SESA '16

2016 USENIX Summit for Educators in System Administration

Introductory Information Security Lab

Authors:

Suzanna Schmeelk (Presenter),

Alfred Aho,

Junfeng Yang

DECEMBER 6, 2016
BOSTON, MA

Co-located with LISA16

About The Authors

- **Suzanna Schmeelk –** Dr. Schmeelk is a Senior Security Analyst at Memorial Sloan Kettering Cancer Center in Manhattan, New York. Suzanna holds an Ed.D. in Mathematics Education from Rutgers University and is a Ph.D. student in Computer Science at Columbia University. She holds a MS degrees in Computer Science, a MS degree in Technology Management-Cyber Security and a BS degree in Computer Science with Mathematics. Suzanna has worked and/or interned with MSKCC, Bell Labs, a subsidiary of Bell Labs, eBay, Yahoo!, UC-Berkeley, Battelle and Paradyne. In addition, Suzanna is an Adjunct Associate Professor at UMUC, an instructor at Parsons School of Design in Manhattan and Instructor with Cooper Union. Suzanna's website is http://www.suzannaschmeelk.com.

- **Alfred Aho –** Dr. Aho is the Lawrence Gussman Professor in the Department of Computer Science at Columbia University. He has a Ph.D. in Electrical Engineering/Computer Science from Princeton University. Professor Aho is well known for his papers and books on algorithms and data structures, programming languages, compilers, and the foundations of computer science. Prior to his current position, Professor Aho was Vice President of the Computing Sciences Research Center at Bell Labs, the lab that invented UNIX, C and C++. Dr. Aho's website is www.cs.columbia.edu/~aho.

- **Junfeng Yang –** Dr. Yang is a Computer Science professor at Columbia University; Co-director of Columbia's Software Systems Lab; and Co-founder and CEO of NimbleDroid, a Columbia spin-off in NYC that invents cutting-edge tools to redefine how developers craft awesome apps. Previously he was a consultant and researcher at Microsoft and earned his PhD in Computer Science at Stanford. Junfeng's primary research interests center on making high-performance, reliable, and secure systems. The systems and tools he created have been applied to analyze, test, and run real-world software such as Linux, benefiting hundreds of millions of users. His research has been covered by Communications of ACM, The Register, and numerous sites. His awards include Google Faculty Research Award, Sloan Research Fellowship, Air Force Office of Scientific Research Young Investigator Award, National Science Foundation Career Award, and OSDI Best Paper Award. Dr. Yang's website is www.cs.columbia.edu/~junfeng.

Talk Overview

- We present a introductory lab for Information Security topics.
- The lab introduces information security and system administration concepts to novices of any age group and/or background.
- The talk is interlaced with practitioner advice from executing. the labs multiple times in under an hour with participants with different computer literacy backgrounds and different age ranges.
- The uniqueness of the lab is that it can be widened or narrowed to match required topics, time constraints and cost constraints.

Overarching Challenge?

- How do we effectively introduce core principles of information security to computer novices in a short period of time?

Big Picture Fact

- Lots of people at all levels in society and professional daily life need durable training on information security.

Recent New Articles

In the news



Ransomware attack hit San Francisco train system
USA TODAY - 4 hours ago
The **San Francisco Municipal Transportation Agency** has contained a cyber attack that ...

Muni system hacker hit others by scanning for year-old Java vulnerability
Ars Technica - 4 hours ago

San Francisco Rail System Hacke
Krebs on Security - 15 hours ago



Crisis of the Week: **Dyn's Denial-of-Service** Moment
Wall Street Journal (blog) - Oct 31, 2016
The crisis spotlight shines on **Dynamic** Network Services Inc., a web-technology provider that suffered a massive distributed **denial-of-service** ...

DDoS attack on **Dyn** could have been prevented
CSO Online - Nov 3, 2016

What the **Dyn DDoS** Attacks Taught Us About Cloud-Only EFSS
CloudTweaks News (blog) - Nov 1, 2016



Some **Androi**
Fortune - Nov 15, 2016
Some **Android devices** may be infected with software that tracks users' phone calls, text messages, and other **data**, and then sends that ...

