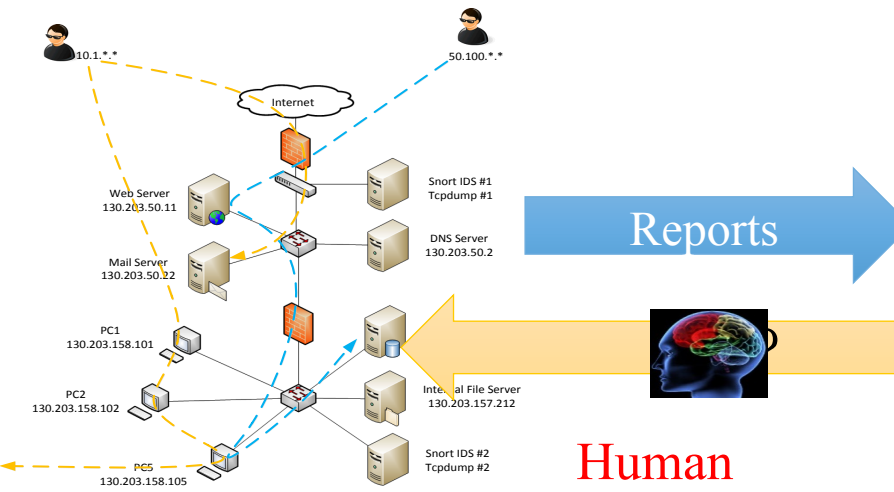


# An Integrated Cognitive Task Analysis Method for Tracing Human Analysts' Cyber Security Analysis Processes

Chen Zhong, John Yen, Peng Liu,  
Pennsylvania State University

Rob Erbacher, Renee Etoty, Christopher Garneau  
Army Research Lab

# Cyber Security Analysis: Defense Technologies + Human Analysts



Reports



Human Analysts

Defense Technologies



No.	Time	Source	Action	Protocol	Source IP	Destination IP	src port	dst port	Size
286	4.431618	00:ac:2f:67:3d:ee							
287	4.455532	00:ac:2f:67:3d:ee							
288	4.520443	192.168.2.14							
289	4.520933	192.168.3.2							
290	4.521082	192.168.2.14							
291	4.536957	CoregaKX_51:51:82							
292	4.545681	27.121.46.57			130.158.6.109	130.158.6.109	TCP	66 18524 > 80	[SYN, ACK] Seq=1609850756 Len=0 MSS=1460 WS=2
293	4.556308	130.158.6.109			27.121.46.57	130.158.6.109	TCP	66 80 > 18524	[SYN, ACK] Seq=1023111223 Ack=1609850757 Win=8192 Len=0 MSS=1460
294	4.556331	27.121.46.57			130.158.6.109	130.158.6.109	TCP	54 18524 > 80	[ACK] Seq=1609850757 Ack=1023111226 Win=16425 Len=0
295	4.558064	111.67.226.84			192.168.2.14	192.168.2.14	TCP	60 80 > 59424	[SYN, ACK] Seq=2432907758 Ack=183620120 Win=5840 Len=0 MSS=1440
296	4.553199	192.168.2.14							
297	4.553199	192.168.2.14							
298	4.584518	130.158.6.109							
299	4.584522	130.158.6.109							

What are the "true signals"?

How are they connected?

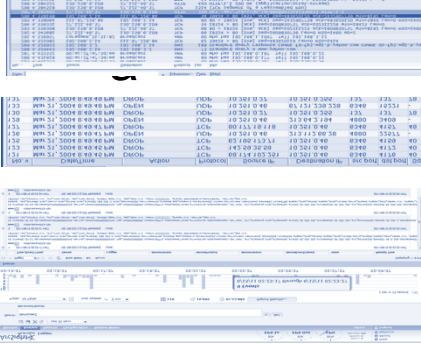
No.	v	Date/Time	Action	Protocol	Source IP	Destination IP	src port	dst port	Size
121		Mar 21, 2004 8:49:45 PM	DROP	TCP	68.174.102.251	10.251.0.46	6346	4176	40
123		Mar 21, 2004 8:49:45 PM	DROP	TCP	142.59.35.58	10.251.0.46	6346	4172	40
125		Mar 21, 2004 8:49:46 PM							
126		Mar 21, 2004 8:49:47 PM							
127		Mar 21, 2004 8:49:47 PM							
128		Mar 21, 2004 8:49:48 PM							
133		Mar 21, 2004 8:49:48 PM	OPEN	UDP	10.251.0.46	67.121.239.228	6346	15221	-
137		Mar 21, 2004 8:49:49 PM	DROP	UDP	10.251.0.27	10.251.0.255	137	137	78

What's the story of the attack?

How did it happen and what's next?



# Cyber Security Analysis: A Complex Cognitive Process

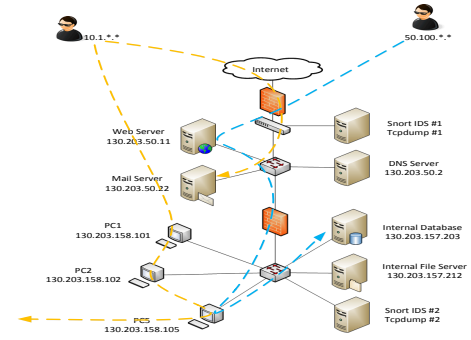


Time	Src IP	Src Port	Dest IP	Dest Port	Protocol	Length	Flags	Window	Seq	Win	Options	Info
17.21	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.22	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.23	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.24	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.25	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.26	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.27	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.28	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.29	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.30	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.31	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.32	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.33	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.34	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.35	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.36	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.37	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.38	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.39	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.40	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.41	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.42	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.43	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.44	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.45	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.46	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.47	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.48	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.49	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...
17.50	192.168.1.100	4880	192.168.1.1	80	TCP	60	...	...	...	...	...	...

Network Monitoring Data



## Analytical Reasoning Process



Cyber Attacks



How did you make it?

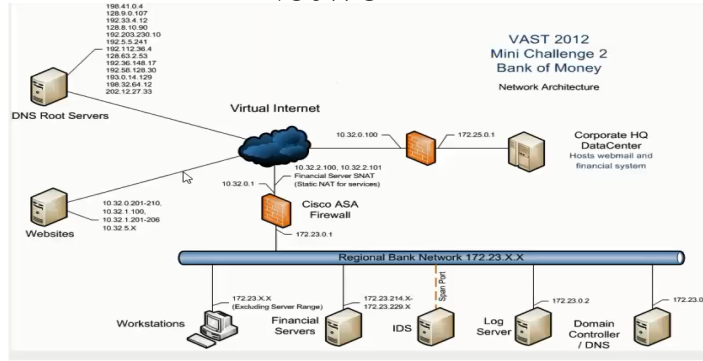
I took the data and conducted reasoning based on my experience and domain knowledge.

