Adapting Cybersecurity Practice to Reduce Wildlife Cybercrime

Timothy C. Haas, Associate Professor (Statistics)

Sheldon B. Lubar College of Business, University of Wisconsin-Milwaukee, haas@uwm.edu, https://sites.uwm.edu/haas/, https://profitablebiodiversity.com

Biodiversity is going away

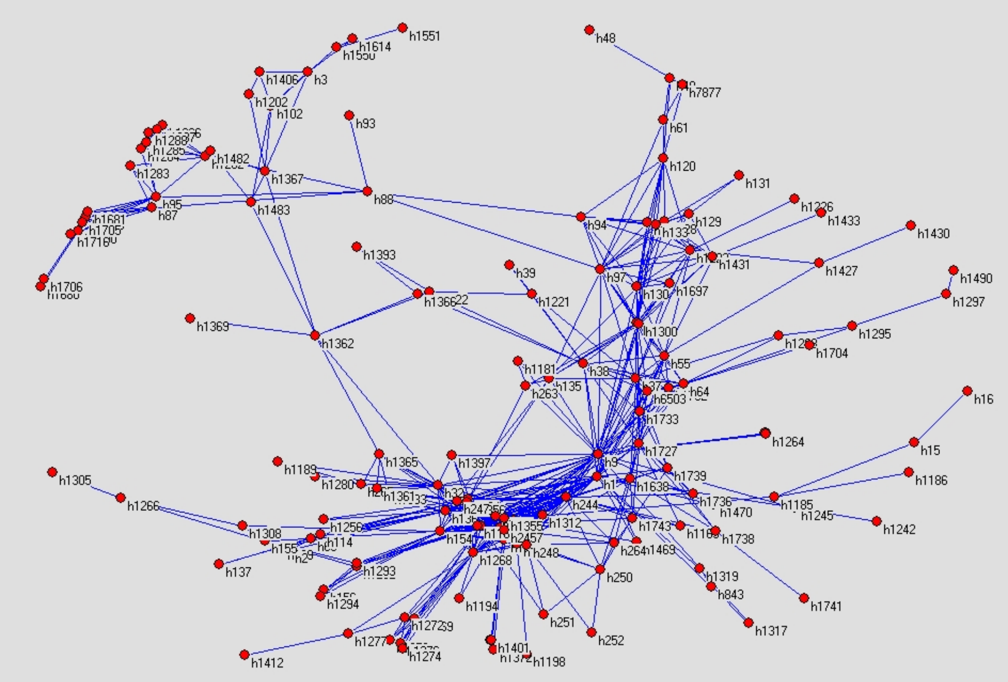
- The sixth mass extinction in the history of the planet is underway.
- Most large, wild mammals, many fish species, and many rare plants will be gone by 2060.

Cycads, sharks, and elephants

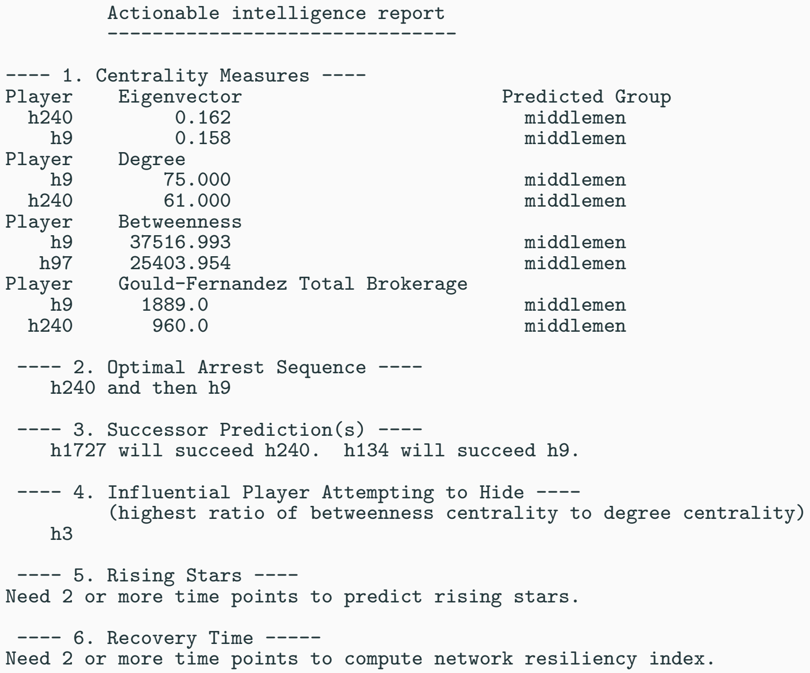
- For instance, the cycad plant, poached as a status symbol and investment, has been on this planet for about 280 million years. Dinosaurs didn't show up until 245 million years ago.
- The great white shark, a particular species of fish is endangered.
- And the African savanna elephant was added to the IUCN Red List in 2021.

