Lecture 2
Threat Modeling

Dr. Lotfi ben Othmane

23 October 2015

Fraunhofer
SIT

TECHNISCHE
UNIVERSITÄT
DARMSTADT

SECURE
SOFTWARE ENGINEERING
GROUP

EC SPRIDE

Agenda

1. Vulnerabilities in the news: Adobe flash player vulnerability by Manjiri Birajdar
2. SSD Labs by Lisa
3. Lecture by Sven Türpe and Andreas Poller from Fraunhofer SIT

Survey

Thanks to the students who took the survey (even incomplete).

SVN

- The SVN for the course is now available
  https://repository.st.informatik.tu-darmstadt.de/sse/secdev/2015/

- Accessible from the TU network
  - VPN information: http://www.hrz.tu-darmstadt.de/netz/netz_datennetz_internet_1/netz_datennetz_internet_vpn_1/netz_vpn_downloads_1/index.de.jsp

Labs

- Only the groups who have registered through the **form** (not the spreadsheet) will be registered for the labs
- The registered groups are considered **final**
- Group numbers will be communicated via the students‘ TU emails
- Groups with at least one member not registered in TUCaN will **not** be registered
- Groups **not** submitting on time will **not** be graded

Responsible Disclosure

- When finding vulnerabilities:
  - No disclosure
  - Limited disclosure
  - Full disclosure
  - Responsible disclosure

- Balance between
  - Informing the public
  - Giving the vendor‘s time to respond properly

SECURE SOFTWARE ENGINEERING GROUP

EC SPRIDE

Responsible Disclosure

- ➢ It is tempting to gloat …

Look at me! I did it!

The vulnerability
in the powerplant‘s
control system
is right here!

Responsible Disclosure

- … but it is also dangerous to the public …

Responsible Disclosure

- … and to yourself

Responsible Disclosure

- What is responsible disclosure?

Keep silent

Inform vendors

Wait

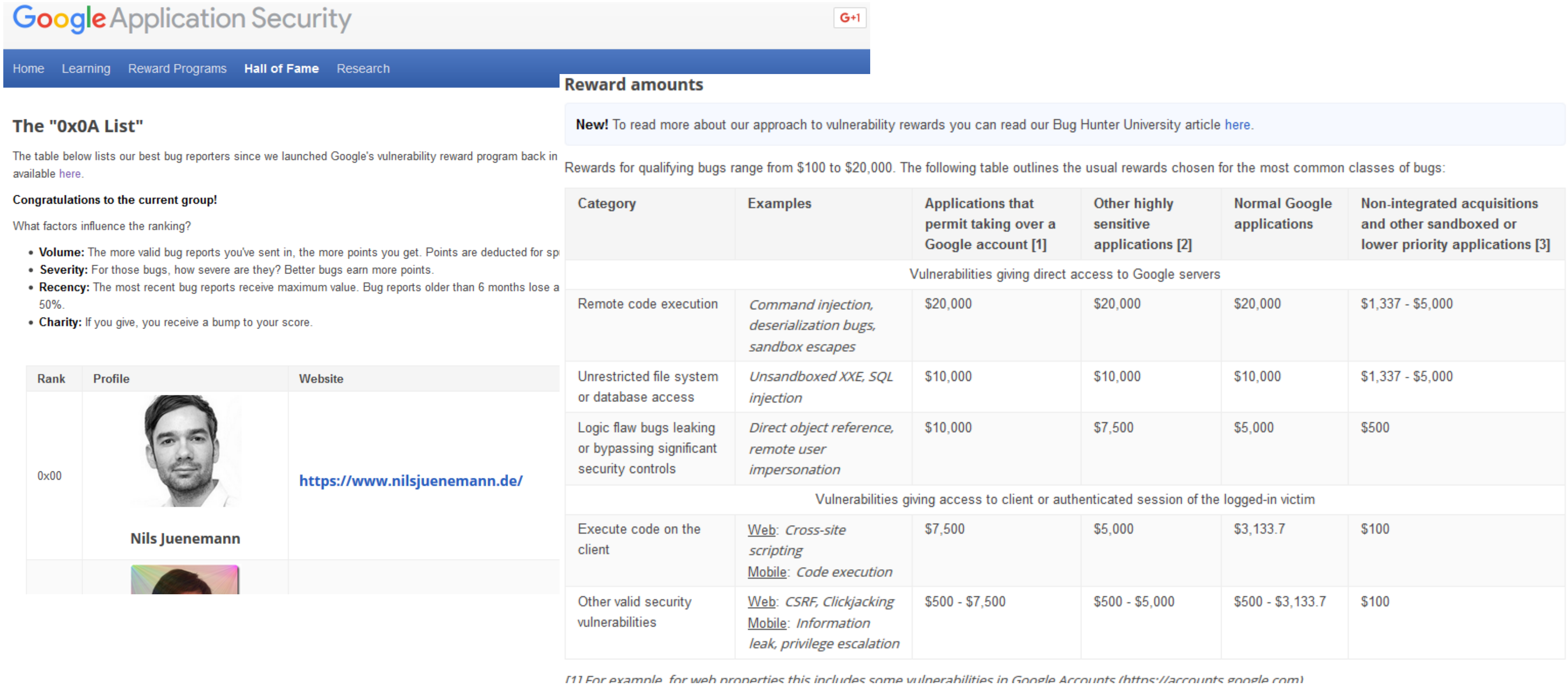
Gloat moderately

- Short term anonymous buzz

+ Long lasting reputation

Responsible Disclosure

- Responsible disclosure
  - Is encouraged, and sometimes rewarded



The "0x0A List"

The table below lists our best bug reporters since we launched Google's vulnerability reward program back in available here.

Congratulations to the current group!

What factors influence the ranking?

- **Volume:** The more valid bug reports you've sent in, the more points you get. Points are deducted for sp
- **Severity:** For those bugs, how severe are they? Better bugs earn more points.
- **Recency:** The most recent bug reports receive maximum value. Bug reports older than 6 months lose a 50%.
- **Charity:** If you give, you receive a bump to your score.

Rank	Profile	Website
0x00	Nils Juenemann	https://www.nilsjuenemann.de/

Reward amounts

New! To read more about our approach to vulnerability rewards you can read our Bug Hunter University article here.

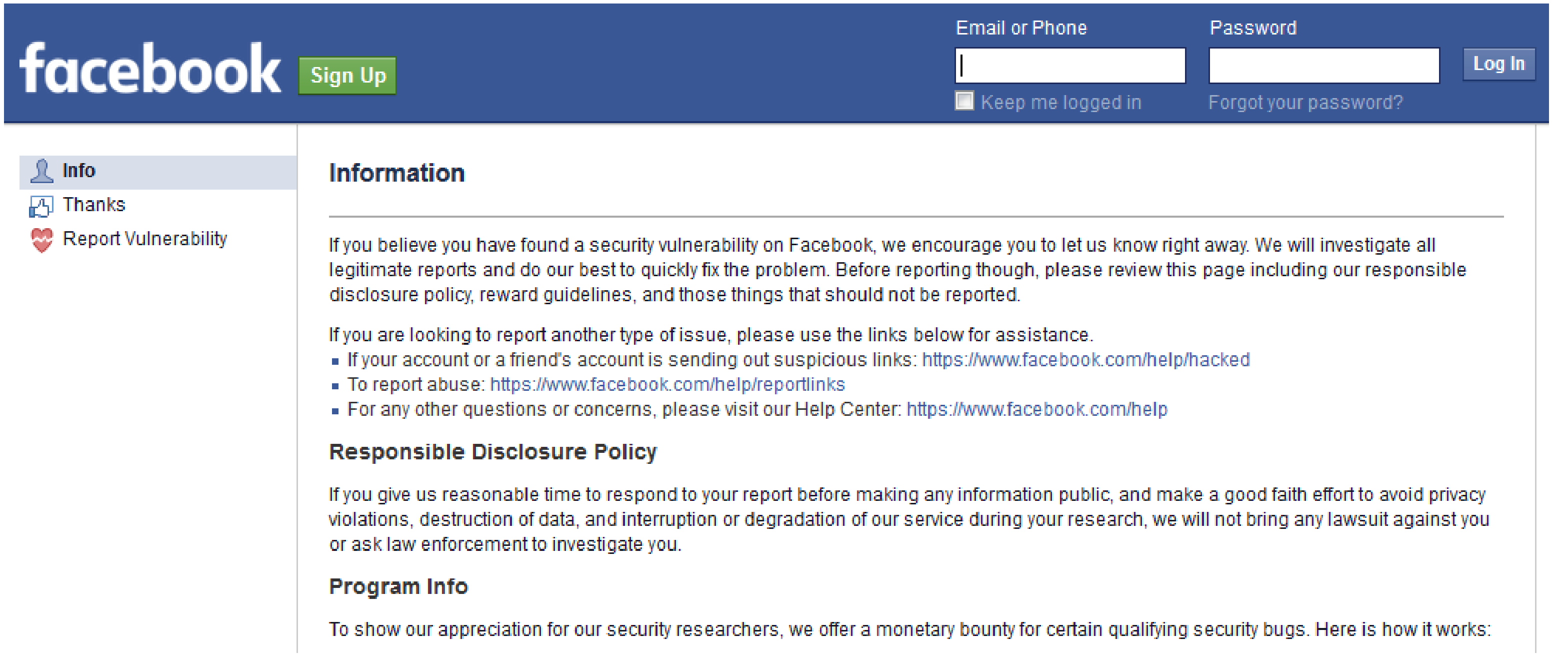
Rewards for qualifying bugs range from $100 to $20,000. The following table outlines the usual rewards chosen for the most common classes of bugs:

Category	Examples	Applications that permit taking over a Google account [1]	Other highly sensitive applications [2]	Normal Google applications	Non-integrated acquisitions and other sandboxed or lower priority applications [3]
Vulnerabilities giving direct access to Google servers					
Remote code execution	*Command injection, deserialization bugs, sandbox escapes*	$20,000	$20,000	$20,000	$1,337 - $5,000
Unrestricted file system or database access	*Unsandboxed XXE, SQL injection*	$10,000	$10,000	$10,000	$1,337 - $5,000
Logic flaw bugs leaking or bypassing significant security controls	*Direct object reference, remote user impersonation*	$10,000	$7,500	$5,000	$500
Vulnerabilities giving access to client or authenticated session of the logged-in victim					
Execute code on the client	Web: *Cross-site scripting* Mobile: *Code execution*	$7,500	$5,000	$3,133.7	$100
Other valid security vulnerabilities	Web: *CSRF, Clickjacking* Mobile: *Information leak, privilege escalation*	$500 - $7,500	$500 - $5,000	$500 - $3,133.7	$100

[1] For example, for web properties this includes some vulnerabilities in Google Accounts (https://accounts.google.com).

