DEFENCE AGAINST DARK ARTEFACTS

PROTECTING THE SMART HOME

RULES BOOK

INTRODUCTION

The home is a private, secure and personal space for many, but the introduction of smart and IoT devices can potentially open up doors to threats as hackers are able to leverage insecure devices and gain access to your household.

“Defence Against Dark Artefacts: Protecting the Smart Home” is designed to help developers and users of smart technologies to think about the strategies to manage cyberthreats in smart homes. They can play in the shoes of a hacker or a defender of the home network– and discuss the issues they see with colleagues, friends and family. This allows discussion of serious cybersecurity issues in a playful, reflective way. We encourage players to talk about the ways they can relate the game elements to real-life scenarios during their gameplay too.

This board game has been developed as part of the EPSRC-funded research project “Defence Against Dark Artefacts”. Team members were also supported by EPSRC research grants EP/R03351X/1, EP/M02315X/1, and EP/T022493/1.

The team members, Dr Lachlan Urquhart, Dr Jiahong Chen, Stanislaw Piasecki, Adam Jenkins, and Dr Tommy Nilsson would like to thank the participants who took part in our pilot group study as part of the game development.

A digital copy of the game components can be downloaded from [link to github here], or if you would like a professionally printed, ready to play box of the game, it can be purchased from [link to printing service here].

The attribution is “Defence Against Dark Artefacts: Protecting the Smart Home” and authors Dr Lachlan Urquhart, Dr Jiahong Chen, Stanislaw Piasecki, Adam Jenkins, and Dr Tommy Nilsson.

University of Nottingham UK | CHINA | MALAYSIA
THE UNIVERSITY of EDINBURGH
UKRI Engineering and Physical Sciences Research Council
horizon DIGITAL ECONOMY RESEARCH

OBJECTIVES

Defenders

- Remove all Security Bugs from your Smart Home Network, or:
- Capture the Hacker

Hacker

- Compromise a total of 13 Devices.
- Compromise their Secret Target.

GAME SETUP

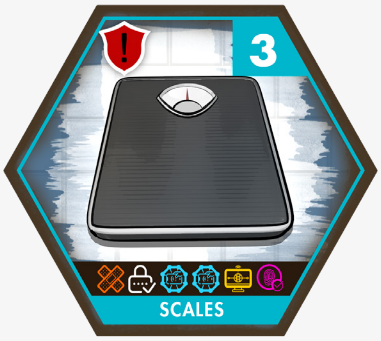
1. Shuffle the Device Tiles and lay them out face-up to create a Smart Home network. Players are welcome to create their own custom layout; however, we su gest the following set up:

2. Set Up the Security Bugs, Firewalls and DDoS tokens where all players can reach them.

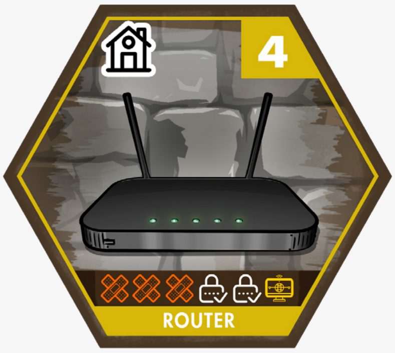
3. Shuffle and place the Knowledge Tokens face-down where all players can reach them.

4. Shuffle the Hacker Deck and place it face down in the Hacker Attacks Position. Then take the Hacker's Secret Target cards and shuffle those placing them to the side of the board.

5. Place the starting Security Bugs on all tiles containing the 🛡 symbol. Each Tile will receive Bug tokens equal to 2 lower than the Security Capacity. For example, the tile here will receive 1 token on it:



6. Player's should decide who is the Hacker (We recommend the player with the most board game experience). The remaining players should choose roles from the Defender characters and place them on their starting position on the Router (seen below). The defending team/player should use all of the Characters available to tackle the Hacker.



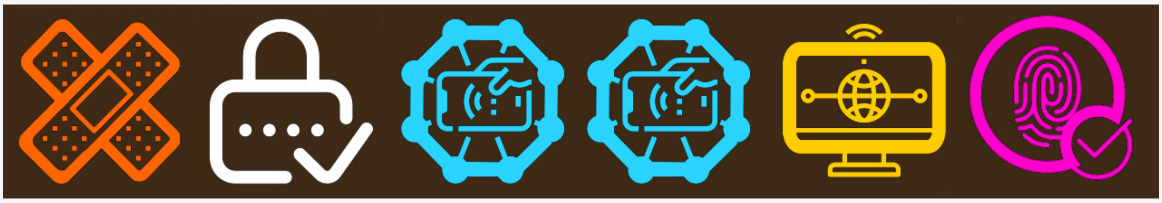
7. The Hacker will then draw one Secret Target Card, giving them their secret objective for the game.