Android phones **leaking** private **data** to China
MyBroadband - Nov 16, 2016

Android Smartphone Manufacturer Blu is secretly **leaking** your text ...
Reporter Times - Nov 16, 2016

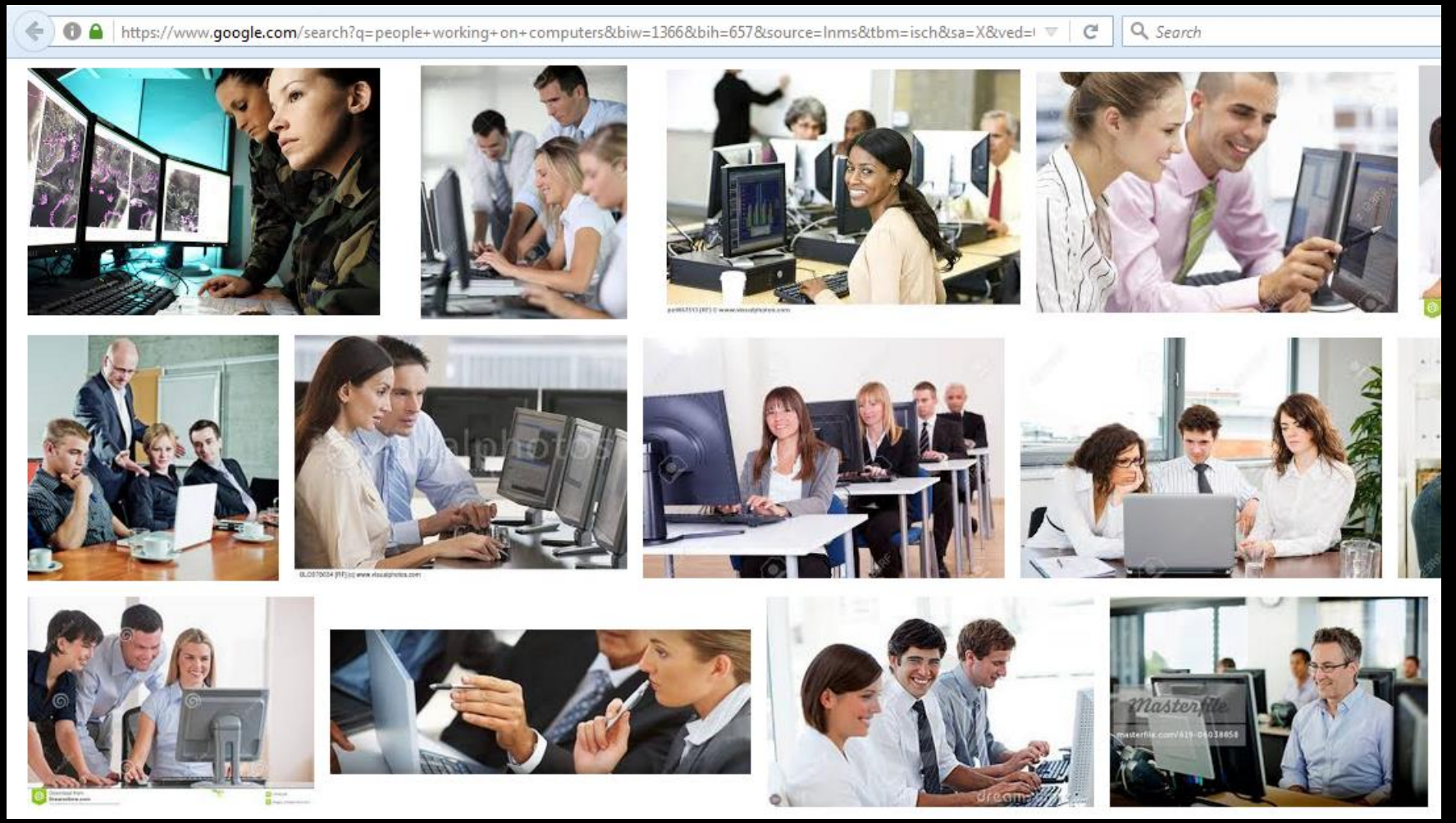
Education Silo Challenges

- It turns out that cyber security is really only taught in special programs and/or a few courses at some universities.
- At most, colleges teach best practices and ask students to read and/or acknowledge school computing policies.
- How do students with diverse computer training backgrounds enter Info Sec with agility?

