Department of Security and Crime Science

Systematic evaluation of security attacks to household consumer smart doorbells

Ashley Mark Brown ashley.brown.21@ucl.ac.uk
Nilufer Tuptuk n.tuptuk@ucl.ac.uk
Enrico Mariconti e.mariconti@ucl.ac.uk
Shane D Johnson shane.johnson@ucl.ac.uk

Overview of presentation

- Background and motivation
- Overview of the threat model
- Sampling methodology used to select 9 doorbells
- Methodology for testing doorbells against security threats

- Are the doorbells secure?
- What cybercrimes could be facilitated?
- Do the 9 doorbells meet UK regulatory requirements?

- Process of responsible disclosure

Background

- Smart doorbells are becoming more popular
- They are becoming a part of our everyday lives
- They assist in tackling urban crimes
- Almost one in three Brits (29%) have installed security measures such as smart doorbells and security cameras (Aviva, 2025).

Gadgets in the home	Percentage of UK adults who own this already	Percentage of UK adults who plan to buy in next 12 months
Wireless charging station	21%	14%
Air purifiers	20%	12%
Robot vacuum cleaners	10%	15%
Portable projector	9%	11%
Electric standing desk	7%	10%
Connected exercise equipment e.g. exercise bike	8%	10%

Source: Aviva

Motivation

- A systematic search identified a couple of Master dissertations that explored security threats to doorbells
  - Liu, X. (2021). Ethical Hacking of a Smart Video Doorbell, KTH Royal Institute of Technology.
  - Pétursson, A. (2023). Ethical Hacking of a Ring Doorbell, KTH Royal Institute of Technology.

- These two studies only examined one doorbell and selected this doorbell in an ad-hoc fashion.
  - One of the studies did no Wi-Fi attacks
  - The other only conducted part of a Wi-Fi attack
  - These studies did a limited set of attacks
- To the best of our knowledge, no peer-reviewed studies have examined the vulnerabilities of consumer smart doorbells.

Threat Model

Threat Model was divided into 5 causal categories:

Victims	Adversaries	Vulnerabilities	Security threats	Crimes

Victims

General victim profiles that were considered for security threats to smart doorbells were:

Victims
General population
Wealthy Civilians
High-profile individuals
Organisations and Institutions

Adversaries

General adversaries that were considered for security threats to smart doorbells were:

Victims	Adversaries
General population	Opportunistic criminals Personally known individuals
Wealthy Civilians	Individual criminals Personally known individuals Organised crime groups
High-profile individuals	Organised crime groups State-level adversaries
Organisations and Institutions	Competitors Organised crime groups State-level adversaries

Vulnerabilities

Different vulnerabilities associated with consumer smart doorbells that pose a threat to all victim and adversary profiles include:

Victims	Adversaries	Vulnerabilities
General population	Opportunistic criminals Personally known individuals	Default or weak credentials Weak encryption Missing security updates/patching Insecure protocols Absence of data backup Insecure cloud storage Supply chain issues (e.g. backdoors)
Wealthy Civilians	Individual criminals Personally known individuals Organised crime groups	
High-profile individuals	Organised crime groups State-level adversaries	
Organisations and Institutions	Competitors Organised crime groups State-level adversaries	

Security threats

Different security threats consumer smart doorbells pose to all victim and adversary profiles include:

Victims	Adversaries	Vulnerabilities	Security threats
General population	Opportunistic criminals Personally known individuals	Default or weak credentials Weak encryption Missing security updates/patching Insecure protocols Absence of data backup Insecure cloud storage Supply chain issues (e.g. backdoors)	Account compromise Data leakage Malware injection Cloud attacks Man-in-the-middle (MiTM) DoS/DDoS Wireless Jamming Supply chain compromise Malicious updates Unauthorised physical access
Wealthy Civilians	Individual criminals Personally known individuals Organised crime groups		
High-profile individuals	Organised crime groups State-level adversaries		
Organisations and Institutions	Competitors Organised crime groups State-level adversaries		

