A ``DIVERGENT''-THEMED CTF AND URBAN RACE FOR INTRODUCING SECURITY AND CRYPTOGRAPHY

Motivation

Curriculum

CTF

Storyline

Security Jeopardy!

Urban race

Why?

Using the material

A ``DIVERGENT''-THEMED CTF AND URBAN RACE FOR INTRODUCING SECURITY AND CRYPTOGRAPHY

Motivation

Curriculum

CTF

Storyline

Security Jeopardy!

Urban race

Why?

Using the material

Motivation

Expanding the security pipeline

Introduce students to computer security early

Camps and classes
- CyberDiscovery, CyberPatriot, CyberAcademy, GenCyber

Capture-the-Flag (CTF) security games
- picoCTF, hs-CTF, abctf

This work

Combined camp and CTF for introducing security topics in an engaging way

Focus on intrinsic motivation
- Scaffolded CTF game to cultivate confidence and competence
- Urban Race to augment learning with physical activity
- Embedded fictional storyline to blend real and virtual world

Goal: Create a positive first experience with computer security

Expanding the security pipeline

Introduce students to computer security early

Camps and classes

- CyberDiscovery, CyberPatriot, CyberAcademy, GenCyber

Capture-the-Flag (CTF) security games

- picoCTF, hs-CTF, abctf

This work

Combined camp and CTF for introducing security topics in an engaging way

Focus on intrinsic motivation

- Scaffolded CTF game to cultivate confidence and competence
- Urban Race to augment learning with physical activity
- Embedded fictional storyline to blend real and virtual world

Goal: Create a positive first experience with computer security

A ``DIVERGENT''-THEMED CTF AND URBAN RACE FOR INTRODUCING SECURITY AND CRYPTOGRAPHY

Motivation

Curriculum

CTF

Storyline

Security Jeopardy!

Urban race

Why?

Using the material

Curriculum

Overview

Curriculum goals
- Data encoding and cryptography
- Security concepts and tools

Structure
- 5 modules and a movie ("The Imitation Game")
- No prior experience assumed

Modules

Module #1: Motivation
- Importance of cryptography and security in history

Module #2: Data encoding
- Information in the digital age
- Binary, hexadecimal, ASCII, barcodes, QR codes, steganography



Module #3: Simple ciphers
- Transposition ciphers
  - Columnar transposition, Scytale
- Substitution ciphers
  - Monoalphabetic substitution (Caesar, simple)
  - Polyalphabetic substitution (Vigenere, Enigma)



Module #4: Modern ciphers
- Public-key cryptography
- Dominating set problem

Module #5: Cryptographic protocols
- Man-in-the-Middle attacks

Lecture format

Alternating lecture and collaborative practice
- Each team given a puzzle made up of sub-puzzles
- Individual members solve a sub-puzzle
- Solutions combined

Overview

Curriculum goals

- Data encoding and cryptography
- Security concepts and tools

Structure

- 5 modules and a movie ("The Imitation Game")
- No prior experience assumed

Modules

Curriculum

Overview

Curriculum goals
- Data encoding and cryptography
- Security concepts and tools

Structure
- 5 modules and a movie ("The Imitation Game")
- No prior experience assumed

Modules

Module #1: Motivation
- Importance of cryptography and security in history

Module #2: Data encoding
- Information in the digital age
- Binary, hexadecimal, ASCII, barcodes, QR codes, steganography



Module #3: Simple ciphers
- Transposition ciphers
  - Columnar transposition, Scytale
- Substitution ciphers
  - Monoalphabetic substitution (Caesar, simple)
  - Polyalphabetic substitution (Vigenere, Enigma)



Module #4: Modern ciphers
- Public-key cryptography
- Dominating set problem

Module #5: Cryptographic protocols
- Man-in-the-Middle attacks

Lecture format

Alternating lecture and collaborative practice
- Each team given a puzzle made up of sub-puzzles
- Individual members solve a sub-puzzle
- Solutions combined