Responsible Disclosure

- ➢ Responsible disclosure
  - – Is encouraged, and sometimes rewarded



Information

If you believe you have found a security vulnerability on Facebook, we encourage you to let us know right away. We will investigate all legitimate reports and do our best to quickly fix the problem. Before reporting though, please review this page including our responsible disclosure policy, reward guidelines, and those things that should not be reported.

If you are looking to report another type of issue, please use the links below for assistance.

- If your account or a friend's account is sending out suspicious links: https://www.facebook.com/help/hacked
- To report abuse: https://www.facebook.com/help/reportlinks
- For any other questions or concerns, please visit our Help Center: https://www.facebook.com/help

Responsible Disclosure Policy

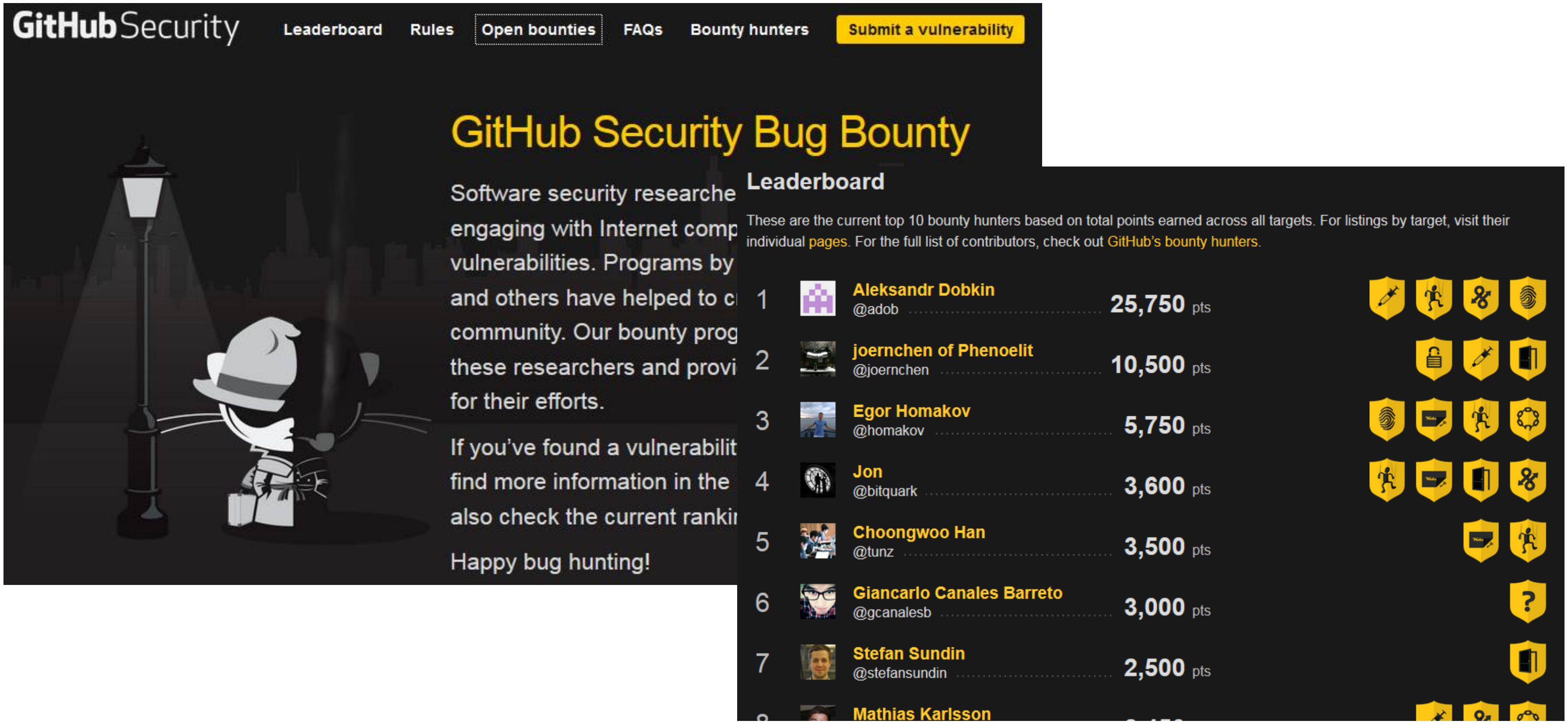
If you give us reasonable time to respond to your report before making any information public, and make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service during your research, we will not bring any lawsuit against you or ask law enforcement to investigate you.

Program Info

To show our appreciation for our security researchers, we offer a monetary bounty for certain qualifying security bugs. Here is how it works:

Responsible Disclosure

- Responsible disclosure
  - Is encouraged, and sometimes rewarded



GitHub Security Bug Bounty

Software security researche
engaging with Internet comp
vulnerabilities. Programs by
and others have helped to c
community. Our bounty prog
these researchers and provi
for their efforts.

If you've found a vulnerabilit
find more information in the
also check the current rankii

Happy bug hunting!

Leaderboard

These are the current top 10 bounty hunters based on total points earned across all targets. For listings by target, visit their individual pages. For the full list of contributors, check out GitHub's bounty hunters.

1	Aleksandr Dobkin @adob	25,750 pts
2	joernchen of Phenoelit @joernchen	10,500 pts
3	Egor Homakov @homakov	5,750 pts
4	Jon @bitquark	3,600 pts
5	Choongwoo Han @tunz	3,500 pts
6	Giancarlo Canales Barreto @gcanalesb	3,000 pts
7	Stefan Sundin @stefansundin	2,500 pts
8	Mathias Karlsson	

Examples of Responsible Disclosure

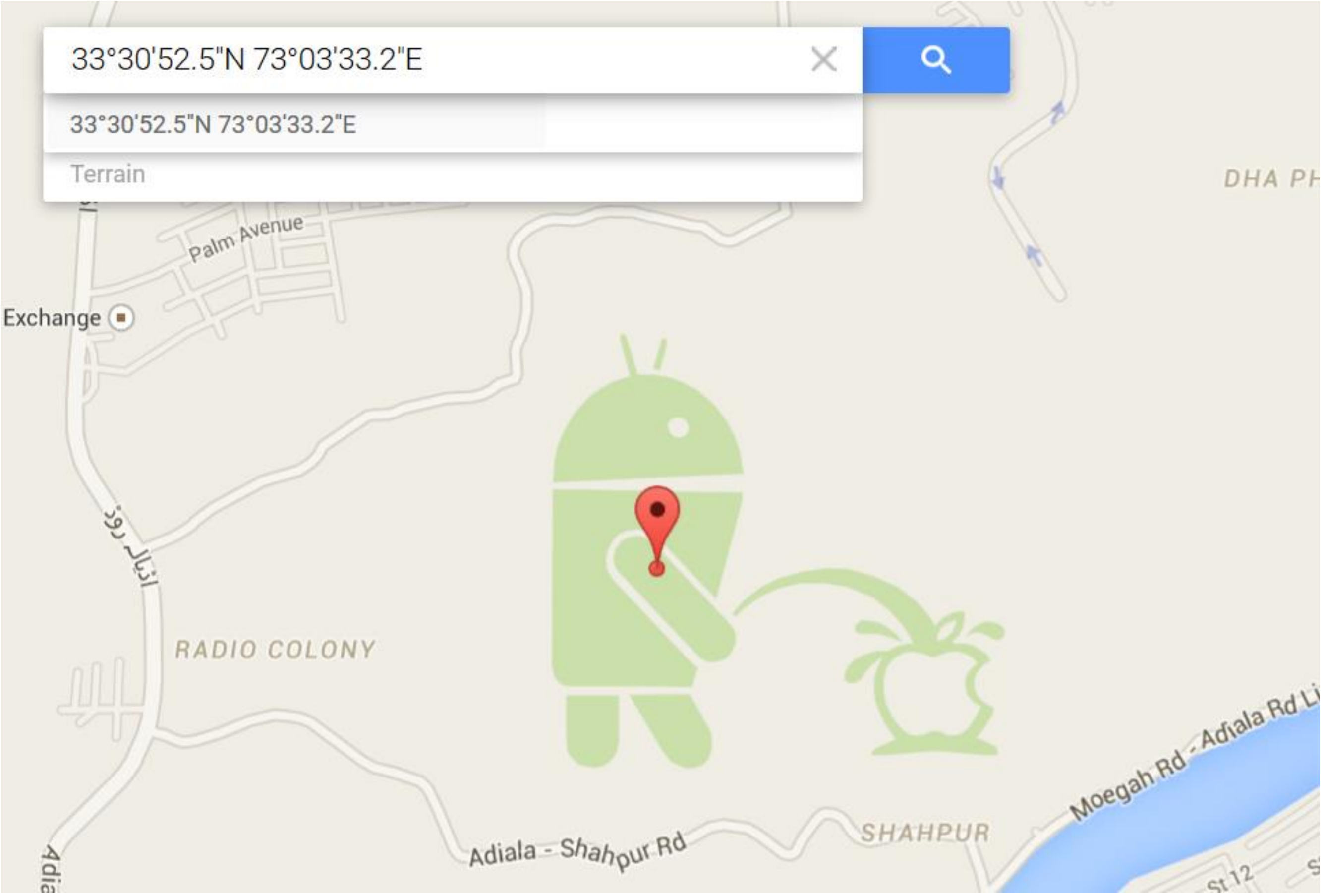
- 769 Google Security Reward recipients between 2010 and 2015
- 519 people additionally reported confirmed vulnerabilities

- 155 GitHub bounty hunters since June 2013

- And many more, especially in research groups

https://www.google.com/about/appsecurity/
https://bounty.github.com/

Example of Irresponsible Disclosure



33°30'52.5"N 73°03'33.2"E

33°30'52.5"N 73°03'33.2"E

Terrain

- ➢ Why is this an irresponsible disclosure?
- ➢ What should the bug finder have done?

