HERIOT WATT UNIVERSITY

Empower New Code Citizens to Reflect and Communicate on Code Security

Manuel Maarek
Heriot-Watt University

May 20, 2025
SoSySec Seminar
Rennes

LEADERS IN IDEAS AND SOLUTIONS

HERIOT WATT UNIVERSITY

Outline

- Background
  - Curriculum Vitae
  - Developer-Centred Security
  - A Serious Game for Software Security, the Citadel Programming Lab
- Code Security Empowering Workshop
  - Securing New Code-Citizens
  - Provoking Games
  - Cybersecurity Cards
  - Secrious Project
- Perspectives
- Rennes Research Visits

Manuel Maarek

Associate Professor – Computer Science Department – Heriot-Watt University
Director of NCSC-certified MSc Computer Science for Cyber Security

- Since 2014 Heriot-Watt University Edinburgh
- 2010-2014 Research Engineer at SafeRiver Paris
- 2008-2010 Research Assistant at INRIA Grenoble
- 2007-2008 ERCIM Fellow at CRP Henri Tudor Luxembourg
- 2007 PhD Heriot-Watt University Edinburgh
- 2002 MSc-UG Studies University Pierre et Marie Curie Paris

Developer-Centred Security – Safety-Security-Usability Analysis – Security by Design – Formal Methods – Programming Languages – Computing Education – Serious Games

HERIOT WATT UNIVERSITY


Support us

The Guardian
News provider of the year

News Opinion Sport Culture Lifestyle

The Guardian view Columnists Cartoons Opinion videos

The Observer

One engineer's curiosity may have saved us from a devastating cyber-attack

John Naughton

In discovering malicious code that endangered global networks in open-source software, Andres Freund exposed our reliance on insecure, volunteer-maintained tech

Sat 6 Apr 2024 16.00 BST

Share 145

2016 IEEE Symposium on Security and Privacy

You Get Where You're Looking For
The Impact of Information Sources on Code Security

Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim†, Michelle L. Mazurek†, Christian Stransky
CISPA, Saarland University; †University of Maryland, College Park

Making Sense of the Unknown: How Managers Make Cyber Security Decisions

BENJAMIN SHREEVE, University of Bristol, United Kingdom
CATARINA GRALHA, NOVA LINCS, Universidade NOVA de Lisboa, Portugal
AWAIS RASHID, University of Bristol, United Kingdom
JOÃO ARAÚJO and MIGUEL GOULÃO, NOVA LINCS, Universidade NOVA de Lisboa, Portugal

2021 IEEE Secure Development Conference (SecDev)

Developers Are Neither Enemies Nor Users: They Are Collaborators

Partha Das Chowdhury, Joseph Hallett, Nikhil Patnaik, Mohammad Tahaei and Awais Rashid
Bristol Cyber Security Group
University of Bristol, UK
{partha.daschowdhury, joseph.hallett, nikhil.patnaik, mohammad.tahaei, awais.rashid}@bristol.ac.uk

2022 IEEE Symposium on Security and Privacy (SP)

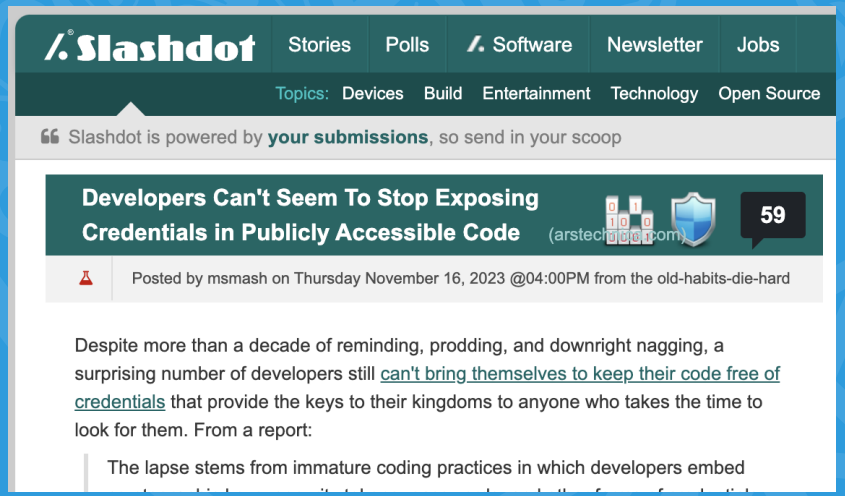
How Does Usable Security (Not) End Up in Software Products? Results From a Qualitative Interview Study

Marco Gutfleisch*, Jan H. Klemmer†, Niklas Busch†,
Yasemin Acar‡, M. Angela Sasse*, and Sascha Fahl†§
*Ruhr University Bochum, Germany, {marco.gutfleisch, martina.sasse}@ruhr-uni-bochum.de
†Leibniz University Hannover, Germany, {klemmer, busch}@sec.uni-hannover.de
‡Max Planck Institute for Security and Privacy, Germany, yasemin.acar@mpi-sp.org
§CISPA Helmholtz Center for Information Security, Germany, sascha.fahl@cispa.de

2017 IEEE Symposium on Security and Privacy

Stack Overflow Considered Harmful?
The Impact of Copy&Paste on Android Application Security

Felix Fischer, Konstantin Böttinger, Huang Xiao, Christian Stransky*, Yasemin Acar*, Michael Backes*, Sascha Fahl*
Fraunhofer Institute for Applied and Integrated Security; *CISPA, Saarland University


Slashdot Stories Polls Software Newsletter Jobs

Topics: Devices Build Entertainment Technology Open Source

Slashdot is powered by **your submissions**, so send in your scoop

Developers Can't Seem To Stop Exposing Credentials in Publicly Accessible Code (arstechnica.com) 59

Posted by msmash on Thursday November 16, 2023 @04:00PM from the old-habits-die-hard

Despite more than a decade of reminding, prodding, and downright nagging, a surprising number of developers still can't bring themselves to keep their code free of credentials that provide the keys to their kingdoms to anyone who takes the time to look for them. From a report:

> The lapse stems from immature coding practices in which developers embed

CHI 2020 Paper **CHI 2020, April 25–30, 2020, Honolulu, HI, USA**

Listen to Developers! A Participatory Design Study on Security Warnings for Cryptographic APIs

Peter Leo Gorski, Yasemin Acar*, Luigi Lo Iacono, Sascha Fahl*
TH Köln/University of Applied Sciences, *Leibniz University Hannover

LEADERS IN IDEAS AND SOLUTIONS

HERIOT WATT UNIVERSITY

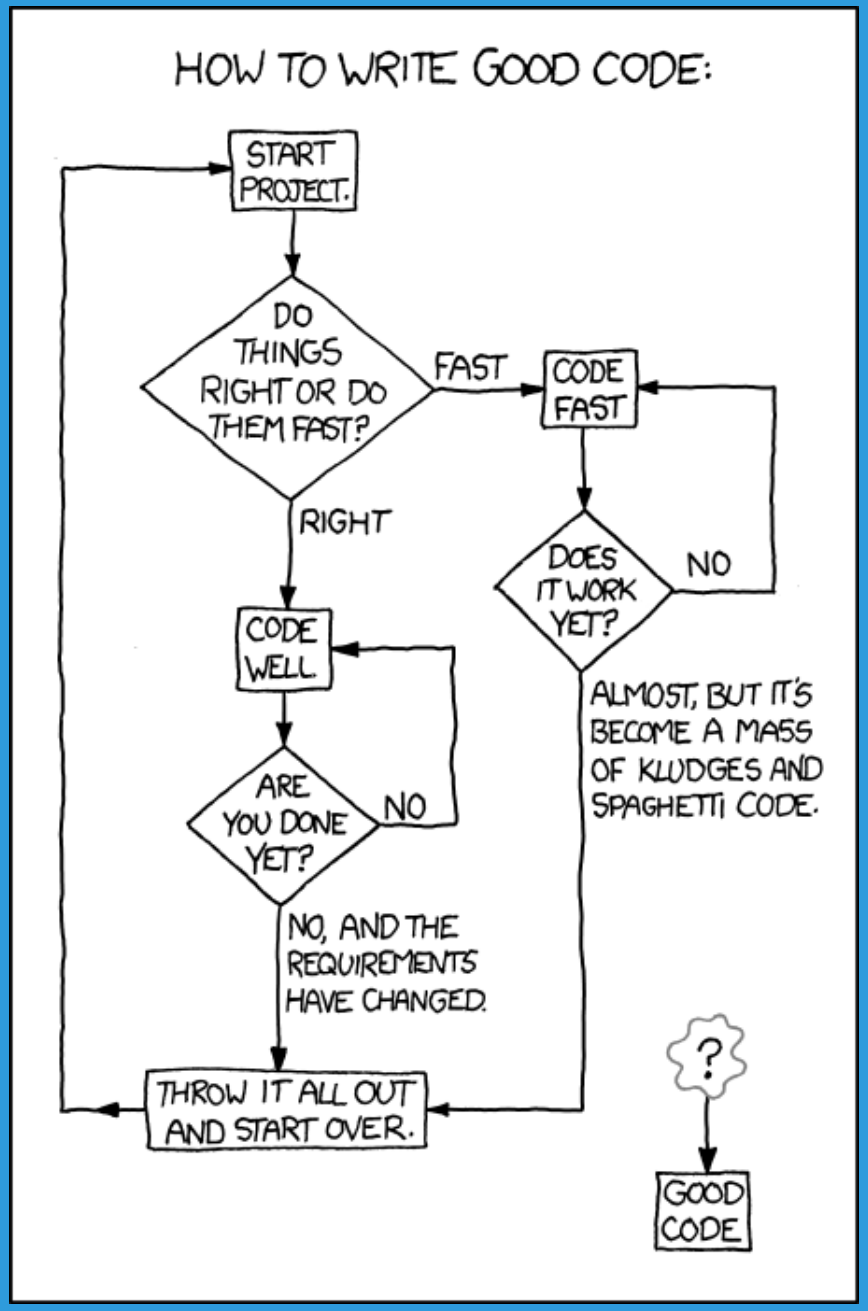
Software Security

Context

- Cyber security is a worldwide concern
- Software vulnerability is a vector of attack
- Making software is now widely accessible

