# InterSec: An *Inter*action System for Network *Sec*urity Applications

Troy Nunnally *, A. Selcuk Uluagac†, and Raheem Beyah*

*GT CAP Group, The School of ECE
Georgia Institute of Technology
Atlanta, GA 30332,USA
troy.nunnally@gatech.edu, rbeyah@ece.gatech.edu

†ECE Dept
Florida International University
Miami, FL, USA
suluagac@fiu.edu

***Abstract*—Traditional two-dimensional (2D) and three-dimensional (3D) visualization tools for network security applications often employ a desktop, mouse, and keyboard setup of WIMP (Windows, Icons, Menus, and a Pointer) interfaces, which use a serial set of command inputs (e.g., click, rotate, zoom). However, research has shown that multiple inputs (e.g., Microsoft Kinect [8] and multi-touch monitors) could reduce the selection time of objects, resulting in a quicker response time than its traditional counterparts. In this work, we investigate these alternative user interfaces that are ”natural” to the user for multiple inputs that reduce response time as a user navigates within a complex three-dimensional (3D) visualization for network security applications. Specifically, we introduce a visualization tool called *InterSec*, an *interaction system* prototype for interacting with 3D network security visualizations. InterSec helps developers build and manage gestures that require the coordination of multiple inputs across multiple interaction technologies. To our knowledge, InterSec is the first tool that proposes a system to reduce number of interactions within 3D visualizations for network security tools. Through our evaluation of live Honeynet data and a user study, the results reveal InterSec's ability to reduce the number of interactions to aid in 3D navigation in comparison to the mouse user interface.**

***Index Terms*—Natural User Interface, Human Computer Interaction, Security Visualization, 3D Visualization, Network Security**

## I. Introduction

Administrators are often given tasks to evaluate and quickly discover security risks and malicious activity using visual two-dimensional (2D) and three-dimensional (3D) representations of network activity [1], [10]. Futhermore, a large body of work uses 2D/3D visualizations to visualize IDS logs, network management systems, malware, and firewalls [5]. These visualizations for network security applications are often employed on traditional desktop, mouse, and keyboard setup of WIMP (Windows, Icons, Menus, and a Pointer) interfaces. These WIMP interfaces use a pointing device (e.g., a mouse) where users must position and track a digital cursor to target an object that represents network attributes such as a node on a network. The benefit of these WIMP interfaces is that these interfaces provide simple, easy-to-learn, and easy-to-use ”point-and-click” interaction [6]. However, a single mouse cursor provides a maximum of two spatial degrees of freedom (e.g., cursor movement along the x and y axes), so tasks that require manipulating more than two degrees of freedom must be broken up into multiple user actions. Furthermore, with a single cursor, users must make long traversals between spatially distant elements within an interface. The limited amount of degrees of freedom and long traversal cause difficulty in scaling mouse interactions for more complex applications [6]. However, as the amount of datasets continue to increase, it becomes more complex to detect network attacks even when using these visualizations [2]. Often, these user interfaces (UI) require a user to perform many interactions while a user is navigating through a vast visualization environment to make accurate decisions about network activity.

As a result, researchers in the network security field have started to investigate mouseless technologies (e.g., touch-enabled phones/monitors and Microsoft Kinect) that allow for more than two degrees of freedom. These mouseless technologies are referred to as *Natural User Interfaces* (NUIs).

NUIs provide several key advantages from traditional mouse and keyboard input. One advantage is NUIs, such as multi-touch interfaces, provide interactions that can recognize up to 10 fingers and provide up to 20 degrees of freedom. This allows users to perform more interactions and allow interactions to be performed in parallel. Research has shown that multi-touch interaction is about twice as fast as mouse interaction for tasks such as selecting objects that may represent nodes on a network [11]. As a result, researchers can begin developing more complex applications while maintaining quick response times.

In this paper, we study the use of NUI interactions in the context of network security visualizations. Specifically, we propose a visualization module called *InterSec*, an *interaction system* prototype for interacting with 3D network security visualization tools. Using InterSec, we introduce a gesture set that combines multiple interactions into a single interaction to further reduce response times for accomplishing a task such as finding a set of scanned ports for a node. Gesture sets allow users to combine the use of multiple network tools to evaluate network data more efficiently than its traditional WIMP counterparts. As a result, network security users possess more interaction options with visualization tools to identify network attacks. InterSec takes advantage of this increased set of interactions to intuitively represent a series of smaller interactions or a commonly-used network security task (e.g., filter a packet capture). On the other hand, Kinect's natural interactions could be beneficial in assisting in the learnability of complex network security visualizations. The Kinect allows InterSec to reduce the cognitive load of network administrators and produce an easy-to-use visualization. We evaluate both multi-touch and mouse interactions by analyzing the number of interactions and response times of common network attacks of users with basic networking knowledge. Using a network security gesture set, we demonstrate that InterSec reduces the number of interactions of honeynet capture data for advanced users and reduce response times to identify and detect malicious attacks. To the best of our knowledge, this is the first work to introduce a NUI interaction system for efficiently navigating within 3D visualization tools for network security applications.