Responsible Disclosure

- We encourage you to find flaws
- BUT do it ethically.

- From now on in this course:
  - Responsible disclosure will be rewarded
  - Irresponsible disclosure will be sanctioned

Lab 1

- Students will choose one of two subjects:
  - Set-UID
  - Web same-origin policy
- Available on TUCAN and the course‘s webpage
- Due: **Thursday, Nov 5th, 23:59**

Secure Software Development Course

Threat Modeling

Sven Türpe, Andreas Poller

Fraunhofer

SIT

Introduction to Threat Modeling

Lets talk about threats!

What is a threat?

Definition..

- "A threat is an intent to inflict damage on a system.” (Landwehr 2001)
- "A threat consists of an adverse action performed by a threat agent on an asset." (Common Criteria)
- "Who might attack against what assets, using what resources, with what goal in mind, when/where/why, and with what probability.” (Johnston 2010)
- "Threats remain ideas until practical examples have been demonstrated.“ (Schäfer 2009)
- "A threat is a potential cause of an unwanted incident.” (Lund 2011)

What is a threat?

More definitions..

- “A threat is an entity that wants to do harm to you or something you care about” (http://www.bitsmasherpress.com/?p=67)
- “intended cause” (Pieters 2011)
- "A potential for harm of an asset.“ (Yoshioka 2008)
- “Threats are the likelihood of, or potential for, hazardous events occurring.” (Schumacher 2006)
- "A threat is the potential for abuse of an asset that will cause harm in the context of the problem“ (Haley 2004)
- “Threat is a general condition, situation, or state ([…]) that may result in one or more related attacks” (Firesmith 2004)

The concept of „threats“ is ….

- … ambiguous
- … approached from various perspectives
- … subjective dependent on *who* talks about threats
- … often used inappropriately (e.g. as synonym for vulnerabilities)
- … but crucial to understand security problem at hand.

Components of a Security Problem

Threats

Petty criminals
Organized crime
Law enforcement

No encryption
Software defects
Mobile gadget

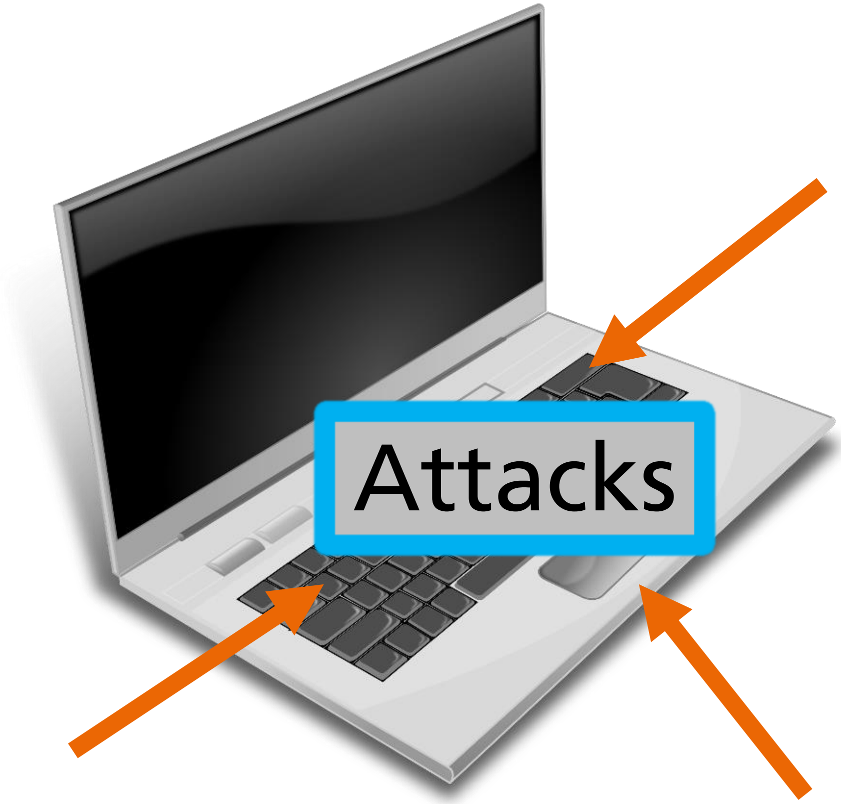
Vulnerabilities

Secrets
System integrity
Hardware value

Assets

(all going after assets..)

Components of a Security Problem



Attacks

Threats

Petty criminals
Organized crime
Law enforcement

No encryption
Software defects
Mobile gadget

Vulnerabilities

Secrets
System integrity
Hardware value

Assets

Approaches to Threat Modeling

Attacker-Centric

Who are my opponents?
How will they act?

How am I vulnerable?
What can attacks achieve?

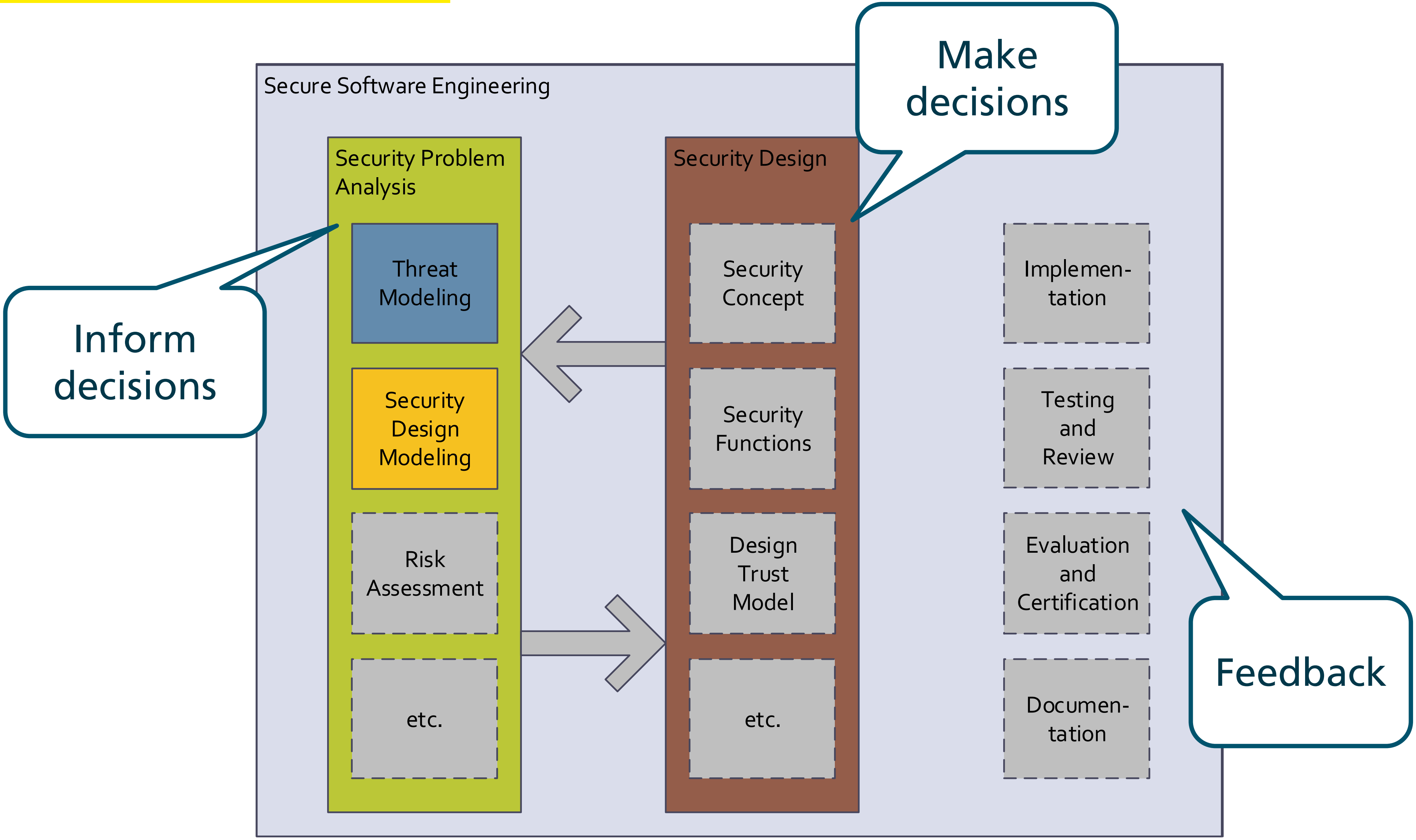
Software-Centric

What's there to protect?
What would hurt me?