8. Then, the Hacker will then draw 5 hacker cards and must then secretly choose a starting position on the Smart Home network.

9. After this step the game is ready to begin, and the Defenders will decide the order in which each character plays. This order is maintained for the rest of the game.

DEVICE TILES

Each Device tile is double-sided, with the front displaying the device and its security requirements (For this version devices are not shown) and the back shows the device's compromised state. All devices will start face up but will be flipped as the game is played and the Hacker's influence spreads.



DICE COMBINATIONS

All Tiles have a series of 6 numbers along the bottom of the tile and represent the security mechanisms you must roll in order to successfully defend a device. The symbols represent:

Patching – Patches, or updates, are changes to existing software or firmware. Along with introducing new features, patches are also used to plug existing Security Vulnerabilities. Keep devices secure by keeping them up to date!

Password Change – A strong password is your first line of defence against intruders and Hackers, however IoT devices have been shown to have weak or insecure default passwords. Combat this by changing the passwords of the device to one that is strong and secret!

Privilege Access Management – To maintain control over a device, we must first know which functions and features are active. By restricting the Privileges of a device to only those resources absolutely required to perform routine, legitimate activities, you reduce the potential avenues for Hacker's to use.

Anti-Virus Software – Similar to Anti-virus software on your Laptop or PC, Anti-virus software exists for your IoT devices. The software will monitor and protect your devices from known viruses which are active in the wild.

Network Monitoring – Through monitoring the traffic entering and leaving an IoT device, you will be able to detect unwanted behaviours which may indicate a breach in your Smart Home Security. Keep aware of the traffic shared on your network and the between connected devices.

Two Factor Authentication – Like the one-time codes sent to your mobile — can keep the bad guys out of your accounts and out of your devices. If your smart-device apps offer two-factor authentication, or 2FA, use it!

Security Bug Limit – All tiles have a number on them that indicates how many Bugs are needed to overcome the Security limit of that tile. Once the number of Bug tokens on that tile equals or exceeds the Security limit, that tile will become Compromised.

PLAY DETAILS

Order of Play – Each defending player's turn consists of these 3 phases in this order:

1. Move up to 2 tiles
2. Defend a Device or Attempt to Capture the Hacker.
3. Hacker will then have their turn after each Defender's turns
   -Play an Attack available in their hand.

Steps 1-3 are repeated 4 times until all Defenders have had their turn and the Hacker has reacted to each Defender, the Hacker may now move from their starting position.

DEFENDER DETAILS - MOVE UP TO 2 TILES

- You are not required to move.
- You immediately end your movement when you enter a tile that is Compromised.
- You cannot enter a DDoS tile.
- You can leave a Compromised and DDoS tiles.
- You can move through Firewalls, but the Hacker can't.
- There is no limit to the number of players that can be on the same tile. In fact, there are advantages to teaming up

DEFENDER DETAILS - DEFEND DEVICE

- After you have finished moving, you have the option of rolling the dice to defend against an attack on the tile you are on.
- If you end your movement on a tile that is not under attack, you still have the option of rolling the dice to place a Firewall (see details in the section under Match 3 dice).
- To defend the device, roll all 6 defender's dice and attempt to match as many symbols as possible to the combination shown on the current tile.

- The dice do not need to be matched in any particular order. Only the number of matching symbols matters.
- You may set aside as many matching dice as you wish after each roll, but you MUST set aside AT LEAST 1 matching die after every roll.
- As long as you set aside at least 1 matching die, you may continue by rerolling as many remaining dice as you wish.
- Once the remaining dice have been rolled, any matching dice that were set aside are now locked and cannot be rerolled.
- You may stop at any time and resolve your results, but there are no rewards for matching fewer than 3 dice. (See Failure.)

Success — The more dice that match the combination, the better your battle against Security Bugs and the greater the rewards.

- **Match 3** dice = Take 1 Firewall token from the supply and place it between any side of the tile you are on and an adjacent tile. This can be done even on tiles that are not currently under attack.
- Firewalls affect both tiles they border.
- Firewalls prevent the Security Bugs from being spread by a BotNet Spread attack or Compromised device (see below).
- You must place the Firewalls when you earn it and cannot save it for later use.
- **Match 4** dice = Remove 1 Bug token from the tile you are on.
- **Match 5** dice = Remove 1 Bug token from the tile you are on and then choose to either take and place 1 Firewall OR take 1 Knowledge Token for later use
- **Match 6** dice = Remove 2 Bug tokens from the tile you are on and then take and place 1 Firewall AND take 1 Knowledge token for later use.
- If your success would allow you to remove more Bug tokens than there are on the tile, you just remove all Bug tokens on your tile. Any “extra” are lost.
- You may choose to take a lesser reward instead of the one you rolled. (For example, placing a Firewall instead of removing 1 Bug token, even if you matched 4 dice.

