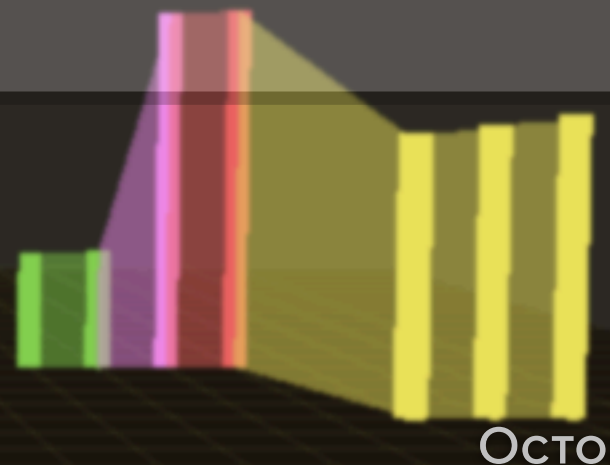
Visualization of Complex Attacks and State of Attacked Network

Anatoly Yelizarov & Dennis Gamayunov

Department of Computational Mathematics and Cybernetics, Moscow State University

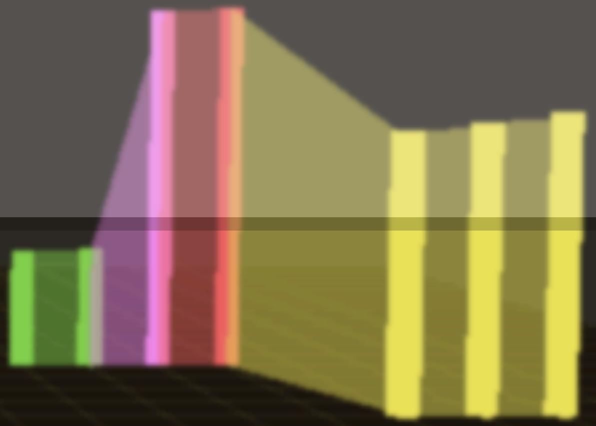


VizSec 2009
Workshop on Visualization for Cyber Security

October 11th, 2009
Atlantic City, NJ USA

Outline

- Complex Attacks
  - Introduction
  - Examples
  - Characteristics
- Visualization Requirements
- Reference Example
- Technical Approach
  - Visualization Techniques
  - Visualization of Key Complex Attack Properties
- Results
- Future Work



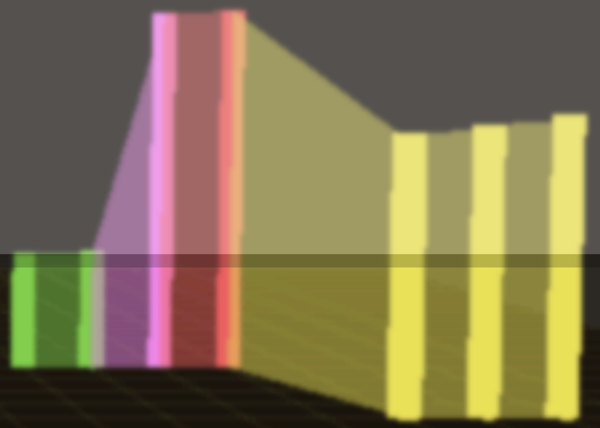
Complex Attacks: Introduction

- Simple Attack
  - Single Attacker/Action/Vulnerability

🟡 DOS Apache mod_ssl non-SSL connection to SSL port denial of service attempt
🔴 EXPLOIT x86 Linux mountd overflow
🟢 SCAN synscan portscan

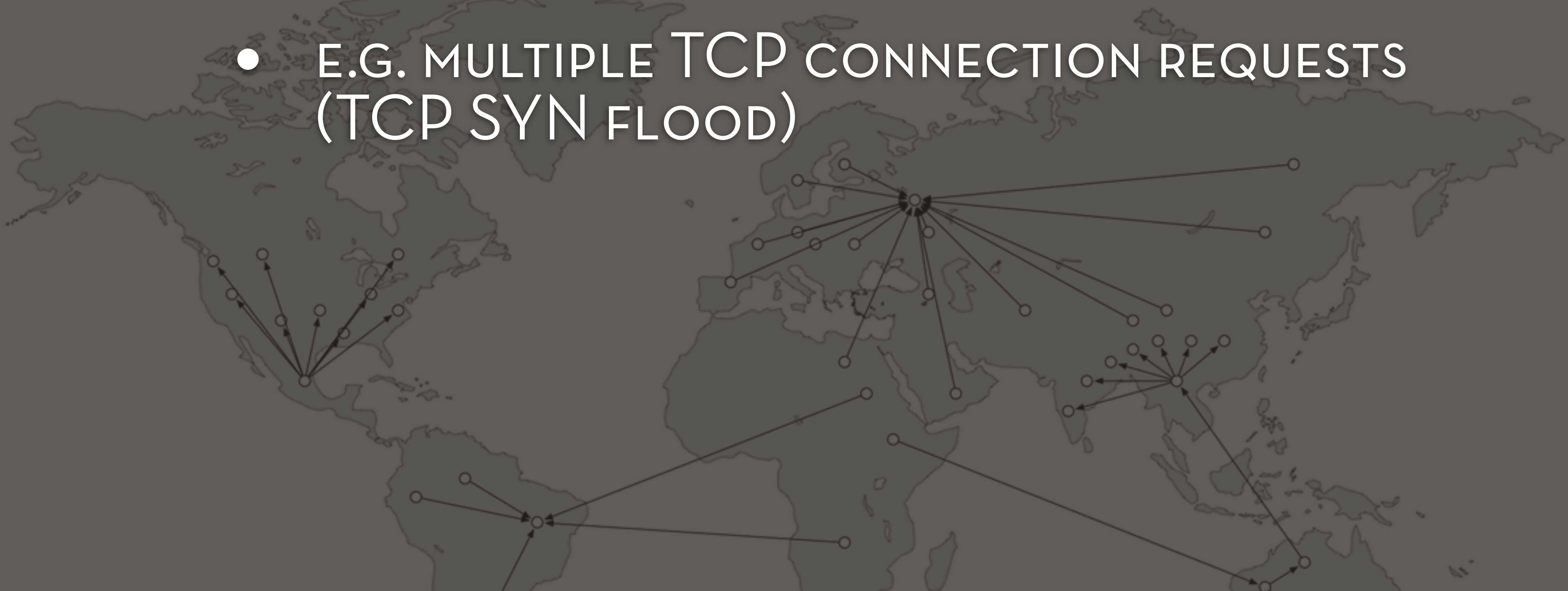
- Complex Attack
  - Preplanned set of simple attacks

