Computer Security - CheatSheet

IN BA5 - Martin Werner Licht

Notes by Ali EL AZDI

October 26th, 2025

CompSec Properties

- **Confidentiality**. prevention of unauthorized disclosure of information.
- **Integrity.** prevention of unauthorized modification of information.
- **Availability.** prevention of unauthorized denial of service or access to information and resources.
- **Authenticity.** assurance that entities (users, systems, or data) are genuine and can be verified as such.
- **Anonymity.** protection of an individual's identity from being disclosed or linked to specific actions or data.
- **Non-repudiation.** assurance that a party in a communication cannot deny the authenticity of their signature or the sending of a message.

The Adversary. malicious entity aiming at breaching the security policy and **will** choose the optimal way to use her ressources to mount an attack that violates the security properties.

Threat Model. describes the ressources available to the adversary and their capabilities *(has access to internet, but doesn't have access to the internal network of the company.)*

Threat. Who might attack which assets, using what resources, with what goal, how, and with what probability

Vulnerability. Specific weakness that could be exploited by adversaries with interest in a lot of different assets *(API is not protected, password appears in plain text...)*

Harm. The bad thing that could happen when the **threat** materializes. *(adversary steals the money, learns my password...)*

Security Policy

A high level description of the security properties that must hold in the system in relation to assets and principals

- **Assets (objects).** anything with value (data, files , memory) that needs to be protected
- **Principals (subjects).** people, computer programs, services

Confidentiality. authorized users may read a file
Integrity. authorized programs may write a file
Availability. authorized services can access a file

Security Mechanism. Technical mechanism used to ensure that the security policy is not violated by an adversary within the threat model, **we can only prepare for threats we're aware of**
(Policy. ensure messages cannot be read by anyone but the sender and the receiver, Mechanism. encrypt the message before sending)

Composition of Security Mechanisms

- **Defence in depth.** As long as one remains unbroken the Security Policy isn't broken) *(two-factor auth)*
- **Weakest Link.** if anyone fails the Security Policy is broken security questions in case of a lost password, no need to know the password but just the answer

Humans are also part of the mechanism and allow vulnerabilities like phishing attacks, bad use of passwords...)

To show a system is secure. (under a *specific* threat model)
Attacker - Just one way to violate **one** security property is enough (within the threat model).
Defender - No adversary strategy can violate the security policy.

Security Argument

Rigorous argument that the security mechanisms in place are indeed effective in maintaining the security policy subject to the assumptions of the Threat Model.

Piecewise Continuity & Differentiability
$f:[a,b]\to\mathbb{R}$ is *piecewise continuous* if there is a partition

$$a=a_0<a_1<\cdots<a_n=b$$

such that $\lim_{x\to a_i^-} f(x)$ and $\lim_{x\to a_i^+} f(x)$ exist (finite).
Similarly, f is *piecewise* C^1 if it is continuously differentiable on each open subinterval and the one-sided derivatives at boundaries exist.

Euler's Formulas

$$e^{x+iy}=e^x\big(\cos y+i\sin y\big),\ \sin x=\frac{e^{ix}-e^{-ix}}{2i},\ \cos x=\frac{e^{ix}+e^{-ix}}{2}.$$

Orthogonality (Sine/Cosine Products)
For $n,m\in\mathbb{N}_{\geq 1}$ and period $T>0$:

$$\frac{2}{T}\int_0^T \cos\Big(\tfrac{2\pi n}{T}x\Big)\cos\Big(\tfrac{2\pi m}{T}x\Big)\,dx=\begin{cases}1 & n=m,\\ 0 & n\neq m\end{cases}$$

(Same for $\sin\sin$, and $\cos\sin$ integrates to 0.)

Integration Over One Period
If f is T-periodic and piecewise continuous, then for any $a\in\mathbb{R}$:

$$\int_a^{a+T} f(x)\,dx=\int_0^T f(x)\,dx.$$

Dirichlet's Theorem (Pointwise Convergence)
Let $f:\mathbb{R}\to\mathbb{R}$ be T-periodic and piecewise C^1. Then, for all $x\in\mathbb{R}$,

$$Ff(x)=\lim_{t\to 0}\frac{f(x-t)+f(x+t)}{2}.$$

Real Fourier Series
For $f:\mathbb{R}\to\mathbb{R}$, T-periodic, piecewise C^1, the real Fourier series is

$$Ff(x)=\frac{a_0}{2}+\sum_{n=1}^{\infty}\Big[a_n\cos\big(\tfrac{2\pi n}{T}x\big)+b_n\sin\big(\tfrac{2\pi n}{T}x\big)\Big].$$

Fourier Coefficients:

$$a_n=\frac{2}{T}\int_0^T f(x)\cos\Big(\tfrac{2\pi n}{T}x\Big)\,dx,\quad b_n=\frac{2}{T}\int_0^T f(x)\sin\Big(\tfrac{2\pi n}{T}x\Big)\,dx,$$
$$a_0=\frac{2}{T}\int_0^T f(x)\,dx.$$

Parity: If f is even, $b_n=0$; if f is odd, $a_n=0$.