The rest of this paper is organized as follows. A background and motivation on interactions in 3D visualizations for network security applications is presented in Section 2. Next, related work is discussed in Section 3. We discuss the details of InterSec design for assisting users navigating in 3D environments in Section 4. Next, we illustrate InterSec using use-case scenarios and user study of common network attacks and evaluate this use-case using the number of interactions and response time. Finally, we conclude the paper and discuss our future work in Section 6.

## II. Background and Motivation

Navigating within a 3D visualization for network security applications can be difficult because a large amount of network data is portrayed in a screen-size visualization. There are hundreds of details to track and different interactions must be utilized to navigate through a 3D environment. Our system, InterSec, provides a system for managing input gestures, tailored specifically to network security that would allow both the reduction of interactions to detect and identify a network attack. Furthermore, using NUI, InterSec allows a single gesture to serve as multiple serial gestures to better achieve faster response times.

Moreover, interaction particularly rises in significance as datasets continue to become large and complex. In parallel, interface and interaction technology have rapidly advanced. The wide adoption of touch-enabled phones and multi-touch computing platforms demonstrates a growing popularity for mouseless interfaces, often denoted as *Natural User Interfaces* (NUIs). NUIs are based-on interactions that are ”natural” to the user through commonly performed actions in applications outside of UI design. A well-designed NUI aids in a user's understanding of and productivity in the operation of software programs in a shorter time frame which enables the user to increase his/her efficiency in completing a certain task [6]. Research has also shown the direct-touch nature of multi-touch interfaces accounts for 83% of the reduction in selection time and with training, making strokes bimanually (i.e., using two hands), outperforms making strokes serially by 10-15% which further enhances the user's efficiency [11]. In this paper, we adopt the usage of NUI, commonly-used in applications to minimize response time to identify harmful network security threats.

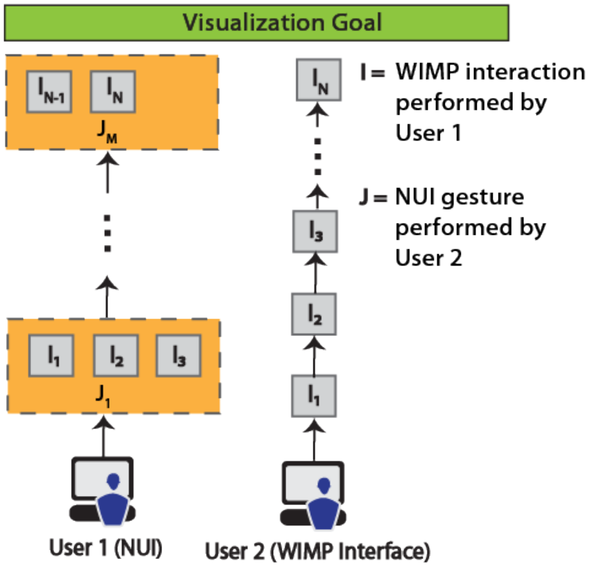


Fig. 1: Motivation.

As shown in Figure 1, our interaction system applies a gesture set from the NUIs to enable a user to perform multiple interactions quickly and to discover a network attack (e.g., DoS or an advanced stealthy port scan aiming to bypass a firewall or subvert an IDS). For example, two users, User 1 and User 2 use a NUI, but User 2 uses the traditional WIMP interface. By using a gesture set within InterSec, User 1 could use one gesture $J_1$ to implement a set of simultaneous interactions ($I_1$, $I_2$, $I_3$) portrayed by User 2. In this scenario, our intention is to reduce the number of individual interactions to assist in reducing the complexity of analyzing network activity in 3D environments.

In addition, due to the parallel nature of multi-touch interactions, the time required to perform a gesture $J_1$ could be less than a single interaction, $I_1$, especially in the selection of tasks. For example, assume a network administrator is attempting to discover problematic nodes performing an Internet Relay Chat (IRC) within a botnet and decides to send his findings to a colleague using a 3D visualization tool. Using Intersec, the network administrator can use a NUI to perform a zoom/rotate interaction (a combination of zoom and rotate) rather than rotate and zoom interaction in series on a WIMP interface. Thus, NUI would take one command instead of two separate commands and reduce the number of interactions. In addition, once the network administrator finds the command and control node, the network administrator may use a collaborative sharing gesture (e.g., four finger swipe) to notify a colleague by sending a filtered packet capture attached to an email for further investigation.

