SECURE
CODE
WARRIOR

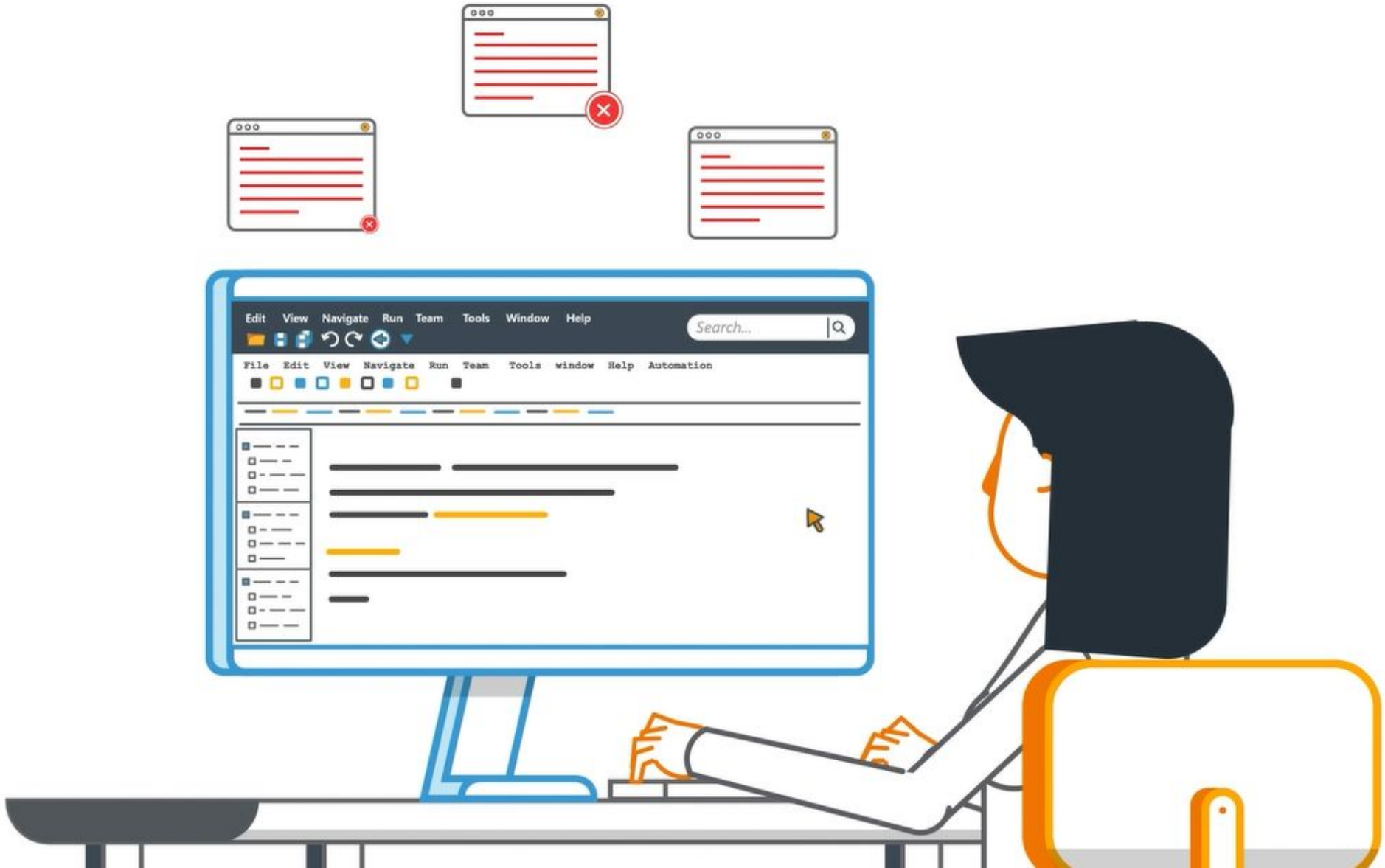
we'll be looking at

STRIDE Threat Modeling

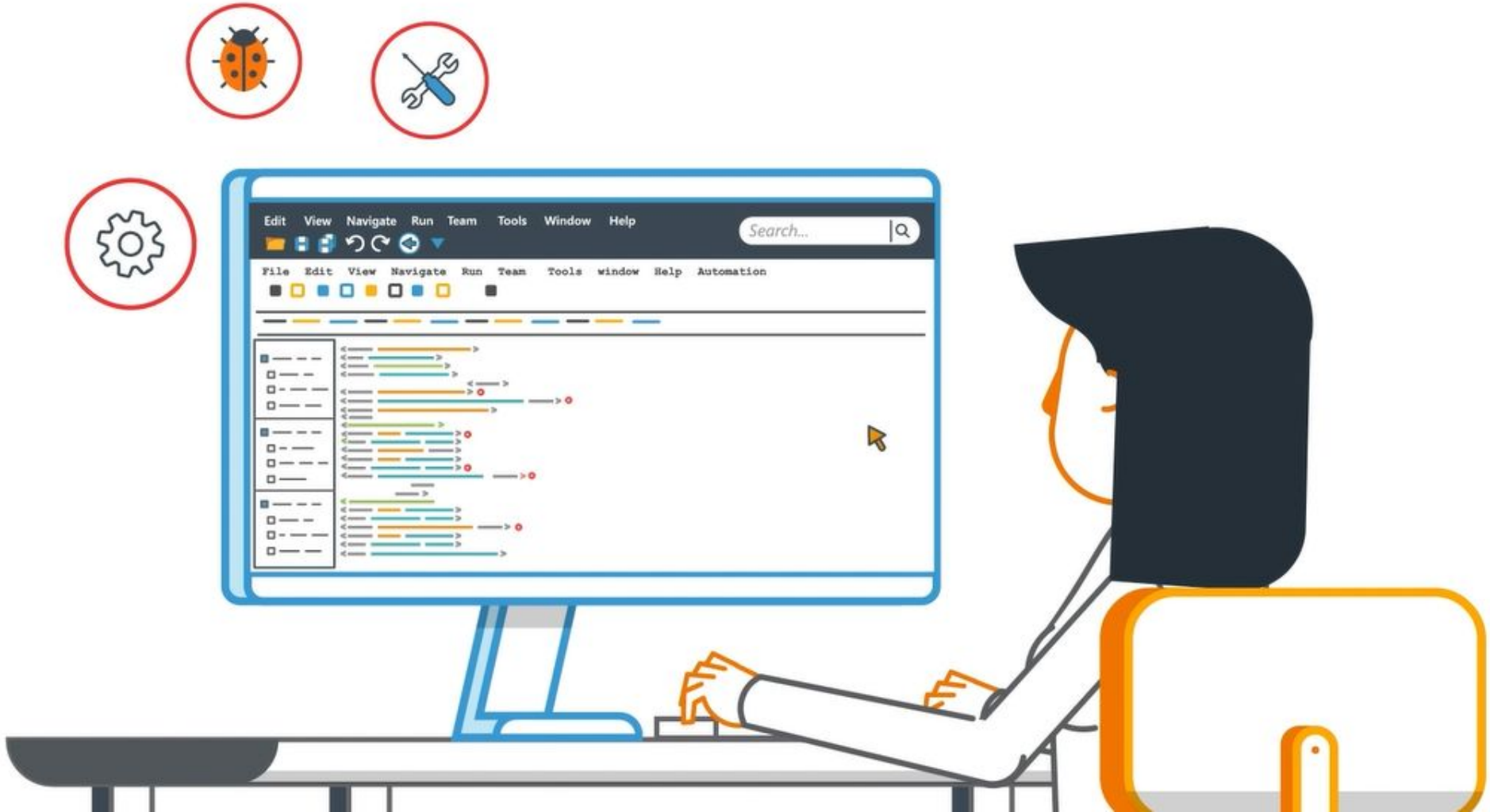
STRIDE is a threat modeling methodology that helps you

STRIDE

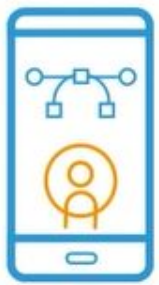
identify potential security issues in the app you're developing.



Developed by Microsoft, STRIDE is considered one of the most comprehensive ways to identify threats.



It's most commonly used by application designers, developers, testers and security experts.



