Cyber Security Education in San Antonio:

The First Fifteen Years, and Connections to Computational Thinking

Cliff Zintgraff, Ph.D.
IC² Institute, The University of Texas at Austin
SASTEMIC *STEM non-profit in San Antonio*

Joe Sanchez
CyberTexas Foundation

Michael Maldonado
Southwest ISD

ISTE 2017 CS Firehose
June 24, 2017

Lutheran High School, San Antonio. http://www.lhssa.org/cyberpatriot/

Goals for our Session

Share broad overview of K-12 cyber security education in San Antonio

Frame that education

- *As important to our region's high-tech development*
- *As advancing Computational Thinking in students*

Demonstrate how these programs developed

- *Via community leadership*
- *Via educational leadership*

On-the-ground program descriptions

Two Reasons We Think This is Interesting

San Antonio had 200+ teams, high school and middle school, in the 2016-2017 CyberPatriot competition.

San Antonio has the second highest # of certified information security professionals in the U.S.

CyberPatriot 2012 Open Division National Champions from the Information Technology and Security Academy (ITSA). With Mayor Julian Castro.

The First Fifteen+ Years

- **Decades Ago**
  Air Intelligence Agency, other functions, located in San Antonio.
- **~2000: University**
  UTSA, Center for Infrastructure Assurance and Security (CIAS)
- **2002: Grades 11-12**
  2002, Information Technology and Security Academy (ITSA)
- **2005: University expansion**
  Cyber Innovation and Research Consortium (CIRC)
  Multiple NSA and DHS Centers of Academic Excellence
  NCCDC (collegiate competition)

The First Fifteen+ Years

- **2008: High school,** extracurricular
  Cyber Patriot. Over 100 teams in 2014-2015. 200+ in 2017.
  Open Division Champions, 2012
- **2009: 24th Air Force**
- **~~2012~~ 2003: High School certification programs**
  Four years, IT, cyber, certifications
- **2013: Middle school, extracurricular**
  Cyber Patriot / CyberStar
- **2014: Middle school curricular**
  Cyber program at Southwest ISD

Information Technology and Security Academy (ITSA)

Partnership between San Antonio cyber security industry, 17 San Antonio locally-controlled school districts, and community college.

http://www.youtube.com/watch?v=PrqEEpi-mrQ

- 11th and 12th grade
- Central campuses
- Academic and technical courses
- Industry internships
- 27 hours of dual credit
- Articulates into multiple local college programs