Motivation

- Understand how to raise security awareness and to train the masses of software developers



https://xkcd.com/844/

HERIOT WATT UNIVERSITY

Serious game and gamification for development and security

Coding-based games

Secure-coding games

Coding competitions

Software Development gamification

Interactions for programming education

Gamification for security

LEADERS IN IDEAS AND SOLUTIONS

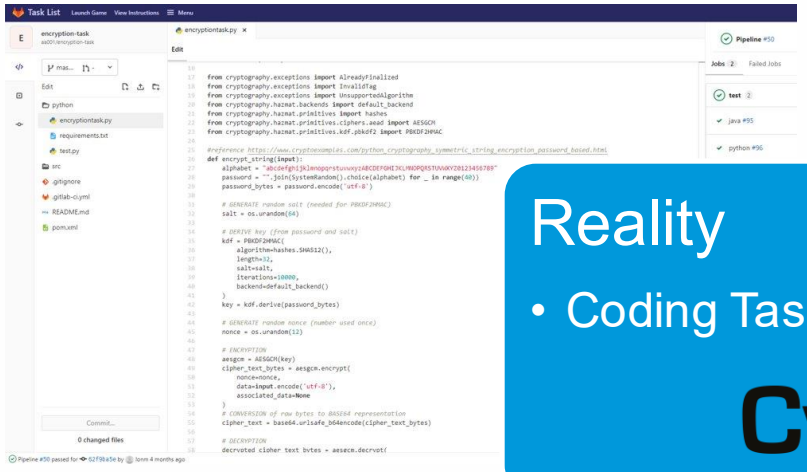
A Serious Game for Software Security

Citadel Programming Lab

with Léon McGregor, Sandy Louchart, Sheung Chi Chan, Szymon Wlodarczyk, Ross McMenemy

[GaLA18,EuroUSEC19,EuroCSEP22]