Cost Challenges

- Much training is left as either
  - On-the-job training or
  - College credits
- This can be $$$$ (e.g. $2K/person)
- In organizations of 20K people, can they afford to train people at a rate of $2K plus time and travel?
- Many places ask employees to do it on their own time or give mandatory online module to view.

Information Security Learning



Background Challenges

- How to quickly train students with diverse backgrounds quickly and in ad-hoc settings?
- Learners:
  1. Field experts (e.g. recipients of Wolf Prizes, Fields Medals, Nobel Prizes, etc.)
  2. C-suites executives
  3. Student novices and
  4. Other learners inside an organization

Environment Challenges

- Parameters:
  - Quick
  - Ad Hoc
  - Cost Range ($ to $$$)
  - Durable
  - Any age
  - Any computer literacy level

Finding a Solution for Challenges?

- Looked online for training, but …
- We could not identify a match for our needs
- So, …

We had to Invent a Solution

- Designed a lab:
  - Met wide-range of needs
  - With parameters given on prior slides
  - Time Ranges (short – to –long)
  - Content Ranges
  - Teachable Moments

Question

- What guided the construction of our lab?

Robert B. Davis, "Learning Mathematics (1984)"

- Assimilation Paradigm
- Which has been show by many mathematics eduction researchers to be a durable technique over time:
  - Davis & Maher (1998)
  - Maher, Martino, & Alston (1993)
  - Speiser, Walter & Maher (2003)
  - Schmeelk (2010)
  - Yankelewitz, Mueller & Maher (2010)

Assimilation Paradigm

- Davis and Maher (1993):
  - Describe assimilation paradigms
  - Using Piagetian language
  - As a a set of information processing activities in which the learner sees a new experience as “just like” or “similar to” some recalled earlier experience.
  - New experiences create opportunities for the learner to organize and work with data.

Assimilation Paradigm

- Using a 'Paradigm' Teaching Strategy (Davis, 1984).
- These data are internalized through a learner's well-coordinated actions on objects that may occur in response to explorations of a **problematic situation** (Maher, 1998).

‘Paradigm’ Teaching Strategy

- The learner responds by drawing upon existing mental representations that are already built.
- As new data are entered by the learner, these representations are either validated, modified or rejected on the basis of the fit with existing knowledge structures.

Carefully Chosen Problem Solving Activities

- Following a 'Paradigm' Teaching Strategy
- May trigger the construction of a more adequate representation and provide the learner incentive to reorganize or extend their available existing knowledge.
- (Davis, 1984; Davis and Maher, 1997; Maher et al., 1993)

Carefully Chosen Problem Solving Activities

- Durable Ideas
- Isomorphic Information Security Problems
- Flexible Lab Time Lengths
- Constructivist Learning Approach
- Targets Any Background
- Targets Any Cost Range
- Adaptable
- Hands-On
- Develop learners personal representation of problem (i.e., “just like”, “similar to”)

An abbreviated lab overview

Lab: Three-Step Overview

- ***Step 1*** – Prepare Lab (20min +)
- ***Step 2*** – Students Collect Data (10min +)
- ***Step 3*** – Students Analyze Data (20min +)
- ***Step 4 – (Optional)*** Winning Team(s) (5min +)

Lab: Step 1 – Prepare Lab

- ***Prepare devices***
- ***Set-Up Accounts***
- ***Install Software***
- ***Arrange devices***
- ***Set-up website***

