EITP20: Secure Systems Engineering - Reference Sheet

Karl Hallsby

Last Edited: January 24, 2020

Contents

List of Theorems

1 Threat Analysis

To perform any kind of threat analysis, the system's specification must be considered. The state of the system (new or existing) must also be considered.

- The specification of the system to be analyzed
  - If a completely new system is about to be built, there might not even exist a system specification and it needs to be created.
  - If the analysis is to done on an existing system, the first task is to read existing system specifications, source code and/or make interviews with people familiar with the system.
- The specification must not necessarily be very detailed but can be a high-level description of the system.

Defn 1 (Attack Goal)**.** An *attack goal* is a technology, process, or thing that an attacker would like to gain access to. These are the things we are trying to protect against or mitigate.

1.1 Attack Trees

Defn 2 (Attack Tree)**.** The Schneider *attack tree* method is a straight-forward and step-by-step type of attack analysis. However, it is quite basic, so it might not be the best method to perform this analysis.

The steps involved are:

1. The starting point is a *good* system description.
2. Next, Attack Goals are identified.
3. Attack Goals are then broken down to specific attacks to form a so-called attack tree. Identify different attack vectors for the same Attack Goal with several iterations.
4. Identify dependencies in the Attack Goals.
5. Once the attack tree is created, it is transferred to a table where scores on risks/costs can be added as well as more details.

In a Single Sign-On system (SSO), there any many different points of failure. These will be illustrated with a basic Attack Tree. Some Attack Goals for this system are:

1. Get access to all services provided by all entities in the system
   (a) Get access to all services provided to all users at the ID Provider
   (b) Get access to all services offered through an OIDC Client
   (c) Get access to all services offered at the Hosting Server
2. Get access to all services provided to a single user provided by the ID Provider
3. Get access to all services provided to single user at the OIDC Client
4. Get access to all services provided to a single user at the Hosting Service
5. Get access to all services provided to an OIDC Client at the Hosting Service

Now, we identify dependencies in the various Attack Goals.

- Attack Goal 1 depends on goals 2, 3, 4, and 5 being completed.
- Goal 1.1 depends on goal 2 being completed.
- Goal 1.2 depends on goal 3 being completed.
- Goal 1.3 depends on goals 4 and 5 being completed.
- Goal 5 depends on goal 4 being completed.

We can now break each of the smaller goals down into concrete attack vectors.

1. Access to all services provided to all entities in the system.
   1.1. Access to all services offered by the ID Provider to all users.
      1.1.1. Get KeyCloak admin rights.
         1.1.1.1. Successful phishing attack.
         1.1.1.2. Break administrator authentication.
      1.1.2. Root access on the KeyCloak server.
         1.1.2.1. Utilize an OS vulnerability
         1.1.2.2. Break server isolation (For example, Docker or VMs)
2. Access to all services provided to a single user by the ID Provider
   2.1. Successful end-user password phishing attack.

2.2. Take over the end-user's client device.
  2.2.1. Place malware on the client device.
  2.2.2. Successful network attack on the end-user's client device.
2.3. Break the end-user authentication mechanism.
  2.3.1. Break authentication algorithm. (Difficult, if not impossible)
  2.3.2. Find flaw in authentication protocol.
  2.3.3. Find flaw in authentication algorithm implementation on the client or on the server.

As this "tree" shows, the when accounting for attack vectors, it can become quite large. You should start with the obvious cases, and move onto the les obvious as you go. The most important thing while doing this is you should think like an attacker.

Remark. Depending on the information of the system available, a very detailed attack break-down might be possible or not. The tree can later be complemented when more implementation information is available

Remark. The attack tree is a useful tool, but is not a final or complete solution to a security analysis problem.

