CS 6600 Project Report: Unmanned Aircraft System

Matthew Whitesides and Bruce M. McMillin
Department of Computer Science
Missouri University of Science and Technology, Rolla, MO 65409-0350

Abstract—The following paper will look at various security models applied to an Unmanned Aircraft System's typical usage scenario. We evaluate the pros and cons of each method and give an example implementation of the model to determine the effectiveness of detecting security leaks within the system.

1 INFRASTRUCTURE

1.1 Infrastructure Description

In its simplest form, an unmanned aircraft system (UAS), is an aircraft system that operates without an onboard pilot. UAS are either controlled remotely through some form of wireless radio communication, semi-autonomously in conjunction with a remote pilot, or fully autonomously using some form of computational intelligence as navigation. These intelligent crewless vehicles have many potential uses in the defense sector, including surveillance, strategic mission execution, aerial sustainability support, and training systems, to name a few. These aircraft fall under the umbrella of cyber-physical systems (CPS), merging the intelligent navigation processes, system health monitoring, and communication with the physical mobile aerial vehicle.

We will design a proposed infrastructure security policy for the Boeing MQ-25 unmanned aircraft system, but it will also apply to similar mission support drones. The MQ-25 is an unmanned aircraft system designed for the U.S. Navy, and it provides autonomous refueling capability for the Boeing F/A-18 Super Hornet, Boeing EA-18G Growler, and Lockheed Martin F-35C fighters. This capability extends the combat range of the supported aircraft, seamlessly and semi-anonymously navigating to the plane, refueling, and returning to base. MQ-25 is the first unmanned aircraft to support aerial refueling another aircraft and is currently in the flight test phase of development [1], making it the perfect system to analyze security impacts for current and future unmanned aircraft systems. For the purposes of this document we will take the basic idea of the MQ-25 and model a UAS system referred to as the MX-01 UAS.

1.1.1 Infrastructure Security Policy

Our infrastructure security policy breaks down the various actions a system user can perform using the following terms.

- *Subject*: Any entity that contains the proper rights can request the UAS perform operations, access objects, or grant rights to another subject.
- *Object*: An entity that is part of the UAS functionality or data that does not have control over another entity.
- *Rights*: A property assigned to a subject that defines its right to access an object or grant permissions to another subject.

TABLE 1
Description of rights over objects in the UAS.

Right	Description
Owns (O)	The owner of the given object.
Read (R)	Can observe the given object.
Write (W)	Can modify the given object.
Execute (E)	Can execute the functionality of the given object.
Grant (G)	Can grant a given right to another subject.
Control (C)	Can control a given system object.
Delete (C)	Can delete a given object or right.
Create (C)	Can create a new subject or object.

Table 1 describes the rights and their associated functionality. Table 2 breaks down the subject roles involved in operating the UAS during a refueling mission. Table 3 contains the access control matrix (ACM) showing each Subject's rights over the objects.

1.2 HRU

The Harrison, Ruzzo, Ullman security model (HRU) establishes a finite set of mono-operational procedures our system can perform on subjects and objects. Given our set of rights and ACM, we will establish a set of commands available to the system that acts upon the subjects and objects in the system. The commands will consist of mono-operational modifications and pre-condition checks. Therefore given these sets, we can show how a specific set of commands can create a rights leakage.

The following shows the basic HRU commands related to our UAS mission. A fundamental UAS refueling mission follows these basic steps.

1) UAS is verified flight-ready by the MC.
2) The PC plans the mission.
3) The PC and IP execute the mission.

TABLE 2
Description of actor subject roles during a UAS refueling mission.

Subject	Description
Pilot Commander (PC)	The primary remote pilot of the UAS during the mission.
Instructor Pilot (IP)	Assists the Pilot Commander and can pilot the UAS if given permission from the PC or MC.
Maintenance Crew (MC)	Handles work orders created by the PC, IP, or FDA, responsible for the maintenance of the UAS.
Flight Data Admin (FDA)	Handles and analyses all mission flight data.
External Contractor (Bad Actor) (EC)	Has a similar job to the MC however only has read rights to the FED.

TABLE 3
Initial UAS Refueling Mission Access Control Matrix

	PC	*IP*	*MC*	*FDA*	*EC*	**ANC**	**RO**	**FED**	**RTD**	**FRS**
Pilot Commander (PC)	O,R,W	R,W	R,W	R,W	R,W	O,R,W,E,G,C	O,R,W,E,G,C	R,W,E,G,C	R,W,E,G,C	R,W,E,G,C
Instructor Pilot (IP)	R	O,R,W	∅	∅	∅	R,W,E,C	R,W,E,C	R,E	R,E	R,E
Maintenance Crew (MC)	∅	∅	O,R,W	∅	R	∅	∅	R,E	R,E	R,E
Flight Data Admin (FDA)	∅	∅	R	O,R,W	O,R,W	∅	∅	O,R,W,E,G,C	O,R,W,E,G,C	O,R,W,E,G,C
External Contractor (Bad Actor) (EC)	∅	∅	∅	∅	O,R,W	∅	∅	∅	R	∅
Autonomous Navigation Control (ANC)	∅	∅	∅	∅	∅	R,W,E,C	R	R	R	∅
Refueling Operation (RO)	∅	∅	∅	∅	∅	∅	R,W,E,C	R	R	∅
Flight Engine Data (FED)	∅	∅	∅	∅	∅	∅	∅	R,W,E,C	∅	∅
Refueling Tank Data (RTD)	∅	∅	∅	∅	∅	∅	∅	∅	R,W,E,C	∅
Flight Record System (FRS)	∅	∅	∅	∅	∅	∅	∅	∅	∅	R,W,E,C

TABLE 4
ACM After Create Flight Record

	PC	*IP*	*MC*	*FDA*	*EC*	**ANC**	**RO**	**FED**	**RTD**	**FRS**	**FR**
PC	O,R,W	R,W	R,W	R,W	R,W	O,R,W,E,G,C	O,R,W,E,G,C	R,W,E,G,C	R,W,E,G,C	R,W,E,G,C	R,W,E,G,C
IP	R	O,R,W	∅	∅	∅	R,W,E,C	R,W,E,C	R,E	R,E	R,E	R,E
MC	∅	∅	O,R,W	∅	R	∅	∅	R,E	R,E	R,E	R,E
FDA	∅	∅	R	O,R,W	O,R,W	∅	∅	O,R,W,E,G,C	O,R,W,E,G,C	O,R,W,E,G,C	O,R,W,E,G,C
EC	∅	∅	∅	∅	O,R,W	∅	∅	∅	R	E,W	∅
ANC	∅	∅	∅	∅	∅	R,W,E,C	R	R	R	∅	∅
RO	∅	∅	∅	∅	∅	∅	R,W,E,C	R	R	∅	∅
FED	∅	∅	∅	∅	∅	∅	∅	R,W,E,C	∅	∅	∅
RTD	∅	∅	∅	∅	∅	∅	∅	∅	R,W,E,C	∅	∅
FRS	∅	∅	∅	∅	∅	∅	∅	∅	∅	R,W,E,C	∅
FR	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	R,W,E,C

4) During the flight, the PC and IP execute the ANC and RO as needed.
5) After the refueling operation, the UAS returns to base, and the flight is debriefed.
6) PC, IP, or MC download the flight data from the UAS flight recorder.
7) A flight record (FR) is created that contains flight tracking information, engine usage data, and various UAS health status.
8) This flight record is uploaded by the PC, IP, MC, or EC to the record-keeping system.
9) Mission is completed.

