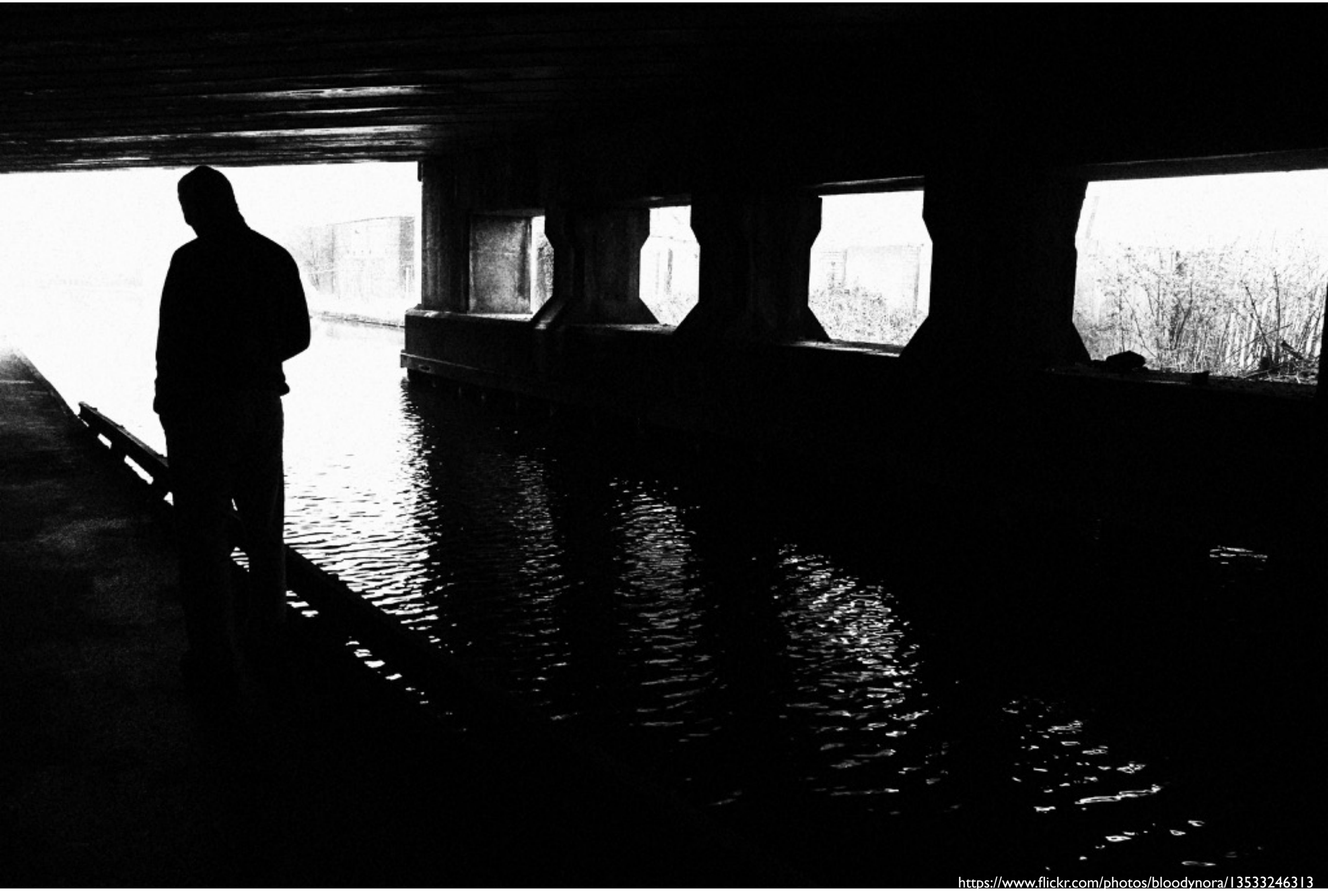
Usability & Security by Design

A Case Study in R&D

Shamal Faily[1], John Lyle[2], Ivan Fléchais[2], Andy Simpson[2]
Bournemouth University[1], University of Oxford[2]



https://www.flickr.com/photos/bloodynora/13533246313

If we knew what we were doing, it wouldn't be called Research.