Failure — If you roll the dice and are not able to match at least 1 symbol on the combination, even after using your Character ability or a Token, you have failed to contain the Bug and cause an Error to be introduced. Error Introduction:

1. Set all the dice aside, cancelling any locked dice.
2. Add 1 Bug token to the tile you are currently on. This may cause the tile to Compromise. (See Compromised Devices). End your Defend phase.

CHECK FOR HACKER

Instead of defending a device, Defensive players are able to attempt to capture the Hacker by Checking a tile they are on or are adjacent to. The Hacker must respond to the check:

- If the hacker is on that tile, they must admit it and the Defender's have won the game
- If the hacker is not on the tile but have previously been on that tile, they must inform the Defenders.

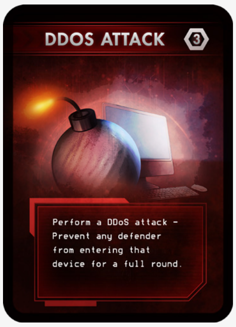
Support — Fixing security issues alone is difficult. Working as a team will increase your odds of success. For every other Defender on the same tile as you, you gain 1 Support. Each Support allows you to avoid 1 Error being introduced when you fail to match at least 1 symbol on a roll of the dice.

HACKER'S TURN

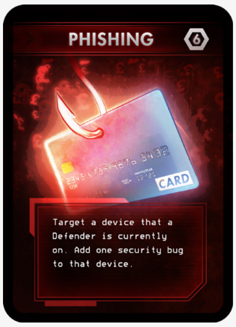
Once a single Defending Character is done with their actions, it is now the Hacker's turn. On their turn they may play one attack card from their hand, and then replenishing their hand (Total of 5 cards) by drawing from the Attack Pile, as illustrated to the right.

Once the Hacker has had 4 goes after each of the 4 Characters, the Hacker may take a movement action. Performing attacks aid the Hacker in spreading their Bot-Net throughout the Smart Home but may reveal some information as to their locations aiding Defenders in capturing the Hacker.

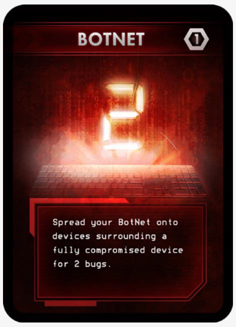
Attacks — Attacks are drawn from the Hacker Attack pile and are played one at a time after each Defender's turn. The Attacks Available are:


DDOS ATTACK
3
Perform a DDoS attack - Prevent any defender from entering that device for a full round.

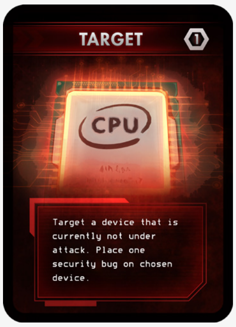
Distributed Denial of Service (DDoS) – The Hacker may choose any device within 3 moves of their location and block any characters from defending or entering that device for one full round (all defenders have a turn)


PHISHING
6
CARD
Target a device that a Defender is currently on. Add one security bug to that device.

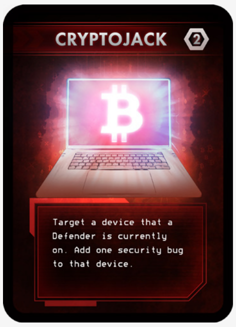
Phishing Attack – The Hacker may target a device that a defender is currently on and can place one Bug token on that device. This attack can be done from any location.


BOTNET
1
Spread your BotNet onto devices surrounding a fully compromised device for 2 bugs.

BotNet Spread – The Hacker may use any Compromised device to spread bugs to any adjacent node. The number of bugs the hacker can add is detailed by the number of that card e.g 3 Security bugs for the example on the left.


TARGET
1
CPU
Target a device that is currently not under attack. Place one security bug on chosen device.

Target Device – The Hacker can target a device that is currently not under attack and place a Security Bug on any device that is within 1 space of the Hacker’s current position.


CRYPTOJACK
2
Target a device that a Defender is currently on. Add one security bug to that device.

CryptoJacking – The Hacker will focus their attack on a device that is already under attack and may place a single Security Bug on the chosen device.

HACKER MOVEMENT

Once all characters have all had a turn and the Hacker has reacted to each move, the Hacker is now free to move within the Smart Home network. The number of spaces the Hacker may move is dependent on the number of Compromised devices they have achieved:

- **0 Compromised Devices** – allows the Hacker to move a total of 1 space.
- **4 Compromised Device** – allows the Hacker to move a total of 2 spaces.
- **9 Compromised Devices** – allows the Hacker to move a total of 3 spaces.

The hacker cannot move through Firewalls or through tiles where a Defender is currently placed.