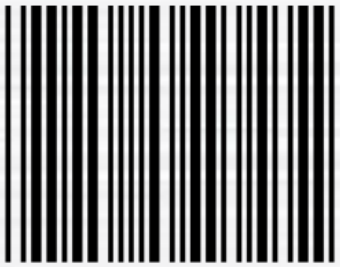
Module #1: Motivation

- Importance of cryptography and security in history

Module #2: Data encoding

- Information in the digital age
- Binary, hexadecimal, ASCII, barcodes, QR codes, steganography

Binary	Hex	Decimal
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

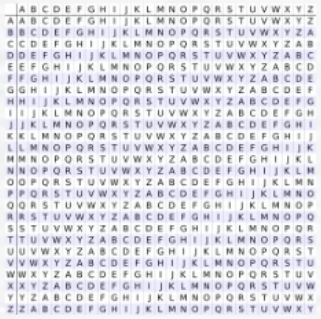


Modules

Module #3: Simple ciphers

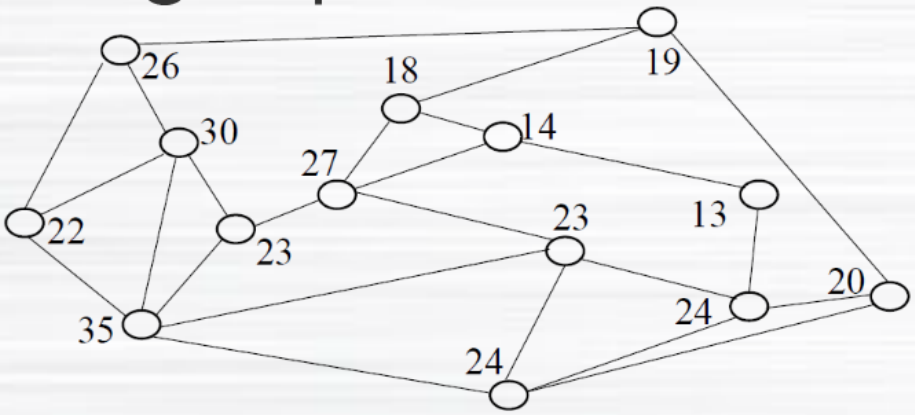
- Transposition ciphers
  - Columnar transposition, Scytale
- Substitution ciphers
  - Monoalphabetic substitution (Caesar, simple)
  - Polyalphabetic substitution (Vigenere, Enigma)

```
GERMAN    AEGMNR
defend    nededf
theeas    ahtese
twallo    lwtloa
ftheca    ctfeah
stle..    .tse.l
```



Module #4: Modern ciphers

- Public-key cryptography
- Dominating set problem



Module #5: Cryptographic protocols

- Man-in-the-Middle attacks

A ``DIVERGENT''-THEMED CTF AND URBAN RACE FOR INTRODUCING SECURITY AND CRYPTOGRAPHY

Motivation

Curriculum

CTF

Storyline

Security Jeopardy!

Urban race

Why?

Using the material

CTF

Format

24 scaffolded challenges
- Given in sets during the week based on daily module
- Designed to cultivate confidence and competence
- Simple, common gameplay mechanism
  - Decode message to find the key that unlocks a file
  - Focus on technical skills being developed

Example

```
116 104 101 32 107 101 121 32 102 111 114
32 116 104 101 32 115 101 118 101 110 116
104 32 105 115
```

```
 t   h   e       k   e   y       f   o   r
     t   h   e       s   e   v   e   n   t
 h       i   s
```

Example

```
the   key   for   june

  thirteenth     is
```

Format

24 scaffolded challenges

- Given in sets during the week based on daily module
- Designed to cultivate confidence and competence
- Simple, common gameplay mechanism
    - Decode message to find the key that unlocks a file
    - Focus on technical skills being developed

Example

```
116 104 101 32 107 101 121 32 102 111 114
32 116 104 101 32 115 101 118 101 110 116
104 32 105 115
```

```
 t   h   e       k   e   y       f   o   r
     t   h   e       s   e   v   e   n   t
 h       i   s
```

Example

☯❖☾ ●☾💧 ⌘♎🖱 🔲✌☮☾

☯❖◆🖱☯☾☾☮☯❖ ◆☽

the key for june

thirteenth is

A ``DIVERGENT''-THEMED CTF AND URBAN RACE FOR INTRODUCING SECURITY AND CRYPTOGRAPHY

Motivation

Curriculum

CTF

Storyline

Security Jeopardy!