–A. Einstein

https://www.flickr.com/photos/astronomyblog/6876694340

Open-source project to get gadgets talking via the net

By Zoe Kleinman
Technology reporter, BBC News

More than 5,400 developers have downloaded a new open-source operating system designed to enable digital devices to communicate with each other.

They are now looking at ways in which Webinos could be used to connect a range of devices such as mobile phones, car stereos, heart monitors and TVs.

Webinos-powered application Zap and Shake can share pictures or videos from a phone to a TV

Webinos is a 15m euro ($18.4m; £11.8m) project supported by more than 30 organisations, including the EU.

BMW, W3C, Sony, Samsung and Telefonica are among its commercial partners.

While other operating systems that use the internet to connect devices to each other already exist, most are pre-installed and cannot be customised by individual users.

Free for all

Technical co-ordinator Nick Allott told the BBC Webinos was designed to provide an alternative to proprietary systems developed by Apple,

Related Stories

Why firms must adopt the open source way

'Open source artists' embrace web tools

Context of use description concepts

goals

intended outcome

user

task

equipment

environment

Context of use

webinos context of use concepts

Persona Characteristic

Characteristic

Attacker Persona

Environment

Activity Scenarios

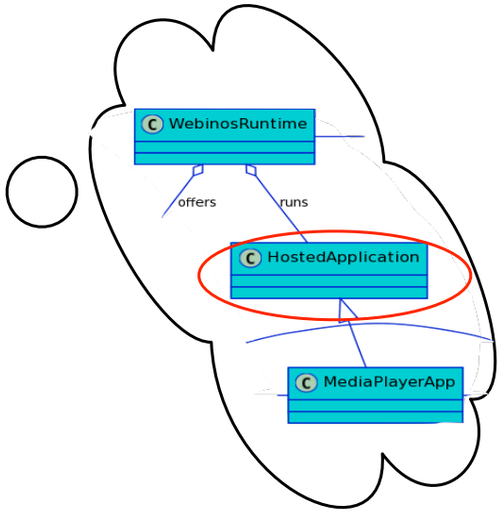
Persona

Asset 1..* **Asset**

*

Attack Tree

Context of use description



Ethan

Access Application

OR

Steal from the WEB

Steal from storage on the device

Steal from the WEB environment on the device

Steal from the OS environment on the device

Leech on service backend

Client authentication and encryption, e.g. DRM scheme integrated in the WEB runtime

WEB application isolation within the WEB environment

OS protection of the WEB environment

Service API access control

Extract service credential from the application

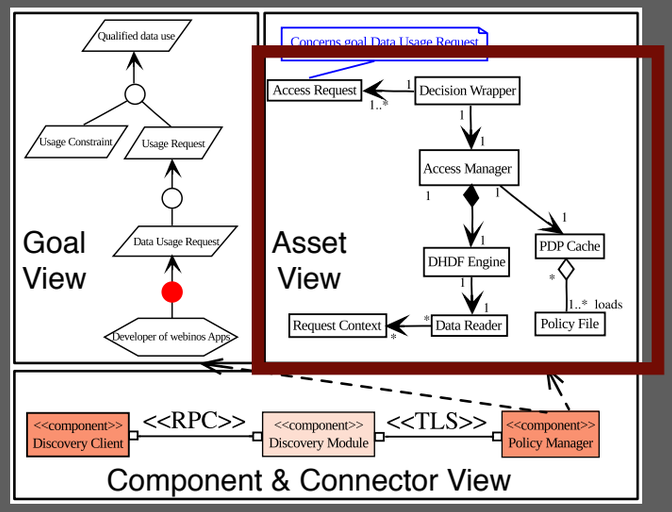
OR

Rooting style attacks

DRM attacks

Modify the WEB runtime

Trusted boot



Architectural pattern	DER_m	DER_c	DER_i
Context Policy Management	1.2	6.1	28.6
NFC	1.4	4	39.5
PZH Authentication	9.6	6.1	29.7
PZP Enrolment	11.2	5	16.6
TV Service Discovery	3.7	4.2	29
Widget Processing	1.1	1	22.9
Widget Rendering	2.8	2	28.6