- Complex Attacks → Greater Threat
  - Can reach better protected hence more valuable targets

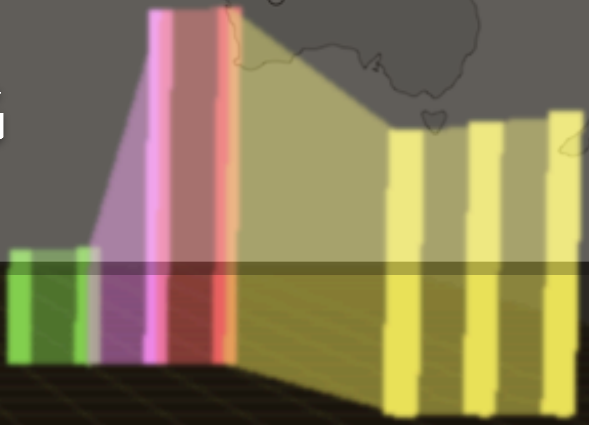


Complex Attacks: Example

- DDoS (distributed denial of service)
  - e.g. multiple TCP connection requests (TCP SYN flood)



- Distributed Scanning

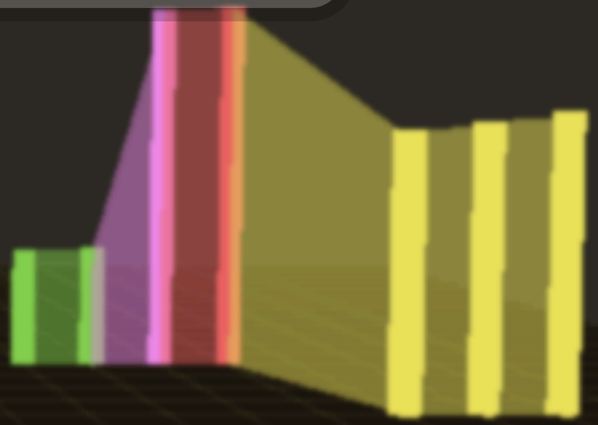


Complex Attacks: Characteristics

- Severity level
- Massive scaling
- Duration
- Positional relationship in time
- Events' relations within attack

Visualization Requirements

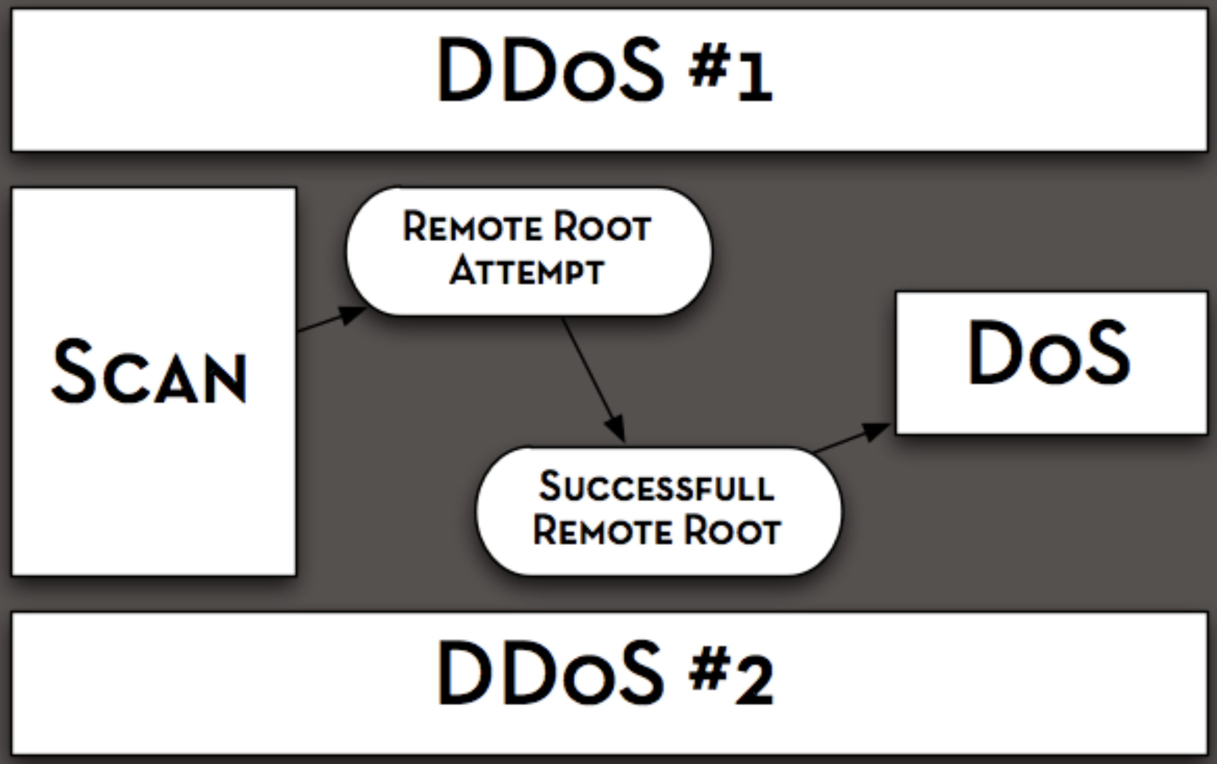
- Single screen
- Passive monitoring
- Perceive simple events
- Perceive complex attacks
  - Completely with all their internal connections



Events' preprocessing is done by IDS

Reference Example

- Initial Data
  - 25 local hosts
  - Short time (10 seconds)
  - Several attacks at once
- Distributed scanning
- Multistep attack
  - Scan → Node Capture / Remote Root → DoS Attack
- DDoS



