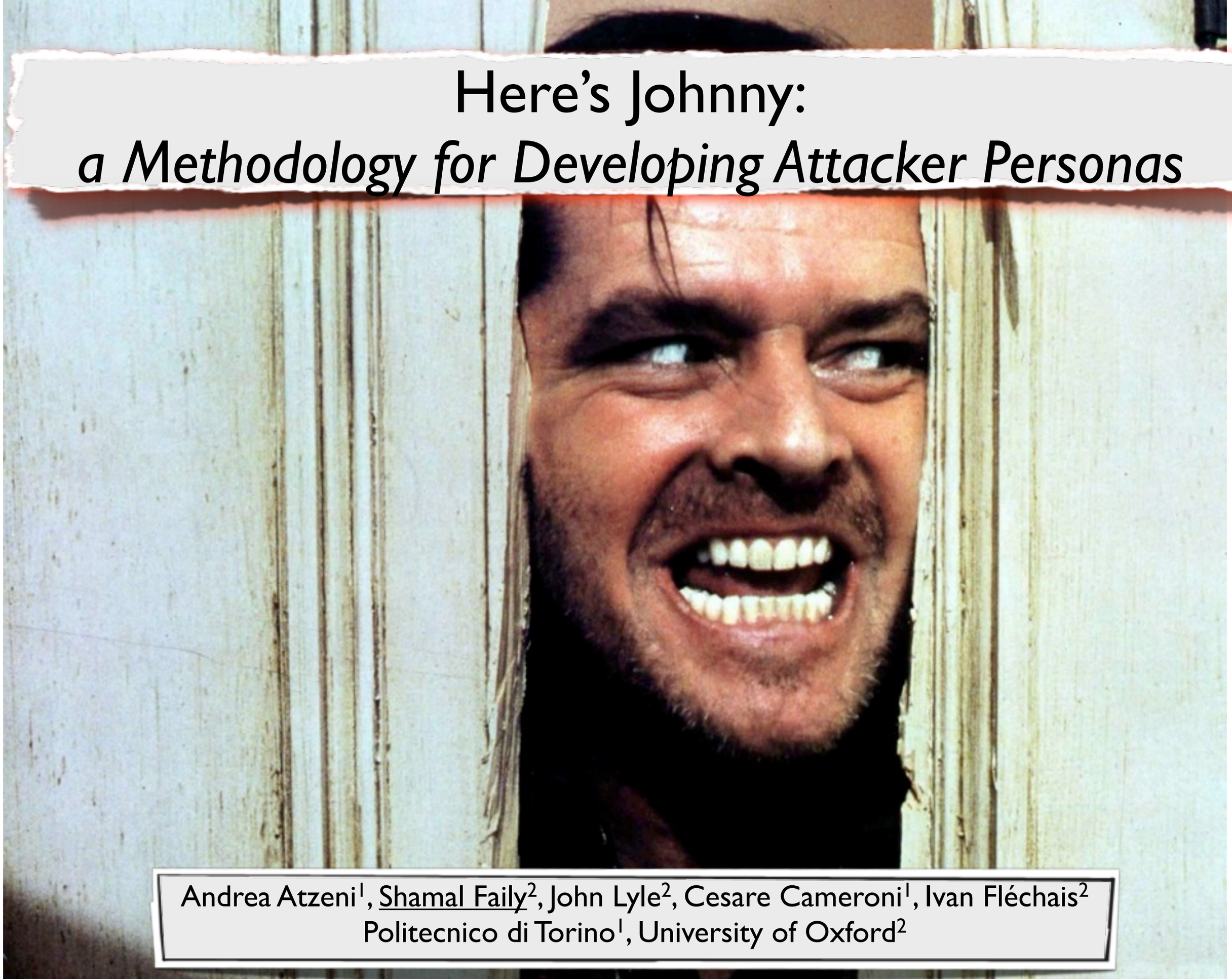
Here's Johnny:
a Methodology for Developing Attacker Personas



Andrea Atzeni[1], Shamal Faily[2], John Lyle[2], Cesare Cameroni[1], Ivan Fléchais[2]
Politecnico di Torino[1], University of Oxford[2]

http://www.flickr.com/photos/22611996@N02/4140053212/

Personas


Alice


Georg


Justin


Clara


Gloria


Carlos


Helen


Richard


Jimmy


Jessica


Anna


Peter

https://www.owasp.org/index.php/Category:Threat_Agent

OWASP

WP2.8 PCS Scopus BBC News

OWASP
The Open Web Application Security Project

Go Search

Category Discussion View source History

Navigation
- Home
- News
- OWASP Projects
- Downloads
- Local Chapters
- Global Committees
- AppSec Job Board
- AppSec Conferences
- Presentations
- Video
- Press
- Get OWASP Books
- Get OWASP Gear
- Mailing Lists
- About OWASP
- Membership

Reference
- How To...
- Principles
- Threat Agents
- Attacks
- Vulnerabilities
- Controls
- Activities
- Technologies
- Glossary
- Code Snippets

Category:Threat Agent

This category is for tagging articles related to common application security threat agents.

What is a Threat Agent?

The term *Threat Agent* is used to indicate an individual or group that can manifest a threat. It is fundamental to identify who would want to exploit the assets of a company, and how they might use them against the company.

Threat Agent = Capabilities + Intentions + Past Activities

These individuals and groups can be classified as follows:

- Non-Target Specific: Non-Target Specific Threat Agents are computer viruses, worms, trojans and logic bombs.
- Employees: Staff, contractors, operational/maintenance personnel, or security guards who are annoyed with the company.
- Organized Crime and Criminals: Criminals target information that is of value to them, such as bank accounts, credit cards or intellectual property that can be converted into money. Criminals will often make use of insiders to help them.
- Corporations: Corporations are engaged in offensive information warfare or competitive intelligence. Partners and competitors come under this category.
- Human, Unintentional: Accidents, carelessness.
- Human, Intentional: Insider, outsider.
- Natural: Flood, fire, lightning, meteor, earthquakes.