Crimes

Different crimes consumer smart doorbells might facilitate include:

Victims	Adversaries	Vulnerabilities	Security threats	Crimes
General population	Opportunistic criminals Personally known individuals	Default or weak credentials Weak encryption Missing security updates/patching Insecure protocols Absence of data backup Insecure cloud storage Supply chain issues (e.g. backdoors)	Account compromise Data leakage Malware injection Cloud attacks Man-in-the-middle (MiTM) DoS/DDoS Wireless Jamming Supply chain compromise Malicious updates Unauthorised physical access	Burglary/robbery Stalking Unauthorised surveillance Harassment Domestic abuse and coercive control Data theft Identity theft Computer misuse Extortion
Wealthy Civilians	Individual criminals Personally known individuals Organised crime groups			
High-profile individuals	Organised crime groups State-level adversaries			
Organisations and Institutions	Competitors Organised crime groups State-level adversaries			

Sampling method for doorbell selection

AIM:

- To select consumer smart doorbells that are popular in the UK

METHODOLOGY:

- Four most popular electronics merchants searched (i.e. Currys, Amazon, Argos and John Lewis)
- A set of search terms that included “Smart” AND “Video” AND “Doorbell”
- A set of pre-selected pricing categories (i.e. High, Medium, Low and Cheap)
- Selected doorbells with the highest number of total reviews and an average rating of 4 stars or more

Doorbells Sampled

From 123 available in major UK stores including Amazon

Doorbell	Retailer	Total # of Reviews	Mean Rating	Price Category	Price (£)
EZVIZ CP4	Amazon	4300	4.3	High	104.54
AOSU	Amazon	5530	4.4	High	119.99
Amazon Ring	Amazon	77018	4.6	Medium	99.99
Amazon Blink	Amazon	18344	4.1	Medium	59.99
*Arlo AVD2001	John Lewis	67	4.8	Medium	99.99
XTU	Amazon	3260	4.3	Low	49.99
eudic T3	Amazon	2629	4	Low	29.99
Demtom	Amazon	35	4	Cheap	24.40
WASHLA	Amazon	4	3	Cheap	18.99

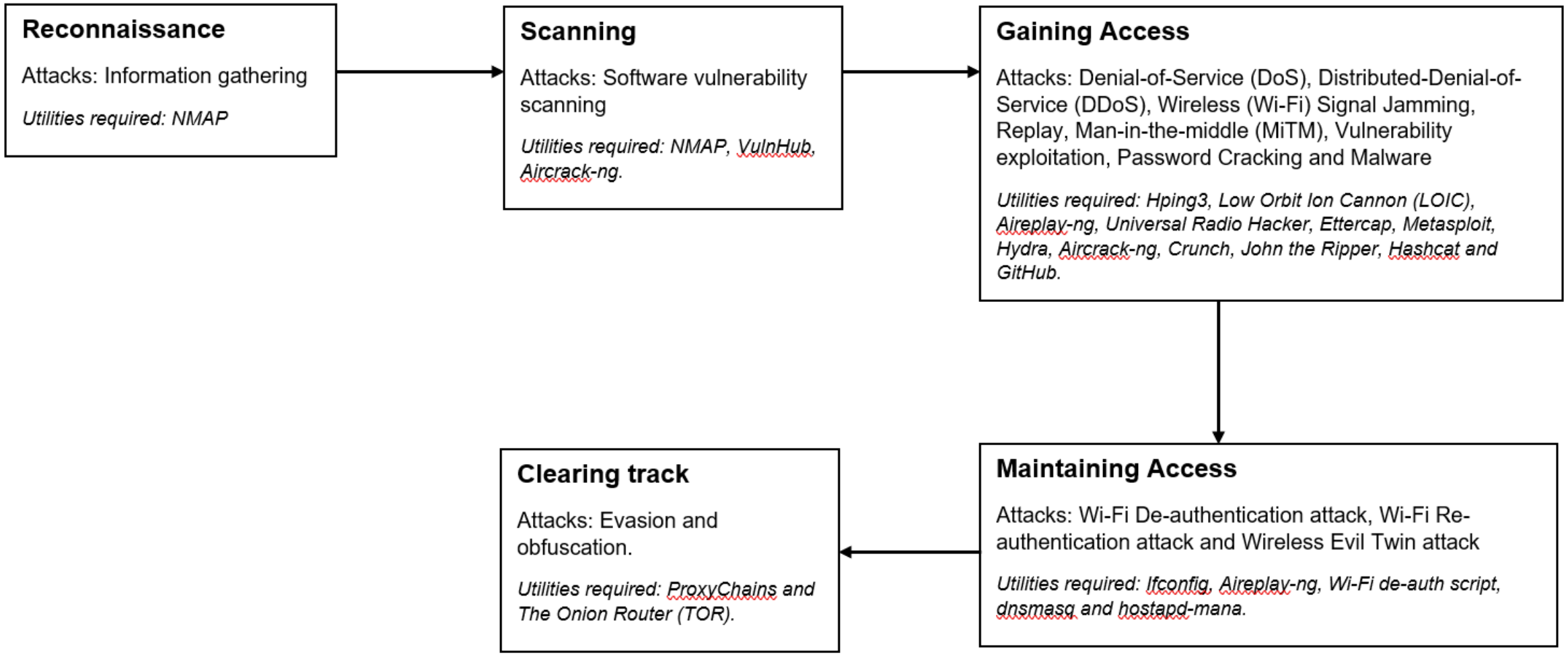
The four pricing categories were defined as:
Cheap: < £25
Low: £25 ≤ price < £50
Medium: £50 ≤ price ≤ £100
High: > £100