1.2 Example Application of Attack Trees

1.3 Microsoft STRIDE Analysis

1.4 MITRE TARA Analysis

A Complex Numbers

Complex numbers are numbers that have both a real part and an imaginary part.

$$z = a \pm bi \tag{A.1}$$

where

$$i = \sqrt{-1} \tag{A.2}$$

Remark (i vs. j for Imaginary Numbers). Complex numbers are generally denoted with either i or j. Since this is an appendix section, I will denote complex numbers with i, to make it more general. However, electrical engineering regularly makes use of j as the imaginary value. This is because alternating current i is already taken, so j is used as the imaginary value instad.

$$Ae^{-ix} = A\left[\cos\left(x\right) + i\sin\left(x\right)\right] \tag{A.3}$$

A.1 Complex Conjugates

If we have a complex number as shown below,

$$z = a \pm bi$$

then, the conjugate is denoted and calculated as shown below.

$$\overline{z} = a \mp bi \tag{A.4}$$

Defn A.1.1 (Complex Conjugate)**.** The conjugate of a complex number is called its *complex conjugate*. The complex conjugate of a complex number is the number with an equal real part and an imaginary part equal in magnitude but opposite in sign.

The complex conjugate can also be denoted with an asterisk ($*$). This is generally done for complex functions, rather than single variables.

$$z^* = \overline{z} \tag{A.5}$$

A.1.1 Complex Conjugates of Exponentials

$$\overline{e^z} = e^{\overline{z}} \tag{A.6}$$

$$\overline{\log(z)} = \log(\overline{z}) \tag{A.7}$$

A.1.2 Complex Conjugates of Sinusoids

Since sinusoids can be represented by complex exponentials, as shown in Appendix B.2, we could calculate their complex conjugate.

$$\begin{aligned} \overline{\cos(x)} &= \cos(x) \\ &= \frac{1}{2}\left(e^{ix} + e^{-ix}\right) \end{aligned} \tag{A.8}$$

$$\begin{aligned} \overline{\sin(x)} &= \sin(x) \\ &= \frac{1}{2i}\left(e^{ix} - e^{-ix}\right) \end{aligned} \tag{A.9}$$

B Trigonometry

B.1 Trigonometric Formulas

$$\sin(\alpha) + \sin(\beta) = 2\sin\left(\frac{\alpha+\beta}{2}\right)\cos\left(\frac{\alpha-\beta}{2}\right) \tag{B.1}$$

$$\cos(\theta)\sin(\theta) = \frac{1}{2}\sin(2\theta) \tag{B.2}$$

B.2 Euler Equivalents of Trigonometric Functions

$$e^{\pm j\alpha} = \cos(\alpha) \pm j\sin(\alpha) \tag{B.3}$$

$$\cos(x) = \frac{e^{jx} + e^{-jx}}{2} \tag{B.4}$$

$$\sin(x) = \frac{e^{jx} - e^{-jx}}{2j} \tag{B.5}$$

$$\sinh(x) = \frac{e^{x} - e^{-x}}{2} \tag{B.6}$$

$$\cosh(x) = \frac{e^{x} + e^{-x}}{2} \tag{B.7}$$

B.3 Angle Sum and Difference Identities

$$\sin(\alpha \pm \beta) = \sin(\alpha)\cos(\beta) \pm \cos(\alpha)\sin(\beta) \tag{B.8}$$

$$\cos(\alpha \pm \beta) = \cos(\alpha)\cos(\beta) \mp \sin(\alpha)\sin(\beta) \tag{B.9}$$

B.4 Double-Angle Formulae

$$\sin(2\alpha) = 2\sin(\alpha)\cos(\alpha) \tag{B.10}$$

$$\cos(2\alpha) = \cos^2(\alpha) - \sin^2(\alpha) \tag{B.11}$$

B.5 Half-Angle Formulae

$$\sin\left(\frac{\alpha}{2}\right) = \sqrt{\frac{1-\cos(\alpha)}{2}} \tag{B.12}$$

$$\cos\left(\frac{\alpha}{2}\right) = \sqrt{\frac{1+\cos(\alpha)}{2}} \tag{B.13}$$