CyberPatriot

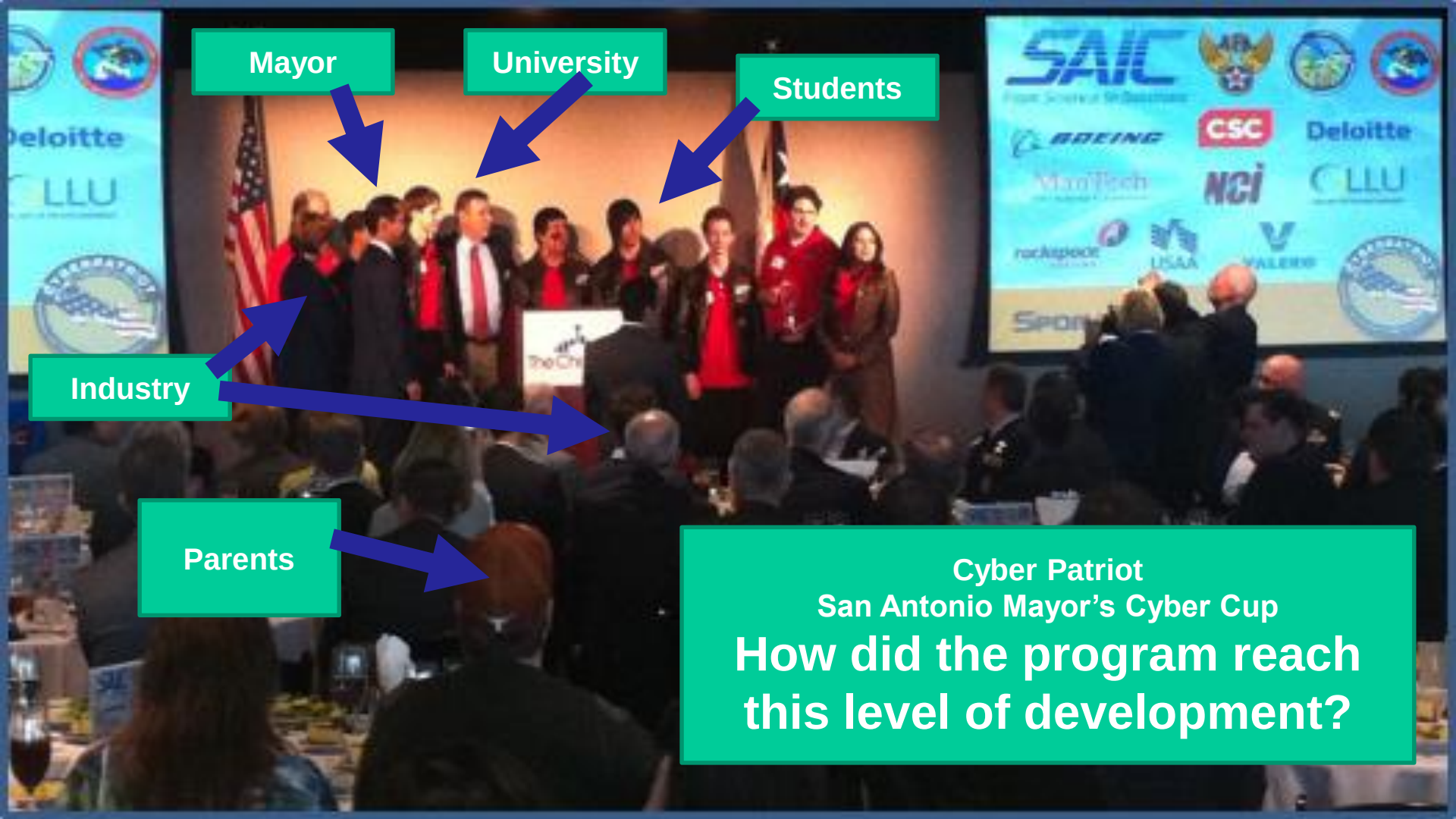
The [CyberPatriot] competition puts teams of high school and middle school students in the position of newly hired IT professionals tasked with managing the network of a small company. https://www.uscyberpatriot.org/

http://www.24af.af.mil/News/Article-Display/Article/458646/24th-air-force-recognizes-top-cyberpatriot-iv-teams/