COMPROMISED DEVICES

Any time the number of Bug tokens on a tile equals or exceeds the Security Limit shown, that tile is now under the full control of the device and is Compromised. Tiles can become Compromised when a player fails to fix a Bug and causes an Error to be introduced or after a Hacker's attack card is played. Compromising is resolved in this order:

1. Remove all Bug tokens from the Compromised tile and return them to the supply.
2. Flip the tile over so that the Compromised side is facing up and return the tile to its position on the board.
3. Add 1 Bug token to the adjacent tile with the lowest Security limit that is not blocked by a Firewall.
4. If there is more than 1 tile with an equally low Security limit, then the Hacker decides where the bug is placed.
5. Bug tokens spread by a device being Compromised are added to a tile whether that tile is already under attack or not. This may cause additional devices to Compromise. If all edges of a Compromised tile are blocked by Firewalls or the edges of the board, then no Bug tokens are added. Resolve the first Compromise before adding bugs to additional tiles.

    a. If multiple tiles receive enough Bug tokens to become Compromised at the same time (from a BotNet Spread, etc.), resolve Compromised devices in numerical order by the Security Limits of those tiles.

    b. If there is more than 1 tile that will Compromise and they all have the same Security Limit, the hacker may choose the order in which those tiles become Compromised.

Secret Targets – There are a number of rooms in the house and each come with their own risks to the inhabitants. As a Hacker, you will have a secret goal of attacking and compromising one of the devices in a particular room. This Secret Target is chosen randomly at the beginning of the game and is kept secret from the Defenders.

The targeted device is usually the device with the Highest Security Capacity for that Room or Type of device. If the Hacker is able to compromise this device, they must immediately reveal their Secret Target card and announce they have won the game.

CHARACTERS

Each character has a special ability that is related to their role on the team. All Defender's begin on the Router.

NETWORK KNOW-IT-ALL
One time on your turn, you may move 1 other player 1 tile, with their permission.

Network Know-it-All - Coordinates the household and helps them choose where to fight the fire.

- One time on your turn, you may move 1 other player 1 tile, with their permission.
- You are unable to move players into Devices that are fully Compromised.

SECURITY EXPERT
On your turn, you may change any Patch rolled into Anti-Virus or change Anti-Virus into Patch.

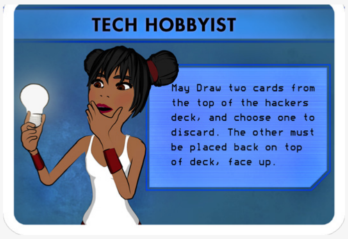
Security Expert - An expert in device security, knows where to find patches and manage anti-virus software

- On your turn, you may change any Patch rolled into Anti-Virus or change Anti-Virus into Patch.
- You may change as many Patch or Anti-Virus as you wish each time you roll.
- Once you roll any remaining dice, any dice that were set aside are locked and cannot be changed.

PASSWORD WHIZZ
On your turn, you may change any Passwords rolled into 2FA or change 2FA into Passwords

Password Wizz - Adept at changing passwords and organising two factor authentications for devices.

- On your turn, you may change any Passwords rolled into 2FA or change 2FA into Passwords
- You may change as many Passwords or 2FA as you wish each time you roll.
- Once you roll any remaining dice, any dice that were set aside are locked and cannot be changed.


TECH HOBBYIST
May Draw two cards from the top of the hackers deck, and choose one to discard. The other must be placed back on top of deck, face up.

Tech Hobbyist - Instead of allowing the hacker to choose their attack, the Hobbyist draws the 2 cards from the hacker's deck

- You can show the cards to the other players and discuss strategy.
- Choose 1 card to play and return the other card facedown to the top of the deck.

KNOWLEDGE TOKENS

- Knowledge tokens are gained by rolling at least 5 dice that match the faces on the tile
- Keep tokens you gain faceup near your Defender's card until you use or discard them.
- All tokens are single use only.
- Put used and discarded tokens in a faceup discard pile near the token supply. If a player needs to draw a token and none are available, mix up the discarded tokens facedown to create a new draw pile.
- Tokens cannot be played on the same turn they are acquired by success fighting a fire.
- You may have a maximum of 3 tokens at any time. If you gain a 4th token, you must immediately discard 1 token of your choice.
- You can play tokens only on your turn.
- You can play as many tokens as you have, but they must be played before the Hacker's action.
- Tokens with dice icons on them are used as if they were a die with the icons shown. It may be helpful to think of them as a 7th die.
- Dice icon tokens can be played after rolling to prevent you from failing.
- Once a token with dice icons is played, you must declare which face it is being used as, and it cannot be changed.

Sharing Tokens

- Any time on your turn that you are on the same tile with another player, you may take 1 token from that player, with their permission.