# An Example of Cyber Security Analysis

## Network



Alice



## Intrusion Detection System (IDS) Alerts

DateTime	SourceIP	DestIP	Category	Priority	Description
4/5/2012 10:15:00 PM	172.23.0.246	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.246	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPCS unicode
4/5/2012 10:15:00 PM	10.32.5.54	172.23.233.150	Misc activity	3	[1:2000355:5] ET POLICY IRC authorization messag
4/5/2012 10:15:00 PM	10.32.5.58	172.23.233.33	Misc activity	3	[1:2000355:5] ET POLICY IRC authorization messag
4/5/2012 10:15:00 PM	10.32.5.56	172.23.233.9	Misc activity	3	[1:2000355:5] ET POLICY IRC authorization messag
4/5/2012 10:15:00 PM	172.23.0.227	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.227	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPCS unicode
4/5/2012 10:15:00 PM	172.23.0.236	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.236	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPCS unicode
4/5/2012 10:15:00 PM	172.23.0.215	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.215	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPCS unicode
4/5/2012 10:15:00 PM	172.23.0.229	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.229	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPCS unicode
4/5/2012 10:15:00 PM	172.23.0.216	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.216	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPCS unicode
4/5/2012 10:15:00 PM	172.23.0.219	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.249	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.249	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPCS unicode
4/5/2012 10:15:00 PM	172.23.0.245	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.245	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPCS unicode
4/5/2012 10:15:00 PM	172.23.0.239	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.239	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPCS unicode
4/5/2012 10:15:00 PM	172.23.0.233	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.233	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPCS unicode

## Firewall logs

DateTime	Priority	Operation	Protocol	SrcIP	DestIP	SrcPort	DesPort	DestService	Direction
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.240.152	10.32.5.56	5203	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.235.50	10.32.5.52	2316	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.238.127	10.32.5.54	3330	6667	6667_tcp	(empty)
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.238.124	10.32.5.54	3329	6667	6667_tcp	(empty)
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.238.121	10.32.5.59	3306	6667	6667_tcp	(empty)
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.238.78	10.32.5.52	3336	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.51	10.32.5.51	6637	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.50	10.32.5.57	6638	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.56	10.32.5.58	6639	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.233.50	10.32.5.57	6638	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.233.56	10.32.5.58	6639	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.58	10.32.5.51	6640	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.52	10.32.5.59	6641	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.233.58	10.32.5.51	6640	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.233.52	10.32.5.59	6641	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.57	10.32.5.58	6642	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.233.57	10.32.5.58	6642	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.54	10.32.5.57	6643	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.53	10.32.5.52	6644	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.233.53	10.32.5.52	6644	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.233.54	10.32.5.57	6643	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Deny	TCP	172.23.233.54	10.32.5.57	6643	6667	6667_tcp	(empty)

# Alice started with browsing the IDS alerts.

DataTime	SourceIP	DestIP	Category	Priority	Description
4/5/2012 10:15:00 PM	172.23.0.246	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.246	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode
4/5/2012 10:15:00 PM	10.32.5.54	172.23.233.150	Misc activity	3	[1:2000355:5] ET POLICY IRC authorization messag
4/5/2012 10:15:00 PM	10.32.5.58	172.23.233.33	Misc activity	3	[1:2000355:5] ET POLICY IRC authorization messag
4/5/2012 10:15:00 PM	10.32.5.56	172.23.233.9	Misc activity	3	[1:2000355:5] ET POLICY IRC authorization messag
4/5/2012 10:15:00 PM	172.23.0.227	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.227	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode
4/5/2012 10:15:00 PM	172.23.0.236	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.236	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode
4/5/2012 10:15:00 PM	172.23.0.215	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.215	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode
4/5/2012 10:15:00 PM	172.23.0.229	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.229	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode
4/5/2012 10:15:00 PM	172.23.0.216	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.216	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode
4/5/2012 10:15:00 PM	172.23.0.219	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.249	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.249	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode
4/5/2012 10:15:00 PM	172.23.0.245	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.245	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode
4/5/2012 10:15:00 PM	172.23.0.239	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.239	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode
4/5/2012 10:15:00 PM	172.23.0.233	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.233	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode

She noticed a sequence of alerts which reports connections via port 6667.

	Priority	Description	SourcePort	DestPort
icol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setup NTLMSSP unicode asn1 overflow attempt	1912	445
icol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode share access	1912	445
	3	[1:2000355:5] ET POLICY IRC authorization message	6667	6650
	3	[1:2000355:5] ET POLICY IRC authorization message	6667	6651
	3	[1:2000355:5] ET POLICY IRC authorization message	6667	6657
icol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setup NTLMSSP unicode asn1 overflow attempt	3420	445
icol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode share access	3420	445
icol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setup NTLMSSP unicode asn1 overflow attempt	3504	445
icol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode share access	3504	445
icol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setup NTLMSSP unicode asn1 overflow attempt	3444	445
icol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode share access	3444	445
icol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setup NTLMSSP unicode asn1 overflow attempt	3484	445
icol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode share access	3484	445
icol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setup NTLMSSP unicode asn1 overflow attempt	3471	445
icol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC\$ unicode share access	3471	445



She knew that this port is used for IRC (Internet Relay Chat) connections and IRC connections could be used for malicious purpose.

So she generated a **hypothesis** about an attack event: malicious communications are going through this port (true alert).

To investigate the hypothesis, she decided to check the detailed information about these connections in firewall logs.

DataTime	Priority	Operation	Protocol	SrcIP	DesIP	SrcPort	DesPort	DestService	Direction
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.240.152	10.32.5.56	5203	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.235.50	10.32.5.52	2316	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.238.127	10.32.5.54	3330	6667	6667_tcp	(empty)
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.238.124	10.32.5.54	3329	6667	6667_tcp	(empty)
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.238.121	10.32.5.59	3306	6667	6667_tcp	(empty)
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.238.78	10.32.5.52	3336	6667	6667_tcp	(empty)
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.51	10.32.5.51	6637	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.50	10.32.5.57	6638	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.56	10.32.5.58	6639	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.233.50	10.32.5.57	6638	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.233.56	10.32.5.58	6639	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.58	10.32.5.51	6640	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Built	TCP	172.23.233.52	10.32.5.59	6641	6667	6667_tcp	outbound
4/5/2012 10:15:00 PM	Info	Teardown	TCP	172.23.233.58	10.32.5.51	6640	6667	6667_tcp	outbound

It indicates that such connections are between internal workstations and external web servers.

**Policy Violated!**



Strengthen previous hypothesis (i.e. malicious IRC connections).

# Motivation: The Potential Benefits of Understanding the Analysis Process

## **Decision Maker:**

Assess how  
valid and  
reliable the  
conclusion is.

## **Analyst:**

Reflect and  
improve.

## **Analyst/ Instructor:**

Extract  
knowledge  
and  
experience.

## **Instructor/ Program Manager:**

Training

## **Technology Provider:**

Identify  
analysts' need  
and improve  
tools.



# Cognitive Task Analysis (CTA)

**Cognitive Task Analysis (CTA)** is a family of methods that help researchers understand the human's cognitive activities in performing tasks.