Funded by NCSC-RISCS, EPSRC, CyBOK



Meaning

- Learning Outcomes

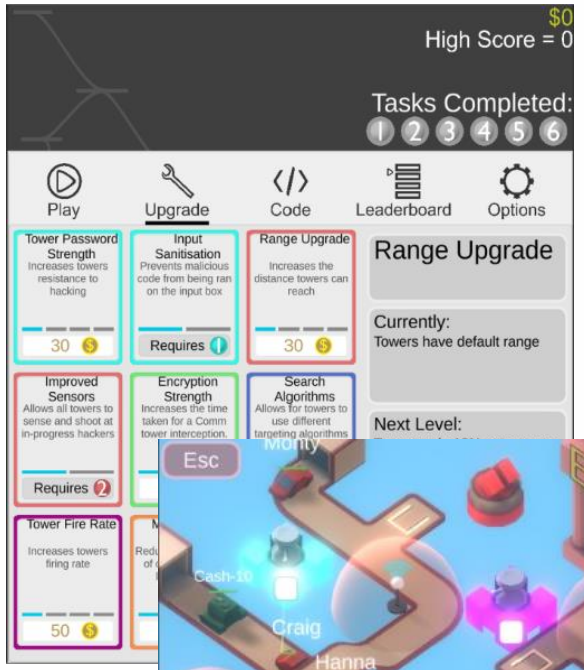
Reality

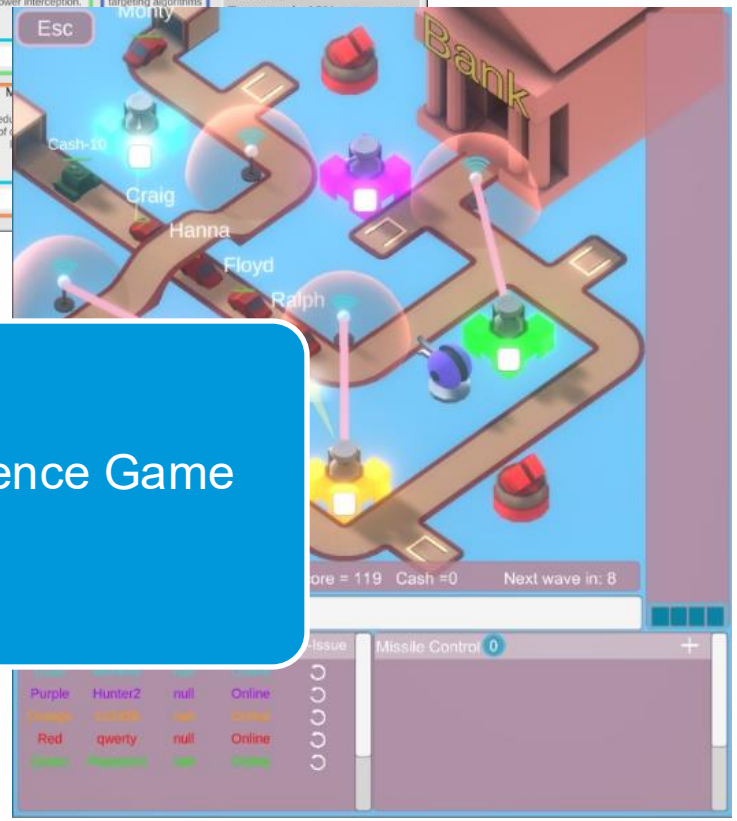
- Coding Tasks

CyBOK

Play

- Tower Defence Game

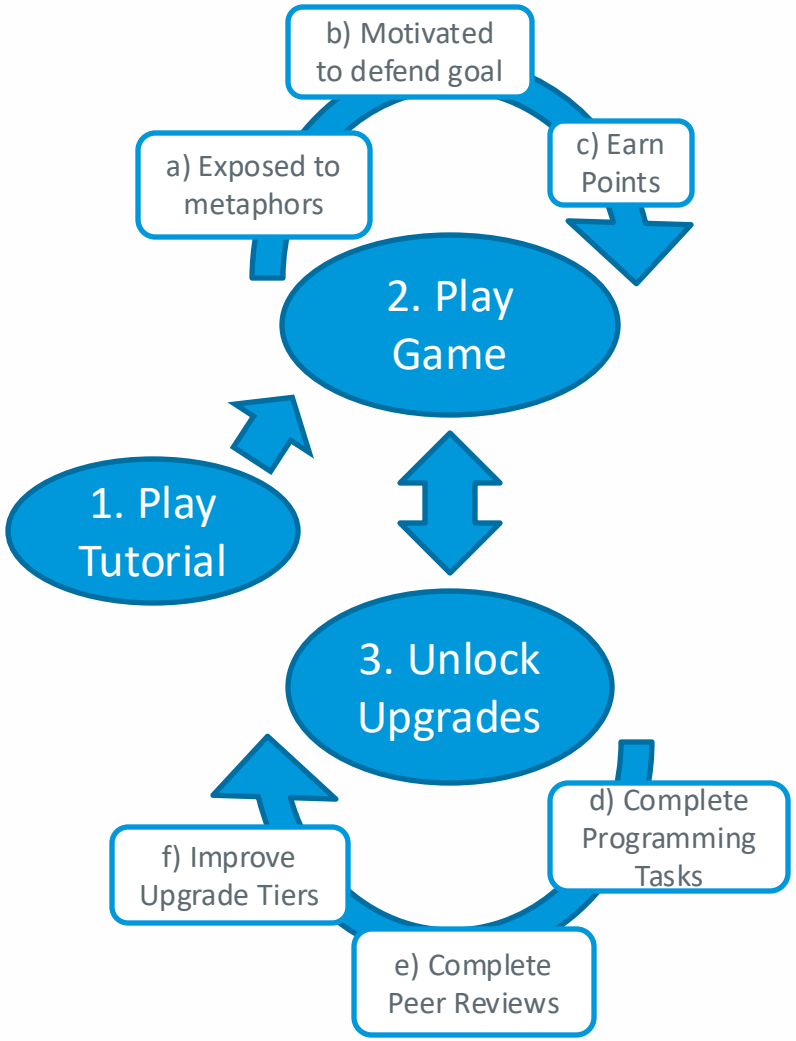




https://citadel-programming-lab.gitlab.io/

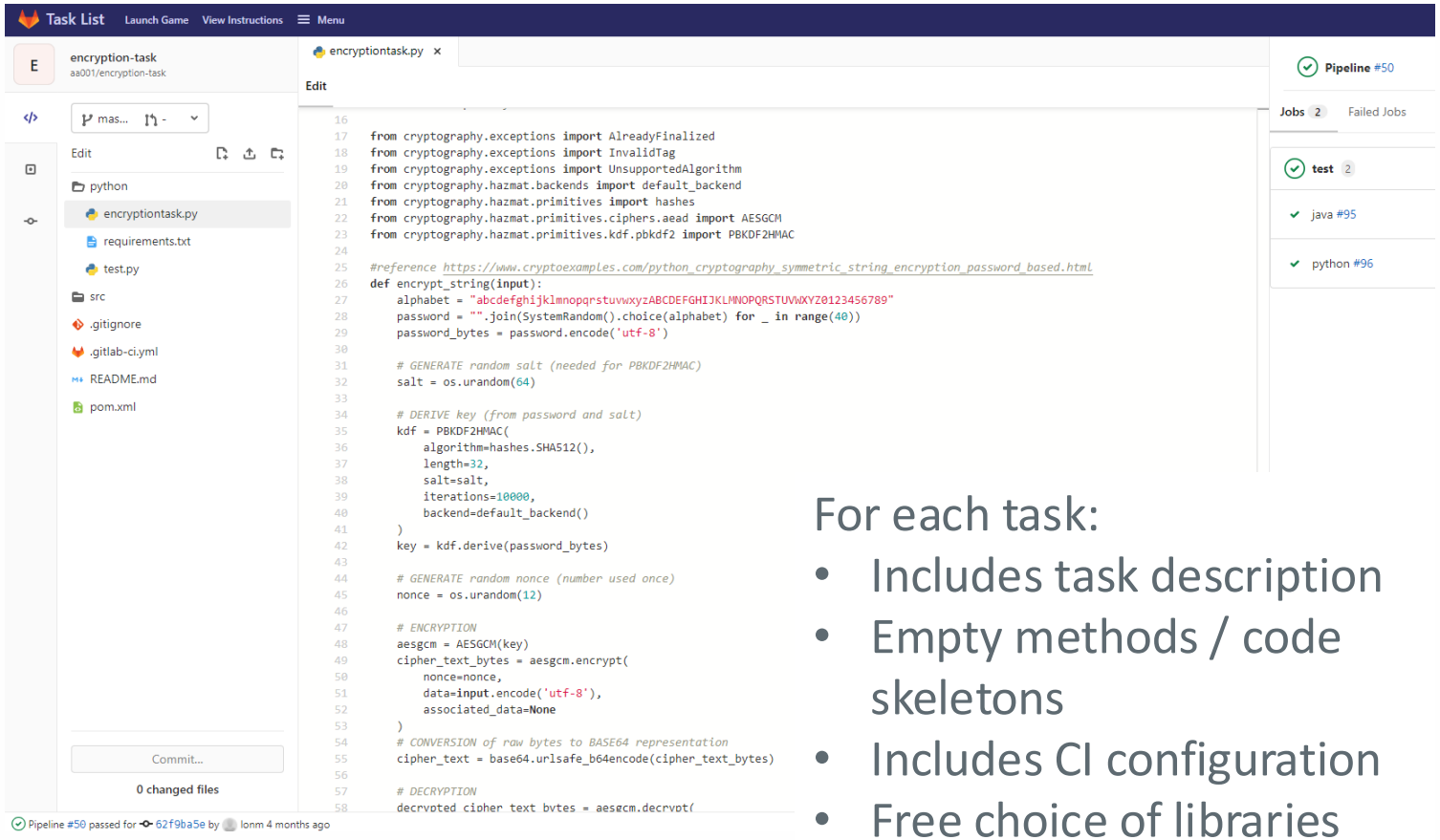
HERIOT WATT UNIVERSITY

Citadel Programming Lab – Game Loops



Unity

Citadel Programming Lab – Tasks




```python
from cryptography.exceptions import AlreadyFinalized
from cryptography.exceptions import InvalidTag
from cryptography.exceptions import UnsupportedAlgorithm
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.ciphers.aead import AESGCM
from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC

#reference https://www.cryptoexamples.com/python_cryptography_symmetric_string_encryption_password_based.html
def encrypt_string(input):
    alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"
    password = "".join(SystemRandom().choice(alphabet) for _ in range(40))
    password_bytes = password.encode('utf-8')

    # GENERATE random salt (needed for PBKDF2HMAC)
    salt = os.urandom(64)

    # DERIVE key (from password and salt)
    kdf = PBKDF2HMAC(
        algorithm=hashes.SHA512(),
        length=32,
        salt=salt,
        iterations=10000,
        backend=default_backend()
    )
    key = kdf.derive(password_bytes)

    # GENERATE random nonce (number used once)
    nonce = os.urandom(12)

    # ENCRYPTION
    aesgcm = AESGCM(key)
    cipher_text_bytes = aesgcm.encrypt(
        nonce=nonce,
        data=input.encode('utf-8'),
        associated_data=None
    )
    # CONVERSION of raw bytes to BASE64 representation
    cipher_text = base64.urlsafe_b64encode(cipher_text_bytes)

    # DECRYPTION
    decrypted_cipher_text_bytes = aesgcm.decrypt(
```

For each task:

- Includes task description
- Empty methods / code skeletons
- Includes CI configuration
- Free choice of libraries

Designing tasks to meet learning outcomes derived from CyBOK

1. Credential Storage* — Store password in a database
2. URL Shortener* — Shorten a long URL
3. String Encryption* — Encrypt a text message
4. Public Key Certificates — Validate an X.509 Certificate
5. PGP — Verify the signature of a message signed via PGP
6. SSL Connections — Implement an SSL/TLS handshake

* Secure programming tasks repurposed from earlier study

Java

python

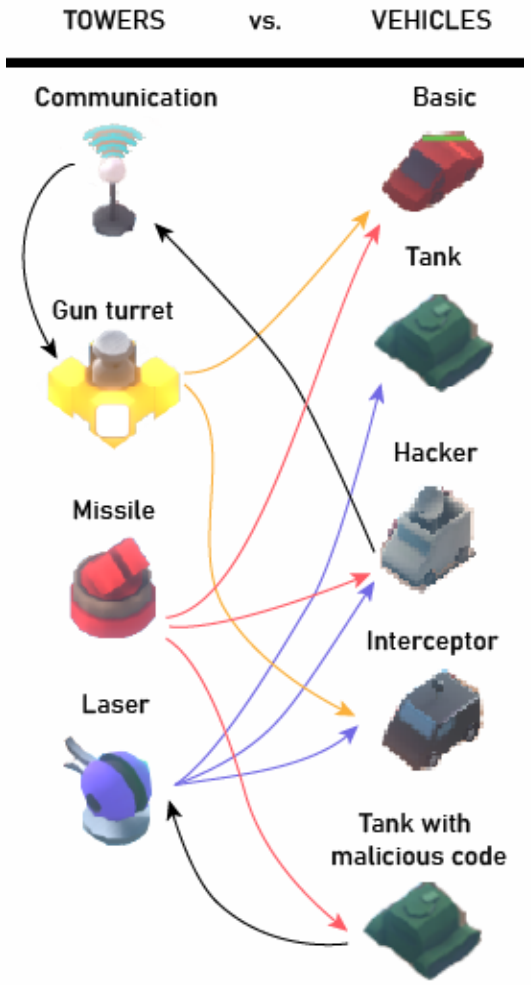
Citadel Programming Lab – Design

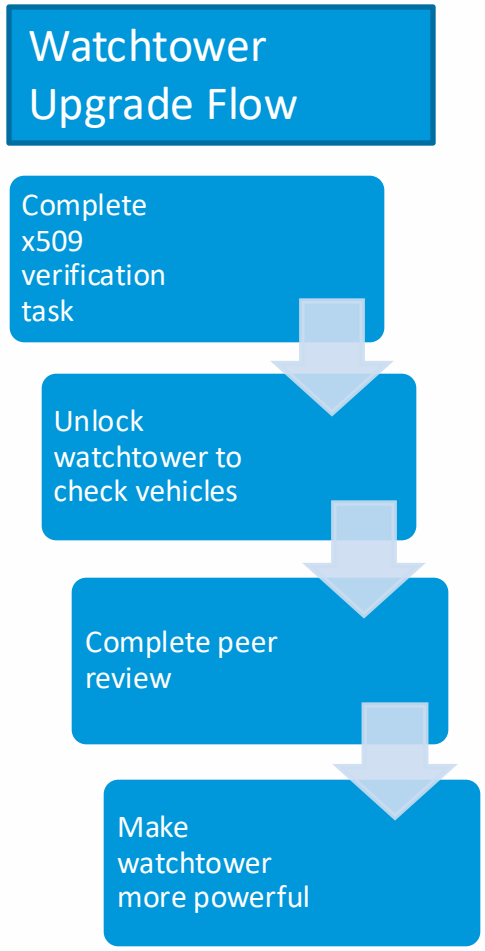
Earn upgrades by completing tasks

- Each task maps to upgrades
- Review other task solutions to enhance upgrades further
- This encourages critical thinking

Metaphors

Gameplay elements and mechanics in the game match elements and concepts from the tasks



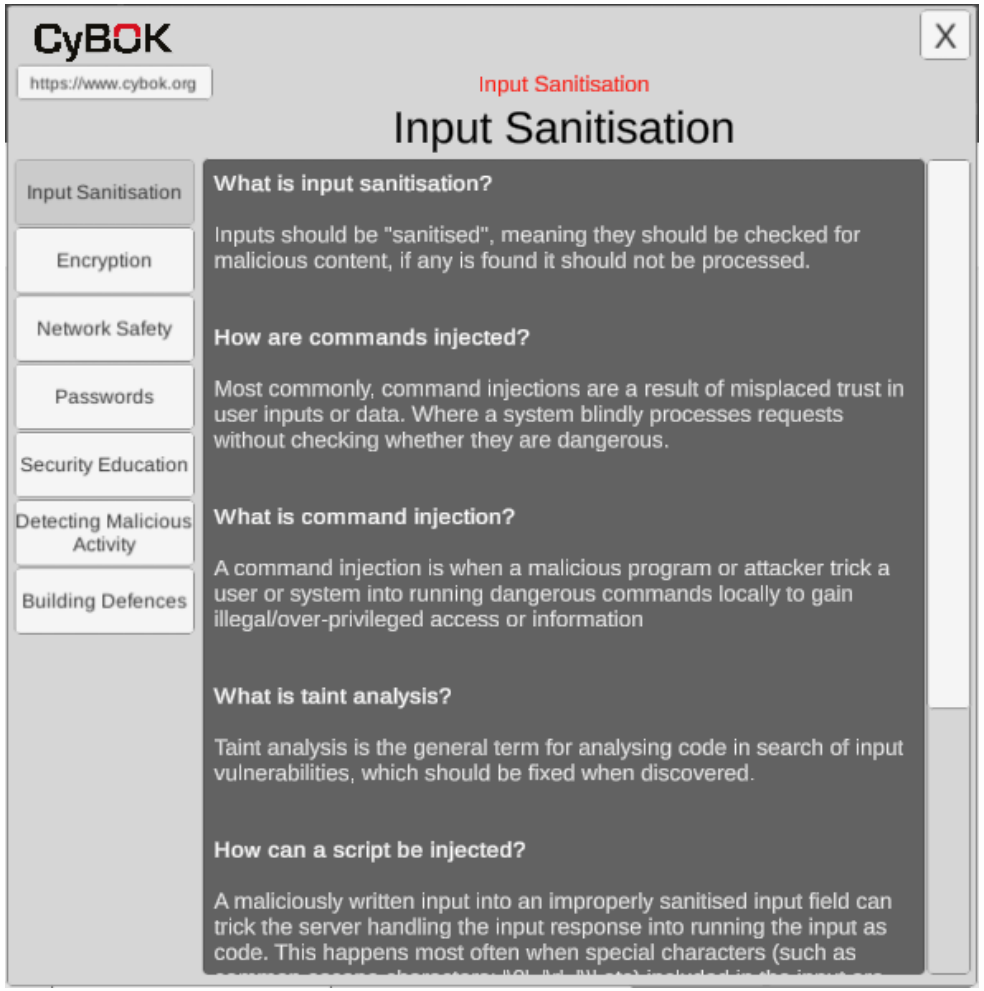


Citadel Programming Lab – Metaphors

Vehicle	Task	Metaphor
Standard	All	Actor that may be good or bad
Tank	1	Attacker that targets infrastructure
Hacker	3	Attacker that interrupts communications
Interceptor	4	Attacker that steals communications