DDoS #1

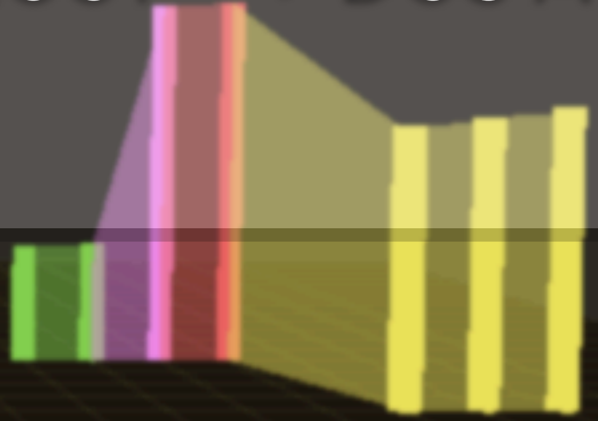
Scan

Remote Root Attempt

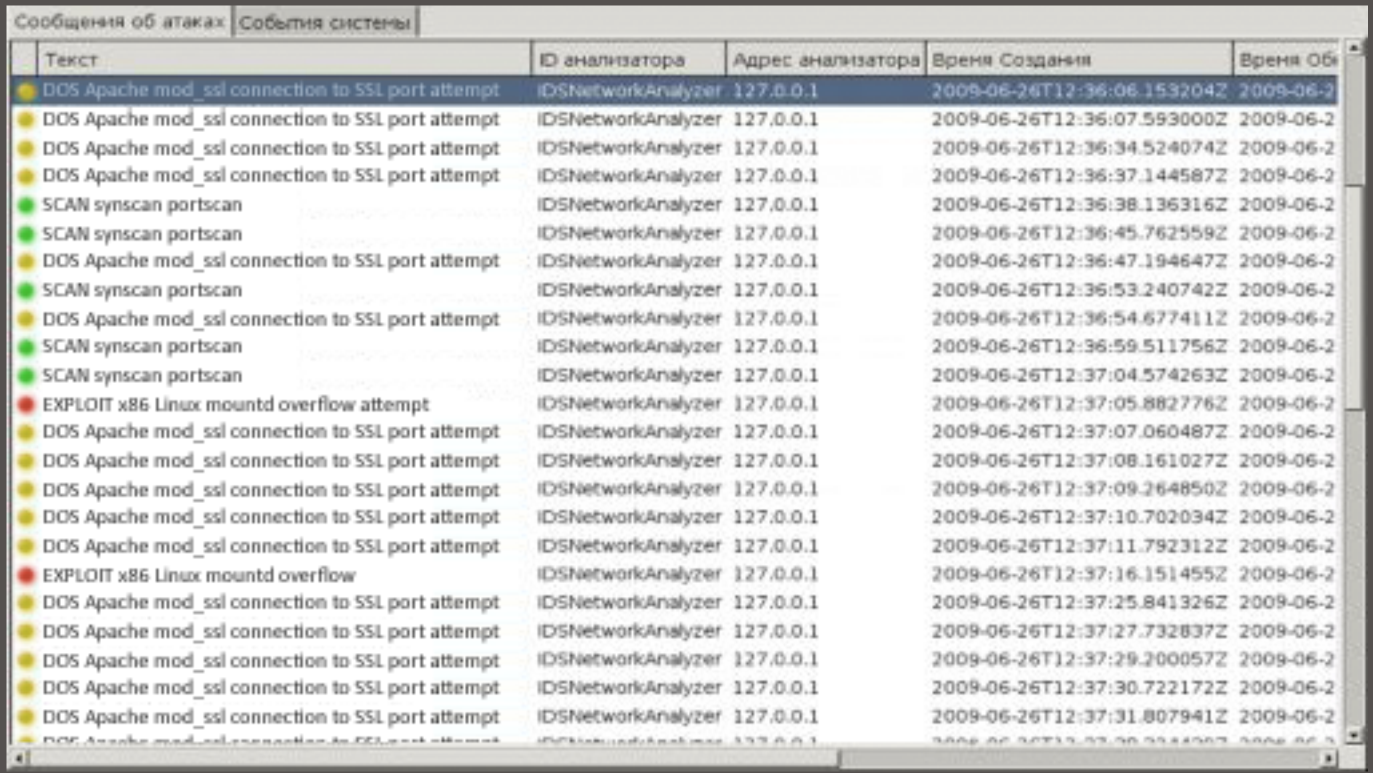
Successfull Remote Root

DoS

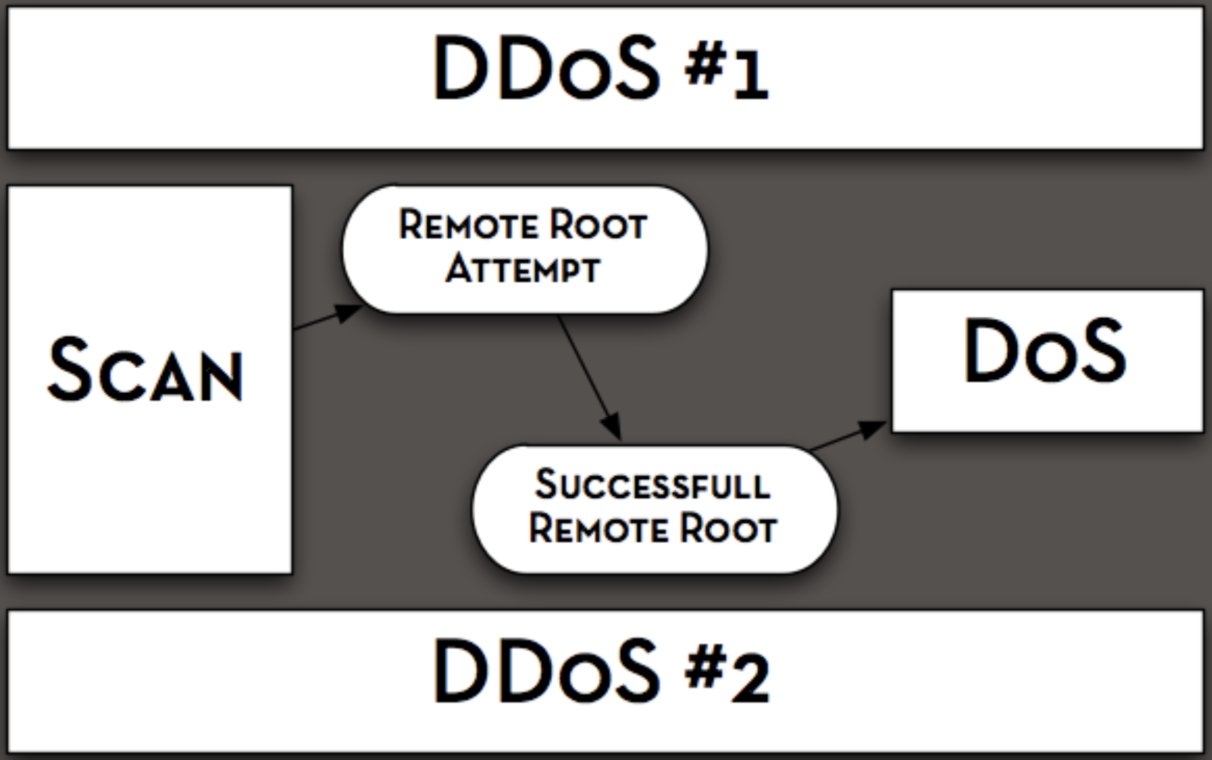
DDoS #2



Reference Example



	Текст	ID анализатора	Адрес анализатора	Время Создания	Время Об
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:36:06.153204Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:36:07.593000Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:36:34.524074Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:36:37.144587Z	2009-06-2
●	SCAN synscan portscan	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:36:38.136316Z	2009-06-2
●	SCAN synscan portscan	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:36:45.762559Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:36:47.194647Z	2009-06-2
●	SCAN synscan portscan	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:36:53.240742Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:36:54.677411Z	2009-06-2
●	SCAN synscan portscan	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:36:59.511756Z	2009-06-2
●	SCAN synscan portscan	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:04.574263Z	2009-06-2