Threat Risk Modeling is an activity to understand the security in an application. The specific vulnerability, related countermeasures, and impact are not required to discuss a threat, because the threat exists even if the target is well protected against it. For example, there is a threat that an attacker could launch a denial of service attack against your application even if you have

http://capec.mitre.org/

CAPEC

WP2.8 PCS Scopus BBC News

CAPEC Common Attack Pattern Enumeration and Classification
A Community Knowledge Resource for Building Secure Software

Search by ID: Go

CAPEC List
- Full CAPEC Dictionary
- Methods of Attack View
- Reports

About CAPEC
- Documents
- Resources

Community
- Related Activities
- Collaboration List
- T-Shirt

News & Events
- Calendar
- Free Newsletter

Contact Us
- Search the Site

Building software with an adequate level of security assurance for its mission becomes more and more challenging every day as the size, complexity, and tempo of software creation increases and the number and the skill level of attackers continues to grow. These factors each exacerbate the issue that, to build secure software, builders must ensure that they have protected every relevant potential vulnerability; yet, to attack software, attackers often have to find and exploit only a single exposed vulnerability. To identify and mitigate relevant vulnerabilities in software, the development community needs more than just good software engineering and analytical practices, a solid grasp of software security features, and a powerful set of tools. All of these things are necessary but not sufficient. To be effective, the community needs to think outside of the box and to have a firm grasp of the attacker's perspective and the approaches used to exploit software.

Attack patterns are a powerful mechanism to capture and communicate the attacker's perspective. They are descriptions of common methods for exploiting software. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples.

To assist in enhancing security throughout the software development lifecycle, and to support the needs of developers, testers and educators, the **Common Attack Pattern Enumeration and Classification (CAPEC)** is sponsored by the Department of Homeland Security as part of the Software Assurance strategic initiative of the National Cyber Security Division. The objective of this effort is to provide a publicly available catalog of attack patterns along with a comprehensive schema and classification taxonomy. This site now contains the initial set of content and will continue to evolve with public participation and contributions to form a standard mechanism for

http://cyb3rcrim3.blogspot.com/

CYB3RCRIM3

WP2.8 PCS Scopus BBC News

Share Report Abuse Next Blog» Create Blog Sign

CYB3RCRIM3
Observations on technology, law and lawlessness.

Friday, August 19, 2011

Grades, Keylogging and Fraud

As Wikipedia notes, "[i]n criminal law, . . . fraud is an intentional deception made for personal gain". This post deals with a case in which three undergraduate students at Florida A&M University [FAMU] were charged with and ultimately convicted of fraud and identity theft in violation of federal law. *U.S. v. Barrington,* __ F.3d __, 2011 WL 3503206 (11th Cir. 2011).

Barrington, Christopher Jacquette and Lawrence Secrease were charged with conspiracy to commit wire fraud in violation of 18 U.S. Code §§ 371 & 1349, use of a computer to further a scheme to defraud in violation of 18 U.S. Code § 1030(a)(4) and three counts of aggravated identity theft in violation of 18 U.S. Code § 1028A. *U.S. v. Barrington, supra.* According to