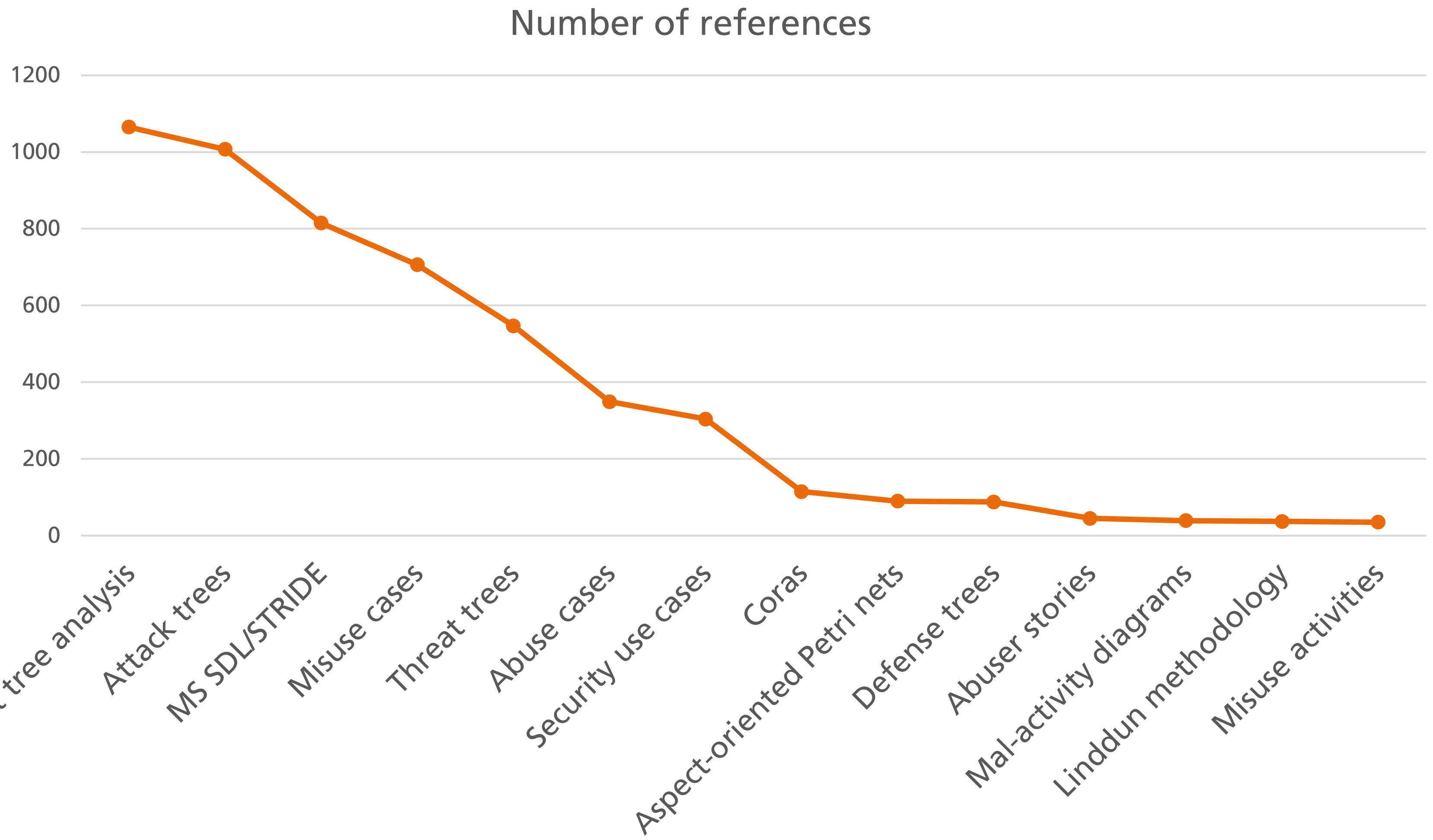
Asset-Centric

Threat Modeling as a Development Activity

Threat Modeling in Software Development

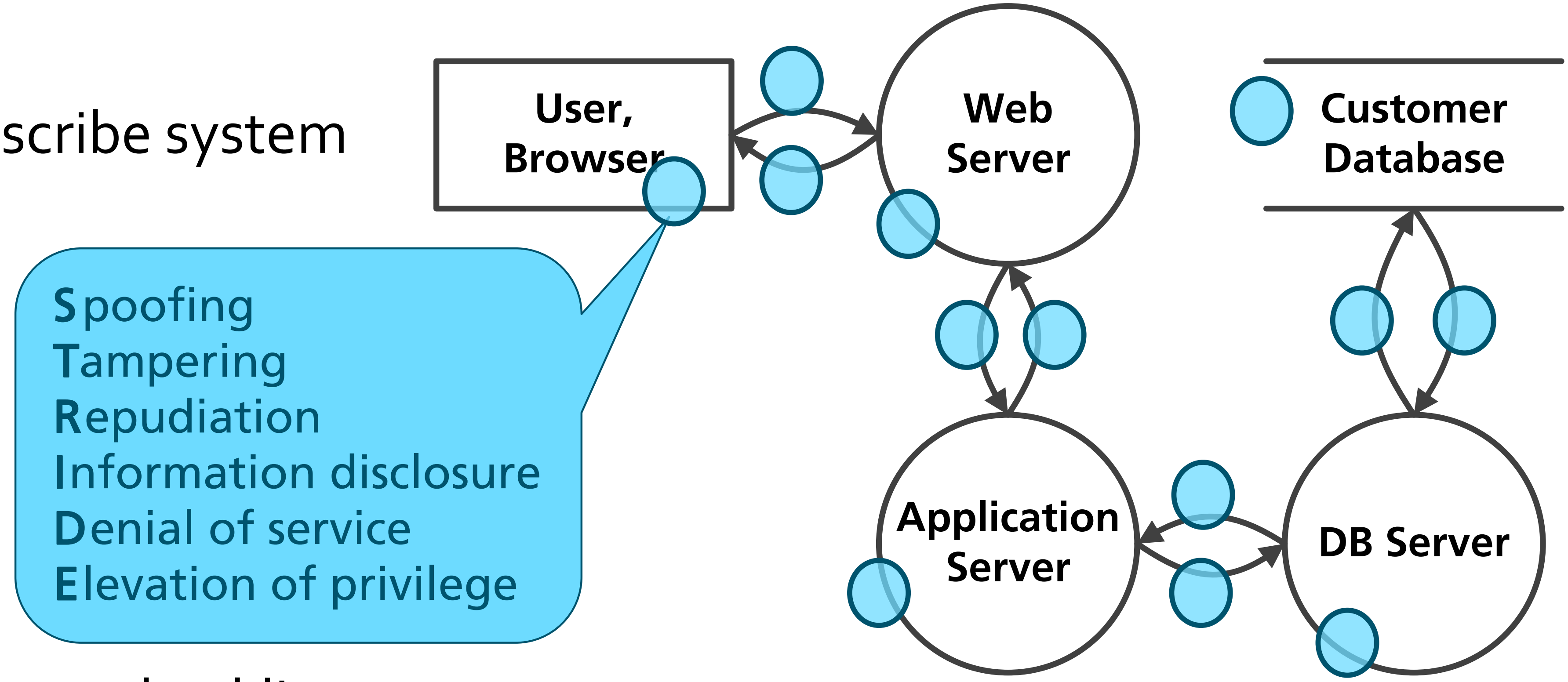


Threat Modeling Techniques



MS SDL Threat Modeling

1. Describe system



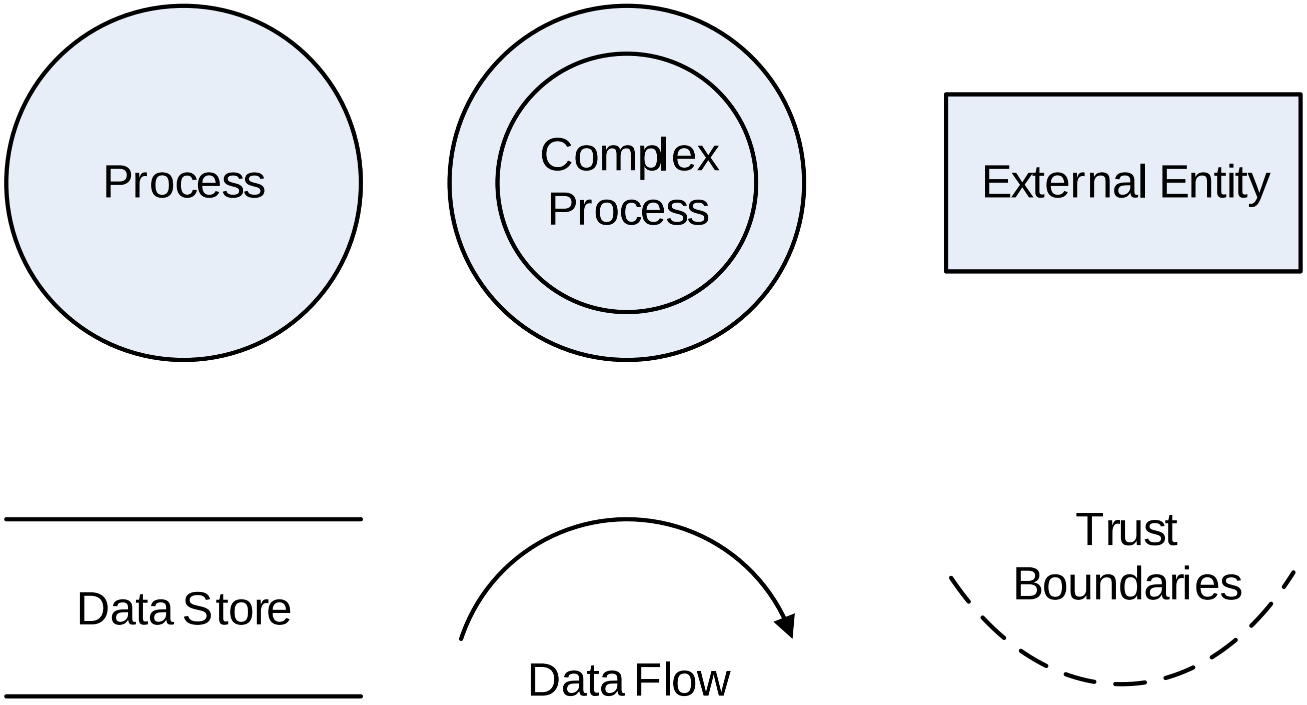
Spoofing
Tampering
Repudiation
Information disclosure
Denial of service
Elevation of privilege

