Course memo EP2790 HT20 Security Analysis of Large-Scale Computer Systems

Motivation

Companies today have thousands of software based computer systems that all are depending on one another in a large complex network, a system-of-systems. That IT attacks succeed to a large extent due to this complexity. A company needs to understand the whole system while an attacker only needs find one way in. At the same time, there is a large set of attack types that are utilised and plenty of proposed defence mechanisms. This course main content aims to develop students' understanding of:

- the complex IT landscape of today by creating models of such.
- which attacks that are utilised today to cause harm and how these can propagate through a large network.
- what defences there are and when they are best suited against different attack types.
- how risk can be calculated and used to prioritise security work.

Intended learning outcomes

After passing the course, the students should be able to:

- model threats in large-scale computer systems (including software, networks etc),
- simulate attacks in large-scale computer systems
- carry out risk analysis based on a model and simulation
- describe which defence mechanisms computer system can have
- report and present models, simulation, risk analysis, and defense strategy for a given system

In order to:

- understand and explain which threats a specific system can have
- understand and explain how attacks work and propagate through a system architecture
- argue why certain risks should be prioritised
- choose the right defence to decrease risk.

Main assignment description - project

Preliminaries

The purpose of the course assignment is to give skills in, and understanding of, the area of security analysis of large-scale computer systems. More specifically to learn a methodology, threat modeling, to assess cyber security risk of a (large-scale) IT system. The assignment, your project, is designed to be as realistic as possible. This means that not all information needed to solve the assignment is provided in the description. It is therefore necessary for you to make assumptions that are realistic as well as seek new information in order to pass the assignment. (*Realistic* here is not to be confused with *real*, since the assignment will for most students be done on fictitious cases.)

Introduction

You have just been hired as the chief security architect at an enterprise (what enterprise is up to you to decide). The enterprise's Chief Information Security Officer (CISO), who is also quite new in office, is giving you the assignment to do the annual risk analysis. Today the

enterprise has a large number of information systems that provides services to various parts of the business. During the recent years, the systems have been integrated with each other using different integration mechanisms to support various processes, such as sales, marketing, accounting and IT-support.
Unfortunately, the company has lost control over the complete picture of this system-of-systems since it has been, and still is, under constant change. In fact, the company has never really had the complete picture. Every year, new systems are developed and introduced, old systems are extended, modified, integrated with each other, and retired. These changes are the result of many different stakeholders' requirements and many developers' actions and not of a grand master plan.
The CISO, however, has realized that it is difficult to do a good (quantitative) risk analysis of the company IT infrastructure without knowing what systems they have, how these depend on each other, what data that is flowing, what roles that have access to different parts, what network technologies that are being used et cetera.
The Chief Executive Officer (CEO) and the board of directors have during the last years experienced that it has been hard to make good decisions based on the qualitative and ad-hoc risk analyses they get. Also, the pressure from new laws, increasing digitization, and an increasing number of malicious attack attempts have made them prioritize these questions.
And this is where you as the chief security architect come in. You are assigned to do a more thorough risk analysis, one that is quantitative and data-driven, that reflects the business, the IT environment, and the current threats, so that the CISO and people responsible for making strategic decisions have an up-to-date understanding of the current situation. The risk analysis should be created in order to support the CISO.

The Main Assignment

Individual work

Mandatory

(*For the assignment, the first thing you need to do is decide what enterprise you have been hired at - this is up to you to decide. A good strategy could be to choose an organization you are already comfortable with, maybe you have work experience you can have use of, or an organizational type that you want to learn more about and thus have a motivation to dig deeper into. Another suggestion is to choose a known cyber attack incident and read up on it as has been publicly reported and from this material deduct and make additional assumptions about this organization. Then you would also have a very specific attack to study as astrating point. E.g., what happened at the U.S. Democratic National Committee in 2016, in Natanz around 2010, at the central bank of Bangladesh in 2016, or at Capital One in 2019?*)
You know that threat modeling is appropriate to assess the security level of the enterprise and its applications. Further, it allows identifying weaknesses within the architecture. With this approach you can visualize and concretize what the risks are and how these could be mitigated.
Fortunately, you have heard about a method called CySeraf that that seems to fit your needs perfectly.
As the **main delivery**, the CISO is expecting a report consisting of five main parts;
0) scope & delimitations,
1) business analysis,
2) system definition & decomposition,
3) threat analysis,

4) attack & resilience analysis, and
5) risk assessment & recommendations.
You are free to use any tools you like to support the work in the different phases of the assignment.
Using graphical models, tables, and such can solve many steps. However, these can't stand by themselves, but need to be complemented with text explaining the figures and your analysis. Furthermore, you are creating a report, and as such, some text is likely needed to guide the reader throughout the report, i.e. understandability is important, thus it must neither be too big and complicated nor to small and trivial.