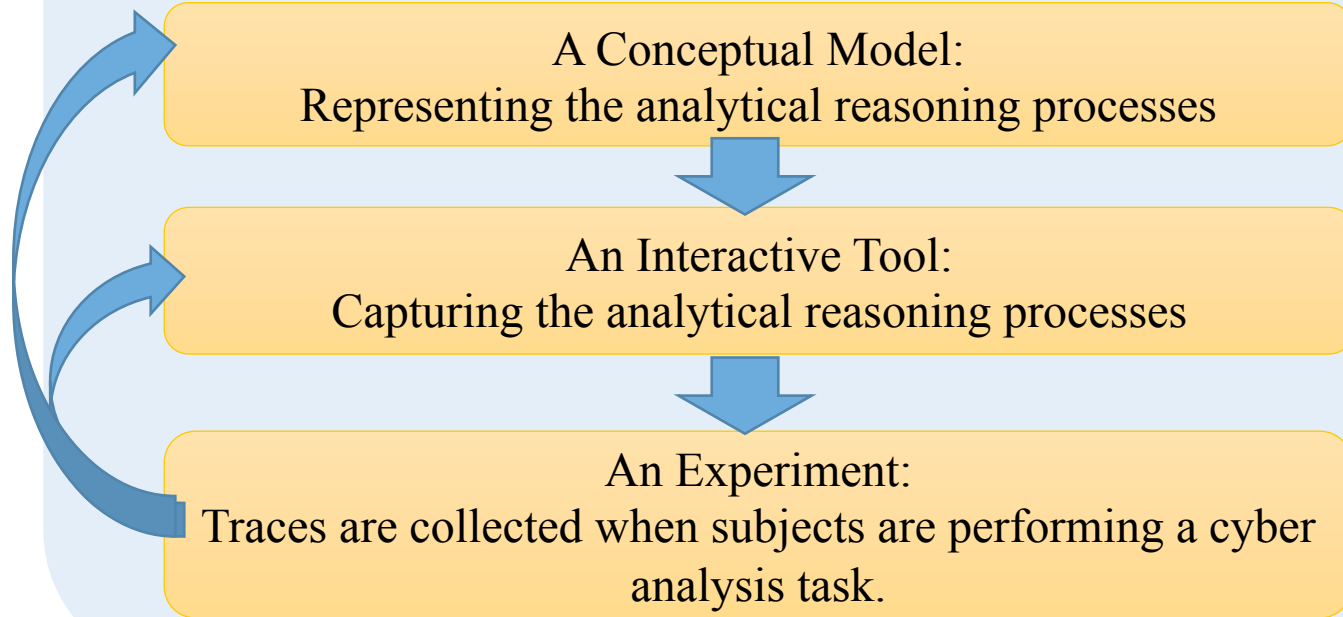
## Related Work: Existing CTAs in this Domain



- Resource-intensive, hard for researcher/administrator to replicate.
- Growing need for studying the analysts' analysis process

# Our Method for Capturing Analysts' Cognitive Processes

## An Integrated Computer-Aided Cognitive Task Analysis Data Collection Method



# Part 1: What to Capture

## An Integrated Computer-Aided Cognitive Task Analysis Data Collection Method

A Conceptual Model:  
Representing the analytical reasoning  
processes



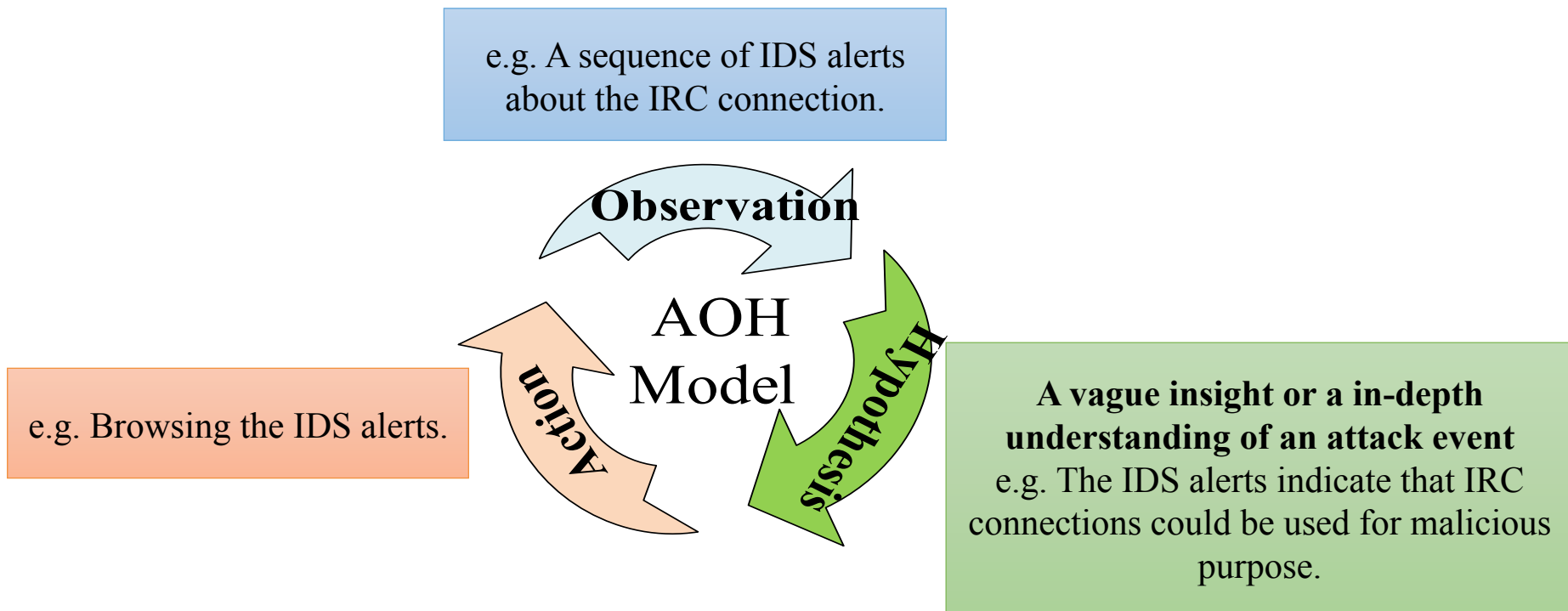
An Interactive Tool:  
Capturing the analytical reasoning processes



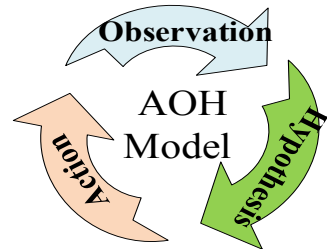
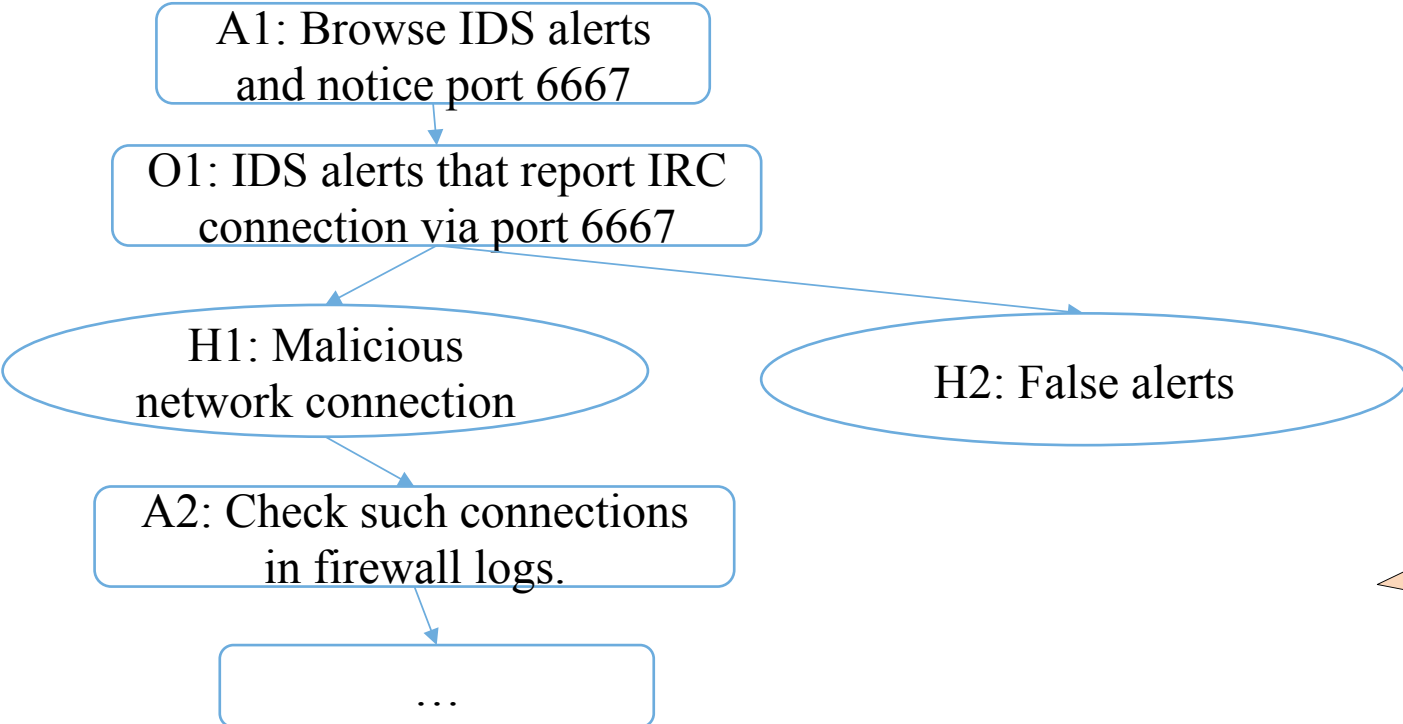
An Experiment:  
Traces are collected when subjects are performing a cyber  
analysis task.

