FULL CONTROL OF YOUR SYSTEM
COMING SOON
ETHM-A
Universal, multi-purpose Ethernet communication module
LAN
NEW
GPRS-A LTE
Universal monitoring module
GSM
IoT
SMS / MOBILE NETWORK (LTE/HSPA+/EDGE/GPRS)
SMS / CLIP / PUSH
SMS / CLIP / MOBILE NETWORK (LTE/HSPA+/EDGE/GPRS)

SECURITY THROUGH CARE: ABUSABILITY INSIGHTS FROM TECH ABUSE

JULIA SLUPSKA

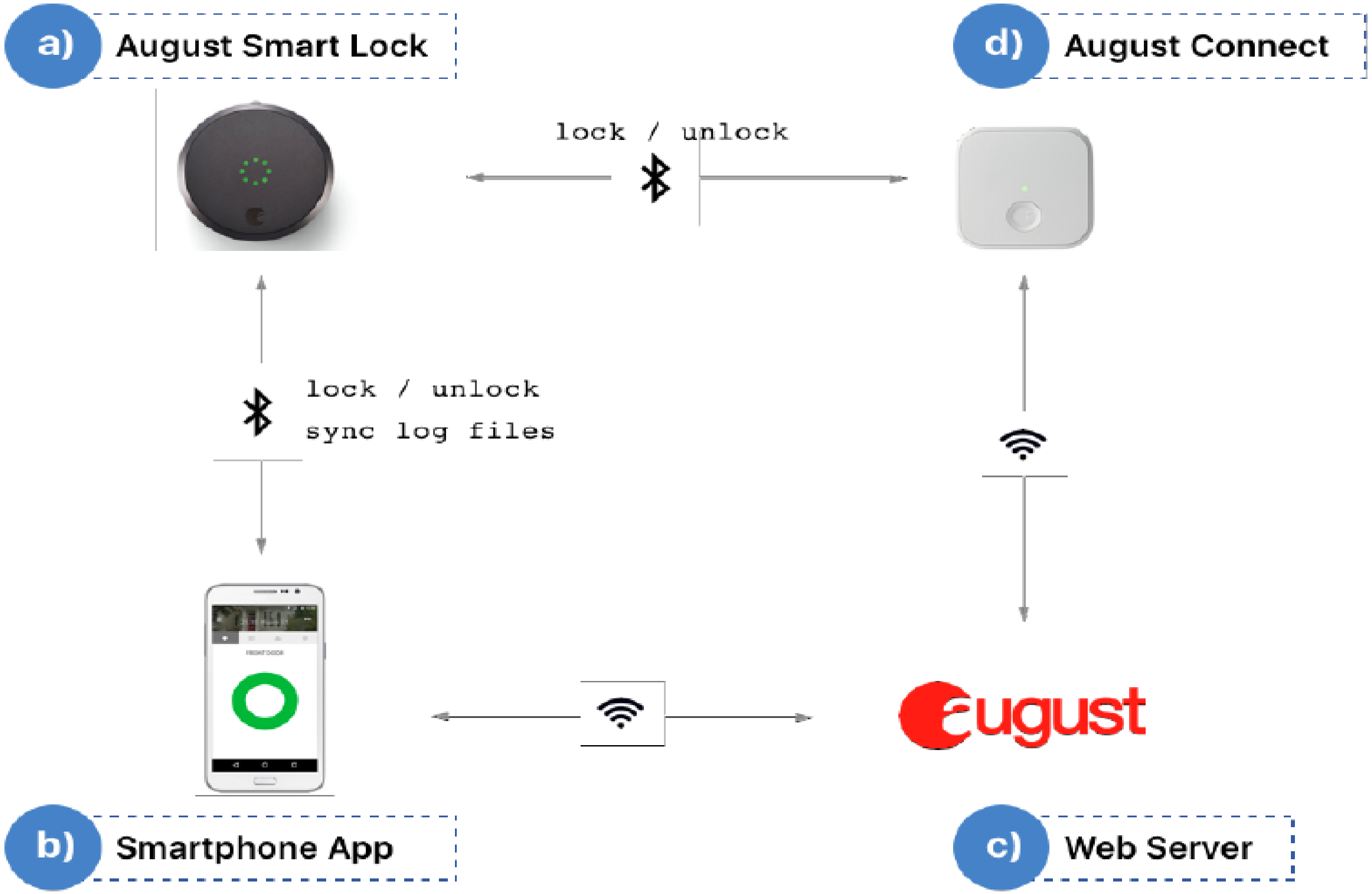
PRIVACY ENGINEERING PRACTICE AND RESPECT ‘21

OXFORD INTERNET INSTITUTE

CENTRE FOR DOCTORAL TRAINING *in* CYBER SECURITY

1. Problem: gendered surveillance & technology abuse is missed in many cybersecurity threat models
2. Solution space: safety work vs abusability
3. Case study: tech abuse advocates security & care practices

(1) PROBLEM



Fuller, Madeline Jenkins, and Katrine Tjølsen, "Security Analysis of the August Smart Lock," *Massachusetts Institute of Technology*, 2017, 1–16 .

