“We’re All Happily Married Here!”

Developing an Intimate Threat Security Review

Julia Slupska

DPhil Candidate

UNIVERSITY OF OXFORD

CENTRE FOR DOCTORAL TRAINING *in* CYBER SECURITY

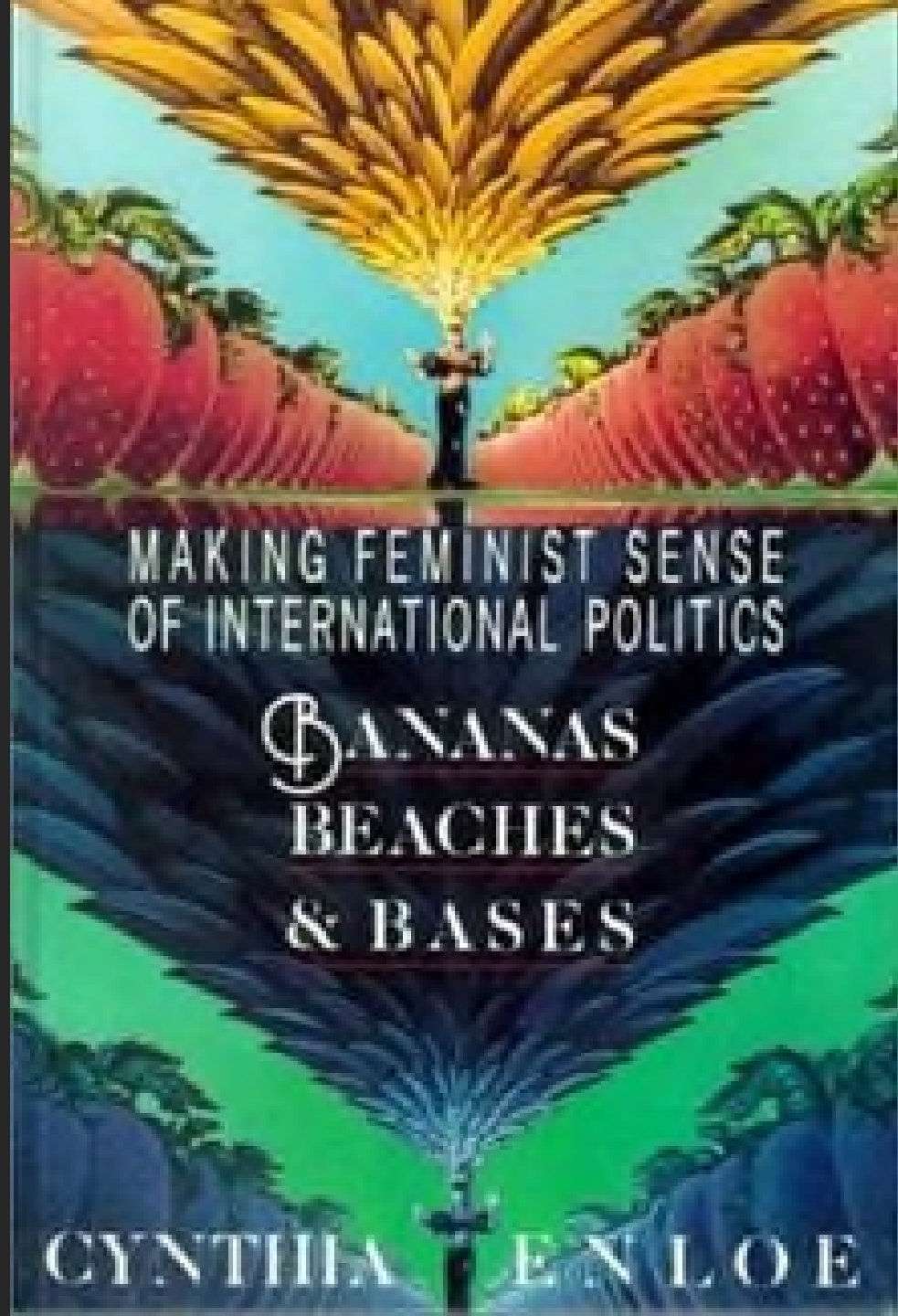
EPSRC Engineering and Physical Sciences Research Council

What is feminist international relations?

Cynthia Enloe: Critique of “high politics”

- Who makes decisions?
- What kind of assumptions and blind spots do they have?