With this in mind, we have the following basic HRU commands available for post-flight maintenance (steps 5 - 9). We will then show how improper use of these commands can lead to a rights leakage with our external contractor standing in as our "bad actor" gaining a leak of Integrity and confidentiality rights beyond our initial ACM.

The first command is a generic *Grant r Rights* that allows a subject to grant any right they have over a subject/object to another subject/object.

```
command grant_r_right(r, o, p, q)
  if grant in A[p, o] and r in A[p, o]
  then
    enter r into A[q, o];
end
```

Next we have command *Make Owner* allowing a subject p to make another subject q the owner of a object o they currently have owner rights over.

```
command make_owner(p, q, o)
  if owns in A[p, o]
  then
    enter owns into A[q, o];
```

```
end
```

When the *PC* and *IP* return from a flight they or a *MC* will read the flight data and create a new object **Flight Record (FR)** holding the flight data, available to subjects who have **FED** access. After running this command, our ACM would transition to a new state similar to Table 4, representing the subjects and objects involved in the create flight record procedure. This command will also give rights to the FRS to control the flight record data once uploaded.

```
command create_flight_record(p)
  if create in A[p, FED]
  then
    create object FR;
    enter own into A[p, FR];
    enter delete into A[p, FR];
    enter read into A[p, FR];
    enter grant into A[p, FR];
end
```

After creating a flight record which may be done by a PC, IP, or MC, they may choose to give the task of processing and uploading the flight record to an external external contractor and execute the following command to provide them with access to the record. In the command *Grant Flight Record Access*, *p* is the subject granting the right to subject *q*, for the *fr* flight record.

```
command grant_flight_record_access(p, q,
    fr)
if own in A[p, fr]
then
  enter read into A[q, FR];
  enter write into A[q, FR];
  enter execute into A[q, FR];
end
```

Finally, the flight record needs to be uploaded to our flight record system using the following *Upload Flight Record* command with *p* being the subject executing the command and *fr* being flight record to upload.

```
command upload_flight_record(p, fr)
if own in A[p, fr] and read in A[p, FRS]
then
  enter read into A[FRS, FR];
  enter write into A[FRS, FR];
  enter execute into A[FRS, FR];
  enter control into A[FRS, FR];
end
```

Similar to *Create Flight Record* a subject may need to delete or update a flight record from the system.

```
command
    delete_flight_record_from_system(p, FR)
if delete in A[p, FR]
then
  delete read from A[FRS, FR];
  delete write from A[FRS, FR];
  delete execute from A[FRS, FR];
  delete control from A[FRS, FR];
end
```

If any modifications need to be made to the FRS, the following command begins an update transaction and ends one for a given subject and flight record.

```
command update_flight_record_system(p, FR)
if own in A[p, FR]
 then
   enter read into A[p, FED];
   enter read into A[p, FR];
   enter write into A[p, FED];
   enter write into A[p, FR];
 end
```

1.3 Rights Leakages

1.3.1 Confidentiality

For our example of a confidentiality attack, we simulate a scenario where our *External Contractor* is a bad actor seeking leaked rights beyond the initial ACM utilizing the following HRU commands available for the UAS.

The following sequence of commands is typical among a mission debriefing process.

```
create_flight_record(Maintenance Crew
    (MC));
grant_flight_record_access(Maintenance
    Crew, External Contractor (EC), Flight
    Record (FR));
upload_flight_record(External Contractor
    (EC), Flight Record (FR));
```

However, when running *upload_flight_record*, the EC will find they do not have "own" rights over the record, which is required so that they will go back to the original MC and as to grant them execute privileges to the FRS system. The MC will execute the commands to make EC have permission to upload the FR.

```
make_owner(MC, EC, FR);
command grant_r_right(execute, FRS, MC,
    EC);
```

This command, unfortunately, will lead to a leak as the contractor (EC) now has the execute privileges over the FRS, which they did not initially and is not intended and can lead to other flight records confidential information being exposed to the EC. Table 4 shows the leaked rights in red.

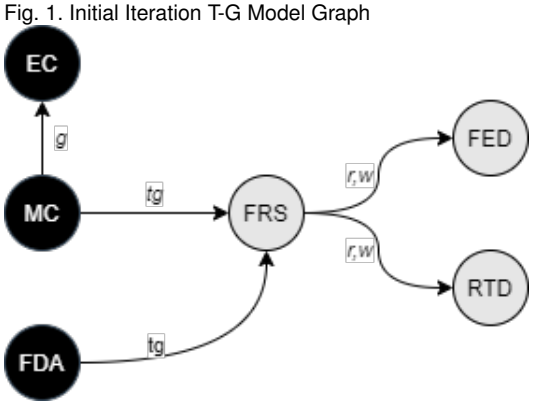
1.3.2 Integrity

In an attempt at an integrity leak, our EC may seek to modify existing data and, to get permission to do so, may attempt the following sequence.

```
create_flight_record(Maintenance Crew
    (MC));
upload_flight_record(External Contractor
    (EC), Flight Record (FR));
grant_flight_record_access(Maintenance
    Crew, External Contractor (EC), Flight
    Record (FR));
make_owner(MC, EC, FR);
update_flight_record_system(EC, FR);
```

However, upon reviewing the FR, the MC notices an issue in the data and wants the EC to update the flight

Fig. 1. Initial Iteration T-G Model Graph



record system. Unfortunately, *Update Flight Record System* checks only for rights to the given flight record and not the initial systems, therefore, giving the EC *write* access to the FRS system, which could lead them modifying the FRS data ruining its integrity. Table 4 shows the result of executing the confidentiality and integrity leaks.