What to do

- To curb this non-reversible destruction, the wholesale killing of animals and plants needs to stop, and habitat destruction needs to be curtailed.
- But achieving these two goals will require initiatives that move people away from these behaviors.
- These initiatives need to be derived from credible models of those **political-ecological** systems that host endangered species.



South African rhino poaching network as of December 2014.



```
         Actionable intelligence report
         -------------------------------

---- 1. Centrality Measures ----
Player    Eigenvector                                 Predicted Group
  h240         0.162                                    middlemen
    h9         0.158                                    middlemen
Player    Degree
    h9        75.000                                    middlemen
  h240        61.000                                    middlemen
Player    Betweenness
    h9     37516.993                                    middlemen
   h97     25403.954                                    middlemen
Player    Gould-Fernandez Total Brokerage
    h9      1889.0                                      middlemen
  h240       960.0                                      middlemen

 ---- 2. Optimal Arrest Sequence ----
    h240 and then h9

 ---- 3. Successor Prediction(s) ----
    h1727 will succeed h240.  h134 will succeed h9.

 ---- 4. Influential Player Attempting to Hide ----
         (highest ratio of betweenness centrality to degree centrality)
    h3

 ---- 5. Rising Stars ----
Need 2 or more time points to predict rising stars.

 ---- 6. Recovery Time -----
Need 2 or more time points to compute network resiliency index.
```

An actionable intelligence report.

1. *Detain list*: A list of those players that the confederation recommends law enforcement detain for maximal disruption effect.

2. *Surveil list*: A list of those players the confederation recommends be placed under surveillance for purposes of gathering evidence and/or information on pending wildlife crime activities.

3. *Interdict list:* A list of predicted WTS actions along with where and when these actions will take place. The confederation recommends law enforcement interdict these actions.

4. *Recovery time:* An estimate of how long the WTS will take to recover from the removal of those players in the Detain list. Law enforcement uses this information to plan detention, surveillance, and interdiction operations.

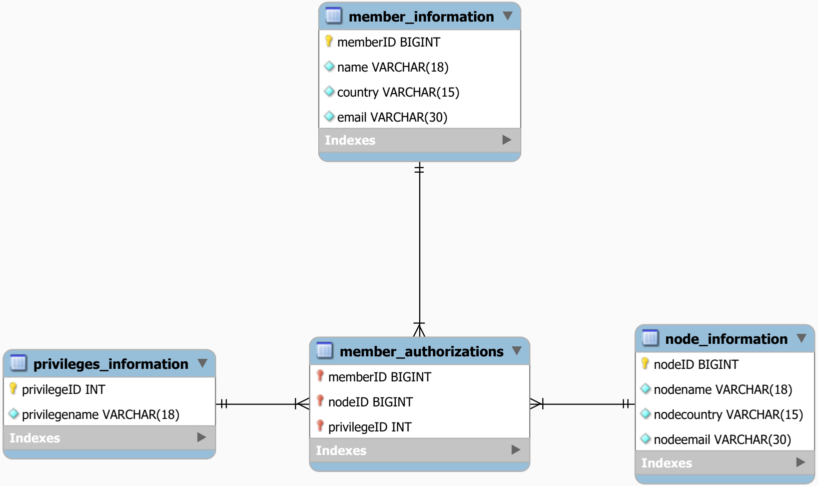
The logistics office has minimal activities.

