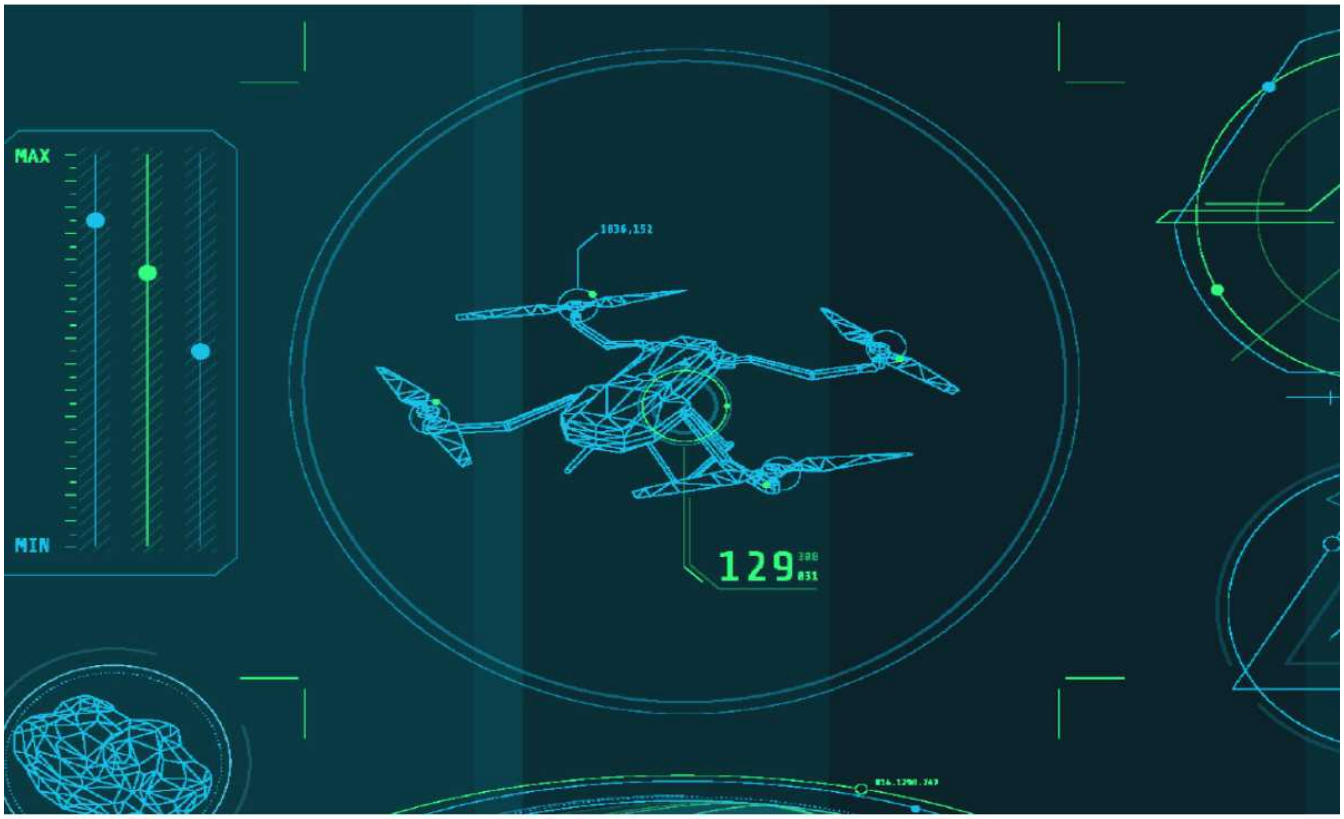
06/04/2022

ictsecuritymagazine.com

Argomento: Exprivia: si parla di noi

EAV: € 972
Utenti unici: 9.867

https://www.ictsecuritymagazine.com/articoli/la-cybersecurity-per-i-droni-tipologie-di-attacchi/



La CyberSecurity per i droni – Tipologie di attacchi

A cura di: Domenico Raguseo, Rosita Galiandro, Giuseppe Marullo e Antonio De Chirico 6 Aprile 2022

Introduzione

Con il progresso della tecnologia, i campi di applicazione dei droni non sono più limitati ai laboratori o alla difesa; pertanto, possono essere utilizzati anche da hobbisti. Si moltiplicano le applicazioni dei droni in svariati ambiti della nostra vita economica e sociale e parallelamente crescono le possibilità che questi siano oggetti di attacchi cyber.