Assignment assessment and grading criteria

The assignment will be evaluated according to the criteria listed in the grading section. (*This means that understanding these criteria a soon as possible is essential for succeeding with the assignment. As your work progresses, carefully cross-examine your work with respect to the criteria*.)
Mapping to intended learning outcomes

Phase 1: Business value of system

- Loss events (breach impact) based on business architecture (use cases) and business goals
Model threats in large-scale computer systems

Phase 2: System definition and decomposition

- Data flow diagrams based on system assets, actors, accounts, and authorization
Model threats in large-scale computer systems

Phase 3: Threat analysis

- Abuse cases based on attacker profiles
Simulate attacks in large-scale computer systems

Phase 4: Attack and resilience analysis

- Attack trees based on vulnerabilities
Simulate attacks in large-scale computer systems / Describe which defense mechanisms computer system can have

Phase 5: Risk assessment and recommendations

Carry out risk analysis based on a model and simulation / Describe which defense mechanisms computer system can have

Grading

To pass the course (E) you need to pass the project assignment (6.0 credits) and the seminar series (1.5 credits), this includes:

- Passing the project report (evaluated based on properties listed below), A-F
- Pass the oral presentation, P/F
- Attend the guest lectures, P/F
- Hand in peer-review learning reports, P/F

The project report will be the main source of evaluation and it will be assessed based on a set of properties, namely; consistency, correctness, coverage, variance, (technical) detail, realism & motivation, and balance/assurance. These are described and exemplified in the table below.
Moreover, the report must be well-structured, understandable and readable. E.g. it must be free of spelling errors, inconsistent or incomprehensible sentences, and grammatical errors. It must have reasonable size of paragraphs and sentences. It must use numbered headings and it must be easy to follow all internal references in the report. It must use figure/table

text and reference figures/tables in text (e.g. figure text description: “Figure 1. A business model”. In text: ”In Figure 1 the business model is described”).
Finally, the **report must be handed in on time**.

Property	Evaluation criterion	Comment and examples
Consistency	The models follow a single and structured underlying framework(metamodel), preferably the one presented in the course. And the terminology is used correct and consistently.	E.g. are multiplicities followed and are phenomena modeled according to the logic of the language? E.g. "threat," "risk," and "vulnerability" should mean different things (unless something else is explicitly stated).
	The models are consistent within eachphase (sub model) and between one another (across the phases).	E.g. are the same assets modelled in the various DFDs? Are the vulnerabilities discussed relate to the assets in the system architecture, the attack vectors/trees relate to the identified vulnerabilities and the assets, etc. It must be possible to follow/track/relate all model elements to one another. Everything needs to be consistent. The consistency should be demonstrated (or rather the report should not leave places where the consistency can be doubted or questioned).
Correctness	The risk calculations, conclusions, and other syntheses are made correctly.	The fusion of parameters should follow the described method or otherwise make sense/be motivated. E.g. it doesn’t make sense to sum the attacker capability with a vulnerability score. And the calculations must match the developed models.
Coverage	The models are covering some well-defined problem domain in a reasonably complete way.	E.g. for attack models - apparent attack vectors should not be missing, for system models - key components should not be missing, for business goals - obvious losses should not bemissing. Unless these parts are explicitly stated as delimitations, then it could be ok with lesscoverage.
		The chosen framework is fully covered.
		Is the chosen resolution appropriate?
Variance	The models cover a variety of phenomena.	Not all models/analyses should follow the same underlying logic. Say three web servers with very similar vulnerabilities. One should demonstrate ability to analyze a wide variety of security topics. Different types of web vulnerabilities, but even better also network vulnerabilities and others.
(Technical) detail	The models should be on such a depth so that they are not trivial or superficial. Also, it should be clear what the technical challenges / implementations/ weaknesses / attacks are.	E.g. a non-technical attack vector is DoS web server <- deploy botnet <- buy botnet. Remedy: buy load balancer.
Realism and motivation	The model input data is realistic. Some things are straight forward and not questionable while other assumptions and interpretations motivation and external references are needed to back up the claims of the models.	In principle there are two ways of motivating non-questionable claims, either (trustworthy) references are put forward as support or you put forward your own argumentation that is convincing the reader about the realism. This can relate to anything from costs of loss to common system architecture solutions and technology stacks, to threat profiles and attack vectors.
		Strong references, and use of, external sources. E.g. we have analyzed some certain MITREATT&CK techniques, or some vulnerability class. E.g. the use of threat emulation profiles.
		For the threat analysis there are many parameters that is qualitatively assessed (e.g. prob. of action). For these assessments some form of reasoning / motivation is needed.
		Motivating why you are not diving deeper into something is a good thing. E.g. we consider TLS 1.3 secure, because ...
Balance/assurance	The confidence of the recommendation analysis and conclusions are declared and discussed.	E.g. this relates to making probabilistic risk calculations, but also the intermediary focus of the threat modeling per se. E.g. it is decided to focus on a certain abuse case or vulnerability. How sure are we that this focus/delimitation is the correct one? Balance the level of detail so that not one part/aspect of the models get a lot of attention and others little unless this difference in importance is clearly motivated. This criteria also relates to the remaining uncertainty after the realism has been motivated.