## III. Related Work

Our work is related to two different fields: 3D visualization environments for network security and Natural User Interfaces (NUIs). A description of each field is as follows:

### A. 3D Visualization Environments

Existing 3D visualizations visualize data from various network security applications (e.g., IDSs [5]) using techniques such as iconic tree structures, bar charts, and 3D scatter plots. In addition, researchers have used various techniques to represent a larger number of attributes such as the size of a packet's payload in bytes, the number of packets, and interarrival time. The primary benefit of these visualizations is that they adequately portray generalizations of a network's behavior. Since these visualizations are limited to five parameters (e.g., source IP, destination IP, source port, destination port, protocol), decoys cannot be detected without more parameters such as TCP flags and flow data. As a result, a deeper analysis of scanning behavior is not possible. InterSec addresses these limitations by providing multi-touch inputs to collaborate with other tools to help users engage in a deeper analysis. NetBytes Viewer visualizes the historical network flow data/per port for an individual host machine or subnet on a network using a 3D impulse graph plot.

Papadopoulos discusses CyberSeer [4], a desktop interactive auto-stereoscopic 3D environment. The environment is integrated with multi-channel immersive sound to enhance security awareness. It introduces a 3D auto-stereoscopic environment to analyze spatial information for intrusion detection [4]. Compared to this tool, we introduce a system that will allow users to be able to administrator and utilize gestures for better integration with other tools in order to produce a more holistic 3D toolset.

### B. Natural User Interfaces (NUIs)

Traditional GUIs adopt mouse and keyboard interactions, which use artificial elements like windows, menus, or buttons. On the other hand, NUIs adopt a direct manipulation style (e.g., touch, voice commands, and gestures). NUIs are useful because NUIs takes a user's pre-existing knowledge about manipulating objects in the real world for application in computer technologies. As a result, this technology makes NUIs easy-to-use and easy-to-remember [6]. Some researchers are beginning to deploy NUIs into visualizations and network security applications [7]. One researcher used multi-touch interaction for brushing in parallel coordinates [7]. Our research adopts a portion of the gestures performed in this research and integrates these gestures into our interaction system for network security applications. As a result, our research extends this tool by introducing new gestures into the gesture set and includes interactions from other devices (e.g., Kinect). Other researchers have attempted to develop NUIs tools, such as using the Kinect device, to perform network attacks. For example, Kinectasploit [8] uses a 3D virtual environment to test security systems for vulnerabilities by interpreting Kinect's natural gestures into a series of Metasploit Framework [9] commands. Our system applies this concept more generally to the research field of network security.

## IV. System Design

As previously mentioned, InterSec takes advantage of direct-touch and bimanual input from state-of-the-art NUI technologies to aid in effectively navigating within 3D visualizations for network security applications. InterSec could be integrated into existing visualizations tools or used to promote new alternative NUI designs. We present our NUI system which helps developers of network security tools to build and manage gestures that require the coordination of multiple fingers and body limbs. Our system uses NUI sensor devices (e.g., Kinect and touch monitor) so that the network administrator could use the advantages of devices with a high degree of freedom unlike traditional WIMP technologies.

In order to allow for efficient monitoring and detection of network traffic, we designed and implemented InterSec. InterSec uses the FRE3DS framework [10] to convert gestures into a series of interactions for visualizing network attacks. The InterSec system consists of 4 stages: *Sensor*, *Gesture Recognition*, *Gesture Mapping*, *Visualization Manipulation* as illustrated in Figure 2. First, the raw data is sent from the NUI sensors (e.g., Kinect) to the Gesture-based detection system as input. Our detection system is adopted from GestureWorks [3], an HCI engine that contains pre-selected gestures, which produce the gesture input for gesture mapping.

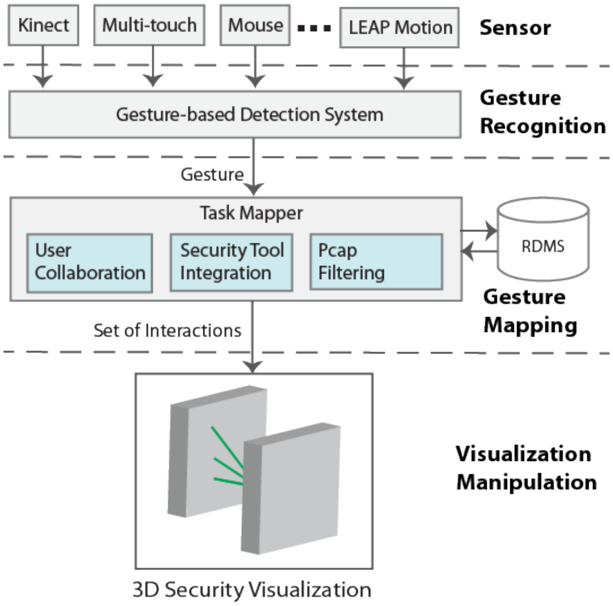


Fig. 2: System Design.