Cyber Patriot

San Antonio Mayor's Cyber Cup

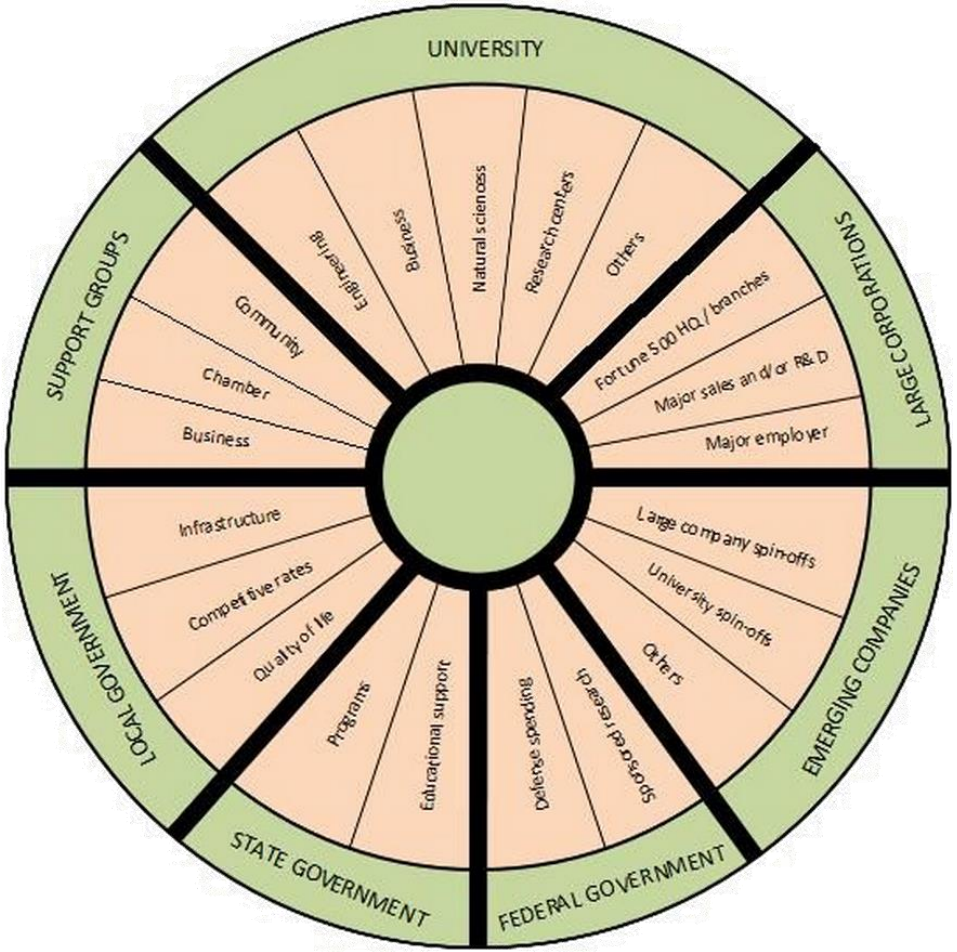
What is happening here?


Mayor
University
Students
Industry
Parents
SAIC
Deloitte
LLU
CSC
NCI
USAA
Cyber Patriot
San Antonio Mayor's Cyber Cup
How did the program reach this level of development?

Technopolis Wheel

Universities
Large Corporations
Emerging Companies
Federal Government
State Government
Local Government
Support Groups

Kozmetsky & Gibson (1988)
Gibson & Butler (2013)



Cyber Security Education & Computational Thinking Survey

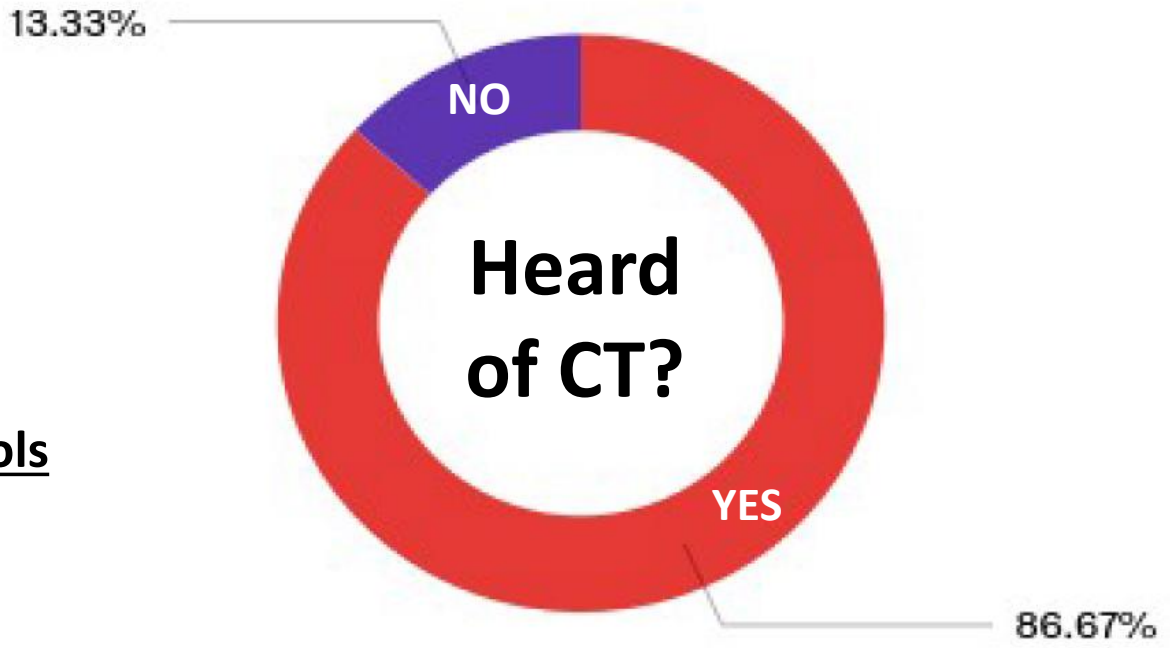
Concept/Capability (Barr & Stephenson, 2011)	Computational Thinking: Cyber Security Learning Activity Cliff's 2013 Speculations — Orange = just an example I highlighted
Data Collection	• **Collect up-to-date lists of vulnerabilities.** • Maintain a list of computer IP addresses.
Data Analysis	• Analyze recorded intrusion attempts manually. • Write programs to track and analyze attempts.
Data Representation	• Interpret common data formats for viruses. • Interpret data in defense against intrusion attempts. • Enter new virus types into databases. • Code lists of configuration setting vulnerabilities. • **Create charts, graphs and statistical representations of possible vulnerabilities and actual activity.** • Write reports on vulnerability attempts.
Problem Decomposition	• Using symptoms from an intrusion attempt, use a decomposition to identify possible vulnerabilities.
Abstraction	• Recognize and categorize vulnerabilities using common attributes. • Understand abstract concepts necessary for use of operating system tools. • Create variations of defensive operations from general tactics.
Algorithms and Procedures	• Study protection algorithms. • **Develop procedures to secure a computer.** • Develop programs to secure a computer.
Automation	• Develop programs. • Automate virus update procedures. • Scan your network for vulnerabilities.
Parallelization	• Study denial of service attacks. • Use multi-computer strategies to defend against intrusions.
Simulation	• Create machine images for competitions.