About Me

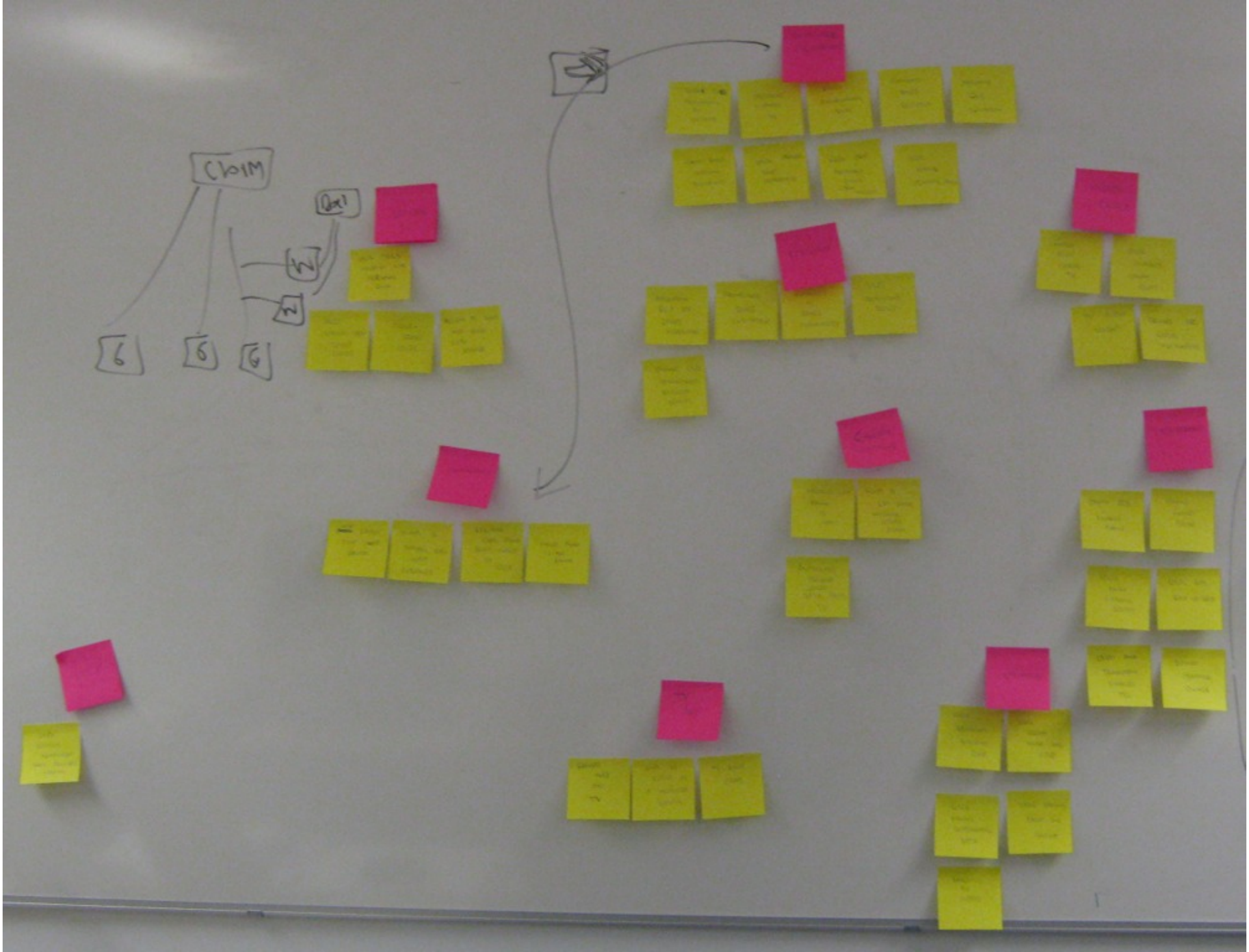
SUSAN BRENNER

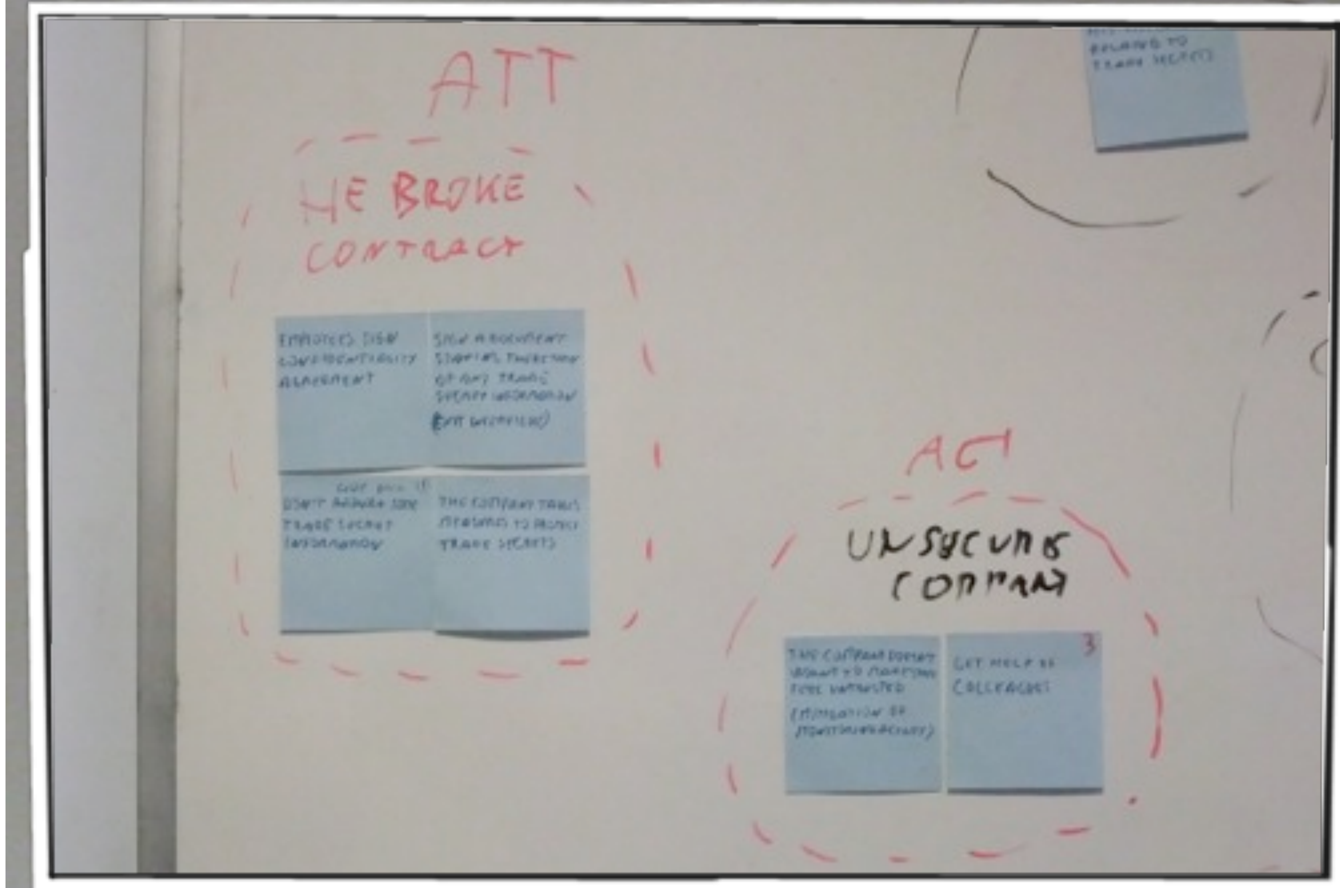
Susan Brenner is a law professor who speaks, writes and consults on cybercrime and cyberconflict.