1. Maintaining communications between all members.
2. Maintaining the *logistics node* of the confederation's database and the GLAD access control tool.
3. Processing membership applications and associated auditor reports.
4. Preparing the budget and billing for for dues.

This is *rule-based management* among peers.

The logistics node holds only administrative data.

1. Member contact information.
2. Each member's corruption index value and information technology (IT) security index value.
3. Contact information for the corruption auditor and the IT security auditor.
4. The confederation's budget.
5. EMT software, including all database software.



member_information

memberID BIGINT

name VARCHAR(18)

country VARCHAR(15)

email VARCHAR(30)

Indexes

privileges_information

privilegeID INT

privilegename VARCHAR(18)

Indexes

member_authorizations

memberID BIGINT

nodeID BIGINT

privilegeID INT

Indexes

node_information

nodeID BIGINT

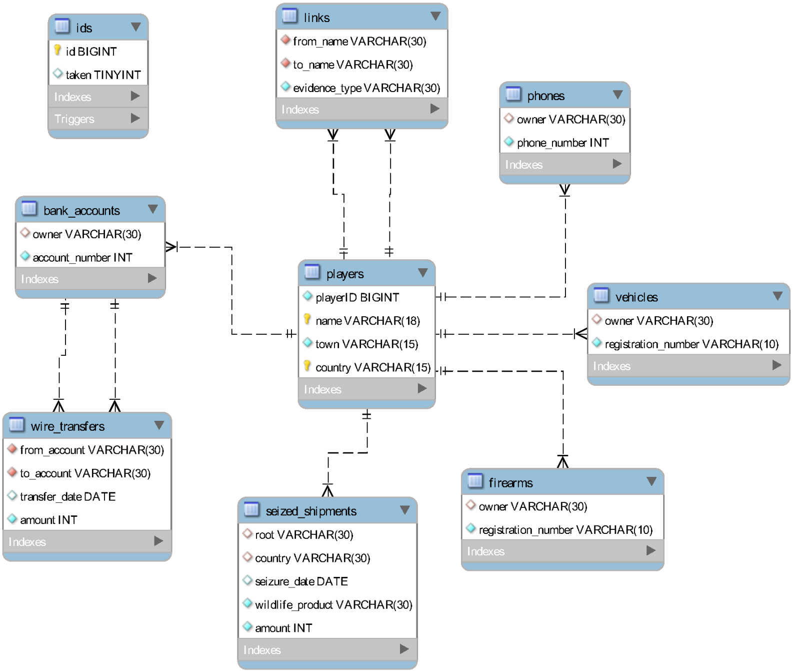
nodename VARCHAR(18)

nodecountry VARCHAR(15)

nodeemail VARCHAR(30)

Indexes

Entity relationship diagram of the logistics node's database. A double bar into an entity indicates a source entity can map to only one entity whereas a trident indicates a source entity can map to many entities.



ids
- id BIGINT
- taken TINYINT
- Indexes
- Triggers

links
- from_name VARCHAR(30)
- to_name VARCHAR(30)
- evidence_type VARCHAR(30)
- Indexes

phones
- owner VARCHAR(30)
- phone_number INT
- Indexes

bank_accounts
- owner VARCHAR(30)
- account_number INT
- Indexes

players
- playerID BIGINT
- name VARCHAR(18)
- town VARCHAR(15)
- country VARCHAR(15)
- Indexes

vehicles
- owner VARCHAR(30)
- registration_number VARCHAR(10)
- Indexes

wire_transfers
- from_account VARCHAR(30)
- to_account VARCHAR(30)
- transfer_date DATE
- amount INT
- Indexes