All seven properties will be assessed and all must pass a minimum bar. If one criterion is assessed and considered as failed the grade Fx will be used in order for you to re-do that part to pass the course.
Each of the eight criteria will be evaluated using a scale of Fail (-1), Sufficient/Pass (0), Good (1), Very good (2), and Excellent (3). Thus, a maximum of 24 points can be gathered. Grades will be set based on the following schema:
A = 20-24
B = 15-19
C = 10-14
D = 5-9
E = 0-4

First iteration drafts for peer-review

Individual work
Mandatory
Description
Before delivering the final report the CISO would like to feel confident that you are on the right track and have thus asked you deliver a few drafts. This enables the CISO to guide you in the right direction for the final report (on which both your future careers depend). Moreover, to really ensure the quality of the work the CISO has ordered a few of your colleagues in the security group to review it (peer-reviewing).
The main goal with this assignment is to familiarize yourself with the threat modeling method used and what kind of challenges each phases of it include, as well as the company you are modeling. You need to collect some general material or other experiences and conjecture how the chosen type of company typically works.

There will be three short iterations with one draft handed in and peer-reviewing for each. These are synchronized with the phases of the CySeraf. That is:
Draft submission 1: Scoping (phase 0), business impact (phase 1), and system definition and decomposition (phase 2).
Draft submission 2: Threat analysis (phase 3) and Attack and resilience analysis (phase 4).
Draft submission 3: Risk assessment and recommendations (phase 5).

The initial drafts does not have to be large or complex but comprehensive enough to show your general direction, it will mainly consist of models, figures, lists, et cetera and not complete text (but some supporting text where needed). But of course, better drafts usually means more relevant feedback. As you will continue working on the drafts, its quality will not impact your final grade. These submissions are for the purpose of directing your continued work.

Each person will peer-review other peoples drafts for each phase.
After each peer-review round you need to write a short 4-7 sentence "This is what I learned during the peer-review process"-report and hand in.

The pedagogical idea with having the drafts and peer-reviews early in the course with a rather tight time schedule is twofold: 1) We want you to get a flying start by thinking and

reading about all the phases early on. You learn a lot going through a full iteration of the method. 2) We want you to have plenty of time left for the second iteration to complete the project assignment. Thus being able to implement all the the things you have learned from the first drafts and peer-reviews (and all the other activities in the course).

Evaluation Criteria
The drafts and peer-reviews are **mandatory** and graded **Pass/Fail**.

Everyone must hand in their drafts on Canvas.
Then either

- you read the two reports assigned to you and provide written feedback on each of the two reports

or

- you attend the peer-review seminar and provide oral feedback live during the seminar. For those attending the peer-review seminar you don't have to read the, in Canvas assigned, reports (these will most likely be different then the ones you review in the seminar). Instead you will get the chance to read drafts during the seminar, listen to others presenting their drafts, and provide feedback during the seminar.

Everyone needs to write the short 4-7 sentence "This is what I learned during the peer-review process"-report and hand in.