2 Survey

2.1 Take-Grant

Next, we take a look at the Take-Grant (TG) model interpretation of our rights leakages. This model represents our system as a directed graph, with our subject and objects represented as vertices (black for subjects, white for objects). Edges represent the rights on vertex has over another, where special take (*t*) and grant (*g*) representing the ability of a subject or object to give or obtain rights from another subject or object. In our case, subjects can execute a grant HRU command representing the grant right, and take can be achieved by rights automatically allocated by granting access to specific objects (i.e., the FRS).

This models our HRU example in terms of a TG model where the *Flight Record* created object has *read, write* rights over the *Flight Record System* that our **External Contractor (EC)** can utilize to gain *read, write* access to the *Flight Engine Data*.

Our bad actor could achieve this leak through the following TG commands.

1) **MC** creates object **FR**.
2) **MC** grants (*t* to **FR**) to **EC**.
3) **EC** takes (*r,w* to **FRS**) from **FR**.
4) **EC** takes (*r,w* to **FED**) from **FRS**.

Figure 1 shows the initial state of rights among actors and objects in the **FRS** system.

Figure 2 shows the state of rights after the **MC** runs the HRU command *create_flight_record(MC)* which a new **FR** object.

Figure 3 shows the state after the **EC** leads the **MC** into giving them *t* rights over **FR** they can exploit the system to take our leaked rights to **FED** through the **FRS**. This would be established after the command *grant_flight_record_access(MC, EC, FR)*.

Therefore allowing EC to execute *update_flight_record_system(EC, FR)* which leaks access to the FED as shown by the state in Figure 4.

Fig. 2. Iteration 2 T-G Model Graph

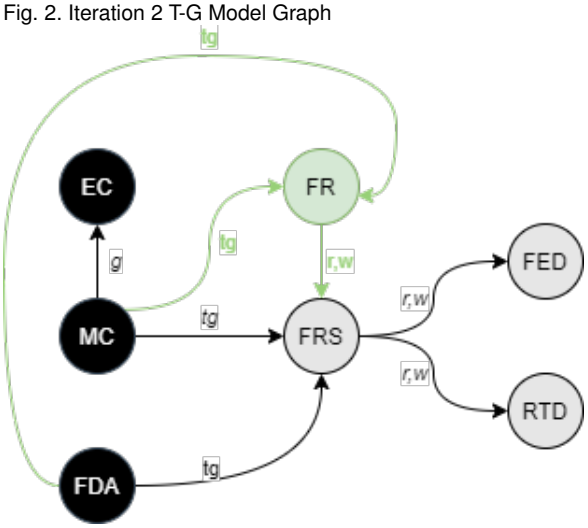
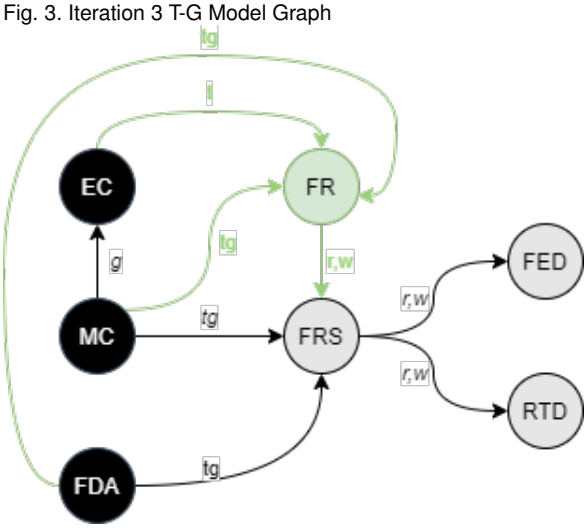


Fig. 3. Iteration 3 T-G Model Graph



Using this TG protection model instead of the simple HRU commands, we demonstrate that the safety question is decidable in linear time based on our graph consisting of seven nodes.

2.2 Bell-LaPadula

The Bell-LaPadula Model (BLP) focuses on establishing access control confidentiality through security levels and categories. BLP focuses on two simple rules in a security policy within a given ACM. The simple security property states a subject can not read an object at a higher security level. The star property states that a subject may not write to any object at a lower security level.

The primary limitation we see when implementing a BLP model into our existing policy is our external contractor and maintenance controllers. We need access to the flight records, so they require at least *confidential* clearance levels. These restrictions make it hard to read the flight record system at a *secrete* level and our FRS to write to the flight records.

For our BLP implementation, we first define the security classifications for our subjects and objects. Given we are

Fig. 4. Final Iteration T-G Model Graph

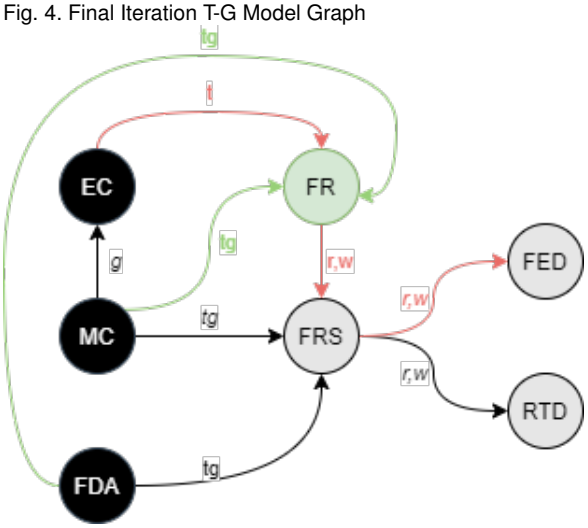


TABLE 5
Security Classifications for the UAS

Clearance Level	Subjects	Objects
Top Secret (TS)	PC, FDA	ANC, RO
Secret (S)	IP	FRS, RTD
Confidential (C)	MC, EC	FED, FR
Unclassified (UC)		

dealing with military records, it makes sense to use the standard government security levels. In addition to the security level, subjects and objects will fall into categories based upon the appropriate work unit. Table 5 shows the security clearance levels and the subjects/objects at the given levels. Table 6 shows the work unit categories of each subject/object.