La CyberSecurity per i droni – Tipologie di attacchi

A cura di:
Domenico Raguseo, Rosita Galiandro, Giuseppe Marullo e Antonio De Chirico
6 Aprile 2022

Introduzione

Con il progresso della tecnologia, i campi di applicazione dei droni non sono più limitati ai laboratori o alla difesa; pertanto, possono essere utilizzati anche da hobbisti. Si moltiplicano le applicazioni dei droni in svariati ambiti della nostra vita economica e sociale e parallelamente crescono le possibilità che questi siano oggetti di attacchi cyber.

CyberSecurity e droni

Durante la cerimonia di apertura delle Olimpiadi di Tokyo, 1824 droni hanno disegnato coreografie nel cielo che erano tanto sorprendenti quanto impressionanti se si pensa al livello di raffinatezza e tecnologia che uno spettacolo del genere abbia potuto supportare.

Non si tratta solo di creare coreografie spettacolari, ma anche di utilizzare veicoli aerei gestiti remotamente in ambito militare, utili per portare connettività in posti difficilmente raggiungibili, registrare riprese per realizzare servizi fotografici e a supporto di attività turistiche, di arte e cultura, eventi. Anche l'industria fa abbondante utilizzo di droni. Si va da attività di monitoraggio in ambienti pericolosi a monitoraggio continuo di aree di grande estensione. Il monitoraggio è un servizio di cui anche il territorio, le città intelligenti ne beneficiano. Ovviamente gli utilizzi sono molteplici e lo saranno sempre di più in funzione di una tecnologia che sta facendo enormi progressi e costi che progressivamente si abbassano rendendo accessibile questi dispositivi sempre ad un maggior numero di persone.

Il successo dei droni è legato all'accelerazione digitale. Molti servizi costruiti sui droni possono essere realizzati grazie al fatto che possono raccogliere informazioni e trasmetterle, possono essere connessi a Internet e questo introduce un tema da non sottovalutare per IoT, e ancor meno per IoD (Internet of Drones): la possibilità che i dispositivi possano subire un attacco di tipo cyber. Sui droni, infatti, è presente un software che permette di essere controllati, di svolgere attività, di ricevere comandi da una console che a sua volta è collegata a un sistema complesso, che spesso coinvolge il cloud.

Quindi, anche se si parla di IoD, si tratta di un insieme di elementi IT (non classici) collegati per poter adempiere ad un servizio specifico.

STRIDE Framework

Il primo passo per proteggersi dagli attacchi alla sicurezza informatica è comprendere il possibile spazio delle minacce. Coloro che vogliono proteggersi dagli attacchi di cybersecurity per stare al passo con potenziali avversari devono essere creativi, proattivi e consapevoli delle capacità degli avversari. L'enumerazione dei possibili tipi di attacchi

futuri richiede un'attenta revisione dello spazio delle minacce consentito dalle tecnologie esistenti ed emergenti. Potrebbe essere utile che tale revisione sia radicata in un quadro consolidato di possibili tipi di minacce e potrebbe anche essere utile compilare questo quadro utilizzando metodi di brainstorming formalizzati per aiutare a scoprire possibili minacce. Uno di questi framework è la tassonomia STRIDE di Adam Shostack per la modellazione delle minacce, che delinea sei aree in cui possono essere classificate le minacce alla sicurezza. Sebbene la tassonomia STRIDE sia stata originariamente sviluppata per l'uso nello sviluppo di software, le sei aree che copre sono utili anche per enumerare le minacce relative alla cybersecurity e agli UAS.
All'interno del framework STRIDE, la S rappresenta lo Spoofing" e definisce l'insieme di minacce che violano i protocolli di autenticazione, consentendo a un utente malintenzionato di fingere di essere qualcuno che non è. Nel caso della cybersecurity legata agli UAS, in cui i droni sono un obiettivo, lo spoofing potrebbe includere il fingere di essere la macchina ricevente autorizzata per i dati dei droni.