Multi-touch and Kinect systems enables the user to perform several gestures simultaneously in order to convey multiple tasks at one time with fewer interactions. Unlike traditional WIMP technologies, which possess a single mouse cursor with only two spatial degrees of freedom, these systems allows the user to employ body-motion gestures to perform more complex tasks in less time. A sample gesture set from the GestureWorks [3] system is introduced and used in InterSec (Figure 3). A sample gesture set is as follows: (1) *Five finger flick* employs five fingers of a single hand to be placed on the visualization rendering of the network and the motion of the fingers accelerates immediately before the fingers are released from the interface. This gesture denotes collaborative sharing between a user and a colleague. This gesture is important when a new attack has been detected because the *Five Finger Flick* can be used to quickly send a filtered packet capture file via email to a colleague or supervisor for further investigation. (2) *Two finger rotate/zoom* combines both the rotate and zoom gestures in order to quickly manipulate the visualization environment to produce fewer interactions than two separate gestures. (3) *Four finger hold* denotes four fingers touching the interface for a set period of time. These four touch points created on a multi-touch screen produces a visualization window. This visualization can be used as a filter mechanism to show only the packets that are visually shown in the selected visualization window. This allows users to quickly display pcap data of interest and filter unwanted pcap files in one gesture. (4) *Lock one and 2 finger flick* refers to the selection of a visual data set using a single finger and flicking downward with two fingers. Once the user flicks down, InterSec selects the TCP flow and runs a companion tool, such as Wireshark, for the TCP flow data in order to investigate the textual data in greater detail.

The sample gesture set is used specifically for a network security analyst to reduce the number of interactions performed. As a result, response time of the user could be reduced.

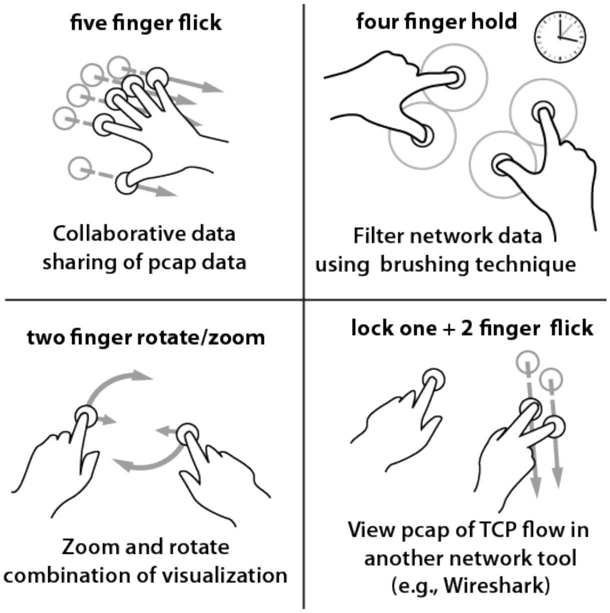

five finger flick
Collaborative data sharing of pcap data
four finger hold
Filter network data using brushing technique
two finger rotate/zoom
Zoom and rotate combination of visualization
lock one + 2 finger flick
View pcap of TCP flow in another network tool (e.g., Wireshark)

Fig. 3: NUI Gesture Set for Network Security Applications [3].

InterSec uses the C++ Object Oriented Model-View-Controller paradigm for higher modularity and extensibility in the 3D visualization tools. We used a custom class using the Microsoft SDK. To render the raw data, we used an interaction testbed on Kinect device and 3M's multi-touch 32-inch monitor, which supports up to 20 fingers.

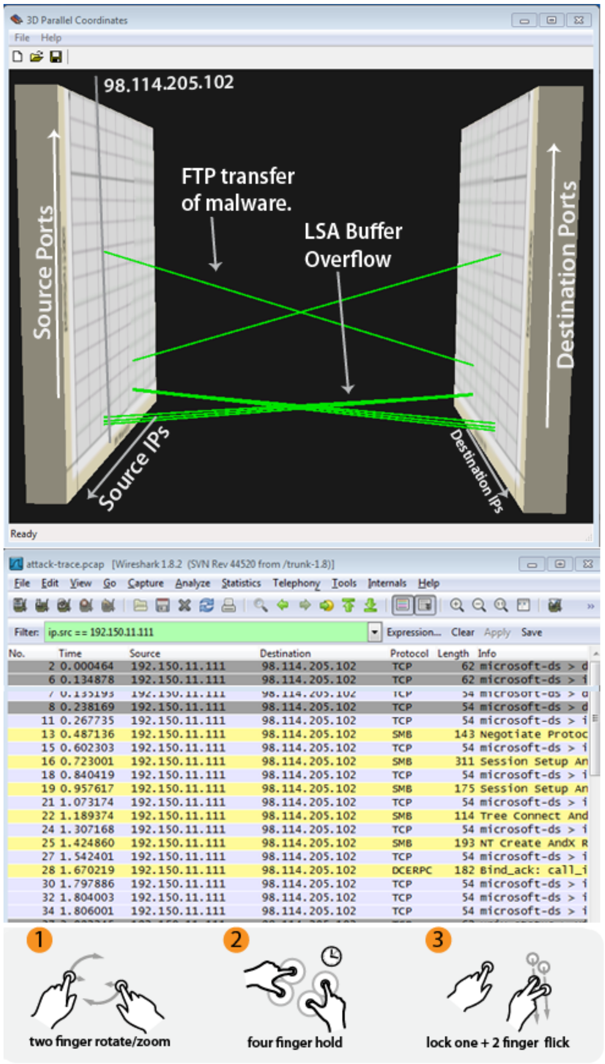
We implemented InterSec as a module of Parallel 3D coordinate system (P3D) [1] and illustrated the functionality of InterSec with different use-case scenarios for analyzing a compromised host on the network. P3D is used because unlike most 3D counterparts, this tool has no theoretical limit in the number of network parameters that can be visualized. Therefore, P3D is able to better detect visualization attacks [1] in comparison to a 2D/3D scattered plot matrix and uses stereoscopic 3D support and interactive techniques such as zooming and panning. To incorporate the InterSec into P3D, we extended P3D by modifying the interaction layer of the Framework for Rendering Enhanced 3D Stereoscopic Visualization (FRE3DS) [10]. Using FRE3DS, network administrators can easily and quickly develop various visualizations to efficiently investigate data.