2. Create checklist

3. Assess impact and find countermeasures for each item

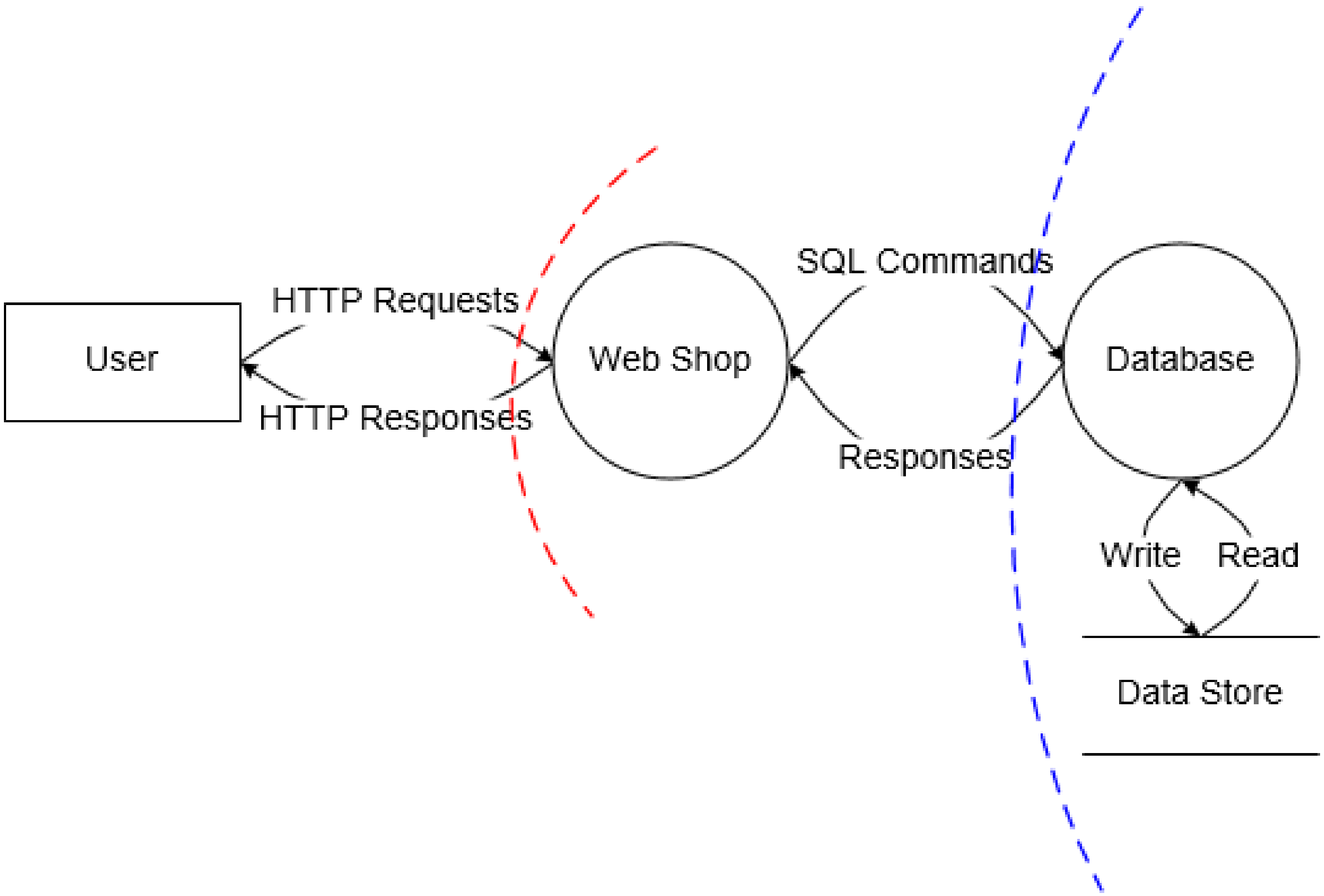
STRIDE, Data Flow Diagrams

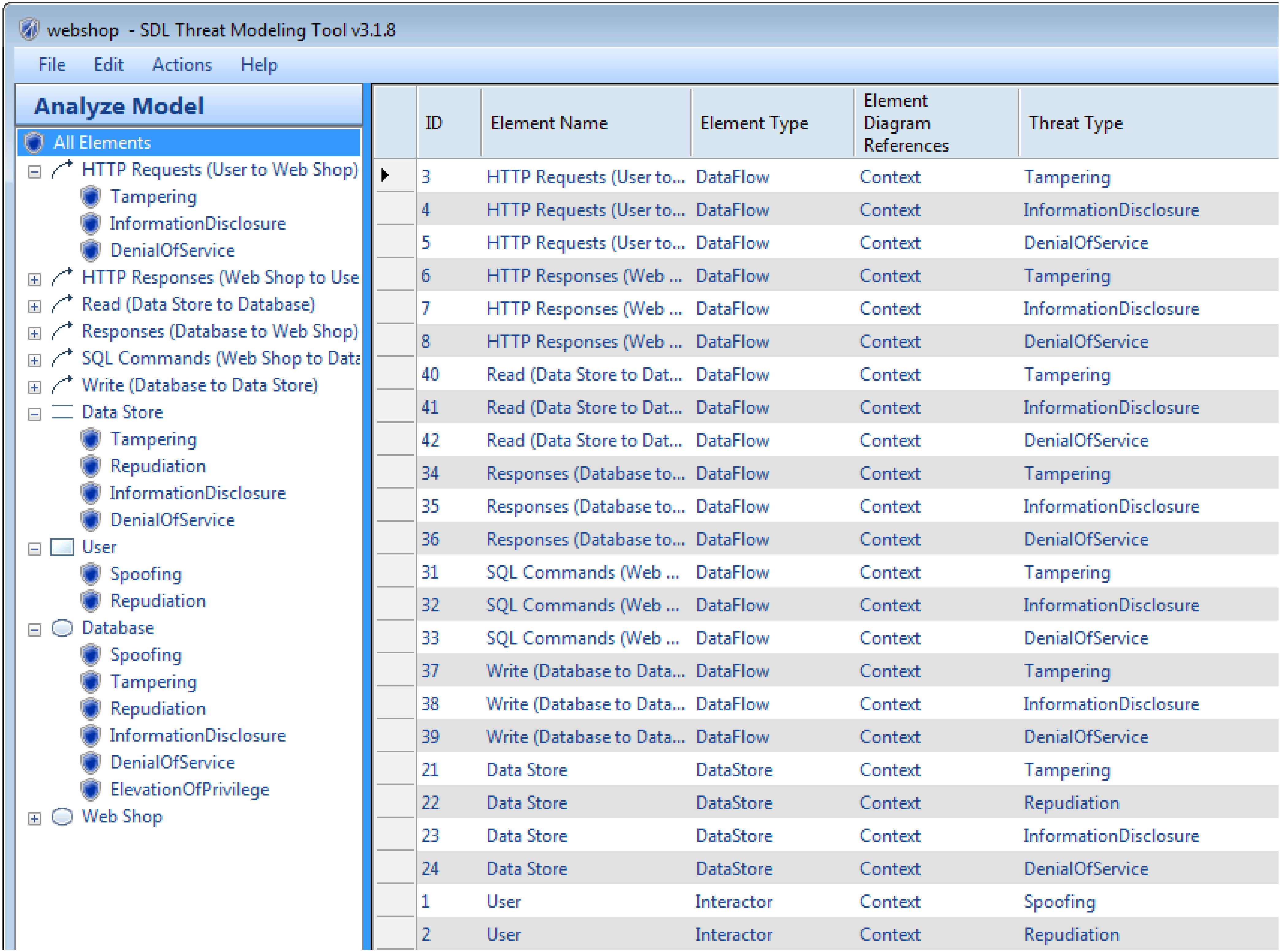
DFD entity	S	T	R	I	D	E
External Entity	X		X			
Data Flow		X		X	X	
Data Store		X	(X)	X	X	
Process	X	X	X	X	X	X