Urban race

Why?

Using the material

Storyline

Idea

Embed CTF challenges into a familiar, contemporary story
- Provide extra level of engagement
- Challenges open up individual parts of story
- "Divergent" series by Veronica Roth

Why Divergent?

Familiar to this generation
- Books > 30 million copies

Relevant plot to overall CyberPDX GenCyber camp
- Use and abuse of technology
- Diversity theme
  - Female protagonist
  - Importance of people with diverse skills and expertise
- Computer security subplot amenable to adaptaion

Plot

Story of 5 clans
- Dauntless, Abnegation, Erudite, Candor, Amity

"The Traitor" short story
- Divergent as told through the eyes of Four
- Four suspects plan to eliminate Abnegation
- Works to break into computer systems of Dauntless and Erudite leaders to thwart plan
- Uses shoulder surfing, backdoors, trojans, and rootkits

CTF adaptation

Four has disappeared just before camp
Tris contacts campers for help
- Clues include a USB key with an electronic diary on it and some printouts of encoded messages
- Printouts encode keys to unlock diary entries
  - From Four's control room security training
  - Training that is now being given to students
- Tris asks campers to find out what Four was working on

Challenges

Encoded messages are CTF challenges
- Printouts containing scaffolded levels
- Must decode each to reveal key
- Key unlocks an individual diary entry
- Difficulty steadily increases

Idea

Embed CTF challenges into a familiar, contemporary story

- Provide extra level of engagement
- Challenges open up individual parts of story
- "Divergent" series by Veronica Roth

Why Divergent?

Familiar to this generation

- Books > 30 million copies

Relevant plot to overall CyberPDX GenCyber camp

- Use and abuse of technology
- Diversity theme
  - Female protagonist
  - Importance of people with diverse skills and expertise
- Computer security subplot amenable to adaptaion

Plot

Story of 5 clans

- Dauntless, Abnegation, Erudite, Candor, Amity

"The Traitor" short story

- Divergent as told through the eyes of Four
- Four suspects plan to eliminate Abnegation
- Works to break into computer systems of Dauntless and Erudite leaders to thwart plan
- Uses shoulder surfing, backdoors, trojans, and rootkits

CTF adaptation

Four has disappeared just before camp
Tris contacts campers for help

- Clues include a USB key with an electronic diary on it and some printouts of encoded messages
- Printouts encode keys to unlock diary entries
  - From Four's control room security training
  - Training that is now being given to students
- Tris asks campers to find out what Four was working on

Challenges

Encoded messages are CTF challenges

- Printouts containing scaffolded levels
- Must decode each to reveal key
- Key unlocks an individual diary entry
- Difficulty steadily increases

A ``DIVERGENT''-THEMED CTF AND URBAN RACE FOR INTRODUCING SECURITY AND CRYPTOGRAPHY

Motivation

Curriculum

CTF

Storyline

Security Jeopardy!

Urban race

Why?

Using the material

Security Jeopardy!

Revisiting curricular goals

Introduce cryptography
- Done via CTF challenges

Introduce security concepts and tools
- Attempt to inspire curiosity and appreciation for computer security
- Best done in context in a memorable way
- Use engagement in story and plot device of the diary
  - Four's first-person account of penetration testing

Mechanics

Diary set in preceding month
Each entry describes a method Four employs
Tools and techniques central to computer security
Jeopardy! mechanic
- Actual tool or technique not disclosed directly
- Puzzle within a puzzle
- Students research an aspect of computer security to identify Four's method

Example entry

June 25

Before getting caught on Mark's computer, I managed to get a packet trace revealing Mark's network connections to, among other things, Kindle servers. Since the Kindle have likely blocked many incoming connections to their systems, it will be helpful to find out which services are available. Manually checking each potential network address and port would take me forever, but I've learned that there are many automated tools that can help. One such tool is called nmap. It is a network scanner that will automatically probe a network to see what servers and services are open. While that will be clearly helpful, what I really need is something to tell me what is open "and" vulnerable. For that, there is another tool that people in the past used. The scanner I found that does this was released in 1998 and is quite broable (pun intended).