Architectural Modelling & Attack Surface Measurement

Attacker	Motives	Capabilities (Value)
Ethan	System resource theft	Methods (Med), Software (Med), Techology

Attack	Origin
Locate and Exploit Test APIs	CAPEC-121

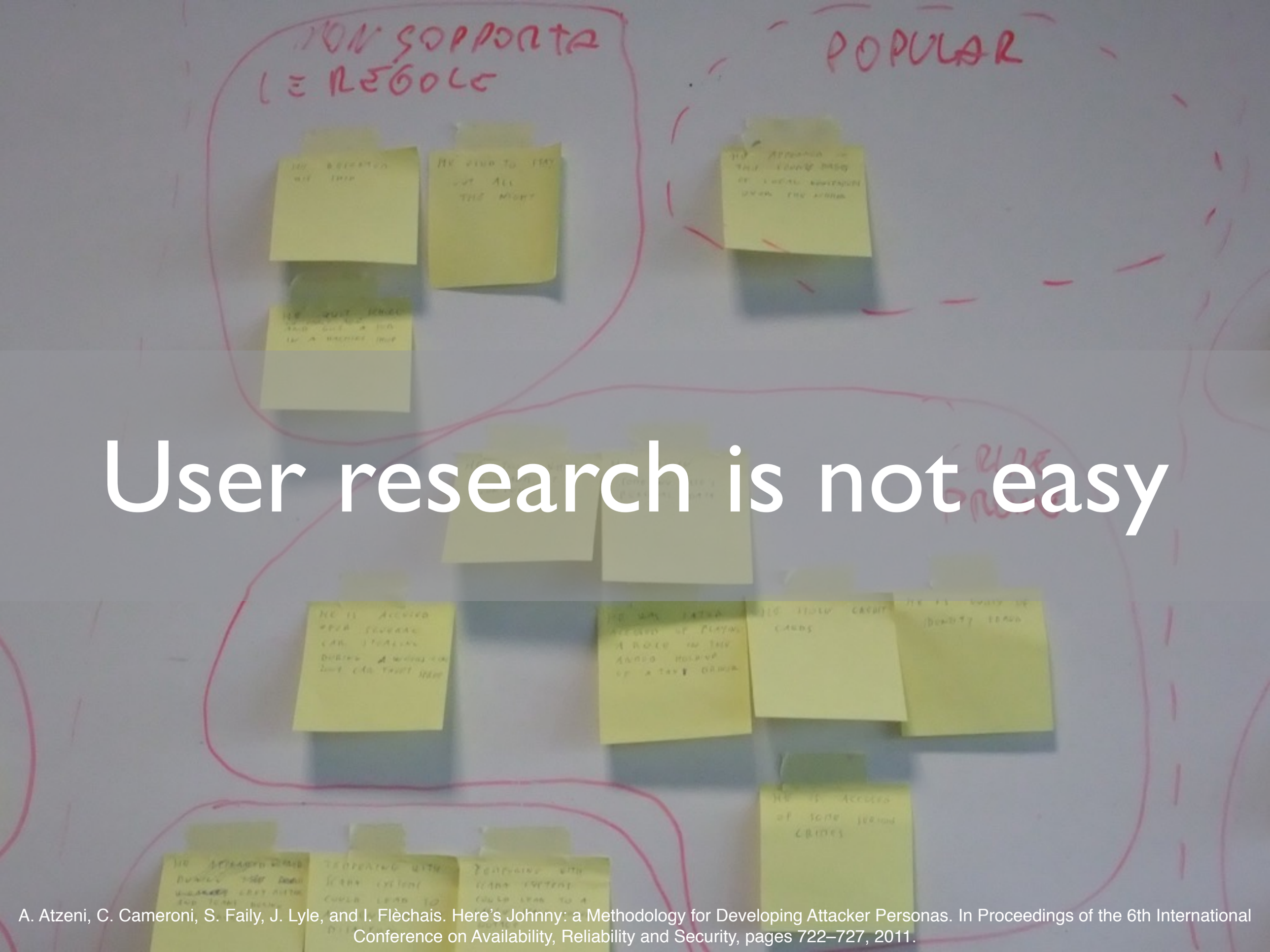
Target	Exploit
Application Data	Access Request

Obstacle	Requirement	Affected Componen	Satisfied (Y/N)	Rationale
Ambiguous request specification	Canonical request specification	Policy Manager	Y	Each request is enforced separately by definition. Impossible to grant access to
Test API enabled	Test API disabled	Widget Manager	N	There are no supported means for distinguishing test APIs from those which are

Architectural Risk Analysis

S. Faily, J. Lyle, C. Namiluko, A. Atzeni, and C. Cameroni. Model-driven architectural risk analysis using architectural and contextualised attack patterns. In Proceedings of the Workshop on Model-Driven Security, pages 3:1–3:6. ACM, 2012.