## V. Performance Evaluation

### A. Security Evaluation

In this sub-section, we evaluate InterSec based on a real-world network attack collected from the Honeynet project. Specifically, we examined the number of interactions to perform tasks for mouse-keyboard vs. multi-touch interactions using P3D [1]. We assume the model for determining the number of interactions by an error-free expert user. Although the user is practically error-proned, this model can be used as a preliminary indicator for determining how long it takes to perform a task, specifically a network attack. An expert is a user that knows the network task domain well and knows how to perform all the tasks that need to be completed. For evaluation, we used live network data adopted from the Honeynet project's 2010 Forensic Challenge [13]. The honeynet pcap portrayed a ”LSASS buffer overflow”, which caused a vulnerability (CVE-2003-0533), exploited by the Sasser worm. The attacker (source IP 98.114.205.102) established a TCP connection with the victim or honeypot (192.150.11.111) on Microsoft-ds port 445 and exploits the victim using the Windows Local Security Authority (LSA) Remote Procedure Call (RPC) service. From this exploit, the attacker opens a new port on the socket listening on port 1957 with a command shell bound to it. Finally, the victim initiated an FTP connection to the attacker and the attacker sent commands to the victim to download the malware. This scenario is beneficial because it is commonly used by attackers. Although the exploit commonly exists, we believe the methods for analysis could be applied more generally to new attacks and discoveries. Note that our intent of this work is to analyze the method for discovering a new attack rather than analyzing the attack itself.

We analyze InterSec based on 4 common tasks: 1) Discover peculiar network activity (e.g., port scans). 2) Filter TCP flows. 3) Analyze IP/TCP header and TCP trace using a Wireshark filter. 4) Report to a colleague or upper management for verification and further investigation. We use these steps because these tasks are commonly used when visualizing network traffic. First, the user uses Kinect's 3-point skeleton tracking tool to configure and show the preferred visualization while away from the monitor. Next, the user employs a sequence of interactions to discover peculiar network activity such as port scans or denial of service attacks. In addition to these interactions, a user can also use InterSec to discover peculiar traffic by analyzing the source IP, source port, destination IP, and destination port by using a translation interaction. Next, the administrator can use two finger rotate/zoom interactions to view the ports from a source IP. After the administrator finds a peculiar port, the user filters the TCP data from a source IP using a four finger hold interaction. After the user filters the network data, the network administrator performs a lock one and 2 finger flick to investigate the TCP flow data and packet payloads in a supplement tool such as Wireshark (Figure 4). If the user finds a binded shell or a malicious executable transfer, then the user performs a five finger flick to send a filtered pcap file of the shell and/or executable to a colleague for further analysis.


3D Parallel Coordinates
File Help
98.114.205.102
FTP transfer of malware.
LSA Buffer Overflow
Source Ports
Destination Ports
Source IPs
Destination IPs
Ready
attack-trace.pcap [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
1
2
3
two finger rotate/zoom
four finger hold
lock one + 2 finger flick