2017 Update: Educator Survey

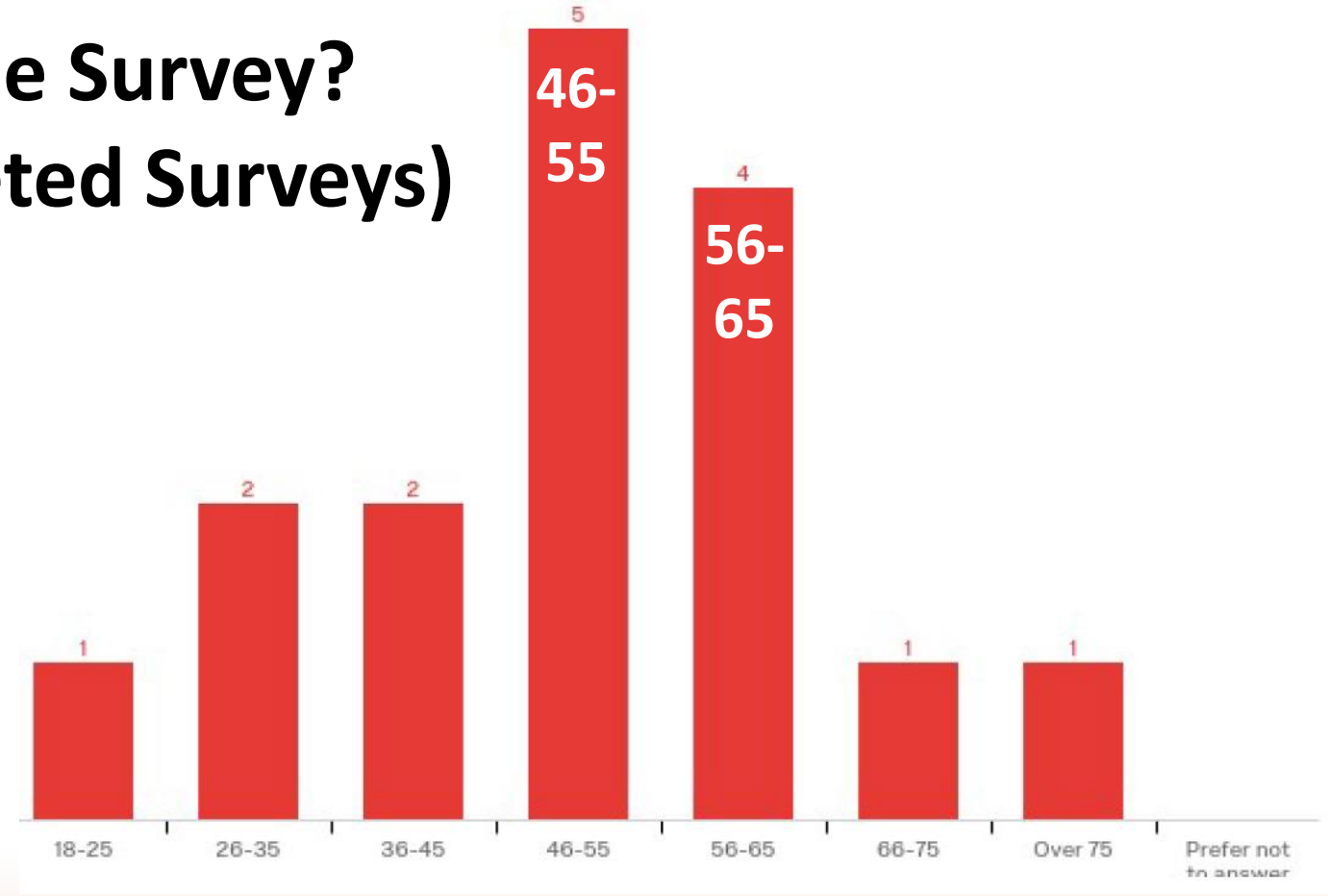
- Participants: K-12 cyber security educators
- Questions about their overall understanding of CT
- Questions about 9 CT attributes
  - Open-ended comments
  - Rating of relevance for cyber security education