Interaction	Task	Metaphor
Command	1	Command line interactions
Targeting	2	Identifying and targeting a threat
Vehicle Payloads	5	What an actor may be delivering to you
Leaderboard	All	How are you, compared to competitors
Scores	All	A metric of your defensive ability
Coins	All	The data, services you are trying to protect

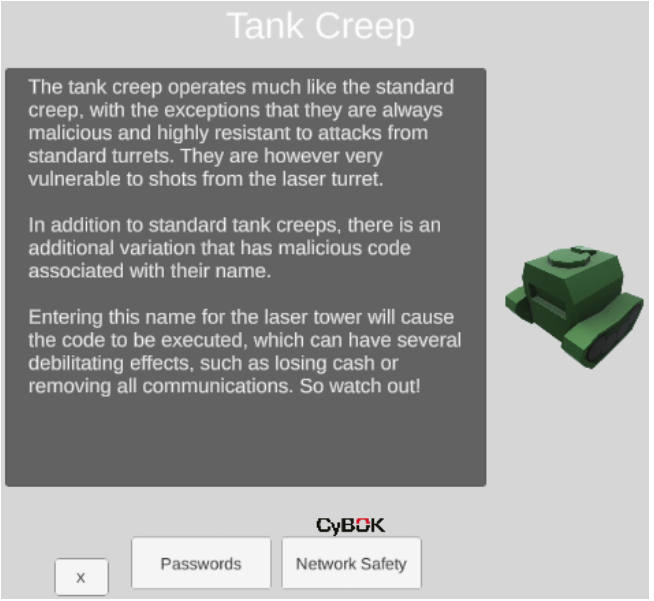
Citadel Programming Lab – Guidance



- Embedding knowledge and learning in the game
- Developed Q&A format to distil CyBOK Guidance

7 Topics, each has Q&A in the form of:

- “How do I defend against this”
- “How does an attacker exploit this”
- “How is this a vulnerability”



Securing New Code-Citizens?

SECRIOUS PROJECT
HERIOT WATT UNIVERSITY
THE GLASGOW SCHOOL OF ART
University of St Andrews
Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits

Building awareness of code security to the wider audience of coders

Wider audience of coders:

New Code-Citizens

- Proximity to software systems
- Not just as users, but as potential creators or contributors
- No formal training in coding
- No particular interest in security

Code Security Training

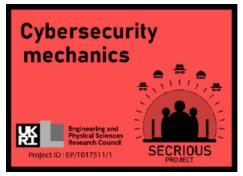
- Formal training as courses or gamified hacking platforms
- Resources freely available to developers, e.g. OWASP Developer Guide
- *Essential for upskilling but often hard to grasp by nonexperts*

Accessing Common Code Security Knowledge

- Open datasets, curricula
- In the UK, the Cybersecurity Body of Knowledge (CyBOK)
- Dedicated exhaustive information, includes: software security, web and mobile security, secure software lifecycle KAs
- *Requires prior knowledge*

Cybersecurity Cards

Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits



Attacks

- Injection
- Memory
- Race Condition
- Side Channel
- Authentication
- Web
- System
- Human Factors

Vulnerabilities

- Code
- System
- Environment
- User
- Management

Defences

- Detection
- Mitigation
- Education
- Prevention

Objectives

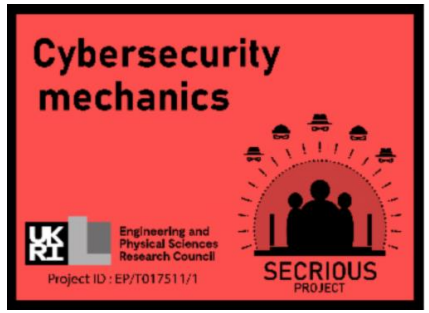
1. Provide **introductory** cybersecurity knowledge to novice users
2. Provide material for expressing interpretation of key cybersecurity topics, that supports independent learning and **self-efficacy**
3. Act as an **index** for the CyBOK knowledge base, which provides an interface for discussion on key cybersecurity topics
4. Provide **links** between key cybersecurity topics, allowing for the capture of various cybersecurity scenarios

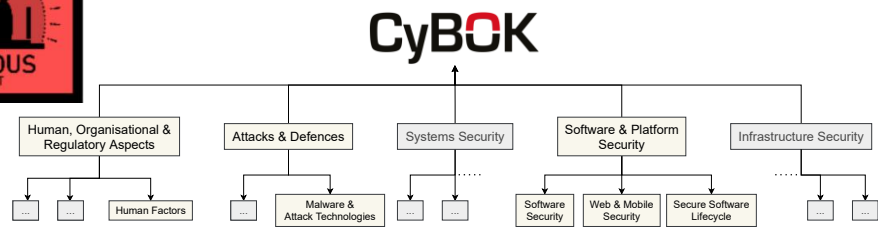
[DGASP23]

Cybersecurity Cards

Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits

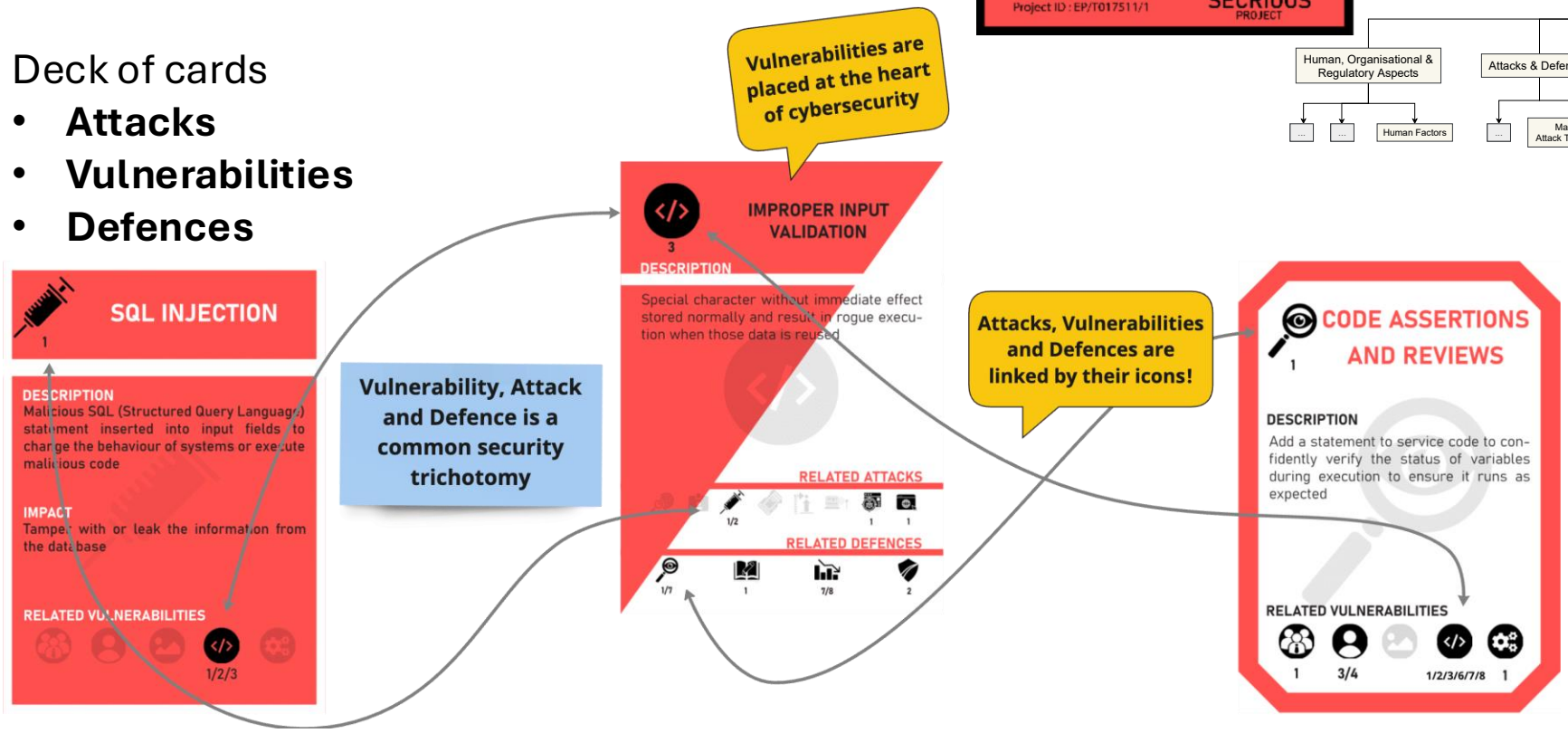
Cybersecurity Cards designed to provide introductory knowledge of cybersecurity and to support learning and discussion