Demo: MS Threat Modeling Tool

Example: The famous web shop

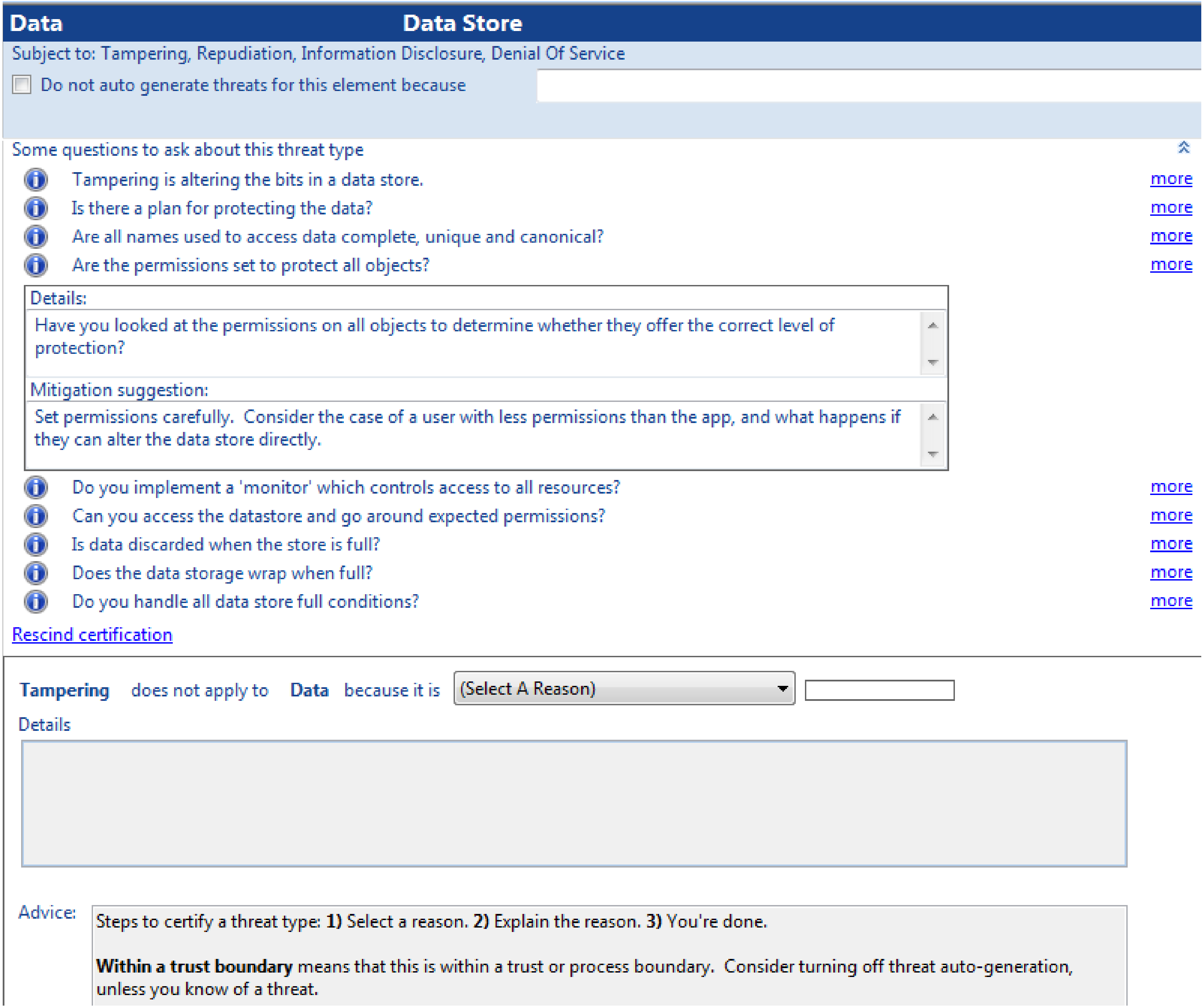




Analyze Model

- All Elements
- HTTP Requests (User to Web Shop)
  - Tampering
  - InformationDisclosure
  - DenialOfService
- HTTP Responses (Web Shop to Use
- Read (Data Store to Database)
- Responses (Database to Web Shop)
- SQL Commands (Web Shop to Data
- Write (Database to Data Store)
- Data Store
  - Tampering
  - Repudiation
  - InformationDisclosure
  - DenialOfService
- User
  - Spoofing
  - Repudiation
- Database
  - Spoofing
  - Tampering
  - Repudiation
  - InformationDisclosure
  - DenialOfService
  - ElevationOfPrivilege
- Web Shop

ID	Element Name	Element Type	Element Diagram References	Threat Type
3	HTTP Requests (User to...	DataFlow	Context	Tampering
4	HTTP Requests (User to...	DataFlow	Context	InformationDisclosure
5	HTTP Requests (User to...	DataFlow	Context	DenialOfService
6	HTTP Responses (Web ...	DataFlow	Context	Tampering
7	HTTP Responses (Web ...	DataFlow	Context	InformationDisclosure
8	HTTP Responses (Web ...	DataFlow	Context	DenialOfService
40	Read (Data Store to Dat...	DataFlow	Context	Tampering
41	Read (Data Store to Dat...	DataFlow	Context	InformationDisclosure
42	Read (Data Store to Dat...	DataFlow	Context	DenialOfService
34	Responses (Database to...	DataFlow	Context	Tampering
35	Responses (Database to...	DataFlow	Context	InformationDisclosure
36	Responses (Database to...	DataFlow	Context	DenialOfService
31	SQL Commands (Web ...	DataFlow	Context	Tampering
32	SQL Commands (Web ...	DataFlow	Context	InformationDisclosure
33	SQL Commands (Web ...	DataFlow	Context	DenialOfService
37	Write (Database to Data...	DataFlow	Context	Tampering
38	Write (Database to Data...	DataFlow	Context	InformationDisclosure
39	Write (Database to Data...	DataFlow	Context	DenialOfService
21	Data Store	DataStore	Context	Tampering
22	Data Store	DataStore	Context	Repudiation
23	Data Store	DataStore	Context	InformationDisclosure
24	Data Store	DataStore	Context	DenialOfService
1	User	Interactor	Context	Spoofing
2	User	Interactor	Context	Repudiation



Data **Data Store**

Subject to: Tampering, Repudiation, Information Disclosure, Denial Of Service

□ Do not auto generate threats for this element because

Some questions to ask about this threat type

- Tampering is altering the bits in a data store. more
- Is there a plan for protecting the data? more
- Are all names used to access data complete, unique and canonical? more
- Are the permissions set to protect all objects? more

Details:

Have you looked at the permissions on all objects to determine whether they offer the correct level of protection?

Mitigation suggestion:

Set permissions carefully. Consider the case of a user with less permissions than the app, and what happens if they can alter the data store directly.

- Do you implement a 'monitor' which controls access to all resources? more
- Can you access the datastore and go around expected permissions? more
- Is data discarded when the store is full? more
- Does the data storage wrap when full? more
- Do you handle all data store full conditions? more

Rescind certification

Tampering does not apply to **Data** because it is (Select A Reason)

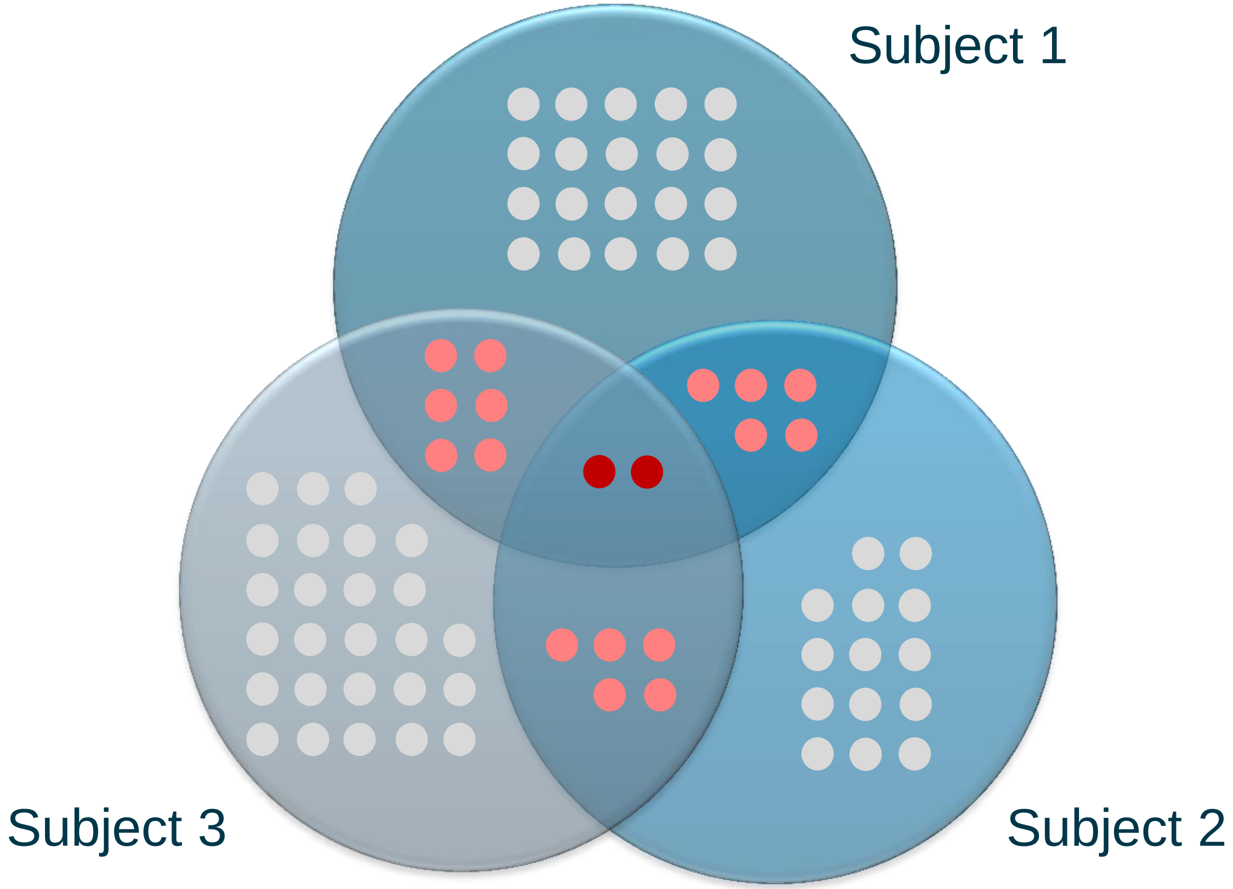
Details

Advice: Steps to certify a threat type: **1)** Select a reason. **2)** Explain the reason. **3)** You're done.