●	EXPLOIT x86 Linux mountd overflow attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:05.882776Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:07.060487Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:08.161027Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:09.264850Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:10.702034Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:11.792312Z	2009-06-2
●	EXPLOIT x86 Linux mountd overflow	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:16.151455Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:25.841326Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:27.732837Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:29.200057Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:30.722172Z	2009-06-2
●	DOS Apache mod_ssl connection to SSL port attempt	IDSNetworkAnalyzer	127.0.0.1	2009-06-26T12:37:31.807941Z	2009-06-2



DDoS #1

Scan

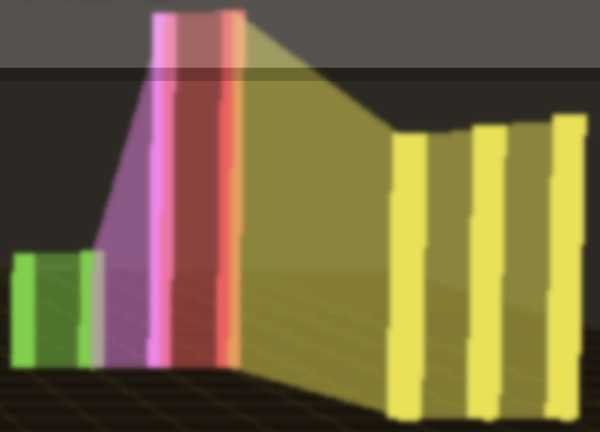
Remote Root Attempt

Successfull Remote Root

DoS

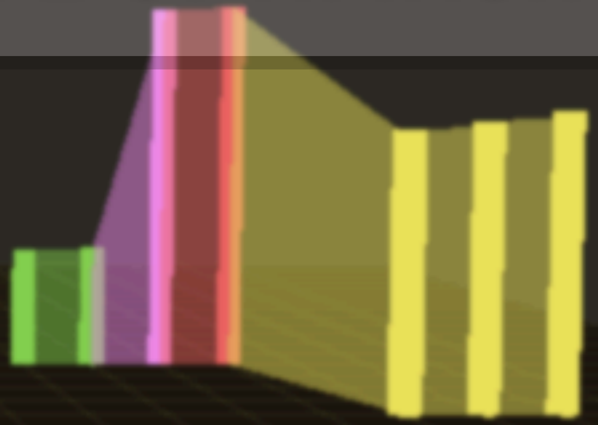
DDoS #2

200 MESSAGES IN 10 SECONDS



Visualization Techniques

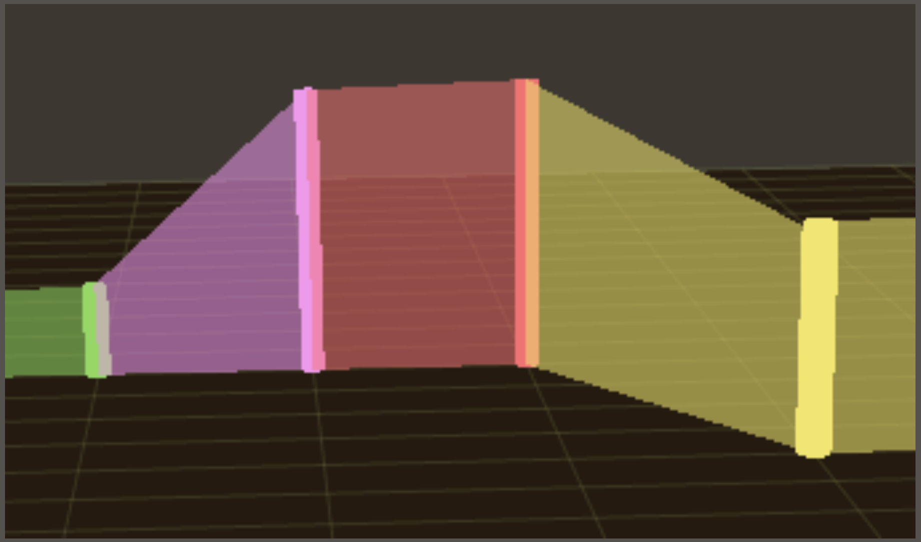
- Histograms — instant comparison of any activity
- Glyphs — mapping hosts and events
  - Glyph sizes — gleaning additional data
- Scatter plots / Parallel coordinate axes — local and foreign host relationships
- Color maps — severity or type of attack