Filter: ip.src == 192.150.11.111

```
No.   Time      Source          Destination     Protocol Length Info
    2 0.000464  192.150.11.111  98.114.205.102  TCP       62 microsoft-ds > d
    6 0.134878  192.150.11.111  98.114.205.102  TCP       62 microsoft-ds > i
    7 0.135193  192.150.11.111  98.114.205.102  TCP       54 microsoft-ds > d
    8 0.238169  192.150.11.111  98.114.205.102  TCP       54 microsoft-ds > d
   11 0.267735  192.150.11.111  98.114.205.102  TCP       54 microsoft-ds > i
   13 0.487136  192.150.11.111  98.114.205.102  SMB      143 Negotiate Protoc
   15 0.602303  192.150.11.111  98.114.205.102  TCP       54 microsoft-ds > i
   16 0.723001  192.150.11.111  98.114.205.102  SMB      311 Session Setup An
   18 0.840419  192.150.11.111  98.114.205.102  TCP       54 microsoft-ds > i
   19 0.957617  192.150.11.111  98.114.205.102  SMB      175 Session Setup An
   21 1.073174  192.150.11.111  98.114.205.102  TCP       54 microsoft-ds > i
   22 1.189374  192.150.11.111  98.114.205.102  SMB      114 Tree Connect And
   24 1.307168  192.150.11.111  98.114.205.102  TCP       54 microsoft-ds > i
   25 1.424860  192.150.11.111  98.114.205.102  SMB      193 NT Create AndX R
   27 1.542401  192.150.11.111  98.114.205.102  TCP       54 microsoft-ds > i
   28 1.670219  192.150.11.111  98.114.205.102  DCERPC   182 Bind_ack: call_i
   30 1.797886  192.150.11.111  98.114.205.102  TCP       54 microsoft-ds > i
   32 1.804003  192.150.11.111  98.114.205.102  TCP       54 microsoft-ds > i
   34 1.806001  192.150.11.111  98.114.205.102  TCP       54 microsoft-ds > i
```

Fig. 4: P3D tool using InterSec's NUI Interactions.

In Figure 5, we show the number of interactions for NUI vs. mouse/keyboard interactions performed by an error-free expert user for each of the four tasks previously discussed. We examine this number by exploring the number of minimum combinations of error-free interactions to successfully accomplish tasks. Each number along the x-axis in the figure represents each task presented in this paper. With InterSec, we show at least a 50 % reduction in the number of interactions compared to traditional mouse/keyboards interactions for analyzing a Windows LSA RPC buffer overflow. As a result, this reduction in interactions will significantly reduce a user's response time. A user's response time refers to the time taken by a user to react to a given visualization. In task 3 (Analyze IP/TCP header and TCP trace using a Wireshark filter), InterSec shows a substantial interaction reduction from 32 mouse/keyboard interactions in comparison to 5 NUI gestures using InterSec. This is partly due to the large amount of interactions to open Wireshark, scroll to an interesting packet, and investigate the packet payload. Our analysis shows the number of interactions of a Windows LSA RPC buffer overflow analysis will be reduced from 55 mouse/keyboard interactions to 13 NUI interfaces using InterSec. Although our analysis is error-free (i.e., no mistakes are perform by a user), we expect our analysis to apply more generally to more practical error-proned scenarios. In error-proned scenarios, a user performs non-optimal paths and introduces gestures that do not attribute to the detection of an attack. If the error introduced is constant across WIMP interfaces and NUIs, the reduction of interactions will still apply.

### B. *User Study Evaluation on Efficacy of InterSec*

In this sub-section, InterSec and WIMP interfaces are evaluated utilizing user testing methods. As previously mentioned, within the user testing, a user was presented with network security scenarios from a 3D visualization tool such as P3D and the task *response time* and *number of interactions* were measured. The response time is defined as the time span for recognizing a visualization goal (i.e., successfully detect an attack) and the number of interactions is defined as the sum of interactions that is used to determine an attack. Within user testing, two subsets of the users were asked to complete tasks using a mouse and multi-touch system respectively. Next, these tasks completion times of various users were compared.

Each scenario contains a 3D Parallel coordinate system using a WIMP interface or a NUI interface from the InterSec system. With user testing, 200 network attack scenarios are analyzed using InterSec to determine if InterSec validates the hypothesis of reducing the number of interactions and increasing response rates. Each task is evaluated using the timespan to complete each task. Also, both the number of user interactions and the sequence of interactions are measured. This data collection, in conjunction with post-survey responses provides valuable insights to understand the efficacy of the InterSec system. Both quantitative and qualitative data were collected from participant interactions with the user interface and the questionnaires, using the 5-point Likert scales.

*1) User Testing Method :* Approved by the Institutional Review Board (IRB), the user testing method contained a group of network visualizations scenarios in which users were asked to analyze and identify malicious activity on the network. Each network visualization scenario ranged in

| ***Scenario*** | ***Response time (s)*** | | ***Number of interactions*** | |
|---|---|---|---|---|
| | WIMP | InterSec | WIMP | InterSec |
| Port scan | 49.0 | 38.6 | 19.5 | 13.4 |
| DoS | 46.5 | 35.7 | 25.0 | 18.2 |
| Port Confusion with DDoS and Scan | 115.2 | 85.1 | 48.6 | 32.2 |
| Port source confusion attack | 125.7 | 80.7 | 50.4 | 32.8 |
| DDoS using SYN Flood | 126.9 | 87.9 | 60.2 | 40.4 |
| DoS with background noise | 182.9 | 132.2 | 63.4 | 38.8 |
| 2 port scans with large noise | 180.7 | 132.2 | 67 | 36.2 |
| FTP disguised attack | 191.7 | 120.5 | 65.02 | 55.6 |
| Legitimate traffic with no attacks | 230.3 | 193.4 | 83.0 | 70.6 |
| Average | 138.8 | 100.7 | 53.6 | 37.58 |

TABLE I: Response time and number of interactions for WIMP and InterSec, on average.

difficulty from beginner to expert level. When each participant arrived at the lab, the tasks were explained to the participants and each participant was asked to sign a consent form. Next, a pre-survey was given to list any related classes taken in the field of network communications and network security to further confirm the expertise of the user. At the conclusion of the pre-survey, the components of the user interface and visualization techniques were explained to the participants involved in the survey. In addition, various scenarios, were given to ensure that all participants understood the concept of the visualization techniques during the experiment.