Methodology for testing doorbell vulnerability to attacks

Two cybersecurity frameworks were used when testing the doorbells to develop the attack strategy. These frameworks were:

- EC-Council's Five-Phase Process to Penetration Testing
- The Open Web Application Security Projects (OWASPs) Web Application Penetration Testing Framework

EC-Council's Five-Phase Process to Penetration Testing

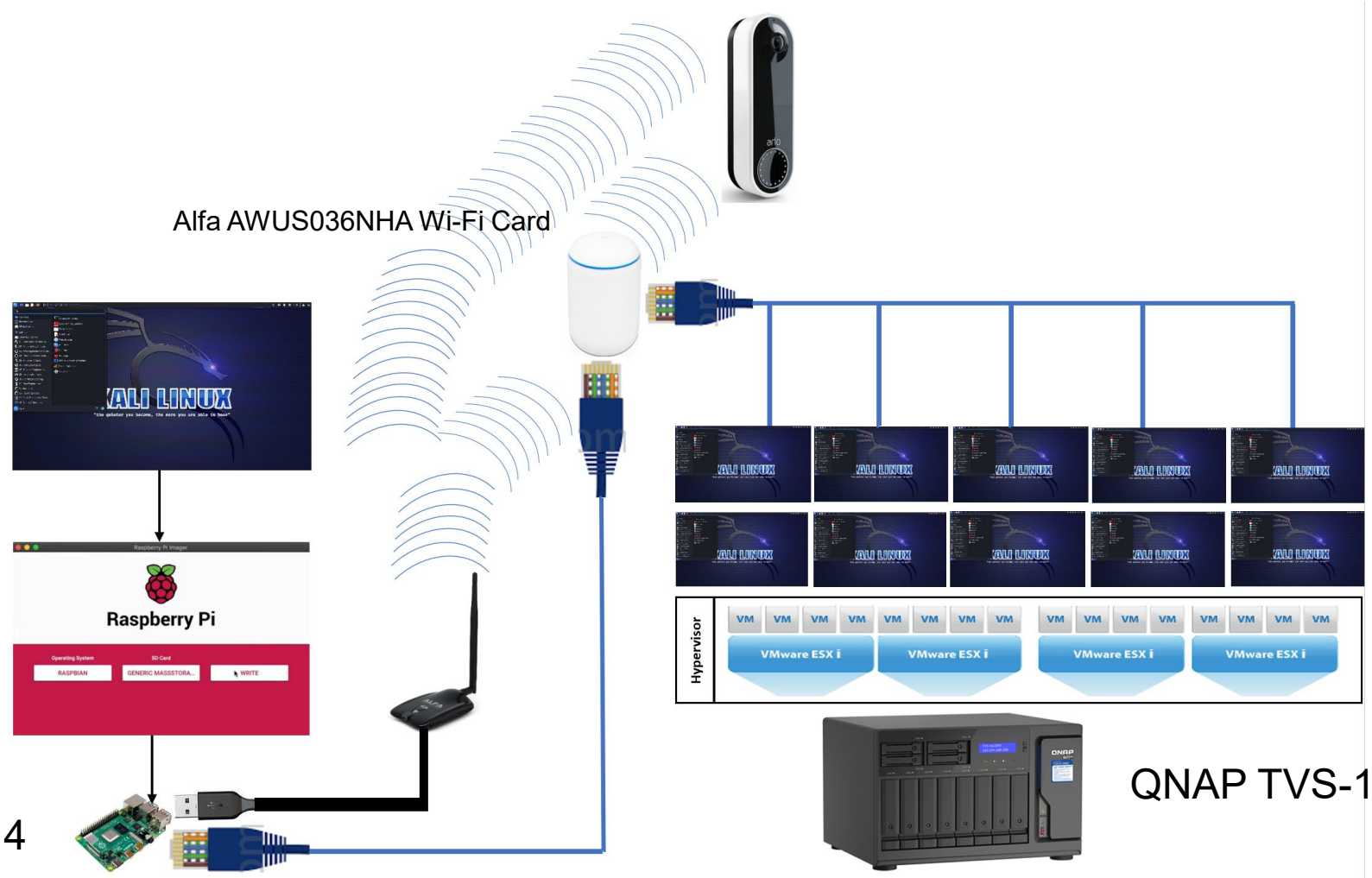


OWASPs Web Application Penetration Testing Framework

- Injection attacks
- Cross-site Scripting (XSS)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross-site Request Forgery (CSRF)
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to restrict URL access
- Insufficient Transport Layer Protection
- Unvalidated Redirects or Forwards

Topology of Lab Environment used for attacks

Isolated Lab Environment used to test the nine doorbells against the cyber-attacks identified:



Offensive Security
Kali Linux 2022.1
ARM64 Version

Raspberry Pi Imager
Version 1.7.3

Raspberry Pi 4

Offensive Security
Kali Linux

VMware vSphere
ESXi Hypervisor 6

QNAP TVS-1282T3 NAS

Attacks Employed

On Premises attacks	Remote attacks	Outside Dwelling
Denial-of-Service (DoS) attacks	Manufacturer Website Password Cracking attacks	Wi-Fi Jamming attacks
Distributed-Denial-of-Service (DDoS) attacks	Brute Force Wi-Fi Handshake Password Cracking attacks	Wi-Fi Evil Twin attacks
Man-in-the-Middle (MiTM) attacks	Dictionary Wi-Fi Handshake Password Cracking attacks	Replay attacks
Metasploit Vulnerability Exploitation	Malware	
OWASP Web Application Vulnerabilities		