Now that we've established security classifications for our subjects and objects, we can see how the system and security policy could still allow leakage and further theft of flight record data.

```
create_flight_record(Maintenance Crew
    (MC));
grant_flight_record_access(Maintenance
    Crew, External Contractor (EC),
    Flight Record (FR));
upload_flight_record(External Contractor
    (EC), Flight Record (FR));
make_owner(MC, EC, FR);
update_flight_record_system(EC, FR);
```

1) **MC** executes *create flight record* creating flight record object **FR**.
   - This write is allowed as the object **FR** created has clearance level of *Confidential* which is greater than or equal to **MC's** level of *Confidential* and **FR** dominates **MC** by categories.
2) **MC** executes *upload flight record* granting the object **FRS** access to the flight record object **FR**.
   - This write is allowed as the object **FRS** created has clearance level of *Secret* which is greater than **FR's** level of *Confidential* and **FRS** dominates **MC** by categories.
3) **MC** executes *grant flight record access* granting **EC** access flight record object **FR**.
   - This read is allowed as the subject **EC** created has clearance level of *Confidential* which is greater than or equal to **FR's** level of *Confidential* and **MC** dominates **EC** by categories.
4) **MC** executes *make owner* making **EC** have owner rights over flight record object **FR**.
   - This write is allowed as the subject **EC** created has clearance level of *Confidential* which is greater than or equal to **FR's** level of *Confidential* and **FR** dominates **EC** by categories.
5) **EC** executes *update flight record system* allowing **EC** write to the flight record system object **FRS**.
   - This write is allowed as the subject **EC** created has clearance level of *Confidential* which is less than or equal to **FRS's** level of *Secret* and **FRS** dominates **EC** by categories.

TABLE 6
Work Unit Categories for the UAS

Category	Subjects	Objects
Flight Ops (FO)	PC,IP	ANC,RO
Maintenance Ops (MO)	PC,IP,MC,FDA	FED,RTD,FR,FRS
Flight Data Ops (FDO)	PC,IP,FDA,EC	FED,FR,FRS

As you can see, while this system does keep our bad actor **EC** from reading the confidential flight records from the flight record system, it does not prevent an integrity attack of writing up to the **FRS** and **FR**.

We can setup our BLP system state in the context of the command leakages as follows:

- $S = \{MC, EC\}$
- $O = \{FRS, FR\}$
- $P = \{owner, read, write\}$
- $C = \{Secret(S), Confidential(C)\}$
- $K = \{MO, FDO\}$
- $f_c(s) = \{(C, \{MO\}), (C, \{FDO\})\}$
- $f_c(o) = \{(S, \{MO, FDO\}), (C, \{MO, FDO\})\}$

Then as the commands are executed we can see the resulting states in Table 7.

2.3 Biba

The Biba model focuses on data integrity as opposed to the BLP model, which enforces confidentiality by restricting access. The Biba model ensures the data objects once created remain unmodified by untrusted sources by establishing integrity levels. The model achieves this by ensuring ACM transitions do not allow subjects to write/modify data above their integrity level. Subjects do not read data below their level to avoid being influenced by data below their trusted level.

TABLE 7
BLP System State Commands

	i_0	i_1	i_2	i_3	i_4
X	{(r, ∅), (∅, ∅)}	{(r, ∅), (r, o)}	{(∅, r), (∅, ∅)}	{(∅, o), (∅, ∅)}	{(∅, w), (∅, ∅)}
Y	{(y, n), (n, n)}	{(y, n), (y, y)}	{(y, y), (∅, y)}	{(y, y), (∅, y)}	{(∅, y), (y, y)}
Z	V_1	V_2	V_3	V_4	V_5

TABLE 8
Security Categories for the UAS

Security Category	Subjects	Objects
Archived Data (AD)	PC,MC,FDA	FRS
Operational Data (OD)	PC,IP,MC	ANC,RO,FED,RTD
Ready To Load (RTL)	FDA,MC,EC	FR,FRS

These notions apply to our infrastructure well as the bad actor (External Contractor), in theory, could either read data they're not supposed to (violating confidentiality). Or the EC could modify existing flight record data (violating integrity). If the confidentiality policy is perfectly implemented, no data is accessed that is outside their security level. However, there's still an amount of "trust" we have in the EC and system preventing the integrity of the data from being violated. The Biba model attempts to quantify this level of trust and maintain the flow of information, inhibiting its modification by lower trusted subjects/objects.

2.4 BLP-Biba Lipner Like

Lipner proposed an integrity model that combined aspects of the BLP and Biba model to fit a more real-world commercial software development environment. Lipner created security levels and categories similar to BLP to prevent various software development lifecycle subjects from accessing different systems. Lipner then added to the security classifications with integrity classifications for system programs and integrity categories to differentiate development and production environments.

In our BLP model we established various security classifications (Table 5) and work unit categories (Table 6) so we need to establish security categories to define the area of impact in the given category (Table 8).

We can now incorporate integrity categories to allow distinction between on aircraft systems and the flight record keeping system (Table 9) and integrity classifications to determine the trust of the data combing from that source (Table 10 highest to lowest level).

This gives us an overall security and integrity clearance levels for subject categories (Table 11) and objects (Table 12).

Ideally, these classifications would block EC from accessing FRS by putting them in a lower classification stopping our rights leakage. However, due to the requirement of MC to allow EC to read a flight record, our system would not operate otherwise.

2.5 Clark Wilson

The Clark Wilson is an integrity verification model that enforces a principle of *separation of duty* in that a subject/object that verifies a data state transition is not the same one that caused it. Data with valid integrity is defined to be in a *consistant state*, and processes can only transform data through valid *transactions* that preserve this consistency. Data that is constrained by the separation of duty and transaction controls are said to be *constrained data items (CDIs)*. In contrast, data not constrained by these are called *unconstrained data items (UDIs)*.

TABLE 9
Integrity Categories for the UAS

Integrity Category	Subjects	Objects
On Aircraft (IOA)	PC,IP,MC	ANC,RO,FED,RTD
Flight Record System (IFRS)	FDA,MC,EV	FRS

TABLE 10
Integrity Classifications for the UAS

Integrity Classifications	Subjects	Objects
System Programs (ISP)	∅	ANC,RO,FRS
Operational (IO)	PC,IP,FDA	∅
Maintenance (IM)	MC,EC	FRS,FED,RTD,FR

After defining out CDIs, we define two procedures, an *integrity verification procedure (IVP)* that tests the system is in a valid state, and *transformation procedures (TPs)* that will change the state of the system using transactions. To ensure valid TPs occur on valid CDIs, the Clark Wilson model has various *certification rules (CR)* that ensures the TPs and IVPs

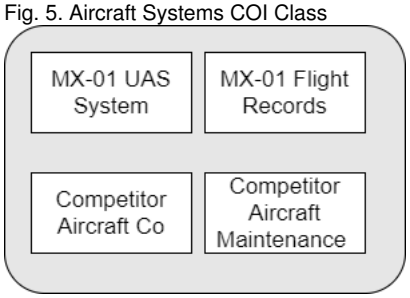
TABLE 11
Security and Integrity Levels for Work Units

Work Unit Category	Security	Integrity
Flight Ops	({TS,{OD})	(ISP,{IOA})
Maintenance Ops	({S,{AD,RTL})	(IO,{IOA,IFRS})
Flight Data Ops	({S,{OD,RTL})	(IM,{IFRS})

TABLE 12
Security and Integrity Levels for Objects

Object	Security	Integrity
ANC	({TS,{OD})	(ISP,{IOA})
RO	({TS,{OD})	(ISP,{IOA})
FED	({S,{AD,OD,RTL})	(IO,{IOA,IFRS})
RTD	({S,{OD})	(IO,{IOA,IFRS})
FRS	({S,{AD,OD,RTL})	(IM,{IFRS})

Fig. 5. Aircraft Systems COI Class



that operate on CDIs keep a valid state and *enforcement rules ER* that prevent TPs from operating on CDIs that have not been certified.