UNSESS

Story

Follow Four and figure out how he....

Revisiting curricular goals

Introduce cryptography

- Done via CTF challenges

Introduce security concepts and tools

- Attempt to inspire curiosity and appreciation for computer security
- Best done in context in a memorable way
- Use engagement in story and plot device of the diary
    - Four's first-person account of penetration testing

Mechanics

Diary set in preceding month
Each entry describes a method Four employs
Tools and techniques central to computer security
Jeopardy! mechanic

- Actual tool or technique not disclosed directly
- Puzzle within a puzzle
- Students research an aspect of computer security to identify Four's method

Example entry

June 25

Before getting caught on Max's computer, I managed to get a packet trace revealing Max's network connections to, among other things, Erudite servers. Since the Erudite have likely blocked many incoming connections to their systems, it will be helpful to find out which services are available. Manually checking each potential network address and port would take me forever, but I've learned that there are many automated tools that can help. One such tool is called nmap. It is a network scanner that will automatically probe a network to see what servers and services are open. While that will be clearly helpful, what I really need is something to tell me what is open *and* vulnerable. For that, there is another tool that people in the past used. The scanner I found that does this was released in 1998 and is quite tenable (pun intended):

U N S E S S

Story

Follow Four and figure out how he....

- Uses a surveillance camera to obtain Max's password
- Installs a backdoor to maintain access to Max's computer
- Discovers an intrusion detection system protecting the computer
- Exfiltrates data covertly from the system
- Covers his activity to avoid detection
- Breaks the encryption employed on Max's files
- Attempts to monitor all network traffic
- Is caught via the use of a fake program
- Attempts to subvert Max's hardened replacement computer
- Employs a social engineering attack that fails as a result of a password manager
- Attempts a session hijacking attack that fails due to script blocking and encryption
- Performs anonymous reconnaissance on Erudite systems
- Exploits vulnerabilities to move laterally within the Erudite network
- Uncovers an air-gapped system at the heart of the Erudite plan

- Uses a surveillance camera to obtain Max's password
- Installs a backdoor to maintain access to Max's computer
- Discovers an intrusion detection system protecting the computer
- Exfiltrates data covertly from the system
- Covers his activity to avoid detection

- Breaks the encryption employed on Max's files
- Attempts to monitor all network traffic
- Is caught via the use of a fake program
- Attempts to subvert Max's hardened replacement computer
- Employs a social engineering attack that fails as a result of a password manager

- Attempts a session hijacking attack that fails due to script blocking and encryption
- Performs anonymous reconnaissance on Erudite systems
- Exploits vulnerabilities to move laterally within the Erudite network
- Uncovers an air-gapped system at the heart of the Erudite plan

A ``DIVERGENT''-THEMED CTF AND URBAN RACE FOR INTRODUCING SECURITY AND CRYPTOGRAPHY

Motivation

Curriculum

CTF

Storyline

Security Jeopardy!

Urban race

Why?

Using the material

Urban race

Live story

Capstone activity
CTF storyline leads to climax in the present
- Pivot from scheduled lecture to live action
- Students inserted into plot directly
- ~2 hour Urban Race finale

Story setup

Tris relays urgent message from Four
- Trapped outside of Erudite control room
- Protected by puzzles to ensure only Erudite get in
  - Requires advanced cryptography skills
  - Knowledge of the Erudite (PSU) campus
  - Must be solved quickly with under 10 incorrect attempts
- Gives each team Four's Twitter handle

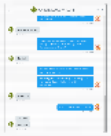
Race

Modeled after CitySolve, ChallengeNation, Amazing Race
- Tris relays a set of cryptographic clues given to Four
- Once decrypted, clues send teams throughout campus
- Communication with "virtual" Four to relay answers