seized_shipments
- root VARCHAR(30)
- country VARCHAR(30)
- seizure_date DATE
- wildlife_product VARCHAR(30)
- amount INT
- Indexes

firearms
- owner VARCHAR(30)
- registration_number VARCHAR(10)
- Indexes

The GLAD access control tool

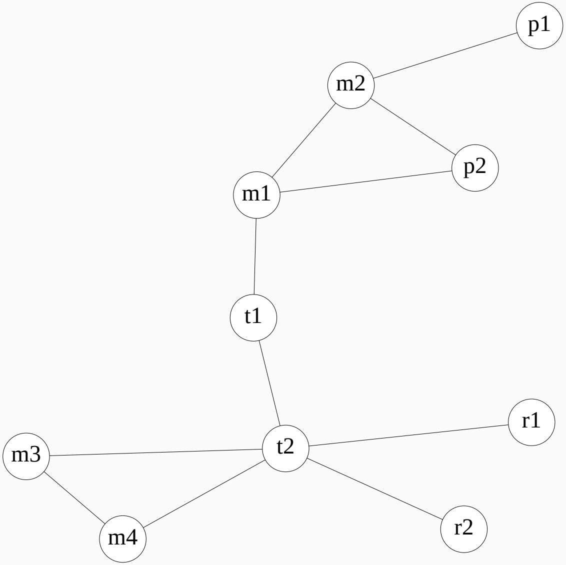
This tool automates the task of deciding who may access what in a federated database and enforces all restrictions imposed by nodes for access to their local databases. The tool consists of three modules: A *local security* module that specifies the local authorization policy of each node; a *global security* module that runs algorithms to combine all exported local authorizations into global ones; and a *dictionary* module that executes operations on nodes as per requests from access-controlled members.

GLAD access control is conservative.

The GLAD access control tool can be configured to implement a *strictly conservative* access authorization strategy that ensures global authorizations derived from exported local authorizations do not result in a member being given global access privileges that exceed the lowest level of privileges given to that member across all nodes.

Script	Purpose
Local Security module	
1. `create_node.sql`	Create a database node.
2. *`required_changes.sql`	Change the privileges of one or more members as dictated by a single node.
Global Security module	
3. `create_logistics.sql`	Create the logistics node database.
4. `update_glad.ps1`	Manage an update of GLAD authorizations.
5. *`compute_glad.sql`	Compute GLAD authorizations.
6. *`update_privileges.sql`	Create an SQL script to update privileges.
7. `global_privileges.sql`	Update a node's GLAD authorizations.
8. *`update_email.ps1`	Send an email to a node directing it to run the attached `global_privileges.sql`.
Dictionary module	
9. `fedquery.ps1`	Run a query against the database.
10. `example_query.sql`	An example query.

*script is executed within `update_glad.ps1`.



A hypothetical WTS. Poacher names begin with “p,” middlemen with “m,” traders with “t,” and retailers with “r.”

Player	Eigenvector	Betweeness	Degree	Betweenness / Degree
t2	0.552	68	5	13.6
m4	0.361	18	2	9.0
m3	0.361	18	2	9.0
t1	0.352	58	2	29.0
m1	0.300	54	3	18.0
m2	0.244	34	3	11.3
r2	0.228	18	1	18.0
r1	0.228	18	1	18.0
p2	0.216	18	2	9.0
r1	0.092	18	1	18.0