First, for our scenario, we'll define the CDIs and UDIs. In this, we'll describe the contained data items as data related to the flight record and the unconstrained being the autonomous operations. While on their own, the ANC and RO are vital, and access should be confidential. The integrity check, in this case, is specific to the flight record data.

- $CDIs = \{FED, RTD, FRS, FR\}$
- $UDIs = \{ANC, RO\}$

Next, we need to establish the *integrity constraints* over the flight record data.

- The FRs uploaded to the FRS must be equivalent to the data on the UAS as it is transferred over to the FRS.
- The FRS can only be written via new FRs or deleted, but FRs themselves cannot change.

Next, we will define the IVP commands that run on the system to ensure these constraints have been adhered to. After an executed upload, the first IVP check rereads the FR from the UAS and compares it to the FR in the FRS. The next IVP ensures that the FRS is not modified and will run before and after an upload is executed.

To execute IVP1 a different user would have to re-download the flight record from the UAS and verify against the data in the FRS system. Then to test IVP2 likely a system program would record the state of the FRS before a transaction and compare it to the state of the system after the transaction to verify none of the integrity constraints in IVP2 are invalid. Some examples of incorrect data could include the flight record dates such as the start time being after the end time, the aircraft location data indicating speeds or movements beyond the capabilities of the UAS, corrupted data in the flight record causing the inability to read basic information such as the aircraft identifier, attached components, data header parameters, etc.

- IVP1

```
read uac_flight_record uac_fr

if uac_fr != FRS[fr]
  return invalid
else
  return valid
```

- IVP2

```
read FRS initial_FRS

\\ Execute any TP

read FRS after_FRS

foreach FR in after_FRS
  if FR in initial_FRS
    if FR.FlightData !=
        initial_FRS[FR.ID].FlightData
      return invalid

return valid
```

Now we can define the TPs that our model can execute to preform the FRS functionality. These commands themselves enforce the CR rules.

- TP1: execute create_flight_record(p)
- TP2: execute upload_flight_record(p)
- TP3: execute delete_flight_record_from_system(p)
- TP4: execute update_flight_record_system(p)

2.6 Chinese Wall

The Chinese Wall model is a hybrid approach that enforces both confidentiality and integrity. It establishes a separation or "wall" between subjects and objects that would have a conflict of interest between them. For example, a subject who has read the engine data of our MQ-25 UAS would have a conflict of interest if they were to work on another UAS from another company. Our policy enforces that subjects who have a conflict of interest do not have access to specific data defined in our *conflict of interest classes*. In our scenario, we describe our *objects* related to our UAS data from Table 3. These objects will be contained in our *company datasets (CD)*, containing our various UAS data. Above that, our *conflict of interest class (COI)* defines what CDs our subjects will have access to and how they will be protected if later transferred to another company/organization.

First we'll define our *company datasets (CD)* and our *objects* in our datasets that contain information related to our UAS. These datasets will fall under an **Aircraft Systems** COI class (Figure 5).

$$CD = (\{FlightRecords, \{FED, RTD, FRS\}\}, \{UASOperations, \{ANC, RO\}\})$$

In this scenario, any subject having read a from a competitor dataset could not access a dataset in our COI class. If we wanted to allow access to a specific object in our dataset (i.e., a **Flight Record**), we could implement a sanitization method on the **Flight Records**. We could establish a new **Sanitized Flight Record** and only allow the EC access to this sanitized object. However, a new process would need to create the sanitized record off the original FR after upload and be maintained on a new sanitized FRS, which does not allow the MC and EC to do their jobs thoroughly. Also, this would only allow the EC not to conflict when later moving to a competitor company.

3 NON-INTERFERENCE (NI)

The Non-Interference (NI) model focuses on information flow to ensure that objects and subjects at each security level do not "interfere" with those at different levels. It achieves this by modeling inputs and outputs at different sensitivity levels, i.e., High and Low. It intends to ensure that those modifying data at a low level of security clearance can only see the machine's state as if only low-level interactions were occurring regardless of what the high-level entities are doing. For example, in our system, the Pilot Commander executing flight instructions on the ANC should not change their system state or be visible by a Maintenance Contractor reading old flight records. These rules are all in an attempt to ensure high-level activities are not visible by low levels, with the theory being low levels would be able to infer information about high-level activities by these changes.

To detect interference, we will utilize a scenario similar to our BLP situation where the following commands are executed from the MC and EC that produces a rights leakage. Essentially to detect interference, we need to determine if actions that modify the FRS (which is at a *Secret* clearance level) produce outputs that can be seen by the EC (at a lower *Confidential* level).

```
create_flight_record(Maintenance Crew
    (MC));
grant_flight_record_access(Maintenance
    Crew, External Contractor (EC),
    Flight Record (FR));
upload_flight_record(External Contractor
    (EC), Flight Record (FR));
make_owner(MC, EC, FR);
update_flight_record_system(EC, FR);
```

3.0.1 Confidentiality

Using NI to verify a breach in confidentiality, we need to trace the output of commands from the EC's point of view, then compare that with trace with the higher-level commands removed from the process and determine if we have the same output. In our case, the EC modifies the FRS and adds a new FR into the system. The question is, will the system still produce the same output with the higher-level commands purged.

This sequence can be formulated as an equality check of the projection of the EC's command sequence output and the projection of the command sequence with the high-level commands removed.

$$proj(EC, C_s, \sigma_0) = ?Proj(EC, \pi FR(C_s), \sigma_0)$$
$$C_s = (MC, cfr()), (MC, gfra()), (EC, ufr), (EC, ufrs())$$

The projection of the initial system for the EC and MC gives us the following states:

$$proj(MC, C_s, \sigma_0) = (\{FRS = \{FR\}\})$$
$$proj(EC, C_s, \sigma_0) = (\{FRS = \{FR'\}\})$$

$$\pi MC(C_s) = (MC, cfr()), (MC, gfra())$$
$$\pi EC(C_s) = (EC, ufr), (EC, ufrs())$$

Ultimately we are checking if the FR exists in the same state and the FR exists in both states; however, the EC's commands do modify the FR, thus making the final output state differ so the system is not NI secure regarding confidentiality.