J. Ann Tickner: Subordinate status of women’s insecurities



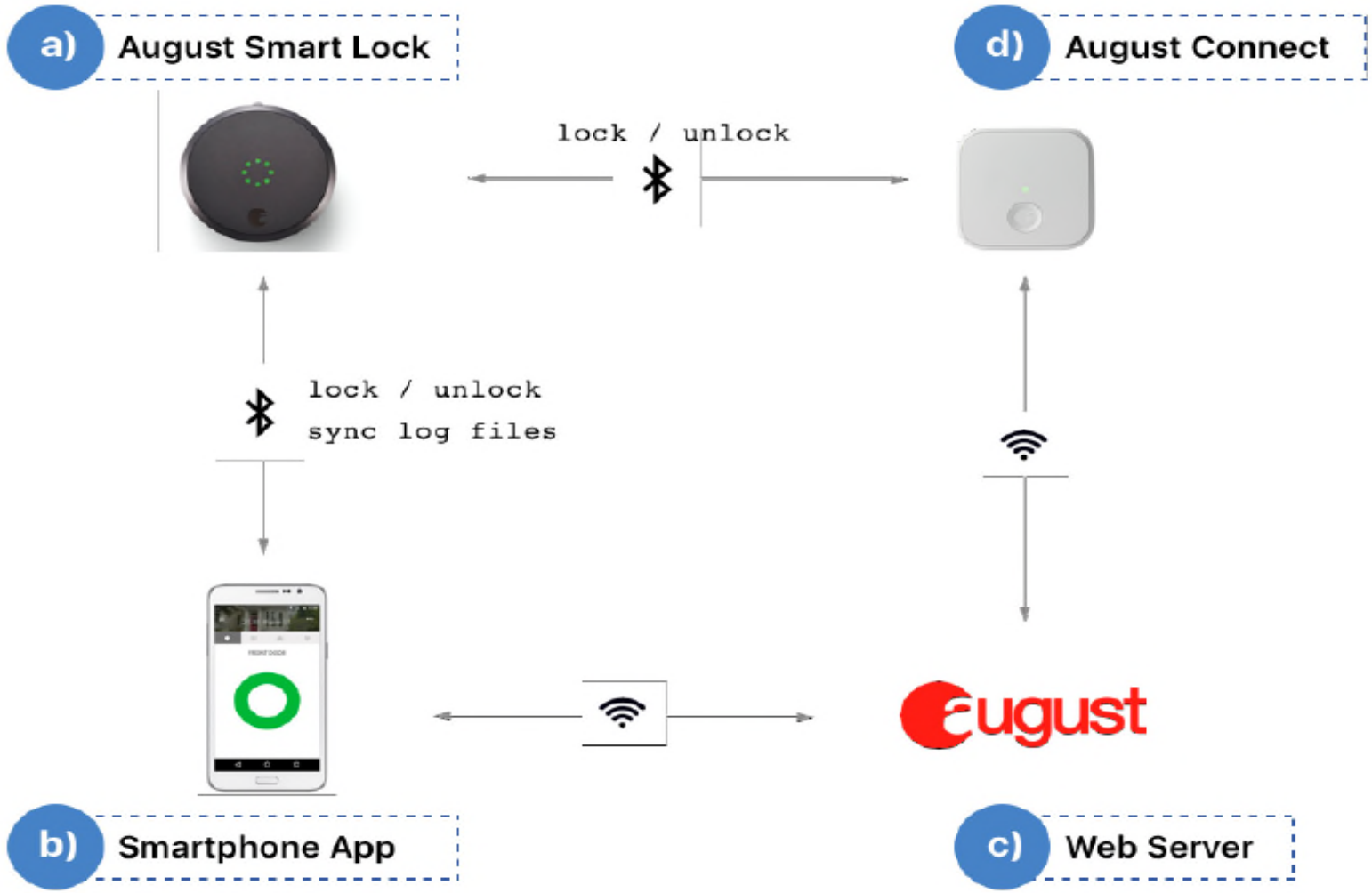

a) August Smart Lock
d) August Connect
lock / unlock
lock / unlock
sync log files
b) Smartphone App
c) Web Server

TABLE IV
AUGUST SMART LOCK OPERATIONS FOR DIFFERENT USER LEVELS

	Owner	Guest
Lock/Unlock Door	✓	✓
Lock Activity	✓	
Guest List	✓	
User Invitation	✓	
User Level Control	✓	
User Permission Control	✓	

1. Alice gives Bob OWNER-level access.
2. Alice gets out of Bluetooth range of the lock.
3. Bob maliciously puts his phone in airplane mode, preventing it from communicating with the August servers, but leaving Bluetooth enabled.
4. Alice revokes Bob's access.