Deck of cards

- **Attacks**
- **Vulnerabilities**
- **Defences**



Based on CyBOK for knowledge and technical content and coverage

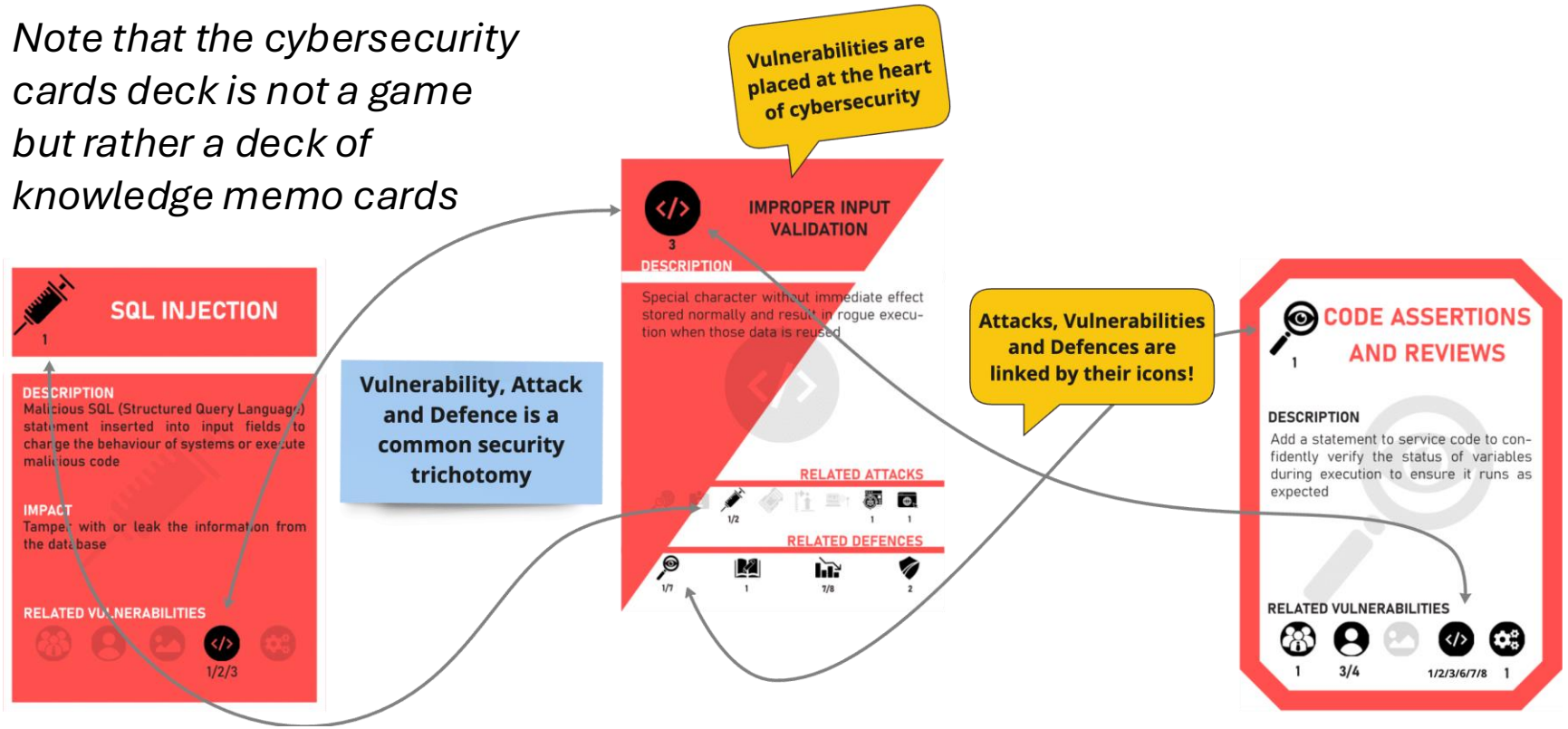
Our cards provide a more accessible entry to the rich and complex content of CyBOK

Cybersecurity Cards

Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits

- Each card focuses on one code security concept
- Classified by topic-icon, unique number within a topic
- Attacks-vulnerabilities-defences trichotomy

Note that the cybersecurity cards deck is not a game but rather a deck of knowledge memo cards

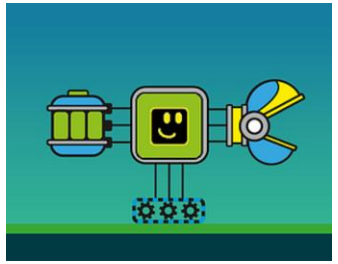


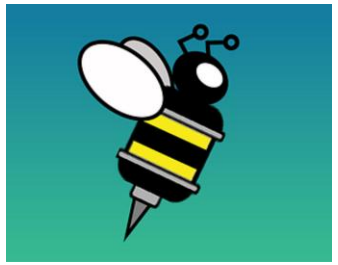
- Vulnerabilities-attacks / Vulnerabilities-defences relationships
- No direct attacks-defences link: instil the notion of attack surface
- No one-to-one single link between cards: no simplistic solutions

Triggering Reflection on Code Security

SECRIOUS PROJECT
HERIOT WATT UNIVERSITY
THE GLASGOW SCHOOL OF ART
University of St Andrews
Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits

Provoking Games





- Small serious games designed to provoke reflection
- Not to convey knowledge but to make player think
- Initiate discussion and reflection
- Create behavioural change in nonexperts

- *Protection* on Code Security
- *Collaboration* on Secure Software Development Lifecycle and communications
- *API-ary* on API Security

Provoking Games

Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits

https://www.youtube.com/watch?v=Saf8sxlm1Gs [ICGBL22]

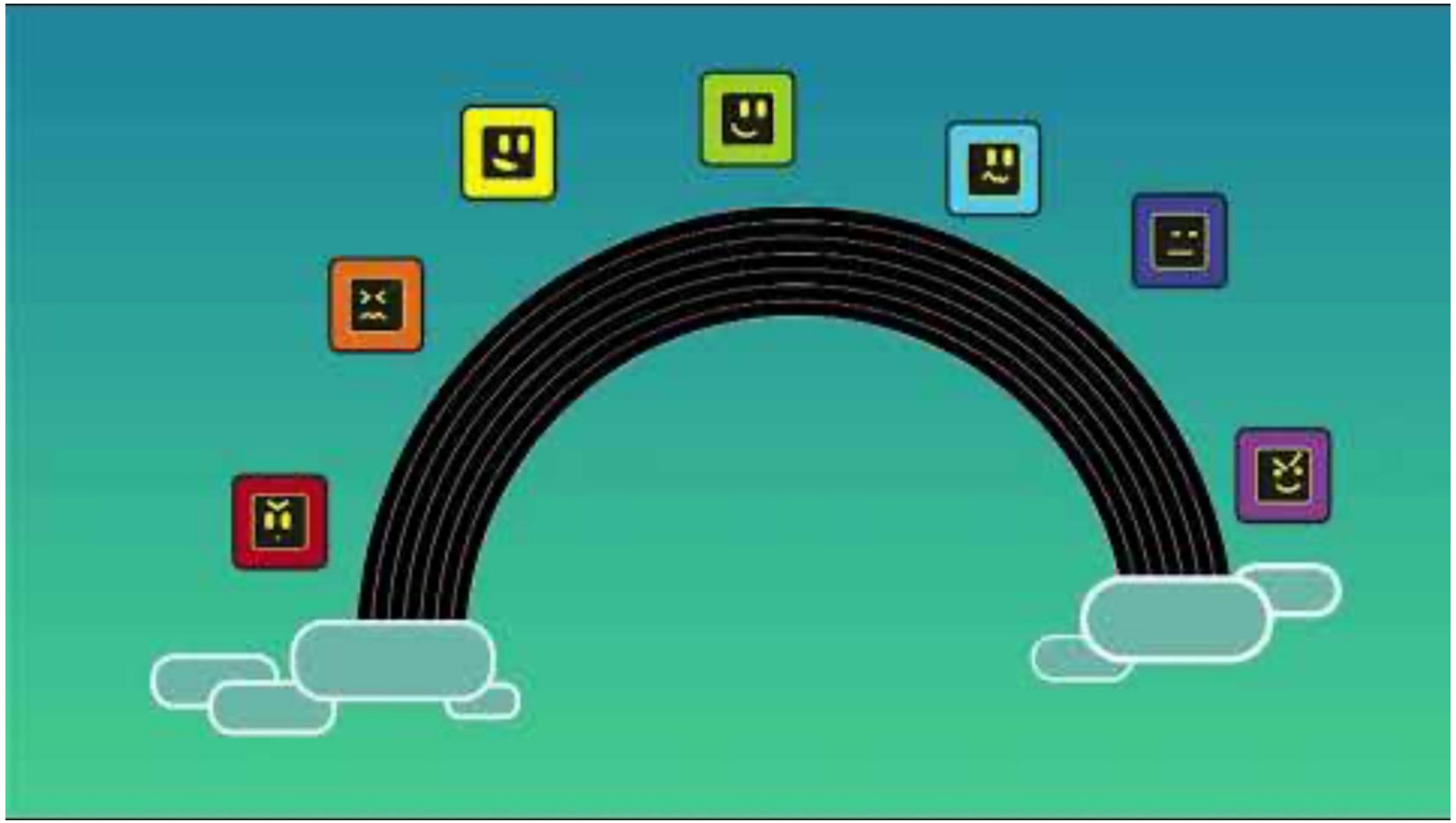
Provoking Games #1 Protection

Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits

https://www.youtube.com/watch?v=LisU_9lc2b0

Provoking Games #2 Collaboration

Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits



https://www.youtube.com/watch?v=hksB27sqGpo

Cybersecurity Cards & Provoking Games

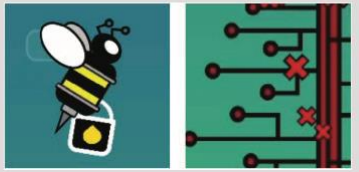
SECRIOUS PROJECT

HERIOT WATT UNIVERSITY
THE GLASGOW SCHOOL OF ART
University of St Andrews

Funded by
UKRI Engineering and Physical Sciences Research Council

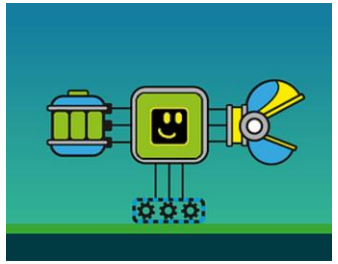
External consultants:
civic digits

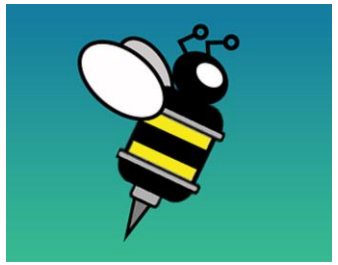
Correspondence between code security **misconceptions**, **reflective motives**, and **cybersecurity cards** or **provoking games** features