3.0.2 Integrity

For integrity we simply want to know if from the MC's prespective we can detect if changes were made to the system from the EC.

$$proj(MC, C_s, \sigma_0) = ?Proj(EC, \pi FR(C_s), \sigma_0)$$
$$\{FRS = \{FR\}\} \neq \{FRS = \{FR'\}\}$$

We can see from our previous projections that the MC can in fact detect changes to the FR thus making the system NI secure in regards to integrity.

4 NON-INFERENCE (NF)

Non-Inference is similar to Non-Interference in that it wants to limit the ability of low-level entities to detect the actions of high-level ones. However, NF allows high-level actions as long as the same output could be achieved by low-level ones, thus obfuscating the guarantee to the low-level entity whether the result came from a high or low-level action.

For example, in our scenario, we want the actions of S and TS clearance levels to be hidden from the MC and EC subjects at the C security level. In the NI example, we showed how the standard flight record creation BLP procedure that produced a leak earlier was not NI secure based upon the actions taken by the EC when executing on the FRS.

The question becomes, is it indistinguishable if the FR is written by the MC, or is it due to something within the External Contractor's domain. We showed in NI that the output of the EC and MC can alter the FR; however, one FR is not inherently at a different level than another FR or indicates where it came from. Thus there's no distinct difference in the output of the following command sequences.

$$C_s(MC) = ((MC, cfr()), (MC, ufr()), (MC, ufr()))$$
$$C_s(EC) = ((EC, cfr()), (EC, ufr()), (EC, ufr()))$$

Each produce the output of $\{FRS = \{(FR_0), (FR_1)\}\}$ regardless of order of execution or the FR uploaded. Therefore the system is considered NF secure.

Overall I don't think being NF secure is as helpful as NI for this system regarding confidentiality. It allows the EC to hide whether the FRs came from them or a higher-level entity. The FRS procedures could update the system to indicate the owner or uploader of the records, then differentiate the outputs. This split system could combine with a Clark Wilson model to have a verification procedure that a higher level subject uses to verify the actions performed at the lower level since they would not have access to any FRs from the system.

Similarly, if the MC was to utilize NF to validate the integrity of the data, this could be more plausible. We have the actions performed split into higher and lower levels.

The actions performed by the lower levels could lead to the same output as a higher levels action sequence. However, if we had some verification procedure, we could trace back the actions to the level performing them, thus knowing the integrity of the output data.

5 Non-Deducibility (ND)

Our NI and BLP model focuses on the inability of information from higher levels to flow down to lower levels. In other words that our low-level outputs should not reveal any information about high-level outputs. On the other hand, Nondeducibility is similar but considers a scenario of low and high-level inputs and low and high-level outputs. Given a low-level subject can only see the series of low-level outputs, can they deduce any information about the high-level inputs or outputs? In other words, could the trace of multiple low-level outputs with a mix of high-level inputs be achieved purely by low-level inputs? This scenario would not allow a low-level observer to deduce for sure that the outputs were from high-level inputs, and vice versa if low-level inputs create high-level outputs.

In our scenario, we can think of this by thinking of the EC seeing the output of multiple FRs going through the system and attempting to deduce any information about the higher level FRS secrete clearance inputs/outputs. Let us take a scenario of three flight records going through the system. Two fully uploaded by the MC and one utilizing the rights leakage scenario where the MC grants access to one of the FRs to the EC attacker.

5.1 Confidentiality

To detect our potential confidentiality non-deducibility leak, we will look at the projections from the lower level EC output given a scenario of transitions from the MC and the EC and determine if those projections could have occurred by only low-level inputs.

Over the following iterations, we show the projection results of the FRS system given an observer and one of the following command sequences.

scenario_one(Subject a)

```
create_flight_record(a);
upload_flight_record(b, FR_i);
```

scenario_two(HighSubject a, LowSubject b)

```
grant_flight_record_access(a, b, FR_i);
make_owner(a, b, FR_i);
update_flight_record_system(b, FR_i);
```

1) $proj(observer(EC), scenario\_one(MC)) = (\{FRS = \{\varnothing\}\})$
$proj(observer(MC), scenario\_one(MC)) = (\{FRS = \{FR_1\}\})$

2) $proj(observer(EC), scenario\_one(MC)) = (\{\varnothing\}\})$
$proj(observer(MC), scenario\_one(MC)) = (\{FRS = \{FR_1, FR_2\}\})$

$proj(observer(EC), scenario\_two(MC, EC)) = (\{FRS = \{FR_2\}\})$
$proj(observer(MC), scenario\_two(MC, EC)) = (\{FRS = \{FR_1, FR_2\}\})$

Given that the EC output only contains the FR, they had a hand in creating the same output that could be achieved by both the MC or another EC executing the following commands.

1) $proj(observer(EC_1), scenario\_one(EC_2)) = (\{FRS = \{\varnothing\}\})$

2) $proj(observer(EC_1), scenario\_one(EC_2)) = (\{\varnothing\}\})$
$proj(observer(EC_1), scenario\_two(EC_2, EC_1)) = (\{FRS = \{FR_2\}\})$

Given that both produce the same outputs at each iteration from the EC's perspective, he cannot deduce that the output came from another EC or the higher level MC, thus making the system non-deducibly secure regarding confidentiality.

5.2 Integrity

To deduce an integrity attack, we can go about it similar to NI, where our MC will attempt to deduce any integrity attacks from the EC by verifying if they can detect any changes in the FRS in an inverse of the confidentiality attack.

Here we will introduce scenario three that updates the flight record, creating our full rights leakage scenario.

scenario_three(HighSubject a, LowSubject b, FR_i)

```
update_flight_record_system(b, FR_i);
```

First, we will execute the two standard scenarios and then our leakage scenario and verify if the MC can deduce the output.

1) $proj(observer(EC), scenario\_one(MC)) = (\{FRS = \{\varnothing\}\})$
$proj(observer(MC), scenario\_one(MC)) = (\{FRS = \{FR_1\}\})$

2) $proj(observer(EC), scenario\_one(MC)) = (\{\varnothing\}\})$
$proj(observer(MC), scenario\_one(MC)) = (\{FRS = \{FR_1, FR_2\}\})$

$proj(observer(EC), scenario\_two(MC, EC)) = (\{FRS = \{FR_2\}\})$
$proj(observer(MC), scenario\_two(MC, EC)) = (\{FRS = \{FR_1, FR_2\}\})$

3) $proj(observer(EC), scenario\_three(MC, EC, FR_2)) = (\{FRS = \{FR_2'\}\})$
$proj(observer(MC), scenario\_three(MC, EC, FR_2)) =$

$$(\{FRS = \{FR_1, FR_2'\}\})$$

Now the MC can detect FR prime indicating changes to the FR. However, they cannot deduce who the record was changed by as scenario three would produce the same output.