Results for the nine doorbells tested

Price Category	Doorbell	DoS attack	DDoS attack	Wi-Fi Radio Signal Jamming	Replay attack	MiTM attack	Metasploit vulnerability exploitation	Wi-Fi evil twin attack	Wi-Fi Handshake Password cracking attack	Web-based Password Cracking attack	Malware attack	OWASP Web App
High	EZVIZ CP4	✓	✓	✓	✗	✓	✗	✓	✓	✗	N/A	✗
	AOSU	✓	✓	✓	✗	✓	✗	✓	✓	✗	N/A	✗
Medium	Arlo AVD2001	✓	✓	✓	✗	✓	✗	✓	✓	✓	N/A	✗
	Amazon Ring 2nd Gen	✓	✓	✓	✗	✓	✗	✓	✓	✗	N/A	✗
	Amazon Blink	✓	✓	✓	✗	✓	✗	✓	✓	✗	N/A	✗
Low	XTU	✓	✓	✓	✗	✓	✗	✓	✓	✗	N/A	✗
	eudic T3	✓	✓	✓	✗	✓	✗	✓	✓	✗	N/A	✗
Cheap	Demtom	✓	✓	✓	✗	✓	✗	✓	✓	✗	N/A	✗
	WASHLA	✓	✓	✓	✗	✓	✗	✓	✓	✗	N/A	✗

Compliance with UK DSIT regulation?

THE PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE (SECURITY REQUIREMENTS FOR RELEVANT CONNECTABLE PRODUCTS) REGULATIONS 2023

2023 No. 1007

DSIT Requirement	Arlo AVD2001	EZVIZ CP4	AOSU	Amazon Ring	Amazon Blink	XTU Wireless	Eudic T3	Demtom	WASHLA
1 - Unique passwords that are not resettable to any universal factory setting	✓	✓	✓	✓	✓	✓	✓	✓	✓
2 - Public point of contact to report security vulnerabilities	✓	✗	✓	✓	✗	✗	✗	✗	✗
3 - Explicitly state the minimum length of time before software update are no longer available	✗	✗	✗	✗	✗	✗	✗	✗	✗

Responsible disclosure of vulnerabilities

Price Category	Doorbell	Responded
High	EZVIZ CP4	✗
	AOSU	✗
Medium	Arlo AVD2001	✓
	Amazon Ring 2nd Generation	✓
	Amazon Blink	✗
Low	XTU	✗
	eudic T3	✗
Cheap	Demtom	✗
	WASHLA	✗

Estimated cost of conducting attacks

	DoS attack	DDoS attack	Wi-Fi Radio Signal Jamming	Replay attack	MiTM attack	Metasploit VE	Wi-Fi Evil Twin attack	Password Cracking attack	OWASP Web App Vulnerabilities
Attacker skill level	Beginner	Beginner	Advanced	Intermediate	Intermediate	Intermediate	Advanced	Advanced	Advanced
Items required	Raspberry Pi 4 running Kali Linux	Raspberry Pi 4 running Kali Linux	Raspberry Pi 4 running Kali Linux and Alfa AWUS036NHA	Raspberry Pi 4 running Kali Linux, HackRF and Universal Radio Hacker	Raspberry Pi 4 running Kali Linux	Raspberry Pi 4 running Kali Linux	Raspberry Pi 4 running Kali Linux and Alfa AWUS036NHA	Raspberry Pi 4 running Kali Linux	Raspberry Pi 4 running Kali Linux
Estimated attack cost	£80	£80	£100	£300	£80	£80	£100	£80 - £100	£40
Execution	On premises	On premises	On premises/outside dwelling	On premises/outside dwelling	On premises	On premises	Outside dwelling	Remote	On premises

Conclusion

- Higher doorbell price did not equal better security
- DoS and DDoS attacks can be perpetrated at relatively low cost and skill level – offences facilitated include domestic abuse or stalking

- Wi-Fi Jamming and Evil Twin attacks require a higher level of skill and are relatively more costly

  - Evil Twin attacks can facilitate all other attacks even if the attacker does not know the victim as the doorbell is forced onto a malicious network controlled by the attacker

  - Can be conducted 10 metres away (probably much further) - attacker could perpetrate this against a wealthy or high-profile individual

- Limited compliance with DSIT's IoT legislation

  - All doorbells compliant with the 1st requirement,
  - Some compliant with the 2nd, none with the 3rd

- Wi-Fi Jamming and Wi-Fi Evil Twin attacks can be mitigated by Power over Ethernet (higher cost)

- Future research should look to investigate the attack to mitigation association for smart doorbells

Thank you very much for listening

Any Questions?