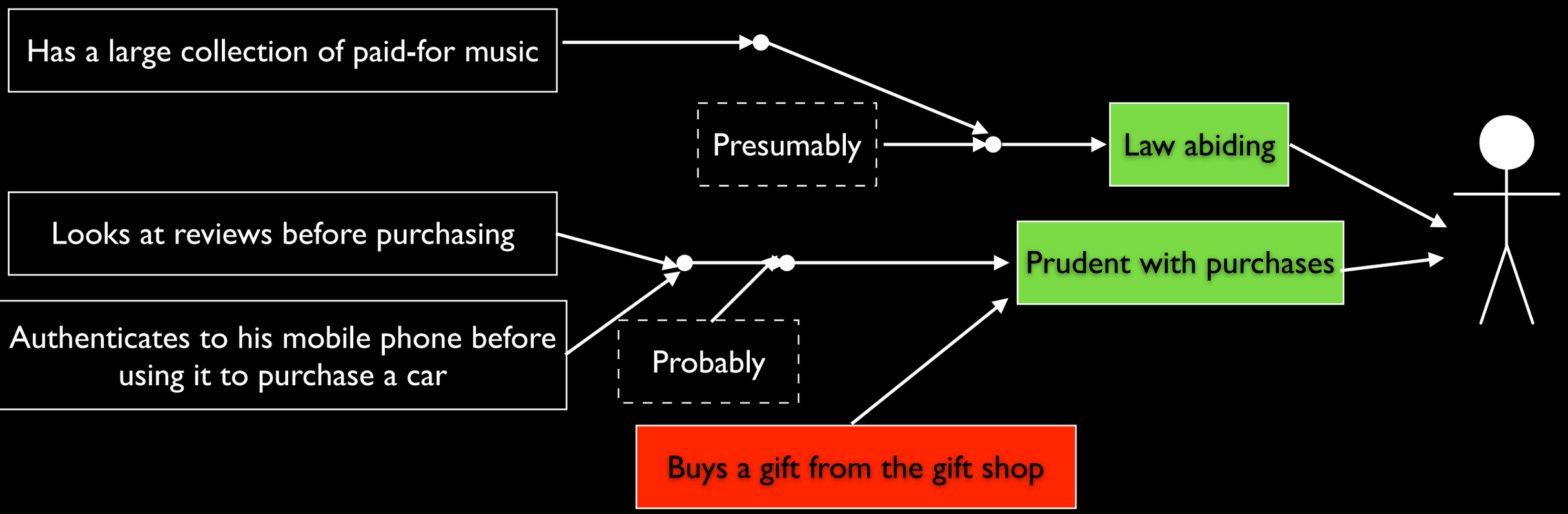
User research is not easy



A. Atzeni, C. Cameroni, S. Faily, J. Lyle, and I. Flèchais. Here's Johnny: a Methodology for Developing Attacker Personas. In Proceedings of the 6th International Conference on Availability, Reliability and Security, pages 722–727, 2011.

Usability is not a priority

Technique misappropriation is easy



"Peter is generally law-abiding and rule following. He is prudent with his purchases, and has an expectation of some security around financial transactions."

Sustaining adoption requires creativity

S. Faily, J. Lyle, A. Paul, A. Atzeni, D. Blomme, H. Desruelle, and K. Bangalore. Requirements sensemaking using concept maps. In Proceedings of the 4th International Conference on Human-Centered Software Engineering, pages 217–232. Springer, 2012.

Lessons Learned

- Learn to work with imperfect data and expertise
- Security and usability design: better together
- Make time for designing security
- Designing for security is not just a process

Thank you for listening!

- Any questions?