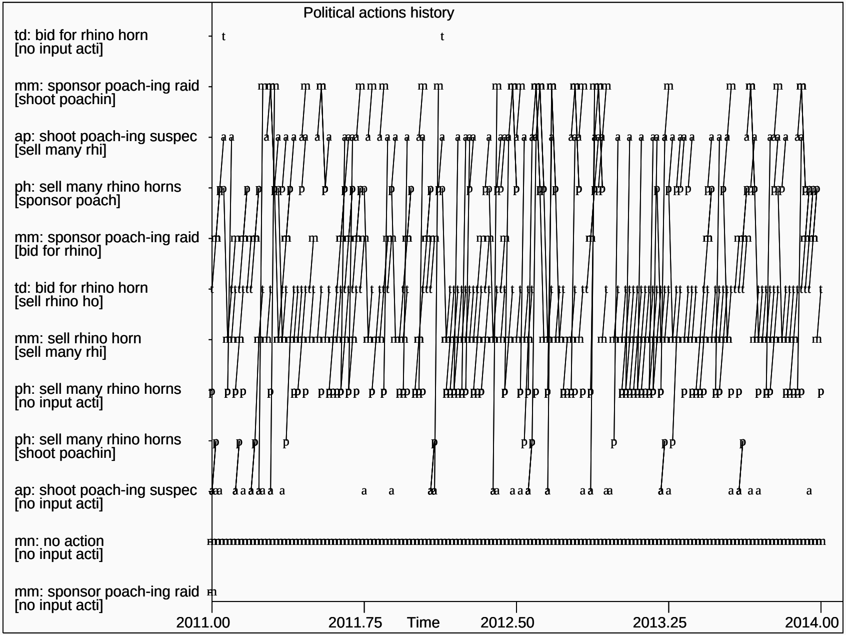
Centrality measures of the actual WTS network.

Internal identifier	Player name	Town	Country	Number of vehicles	Vehicles
h1	r1	A	Y	0	
h2	m3	B	Y	0	
h3	m4	A	Y	0	
h4	r2	A	Y	0	
h5	t2	B	Y	0	
h6	t1	A	Y	1	lu7
h7	p2	D	Z	0	
h8	m1	D	Z	0	
h9	m2	E	Z	0	
h10	p1	D	Z	0	
h11	t11	C	Z	1	lu7

Intelligence gathered on player attributes.

Player 1	Player 2	Interaction type
p1	m2	call
m2	p2	call
m2	m1	shipment
p2	m1	shipment
t1	m1	transfer
t2	t1	call
t2	r2	call
t2	r1	call
t2	m3	call
t2	m4	call
m3	m4	call
t11	m1	call
t11	r1	transfer

Intelligence gathered on player-to-player interactions.



Actions history generated by the fitted simulator.

Access control update dictated by node 2.

```
************** User privileges granted at database creation *********
GRANT SELECT, INSERT, DELETE ON *.* TO ‘Jay Lee‘@‘%‘
GRANT SELECT, INSERT, DELETE ON *.* TO ‘Jeff Lee‘@‘%‘
GRANT SELECT, INSERT, DELETE ON *.* TO ‘John Doe‘@‘%‘

************** update_glad.ps1: Running required_changes.sql ********
delete from member_authorizations where memberID = 51 and nodeID = 2

insert into member_authorizations
   (memberID, nodeID, privilegeID) values (51, 2, 1)

************** update_glad.ps1: Running compute_glad.sql ************
set @nmnodes = (select count(nodeID) from node_information)

delete from member_authorizations where nodeID = 0
```

Access control update continued.

```
create temporary table n (
   memberID bigint unsigned not null default 0,
   privilegeID int unsigned not null default 0,
   nmgivenpriv int unsigned not null default 0,
   nodeID int unsigned not null default 0)

insert into n (memberID, privilegeID, nmgivenpriv)
   select memberID, privilegeID, count(*) as nmgivenpriv
   from member_authorizations
   group by memberID, privilegeID
   having nmgivenpriv = @nmnodes

delete from n where memberID = 0
update n set nodeID = 0
set foreign_key_checks=0
insert into member_authorizations (memberID, nodeID, privilegeID)
   select memberID, nodeID, privilegeID from n
```

Updated authorizations for confederation members.

```
select * from member_authorizations

1    0   1
1    1   1
1    2   1
9    0   1
9    1   1
9    2   1
51   0   1
51   1   1
51   2   1
1    0   2
1    1   2
1    2   2
51   1   2
```