Final Presentations

To be performed individually
Mandatory
Description
One of the key success factors for a long-lived threat modeling initiative is that it is supported by senior management as well as by the operative staff at the business units and the people in the IT organization. One of the most important assignments for chief security architects is to communicate and explain the purpose of threat modeling as well as the ongoing and future work within the area. Your assignment is to hold a 10-minute executive presentation about the current threat and risk status, as well as your proposed mitigations, for the employees of the enterprise (i.e. the course participants) as well as the CISO and the CEO (the teachers). This presentation will serve as the beginning of an era of more structured and efficient cyber security risk management at the enterprise.
It is important that the audience after the presentation has understood the following:

- Background information, explaining the need for the presented work. (This is an important thing to communicate and synchronize within enterprises; a common goal!)
- How the business works, and your business impact analysis.
- What is the IT support offered to the business or, vice versa, how dependent on IT are the various parts of the business? What does the system architecture look like.
- What are the most important threats and attack profiles you worry about at your enterprise?
- What kind vulnerabilities did you find and what type of attacks did that enable?
- What does your risk analysis result in?

- Which mitigations do you suggest based on the risk analysis? Explain your reasoning.

Focus on the particulars of your case and company and not too much on the underlying methodology. The employees of the company are more interested in the results and what to do rather than exactly how you got there (especially the parts that are the same for others doing similar work).

Note! The presentation must be prepared so that it can be **given in English**. If only Swedish-speaking people are present at the presentation seminar, Swedish is also OK.

Evaluation Criteria

The oral presentation is **mandatory**. The presentation is **Pass/Fail** graded. The presentations will be evaluated on the communicative performance, i.e. on the extent to which the contributions are correctly and efficiently communicated to the audience. This will typically be affected by the structure and form of the presentation and slides, the clarity of the argumentation, the presenter's oral performance, the timeliness of the presentation, and on the responses to questions posed by the audience.

Flipped classroom

Flipped Classroom describes a concept where the lecture time is not used to present the content that the students should be aware of, but to discuss the content and solve open questions.

The basic concept follows the scheme that the students are provided with material that they have to go through until a certain date. At this date, there will be a lecture where the students can ask questions related to the material. To guarantee that the questions can be answered, we ask the students to provide the questions by 18:00 the day before the lecture. For those questions, we guarantee that they will be answered during the lecture. Other questions can be asked during the lecture as well, but it might be that we will answer them afterwards. If there are no further questions, we are going to end the lecture even if there is still time left.

The flipped classroom concept will be used for all activities listed in the schedule as Q&A sessions.

An exemplary time schedule:

Day X - N	We release a list of material and videos that should be studied by the students.
Day X – 1 18:00	The students have watched the videos and studied the material. On Canvas, the students write a list of questions that they want to have answered during the lecture the next day.
Day X	The lecture starts (Zoom) and the in-time on Canvas listed questions are discussed. Further questions are answered if possible. The lecture ends when all questions are answered and no additional are brought up.

Guest lectures

Individual

Mandatory

Description

Since it is hard to know everything and keep the motivation in a large project the CISO has ordered you to participate in lectures given by experts in the area.

w46	Friday	2020-11-13	10:15-12:00	Guest lecture	Digital	Jesper Kråkhede, cyber security architect at Microsoft
w47	Thursday	2020-11-19	18:00 (sharp, no academic 15 min.)	Guest lecture	Digital	Adam Shostack, Author of Threat Modeling: Designing for Security
w48	Friday	2020-11-27	10:15-12:00	Guest lecture	Digital	Olle Segerdahl, principal security consultant at F-Secure
w49	Friday	2020-12-04	10:15-12:00	Guest lecture	Digital	Georgios Kryparos, head of security at Tink
w50	Monday	2020-12-07	10:15-12:00	Guest lecture	Digital	Niklas Wiberg, senior cyber security architect at Scania

This part is graded Pass/Fail. If you miss a guest lecture there will be an extra assignment making up for it. Depending on which lecture you miss there will be an academic paper or similar to read and write a two-page reflection on. This needs to be handed in and passed before course credits for the seminar series is approved.

Course material

This page introduces the course material and serves as a guidance for students to help navigate through the course. It should however be noted that there are several sources under the “other material” heading that are not consistent with the threat modelling approach adopted in the course. Hence, all material must be approached with an active and critical mind, and please do not read/look at all material from A to Z! If you find more material that you feel is worthy, please share by a post to the whole course so that we can update this repository.

Background

The main goal of the course is to teach different methods for analysing threats, risks, and defences of large-scale computer systems. You will be required to put the gained theoretical knowledge from lectures into practice in an individual project. The project assignment is about assessing the cyber security risks of a large-scale IT system using the CySeraf threat modelling method and to identify possible mitigations. The assignment description is intentionally designed not to provide all the necessary information to encourage critical thinking.