APPLICATION DESIGNERS

DEVELOPERS

TESTERS

SECURITY EXPERTS

Each letter of STRIDE represents a category of security threat:

S T R I D E

Spoofing,Tampering,Repudiation

S T R I D E

SPOOFING

TAMPERING

REPUDIATION

Information disclosure, including privacy breaches and data leaks,Denial of service and Elevation of privilege.

S T R I D E

SPOOFING

TAMPERING

REPUDIATION

INFORMATION DISCLOSURE

DENIAL OF SERVICE

ELEVATION OF PRIVILEGE

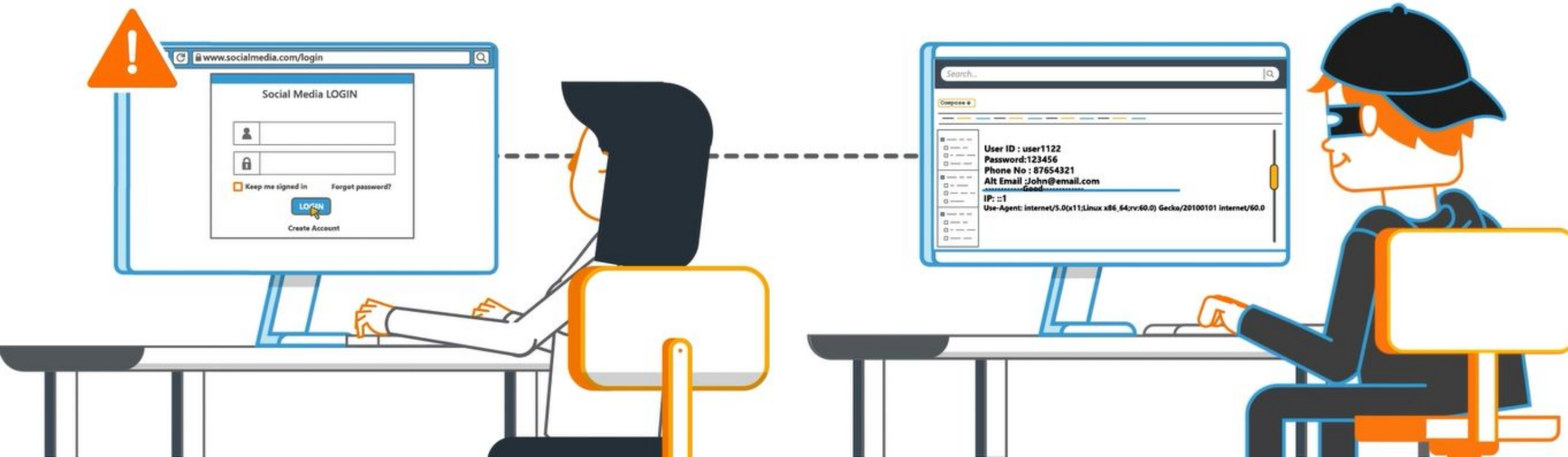
These six threats jeopardize the desired properties of an app or system:

THREAT	DESIRED PROPERTY
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

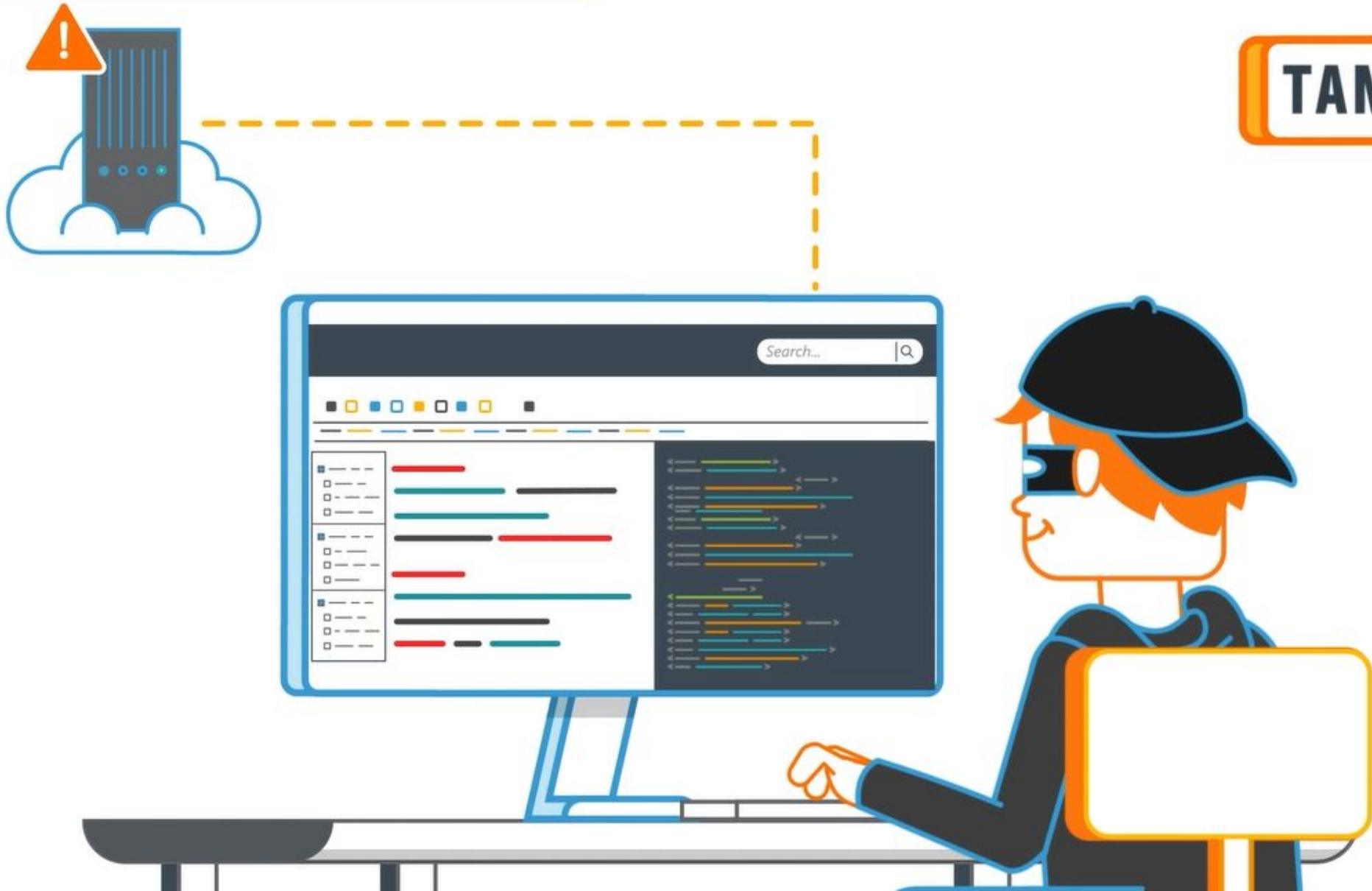
NOW LET'S LOOK AT ALL OF THESE IN MORE DETAIL...

Where Authentication is the ideal property, Spoofing is the impersonation of something or someone else.

SPOOFING



Where Integrity is the ideal property, Tampering happens when attackers modify data or code.



TAMPERING

Where Non-repudiation is the ideal property, Repudiation occurs when someone claims not to have performed an action.