SQL script emailed to every node.

```
************** update_glad.ps1: Running update_privileges.sql *******
************** global_privileges.sql ********************************
grant select  on *.* to ’Jay Lee’;
revoke all on *.* from ’Jay Lee’;

grant select  on *.* to ’Jeff Lee’;
revoke all on *.* from ’Jeff Lee’;

grant select  on *.* to ’John Doe’;
revoke all on *.* from ’John Doe’;
flush privileges;

grant select on *.* to ’John Doe’;
show grants for ’John Doe’;
GRANT SELECT ON *.* TO ‘John Doe‘@‘%‘;

grant select on *.* to ’Jeff Lee’;
show grants for ’Jeff Lee’;
GRANT SELECT ON *.* TO ‘Jeff Lee‘@‘%‘;

grant select on *.* to ’Jay Lee’;
show grants for ’Jay Lee’;
GRANT SELECT ON *.* TO ‘Jay Lee‘@‘%‘;
grant insert on *.* to ’Jay Lee’;
show grants for ’Jay Lee’;
GRANT SELECT, INSERT ON *.* TO ‘Jay Lee‘@‘%‘;
flush privileges;

************** update_glad.ps1: Running update_email.ps1 ************
(output not shown)
```

Trace of the query attempted by the untrusted member.

```
******** example_query.sql: run on node #2 *************
use node2;
insert into phones (owner, phone_number)
   values('m3', 123456789);

******** example_query.sql: output *********************
ERROR 1142 (42000) at line 8: INSERT command denied to user
'John Doe'@'localhost' for table 'phones'
```

Actionable intelligence report.

```
            ACTIONABLE INTELLIGENCE REPORT

---------- Social Network Analysis Metrics -------------
 Player  Eigenvector  Degree       Predicted
         Centrality   Centrality   Level
    t2        00.552       5.000     3
    m4        00.361       2.000     2
    m3        00.361       2.000     2
    t1        00.352       2.000     3
    m1        00.300       3.000     2
    m2        00.244       3.000     2
    r2        00.228       1.000     4
    r1        00.228       1.000     4
    p2        00.216       2.000     1
    p1        00.092       1.000     1

           Betweenness  Between/Degree
    t2        68.000       13.600     3
    t1        58.000       29.000     3
    m1        54.000       18.000     2
    m2        34.000       11.333     2
    m4        18.000        9.000     2
    p2        18.000        9.000     1
    m3        18.000        9.000     2
    r2        18.000       18.000     4
    p1        18.000       18.000     1
    r1        18.000       18.000     4
```

Actionable intelligence report, continued.

```
           Gould-Fernandez
           total brokerage
    t2          9.0        3
    m1          2.0        2
    m2          2.0        2
    t1          1.0        3
    m4          0.0        2
    p2          0.0        1
    m3          0.0        2
    r2          0.0        4
    p1          0.0        1
    r1          0.0        4

 ------------------ Detain list ------------------
SNA sublist.
Optimal Arrest Sequence:
t2 is the first player to arrest and t1 is the second player to arrest.

Ecosystem effects sublist.
players t1, p2, m1
```

Actionable intelligence report, continued.

```
-------------------- Surveil list ---------------------
Successor Prediction(s):
r2 will succeed t2.
m1 will succeed t1

Influential Player Attempting to Hide (highest ratio of betweenness
centrality to degree centrality): t1

Rising Stars:
   Need 2 or more time points to predict rising stars.

Community Structure.
Number of algorithm iterations: 2
Number of communities: 2

 Player    Community
    r1         5
    m3         5
    m4         5
    r2         5
    t2         5
    t1         5
    p2         8
    m1         8
    m2         8
    p1         8
```

Actionable intelligence report, continued.

```
----------------- Interdict list -------------------
January 2016: m3 will sell rhino horns in town B, country Y

------ Network Resiliency Index (Recovery time) ---------
Current network's connectivity index value:   2.592
   Need 2 or more time points to compute network resiliency
   index.
```

Thank you! Questions?