The CySeraf method consists of the following phases:

0. Scope and Delimitations
1. Business Analysis
2. System Definition and Decomposition
3. Threat Analysis
4. Attack and Resilience Analysis
5. Risk Assessment and Recommendations

The main course material consists of lecture slides, recorded presentation videos, and a number of additional videos describing each of the examples mentioned during the lectures. Furthermore, in order to help you navigate your way through the assignment and provide some background where necessary, we have aggregated a list of additional external sources under the “other material” heading. The course material is listed and divided among different phases to help you perform the specific tasks for that particular phase as well as to provide a widened perspective and technical depth on the course topic.

You are free to follow the course material in any order you wish. However, we recommend you to follow the phase wise order and read/watch the mentioned material before you perform the tasks for the particular phase of the assignment.

Preliminaries

A recorded video and accompanying slides introducing the topic of risk analysis with threat modeling are found here (Links to an external site.). Overview diagrams of the CySeraf approach are found here (Links to an external site.).
The threat modeling language follows the structure of conceptual modeling with class and object diagrams, for instance found in the Unified Modeling Language (UML). In brief, class models constitute a modeling language (aka meta model) and object diagrams are instance representations of some piece of the real world and follow the class model/language rules. If you are not familiar with conceptual modeling, UML object and class diagrams are described in the below videos (A note: UML is primarily used for software design meaning that it is designed to support code generation. In conceptual modeling this is not the case so not all of UML is relevant for conceptual modeling and often the examples found in UML material can feel a bit off. In these videos you e.g. have to think of the "frogger game" as the real world you want to model.)

- Object diagrams: UML Class Diagrams - Object Diagrams (Links to an external site.)
- Class diagram, part 1: UML Class Diagrams - Simple Class Diagram (Links to an external site.)
- Class diagram, part 2: UML Class Diagrams - Complex Example (Links to an external site.)

Phase 0 - Scope and Delimitations

Theory:

- The lecture slides and recorded videos can be found here (Links to an external site.).

Example:

- Example models shown during the lectures and their explanation videos can be found here (Links to an external site.).

Other material:

- A good article that explains different categories of information systems which can help you to structure your IT landscape and identify the important components is found here (Links to an external site.).

Phase 1 - Business Analysis

Theory:

- The lecture slides and recorded videos can be found here (Links to an external site.).

Example:

- Example models shown during the lectures and their explanation videos can be found here (Links to an external site.).

Other material:

- An article about business analysis canvas, which is often used to grasp the entire organization from a business centric point of view can be found here (Links to an external site.)
- CATWOE (Links to an external site.) inter alia looks at what a company wants to achieve, and which solutions can influence the stakeholders
- A short youtube video explaining CATWOE:What is CATWOE? (Links to an external site.)

Phase 2 - System Definition and Decomposition

Theory:

- The lecture slides and recorded videos can be found here (Links to an external site.).

Example:

- Example models shown during the lectures and their explanation videos can be found here (Links to an external site.).

Other material:

- In Phase 2, you will create a detailed technical specification of the considered system. Data flow diagrams (DFDs) are to be used to describe the system architecture. To know more about DFDs, you can use the link here (Links to an external site.).
- To help in identifying different system components one could take some inspiration from how stakeholders are identified in project management as mentioned here. (Links to an external site.)The ITIL (Links to an external site.) framework and its CMDB could also serve as information input for the existing system components in your organization.
- Two general tools for data modelling and writing diagrams, charts and data flows (similar to Visio): http://draw.io (Links to an external site.) and https://www.lucidchart.com (Links to an external site.). (Links to an external site.)
- Microsoft's threat modeling tool (Links to an external site.) (not maintained)
- Another tool for writing data flow diagrams is Threat Dragon (Links to an external site.).

It is beneficial to understand and review a number of key concepts around ICT systems and their security before you create DFDs.

ICT System Components

Various types of Information and Communication Technology (ICT) components like Database, Network, Cloud, Operating Systems, Identity and Access Management are used in an enterprise. Short introduction and link to some reading materials related to ICT components are provided in this section for interested candidates. Some standard books are also referred; if someone from non-IT background wants to go deeper in those topics, the books are available in KTH Library.