La T nel framework STRIDE rappresenta "Tampering", che implica la violazione dell'integrità di un sistema sotto attacco apportando modifiche ad esso. Nel caso della sicurezza informatica relativa agli UAS, in cui i droni vengono utilizzati come arma cibernetica, potrebbero verificarsi manomissioni se un drone viene utilizzato per fornire malware a un computer bersaglio utilizzando la vicinanza per accedere a una rete wireless non protetta. Tale malware potrebbe potenzialmente infettare macchinari di alto valore, come apparecchiature in fabbriche o centrali elettriche, o attaccare obiettivi ad alto impatto come sistemi idrici e reti elettriche.

R rappresenta "Repudiation", in cui gli aggressori ripudiano dall'assumersi la responsabilità di un'azione. Questa minaccia è la meno rilevante per il dominio della sicurezza informatica relativo agli UAS. Un possibile esempio è quando un operatore di droni potrebbe affermare di non aver intenzionalmente bloccato un dispositivo accusando la perdita di controllo di un difetto di progettazione nella rete di comunicazione.

Nel caso della cybersecurity relativa agli UAS, la manomissione potrebbe verificarsi se un drone viene utilizzato per fornire malware a un computer bersaglio utilizzando la vicinanza per accedere a una rete wireless non protetta. Tale malware potrebbe potenzialmente infettare macchinari di alto valore, come apparecchiature di fabbriche o centrali elettriche, o attaccare obiettivi ad alto impatto come i sistemi idrici e le reti elettriche.

I si riferisce alla "Information disclosure", ovvero alle violazioni del principio di riservatezza. Negli attacchi di propagazione delle informazioni, un agente rilascia informazioni a qualcuno senza le credenziali appropriate per riceverle. Le minacce alla divulgazione di informazioni potrebbero includere l'infiltrazione in un sistema di dati del sensore UAS per accedere a video, audio o altri dati. Un agente può anche divulgare informazioni e in seguito utilizzare il ripudio per declinare la responsabilità per questa azione

La D sta per "Denial of Service" e si riferisce

all'opposizione della disponibilità di una risorsa necessaria per il corretto funzionamento del sistema attaccato. Un esempio di negazione del servizio è quando gli UAS sono presi di mira e potrebbero causare l'infezione del software di controllo dei droni per rendere i dispositivi non rispondenti agli input dell'utente.

Infine, la E nel quadro STRIDE sta per "Elevation of privilege" e comporta la violazione del principio di autorizzazione a compiere un'azione che non è consentita a compiere. Un esempio di autorizzazione privilegiata è quando gli UAS sono obiettivi e potrebbero comportare il dirottamento di un drone che si spaccia per controllore legittimo. Quando gli UAS vengono utilizzati come arma cibernetica, potrebbero essere utilizzati per fornire dati, codice o altri segnali per debilitare o alterare il comportamento del sistema sotto attacco.

CyberSecurity Kill Chain

All'interno di un dato scenario di attacco, c'è una grande diversità nel modo in cui un drone può essere considerato vulnerabile. Supportando il framework STRIDE, la kill chain della cybersecurity consente a un utente di identificare quando e come un particolare sistema è vulnerabile all'interno di uno scenario. Ciò potrebbe consentire la progettazione di una difesa informata contro una minaccia specifica. Ad esempio, un tale approccio potrebbe identificare un anello debole in una lunga catena di comunicazioni, come l'impossibilità di proteggere un segnale wireless a casa di un dipendente, piuttosto che concentrare gli sforzi sull'ulteriore rafforzamento della crittografia presso il data warehouse centrale.

La kill chain cybersecurity identifica sette fasi (reconnaissance, weaponization, delivery, exploitation, installation, command and control, e actions) di un cyber attacco. La catena rappresenta una sequenza ordinata in cui ogni fase identifica un'azione intrapresa da un attaccante. Ogni fase presenta anche un'opportunità per il rilevamento degli attacchi. Poiché le fasi sono sequenziali, la diagnosi precoce è associata a conseguenze meno dirompenti e soluzioni meno costose.