Lab: Step 2 –Students Collect Data

- ***Students log into Standard User account***
- ***Students Browse Internet***
- ***Browsing Theme***
  - ***Guided by Website***
  - ***Short relevant Task(s)***
- ***Give each Student in pair a Chance to Drive***
- ***Timing: Depends on Lab Parameters***

Lab: Step 2 –Website

- ***Goal relevant to student background***
- ***Assortment of teachable links***
  - ***Save Paper***
  - ***Save Time***
- ***Examples listed at:***
  - ***http://www.technologyinthepark.com/USENIX-SESA16/index.html***

COLUMBIA | ENGINEERING
The City University of New York School of Engineering and Applied Science
Memorial Sloan Kettering Cancer Center

http://www.technologyinthepark.com/USENIX-SESA16/Lab1.html

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

- Lab Home
- Lab1: Office Ex.
- Lab2: Undergrads
- Lab3: Grades 9-12
- Lab4: Grades 6-8
- Lab5: Grades K-5

Level: Mini-Power Office Training

Theme: Plan a CEO Party

Use a few of these links

- Bing
- PartyCity
- Bloomingdales
- California Pizza Kitchen

Use a few of these links

- Yahoo
- Google

DECEMBER 6, 2016
BOSTON, MA
Co-located with LISA16

SESA '16
2016 USENIX Summit for Educators in System Administration

http://www.technologyinthepark.com/USENIX-SESA16/Lab2.html

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

- Lab Home
- Lab1: Office Ex.
- Lab2: Undergrads
- Lab3: Grades 9-12
- Lab4: Grades 6-8
- Lab5: Grades K-5

Level: Undergraduates

Theme: Plan a Research Experience for Undergraduates (REU)

Use a few of these links

- Bing
- Target
- Macy's
- eBay

Use a few of these links

- Bing
- Google

DECEMBER 6, 2016
BOSTON, MA
Co-located with LISA16

SESA '16
2016 USENIX Summit for Educators in System Administration

http://www.technologyinthepark.com/USENIX-SESA16/Lab3.html



Lab Home

Lab1: Office Ex.

Lab2: Undergrads

Lab3: Grades 9-12

Lab4: Grades 6-8

Lab5: Grades K-5

Level: Grades 9-12

Theme: Plan for Graduation

Use a few of these links

- Nordstrom
- Rutgers University
- Columbia University
- Uni. CA at Berkeley

Use a few of these links

- Bing
- Yahoo

DECEMBER 6, 2016
BOSTON, MA
Co-located with LISA16

SESA '16
2016 USENIX Summit for Educators in System Administration

http://www.technologyinthepark.com/USENIX-SESA16/Lab4.html

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

- Lab Home
- Lab1: Office Ex.
- Lab2: Undergrads
- Lab3: Grades 9-12
- Lab4: Grades 6-8
- Lab5: Grades K-5

Level: Grade 6-8

Theme: Plan a Summer Camp

Use a few of these links

- Container Store
- Walmart
- Ask
- Camp Stuff 4 Less

Use a few of these links

- Dogpile
- Google

DECEMBER 6, 2016
BOSTON, MA
Co-located with LISA16

SESA '16
2016 USENIX Summit for Educators in System Administration

http://www.technologyinthepark.com/USENIX-SESA16/Lab5.html

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Lab Home

Lab1: Office Ex.

Lab2: Undergrads

Lab3: Grades 9-12

Lab4: Grades 6-8

Lab5: Grades K-5

Level: Grades K-5

Theme: Let's Play Games

Use a few of these links

- KidsGames
- AOL Search
  - Disney
  - Mattel
  - NickJr
  - Nick

Use a few of these links

- Google
- Scratch

DECEMBER 6, 2016
BOSTON, MA
Co-located with LISA16

SESA '16
2016 USENIX Summit for Educators in System Administration

Lab: Step 3 – Students Analyze Data

- *Rotate Devices (optional)*
- *Students Analyze*
  - *System Administrator Account*
  - *Standard User Account*
- *Timing: Depends on topic depth and breadth*