Four-bot

Four as a Twitter bot
- Gives illusion of interacting with the actual character
- Takes answers and updates storyline state
- Each team given independent story instance
- Allows each team to "save the city"
- First place team quietly given extra challenge
  - Leads to a lock box and special prize



Live story

Capstone activity

CTF storyline leads to climax in the present

- Pivot from scheduled lecture to live action
- Students inserted into plot directly
- ~2 hour Urban Race finale

Story setup

Tris relays urgent message from Four

- Trapped outside of Erudite control room
- Protected by puzzles to ensure only Erudite get in
  - Requires advanced cryptography skills
  - Knowledge of the Erudite (PSU) campus
  - Must be solved quickly with under 10 incorrect attempts
- Gives each team Four's Twitter handle

Race

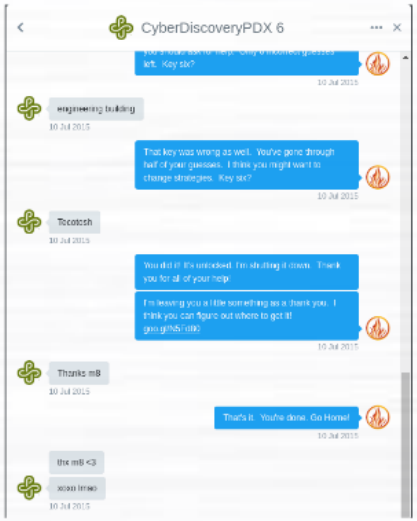
Modeled after CitySolve, ChallengeNation, Amazing Race

- Tris relays a set of cryptographic clues given to Four
- Once decrypted, clues send teams throughout campus
- Communication with "virtual" Four to relay answers

