THE OPEN SOURCE VISUALIZATION ENGINE FOR BUSY HACKERS

Thibault Reuille & Andrew Hay

OpenDNS
THIBAULT REUILLE

• Security Researcher at OpenDNS
• Former Software Engineer @ NVIDIA
• MS IT from EPITA: Ingénierie Informatique
• @ThibaultReuille
ANDREW HAY

• Sr. Security Research Lead & Evangelist
• Former research director, industry analyst, security analyst, and engineering/product/program manager
• @andrewsmhay
WHY VISUALIZE THE DATA?
Why Visualize the Data?

- Aren’t pie charts enough?
- What does advanced visualization give us?
- Can’t I just use R or Excel?
Because, Minority Report
QUICK OVERVIEW OF LEARNING STYLES
Learning Styles

- Neil Fleming's VAK/VARK model

- The 4 types
  1. Visual learners
  2. Auditory learners
  3. Reading-writing preference learners
  4. Kinesthetic learners or tactile learners
Learning Styles

- Key concept of visual learning
- Graphic organizers
- Visual representations of
  - knowledge,
  - concepts,
  - thoughts, or
  - ideas

Photo Credit: modellearning
Learning Styles

• Clarify meaning through relationships

• Best example might be utilizing a mind map
Learning Styles

• Representing information spatially and with images [some*] students are able to
  – focus on meaning
  – reorganize and group similar ideas easily
  – make better use of their visual memory

INTRODUCING OpenGraphiti
Introducing OpenGraphiti

- Open Source visualization engine
- Remove the complexity of creating advanced data visualizations
- Visualize any loosely related data
  - without having to endlessly reformat that data
Introducing OpenGraphiti

OpenGL\v|ES

JavaScript

python

OpenCL

black hat
USA 2014
Introducing OpenGraphitti
OpenGraphiti Workflow

Source Data
Convert Data
Visualize Data
THE MATH AND THE PHYSICS PART
The Math and Physics Part

- Graph theory 101
Suppose you have a graph

$$G = (V, E)$$

Where:

$$V = \{0, 1, 2, 3\}$$ and

$$E = \{(0, 1), (0, 2), (1, 2), (2, 3)\}$$
The Math and Physics Part

- This would provide the following graph:
The Math and Physics Part

\[ k = C \sqrt{\frac{\text{area}}{\text{nodes}}} \]

\[ f_a(d) = \frac{d^2}{k} \]

\[ f_v(d) = -\frac{k^2}{d} \]

Repulsion  \hspace{1cm} Attraction
Using OpenGraphiti

- Requirements
  - OS X (10.9 / Mavericks)
  - Python 2.7.x
How to build:
$ git clone <git repo>
$ pip install networkx
$ cd graphiti
$ make clean native

How to run:
$ ./graphiti <options> output.json
Using OpenGraphiti

• The result is something like this
• Malicious domains graph
  – Nuclear exploit kits (pink)
  – Hosting IP addresses (yellow)
Using OpenGraphiti

- OpenDNS uses OpenGraphiti and discussed methodologies
- Ongoing tracking of...
  - CryptoLocker & CryptoDefense ransomware
  - Red October malware
  - Kelihos botnet
  - and more...
Using OpenGraphiti

• The examples in this presentation presume the following...

1. OpenGraphiti requirements are satisfied
2. OpenGraphiti is located in your home directory
e.g. /Users/ahay/graphiti/
3. Semantic-Net is located in your home directory
e.g. /Users/ahay/semanticnet/
OPENGRAPHITI VISUALIZATION EXAMPLES
EXAMPLE 1 – VISUALIZING DIRECTORY STRUCTURE
Visualizing Directory Structure

• Easiest example
• Visualize the file and directory structure of a specified path
• Script provided to generate and convert the data

Photo Credit: ERA GRUP
Visualizing Directory Structure

• Source Data & Convert Data
  
  .*/semanticnet/examples/fs_graph.py  <directory>

  e.g.
  
  $ ./semanticnet/examples/fs_graph.py  /home

• Visualize Data
  
  $ ./graphiti demo  ../*.semanticnet/examples/fs.json
File/Directory Structure... Visualized!
EXAMPLE 2 – VISUALIZING OPENDNS SECURITY GRAPH
Visualizing The OpenDNS Security Graph

- investigate.opendns.com
- Global visibility of attackers’ infrastructures
  - Global network handles two percent of the world’s Internet requests
  - Powers OpenDNS Umbrella and Investigate
  - 50b+ DNS queries per day
The OpenDNS Security Graph... Visualized!
EXAMPLE 3 – VISUALIZING THE VCDB
Visualizing The VCDB

- vcdb.org
- From the Verizon Risk Team
  - Vocabulary for Event Recording and Incident Sharing (VERIS)
  - VERIS Community Database (VCDB)
The VCDB... **Visualized!**
EXAMPLE 4 – VISUALIZING THE INTERNET (VIA ASN)
Visualizing The Internet

- Autonomous System Number (ASN)
- Collection of connected IP routing prefixes
- Common, clearly defined routing policy to the Internet

Source: http://en.wikipedia.org/wiki/Autonomous_System_(Internet)
The Internet... Visualized!
EXAMPLE 5 – VISUALIZING A SHODAN QUERY
Visualizing a SHODAN Query

- www.shodanhq.com
- Lets you find specific computers (routers, servers, etc.) using a variety of filters
- Some have described it as a public port scan directory or a search engine of banners
Visualizing a SHODAN Query

• Source Data & Convert Data

`./semanticnet/examples/shodan_graph.py -k <key> -s <string>`

e.g.

$ ./semanticnet/examples/shodan_graph.py -k shokey -s aws

• Visualize Data

$ ./graphiti demo ..:/semanticnet/examples/shodan_aws.json
A SHODAN Query... Visualized!
Some Other Examples...Visualized!
WHAT ELSE CAN I USE OpenGraphiti FOR?
Use OpenGraphiti...

• Against **any** relational data
  – Network packet captures
  – IDS alerts
    • e.g. Snort, Bro, Suricata, etc.
  – Environmental data
    • e.g. wind, water, earthquake, temperature, tide, soil statistics
  – Odd data
    • e.g. Migratory patterns of the African and European coconut-laden swallow population
Use OpenGraphiti...

- Provided data generation scripts
  - File system *(from Example 1)*
    - `semanticnet/examples/fs_graph.py`
  - SHODAN query *(from Example 5)*
    - `semanticnet/examples/shodan_graph.py`
  - BRO IDS logs
    - `semanticnet/examples/bro_graph.py`
WHAT’S NEXT FOR OpenGraphiti?
OpenGraphiti 1.0++

- Lots of cool things coming
- Can’t do it without the help of the security community
- And Skyler (the Intern)
OpenGraphiti 1.0++

- Explore enhanced human interaction
  - Oculus Rift (DK2 on order)
  - Leap Motion Controller (we have one!)
- More input/output plugins
- More of that physics and math stuff

Photo Credit: http://www.imdb.com/media/rm2660874752/ch0014870
• **OpenGraphiti** is a
  – Free, Open Source, and awesome data visualization tool...
  – Used to visualize **any** relational data as an interactive 2D or 3D model...
  – And is available at:
    http://github.com/opendns/graphiti
QUESTIONS?

Contact Us:
Thibault Reuille, thibault@opendns.com, @ThibaultReuille
Andrew Hay, ahay@opendns.com, @andrewsmhay

www.opendns.com
labs.opendns.com
OpenDNS
github.com/opendns
labs.opendns.com/blog