A Game-Theoretic Approach for Security Control Selection

Dylan Leveille, Jason Jaskolka

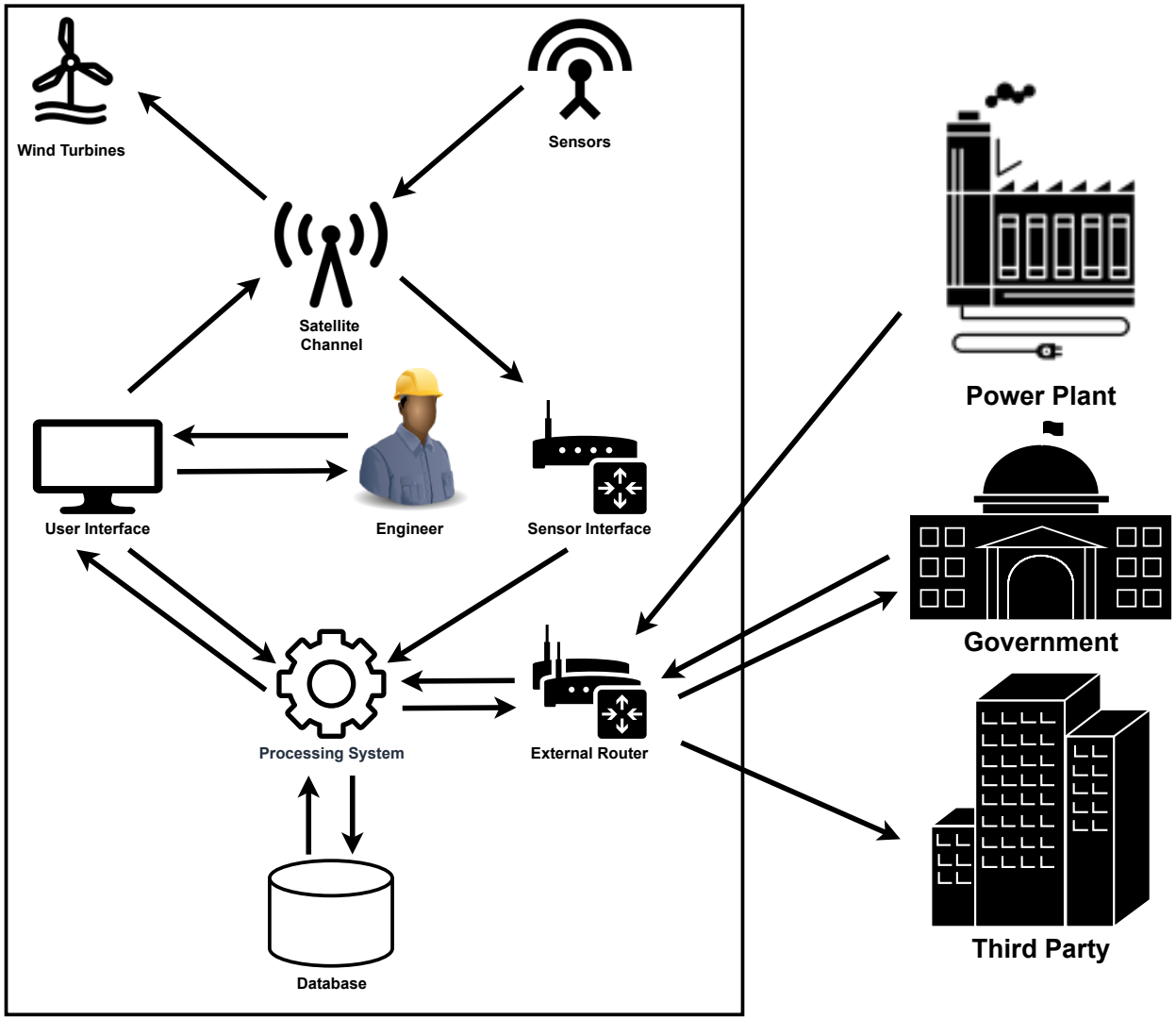
Department of Systems and Computer Engineering
Carleton University, Ottawa, ON, Canada

dylan.leveille@carleton.ca, jason.jaskolka@carleton.ca

@CyberSEA_Lab

June 20, 2024

Story


Wind Turbines
Sensors
Satellite Channel
User Interface
Engineer
Sensor Interface
Processing System
External Router
Database
Power Plant
Government
Third Party