- Critical Elements in Analysts' Analysis Processes
  - **A: Actions** in data exploration
  - **O: Observations** of evidence
  - **H: Hypothesis** about the attack events

# The AOH Conceptual Model: Main Elements



# The AOH Conceptual Model: Relationships Between the Objects of A, O and H



# Cyber Security Analysis: Creating and Linking Actions, Observations and Hypotheses

Operation	Description
BROWSE	$BROWSE(D_i), D_i \subseteq \cup DS_i^*$ : Browse the data sources.
FILTER	$FILTER(DS_i, Cond.)$ : Filter the source data $DS_i$ based on condition $Cond.$
SEARCH	$SEARCH(D_i, K), D_i \subseteq \cup DS_i$ : Search $K$ in data $D_i$ .
INQUIRE	$INQUIRE(T_m)$ : Inquire about a term $T_m$
SELECT	$SELECT(D_i), D_i \subseteq \cup DS_i$ : Select the data of interest in $D_i$ .
SELECTED *	*(Come in pairs with SELECT) $SELECTED(D_i), D_i \subseteq \cup DS_i$ : The selected data of interest
LINK	$LINK(D_i, L), D_i \subseteq \cup DS_i$ : The links $L$ among the selected data $D_i$ (e.g. common features in $D_i$ )
NEW_HYP O	$NEW(h, O)$ : Generate a <i>hypothesis</i> $h$ in the context of <i>observation</i> $O$ .
MODIFY	$MODIFY(h, v_1, v_2)$ : Modify the content of an hypothesis $h$ from $v_1$ to $v_2$
SWITCH CONTEXT	$SWITCH\_CONTEXT(h_1, h_2)$ : Change current focus of attention from <i>hypothesis</i> $h_1$ to <i>hypothesis</i> $h_2$ .
CONFIRM/ DENY	$CONFIRM\_DENY(h_1, Y/N)$ : Confirm or deny an <i>hypothesis</i> $h_1$ .

# Trace: Representation of the Analysis Process

Definition 1: A cognitive trace  $\mathcal{Tr}$  is a sequence of items  $p_1, \dots, p_n, \forall p_i, 1 \leq i \leq n, p_i$  is a tuple  $(t_i, op_i(I, C_i))$ , where  $t_i$  is the timestamp,  $op_i(I, C_i)$  is an operation on a cognitive activity  $I$  under the context  $C_i$ .  $I$  is an action, observation or hypothesis,  $C_i$  is a set of connections between  $I$  with the existing actions, observations and hypotheses.

Timestamp	Operation
t1	<b>FILTER</b> (Firewall logs, Port = 6667)
t2	<b>SELECT</b> (Log entries with Port 6667)
t3	<b>NEW_HYPO</b> (IRC communication)
t4	...



## Part 2: A Tool (ARSCA) for CTA Data Collection

### **An Integrated Computer-Aided Cognitive Task Analysis Data Collection Method**

A Conceptual Model:  
Representing the analytical reasoning processes



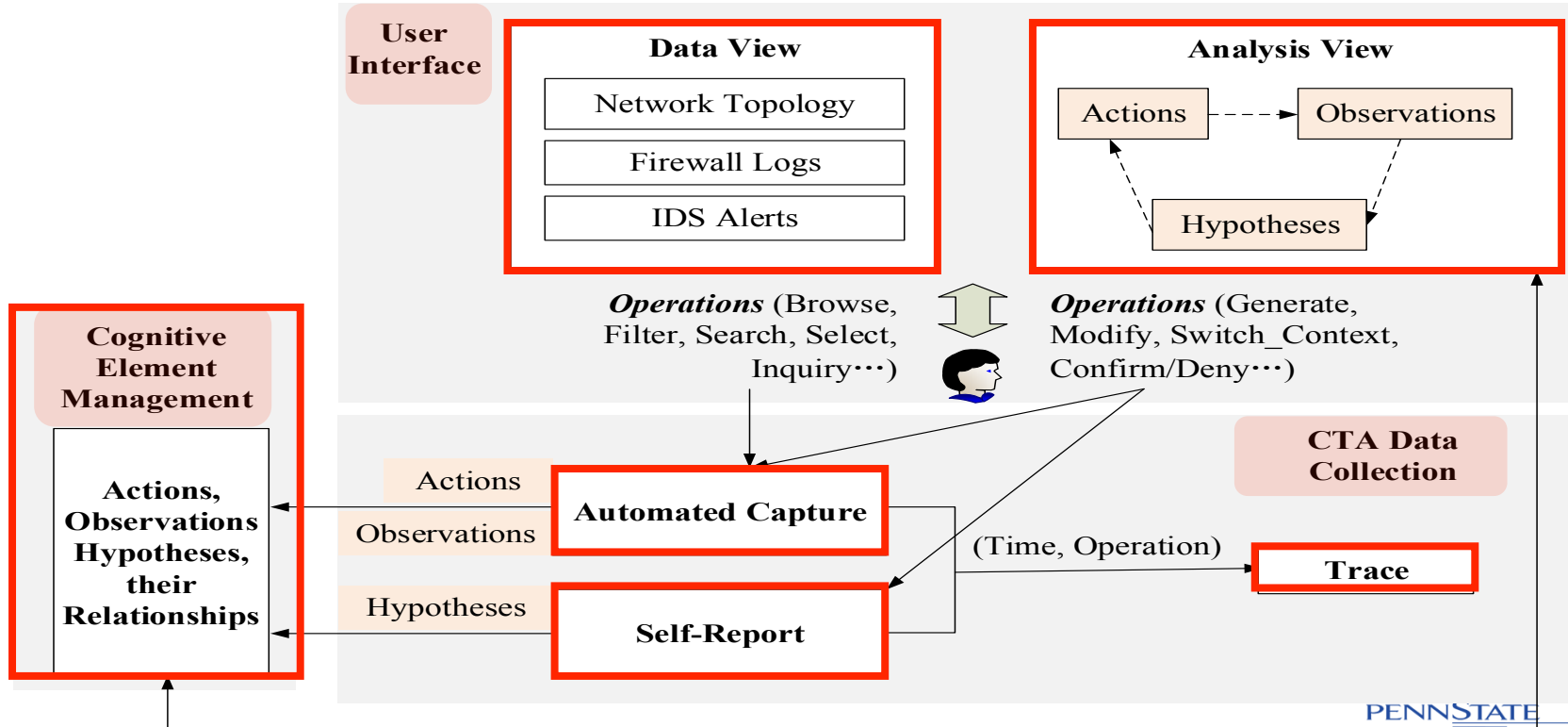
**An Interactive Tool:**  
Capturing the analytical reasoning  
processes



An Experiment:  
Traces are collected when subjects are performing a cyber  
analysis task.