Within a trust boundary means that this is within a trust or process boundary. Consider turning off threat auto-generation, unless you know of a threat.

Summary: Challenges for Using MS SDL Threat Modeling

When Three Engineers Interpret a Threat Model …



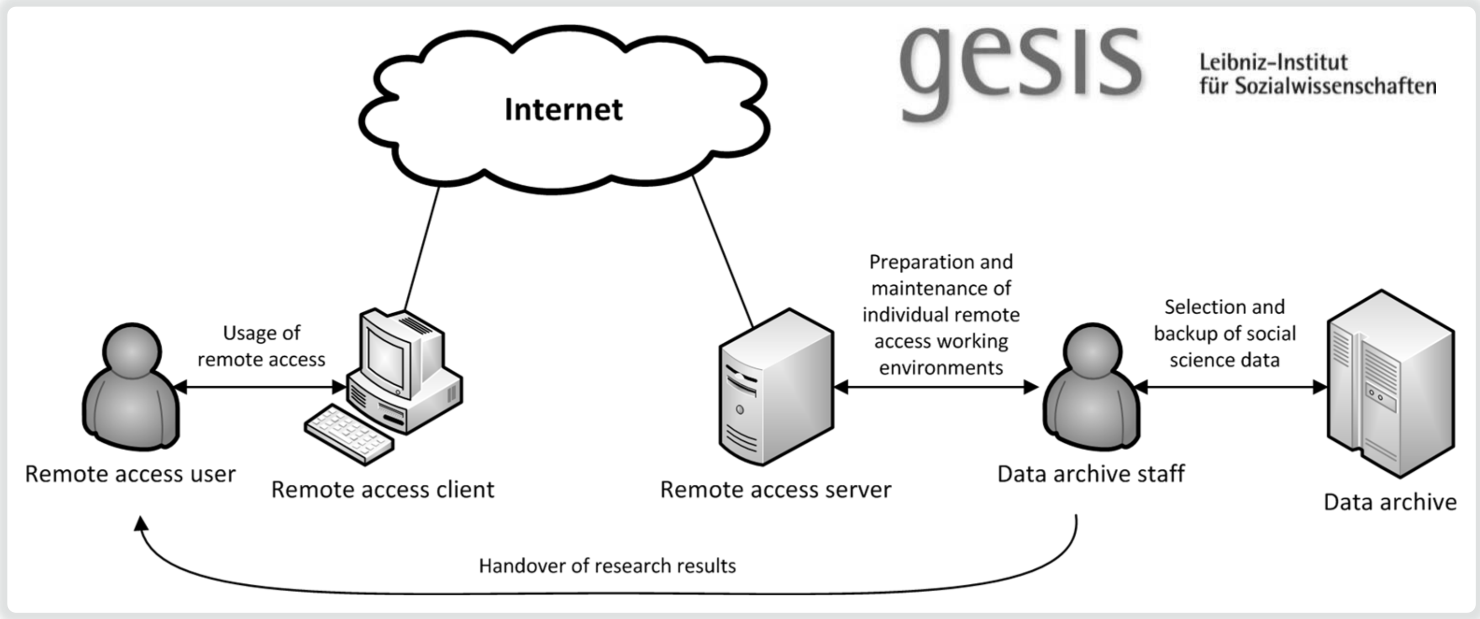
SDL Threat Modeling in the Wild: Research Setting

Social Scientist

Computer Scientist

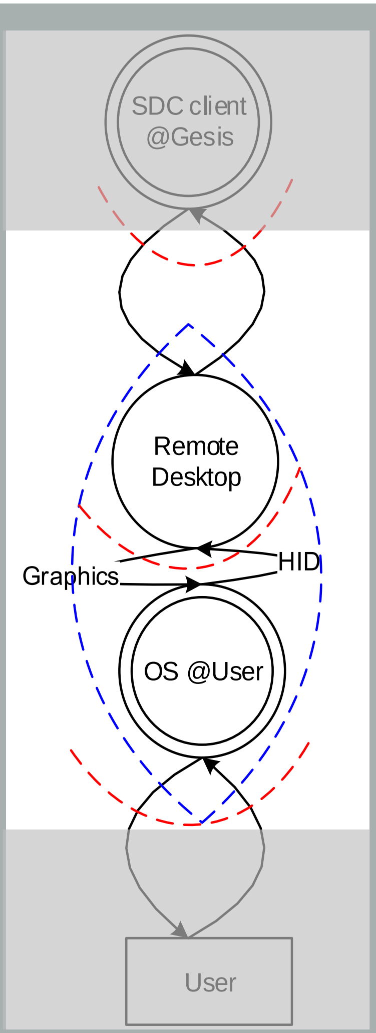
IT Services

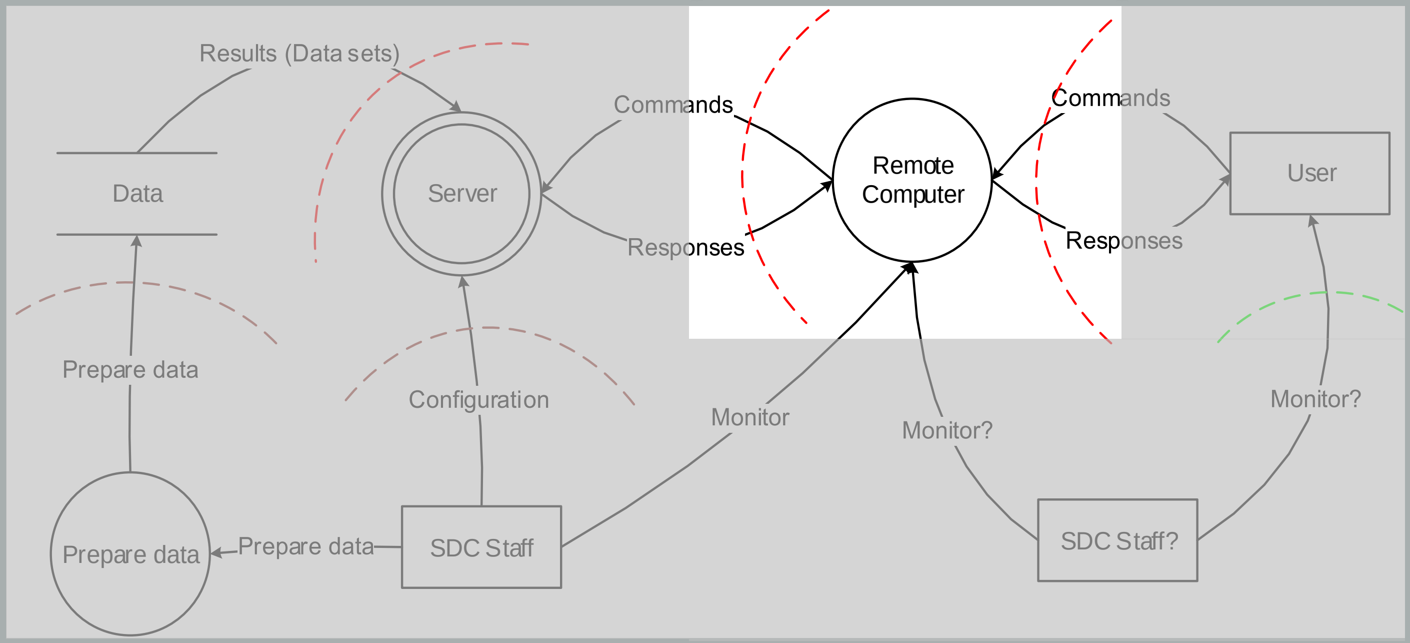
Data Archive Staff


gesis
Leibniz-Institut für Sozialwissenschaften
Internet
Usage of remote access
Preparation and maintenance of individual remote access working environments
Selection and backup of social science data
Remote access user
Remote access client
Remote access server
Data archive staff
Data archive
Handover of research results