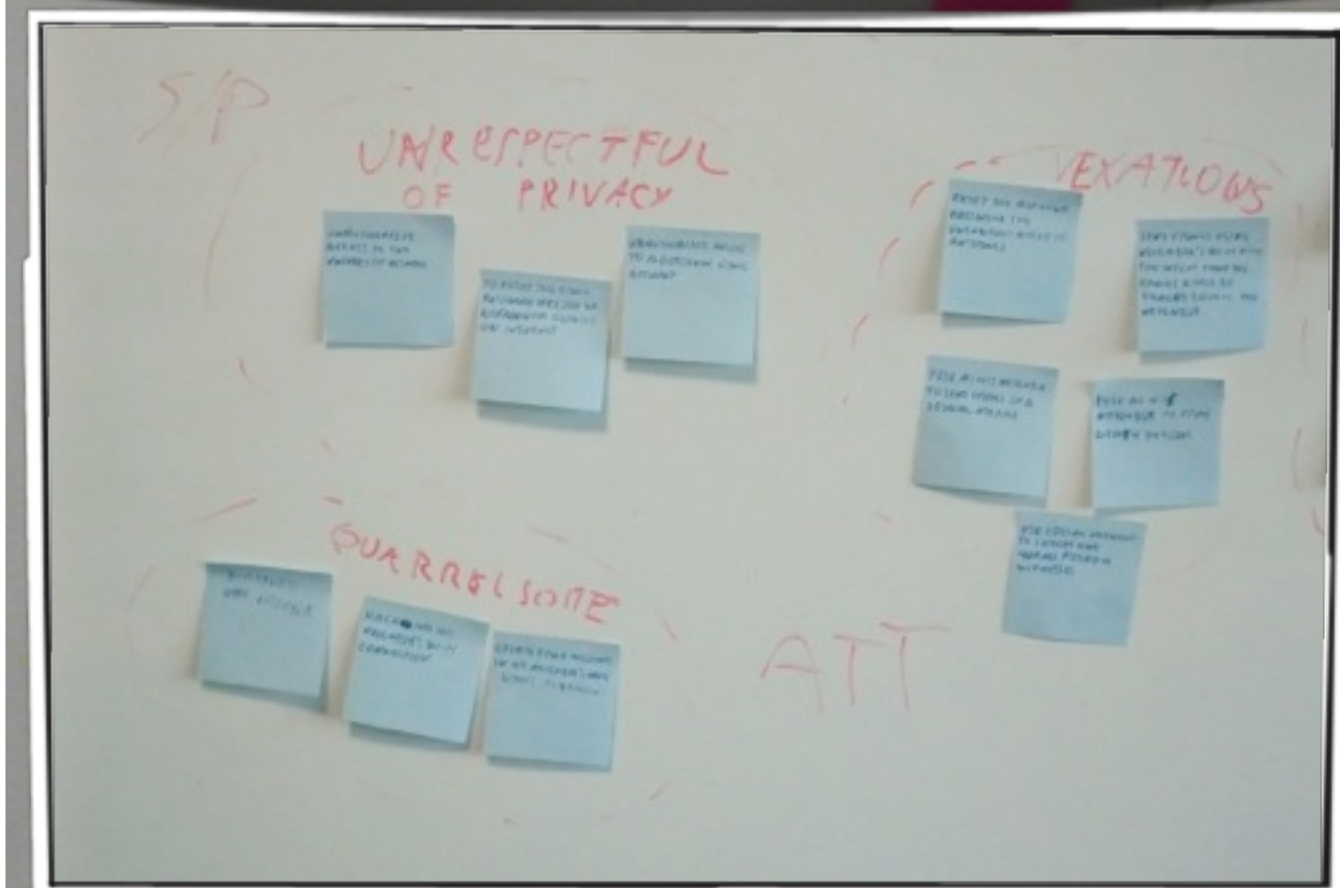
View my complete profile

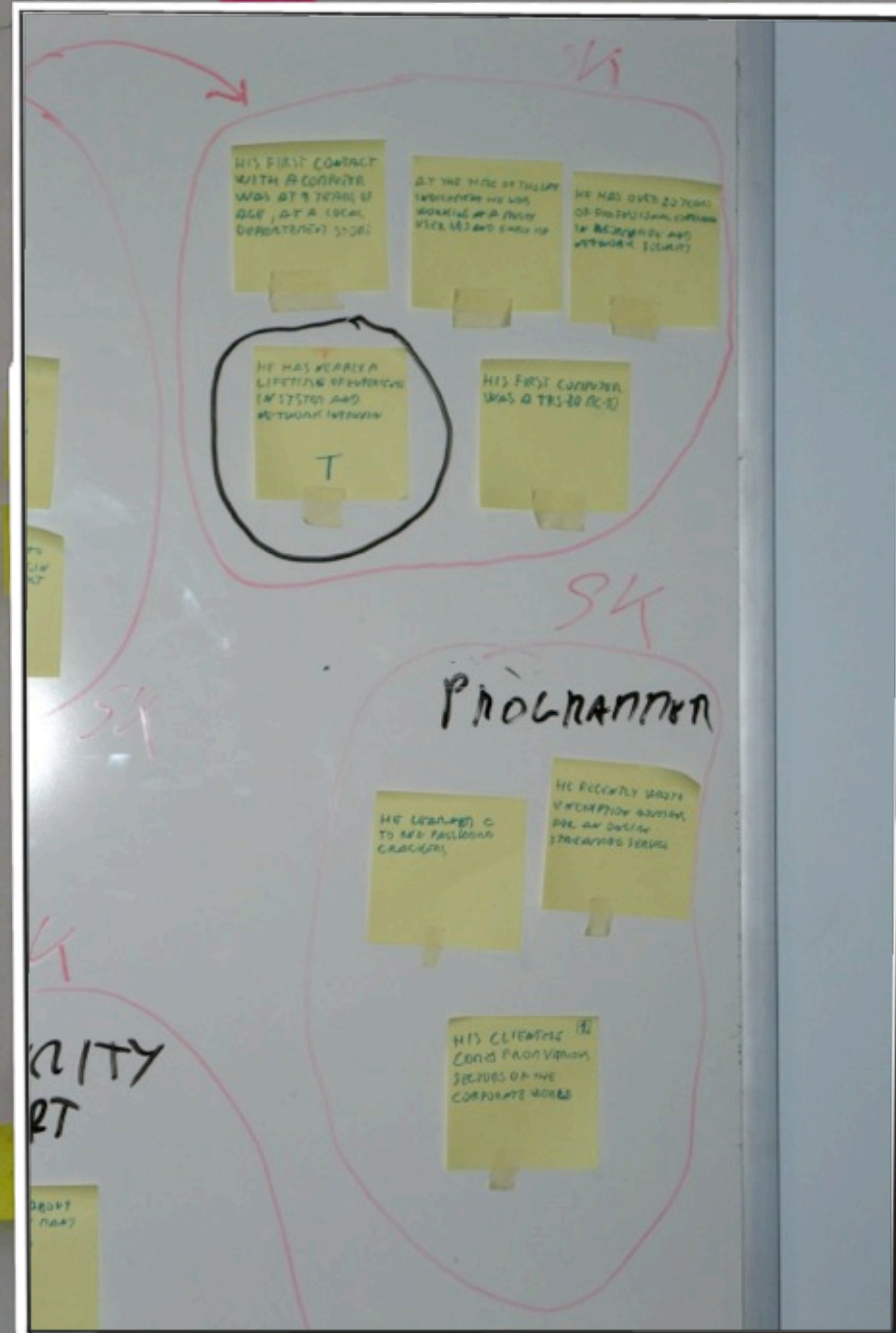
Followers

Join this site
with Google Friend Connect


CLAIM


ATT
HE BROKE CONTRACT
ACT
UNSECURE COMPANY


S/P
UNRESPECTFUL OF PRIVACY
VEXATIOUS
QUARRELSOME
ATT

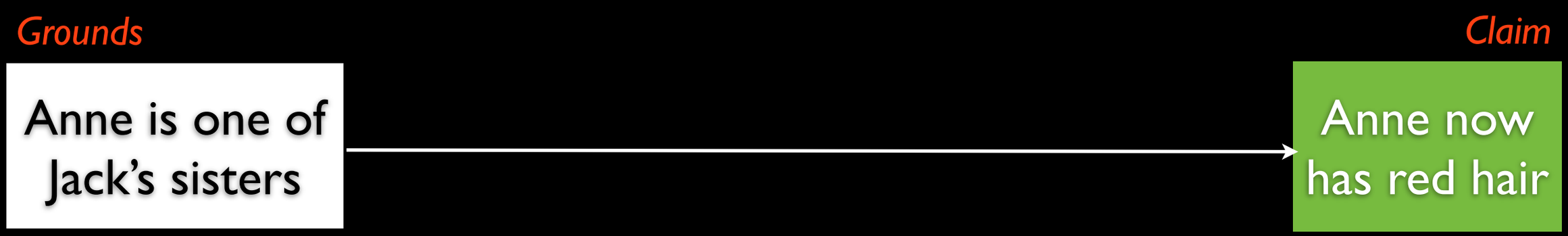

SK
HIS FIRST CONTACT WITH A COMPUTER WAS AT 9 YEARS OF AGE, AT A LOCAL DEPARTMENT STORE
SK
PROGRAMMER
HIS CLIENTS COME FROM VARIOUS SECTORS OF THE CORPORATE WORLD

Toulmin Model

Anne now has red hair

Toulmin, S. (2003). The uses of argument. Cambridge University Press, updated edition.