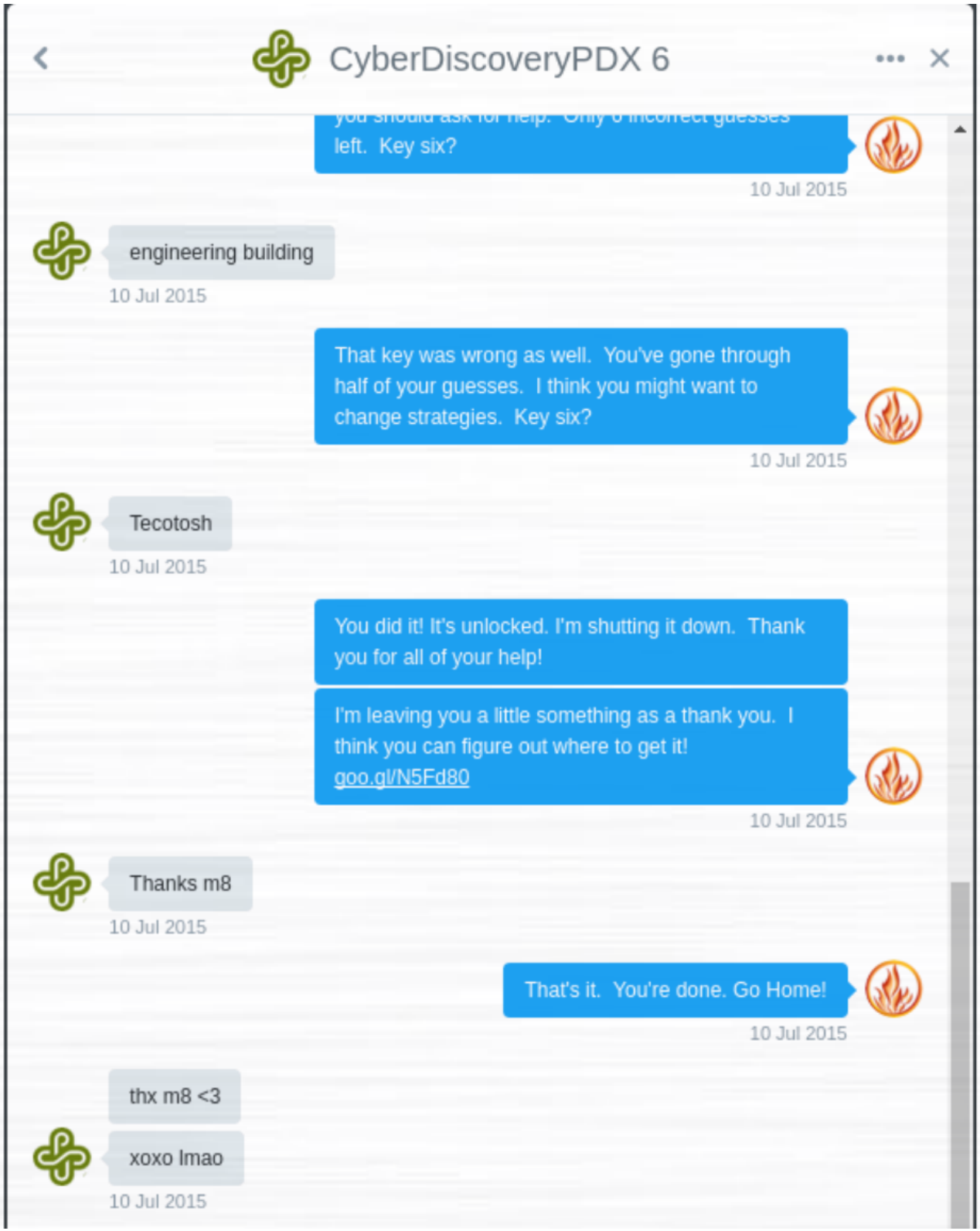
Four-bot

Four as a Twitter bot

- Gives illusion of interacting with the actual character
- Takes answers and updates storyline state
- Each team given independent story instance
- Allows each team to "save the city"
- First place team quietly given extra challenge
    - Leads to a lock box and special prize



nge


CyberDiscoveryPDX 6
left. Key six?
10 Jul 2015
engineering building
10 Jul 2015
That key was wrong as well. You've gone through half of your guesses. I think you might want to change strategies. Key six?
10 Jul 2015
Tecotosh
10 Jul 2015
You did it! It's unlocked. I'm shutting it down. Thank you for all of your help!
I'm leaving you a little something as a thank you. I think you can figure out where to get it!
goo.gl/N5Fd80
10 Jul 2015
Thanks m8
10 Jul 2015
That's it. You're done. Go Home!
10 Jul 2015
thx m8 <3
xoxo lmao
10 Jul 2015

A ``DIVERGENT''-THEMED CTF AND URBAN RACE FOR INTRODUCING SECURITY AND CRYPTOGRAPHY

Motivation

Curriculum

CTF

Storyline

Security Jeopardy!

Urban race

Why?

Using the material

Why?

Flow

Coined in 1990 by Mihaly Csikczentmihalyi
- Single-minded focus on a task that aligns a person's emotions and motivation with objective at hand
- Characterized by deep enjoyment, creativity, and a total involvement with life.
- Powerful intrinsic motivator

Key in making engaging learning experiences
- Often brought out in CTF events and games

Mihaly Csikczentmihalyi, "Flow: The Psychology of Optimal Experience", 1990.

Designing for Flow

Employ known triggers for flow
- Within CTF
  - Clear goals
  - Balance of challenge and skill level
  - Immediate feedback
  - Rich environment
- Additionally in urban race
  - Risk
  - Common, shared goal
  - Constant group communication

Steven Kotler, "The Rise of Superman", 2014

Success?

2016 CyberPDX Urban Race Winners

An elusive unicorn...

Flow

Coined in 1990 by Mihaly Csikczentmihalyi

- Single-minded focus on a task that aligns a person's emotions and motivation with objective at hand
- Characterized by deep enjoyment, creativity, and a total involvement with life.
- Powerful intrinsic motivator

Key in making engaging learning experiences

- Often brought out in CTF events and games

Mihaly Csikczentmihalyi, "Flow: The Psychology of Optimal Experience", 1990.