Designed abstraction is based on these techniques

Severity Level vs. Type of Attack

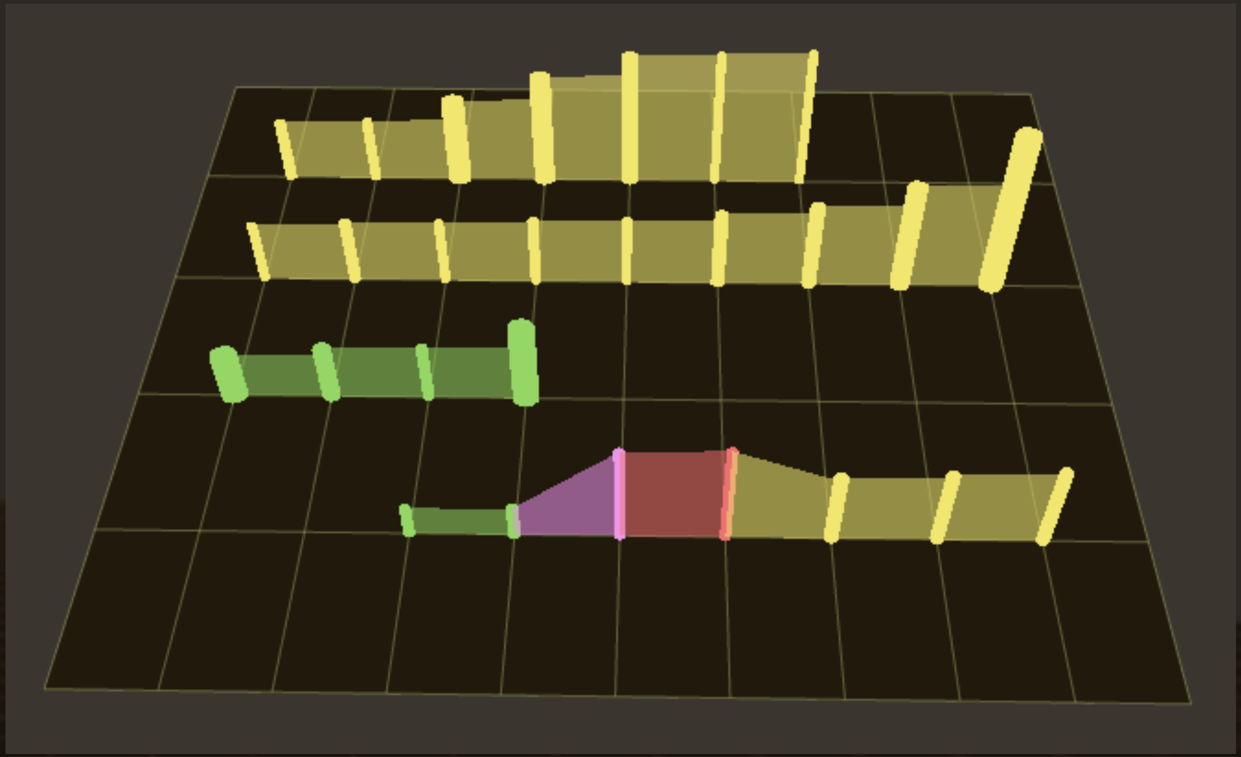
- Events are mapped into cylinder glyphs
- Severity level into cylinder's height
  - Low
  - Medium
  - High
  - Info