Toulmin Model

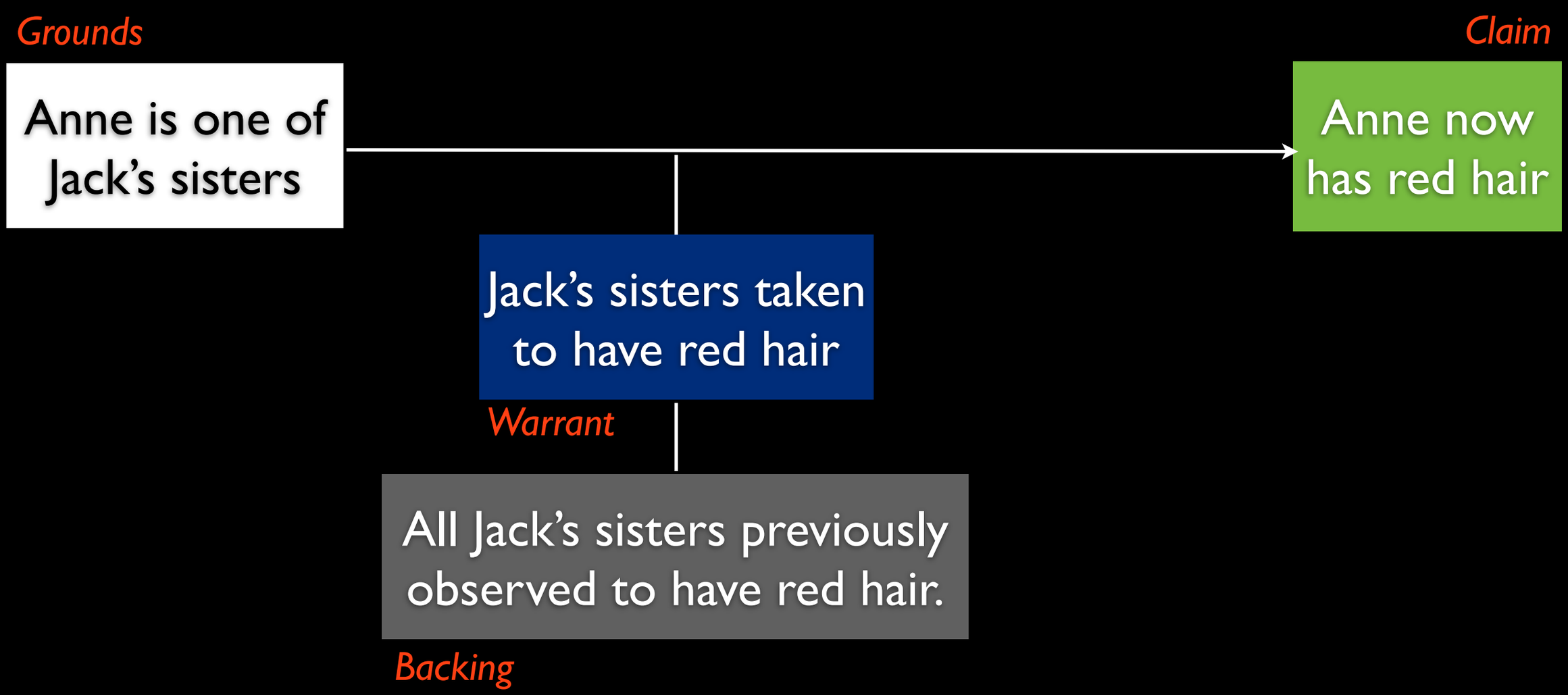


Toulmin, S. (2003). The uses of argument. Cambridge University Press, updated edition.

Toulmin Model

Toulmin, S. (2003). The uses of argument. Cambridge University Press, updated edition.

Toulmin Model

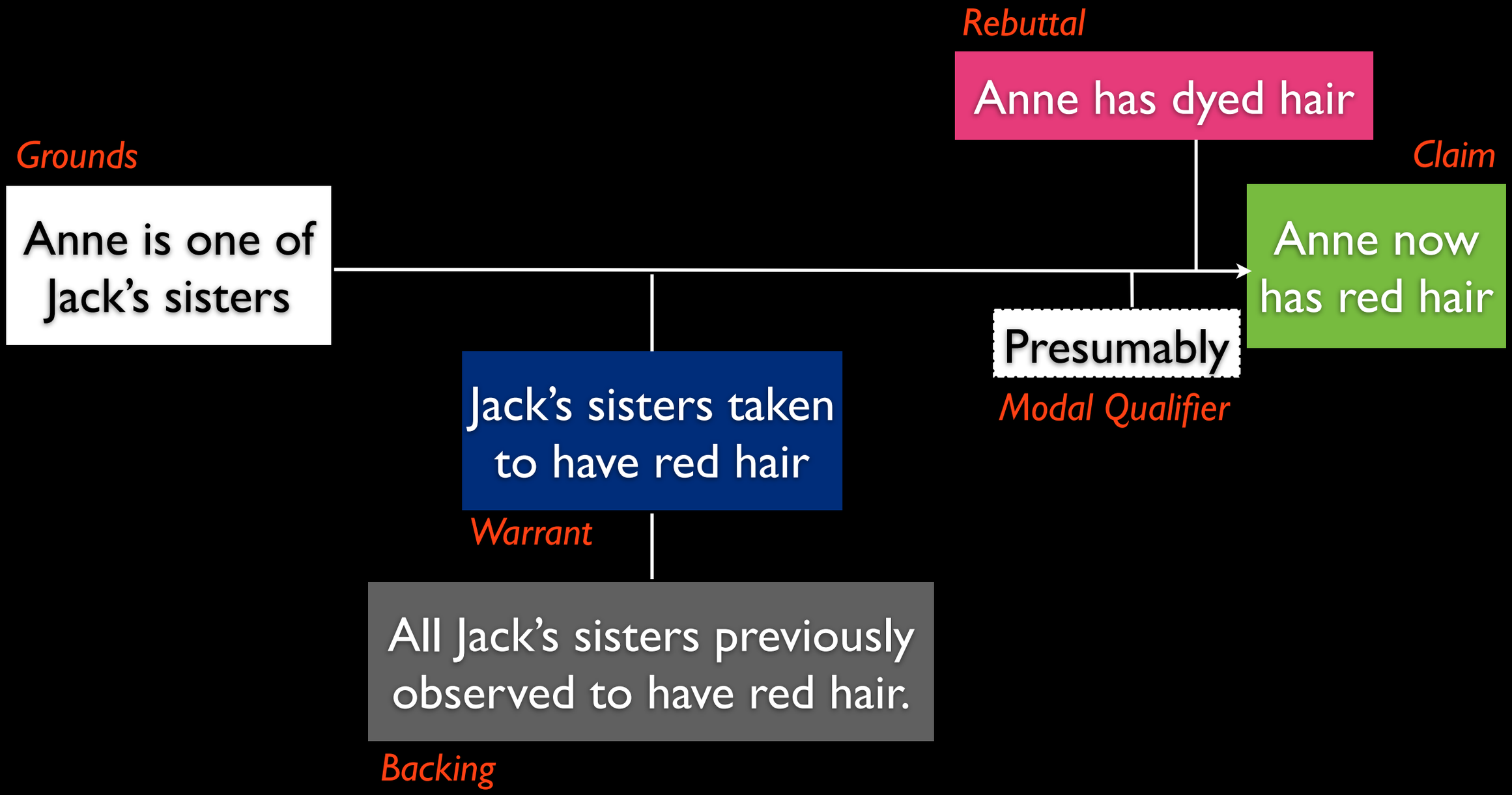


Toulmin, S. (2003). The uses of argument. Cambridge University Press, updated edition.