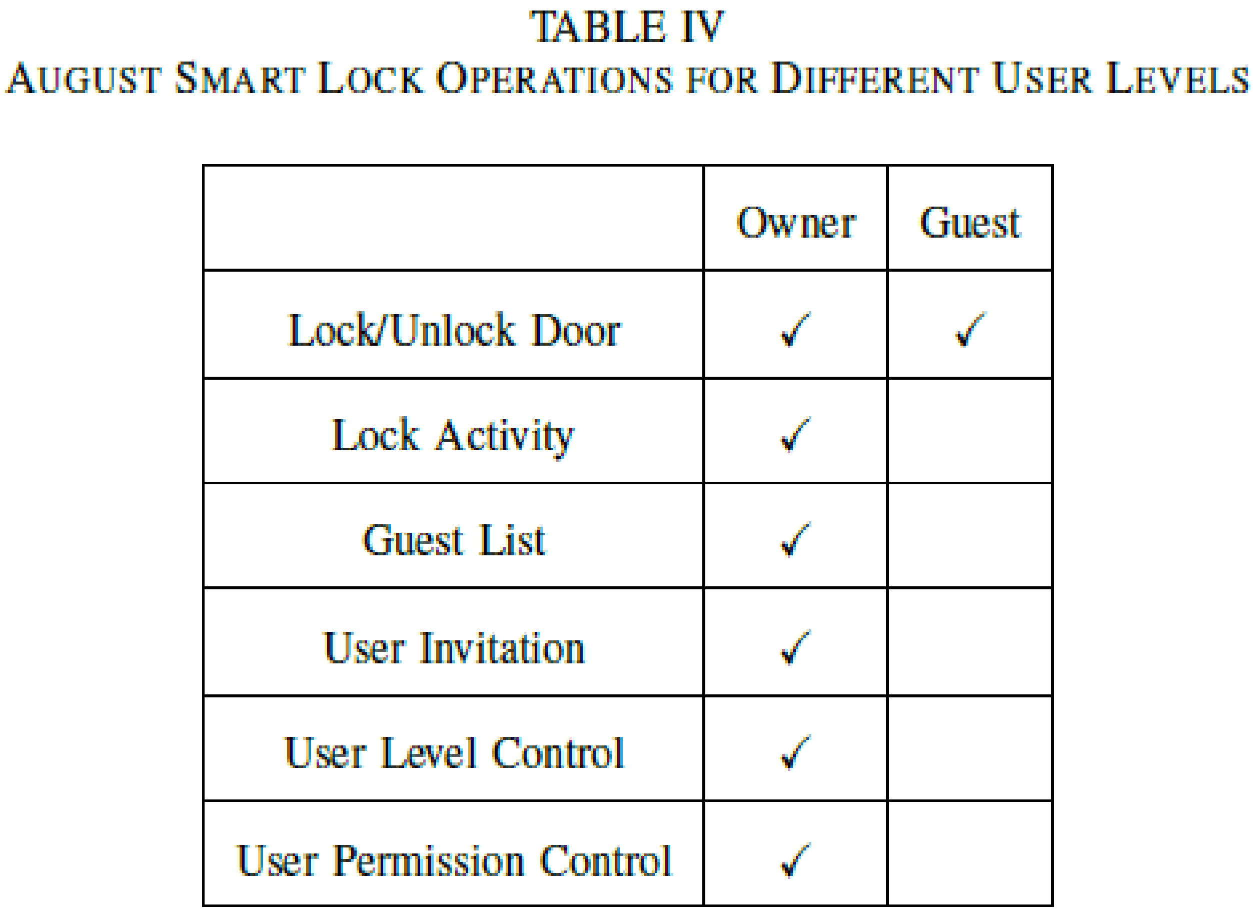


TABLE IV

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	✓	

Ye, Mengmei, Nan Jiang, Hao Yang, and Qiben Yan. “Security Analysis of Internet-of-Things: A Case Study of August Smart Lock.” In *2017 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2017*, 2017. https://doi.org/10.1109/INFCOMW.2017.8116427.

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.

Fuller, Madeline Jenkins, and Katrine Tjølsen, "Security Analysis of the August Smart Lock," *Massachusetts Institute of Technology*, 2017, 1–16 .

“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.”

Fuller, Madeline Jenkins, and Katrine Tjølsen, “Security Analysis of the August Smart Lock,” *Massachusetts Institute of Technology*, 2017, 1–16 .