- Type of event into color map

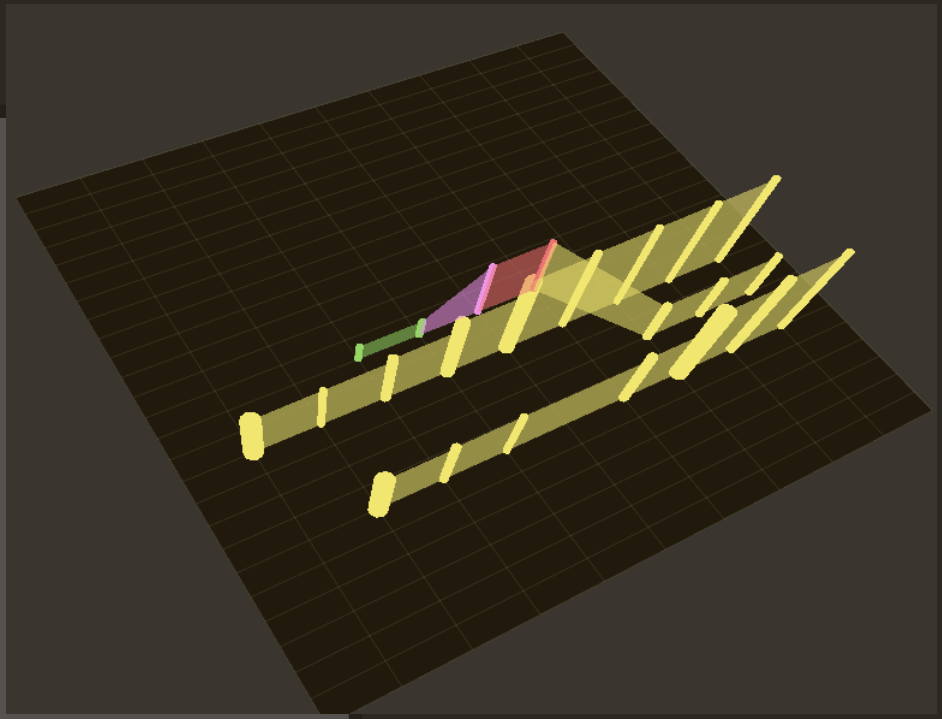
Relations Within Attack

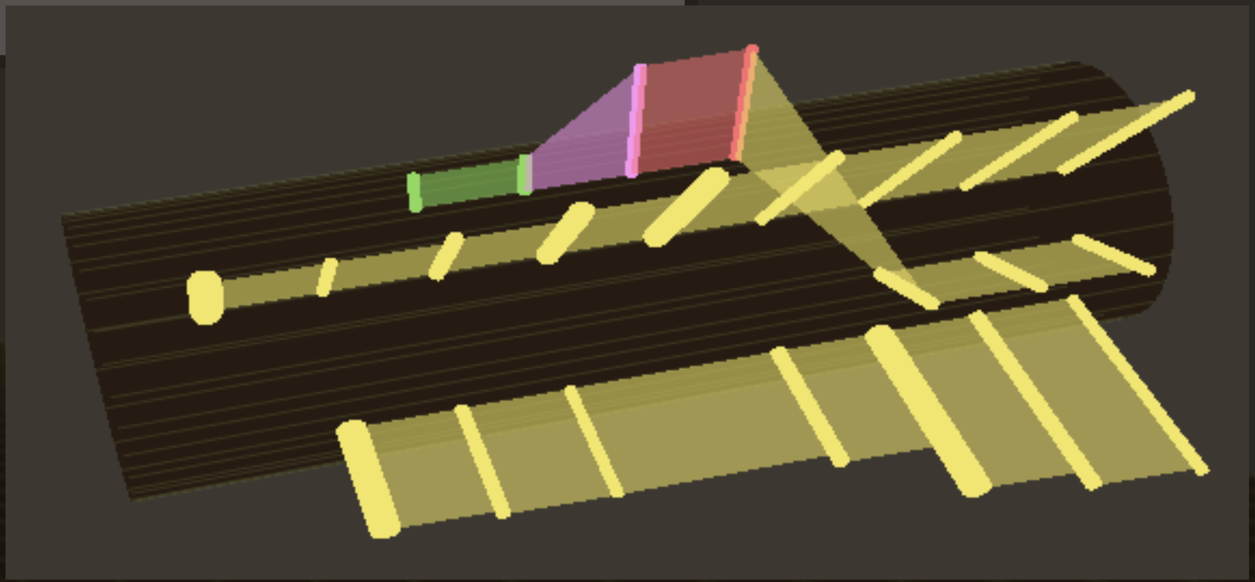
- Concept:
  - Successive linking of the glyphs within attack
- Implementation:
  - Transparent quadrangle through vertices of associated cylinders



Time and Visualization Spaces

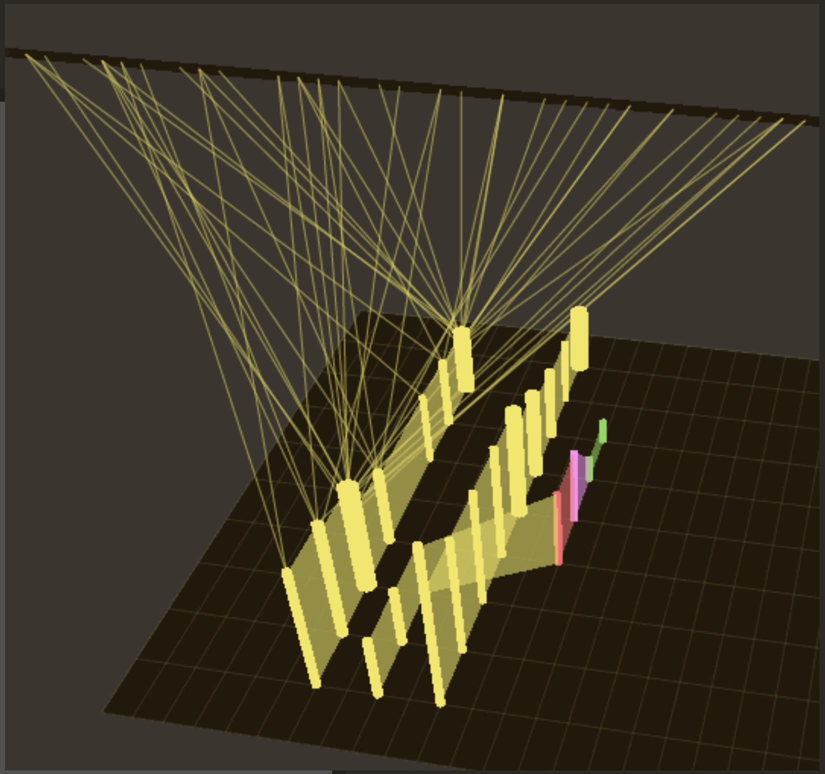
- Coordinate allocation:
  - Classical (Cartesian)
    - More customary
  - Cylindrical
    - Increased volume between neighbor glyphs

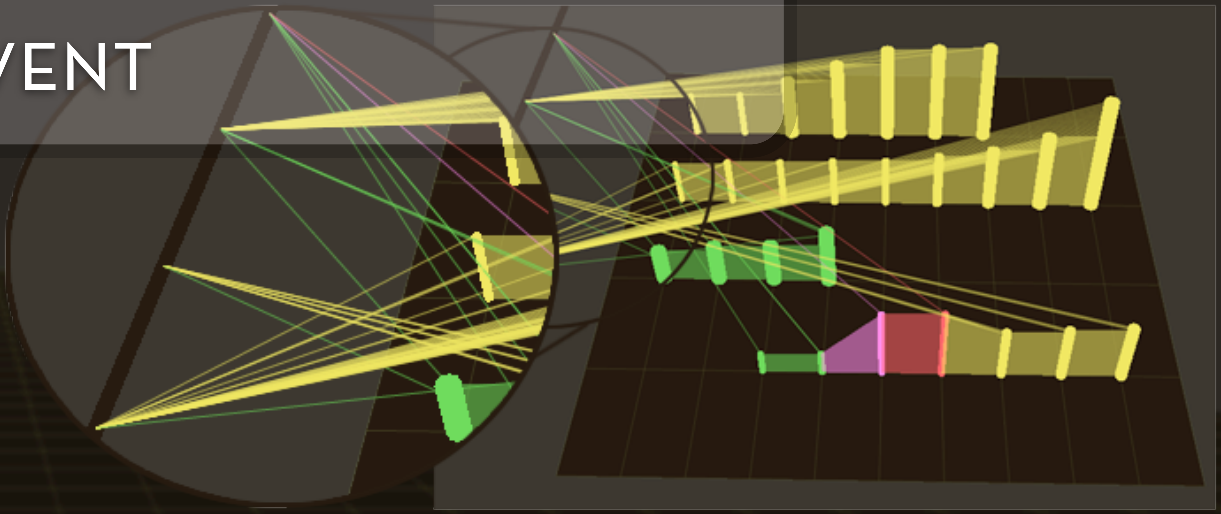




Hosts’ Addresses

- Local hosts:
  - Classical (Cartesian) — one of the axes
  - Cylindrical — angle
- External hosts:
  - Equivalent in terms of danger they may present
  - Subsidiary axis
  - Line connects source and event
  - Line has the same color as event