Term-by-Term Differentiation
If f is T-periodic, continuous, and piecewise C^1, then

$$\frac{d}{dx}\big[Ff(x)\big]=\sum_{n=1}^{\infty}\frac{2\pi n}{T}\big[-a_n\sin(\tfrac{2\pi n}{T}x)+b_n\cos(\tfrac{2\pi n}{T}x)\big]$$
$$=\lim_{t\to 0}\frac{f'(x-t)+f'(x+t)}{2}.$$

Term-by-Term Integration
If f is T-periodic, continuous, and piecewise C^1, then

$$\int Ff(x)\,dx=\sum_{n=1}^{\infty}\frac{T}{2n\pi}\left[a_n\sin\left(\tfrac{2\pi n}{T}x\right)-b_n\cos\left(\tfrac{2\pi n}{T}x\right)\right]+C$$
$$=\lim_{h\to 0}\frac{1}{2h}\int_{x-h}^{x+h}Ff(t)\,dt,$$

where C is the constant of integration.

Poisson on $[a,b]$

$$\begin{cases}-u''(x)=f(x),\\ u(a)=g_a,\quad u(b)=g_b,\end{cases}\qquad L=b-a$$

$$u^g(x)=\frac{g_b-g_a}{b-a}\,x\ +\ \frac{b\,g_a-a\,g_b}{b-a}.$$

$$f(x)=\sum_{n=1}^{\infty}b_n\,\sin\Big(\frac{n\pi x}{L}\Big),\quad b_n=\frac{2}{L}\int_0^L f(t)\,\sin\Big(\frac{n\pi t}{L}\Big)\,dt,$$

$$u^f(x)=\sum_{n=1}^{\infty}b_n\,\frac{L^2}{\pi^2\,n^2}\,\sin\Big(\frac{n\pi x}{L}\Big).$$

$$u(x)=u^g(x)+u^f(x)\quad\text{(superposition principle).}$$

Poisson with mass term on $\mathbb{R}$

$$-u''(x)+k^2\,u(x)=f(x),\quad \widehat{u}(\alpha)=\frac{\widehat{f}(\alpha)}{\alpha^2+k^2}.$$

$$g(x)=\sqrt{\frac{\pi}{2}}\frac{1}{k}\,e^{-k|x|},\quad \widehat{g}(\alpha)=\frac{1}{\alpha^2+k^2},$$
$$u(x)=(g*f)(x)=\frac{1}{2k}\int_{-\infty}^{\infty}f(y)\,e^{-k|\,x-y\,|}\,dy.$$

Complex Fourier Coefficient
Let $f:\mathbb{R}\to\mathbb{R}$ be T-periodic and piecewise continuous. The complex Fourier coefficients are:

$$c_n=\frac{1}{T}\int_0^T f(x)\,e^{-i\frac{2\pi}{T}nx}\,dx,\quad Ff(x)=\sum_{n=-\infty}^{\infty}c_n\,e^{i\frac{2\pi n}{T}x}.$$

For $\phi:\mathbb{R}\to\mathbb{C}$,

$$\int_a^b\phi(x)\,dx=\int_a^b\mathrm{Re}(\phi(x))\,dx+i\int_a^b\mathrm{Im}(\phi(x))\,dx.$$

Relation to (a_n,b_n)

$$c_n=\tfrac{1}{2}(a_n-i\,b_n),\ c_{-n}=\tfrac{1}{2}(a_n+i\,b_n),\ c_0=\tfrac{a_0}{2}.$$
$$a_n=c_n+c_{-n}\ a_0=2c_0\ b_n=\mathrm{Re}(c_{-n}-c_n)$$