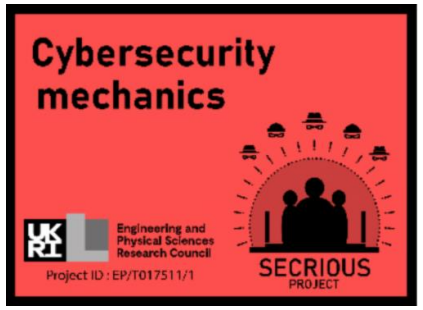
Misconceptions	Reflective Motives	Features of Cards and Games
Code security is for experts	Provide comprehensive code security content in digestible format	
Security is binary with a single solution per issue	One-to-many links with vulnerabilities, and no one-to-one link between attacks and defenses	
Relations between threats and mitigation are straightforward	Discover relationships between threats and mitigation	
The more security, the better	Illustrate the impact of excessive security preventing functionality or usability	
There are no impacts to security mitigation	Make security requirements be an integral part of systems requirements	
Security is only an issue for security experts	Show the impact of disengaging from security matters	
There is a technical solution to all security issues	Illustrate that security technical solutions benefit from being inclusive	
Security is every team's top priority	Highlight that communication about security requires energy and time, which need to be costed	
Using this library works so it can just be added to my code	Show the danger in not vetting library code and external data in the system being developed	
This piece of code is not important so does not need to be secured	Illustrate the impact of insecure code on the ecosystem to advocate for security by default	

Code Security Empowering Workshop

Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits







Code Security Empowering Workshop

1. Cybersecurity cards introduction
2. Deconstructing provoking games
3. Building code security interventions

[IEEE S&P 2025]

The intention in building the participants' confidence and ownership of code security issues is to foster discussion and provide an entry for further information-seeking activities

Secrious Project

Funded by Engineering and Physical Sciences Research Council

External consultants: civic digits

Serious Coding A Game Approach to Security for the New Code-Citizens

HERIOT WATT UNIVERSITY

THE GLASGOW SCHOOL OF ART

University of St Andrews

Funded by Engineering and Physical Sciences Research Council

External consultants: civic digits

EPSRC Project EP/T017511/1

Call: People at the Heart of Software Engineering

New Code-Citizens

- Proximity to software systems
- Not just as users, but as potential creators or contributors
- No formal training

Aim

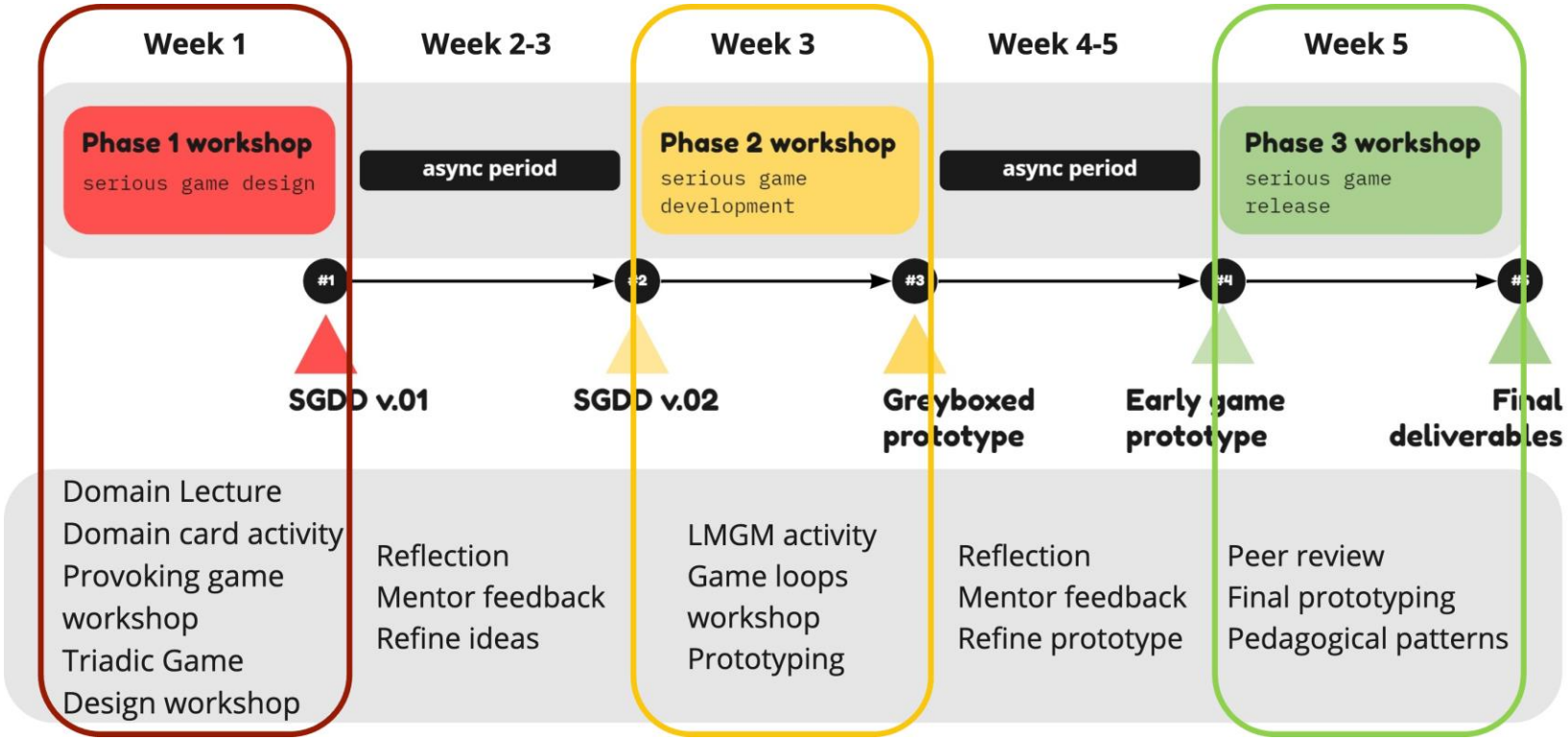
- Engage New Code-Citizens in making the security of software code tangible through the design of serious games

Serious Slow Game Jam

SECRIOUS PROJECT

Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits
HERIOT WATT UNIVERSITY
THE GLASGOW SCHOOL OF ART
University of St Andrews

SSGJ methodology as a mechanism for co-designing serious games with new code-citizens, in the application domain of cybersecurity



Themes

- Code Security
- API Security
- Secure Software Development Lifecycle

[ICGJ23,JCSG23]

Serious Slow Game Jams

SECRIOUS PROJECT

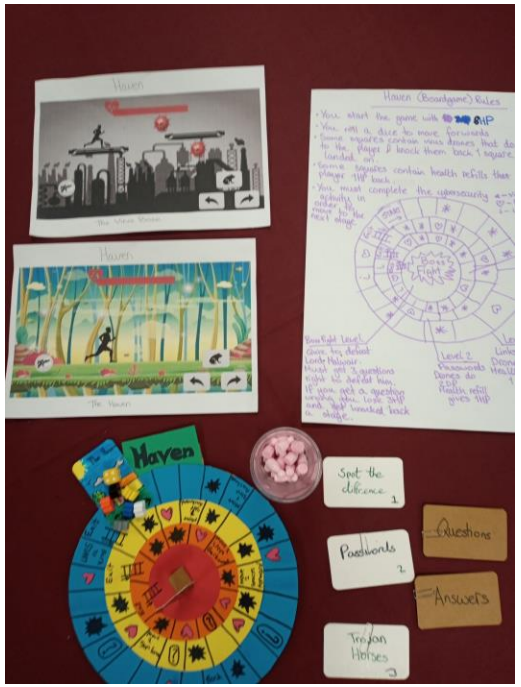
HERIOT WATT UNIVERSITY
THE GLASGOW SCHOOL OF ART
University of St Andrews

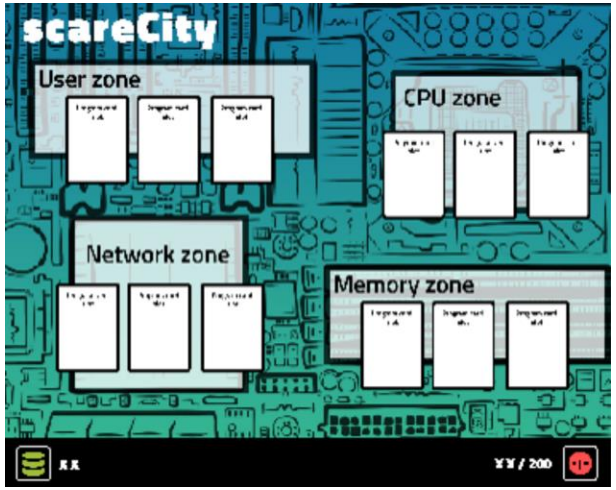
Funded by
UKRI Engineering and Physical Sciences Research Council