Mentre l'azione difensiva dipende da dove si trova un'azione all'interno della catena e specificare dove si trova il drone sulla catena di uccisione della sicurezza informatica facilita l'adozione di misure di sicurezza efficaci.

Cyber attacchi su un UAV

Allargando il contesto allo scenario reale in cui i droni sono inseriti in un ecosistema che include app, mobile, web server, internet, allora le modalità di attacco possono moltiplicarsi in quanto tipiche ed estremamente utilizzate in altri ambiti. Se compromettere infatti un drone richiede competenze specifiche, attaccare un application server è nel DNA degli attaccanti.

Esistono diversi modi per condurre un attacco informatico su un UAV:

Password theft: utilizzando mezzi diversi, tra cui dizionario, forza bruta e assalti matematici. Gli attacchi al dizionario in diverse varianti utilizzano frasi, numeri e simboli specifici per violare la password. Gli attacchi che utilizzano la forza bruta possono essere rilevati in password brevi tentando tutte le possibili configurazioni. Ad esempio, il software Aircrack-ng, i metodi statistici utilizzano dati statistici per decidere se una

parola viene indovinata correttamente da un byte. Si otterranno i dettagli necessari da "leaks" nei vettori di configurazione dell'entità di destinazione e si cercheranno le chiavi fondamentali per utilizzare interamente la forza bruta;
Man in The Middle (MITM): è un processo mediante il quale un utente malintenzionato monitora il contatto tra due parti e ha accesso a dati sensibili (che possono modificare) senza il consenso degli utenti nell'attacco. Si verificano molti tipi di attacchi MITM, come Eavesdropping e la manipolazione degli URL;
Denial of Service (DoS): consente all'intruso di comandare e mantenere l'accesso a un dispositivo o a una rete. L'intrusione richiede risorse applicative inondando il sistema di richieste o pacchetti, come potenza di calcolo o memoria. Un attacco a un UAV può essere un'applicazione di deautenticazione, che inibirà la comunicazione con l'UAV a una velocità estrema;
GPS Jamming: l'attaccante produce un segnale GPS-jamming che interferisce con i segnali GPS, causando un malfunzionamento nell'UAV del ricevitore GPS;
GPS Spoofing: è un attacco simile al GPS Jamming, che è più sofisticato poiché l'attaccante invia un messaggio falso che può modificare la direzione dell'UAV piuttosto che produrre segnali distraenti;
Drone Botmaster: metodo per utilizzare prima un drone per costruire e poi controllare una botnet nascosta rivolta a Internet. Un drone migliorato effettua tre voli su un'area urbana. Durante il primo volo, il drone rileva e raccoglie informazioni sulle reti WiFi all'interno dell'area di attacco. Il secondo volo viene utilizzato per accedere alle reti vulnerabili. Durante il viaggio finale, il drone si unisce alle reti compromesse e arruola gli host locali in una botnet.

Simulazione di un attacco di deauthentication
L'attacco ad un drone sfrutta la vulnerabilità del sistema di comunicazione tra il drone e la stazione di controllo.

Molti dei droni commercializzati e di libero utilizzo (peso sotto i 250gr), si connettono alla stazione di controllo tramite connessione WiFi, presentandosi come Access Point ed accettando connessioni in ingresso.

Questa connessione è una connessione aperta, quindi senza protezione WPA/WPA2.

Il sistema di comunicazione si presta ad un attacco di deauthentication, che consente ad un attaccante di disconnettere la stazione di controllo dal drone e connettersi direttamente al drone prendendone il controllo.

La simulazione dell'attacco condotta sfrutta questa vulnerabilità ed agendo con un semplice apparato Raspberry Pi si è in grado di bombardare la comunicazione WiFi tra stazione base e drone (fase di deauthentication); inoltre, agganciando il drone mediante una seconda scheda WiFi e sostituendosi alla stazione di controllo, si è in grado di prendere il controllo del drone con lo scopo di catturare anche le immagini che il drone acquisisce mediante la sua telecamera.