“Alarming in theory but unlikely to be a problem in practice”

“OWNERS, by definition, can revoke each other's access. In fact, if Bob were truly malicious, he could have revoked Alice's access after he was granted OWNER status. For this reason, the original owner should not give OWNER status to anyone she does not trust immensely.”

Review of 40 smart home security analysis papers

Scopus database: "security analysis" AND smart AND home

Threat actors	
Remote network-based attacker	7
External adversary	6
Internal adversary	5
Burglar/thief	2
Privileged insider	2
Arsonist	1
Bad manufacturer	1
Home intruder	1
Malicious user	1
Physically-present attacker	1
Revoked attacker	1
Suppliers and drivers	1
Total	29

Threats	
Eavesdropping	14
Replay	10
DoS	9
Impersonation	8
Man-In-The-Middle	5
Offline password guessing	5
Identity breach	4
Insider attack	3
Tampering	3
Fraud	2
Privacy Breaches	2
Privileged insider	2
Smart card security breach	2
+31 other attack types	

Safe at Home: Towards a Feminist Critique of Cybersecurity

St. Anthony's International Review 2019 no. 15: Whose Security is Cybersecurity? Authority, Responsibility and Power in Cyberspace

18 Pages • Posted: 5 Aug 2019

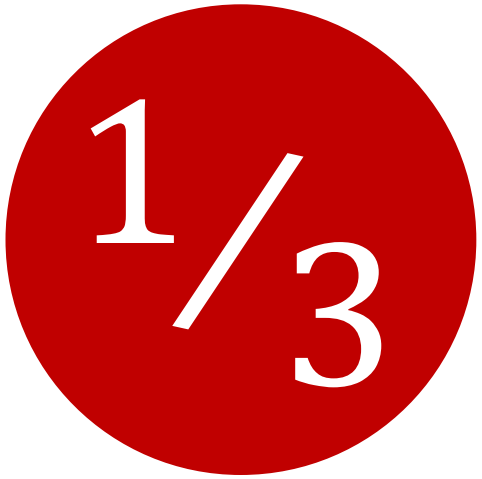
Julia Slupska
Oxford Internet Institute

Date Written: May 1, 2019

Abstract

Feminist theorists of international relations (IR) have long argued that binaries of public/private reinforce the subsidiary status given to gendered insecurities, so that these security problems are 'individualised' and taken out of the public and political domain. This article argues that the emerging field of cybersecurity risks recreating these dynamics by omitting or dismissing gendered technologically-facilitated abuse such as 'revenge porn' and intimate partner violence (IPV). I present a review of forty smart home security analysis papers to show the threat model of IPV is almost entirely absent in this literature. I conclude by outlining some suggestions for cybersecurity research and design, and reaffirming the importance of critical studies of information architecture to the modern study of IR.