Next, the user analyzed a group of warm-up scenarios. During the warm-up scenarios any participant made consistent inaccurate readings, the participant was considered as an ”inadequate user” and data for that user was discarded. After warm-up sessions, the lab-based evaluation was conducted with 15 different subjects who were recruited (13 male and 2 female) with basic networking knowledge, aged between 22 and 32 years (mean = 25, sd = 4.7) to explore 3D stereoscopic conditions, recommender systems, and NUI techniques. A user interface (UI) was developed to automatically guide each participant through a sequence of screens, each prompting them to enter an explanation of each attack. Each sequence consisted of the following 9 attacks: (1) *Port source confusion attack* occurs when multiple source IPs share a common source port [1]. (2) *Port Confusion Attack with DDoS and Scan* is defined as a set of source IPs that sends packets to a a single port on a destination IP. In parallel, 3 source IPs attempts to scan the network under the rate is used commonly in IDS configurations [12]. (3) *Legitimate traffic with no attacks* represents benign legitimate traffic on a network. (4) *Windshield Wiper Attack (WWA)* obscures a range of ports by sending spoofed packets on a network. (5) *FTP disguised attack* is an attack disguised as a concurrent FTP transfer. (6) *Distributed Denial of Service (DDoS) using SYN flood* is used to block services by sending special crafted packets with the SYN flag enabled by multiple hosts. (7) *Port scan* is a scan of various services from a single host. (8) *2 port scans with large noise* occurs when a large amount of background noise is injected into the network while 2 port scans are occurring. (9) *DDoS with background noise* performs a DDoS attack with a large amount of legitimate traffic from remote hosts.

For each scenario, users were expected to spend a maximum of 5 minutes and the completion time for each user was 60 to 90 minutes. Each scenario contained simulated or sample network traffic. While each user performed each task, observation, note-taking, ”thinking- out- loud”, and other survey testing methods were used. Observation and note-taking allowed the observer to notice common mistakes of users, their sequence of logical choices and created a record of the session’s observations. The ”thinking- out- loud” method further enhanced the notes of the user’s experience and led to possible layout reconstruction to decrease confusion during each experiment. We recorded response time and number of interactions during each session. Lastly, all participants were requested to fill out a post experiment survey. This survey served as a means to retrieve quality feedback such as information and comments from users that were not addressed during the experiment.

*2) Response Time Analysis:* Table I lists the response times averaged over the 15 users for both WIMP and multitouch interface. As expected, the response times of the InterSec is reduced approximately by 27.20 % largely due to large reduction in direct touch selection time and the multi-touch gesture set as shown in previous literature [11].

Participants from the main study found that WIMP was easier to use on initial attempts due to the familiarity of WIMP in other tools. However, as the participants became more familiar with the NUI, their interaction with the NUI became more natural. For example, when a user uses an interface on the first attempt, the ability of an interface to allow users to accomplish a task takes significantly longer than the second attempt because the user is unfamiliar with the visualization. During the warm-up sessions, our results shows that the user was able to reduce response time by 23 % in 3 attempts using the NUI.

*3) Interaction Analysis:* During experimentation, the number of user interactions for each session was recorded using programmable hooks. This data was used to determine the average number of user interactions for each scenario using both InterSec and WIMP interfaces. As shown in Table I, InterSec produces a 30.48 % (on average) reduction in the number of interactions for InterSec over its WIMP counterpart. This reduction occurs because InterSec's ability to use one interaction that would require the user to perform multiple interactions within WIMP interfaces. The result shows as much as a 45.97 % reduction for attacks (e.g., 2 Port Scans with large noise) that require the user to perform many zooms and rotates because InterSec can perform a zoom and rotate with one interaction.

To further investigate the number of interactions, users were asked to perform four tasks (mentioned in Section V-A) using both InterSec and WIMP interfaces. For each task, an average of the total number of interactions of the users and minimum amount of interactions to perform each task (WIMP-Min and NUI-Min) for both WIMP and InterSec interfaces were calculated. As denoted in Figure 5, on average, the number of interactions is reduced by as much as 63 % for tasks that require the user to open Wireshark and apply filters. This reduction occurs because the number of interactions the user performs to open tools such as Wireshark could be reduced to one interaction with InterSec.