Who Took the Survey?

- 30 people answered the opening questions.
- **16 fully completed** the survey.
- **11 of 16 were male**.
- **13 of 16 work in high schools** (others in middle schools).

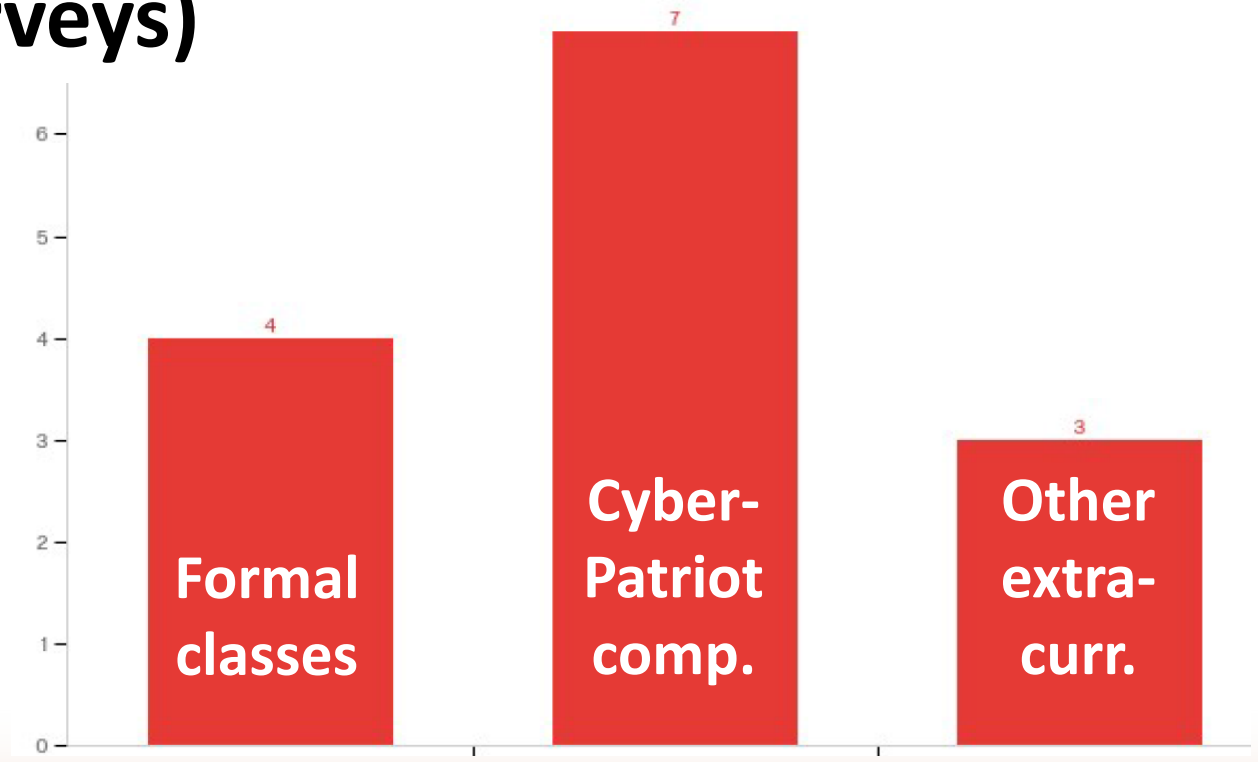


Who Took the Survey?
Age (Completed Surveys)



Who Took the Survey? What they teach. (Completed Surveys)

San Antonio
Austin
Houston
Junction
Kansas City
Lincoln
Evansville
Chicago
Milwaukee
Durham
New Jersey
Lagos



Understanding of CT: Quotes

"A twenty-first century skill that everyone should strive to obtain."

Math, logic

- Solving problems with computations and logic.
- It's just like arithmetic.
- Thinking that involves numbers.
- Thinking that involves math.

Think like a computer

- **Thinking like the computer.**
- The skills and dispositions that computer scientists (and all people working with computers) use when using computers to solve problems and ideate with them.
- Uses the power of computing to solve real world problems and expressing those in a way the computer can understand.

A few talked about: Algorithms, Decomposition, Patterns, Abstraction

- Problem-solving in an algorithmical way.
- Thinking logically, in sequence. Breaking a task down into smaller pieces to figure out how to complete it.
- Decomposing complex problems into tractable pieces
- …four key components: **decomposition, pattern matching, abstraction, and algorithms**.

Other

- …in ways that a **computer, whether a person or a machine**, can successfully carry out…
- Just another **edubabble** term.

Nine CT Attributes in <5 minutes…

- As a way to introduce you to what happens in Cyber Security education.
- To get these CT attributes on the table as you listen to Joe and Mike.
- To share results...

- **NOTE**: Please help me help you get past the fancy words.

Data Collection

- Collection…of a wide variety of data, both from **workstations**, **servers** and the **network** itself.
- Collect data in the form of **logs and audit trails**.
- Collecting data available **about a person or activity**.
- Recording sample discrete data **from high web traffic**
- Designing **surveys** to gather information as to how computer programs can affect an individual's privacy.

Data Analysis

Analyzing network configuration data

- They must review and analyze data regarding ip addresses, and desired configurations (customer specs) to design and protect a network.

Analyzing network traffic and logs / using tools

- Unusual network traffic patterns, hardware failures, and security breaches.
- Looking at logs of application processing and analysis with software such as Wireshark
- Using regexes to validate data and to guard against code injection.

Analyzing user surveys

- Survey administration…analyzing the results

Statistical analyses

- Looking for patterns, performing statistical analysis including sorting, searching, calculating
- Confidence intervals, graphing, linear regression or hypothesis testing.

Data Representation

Presenting data to others

- Graphical representations: pie charts, bar graphs, dot plots, box plots, stem plots, normal probability graphs, line graphs, linear regression, and non-linear regression.
- Graphic/charting survey or experiment results.
- **Making an infographic**.
- They can use various tools to present data--is a spreadsheet, chart, or graph best?

Changing representation to support analysis

- Mapping of data to find patterns, binary representations, numerical representations, categorical representations.

Changing representation to help protect data

- A significant amount of though [sic] has to given to how to best store it in the event its contents have to be protected and the cost of encrypting and decrypting has to be kept in mind.