Conclusioni
L'enorme aumento dell'uso di droni e UAV ha portato a una nuova era dell'aviazione di veicoli aerei autonomi sia in ambito civile che militare, offrendo numerosi vantaggi tra cui economici, commerciali, industriali, principalmente grazie alla loro autonomia, flessibilità e facilità di utilizzare la natura, a basso costo e consumo energetico. Tuttavia, il loro utilizzo ha portato all'emergere di molti

problemi di sicurezza e privacy, che si sono manifestati attraverso vari attacchi informatici, minacce e sfide.

Ad esempio, senza un efficiente IDS (Intrusion Detection System), i droni possono essere seriamente compromessi ed essere utilizzati per condurre attacchi informatici o fisici contro individui e proprietà.

Particolare attenzione va poi data ai dati raccolti dai droni che richiedono consapevolezza e conoscenza delle regole e del senso civico da parte di chi guida il drone, ma richiedono anche estrema attenzione da parte di chi conserva e gestisce questi dati.

La buona notizia è che mentre il perimetro di un attacco a questi dispositivi è estremamente vario, è possibile fare affidamento su diverse pratiche di sicurezza già sviluppate per IoT e IT, inclusi i framework descritti e garantendo che almeno:

il firmware e il software dei droni siano continuamente aggiornati, ci siano sistemi di autenticazione attivi e robusti. Idealmente, tutti i controlli necessari per i dispositivi IoT dovrebbero essere necessari anche sull'IT;
i droni vivano in un ecosistema sicuro e quindi applicano i controlli di sicurezza e che su di essi si attivi l'opportuna governance.
In conclusione, il pericolo è sempre sottovalutato, ed è questa la causa che determina il successo di alcuni cyber-attacchi: in questo caso quelli contro i droni. La CyberSecurity è sempre un parametro imprescindibile da tenere in considerazione: a partire dall'azienda produttrice fino al soggetto finale, dove la security by design ancora una volta si rivela il giusto enabler.
Articolo a cura di Domenico Raguseo, Rosita Galiandro, Giuseppe Marullo e Antonio De Chirico

Informazioni sull'Autore

Domenico Raguseo
Domenico Raguseo è Responsabile della Unit di CyberSecurity di Exprivia. Precedentemente ha ricoperto il ruolo di CTO della divisione IBM Security nel Sud Europa. Ha una decennale esperienza manageriale e nel campo della cybersecurity in diverse aree. Domenico collabora con diverse università nell'insegnamento su tematiche relative alla cybersecurity sia come Professore a contratto che invitato come lettore per seminari. Domenico è stato IBM Master inventor grazie a una moltitudine di brevetti e pubblicazioni in diverse discipline (Business Processes, GLI AUTORI © Clusit 2020 249 ROI, Messages and Collaborations, Networking). Infine, è apprezzato speaker, autore e blogger in eventi nazionali ed internazionali. In particolare, da diversi anni collabora con il Clusit come autore

Informazioni sull'Autore

Rosita Galiandro
Rosita Galiandro ha conseguito la laurea Magistrale in Sicurezza Informatica presso l'Università di Bari.
Attualmente ricopre il ruolo di Responsabile Osservatorio CyberSecurity presso Exprivia.
Contribuisce alle attività di prevendita, ha partecipato a progetti di risk assessment e GDPR compliance e collabora in piani di insegnamento con diverse università nell'ambito CyberSecurity e nel progetto CyberChallenge.IT. Fa parte della community Women For Security.

Informazioni sull'Autore

Giuseppe Marullo
Giuseppe Marullo è responsabile dei Servizi di OT security di Exprivia. Precedentemente è stato presales in Blue Coat e Symantec per clienti enterprise in ambito network and cloud security. Ha fatto parte dello WW SWAT team e di X-Force in IBM, come SME di network security e computer forensics.

Informazioni sull'Autore

Antonio De Chirico
Responsabile del Security Operation Center di Exprivia. Ha lavorato nella Polizia di stato per oltre 27 anni, di cui 15 operando all’interno della Polizia Postale e delle Comunicazioni nelle attività investigative e di contrasto al Cybercrime ed alla pedopornografia online. Ha operato come CTU per diverse Procure e negli ultimi anni coordinava il team di specialisti del Centro Unico di Backup della Polizia di Stato.