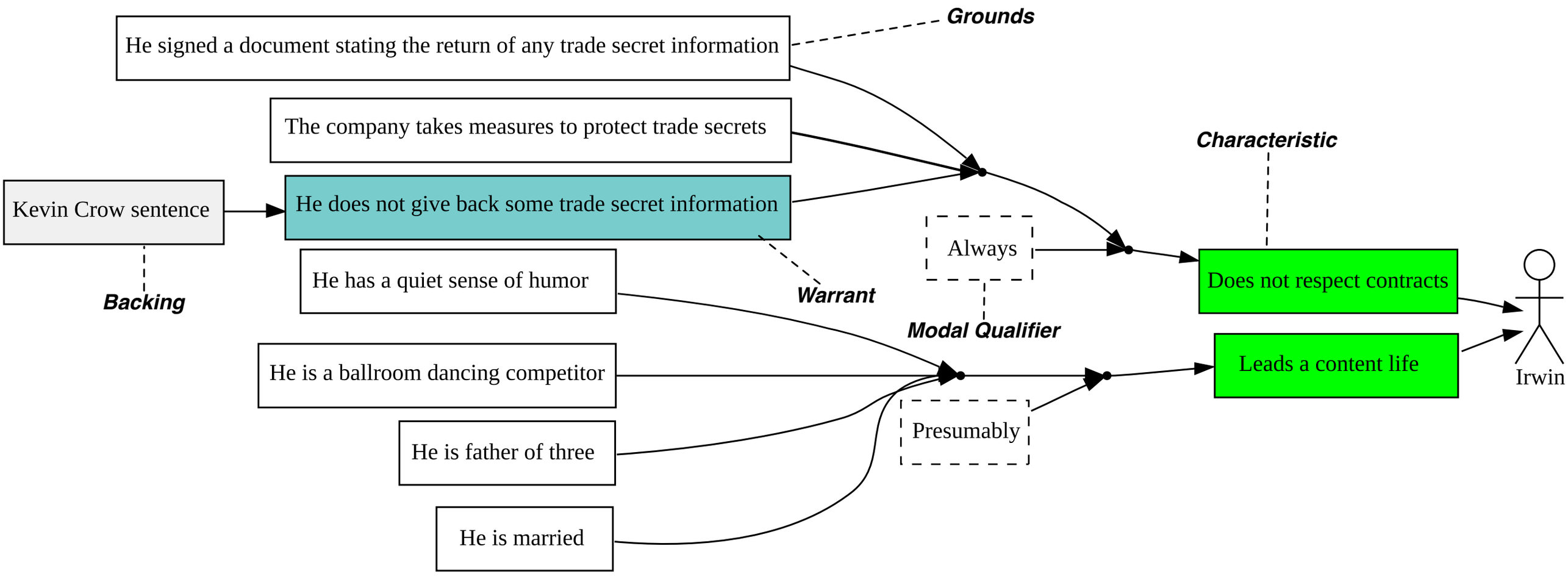
Toulmin Model

Toulmin, S. (2003). The uses of argument. Cambridge University Press, updated edition.

Toulmin Model



Toulmin, S. (2003). The uses of argument. Cambridge University Press, updated edition.


He signed a document stating the return of any trade secret information
Grounds
The company takes measures to protect trade secrets
Characteristic
Kevin Crow sentence
He does not give back some trade secret information
Always
Backing
He has a quiet sense of humor
Warrant
Does not respect contracts
Modal Qualifier
He is a ballroom dancing competitor
Leads a content life
Irwin
Presumably
He is father of three
He is married

Edit persona

Name

Irwin

Type

Primary

Assumption Persona

Activities | Attitudes | Aptitudes

Irwin is married and a father of three. He is described by friends as having a quiet sense of humor and is an excellent competitive ballroom dancer.

He signed a confidentiality agreement with his employer, and on exit interview he will be expected to sign a document promising the return of any information considered to be a trade secret. However, he chose to break both of these agreements.

Environment

Development a

Summary | Narrative

Direct/Indirect Persona

Role
Malicious App user
Malicious Application Developer

Update | Close


Ethan
Frankie
Gary
Harold
Irwin
David
PZH containing an MTM?
-XHR + Attestation
Phase 2
- TRUST 2011 Mobile papers
- Trusted Execution Environments
- TNC
- TPCH+TPZP
-DRM
-More Attestation
-TNC
-IBE+ECC
-Remote mgmt
-Social N/W rep/identity integration