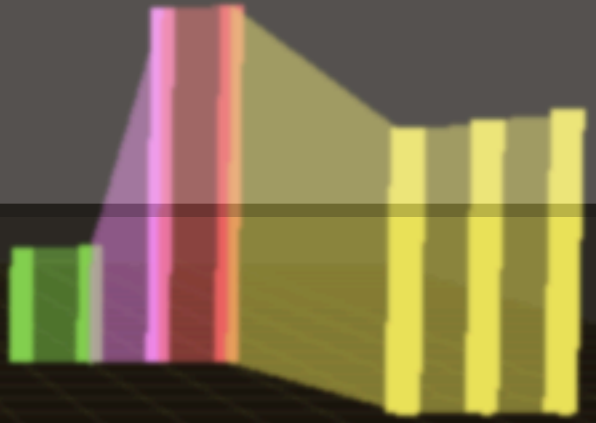




Some Other Features

- Glyph thickness:
  - Highly probable for several events to happen to one host at the same time
  - Thickness depends on quantity of events
  - Limited to avoid overlaps

- Height variations:
  - Maps frequency of events
  - Events interconnected && frequency extends threshold
  - Increases severity level



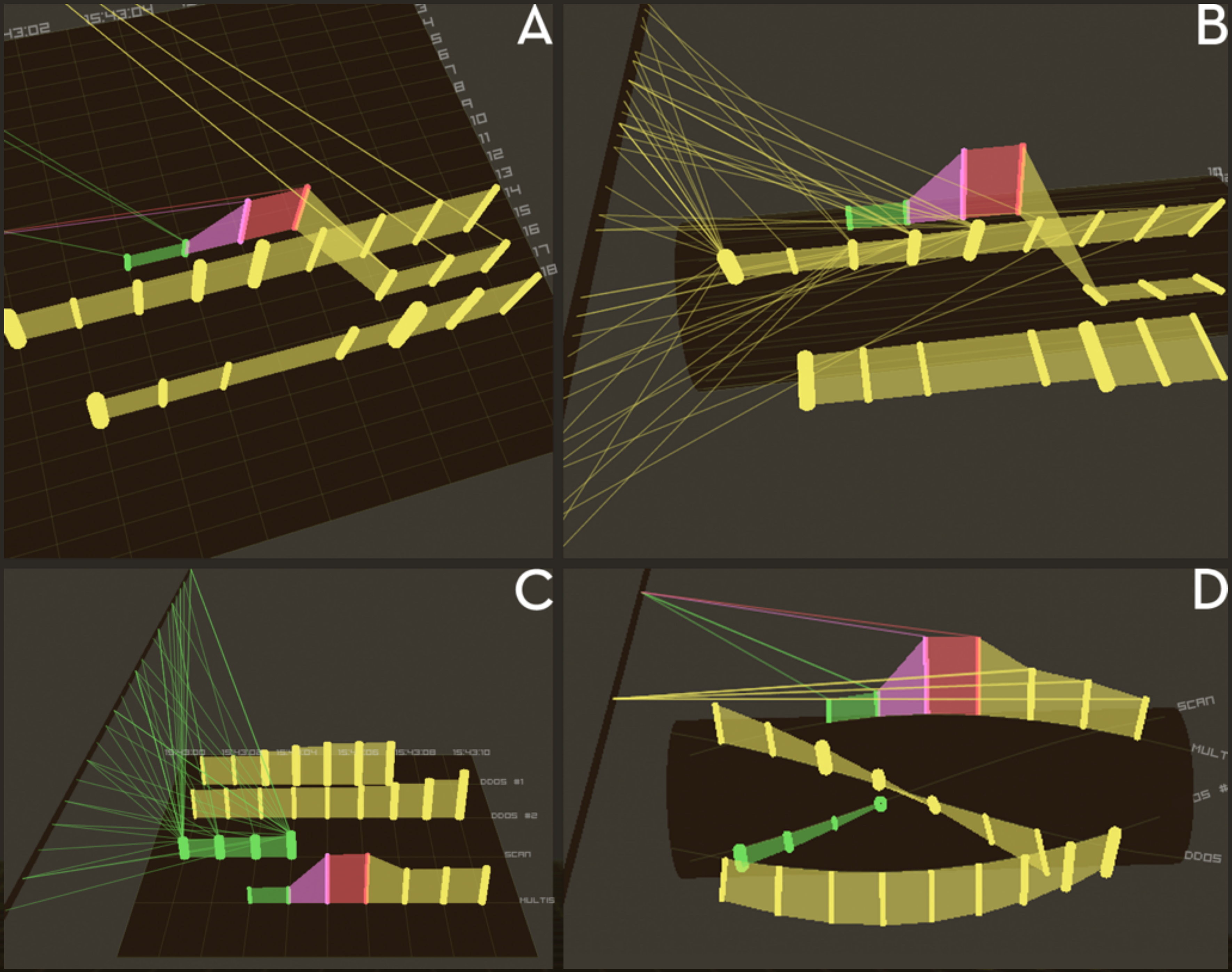
Visualization Modes

Cartesian

Cylindrical

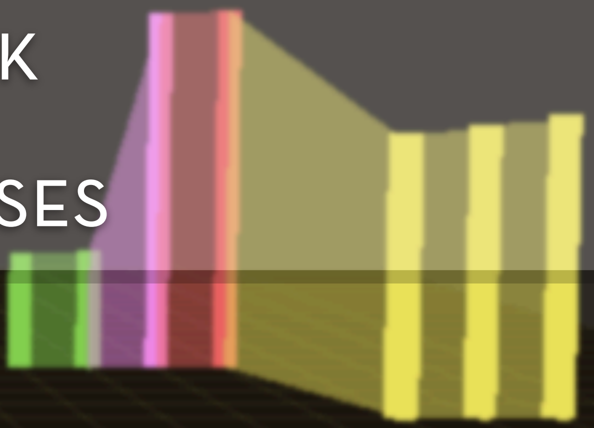
Common

Complex attacks oriented



Results

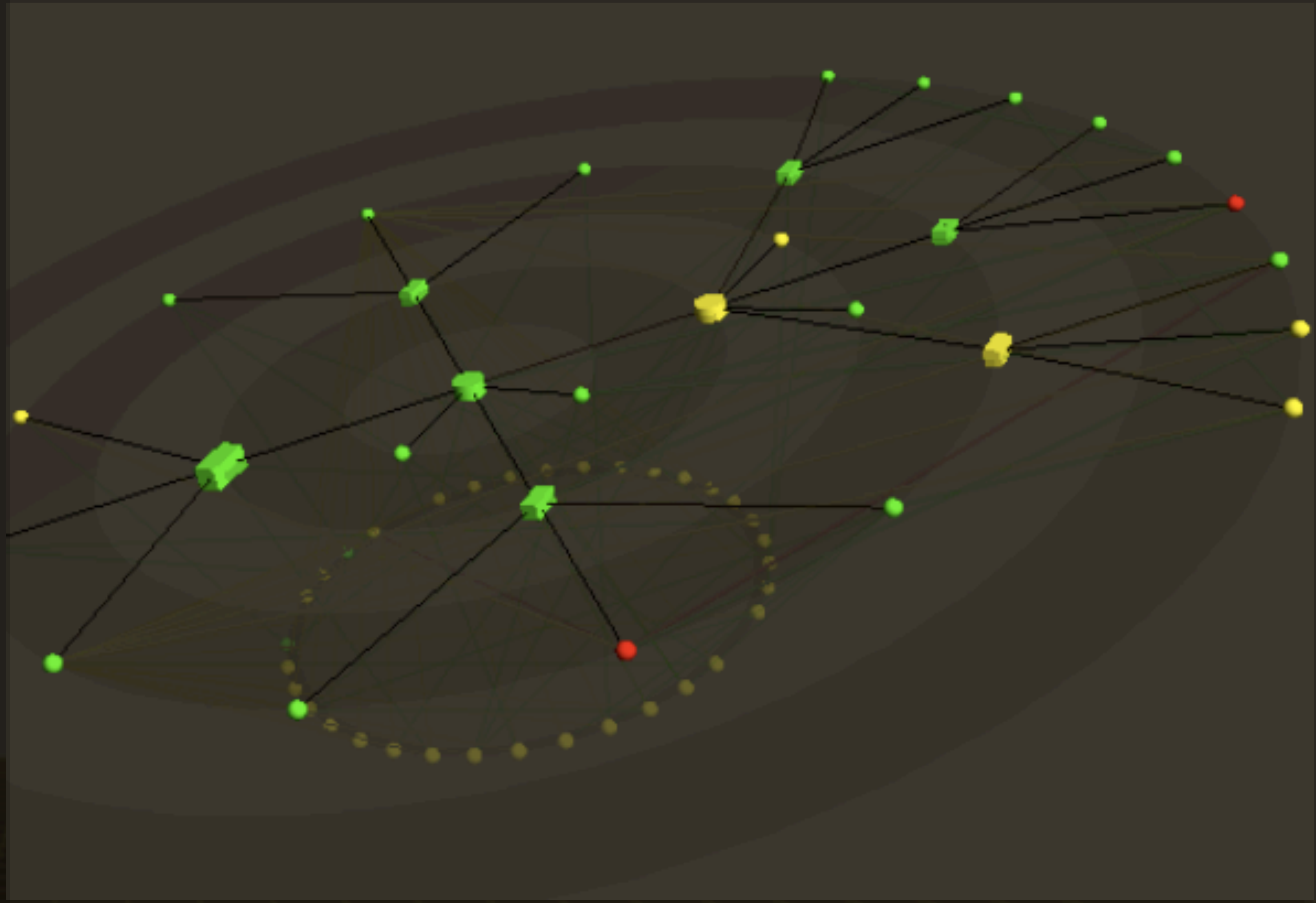
- **Developed visualization module:**
  - Employs OpenGL library
  - Implemented for experimental IDS
- **Operator can perceive:**
  - Duration over time & time of event
  - Interrelations of events within one attack
  - Severity level
  - Component simple event types
  - Event frequencies within attack