External consultants:
civic digits

Themes

- Code Security
- API Security
- Secure Software Development Lifecycle





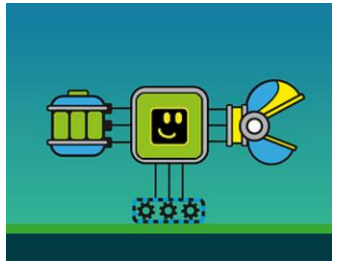
Serious Toolkit

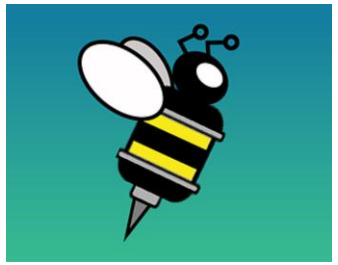
SECRIOUS PROJECT

Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits

HERIOT WATT UNIVERSITY
THE GLASGOW SCHOOL OF ART
University of St Andrews

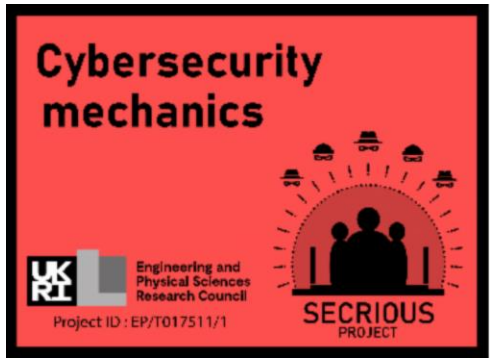
Provoking Games

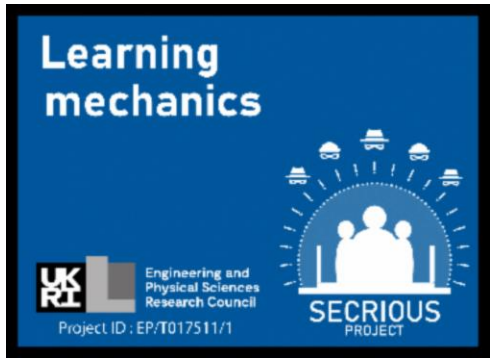


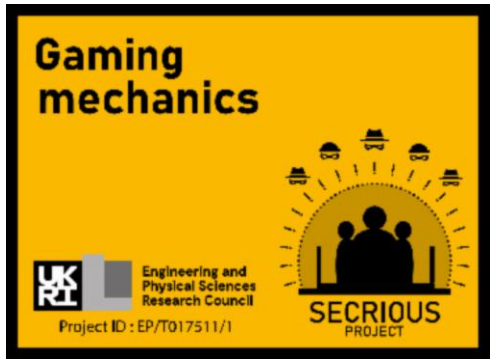


Cards

- Cybersecurity
- Learning Mechanics
- Game Mechanics



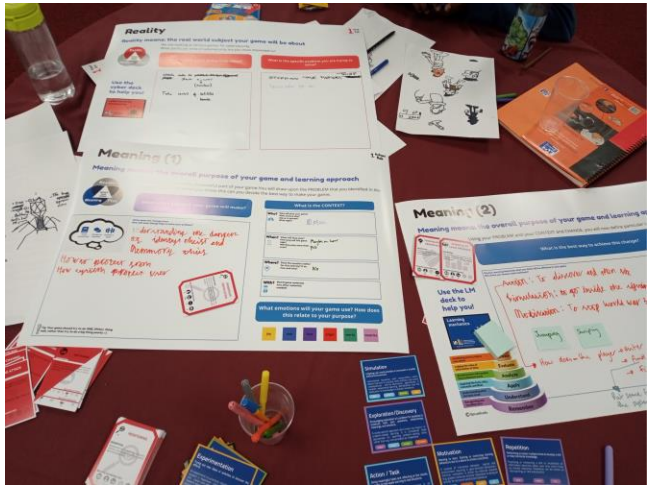




Themes

- Code Security
- API Security
- Secure Software Development Lifecycle

Worksheets



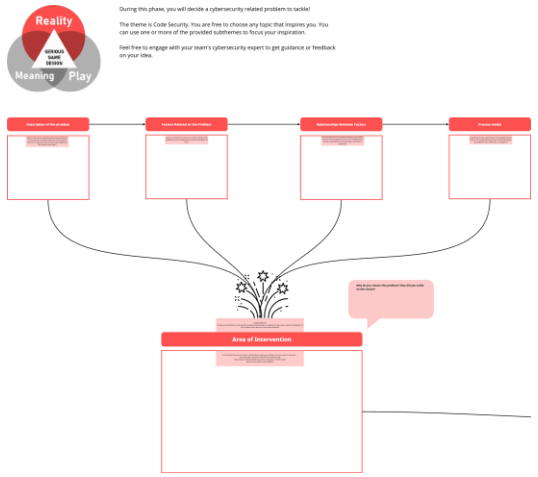
Code Snippets

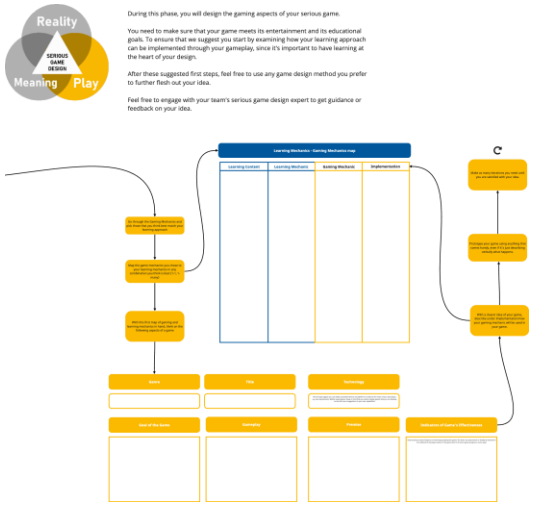
```php
<?php

require_once('../_helpers/strip.php');

// this database contains a table with 2 rows
// This is my first secret (ID = 1)
// This is my second secret (ID = 2)
$db = new SQLite3('test.db');

if (strlen($_GET['id']) < 1) {
  echo 'Usage: ?id=1';
} else {
  $count = $db->querySingle('select count(*) from secrets where id = ' . $_GET['id']);

  if ($count > 0) {
    echo 'Yes!';
  } else {
    echo 'No!';
  }
}
```

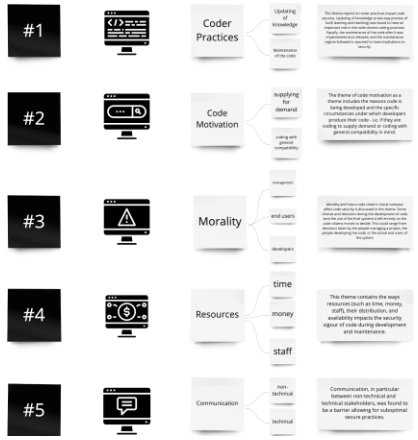
Serious Toolkit

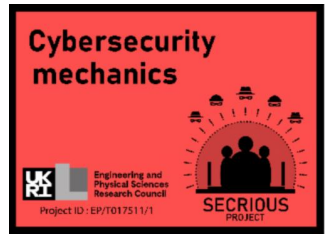
Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits

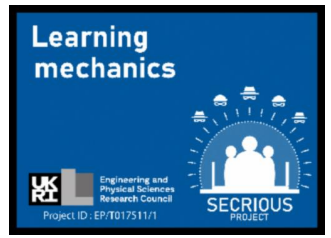
Worksheets

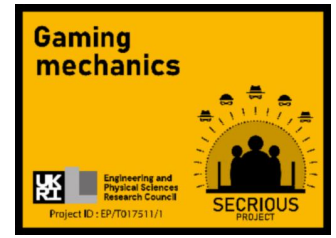












Evaluation

Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits

Slow Game Jam with Students

- 13 participants (11 full answers)
- Conversion MSc computing level
- Game: *Collaboration*
- Theme: Secure software lifecycle
- Cybersecurity cards version 1
- Knowledge and understanding of cybersecurity confidence rose from 12.5% to 62.5%
- 82% students agreed cybersecurity cards provide introductory cybersecurity knowledge to novice users
- 82% students self-efficacy of cards to access knowledge without expert

[ACM Games 2025]

Summer School Slow Game Jam

- 23 participants
- 11–16 yo in late primary or secondary school
- Game: *Protection*
- Theme: Software security
- Cybersecurity cards version 2
- Knowledge and understanding of cybersecurity confidence rose from 41.2% to 76.5%
- 70% of the pupils agreed cybersecurity cards provide introductory cybersecurity knowledge to novice users
- 57% pupils self-efficacy of cards to access knowledge without expert

[CSI 2025]

Evaluation methods

Mixed methods. Pre-/post-Likert questionnaires to measure knowledge; regular questionnaires to measure workload, motivation, and engagement; peer feedback; questionnaire to evaluate how decks of cards used (cybersecurity, learning mechanics, and game mechanics)

Evaluation

Funded by Engineering and Physical Sciences Research Council
External consultants: civic digits

Cybersecurity Cards: User-centred Design, Uses and Evaluation

- Design refined based on user feedback
- **Version 1**: 124-card deck composed of 30 vulnerability, 32 attack, and 47 defence cards, each of which are categorized under one of the 15 general cards
- **Version 2**: 70-card deck composed of 20 vulnerability, 20 attack, and 30 defence cards, with a glossary replacing general cards, with improved linkage among cards

---

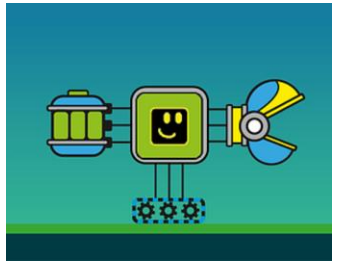
Limitations of Evaluation

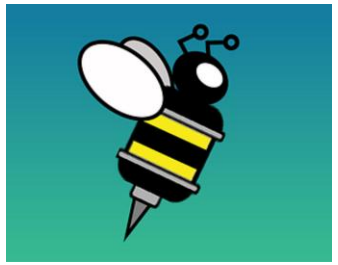
Relatively low number of participants, measure of confidence in knowledge rather than assessed knowledge, evaluation only based on data collection at and immediately after the Slow Game Jam