Communication

USR

UC-TA4-007

Helen

Device smashing

Profile Management

WebApp

AppState

Ethan

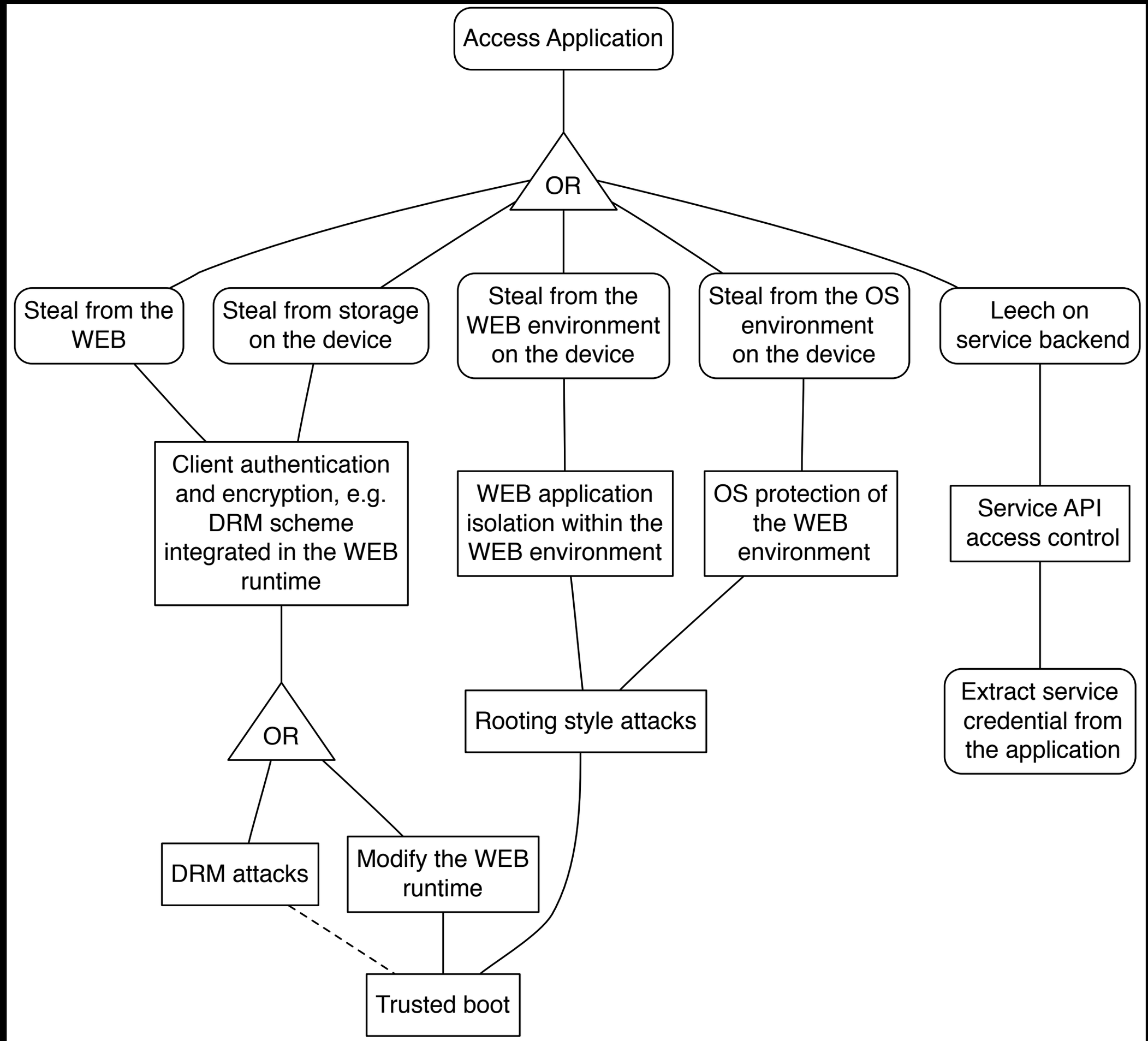
Webinos API vulnerability

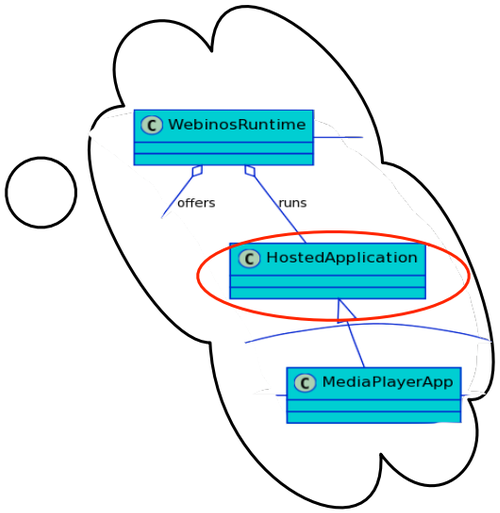
OR

Exploit WebApp

OR

Device Feature Integration


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
Rooting style attacks
OR
DRM attacks
Modify the WEB runtime
Trusted boot



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

3.7.6. Overlay network facilitated relay attack

Threat	NFC relay attack
Vulnerability	System data trust
Rating	Tolerable

3.7.6.1 Context and Events Misuse Case

As Alice was walking away from the bar with her drinks, she narrowly avoided dropping one of her glasses as man brushed past her. "Sorry", he mumbled as he walked briskly towards the toilets.

David deviced a new scam which took advantage of the recent take-off of NFC based mobile payment, and the new webinos platform that could link different apps and devices together. The scam involved dropping a leech mobile phone into someone's bag which contained a webinos enabled NFC phone. The leech would attempt to get the victim's phone to join his personal zone which, David estimated, would not be too difficult. Once in place, David could then purchase things via NFC, while webinos routed the request to the victim's NFC reader via the personal zone overlay network. David tinkered around with different devices, settings, and applications, and was quite surprised at how easy this scam appeared to be. Consequently, he would need to make the most use of this exploit quickly before other people got in on the act.

David's plan was to find somewhere where there would be lots of young but unsuspecting people who might not notice something being put into their bags. David decided a nightclub on a Friday night would be a good bet. As David entered the club at shortly after midnight, he noticed a large group of people mingling near the bar. As he approached, he noticed a large women trying to carry multiple drinks with a hand-bag slung around her shoulder. Confidentally, with his leech device in hand, David walked towards this woman.

What's in it for me?

- Grounds thinking about attackers
- Fits into your design activities
- Helps justify security design decisions