Database

Data has become the most valuable asset for a modern business concern. Safety and security of customer data, intellectual property data, log data, etc are of foremost importance for an enterprise. Databases are used to store data in a structured way for easy update and retrieval. Databases can be of different types like, hierarchical, relational, NoSQL, etc. To manage databases different database management systems are created like MySQL, Oracle, PostgreSQL, MongoDB, etc.

To learn more on databases and database management systems one can look into the following resources:-Database programming tutorial: What are databases? | lynda.com (Links to an external site.) Relational Database Concepts (Links to an external site.)

Text:

Fundamentals of database systems - Ramez Elmasri, Shamkant B. Navathe

Database System Concepts - Abraham Silberschatz, Henry F. Korth, S. Sudarshan

Network

Connectivity is important for doing business and most of the IT or ITES businesses provide their solutions to the customer via internet. Knowing about the computer network and its components is a must for a security researcher who wants to secure an enterprise.
To learn more about network and its components following resources can be useful:-
Computer Networks: Crash Course Computer Science #28 (Links to an external site.)
Text:
Computer Networking: A Top-Down Approach - by James Kurose, Keith Ross

OS

Operating system running in on a computer provides a software interface of the physical machine to a user. Modern-day operating systems are highly configurable and have many user-friendly features. Addition of many features makes these systems complex and hard to manage. Securing these complex collection of software modules, known as the operating system is a highly complicated task.
To start learning about operating systems one can follow the following resources:-
Operating Systems 1 - Introduction (Links to an external site.) Text:
Operating System Concepts - by A. Silberschatz, P.B. Galvin and G. Gagne
Modern Operating Systems - by Andrew S. Tanenbaum

Identity and Access Management (IAM)

Business concerns implement identity and access management to provide security to their data, processes, and other assets. Identity management or access management ensure that only a subject with proper authorization on an object should get access to that object. For a huge enterprise, this management becomes a daunting task.
To know more on identity and access management one can start with the following links:-
Identity Management 101: Unwrapping Identity Management (Links to an external site.) Identity and Access Management: Technical Overview (Links to an external site.)

Cloud

In today's time it would be a tedious job for an enterprise to maintain all the hardware, software, data, security, etc. There is one solution to get rid of these managerial hassles, it is to use the services provided by some third-party cloud provider. These third-party providers will maintain the infrastructure, platform, or software and also look after their security requirements.
For an introduction to cloud computing following one can follow the resources given below:-
Cloud Computing In 6 Minutes | What Is Cloud Computing? | Cloud Computing Explained | Simplilearn (Links to an external site.)

Security topics

To protect their assets against attacks, organizations often deploy a number of security services and functions in their system. It is thus valuable to grasp some of these key security concepts and decide accordingly whether the organization you are modelling makes use of any of these techniques and functions. You can either follow the playlist here (Links to an external site.)or watch the individual videos below:-
Anti-MalwareAnti-Malware Tools - CompTIA A+ 220-1002 - 2.4 (Links to an external site.)
IDS/IPS
Network Intrusion Detection and Prevention - CompTIA Security+ SY0-501 - 2.1 (Links to an external site.)
Firewalls

Firewalls - CompTIA Security+ SY0-501 - 2.1 (Links to an external site.)
Logging Capturing Network Traffic and Logs - CompTIA Security+ SY0-401: 2.4 (Links to an external site.)
Encryption Vulnerability Scanning - CompTIA Network+ N10-006 - 3.1 (Links to an external site.)
Honey pots An Overview of Honeypots - CompTIA Network+ N10-005: 5.6 (Links to an external site.)

Phase 3 - Threat Analysis

Theory:

- The lecture slides and recorded videos can be found here (Links to an external site.).

Example:

- Example models shown during the lectures and their explanation videos can be found here (Links to an external site.).

Other material:

This phase deals with an assessment of the threats that your system might be exposed to. This includes identifying possible attackers and developing different attacker profiles and abuse cases to calculate contact frequency, probability of action, and the threat event probability.

- To know more about the known hacker groups that might attack you, please check https://attack.mitre.org/groups/ (Links to an external site.) and the resource maintained by the homeland security in the US (https://www.us-cert.gov (Links to an external site.)). MITRE ATT&CK framework is described in the following video:-What Is MITRE ATT&CK? Part 1 - Basic Terminology (Links to an external site.)
- Another useful document that describes a way to create organization specific threat profiles is here. (Links to an external site.)
- Structured Threat Information Expression (STIX (Links to an external site.)) is an open language for describing attacker and attacker campaigns. It is quite close to languages for Threat modelling but with a slightly different focus.