- Reduce interruption and alleviate the privacy concern
- Capturing in an efficient way

# ARSCA Architecture



# How an Analyst Works with ARSCA? (Video)

ARSCA-Analytical Reasoning Support for Cyber Analysis

Gather observation... Write down new thought(hypothesis) View ongoing observation buffer Help

Quick Find: Data Filter: Look up a port: Term explanation:

Monitoring Data Analysis

Network Topology IDS Alert (Raw) Firewall Logs (Raw)

Network description

- This Bank of Money regional office has been configured with approximately 4000 workstations and approximately 1000 servers. The office operates 24 hours a day.
- Some of the financial transactions are performed on financial servers inside the regional bank office's network. Other financial transactions travel to the corporate headquarters datacenter.
- The Bank of Money regional office uses web-based mail which is housed in the corporate headquarters datacenter.
- Nodes outside the range 172.x.x.x should be considered external to the Bank of Money network.
- 172.23.X.X, "X" can represent any number from 0-255.
- 10.32.0.201-210 indicates that the IP will be one of a range from 10.32.0.201 through 10.32.0.210.

Use Policy

- 1) The Bank of Money computer network is to be used for business use only. Personal use of company computing resources is prohibited. Staff members may not use their company computers to access personal email, visit social networking or auction sites, or conduct personal banking activity
- 2) Employees cannot connect to the Bank of Money intranet from home or other remote locations. All remote access to the Bank of Money intranet is blocked, including FTP, telnet, remote login, and remote desktop connections.

VAST 2012 Mini Challenge 2 Bank of Money Network Architecture

DNS Root Servers

- 198.41.0.4
- 128.9.0.107
- 192.33.4.52
- 128.8.10.90
- 192.203.230.10
- 192.5.5.241
- 192.112.36.4
- 128.63.2.53
- 192.36.148.17
- 192.56.120.30
- 193.0.14.120
- 198.32.64.12
- 202.12.27.33

Virtual Internet

Corporate HQ DataCenter  
Hosts webmail and financial system

Cisco ASA Firewall

Regional Bank Network 172.23.X.X

Workstations

Financial Servers

IDS

Log Server

Domain Controller / DNS

Websites

- 10.32.0.201-210
- 10.32.1.190
- 10.32.1.201-206
- 10.32.5.X

Financial Server SNAT (Static NAT for servers)

10.32.2.100: 10.32.2.101

10.32.0.1

172.23.0.1

172.23.0.1

172.23.0.2

172.23.0.10

Open Port

# ARSCA Output: Trace

```
23 <Item Timestamp="07/31 13:01:41">
24 FILTER (
25 | SELECT * FROM Task2IDS WHERE SourcePort = '6667',
26 Task2IDS
27 )
28 </Item>
29
30 <Item Timestamp="07/31 13:01:46">,
31 SELECT (
32 A[1:2000355:5]-[10.32.5.54]-[172.23.232.252],
33 A[1:2000355:5]-[10.32.5.56]-[172.23.233.59],
34 A[1:2000355:5]-[10.32.5.54]-[172.23.238.124],
35 ...)
36 </Item>
37
38 <Item Timestamp="07/31 13:02:01">
39 LINK (
40 Same Sourc Port and IDS alert
41 )
42 </Item>
43
44 <Item Timestamp="07/31 13:04:06">
45 NEW (
46 H46131157 The network is not secure,
47 H67531068 IDS IRC Alerts are true: The IDS alerts are showing IRC authorization alerts over tcp/6667.
This is the default IRC communication port, and this communication is between the workstation IPs and
external resources.
48
49 In this situation this could indicate that there has been a policy violating because IRC communication
on this network isn't allowed. Or this could also be an indicator of compromise because malware can
leverage IRC for Command to Control (C2) communication.
50 )
51 </Item>
```

**FILTER:** Filter the IDS alerts

**SELECT:** Select a set of entries as an observation

**LINK:** The selected entries have common source port and alerts

**NEW\_HYPO:** create a hypothesis based on the above observation.

# Integration of Automated Tracing and Self-Reports

## Tracking Actions (A)

Automated Capture

## Tracking Observations (O)

Automated Capture

### Automated tracing

- + Efficient
- + Not interruptive
- No comments from subjects, hard to analyze the captured data

## Management of As, Os and Hs

- Automatically maintain the relationships between A, O, H
  - Facilitate reflection

## Tracking Hypotheses (H)

Self-reports

### Self-reports

- + Information confirmed by the subjects.
- Depends on the subjects' willingness.
- Distraction

## Part 3: Experiment for CTA Data Collection

### **An Integrated Computer-Aided Cognitive Task Analysis Data Collection Method**

A Conceptual Model:  
Representing the analytical reasoning processes



An Interactive Tool:  
Capturing the analytical reasoning processes



Lab Experiment:  
Traces are collected when subjects are  
performing a cyber analysis task.

- Evaluate the method
- Traces can be used for studying the analysis processes

# Overview of the Lab Experiment

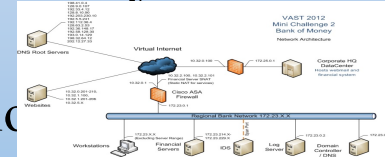
## 30 Participants

- 13 professional analysts
- 17 doctoral students

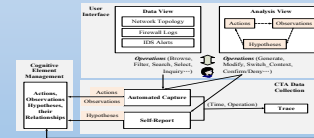


## Simulated Cyber Security Analysis Task

- 2 Network Data Sources
- Multi-step Attack Scenario



## Process Tracing Tool (ARSCA)



ARSCA collected the **Traces** of the participants' cognitive processes.

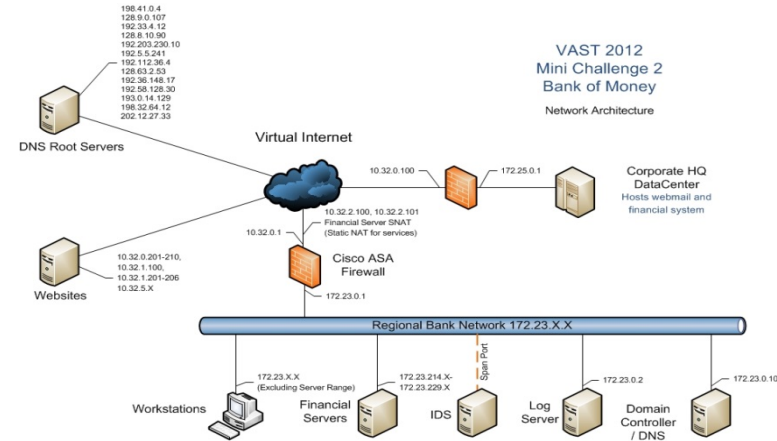
Post-task questionnaires collected **Feedbacks**.

# Experiment Design: Task Design

- Requirements:
  - Reasonable complexity for the analysts
  - Close to the real-world data
    - Volume and Complexity of the monitoring data sets
  - Moderate workload so that analysts can finish the task in the experiment.

## Tailored from VAST 2012 Challenge

- A 10-minute time window (in the original 40-hour attack scenario)
- Contain 3 main attack events
  - IRC communications,
  - Denied FTP connections for data stealing
  - Successful SSH connections for data stealing
- 239 IDS alerts and 115,524 firewall logs.