B.6 Exponent Reduction Formulae

$$\sin^2(\alpha) = \frac{1-\cos(2\alpha)}{2} \tag{B.14}$$

$$\cos^2(\alpha) = \frac{1+\cos(2\alpha)}{2} \tag{B.15}$$

B.7 Product-to-Sum Identities

$$2\cos(\alpha)\cos(\beta) = \cos(\alpha-\beta) + \cos(\alpha+\beta) \tag{B.16}$$

$$2\sin(\alpha)\sin(\beta) = \cos(\alpha-\beta) - \cos(\alpha+\beta) \tag{B.17}$$

$$2\sin(\alpha)\cos(\beta) = \sin(\alpha+\beta) + \sin(\alpha-\beta) \tag{B.18}$$

$$2\cos(\alpha)\sin(\beta) = \sin(\alpha+\beta) - \sin(\alpha-\beta) \tag{B.19}$$

B.8 Sum-to-Product Identities

$$\sin(\alpha) \pm \sin(\beta) = 2\sin\left(\frac{\alpha \pm \beta}{2}\right)\cos\left(\frac{\alpha \mp \beta}{2}\right) \tag{B.20}$$

$$\cos(\alpha) + \cos(\beta) = 2\cos\left(\frac{\alpha + \beta}{2}\right)\cos\left(\frac{\alpha - \beta}{2}\right) \tag{B.21}$$

$$\cos(\alpha) - \cos(\beta) = -2\sin\left(\frac{\alpha + \beta}{2}\right)\sin\left(\frac{\alpha - \beta}{2}\right) \tag{B.22}$$

B.9 Pythagorean Theorem for Trig

$$\cos^2(\alpha) + \sin^2(\alpha) = 1^2 \tag{B.23}$$

B.10 Rectangular to Polar

$$a + jb = \sqrt{a^2 + b^2}e^{j\theta} = re^{j\theta} \tag{B.24}$$

$$\theta = \begin{cases} \arctan\left(\frac{b}{a}\right) & a > 0 \\ \pi - \arctan\left(\frac{b}{a}\right) & a < 0 \end{cases} \tag{B.25}$$

B.11 Polar to Rectangular

$$re^{j\theta} = r\cos(\theta) + jr\sin(\theta) \tag{B.26}$$

C Calculus

C.1 Fundamental Theorems of Calculus

Defn C.1.1 (First Fundamental Theorem of Calculus)**.** The *first fundamental theorem of calculus* states that, if f is continuous on the closed interval $[a, b]$ and F is the indefinite integral of f on $[a, b]$, then

$$\int_a^b f(x)\,dx = F(b) - F(a) \tag{C.1}$$

Defn C.1.2 (Second Fundamental Theorem of Calculus)**.** The *second fundamental theorem of calculus* holds for f a continuous function on an open interval I and a any point in I, and states that if F is defined by

$$F(x) = \int_a^x f(t)\,dt,$$

then

$$\begin{aligned} \frac{d}{dx}\int_a^x f(t)\,dt &= f(x) \\ F'(x) &= f(x) \end{aligned} \tag{C.2}$$

Defn C.1.3 (argmax)**.** The arguments to the *argmax* function are to be maximized by using their derivatives. You must take the derivative of the function, find critical points, then determine if that critical point is a global maxima. This is denoted as

$$\underset{x}{\operatorname{argmax}}$$

C.2 Rules of Calculus

C.2.1 Chain Rule

Defn C.2.1 (Chain Rule)**.** The *chain rule* is a way to differentiate a function that has 2 functions multiplied together.
If

$$f(x) = g(x) \cdot h(x)$$

then,

$$\begin{aligned} f'(x) &= g'(x) \cdot h(x) + g(x) \cdot h'(x) \\ \frac{df(x)}{dx} &= \frac{dg(x)}{dx} \cdot g(x) + g(x) \cdot \frac{dh(x)}{dx} \end{aligned} \tag{C.3}$$

D Laplace Transform

Defn D.0.1 (Laplace Transform)**.** The *Laplace transformation* operation is denoted as $\mathcal{L}\{x(t)\}$ and is defined as

$$X(s) = \int_{-\infty}^{\infty} x(t)e^{-st}dt \tag{D.1}$$