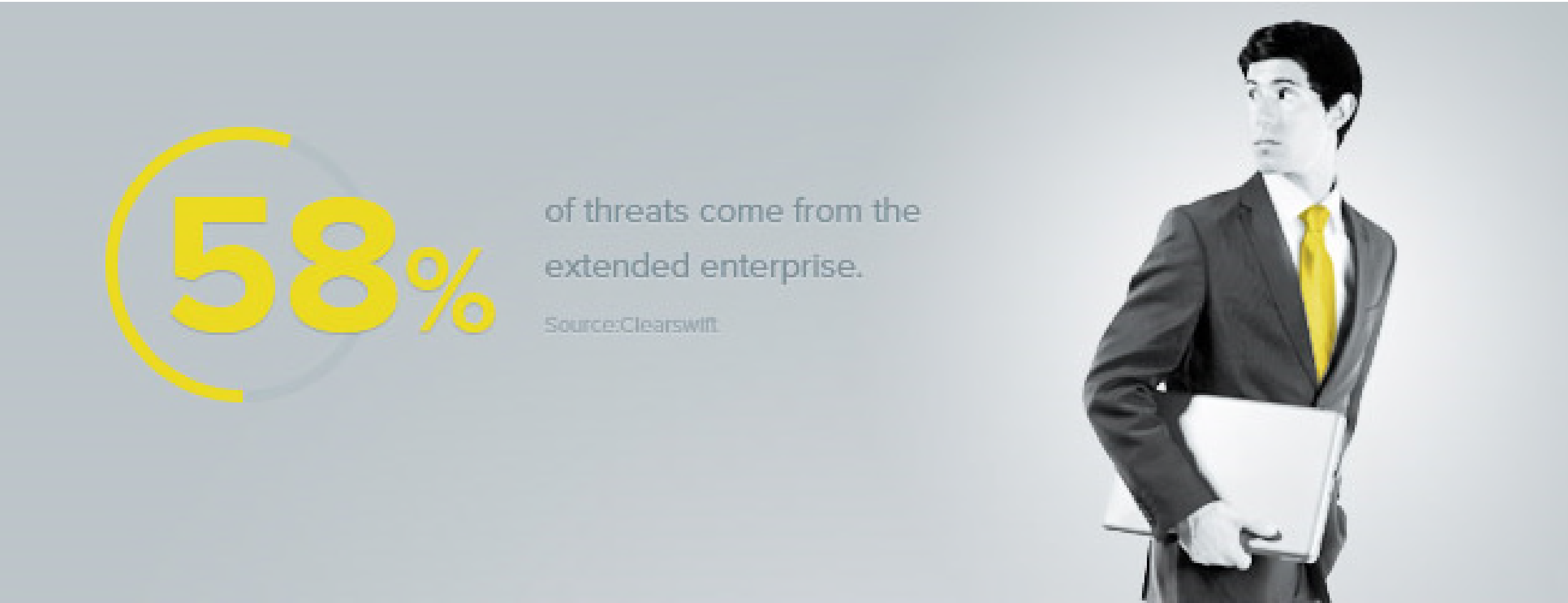
Keywords: cybersecurity, feminist theory, domestic violence, domestic abuse, intimate partner abuse, smart home, security, privacy



of all **violent crimes** recorded by the police in the UK in the year ending March 2018 were **domestic abuse** related

of IPV survivors reported **experiencing tech abuse** as part of a broader pattern of controlling behaviour

Is revenge porn a cybersecurity issue?



Home
About
People
Research
Study
Professional education
News and events
How to Change the World
Contact us
News DPL

Gender and IoT

How will IoT impact on gender-based domestic violence and abuse and what socio-technical measures will need to be implemented in order to mitigate against those risks?

Project Background

Gender and IoT is an interdisciplinary project exploring the implications of IoT on gender-based domestic violence and abuse and is funded by a Social Science Plus+award from UCL's Collaborative Social Science Domain.