  - Target and source host addresses



Such features as rotation and zooming are also implemented

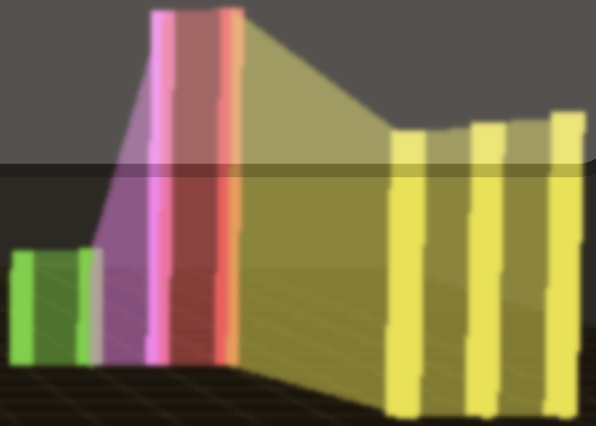
✓ Implemented auxiliary network map/topology module

- Color mapping for severity level
- Different shapes/icons for different host types
- All internal hosts on a one plane
- All external hosts specially distributed in space
- Line connects the source and the target
- Line becomes more transparent in time
- Host information on mouse hover



Future Work

- Make system more user friendly:
  - Adopt natural mouse operations
    - Drag hosts for re-sorting
    - Select events with rectangular area
- Make system more customizable:
  - Custom colors/textures for event types
  - Custom frequency thresholds
  - "On the fly" customization



Questions/ Comments?

Dennis Gamayunov

gamajun@lvk.cs.msu.su

Anatoly Yelizarov

tolya@lvk.cs.msu.su