Designing for Flow

Employ known triggers for flow

- Within CTF
  - Clear goals
  - Balance of challenge and skill level
  - Immediate feedback
  - Rich environment
- Additionally in urban race
  - Risk
  - Common, shared goal
  - Constant group communication

Steven Kotler, "The Rise of Superman", 2014

Success?

2016 CyberPDX Urban Race Winners

An elusive unicorn...

A ``DIVERGENT''-THEMED CTF AND URBAN RACE FOR INTRODUCING SECURITY AND CRYPTOGRAPHY

Motivation

Curriculum

CTF

Storyline

Security Jeopardy!

Urban race

Why?

Using the material

Using the material

Offerings

CyberDiscovery Portland State (7/2015)
Portland State New Beginnings (9/2015, 7/2016)
Lewis and Clark College (1/2016)
Lincoln High School (4/2016)
CyberPDX (7/2016)

For teachers

All course material available at:
- https://cyberd.oregonctf.org

For access to source code to customize CTF or Urban Race
- Contact wuchang@pdx.edu

Play the game
- Copies of CTF challenges
- Demo mini-urban race with prizes after session

CyberPDX student evaluation

54 10th grade students (32 female, 23 male)
1=strongly disagree
5=strongly agree

I am more comfortable learning about cybersecurity.	4.24
I learned a lot about cybersecurity	4.53
I enjoyed learning about cybersecurity	4.36
I enjoyed the projects and activities at this camp	4.40
I would like to learn more about cybersecurity	4.02

Specific feedback

Students
- I liked the crypto challenges a lot because it was really satisfying to figure out the hidden codes.
- Solving the crypto challenges. I thought that it was extremely well put together and was equally challenging and fun...The problem-solving and creativity part of this thread is something that everyone on our team enjoyed and appreciated.
- The cryptography was a lot of fun to crack and solve.

Teachers
- Love the puzzle within a puzzle hook and motivator... Students definitely got into this.
- The interconnectedness built into the progressive challenges was superbly handled, and the scavenger hunt was phenomenal!
- Well planned and implemented. My students were able to apply their knowledge and have fun.

Offerings

CyberDiscovery Portland State (7/2015)
Portland State New Beginnings (9/2015, 7/2016)
Lewis and Clark College (1/2016)
Lincoln High School (4/2016)
CyberPDX (7/2016)

CyberPDX student evaluation

54 10th grade students (32 female, 23 male)
1=strongly disagree
5=strongly agree

I am more comfortable learning about cybersecurity.	4.24
I learned a lot about cybersecurity	4.53
I enjoyed learning about cybersecurity	4.30
I enjoyed the projects and activities at this camp	4.40
I would like to learn more about cybersecurity	4.02

For teachers

All course material available at:

- https://cyberd.oregonctf.org

For access to source code to customize CTF or Urban Race

- Contact wuchang@pdx.edu

Play the game

- Copies of CTF challenges
- Demo mini-urban race with prizes after session

Specific feedback

Students

- I liked the crypto challenges a lot because it was really satisfying to figure out the hidden codes.
- Solving the crypto challenges. I thought that it was extremely well put together and was equally challenging and fun...The problem-solving and creativity part of this thread is something that everyone on our team enjoyed and appreciated.
- The cryptography was a lot of fun to crack and solve.

Teachers

- Love the puzzle within a puzzle hook and motivator.... Students definitely got into this.
- The interconnectedness built into the progressive challenges was superbly handled, and the scavenger hunt was phenomenal!
- Well planned and implemented. My students were able to apply their knowledge and have fun.

A ``DIVERGENT''-THEMED CTF AND URBAN RACE FOR INTRODUCING SECURITY AND CRYPTOGRAPHY

Motivation

Curriculum

CTF

Storyline

Security Jeopardy!

Urban race

Why?

Using the material

Lecture format

Alternating lecture and collaborative practice

- Each team given a puzzle made up of sub-puzzles
- Individual members solve a sub-puzzle
- Solutions combined
- Enables horizontal learning

- Example