# Experiment Design: Procedure

- **Pre-task Questionnaire (5 min)**

- Demographic factors
- Domain knowledge and expertise of cyber security analysis
- Familiarity with VAST Challenge 2012
- Current mental and physical status

- **Tutorial (20 min)**

- Introduce the tool features.
- **Analysts need to pass a quiz before going to the next step.**

- **Conducting the task (At most 60 min)**

- At the beginning, we just introduce the task and background information.
- **We didn't provide any instruction to intentionally ask analysts to self report.**

- **Post-task Questionnaire (15 min)**

- Open-ended questions
- Close-ended rating questions using a 5-point Likert scale

The effect of analysts' proficiency with the tool on their task performance

To ensure self-motivated behavior.

## Evaluate the Method from Four Aspects

- Q1: Whether the method can help us successfully conduct CTA data collection in the cyber security domain?
- Q2: Whether the collected data (traces) contain the key elements in analysts' analysis processes?
- Q3: Whether the analysts' analysis process can be recovered from the captured data (traces)?
- Q4: Whether the analysts' analysis processes recovered from the traces are close to the original ones?

## Evaluate the Method from Four Aspects

- Q1: Whether the method can help us successfully conduct CTA data collection in the cyber security domain?
- Q2: Whether the collected data (traces) contain the key elements in analysts' analysis processes?
- Q3: Whether the analysts' analysis process can be recovered from the captured data (traces)?
- Q4: Whether the analysts' analysis processes recovered from the traces are close to the original ones?

# Participants' Feedbacks

- (1) **TASK\_CMP**: “The task is of reasonable *complexity* regarding the analysis activities it involves (e.g. data exploration, thinking reasoning, making decisions).”
- (2) **SET\_CFT**: “I felt *comfortable* with the provided software, and my *performance* is not hindered by it.”
- (3) **EXP\_RFL**: “My *capability/expertise* of cyber analysis is fully leveraged and is reflected in accomplishing the task.”
- (4) **CONC**: “I’m fully *concentrated* in accomplishing the task.”

Likert Scale Response*	Post-task Questions				Total	
	TASK_CMP	SET_CFT	EXP_RFL	CONC		
Disagree	1	0 (0,0)	1 (1,0)	0 (0,0)	0 (0,0)	1
	2	1 (1,0)	3 (1,2)	4 (3,1)	2 (0,2)	10
Neutral	3	9 (5,4)	7 (2,5)	11 (6,5)	4 (2,2)	31
	4	<b>14</b> (9,5)	<b>14</b> (9,5)	<b>13</b> (4,9)	<b>21</b> (12,9)	<b>62</b>
Agree	5	6 (2,4)	5 (0,5)	2 (0,2)	3 (3,0)	16

\* Numbers in brackets refer to *professional analysts* and *doctoral students* respectively.

## Evaluate the Method from Four Aspects



- Q1: Whether the method enables us successfully collect traces in the cyber security domain?
- Q2: Whether the collected data (traces) contain the key elements in analysts' analysis processes?
- Q3: Whether the analysts' analysis process can be recovered from the captured data (traces)?
- Q4: Whether the analysts' analysis processes recovered from the traces are close to the original ones?

## Evaluate the Method from Four Aspects



- Q1: Whether the method enables us successfully collect traces in the cyber security domain?
- Q2: Whether the collected data (traces) contain the key elements in analysts' analysis processes?
- Q3: Whether the analysts' analysis process can be recovered from the captured data (traces)?
- Q4: Whether the analysts' analysis processes recovered from the traces are close to the original ones?

## Q2: Whether the collected data (traces) contain the key elements in analysts' analysis processes?

### Open-ended Questions in Post-task Questionnaire:

- (1) **IMP\_OBS**: *“Reflecting back, what are the **3 most important evidences** that you observed in the data that contributed to your conclusion?”*
- (2) **FD\_OBS**: *“Please explain how you find the above evidences.”*
- (3) **IMP\_HPY**: *“Reflecting back, what are the **3 most important thoughts** in your mind that contributed to your conclusion?”*
- (4) **EVTS**: *“Based on your analysis, please create one or more narratives that **describe the events on the network** (i.e. tell the storyline of the potential events)”.*

To check whether the information in the answers had been captured in the traces.

# Q2: Whether the method captures the key elements in analysts' analytical reasoning processes?

## Cleaning

To weed out the irrelevant answers (“the tool is helpful”) and vacuous answers (“I don’t have any comment”)

## Compare with Traces

## Content Analysis

I conclude that there was likely IRC communication on the network. This could have  
#[H]: IRC communication #

been a policy violation or malware C2 communication. In addition, I saw attempts for  
#[H]: Policy violation or Malware C2 Communication #

FTP (tcp/21), SSH (tcp/22), and HTTP (tcp/80) from internal address space to the  
#[H]: FTP attempt #   #[H]: SSH attempt #   #[H]: HTTP attempt#

internet, which are policy violations. Lastly, there were a large number of IDS alerts  
#[O]: inside->outside #   #[O]: inside->outside #   #[O]: inside->outside #

that were generated about SMB null sessions and overflow attempts which point to  
#[O]: IDS alerts about SMB null session #   #[O]: IDS alerts about SMB overflow attempts #

potentially malicious activity over SMB.  
#[H] Malicious activity over SMB) #



## Q2: Whether the method captures the key elements in analysts' analysis processes?

- Data Cleaning:
  - “IMP\_OBS”: 30 answers
  - “FD\_OBS”: 27 answers
  - “IMP\_HPY”: 29 answers
  - “EVTS”: 29 answers
- Content Analysis
  - Generated 318 themes in these answers.
- “IMP\_OBS”, “IMP\_HPY” and “EVTS”
  - All the themes are captured in traces.
- “FD\_OBS”
  - 5 themes in its answers are not captured by the trace.
  - Domain knowledge (e.g. “some ports are always used for malicious connections”)
  - Implicit assumption made by the participants (e.g. “outbound connections are not allowed by the network policy”)

Not explicitly captured but can be inferred.

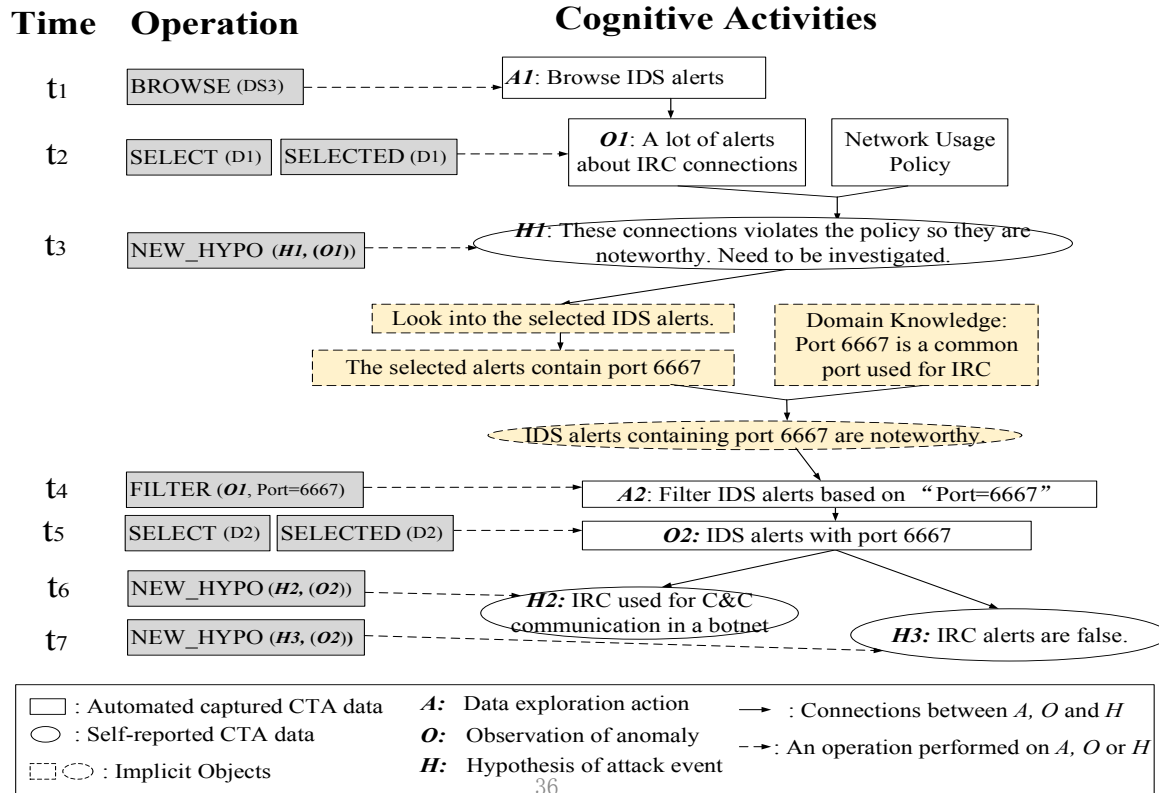
## Evaluate the Method from Four Aspects