Students Analyze Data: As Sys Admin

- *Teachable Moments*
  - *Wireshark – Network Protocol Analyzer*
    - *Filter Commands*
    - *TCP Follow Stream*
    - *Network Protocols*
  - *Secure Applications*
  - *Encryption*
  - *Transport Layer Security (e.g., TLS & SSL)*
  - *Ethics (e.g., Black Hat & White Hat)*
  - *Privacy & Security*

Students Analyze Data: As Stdn User

- *Teachable Moments*
  - *Safe Browsing*
    - *Browsing History*
    - *Browsing Certificates (e.g. "Lock" icon)*
    - *Downloads*
    - *Cookies*
    - *Browsing Privacy*
  - *Sharing Devices*
    - *Internet Cafes*
    - *Sharing accounts*
    - *Information Security Hygiene*

The Next Lab(s)

- *Cross Site Scripting (XSS)*
  - *Cookies*
  - *Proxy (e.g., https://portswigger.net/burp/download.html)*
- *Cross Site Request Forgery (XSF)*
- *Confidentiality*
  - *Encryption*
    - *Browser Certificates*
    - *Session Protocols (e.g., OAuth, etc.)*
    - *Cipher Strengths (e.g., 3DES, RSA, etc.)*
- *Integrity*
  - *Digital Signatures*
  - *Hash Algorithms (e.g., MD5, SHA, etc.)*
- *Availability*
- *RESTful APIs*

The End

- Thank you for coming to USENIX-SESA'16!
- We have included an Appendix
  - Lab details
  - To help you get started

Appendix: A Guide to InfoSec Lab

- Detailed reference for USENIX posterity
- Download PPT from USENIX
- Play IT
- Note. PPT Slides are viewable on mobile device while setting-up

SESA '16

2016 USENIX Summit for Educators in System Administration

Introductory Information Security Lab

Authors:

Suzanna Schmeelk (Presenter),

Alfred Aho,

Junfeng Yang

DECEMBER 6, 2016
BOSTON, MA

Co-located with LISA16

Lab: 3 Step Overview

- ***Step 1*** – Prepare Lab (20min +)
- ***Step 2*** – Students Collect Data (10min +)
- ***Step 3*** – Students Analyze Data (20min +)
- ***Step 4 – (Optional)*** Winning Team(s) (5min +)

Lab: Step 1 – Prepare Lab

- ***Prepare devices***
- ***Set-Up Accounts***
- ***Install Software***
- ***Arrange devices***
- ***Set-up website***

Step 1 – Prepare Lab: Devices

- ***Device Forms***
  - ***Laptops***
  - ***Desktops***
  - ***Tablets***
- ***Any Operating System***
- ***Must support***
  - ***Two accounts***
  - ***One account must run Wireshark***
- ***Timing: Depends if previously set-up***

Lab: Step 1 – Prepare Lab

- *Collect devices - Any OS which support below*
- *Set-Up Two Accounts*
  - *Standard User, and*
  - *Administrator*
- *Install Software*
  - *Administrator – https://www.wireshark.org/*
  - *Standard User – Browser (e.g., IE, Firefox, etc.)*
- *Set-up devices*
- *Set-up website*

Lab: Step 1 – Before Students Arrive

- ***Turn on devices***
- ***Prepare Accounts***
  - ***Standard User***
    - ***Clear Browser History***
    - ***Configure Browser Home Page to Lab Website***
  - ***Administrator***
    - ***Using Wireshark to Collect Network Traffic***
    - ***Leave Wireshark Collecting Network Traffic***
    - ***"Switch User" (i.e., OS Dependent - Don't log-off)***
- ***Arrange devices – one device per student pair***
- ***Create lab website – to guide browsing exercise***

Lab: Step 2 –Students Collect Data

- *Students log into Standard User account*
- *Students Browse Internet*
- *Browsing Theme*
  - *Guided by Website*
  - *Short relevant Task(s)*
- *Give each Student in pair a Chance to Drive*
- *Timing: Depends on Lab Parameters*