Story (Continued) — Security Control Catalogues

ITSG-33

NIST SP 800-53

AC-7	**Unsuccessful Logon Attempts**
AC-7(1)	AUTOMATIC ACCOUNT LOCK
AC-7(2)	PURGE OR WIPE MOBILE DEVICE
AC-7(3)	BIOMETRIC ATTEMPT LIMITING
AC-7(4)	USE OF ALTERNATE AUTHENTICATION FACTOR
AC-8	**System Use Notification**
AC-9	**Previous Logon Notification**
AC-9(1)	UNSUCCESSFUL LOGONS
AC-9(2)	SUCCESSFUL AND UNSUCCESSFUL LOGONS
AC-9(3)	NOTIFICATION OF ACCOUNT CHANGES
AC-9(4)	ADDITIONAL LOGON INFORMATION
AC-10	**Concurrent Session Control**
AC-11	**Device Lock**
AC-11(1)	PATTERN-HIDING DISPLAYS
AC-12	**Session Termination**
AC-12(1)	USER-INITIATED LOGOUTS
AC-12(2)	TERMINATION MESSAGE
AC-12(3)	TIMEOUT WARNING MESSAGE
AC-13	Supervision and Review-Access Control
AC-14	**Permitted Actions without Identification or Authentication**
AC-14(1)	NECESSARY USES
AC-15	Automated Marking
AC-16	**Security and Privacy Attributes**

Story (Continued) — Main Takeaways

Key Challenges

Each System is unique and has different security needs

Threats vary greatly from system to system, and their environment (*Example:* Military vs. Manufacturing)

Many security controls exist in a given control catalogue

Not every control can be selected (dependencies, cost)

Story (Continued) — Main Takeaways

Key Challenges

Each System is unique and has different security needs

Threats vary greatly from system to system, and their environment (*Example:* Military vs. Manufacturing)

Many security controls exist in a given control catalogue

Not every control can be selected (dependencies, cost)

There is a human element to control selection!

Proposed Solution

Proposed Solution

To develop an approach that will assist with control selection while accounting for the challenges mentioned above.

To focus on the human-centric nature of this problem.

Proposed Solution

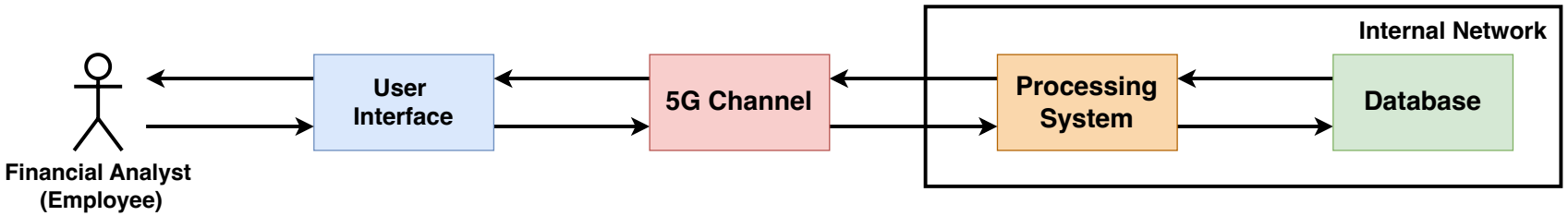
Proposed Solution

To develop an approach that will assist with control selection while accounting for the challenges mentioned above.

To focus on the human-centric nature of this problem.

Game theory is perfect for this!

Illustrative Example – *Firebird*



Step 1: Identify Applicable Atomic Controls

Goal

Identify a list of applicable security controls (*atomic controls*) for a given system from a security control catalogue (common practice).