- ✓ Q1: Whether the method enables us successfully collect traces in the cyber security domain?
- ✓ Q2: Whether the collected data (traces) contain the key elements in analysts' analysis processes?
- Q3: Whether the analysts' analysis process can be recovered from the captured data (traces)?
- Q4: Whether the analysts' analysis processes recovered from the traces are close to the original ones?

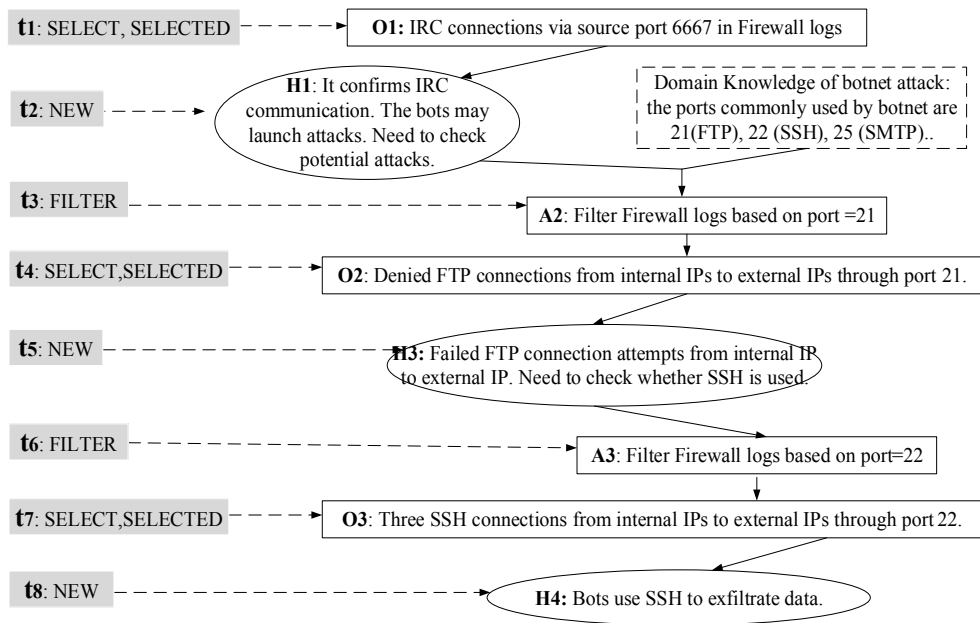
## Evaluate the Method from Four Aspects

- ✓ Q1: Whether the method enables us successfully collect traces in the cyber security domain?
- ✓ Q2: Whether the collected data (traces) contain the key elements in analysts' analysis processes?
- Q3: Whether the analysts' analysis process can be recovered from the captured data (traces)?
- Q4: Whether the analysts' analysis processes recovered from the traces are close to the original ones?

# Q3: Whether the analysts' analysis process can be recovered from the captured data (traces)?



# An Example: Proceeding From One Event to its Associated Events






## Hypotheses:




- Malicious IRC communication to C&C
- →
- Possible Follow-up events: Data Exfiltration

*Largely relies on his experience gained from long-term on-the-job training.*

## Evaluate the Method from Four Aspects

-  Q1: Whether the method enables us successfully collect traces in the cyber security domain?
-  Q2: Whether the collected data (traces) contain the key elements in analysts' analysis processes?
-  Q3: Whether the analysts' analysis process can be recovered from the captured data (traces)?
- Q4: Whether the analysts' analysis processes recovered from the traces are close to the original ones?

## Evaluate the Method from Four Aspects

-  Q1: Whether the method enables us successfully collect traces in the cyber security domain?
-  Q2: Whether the collected data (traces) contain the key elements in analysts' analysis processes?
-  Q3: Whether the analysts' analysis process can be recovered from the captured data (traces)?
- Q4: Whether the analysts' analysis processes recovered from the traces are close to the original ones?

Q4: Whether the analysts' analysis processes recovered from the traces are close to the original ones?



# CTA Data in Traces Complement Each Other

## Automated-captured CTA data

Operations on Action and Observation  
e.g. FILTER, SEARCH, SELECT

## Self-reported CTA data

Operations on Hypothesis  
e.g. NEW\_HYPO

### 1. Automatically captured **action** describes automatically captured **observation**

#### Our Interpretation

**A3:** Go to Firewall logs,  
Filter Firewall logs **based on source  
port 6667**

**O3:** Connections between internal  
IPs and external IPs **via source port  
6667**

#### Information in Trace

```
<Item Timestamp="05/24 13:24:15">  
  FILTER ( SELECT * FROM Task2Firewall WHERE Port = 6667,  
Task2Firewall )  
</Item>  
<Item Timestamp="05/24 13:25:29">  
  SELECT (  
    FIREWALL-[4/5/2012 10:15:00]-[Built]-[TCP]  
    (172.23.240.254, 10.32.5.59),  
    FIREWALL-[4/5/2012 10:15:00]-[Built]-[TCP]  
    (172.23. 30.220, 10.32.5.57) )  
</Item>
```

# CTA Data in Traces Complement Each Other

## Automated-captured CTA data

Operations on Action and Observation  
e.g. FILTER, SEARCH, SELECT

## Self-reported CTA data

Operations on Hypothesis  
e.g. NEW\_HYPO

2. Automatically captured **observation** provides the context information for self-reported **hypothesis**

### Our Interpretation

A2: Filter IDS Alerts based on source port 6667

O2: IDS alerts with port 6667

A3: Go to Firewall logs,  
Filter Firewall logs based on source port 6667

O3: Connections between internal IPs and  
external IPs via source port 6667

H4: IRC communication confirmed

### Information in Trace

```
...
<Item Timestamp="09/12 14:25:33">
  NEW_HYPO(
    Should be malicious IRC communication
  </Item>
```