Phase 4 - Attack and Resilience Analysis

Theory:

- The lecture slides and recorded videos can be found here (Links to an external site.).

Example:

- Example models shown during the lectures and their explanation videos can be found here (Links to an external site.).

Other material:

In this phase, you will be assessing your system for potential vulnerabilities to create a list and devising attack trees/graphs to visualize the abuse cases from the previous phase. To help you create a list of vulnerabilities and know more about different security requirements of a system, vulnerabilities, attack patterns, or penetration testing, you can follow the links below.

- To maintain information security, one needs to protect the confidentiality, integrity, and availability of a system and data. You can watch a small video explaining these three terms:-Confidentiality, Integrity, and Availability of Computer Security (Links to an external site.)

- There are related interesting topics in security like authentication, authorization. It is recommended to know about their differences. Interested students can search for other security aspects or security requirements. Authentication vs Authorization (Links to an external site.)
- IT-systems used for personal or corporate uses have different vulnerabilities in them. Coding errors, misconfiguration of devices, etc. are a few of the various causes from which these vulnerabilities are introduced. Different tools are available to analyse the vulnerabilities of a system viz. NMAP, Nessus, Nexpose. You can follow the video below to get an introduction to the vulnerability analysis. Vulnerability Scanning (Links to an external site.)
- These vulnerabilities are exploited by attackers to harm the system. To check the resilience of a system against an attacker, penetration testing can be done. Metasploit (Links to an external site.) framework is a well-known penetration testing tool.
- The vulnerabilities and/weaknesses found in different standard softwares are listed by some of the organizations for public use:- https://nvd.nist.gov/ (Links to an external site.), (Links to an external site.) (Links to an external site.)https://cve.mitre.org/ (Links to an external site.), https://www.cvedetails.com/ (Links to an external site.)and https://cwe.mitre.org/ (Links to an external site.).
- Vulnerabilities are often related to a level of criticality. Criticality scores for vulnerabilities are also maintained in the databases. Common vulnerability scoring system (CVSS) provides a procedure to compute vulnerability criticalities. Some related links to vulnerabilities and their criticalities are https://infosec-handbook.eu/blog/cvss-cve-cwe-capec/ (Links to an external site.), (Links to an external site.)https://www.first.org/cvss/, (Links to an external site.)https://kb.cert.org/ (Links to an external site.) (Links to an external site.)
- In real world, attacks on information security follow some common patterns. MITRE ATT&CK (Links to an external site.), CAPEC (Links to an external site.) are some of the initiatives taken to organize the common patterns of attack for security research.
- Exploiting a vulnerability (or executing an attack) opens up possibility of executing other attacks to a hacker. It is common to see examples of multi-hop attacks in real life hacking scenarios. The dependency of an attack on one or more other previous attacks can be formalised by using attack trees or attack graphs. For some background on attack trees, please follow the following link for Schneier's original article on attack trees here (Links to an external site.) and a thesis describing a way to create attack trees here (Links to an external site.).
- OWASP Cheat Sheets on security related to web application development. Very useful for technical threat modeling: https://cheatsheetseries.owasp.org/cheatsheets/Web_Service_Security_Cheat_Sheet.html (Links to an external site.)

Phase 5 - Risk Assessment and Recommendations

Theory:

- The lecture slides and recorded videos can be found here (Links to an external site.).

Example:

- Example models shown during the lectures and their explanation videos can be found here (Links to an external site.).

Other material:

In this phase, you will be performing the overall risk assessment of the system you considered and suggest possible course of actions to reduce the risk and improve the security.

- An article on risk impact assessment and prioritization is linked here (Links to an external site.).
- An article (Links to an external site.) on risk management at DoD

More related material

- A collection and summary of different threat modelling approaches: https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html (Links to an external site.)
- Hybrid TMM: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2018_004_001_516627.pdf (Links to an external site.)
- Summarization of Threat Modelling Mindset: https://roberthurlbut.com/r/BSC2017TM (Links to an external site.)
- Other books:
- Securing Systems: Applied Security Architecture and Threat Models ISBN: 978-1482233971
- Threat Modeling: Designing for Security ISBN: 978-1118809990

PASTA method

- PASTA ebook (via KTH library): Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysishttps://learning.oreilly.com/library/view/risk-centric-threat/9780470500965/c08.xhtml#c8 (Links to an external site.)
- Presentation of PASTA: Process for Attack Simulation and Threat Analysis (PASTA) Risk Centric Threat Models (Links to an external site.)
- Another PASTA presentation (Links to an external site.) with examples.