Required Inputs

Control Catalogue

Mandatory Controls

Threat Model

Step 1: Identify Applicable Atomic Controls – *Firebird*

Required Inputs

Control Catalogue: *ITSG-33*

Mandatory Controls: *SI-10: Input Validation*

Threat Model: **next slide**

Step 1: Identify Applicable Atomic Controls – *Firebird*

Table: Threat model and applicable atomic controls for *Firebird*

Assets	Threats	Security Objectives Violated	Applicable Atomic Controls
User Interface	▪ Commands received from unknown sources	▪ Confidentiality ▪ Integrity	▪ *AC-4: Information Flow Enforcement*
	▪ Improper/malicious commands entered	▪ Confidentiality ▪ Integrity	▪ *SI-10: Input Validation*
	▪ Employee freely accesses and changes features provided in the interface	▪ Confidentiality ▪ Integrity	▪ *AC-3: Access Enforcement* ▪ *AC-6: Least Privilege*
Database	▪ SQL injection from an improper analyst input changes or retrieves data	▪ Confidentiality ▪ Integrity	▪ *AC-4: Information Flow Enforcement* ▪ *SI-10: Input Validation*
	▪ Employee freely inspects data in the database	▪ Confidentiality	▪ *AC-6: Least Privilege*

Step 2: Assign Effectiveness to Atomic Controls

Goal

Assign an effectiveness to each atomic control gathered in **Step 1**.

Required Inputs

Threat Model

Atomic Controls (**Step 1**)

Step 2: Assign Effectiveness to Atomic Controls – *Firebird*

Table: Atomic payoff matrix for *Firebird*

	Database			*User Interface*		
	C	*I*	*A*	*C*	*I*	*A*
SI-10: Input Validation	Medium	Very High	None	Medium	High	None
AC-3: Access Enforcement	None	None	None	Medium	High	None
AC-4: Information Flow Enforcement	Medium	Medium	None	Medium	Low	None
AC-6: Least Privilege	High	None	None	Medium	Low	None

Step 2: Assign Effectiveness to Atomic Controls – *Firebird*

Table: Atomic payoff matrix for *Firebird*

	Database			*User Interface*		
	C	*I*	*A*	*C*	*I*	*A*
SI-10: Input Validation	Medium	Very High	None	Medium	High	None
AC-3: Access Enforcement	None	None	None	Medium	High	None
AC-4: Information Flow Enforcement	Medium	Medium	None	Medium	Low	None
AC-6: Least Privilege	High	None	None	Medium	Low	None

This is not the game matrix!

Step 3: Assign Cost to Atomic Controls

Goal

Assign a cost to each atomic control gathered in **Step 1**.

Required Inputs

Atomic Controls (**Step 1**)

Step 3: Assign Cost to Atomic Controls – *Firebird*

Table: Atomic control costs for *Firebird*

Control	**Cost**
SI-10: Input Validation	5
AC-3: Access Enforcement	6
AC-4: Information Flow Enforcement	4
AC-6: Least Privilege	3

Step 4: Specify and Generate Valid Control Combinations

Goal

Generate all valid security control combinations for the game using an algebraic specification.

Required Inputs

Mandatory controls

Effectiveness of atomic controls (**Step 2**)

Cost of atomic controls (**Step 3**)

Security Control Algebra

Definition

Security Control Algebra – A *security control algebra* is a commutative idempotent semiring $\mathscr{C} \stackrel{\text{def}}{=} (C, \oplus, \odot, 0, 1)$ where each element of the semiring $c \in C$ is a security control family.

C: Set of every possible security control family (possible combinations of controls)

$\oplus$: Operator denoting a choice of two security control families

$\odot$: Operator denoting a composition of two security control families

0: Non-implementable security control combination (one that does not exist). Identity with respect to $\oplus$.

1: Empty security control combination (no controls). Identity with respect to $\odot$.

Step 4: Specify and Generate Valid Control Combinations – *Firebird*

Denoting the security control family as F,

$$F \quad = \quad SI\text{-}10 \odot opt\left[AC\text{-}3, AC\text{-}4, AC\text{-}6\right] \qquad \text{such that} \qquad AC\text{-}3 \xrightarrow{F} AC\text{-}6$$

Step 4: Specify and Generate Valid Control Combinations – *Firebird*

$$
\begin{aligned}
F &= \mathit{SI\text{-}10} \odot \mathit{opt}\left[\mathit{AC\text{-}3}, \mathit{AC\text{-}4}, \mathit{AC\text{-}6}\right] \\
F &= \mathit{SI\text{-}10} \oplus \mathit{SI\text{-}10\ AC\text{-}3} \oplus \mathit{SI\text{-}10\ AC\text{-}4} \oplus \mathit{SI\text{-}10\ AC\text{-}6} \oplus \mathit{SI\text{-}10\ AC\text{-}3\ AC\text{-}4} \oplus \\
&\quad \mathit{SI\text{-}10\ AC\text{-}3\ AC\text{-}6} \oplus \mathit{SI\text{-}10\ AC\text{-}4\ AC\text{-}6} \oplus \mathit{SI\text{-}10\ AC\text{-}3\ AC\text{-}4\ AC\text{-}6}
\end{aligned}
$$