# CTA Data in Traces Complement Each Other

## Automated-captured CTA data

Operations on Action and Observation  
e.g. FILTER, SEARCH, SELECT

## Self-reported CTA data

Operations on Hypothesis  
e.g. NEW\_HYPO

3. Self-reported **hypothesis** explains the motivation of the following automatically captured **action**

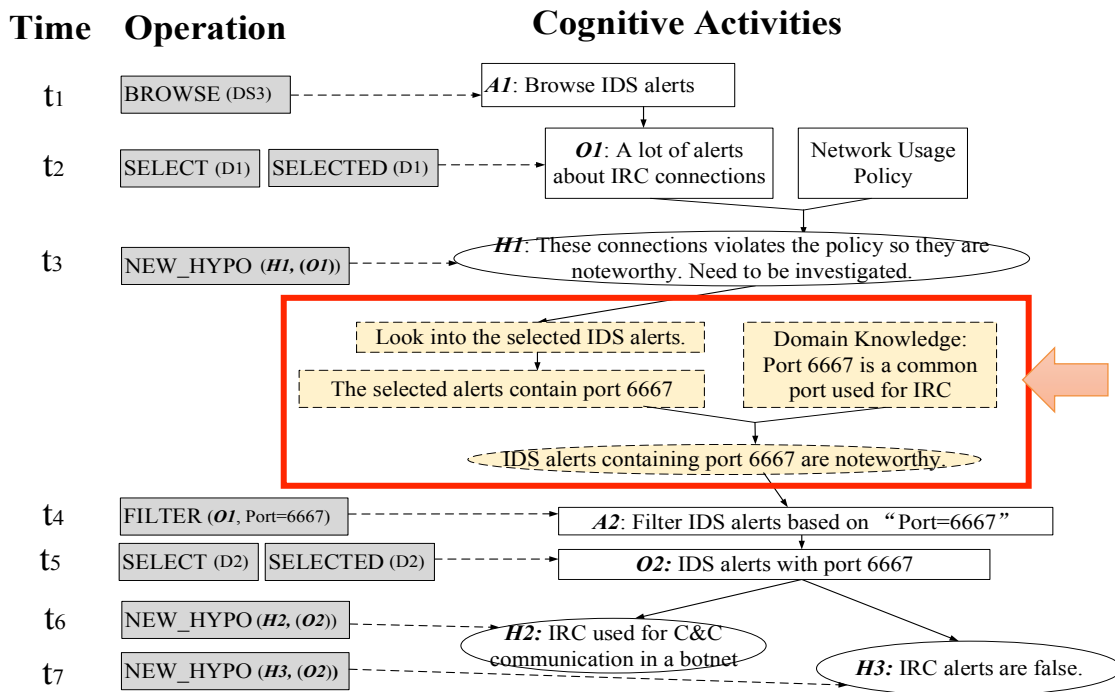
### Our Interpretation

**O2:** Denied FTP connections from internal IPs to external IPs through port 21.

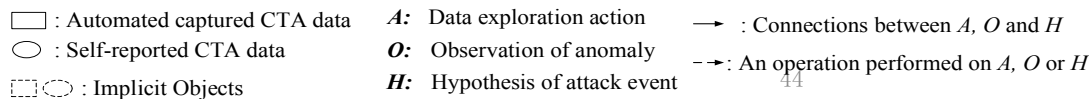
**H3:** Failed FTP connection attempts from internal IP to external IP. Need to check whether SSH is used.

**A3:** Filter Firewall logs based on port=22

# Preliminary Trace-Stimulated Recall with a Professional Analyst



*“I saw strings within the IDS alerts that meant IRC communication/traffic that was based on my prior experience this is a default port for IRC.”*



# Conclusion: Integrating Automated Capture and Self-Report

## An Integrated Computer-Aided Cognitive Task Analysis Data Collection Method

A Conceptual Model:  
Representing the analytical reasoning processes



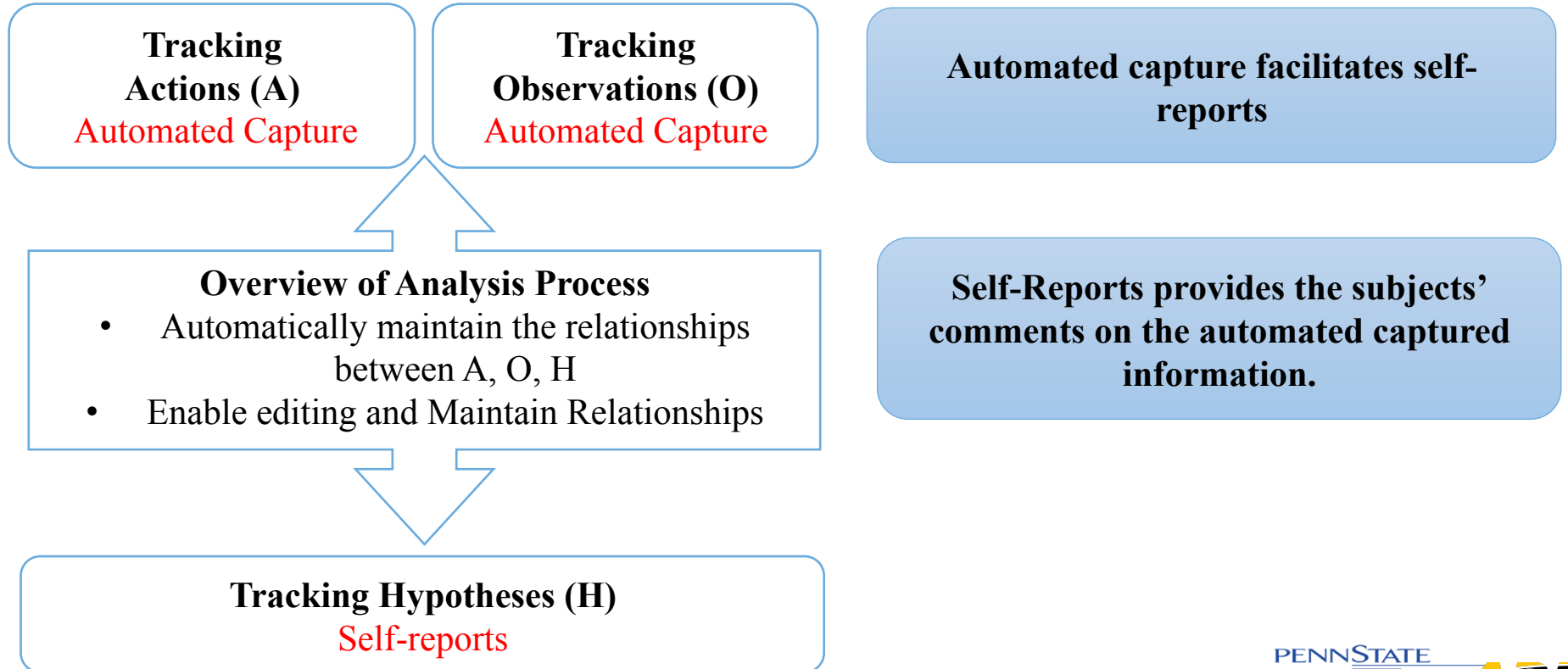
An Interactive Tool:  
Capturing the analytical reasoning processes



An Experiment:  
Traces are collected when subjects are  
performing a cyber analysis task.



# Benefits of Integrated Process Tracing



# Work in Progress...

## An Integrated Computer-Aided Cognitive Task Analysis Data Collection Method

A Conceptual Model:  
Representing the analytical reasoning processes



An Interactive Tool:  
Capturing the analytical reasoning processes



An Experiment:  
Traces are collected when subjects are  
performing a cyber analysis task.



## Next Step: In-depth Trace Analysis

1. Behavior patterns,  
analysis strategy
2. Difference  
between experts  
and novices

Thank You!  
Q&A

Contact: [czz111@psu.edu](mailto:czz111@psu.edu)