Lab: Step 2 –Website

- ***Goal relevant to student background***
- ***Assortment of teachable links***
- ***Examples:***
  - ***http://www.technologyinthepark.com/USENIX-SESA16/index.html***
  - ***http://www.technologyinthepark.com/USENIX-SESA16/Lab1.html***
  - ***http://www.technologyinthepark.com/USENIX-SESA16/Lab2.html***
  - ***http://www.technologyinthepark.com/USENIX-SESA16/Lab3.html***
  - ***http://www.technologyinthepark.com/USENIX-SESA16/Lab4.html***
  - ***http://www.technologyinthepark.com/USENIX-SESA16/Lab5.html***

http://www.technologyinthepark.com/USENIX-SESA16/Lab1.html



- Lab Home
- Lab1: Office Ex.
- Lab2: Undergrads
- Lab3: Grades 9-12
- Lab4: Grades 6-8
- Lab5: Grades K-5

Level: Mini-Power Office Training

Theme: Plan a CEO Party

Use a few of these links

- Bing
- PartyCity
- Bloomingdales
- California Pizza Kitchen

Use a few of these links

- Yahoo
- Google

DECEMBER 6, 2016
BOSTON, MA
Co-located with LISA16

SESA '16
2016 USENIX Summit for Educators in System Administration

http://www.technologyinthepark.com/USENIX-SESA16/Lab2.html

- Lab Home
- Lab1: Office Ex.
- Lab2: Undergrads
- Lab3: Grades 9-12
- Lab4: Grades 6-8
- Lab5: Grades K-5

Level: Undergraduates

Theme: Plan a Research Experience for Undergraduates (REU)

Use a few of these links

- Bing
- Target
- Macy's
- eBay

Use a few of these links

- Bing
- Google

DECEMBER 6, 2016
BOSTON, MA
Co-located with LISA16

SESA '16
2016 USENIX Summit for Educators in System Administration

http://www.technologyinthepark.com/USENIX-SESA16/Lab3.html

- Lab Home
- Lab1: Office Ex.
- Lab2: Undergrads
- Lab3: Grades 9-12
- Lab4: Grades 6-8
- Lab5: Grades K-5

Level: Grades 9-12

Theme: Plan for Graduation

Use a few of these links

- Nordstrom
- Rutgers University
- Columbia University
- Uni. CA at Berkeley

Use a few of these links

- Bing
- Yahoo

DECEMBER 6, 2016
BOSTON, MA
Co-located with LISA16

SESA '16
2016 USENIX Summit for Educators in System Administration

http://www.technologyinthepark.com/USENIX-SESA16/Lab4.html

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

- Lab Home
- Lab1: Office Ex.
- Lab2: Undergrads
- Lab3: Grades 9-12
- Lab4: Grades 6-8
- Lab5: Grades K-5

Level: Grade 6-8

Theme: Plan a Summer Camp

Use a few of these links

- Container Store
- Walmart
- Ask
- Camp Stuff 4 Less

Use a few of these links

- Dogpile
- Google

DECEMBER 6, 2016
BOSTON, MA
Co-located with LISA16

SESA '16
2016 USENIX Summit for Educators in System Administration

http://www.technologyinthepark.com/USENIX-SESA16/Lab5.html



Lab Home

Lab1: Office Ex.

Lab2: Undergrads

Lab3: Grades 9-12

Lab4: Grades 6-8

Lab5: Grades K-5

Level: Grades K-5

Theme: Let's Play Games

Use a few of these links

- KidsGames
- AOL Search
  - Disney
  - Mattel
  - NickJr
  - Nick

Use a few of these links

- Google
- Scratch

DECEMBER 6, 2016
BOSTON, MA
Co-located with LISA16

SESA '16
2016 USENIX Summit for Educators in System Administration

Lab: Step 3 – Students Analyze Data

- *Rotate Devices (optional)*
- *Students Analyze*
  - *System Administrator Account*
  - *Standard User Account*
- *Timing: Depends on topic depth and breadth*