UCL
DIGITAL POLICY LABORATORY

Gender and IoT leaflet

Join our newsletter

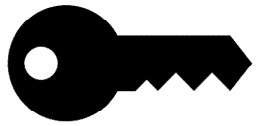
G-IoT tech abuse guide

IoT devices and smart domestic abuse

Domestic abuse consultation

Lab Blog and News

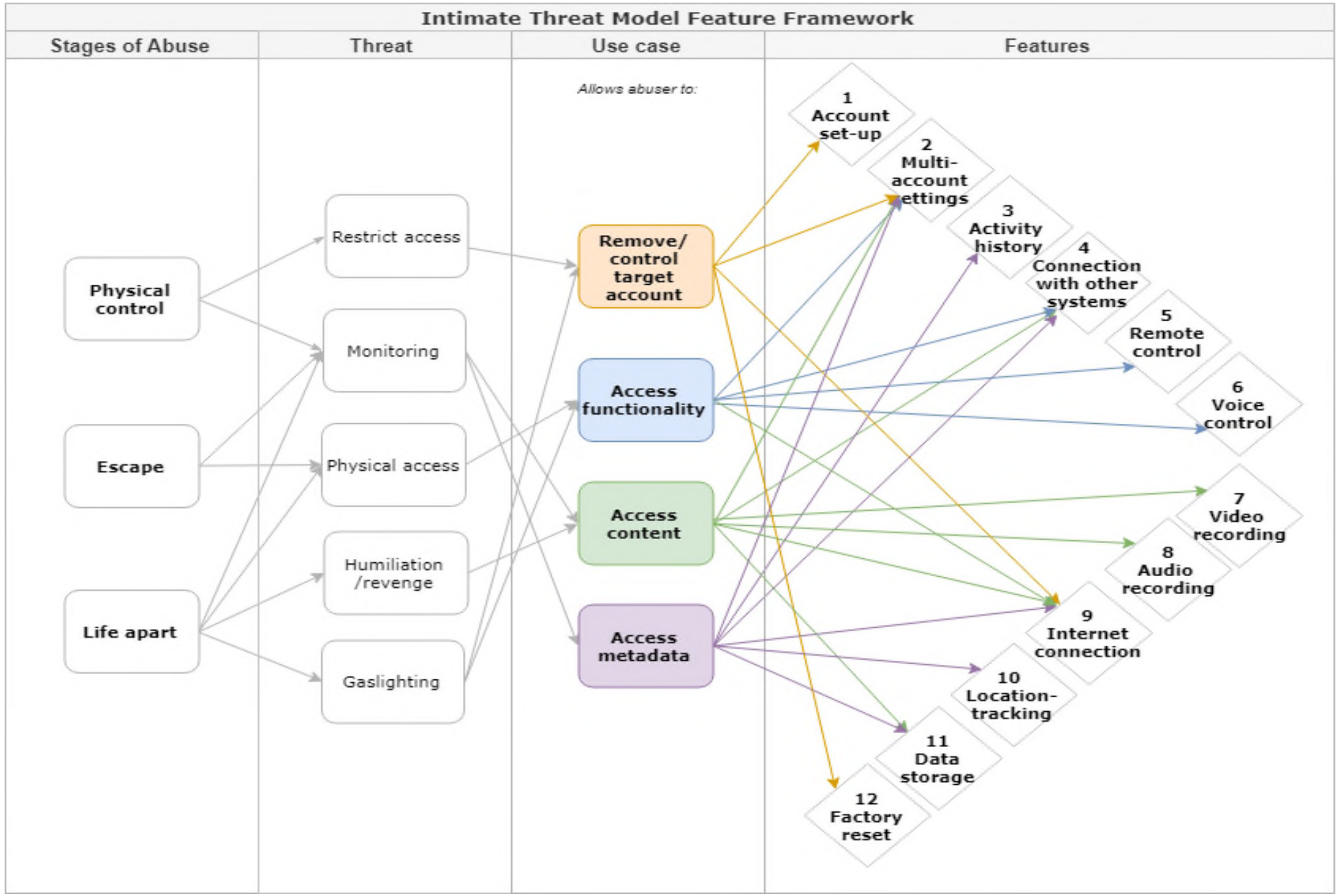
Tech abuse challenges many cybersecurity assumptions



Authentication mechanisms
passwords, security questions

Safety vs security
Features like location-tracking can be coopted

Threat model: external attackers
hackers, thieves, errant AirBnb guests


Intimate Threat Model Feature Framework
Stages of Abuse
Threat
Use case
Features
Allows abuser to:
Physical control
Escape
Life apart
Restrict access
Monitoring
Physical access
Humiliation /revenge
Gaslighting
Remove/ control target account
Access functionality
Access content
Access metadata
1 Account set-up
2 Multi-account settings
3 Activity history
4 Connection with other systems
5 Remote control
6 Voice control
7 Video recording
8 Audio recording
9 Internet connection
10 Location-tracking
11 Data storage
12 Factory reset

IFSEC International: perimeter security expo

Smart lock manufacturer interview

Threat actor	Response
Remote network-based attacker or “hacker”	Yes
Criminal/thief/home intruder	Yes
Errant guest (such as an AirBnb guest)	Yes*
Spouse or partner	“No, we’re all happily married here!”

Any questions?

Please feel free to reach out!

julia[dot]slupska[at]cybersecurity.ox.ac.uk

@julia_slupska

Limitations to IPSR

Validation: no ground truth data for which features are likely to be abused

Usability: no easy black/white answers for developers

Future plans:

- Co-design workshop with cybersecurity, IoT, and tech abuse experts
- Develop abusability testing toolkit with personas, threat model, and design principles
- Interview product managers