Visualization of Complex Attacks and State of Attacked Network

Anatoly Yelizarov & Dennis Gamayunov

Department of Computational Mathematics and Cybernetics, Moscow State University
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

- **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
• **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**
Reference Example

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 and Cylindrical visualizations]

- 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