Problem Decomposition

Problem decomposition – specific case

- Students may be given a case study or specific problem to solve related to security.

Process decomposition

- Determine…tasks that must be performed [to address an issue], and the associated constraints.
- Students may use decomposition in creating scripts to automate security tasks.

Data-oriented decomposition

- Breaking down 'unsolvable' cyber attack data; Observing the trends in some decompose cyber attack data
- **identifying what information is known and what information must be determined**.

Systems decomposition

- …the solution to the problem may be subject to attack and therefor the systems and subsystems involved must be also protected.

Out of reach

- This was beyond what I could teach and instruct my students.

Abstraction

Recognizing vulnerabilities, attack patterns

- We teach about patterns regarding how computers are compromised.
- Pattern-matching (related to abstraction) is important in areas such as determining characteristics of social engineering attacks and insider threats.

Configuration as abstraction

- Abstraction can be part of establishing rules for firewalls, etc.

Procedures/coding as abstraction

- identifying what must be calculated in an algorithm before knowing how to calculate it.
- Writing sentinel code that detects different types of threats. Modularizing.
- Creating scripts to automate tasks.

In problem solving

- **Determining what parts of a problem are missing**, and what parts have yet to be solved
- Well, ideas in cyber security is more a mental process then working on an event such as an attack. Having an idea, might help, but a real practical solution is needed and a **person might come up with several ideas before creating a real solution.**

Algorithms and Procedures

Development and execution of procedures

- Detecting the average cost and critical points of a cyber attack processes data.
- You write procedures that might be bundled in regular expressions.
- **Procedures are all over the place in the various policies used to keep computer systems and networks secure.**

Programming (or not)

- Programming (writing functions).
- Formal algorithms are largely hidden from student view.

Automation

Apply automation tools

- Pre scheduling events on a cyber data processes.
- Scheduled tasks, automatic updates, automatic scans, scripting, etc. At the intro level, students mostly use and enable automation, rather than create it.

Creating automation

- Some students will be able to write scripts to automate security settings, but [see below].
- Writing scripts and programs that harvest data in a safe manner.
- Programming (writing functions).

Not done – much creation of automation

- [Scripts are] typically [written] only by more advanced students.

Parallelization

Using tools that run parallel processes

- Java8 parallelStreams speed up the acquisition of data.
- …using virtualization…students need to consider what can be done in parallel, and what can't, in order to be efficient at solving their challenges.

Not done – much creation of automation

- This concept was way beyond the thinking of my students.

Simulation

Stress testing to expose vulnerabilities

- Testing of cyber data automation process before the real life application of such [CZ: This is similar to software testing].
- Simulation includes the modeling of a situation which generates data for analysis such as the rolling of dice, the flip of a coin, the creation of passwords.
- Testing vulnerabilities by generating a suite of threats that have a random component.

The test environment itself

- **Much of what we do is done in a simulated environment using virtual machines. [CZ: This was stated three times.]**

Cyber Security Education Effectiveness Teaching CT Attributes, High to Low

★ = higher disagreement

CT Concept / Capability Barr & Stephenson (2011)	*Average* *1 (low) to 10 (high)*	*Std Dev*	
1. Simulation	7.88	1.86	
2. Data Analysis	7.56	1.55	
3. Algorithms and Procedures	7.44	2.03	
4. Problem Decomposition	7.38	2.36	★
5. Data Collection	7.19	1.83	
6. Abstraction	7.13	1.67	
7. Parallelization	7.00	1.51	
8. Automation	6.69	1.96	
9. Data Representation	6.50	2.34	★
	7.19	**1.90**	

Cyber Security Education in San Antonio:

The First Fifteen Years, and Connections to Computational Thinking

Cliff Zintgraff, Ph.D.
IC² Institute, The University of Texas at Austin
SASTEMIC

Joe Sanchez
CyberTexas Foundation

Michael Maldonado
Southwest ISD

ISTE 2017 CS Firehose
June 24, 2017

Lutheran High School, San Antonio. http://www.lhssa.org/cyberpatriot/