Notes on CySeraf relation to PASTA

CySeraf Phase 1 relations:

- Stage 1, Activity 1 -list of business requirements/use cases
- S1, A2 -list how assets need to comply with rules and regulations. (An “inverse” loss, non-compliance lead to loss..)
- S1, A3 -describe the impact of confidentiality, integrity, and availability + compliance breaches per asset.
- S1, A4 -List People/process/technology vulnerabilities (inherent risk) -Quite unclear structure and purpose. Not really addressed in CySeraf.

CySeraf Phase 2 relations:

- Corresponds to stage 2 (Definition of Technical Scope) and stage 3 (Application Decomposition). Overall CySeraf and PASTA are well aligned here.
- Step 1 -Listing data and functions corresponds to roughly to stage 2 activities 1, 3, 4, 5.
- Step 1 -Accounts and authorization corresponds roughly to stage 2 activity 2 and stage 3 activity 1.
- Step 2 -Corresponds to stage 3 activities 2 and 3.

CySeraf Phase 3 relations:

- Step 1 -corresponds roughly to stage 4 activities 1, 2, 3, 6. (Stage 4 activity 4 is not considered in CySeraf since it is more related to vulnerabilities and system. Phase 3 focus is on the attackers.)
- Step 2 -corresponds roughly to stage 4 activity 5 and partly stage 5 activity 3.

CySeraf Phase 4 relations:

- Step 1 -Corresponds roughly to stage 5 activity 1 and 2.
- Step 2 -Corresponds roughly to stage 5 activity 3 and stage 6 activities 1, 3, and 4 (However in 4 impact is not assigned in phase 1).
- S5;A4 -PASTA wants to make a risk weighted scoring. This is wrong in relation to CySeraf (since this depends on attack aggregations (coming in Phase 5). Only local difficulty is what should be assigned.
- S5;A5 -Scanning and pentest. out of scope -unless ethical hacking is included.
- S6;A2 -Build your own attack library. -Don't (normally)! Use Attack libraries as source of inspiration rather than maintaining this yourself. S6;A5 -Counter measure testing is out of scope.
- S6;A6 –Pentest is out of scope (for this course).

CySeraf Phase 5 relations:

- S7;A1 -Calculate overall risk for base case. (This includes several abuse cases/threats that needs to be summarized).
- S7;A2 -Identify countermeasures. Component based and architecture based. (Removing vulnerabilities/weaknesses is a form of countermeasure. sometimes we explicitly give these countermeasures names a treat them as official countermeasure, e.g. patching, other times we just remove things, remove account.)
- S7;A3 -Devise a number of scenarios and calculate risk for them. (Defense effectiveness cannot be calculated in isolation, it depend on the attack vector. Thus defenses constitute different scenarios). Defenses are either architectural or component based.
- S7;A4 -The conclusion what is your recommendation in terms of future security development/implementation.

FAIR method

- FAIR ebook (via KTH library): Measuring and Managing Information Risk: A FAIR Approach https://learning.oreilly.com/library/view/measuring-and-managing/9780124202313/XHTML/contents.xhtml (Links to an external site.)
- FAIR overview ppt: https://cdn2.hubspot.net/hubfs/1616664/The%20FAIR%20Model_FINAL_Web%20Only.pdf (Links to an external site.)
- Open group risk taxonomy (Standardization of FAIR): https://www.opengroup.org/forum/security-forum-0/risk-management (Links to an external site.)

Notes on CySeraf relation to FAIR

Overall, the risk aggregation method in CySeraf largely follows the FAIR method. Biggest change are details around how system resilience is estimated, what FAIR labels "vulnerability" (since FAIR does not deploy attack trees/graphs). Primary and secondary loss have been merged, and frequencies have been replaced with probabilities.

Extra material

- A collection and summary of different threat modelling approaches: https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html (Links to an external site.)
- Hybrid TMM: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2018_004_001_516627.pdf (Links to an external site.)
- Summarization of Threat Modelling Mindset: https://roberthurlbut.com/r/BSC2017TM (Links to an external site.)
- Other books:

Securing Systems: Applied Security Architecture and Threat Models, ISBN: 978-1482233971

Threat Modeling: Designing for Security, ISBN: 978-1118809990