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	

Slupska, Julia. “Safe at Home: Towards a Feminist Critique of Cybersecurity.” *St. Anthony's International Review*, no. Whose Security is Cybersecurity? Authority, Responsibility and Power in Cyberspace (2019). https://ssrn.com/abstract=3429851.

Is image-based abuse (‘revenge porn’) a cybersecurity issue?

↓

Gendered technology-enabled abuse is systematically omitted in security “threat models”

Slupska, Julia. “Safe at Home: Towards a Feminist Critique of Cybersecurity.” *St. Anthony’s St Antony’s International Review*, no. Whose Security is Cybersecurity? Authority, Responsibility and Power in Cyberspace (2019). https://ssrn.com/abstract=3429851.

1/3

of all violent crimes recorded by the police in the UK in the year ending **March 2018** were domestic abuse related[1]

72%

of IPV survivors reported experiencing tech abuse as part of a broader pattern of controlling behaviour[2]

[1] UK Office for National Statistics, 2018. “Domestic Abuse in England and Wales: Year Ending March 2018.”
[2] www.refuge.org.uk

Hi!
I'd like a wake up call.
InfoSec's obsession with nation state hacking is at the expense of more common intrusions by abusers

Credit: [@labacdotdev]()

(2) SOLUTION SPACE

EXISTING RESEARCH & ACTIVISM

1. Cornell: IPV Tech Research Team & Clinic to End Tech Abuse
2. UCL's Gender & IoT Lab: Tanczer et al
3. Levy & Schneier: Privacy Threats in Intimate Relationships
4. Researchers from criminology/violence studies: Harris, Woodlock & Dragiewicz
5. Eva Galperin & the Coalition Against Stalkerware

PRIVACY & SECURITY ADVICE FOR SURVIVORS

Digital self-defense guides, while important, risk creating "safety work" for already over-burdened survivors

Bridget A. Harris and Delanie Woodlock, "Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies," *British Journal of Criminology*, 2019, https://doi.org/10.1093/bjc/azy052.

ANDY GREENBERG SECURITY 01.28.2019 04:40 PM

Security Isn't Enough. Silicon Valley Needs 'Abusability' Testing

Former FTC chief technologist Ashkan Soltani argues it's time for companies to formalize and test not just a product's security, but how it can be abused.

Coercive Control Resistant Design

The key to safer technology

Adopt a mindful approach to design, ensuring your technology is resistant to being used as a tactic of domestic abuse

Authors
Lesley Nuttall
Jessica Evans
Miriam Franklin
Sarah Burne James

IPV THREAT MODEL

Adapting Shostack's threat modelling questions:

1. What are you building? *Map features – like location-tracking – which can be co-opted for abuse*
2. What can go wrong? *Connect these features to common vectors of compromise and abuse*
3. What can we do about it? *How can design mitigate potential abuses*
4. Did you do a decent job of analysis? *Monitoring products for abuse to validate threat models*

Slupska, Julia, and Leonie Tanczer. "Intimate Partner Violence (IPV) Threat Modeling: Tech Abuse as Cybersecurity Challenge in the Internet of Things (IoT)." In *Technology-Facilitated Violence and Abuse – International Perspectives and Experiences*. Emerald Publishing, (forthcoming).

Shostack, Adam. (2014). *Threat Modeling: Designing for Security*. Wiley.

(3) CASE STUDY

TECH ABUSE ADVOCATES

CHAYN

Refuge

For women and children.
Against domestic violence.

ATINA

UDRUŽENJE GRAĐANA ZA BORBU PROTIV TRGOVINE
LJUDIMA I SVIH OBLIKA NASILJA NAD ŽENAMA

#notyourporn

GL!TCH

Fix the glitch to end online abuse

ENDTAB

NNEDV

NATIONAL NETWORK
TO END DOMESTIC
VIOLENCE

WESNET

The Women's Services Network

26 QUALITATIVE INTERVIEWS WITH TECH ABUSE ADVOCATES

- Domestic violence & human trafficking shelters including tech support "clinics"
- Sexual violence counselling & advocacy
- Digital privacy advocates
- Hacking collectives

Who does cybersecurity? *Networks of care outside of corporate or state defense*

RECOMMENDATIONS FOR TECH COMPANIES, SOFTWARE ENGINEERS, & SECURITY COMMUNITY

- Digital security beyond technical security: networks of care
- Learn about specific problems faced by survivors of technology abuse
- Trauma-informed design:
  - Difficulties in accessing customer support
  - Support efforts to provide evidence
  - Consent practices: regular reminders re location-tracking
  - Risks of traumatization with "creepy" design
- Partnerships & compensation

ANY QUESTIONS?

JULIA.SLUPSKA@CYBERSECURITY.OX.AC.UK

@JAYSLUPS