Individual Perspectives

I5: Solution Proposal





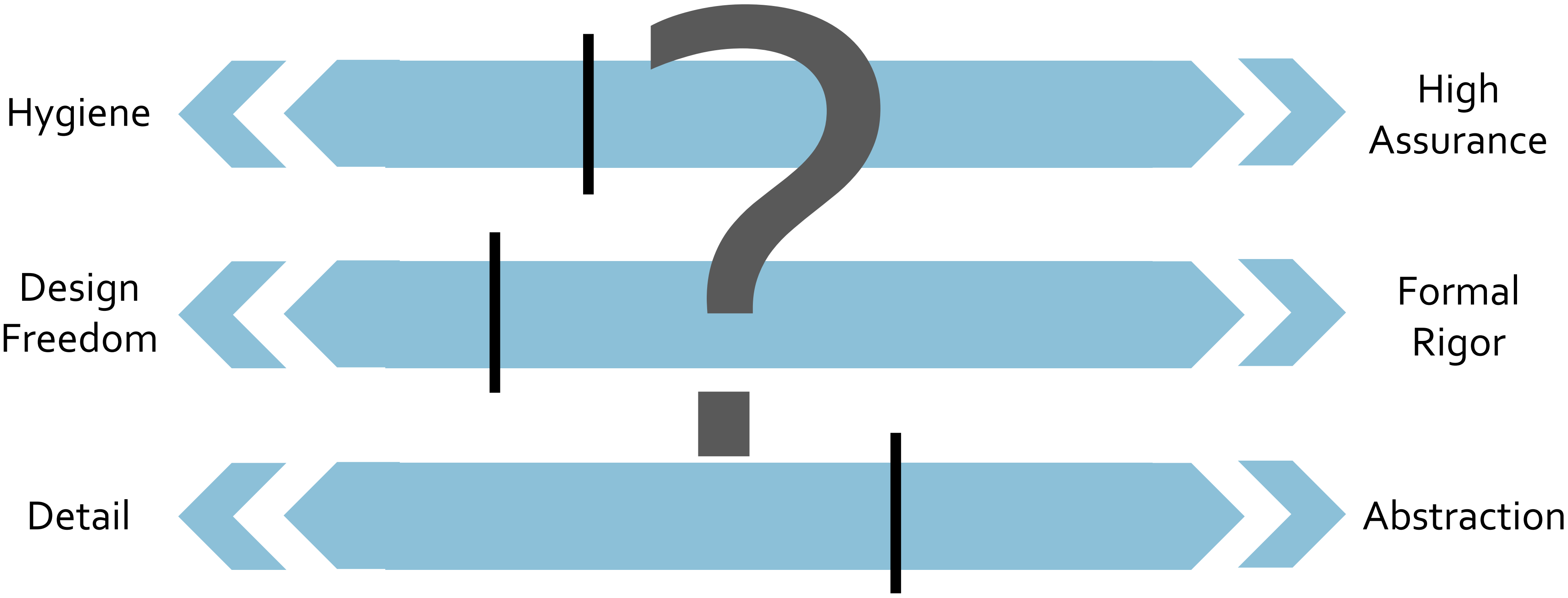
I6: Big Picture

What can you build?

What do you need?

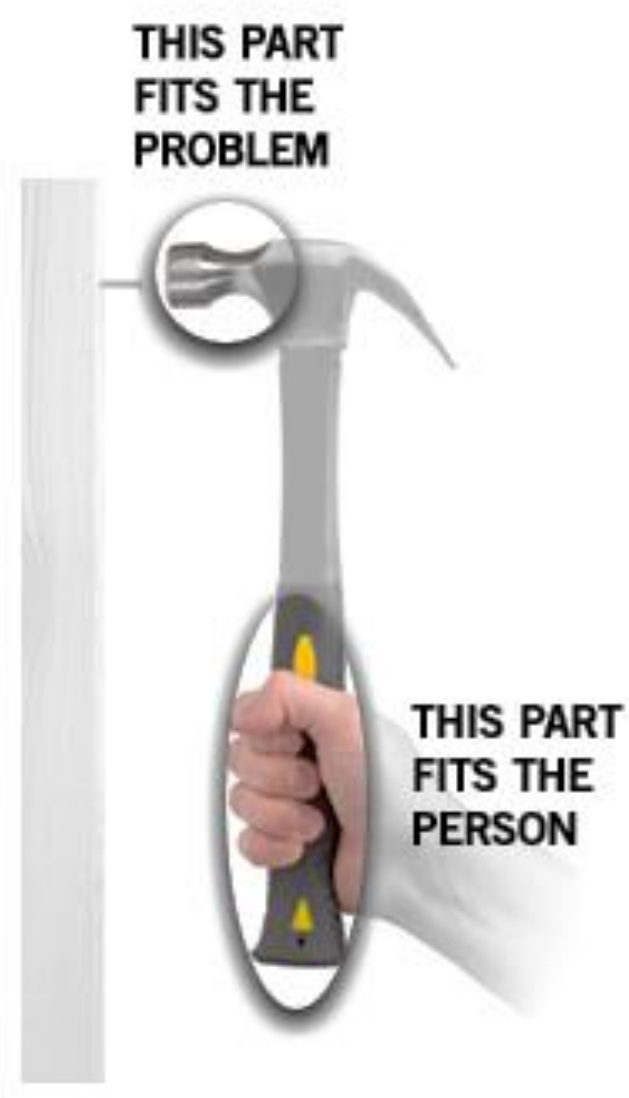
Wrap-up

Where Is the Sweet Spot?



- Little empirical evidence
- Moving targets – security designs evolve
- Tacit knowledge – documentation is always outdated

Tools



Problem:

Identify security concerns

Developer
Team
Process
Organization

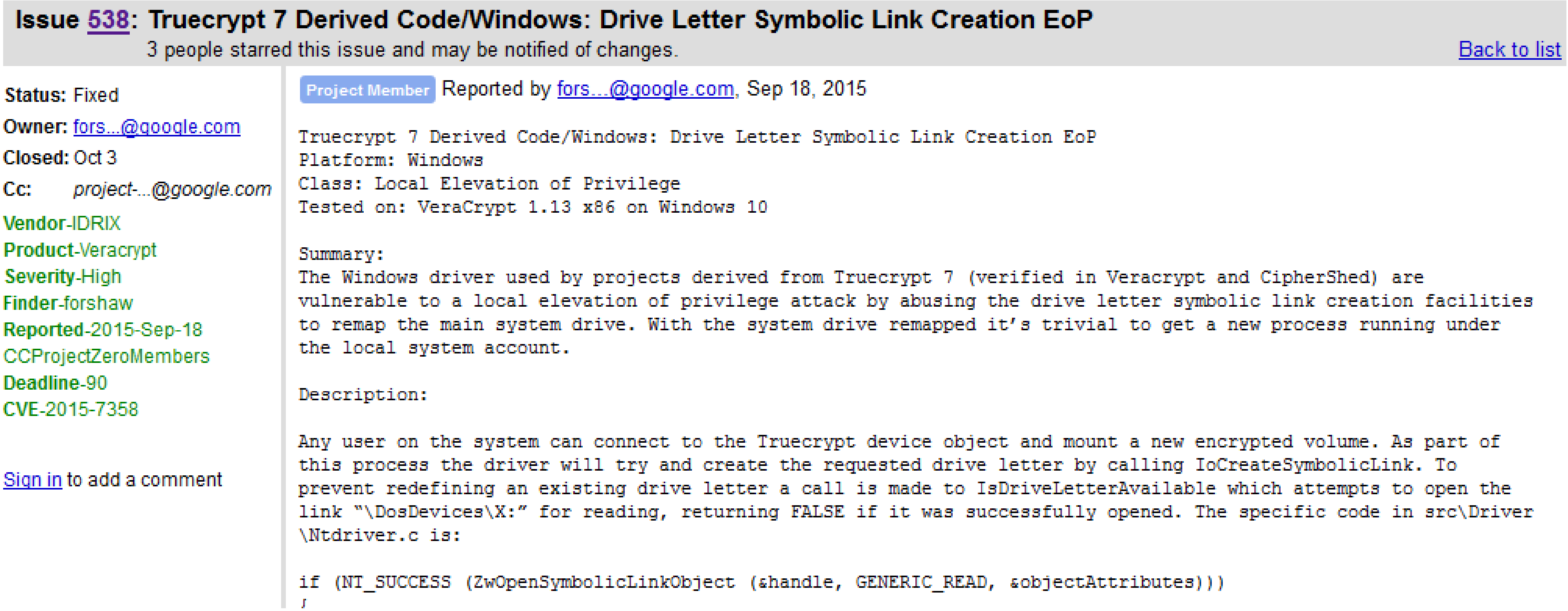
Source: http://worrydream.com/#!/ABriefRantOnTheFutureOfInteractionDesign

Back to Laptop Scenario

When is HDD Encryption required?

When is HDD Encryption *not* required?

Is there a reasonable threat for this bug?



Issue 538: Truecrypt 7 Derived Code/Windows: Drive Letter Symbolic Link Creation EoP

3 people starred this issue and may be notified of changes.

Status: Fixed
Owner: fors...@google.com
Closed: Oct 3
Cc: *project-...@google.com*

Vendor-IDRIX
Product-Veracrypt
Severity-High
Finder-forshaw
Reported-2015-Sep-18
CCProjectZeroMembers
Deadline-90
CVE-2015-7358

Reported by fors...@google.com, Sep 18, 2015

```
Truecrypt 7 Derived Code/Windows: Drive Letter Symbolic Link Creation EoP
Platform: Windows
Class: Local Elevation of Privilege
Tested on: VeraCrypt 1.13 x86 on Windows 10

Summary:
The Windows driver used by projects derived from Truecrypt 7 (verified in Veracrypt and CipherShed) are
vulnerable to a local elevation of privilege attack by abusing the drive letter symbolic link creation facilities
to remap the main system drive. With the system drive remapped it's trivial to get a new process running under
the local system account.

Description:

Any user on the system can connect to the Truecrypt device object and mount a new encrypted volume. As part of
this process the driver will try and create the requested drive letter by calling IoCreateSymbolicLink. To
prevent redefining an existing drive letter a call is made to IsDriveLetterAvailable which attempts to open the
link "\DosDevices\X:" for reading, returning FALSE if it was successfully opened. The specific code in src\Driver
\Ntdriver.c is:

if (NT_SUCCESS (ZwOpenSymbolicLinkObject (&handle, GENERIC_READ, &objectAttributes)))
{
```

CAST-Workshop:
“Sichere Software entwickeln”
12. November

http://www.cast-forum.de/workshops/infos/209

http://testlab.sit.fraunhofer.de

andreas.poller @ sit.fraunhofer.de

sven.tuerpe @ sit.fraunhofer.de