Beaconing Events

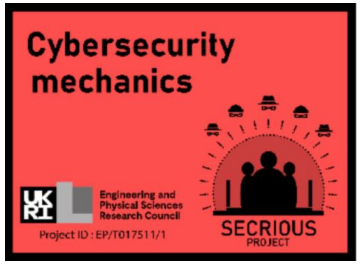
Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits

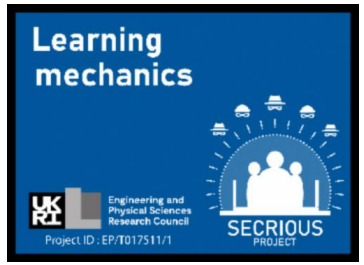
Provoking Games

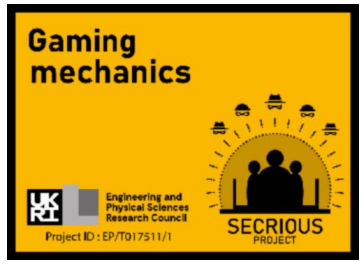




Cards

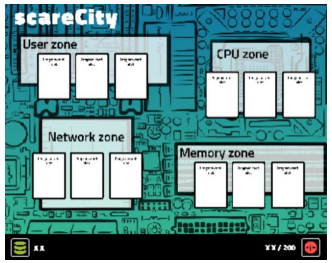






Multiple **Beaconing Events** with experts and new code-citizens to showcase and validate the co-designed serious games, the SSGJ methodology, and SSGJ toolkit

Serious Games

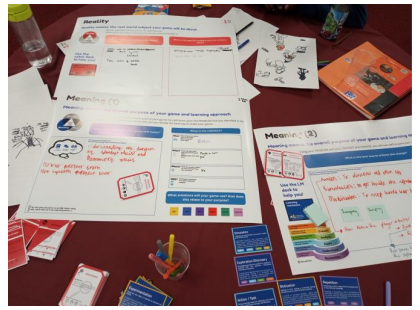


At SOUPS'23

2023 at Abertay cyberQuarter

202X ??

Worksheets



Code Snippets

```php
<?php

require_once('../_helpers/strip.php');

// this database contains a table with 2 rows
// This is my first secret (ID = 1)
// This is my second secret (ID = 2)
$db = new SQLite3('test.db');

if (strlen($_GET['id']) < 1) {
  echo 'Usage: ?id=1';
} else {
  $count = $db->querySingle('select count(*) from secrets where id = ' . $_GET['id']);

  if ($count > 0) {
    echo 'Yes!';
  } else {
    echo 'No!';
  }
}
```

Secrious Project

Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits

Prof. Lynne Baillie
Heriot-Watt University
Principal Investigator

Dr. Manuel Maarek
Heriot-Watt University
Co-Investigator

Sandy Louchart
Glasgow School of Art
Co-Investigator

Dr. Hans-Wolfgang Loidl
Heriot-Watt University
Co-Investigator

Daisy Abbott
Glasgow School of Art
Co-Investigator

Dr. Robert Stewart
Heriot-Watt University
Co-Investigator

Dr. Adam Reed
University of St Andrews
Co-Investigator

Dr. Theodoros Georgiou
Heriot-Watt University
Alumni Research Associate

Dr. Ryan Shah
Heriot-Watt University
Research Associate

Dr. Shenando Stals
Heriot-Watt University
Research Associate

Dr. Jamie Ferguson
Glasgow School of Art
Research Associate

Olga Chatzifoti
Glasgow School of Art
Alumni Research Associate

Dr. Sheung Chi Chan
Heriot-Watt University
Alumni Research Associate

Dr. Laura Whyte
Heriot-Watt University
Public Engagement Co-ordinator

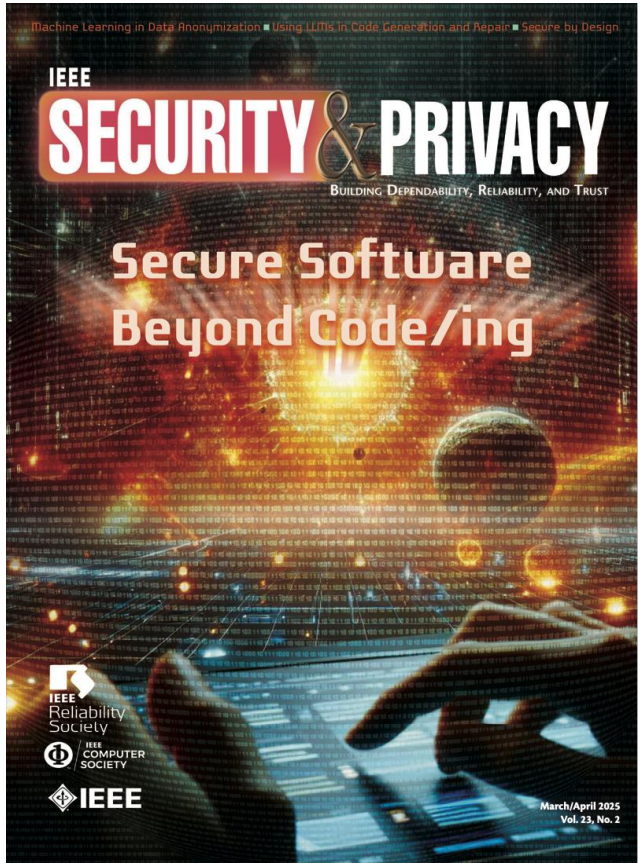
Lauren Hockenhull
Heriot-Watt University
Alumni
Public Engagement Co-ordinator

SECRIOUS PROJECT

https://secrious.github.io/

Secrious Project

Funded by
Engineering and Physical Sciences Research Council
External consultants:
civic digits



[IEEE S&P 2025]

SECRIOUS PROJECT

https://secrious.github.io/

Workshops on Game-Based Approaches for Cyber Security

Workshop on Serious Games for Cyber Security

sicsa* The Scottish Informatics & Computer Science Alliance

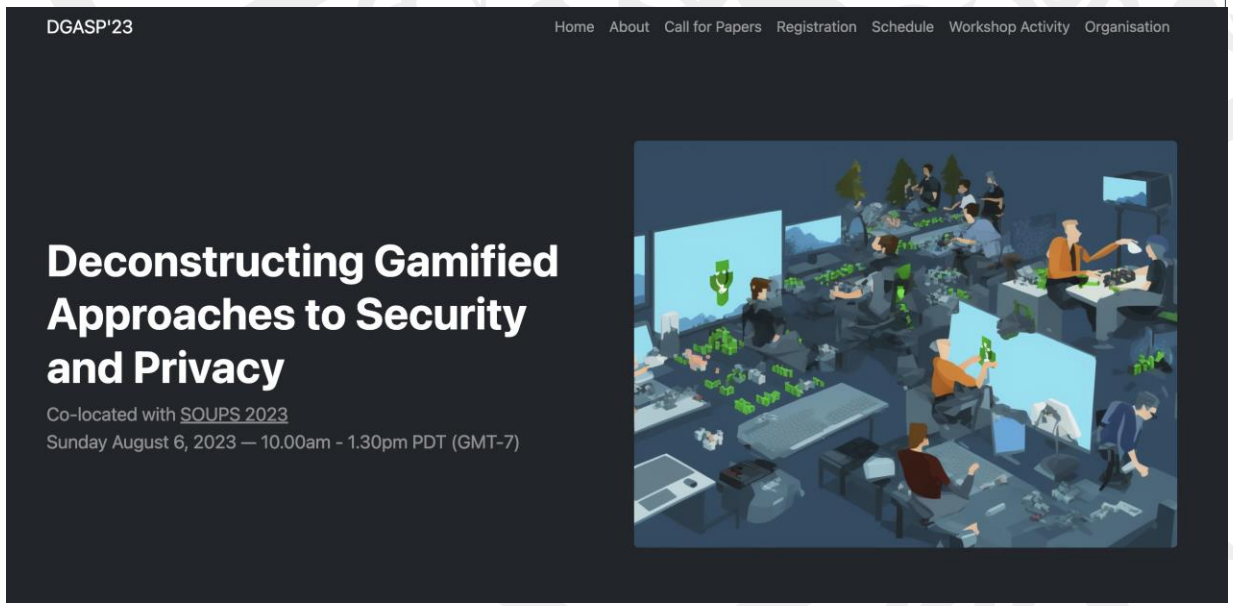
cybersecurity NEXUS

Heriot-Watt University

May 21-22, 2019

https://www.macs.hw.ac.uk/sgcs19/

- 2019 SICSA Workshop in Edinburgh
- 2023 DGASP'23 @ SOUPS'23
- *202X ??*



https://secrious.github.io/dgasp23/

LEADERS IN IDEAS AND SOLUTIONS

Rennes Research Visits

MLSEAN Machine Learning based software systems SEcurity Analysis

- Project supported by the UK-France Science, Innovation, and Technology Researcher Mobility Scheme
- Rennes visits taking place from May 2025 to January 2026
- Preparing Horizon Europe submission
- Building bridges between research communities in Rennes and Edinburgh

Research collaboration

- **Sophie Pinchinat** (formal methods for security)
- **Manuel Maarek** (mixed methods for software security)
- **Michael Lones** (machine learning)
- **Sasa Radomirovic** (formal verification of security protocols)

HERIOT WATT UNIVERSITY

Thank you!
Questions?
Connect!

Manuel Maarek
Heriot-Watt University

May 20, 2025
SoSySec Seminar
Rennes

LEADERS IN **IDEAS** AND **SOLUTIONS**