Step 4: Specify and Generate Valid Control Combinations – *Firebird*

Budget = 15

Table: Security control combination costs for *Firebird*

Security Control Combination	**Cost**
SI-10	5
SI-10 AC-4	9
SI-10 AC-6	8
SI-10 AC-3 AC-6	14
SI-10 AC-4 AC-6	12
SI-10 AC-3 AC-4 AC-6	18

***SI-10 AC-3 AC-4* does not respect dependencies, and therefore not present**

Step 5: Construct the Game Matrix

Goal

Generate the game matrix

Required Inputs

Valid control combinations (**Step 4**)

Effectiveness Definition

Definition (Effectiveness of a Security Control Combination)

$$
\begin{aligned}
Eff(1) &= 0 \\
Eff(a) &= E(a) \text{ if } a \text{ is atomic} \\
Eff(a \odot b) &= 1 - (1 - Eff(a))(1 - Eff(b))
\end{aligned}
$$

Step 5: Construct the Game Matrix – *Firebird*

Table: Game matrix for *Firebird*

	Database			*User Interface*		
	C	*I*	*A*	*C*	*I*	*A*
SI-10	0.5	0.9	0.0	0.5	0.8	0.0
SI-10 AC-4	0.75	0.95	0.0	0.75	0.84	0.0
SI-10 AC-6	0.9	0.9	0.0	0.75	0.84	0.0
SI-10 AC-3 AC-6	0.9	0.9	0.0	0.875	0.968	0.0
SI-10 AC-4 AC-6	0.95	0.95	0.0	0.875	0.872	0.0

This is a one-shot zero-sum game!

Step 6: Play the Game

Goal

Play the game based on expected attacker profiles.

Required Inputs

Game matrix (**Step 5**)

Attacker Profiles

Definition (Attacker Profile)

Ordered sets of security objectives expected to be targeted by an attacker.

Step 6: Play the Game – *Firebird*

Attacker Profile: attacker expected to equally target confidentiality of the interface and confidentiality of the database

	Database			*User Interface*		
	C	*I*	*A*	*C*	*I*	*A*
SI-10	0.5	0.9	0.0	0.5	0.8	0.0
SI-10 AC-4	0.75	0.95	0.0	0.75	0.84	0.0
SI-10 AC-6	0.9	0.9	0.0	0.75	0.84	0.0
SI-10 AC-3 AC-6	0.9	0.9	0.0	0.875	0.968	0.0
SI-10 AC-4 AC-6	0.95	0.95	0.0	0.875	0.872	0.0

***SI-10 AC-4 AC-6* is the suggested strategy**

Step 6: Play the Game – *Firebird*

Attacker Profile: attacker expected to target (1) the confidentiality of the interface followed by (2) the integrity of the interface

	Database			*User Interface*		
	C	*I*	*A*	*C*	*I*	*A*
SI-10	0.5	0.9	0.0	0.5	0.8	0.0
SI-10 AC-4	0.75	0.95	0.0	0.75	0.84	0.0
SI-10 AC-6	0.9	0.9	0.0	0.75	0.84	0.0
SI-10 AC-3 AC-6	0.9	0.9	0.0	0.875	0.968	0.0
SI-10 AC-4 AC-6	0.95	0.95	0.0	0.875	0.872	0.0

***SI-10 AC-3 AC-6* is the suggested strategy**

Discussion and Conclusion

Capturing Human Elements in Control Selection

Viewing control selection as a game captures the opposing dynamics of the attacker and analyst.

Reduction of Assumptions

Practical applications of game theory typically require numerous assumptions.

Limitation: Numerous possible Control Combinations

With N optional controls, there are 2^N possible combinations for the game.

Thank You

CyberSEA
Research Lab
Carleton University

Dylan Leveille
dylan.leveille@carleton.ca, jason.jaskolka@carleton.ca

CyberSEA Research Lab
https://carleton.ca/cybersea/
@CyberSEA_Lab