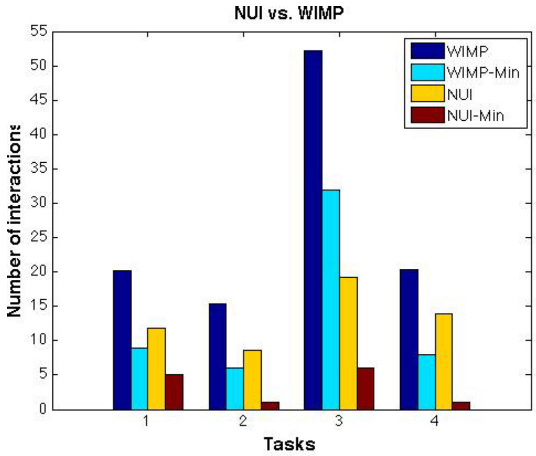


Fig. 5: NUI Interactions for discovery of LSASS buffer overflow [14].

*4) Qualitative Feedback:* To conduct qualitative analysis, the participants were given 5-point Likert scale questionnaires to understand the ease-of-use of the InterSec system. 60 % of the users ranked the InterSec system as very high or as having a high ease-of-use. Also, 40 % of the users ranked the system as having a neutral ease-of-use partly due to difficulties of remembering gestures and using tools (e.g., Wireshark) on the touch monitor that is primarily designed for WIMP interfaces. The qualitative feedback from the study revealed that some participants developed strategies for learning gestures. For example, one participant used the imagery (four finger hold is like creating a window or frame with your fingers). In some cases, participants found difficulty memorizing gestures and these participants constantly referred to the cheat sheet. It is assumed that these participants did not attach the gesture to a natural gesture like taking a picture or physically sliding a task to a colleague using a five-finger swipe. This issue can be addressed by introducing a natural example of why the gesture was chosen for a task. This method allows the user to attach a natural action. For example, physically pushing a sheet of paper to a colleague is similar to five finger swipe because in both cases, data is sent to another user.

## VI. Conclusions and Future Work

In this paper, we introduced the use of novel multitouch interactions to analyze multidimensional data. Although there have been several studies on 2D/3D visualization techniques for network analysis, there has been little work on interaction techniques aimed at understanding and analyzing attacks. Our proposed tool, InterSec, allows administrators to develop NUI gesture sets to reduce the interactions performed on a 3D security tool and assist users in navigating in the 3D visualizations. In addition, we extended the interaction space within a 3D visualization using InterSec and developed a gesture set that is used to simulate multiple actions used to discover new data. InterSec is used to reveal vital scanning characteristics of data and to determine correlations between data and attacker nodes on a network. To the best of our knowledge, InterSec is the first tool that proposes a system to reduce number of interactions within 3D visualizations for network security tools. Through extensive evaluation of live Honeynet data and a user study, the results reveal InterSec's ability to reduce the number of interactions to aid in 3D navigation in comparison to the mouse user interface. In the future, we plan to analyze error-proned scenarios.

## References

[1] T. Nunnally, et al., "P3D: A Parallel Coordinate System for Network Security," in *Proc. of the IEEE ICC Conference*, June 2013.

[2] T. Nunnally, et al.,, "Navsec: A Recommender System for 3D Network Security Applications," in *Proc. of the International Symposium on VizSEC*, 2013.

[3] G. Works, "GestureWorks," 2013. [Online]. Available: http://www.gestureworks.com/

[4] C. Papadopoulos, et al., "Cyberseer: 3D Audio-visual Immersion for Network Security and Management," in *Proc. of the ACM VizSEC Workshop*, 2004, pp. 90–98.

[5] I. Xydas, et al., "3D Graph Visualization Prototype System for Intrusion Detection: A Surveillance Aid to Security Analysts," in *Proc. of the Conference on Computer Graphics and Artificial Intelligence*, May 2006.

[6] D. M. Krum, et al., "Speech and Gesture Multimodal Control of a whole Earth 3D Visualization Environment," in *Proc. of the VISSYM*, 2002, pp. 195–200.

[7] R. Kosara, "Poster: Indirect Multi-Touch Interaction for Brushing in Parallel Coordinates."

[8] J. Bryner, "Kinectasploit," in *Defcon*, ser. Defcon 19, 2011.

[9] D. Kennedy, et al., *Metasploit: The Penetration Tester's Guide*, 1st ed. San Francisco, CA, USA: No Starch Press, 2011.

[10] T. Nunnally, A. S. Uluagac, J. Copeland, and R. Beyah, "3DSVAT: 3D Stereoscopic Vulnerability Assessment Tool for Network Security," in *Proceedings of the 37th IEEE Conference on LCN*, 2012.

[11] K. Kin, "Investigating the Design and Development of Multitouch Applications," Ph.D. dissertation, EECS Department, University of California, Berkeley, Dec. 2012.

[12] Snort, "Snort." [Online]. Available: http://www.snort.org/

[13] "The Honeynet Project." [Online]. Available: https://www.honeynet.org/challenges. 2012.

[14] "Semantic." [Online]. Available: http://www.symantec.com/. 2013.