3 $proj(observer(MC_1), scenario\_three(MC_1, MC_2, FR_2)) = (\{FRS = \{FR_2'\}\})$
$proj(observer(MC_2), scenario\_three(MC_1, MC_2, FR_2)) = (\{FRS = \{FR_1, FR_2'\}\})$

Therefore in regards to integrity our system is non-deducibility insecure, which makes sense as if it is secure from the attacker's perspective. It would logically make it non-deductible from a trusted perspective.

6 MSDND

Much like our other security models, Multiple Security Domain Nondeducibility (MSDND) deals with information flow between the security user domains within a system and the policies that allow or deny the transfer. However, because our system is a cyber-physical system (CPS), we must consider both physical and virtual methods of attack. MSDND accounts for information flow between the system's physical and computing components, allowing for various security domains (SD) without needing a hierarchical security level system. This SD model allows for information-flow restrictions that are not limited to high and low but allow for information flow in both directions and more complex states to be considered.

In our UAV scenario, we have the physical component of the user physically connecting to the UAV, downloading the data, and uploading the flight record to our flight record system. Therefore the cyber component is the FRS itself and the UAV system software. In the traditional Nondeducibility model, we showed the information leak from the EC and MC perspective and how the EC cannot deduce the information, but this, in turn, means the MC cannot infer any information integrity changes. However, let's think about this from a more CPS point of view, emphasizing the physical portion of the environment. The EC and MC must exist within the same physical areas. Physical access to the UAS and the FRS computers leads to the vector of attack using the physical hardware to create the informal leak. Modeling this combination of physical and virtual is where MSDND comes in. We can utilize more complex security domains and valuation functions to test for information leaks.

Table 13 shows us our new MSDND security domains in the context of the EC, MC, UAS, and FRS. Figure 6 similarly shows us how these domains overlap in the physical and virtual space.

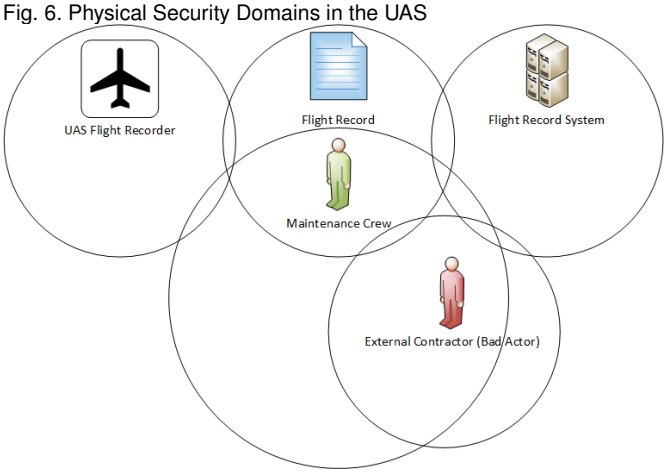
For our scenario, we'll set φ equal to "Each FR in FRS is unmodified from the original FR data in the UAS" to spot our integrity attack after the leakage where the EC gains update access FRS after the series of executions shown previously.

Our first assertion is the state of the FRS after a new upload, "Each FR in the FRS is unmodified after a new FR upload". The evaluation at the FRS only evaluates the latest of the FR in the FRS. Still, it does log when changes are made for $V_{\varphi}^{frs}(W)$ and $V_{\neg\varphi}^{frs}(W)$, therefore, securing change detection for modifications but not the inverse of no changes being made therefore making it not MSDN secure.

TABLE 13
Security Domains in the UAS FRS System

System Component	Domain	Valuation
UAS Flight Recorder	$SD^{recorder}$	$V^{recorder}$
FRS	SD^{frs}	V^{frs}
EC	SD^{ec}	V^{ec}
MC	SD^{mc}	V^{mc}
FR	SD^{fr}	V^{fr}

Fig. 6. Physical Security Domains in the UAS



The following assertion is "If a new FR MSDND secures for SD^{mc} after graning the EC access then MC can detect if changes to the FRS are made after the FR upload" from the MCs domain they can see the logs updating the system allowing them to evaluate both $V_{\varphi}^{frs}(W)$ and $V_{\neg\varphi}^{frs}(W)$. However, this manual evaluation by the MC defeats some of the purposes of the system that the MC relegated the FR upload to the EC to save time. If they need to evaluate the system after the work has been done, not much has been saved. Although this does enable it to be MSDND secure from the MCs domain, the leak would have already occurred. They only would be able to detect it.

Our final assertion is "An FR is unmodified from the UAS to the FRS upload.", the valuation at the UAS Flight Recorder correctly evaluates the download of the FR to the FRS for $V_{\varphi}^{recorder}(W)$ and $V_{\neg\varphi}^{recorder}(W)$ however therefore not allowing the conditions for detection of change to be met by MSDND, which is another point of potential disruption from the UAS system but not the goal of detecting the leak.

To prove this, we can take out the final case "Each FR in the FRS is unmodified from the UAS after a new FR upload" and our invariant procedures that verify the initial FR is equal to the FR in the FRS. Table 14 shows the MSDND proof of the FR becoming modified without the ability to deduce the change. Our final proof shows how this case and the system as a whole are not MSDND secure.

TABLE 14
MSDND Proof

1.	$\sim fr$ = true	FR has been modified.
2.	$w \vDash V^0 fr(w) = true$	FRS cannot verify the FR has been modified.
3.	$I_{1,0} fr$	FRS allows upload of the FR.
4.	$B_1 I_{1,0} \sim fr$	FRS trusts the FR from a verified user.
5.	$T_{1,0} \sim fr$	FRS trusts the FR.
6.	$B_1 I_{1,0} \sim fr \bigwedge T_{1,0} \sim fr \rightarrow B_1 \sim fr$	FRS believes the FR in the FRS.
7.	$I_{1,1} fr$	FRS logs everything is correct.
8.	$B_1 I_{1,1} fr$	MC belives the FRS logs.
9.	$T_{1,1} fr$	MC trusts the FR.
10.	$B_1 I_{1,1} fr \bigwedge T_{1,1} fr \rightarrow B_1 \sim fr$	MC belives the FRS logs are correct but the FR is modified.
11.	$w \vDash V^1 \sim fr(w) = true$	The verification procedure for FR's uploaded to the FRS always return true.