Fourier Series on $[0,L]$
For $f:[0,L]\to\mathbb{R}$ (piecewise C^1):

$$F_cf(x)=\tfrac{\tilde{a}_0}{2}+\sum_{n=1}^{\infty}\tilde{a}_n\cos\Big(\tfrac{\pi n}{L}x\Big),\quad \tilde{a}_n=\frac{2}{L}\int_0^L f(x)\cos\Big(\tfrac{\pi n}{L}x\Big)\,dx.$$

$$F_sf(x)=\sum_{n=1}^{\infty}\tilde{b}_n\sin\Big(\tfrac{\pi n}{L}x\Big),\quad \tilde{b}_n=\frac{2}{L}\int_0^L f(x)\sin\Big(\tfrac{\pi n}{L}x\Big)\,dx.$$

Parseval's Identity (Periodic Case)
If f is T-periodic (piecewise C^1),

$$\frac{2}{T}\int_0^T f^2(x)\,dx=\frac{a_0^2}{2}+\sum_{n=1}^{\infty}(a_n^2+b_n^2)=2\sum_{n=-\infty}^{\infty}|c_n|^2.$$

Plancherel Theorem
Let $f\in L^2(\mathbb{R})$. Then its Fourier transform $\hat{f}$ is also in $L^2(\mathbb{R})$, and:

$$\int_{-\infty}^{\infty}|f(x)|^2\,dx=\int_{-\infty}^{\infty}|\hat{f}(\xi)|^2\,d\xi.$$

The Fourier Transform
If $f:\mathbb{R}\to\mathbb{R}$ with $\int_{-\infty}^{\infty}|f(x)|\,dx<\infty$, its (unitary) Fourier transform is

$$\widehat{f}(\alpha)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}f(x)\,e^{-i\,\alpha x}\,dx,$$

Inverse Transform
If $\varphi(\alpha)$ is similarly integrable,

$$\mathcal{F}^{-1}(\varphi)(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\varphi(\alpha)\,e^{\,i\,\alpha x}\,d\alpha.$$

Convolution Product
Let $f,g:\mathbb{R}\to\mathbb{R}$ such that $\int_{-\infty}^{+\infty}|f(x)|\,dx<+\infty$, $\int_{-\infty}^{+\infty}|g(x)|\,dx<+\infty$.

$$(f*g)(x)=\int_{-\infty}^{+\infty}f(x-t)\,g(t)\,dt=\int_{-\infty}^{+\infty}f(t)\,g(x-t)\,dt$$

Scaling
$\mathcal{F}\{f(ax)\}=\frac{1}{|a|}\hat{f}\big(\frac{\alpha}{a}\big)$

Shifting
$\mathcal{F}\{f(x-x_0)\}=e^{-i\alpha x_0}\,\hat{f}(\alpha)$

Modulation
$\mathcal{F}\{e^{i\omega_0 x}f(x)\}=\hat{f}(\alpha-\omega_0)$

Convolution
$\mathcal{F}[f*g](\alpha)=\sqrt{2\pi}\,\hat{f}(\alpha)\,\hat{g}(\alpha)$

Differentiation
$\mathcal{F}\Big\{\frac{d^n}{dx^n}f(x)\Big\}=(i\alpha)^n\hat{f}(\alpha)$

Integration
$\mathcal{F}\Big\{\int_{-\infty}^{x}f(\xi)\,d\xi\Big\}=\frac{1}{i\alpha}\,\hat{f}(\alpha),\ \alpha\neq 0$

Differentiation of Transform
$\mathcal{F}\big((-ix)^n f(x)\big)(\alpha)=\frac{\partial^n}{\partial\alpha^n}\hat{f}(\alpha)$

Multiplication
$\mathcal{F}\{f(x)\cdot g(x)\}=\sqrt{2\pi}\,(\mathcal{F}\{f(x)\}*\mathcal{F}\{g(x)\}$

Important Trigonometric Identities

$\sin(2x)=2\sin x\cos x,$
$\cos(2x)=2\cos^2x-1=1-2\sin^2x=\cos^2x-\sin^2x,$
$\cos(a\pm b)=\cos a\cos b\mp\sin a\sin b,$
$\sin(a\pm b)=\sin a\cos b\pm\cos a\sin b,$
$\cos a\cos b=\frac{1}{2}\big[\cos(a-b)+\cos(a+b)\big],$
$\sin a\sin b=\frac{1}{2}\big[\cos(a-b)-\cos(a+b)\big],$
$\sin a\cos b=\frac{1}{2}\big[\sin(a+b)+\sin(a-b)\big],$
$\cos a\sin b=\frac{1}{2}\big[\sin(a+b)-\sin(a-b)\big].$
$cos(n\pi)=(-1)^n$