Students Analyze Data: As Sys Admin

- *Students Log-in as System Administrators*
- *Save Wireshark Data into PCAP File*
  - *E.g., infosec_lab4_12_6_2016_4pm.pcap*
- *Students browse PCAP file in Wireshark*

Students Analyze Data: As Sys Admin

- *Teachable Moments*
  - *Wireshark*
    - *Filter Commands*
    - *TCP Follow Stream*
    - *Network Protocols*
  - *Secure Applications*
  - *Encryption*
  - *Transport Layer Security (e.g., TLS & SSL)*
  - *Ethics (e.g., Black Hat & White Hat)*
  - *Privacy & Security*

Students Analyze Data: As Stdn User

- *Teachable Moments*
  - *Safe Browsing*
    - *Browsing History*
    - *Browsing Certificates (e.g. "Lock" icon)*
    - *Downloads*
    - *Cookies*
    - *Browsing Privacy*
  - *Sharing Devices*
    - *Internet Cafes*
    - *Sharing accounts*
    - *Information Security Hygiene*

Lab: Step 4 – Winning Team(s)

- *Optional Step*
- *Decide which team*
  - *Collected the most information*
    - *System Administrator*
    - *Standard User*
  - *Used the most Wireshark filters*
- *Present "White Hat" Awards!*

The Next Lab(s)

- *Cross Site Scripting (XSS)*
  - *Cookies*
  - *Proxy (e.g., https://portswigger.net/burp/download.html)*
- *Cross Site Request Forgery (XSF)*
- *Confidentiality*
  - *Encryption*
    - *Browser Certificates*
    - *Session Protocols (e.g., OAuth, etc.)*
    - *Cipher Strengths (e.g., 3DES, RSA, etc.)*
- *Integrity*
  - *Digital Signatures*
  - *Hash Algorithms (e.g., MD5, SHA, etc.)*
- *Availability*
- *RESTful APIs*

References

- Davis, R. B. (1984). Learning mathematics: the cognitive science approach to mathematics education. London: Croom Helm.
- Davis, R. B., & Maher, C. A. (1998). Introduction. In: C. Maher (Ed.), Can teachers help children make convincing arguments? A glimpse into the process (p. 13). Rio de Janeiro, Brazil: Universidade Santa Ursula.
- Davis, R. B., & Maher, C. A. (1997). How students think: the role of representations. In: L. English (Ed.), Mathematical reasoning: analogies, metaphors, and images (pp. 93–115). Hillsdale, NJ: Lawrence Erlbaum Associates.
- Davis, R. B., & Maher, C. A. (1993). What are the issues? In: R. B. Davis, & C. A. Maher (Eds.), Schools, mathematics, and the world of reality (pp. 9–34). Boston: Allyn and Bacon.

References

- Maher, C. A., Davis, R. B., & Alston, A. S. (1993). Brian's representation and development of mathematical knowledge: the first two years. In: R. B. Davis, & C. A. Maher (Eds.), Schools, mathematics, and the world of reality. Boston: Allyn and Bacon.
- Maher, C. A., Martino, A. M., & Alston, A. S. (1993). Children's construction of mathematical ideas. In: Contexts in mathematics education conference proceedings, MERGA 16. Brisbane, Australia.
- Schmeelk, S. (2010) An Investigation of Fourth Grade Students Growing Understanding of Rational Numbers. Unpublished doctoral dissertation, Rutgers, The State University of New Jersey, New Brunswick.

References

- Speiser, R., Walter, C., & Maher, C. A. (2003). Representing motion: An experiment in learning. *The Journal of Mathematical Behavior, 22*(1), 1-35.
- Steencken, E. P. & Maher, C. A. (2003). Tracing fourth graders' learning of fractions: Episodes from a yearlong teaching experiment. The Journal of Mathematical Behavior, 22(2), 113-132.
- Yankelewitz, Y., M. Mueller and C. A. Maher. (2010). A task that elicits reasoning: A dual analysis. Journal of Mathematical Behavior, 29, 76-85.

Further Viewing on Learning http://www.videomosaic.org/