7 Conclusions

7.1 HRU

The Harrison, Ruzzo, Ullman security model is a great place to learn about security leakages. This model takes real-world surface events and forces us to boil them into definable and provable functions. The pseudo-code functions seem like the most natural starting point for analyzing a CPS coming in from a programming background. Here we were able to define our commands that carry out the system's function. In this case, the maintenance crew downloads the flight data from the UAV and grants access to the external contractor to upload that record to the system where a leak occurs within this sequence of HRU commands.

The pros to this approach are many, and I feel most security models should implement a part. The most basic idea of defining all the rights, subjects, objects, and access relationships between them in the Access Control Matrix is vital to understanding your system and how it interacts with everything else. Then defining the commands available using the simplified mono-operational logic boils down to precisely what your system is doing in logic terms. You can easily spot the rights leakages.

However, due to the strict model standards, it does make some aspects of a physical system more challenging to model. In our case, the scenario was interactions between physical components. Still, the leakage occurred virtually, so it wasn't difficult to model in this approach. Still, I could see more complex physical interactions between larger systems, making the mono-operational commands' strict rules challenging to manage.

7.2 T-G

After defining your subjects and objects, the Take-Grant model proposes a fascinating natural evolution. By creating a relationship graph between them, you can have an excellent visual overview of the relationships in the system. In particular, the TG model looks to spot places where rights can leak utilizing these special rights, take and grant that naturally form in any scenario where any given subject needs to provide access or can take rights from other subjects and objects. This graph also quickly shows the impacts adding, removing, or modifying subjects and things could have on the system.

What is particularly interesting in a CPS is how it forces you to think about rights in terms of what the subjects and objects can do instead of what they are intended to do. Seeing that a subject can inadvertently take rights from an object a few nodes down the chain in the graph is not something you naturally would notice before modeling it. This revelation is especially apparent in terms of thinking about the cooperation that must occur between subjects for some leakages. In our case, granting the rights to the FR doesn't seem on the surface to be wrong as it's required but shows in the model how it ends up leaking unwanted rights.

In our model, the challenge came from figuring out the relationships that cause the leakage because the leakage happens as a side effect of the requirements of the systems function. It ended up being perfect because what this model did do was show the relationships by default. Then once the MC grants access to the EC for the FR, we can immediately see that the unintended side effects of the EC can take rights through the FR into the FRS.

There aren't many cons that come to mind in this approach as long as you realize its intent. It does not fully model the functionality and leakages outside of direct relationships, such as what happens within the system to cause the rights changes. This limitation almost requires you to know that the rights are changing over beforehand, which still may point out unknown leakages but could miss some if you don't know the relationship changes.

7.3 BLP

The Bell-LaPadula model was our first introduction to what first comes to mind when I think of access security. Establishing security levels has been around so long it seems obvious. However, the interesting part comes from the security properties defined in the model. I understood the idea of security levels. Although, I never thought about the interaction between the levels and how you account for that. Not reading an object at a higher level makes sense and is probably what I most associated with security levels. Still,

the no writing down was an interesting idea that does make sense but wasn't something I considered.

In our case, since we're dealing with a presumably military aircraft and sensitive mission flight record data, it's apparent that we would have to have security levels in the real-world implementation of this. If not only that, everyone involved would need to have a specific clearance above baseline. In our leakage, we defined an external contractor that inherently would have a more limited amount of clearance than internal employees. It was natural to establish a level for the subjects and objects. The main issue was keeping the system functional, allowing the lower-level EC to perform their job while separating them from the higher-level subjects. This limitation is a part of how a basic security level doesn't consider lateral rights. Ideally, we could model the records that the EC handles separately from all the others so they don't have the same rights to any record, but this basic level system can't take that into account. Therefore we had to give everyone involved the same level, which probably is how it would be in the real world but couldn't be our only security model.

7.4 Biba

Biba takes a similar approach to the BLP model except focusing on data integrity. In an inverse of the no reads up, we have to enforce a no writes up and no reads down to keep data integrity only at or above the subjects given level. This method applied just as well to our case as the BLP model as our leak unintentionally grants access to more data than our EC is intended to have, thus conflicting with the Biba model standards.

This approach works well in our model to prevent integrity attacks by enforcing the security level write access in theory. Regardless if they have access, they would still not have the appropriate level. Of course, the main issue is we need both to prevent confidentiality of our data and the integrity. If the bad actor can read our flight data, that may be more damaging to our system than modifying data (although both are pretty bad). So we can't both enforce a BLP and Biba simultaneously, which we need to do.

7.5 BLP-Biba Lipner Like

We need to both enforce confidentiality and integrity. That's where our BLP-Biba Lipner Like solution comes in. This system initially came from a software production focus with development and production environments. Using this approach, we were able to keep our security levels and implement new security categories for the various aspects of the workstation. We split up our categories into the archived data integrity, current operational data, and the data ready to be loaded. These categories enable us to theoretically split the bad actor from the FRS, which we can put in separate categories. In our case, we have to allow access to enable the EC to do their job.

This Lipner-like approach is more comprehensive than BLP or Biblia by themselves. If you built the system from the ground up with this in mind could work well depending on the scenario. It could work with an ideal approach to security categories and security and integrity levels for all the objects and subjects. However, it makes a bit more sense in a purely virtual software environment where you truly can separate lower-level environments from higher-level ones. It becomes difficult if there are exchanges between levels due to the work statement requirements.

7.6 Clark-Wilson

Clark-Wilson introduces us to integrity verification through constrained/unconstrained data items and integrity verification procedures. This model mirrors some standard software development rules like the previous Lipner-like model proposed. The idea is that the data creator should not be the one verifying it. In software development, it reminds me of how the developer should not test and deploy the production code. That way, there's a layer of verification and abstraction between the development and production environments that enable data integrity.

This model would work quite well in our system if we implemented the IVPs. Then even if the rights leakage occurred to the EC, any data changes would get caught by the IVPs, thus mitigating the damages. These verification procedures would not stop confidentiality attacks of the EC reading records they should not have access to, but it would benefit from combining with other models.

7.7 Chinese Wall

7.8 Noninference

7.9 Noninterference

7.10 Nondeducibility

7.11 MSDND

REFERENCES

[1] A. Erwin, and J. Gibson, Navy, Boeing Make Aviation History with MQ-25 Becoming the First Unmanned Aircraft to Refuel Another Aircraft, Accessed on: Sept. 1, 2021. [Online]. Available: https://www.boeing.com/defense/mq25/

Matthew Whitesides Master's Student at Missouri University of Science and Technology.