REPUDTATION

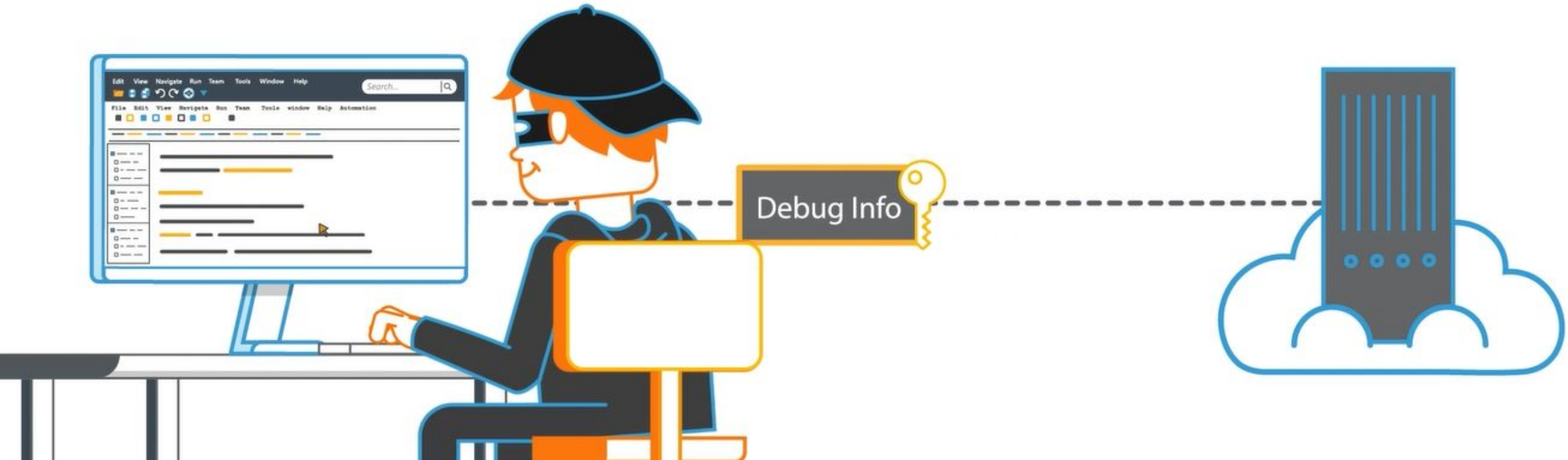
I never requested to transfer $1000 to B

PERSON-A

BANK

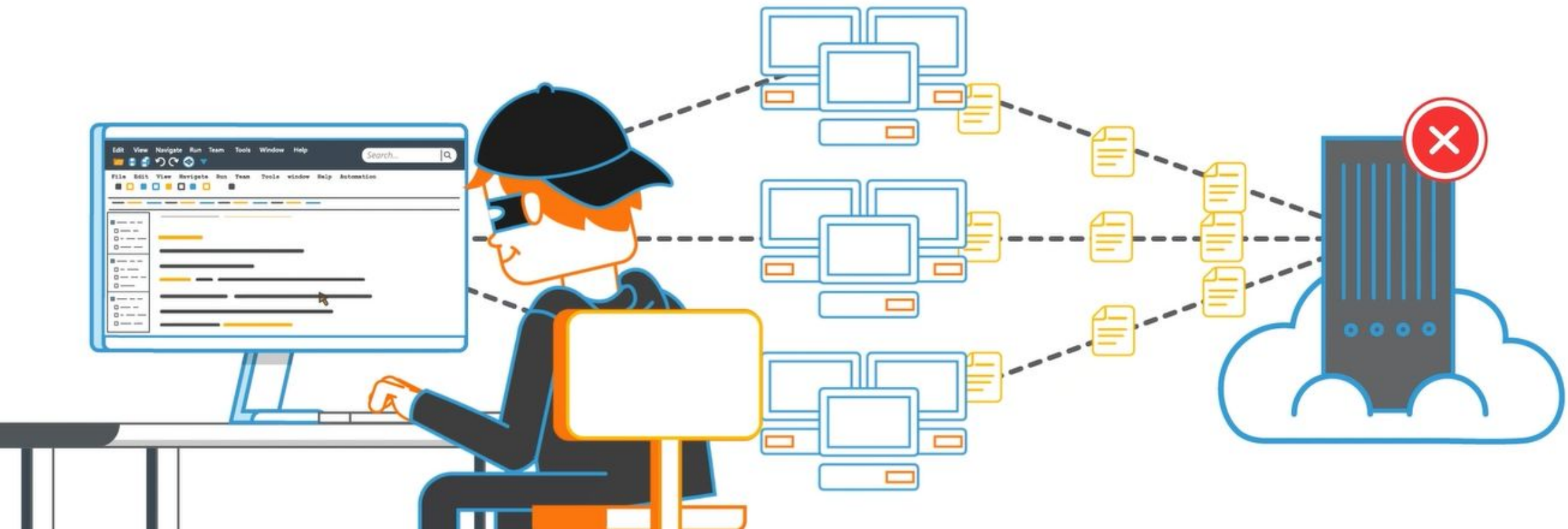
If Confidentiality is the ideal property, Information Disclosure describes when information is exposed to users who are not authorized to see it.

INFORMATION DISCLOSURE



When Availability is the ideal property, Denial of Service happens when service is denied or degraded.

DENIAL OF SERVICE



Finally, when Authorization is the ideal property, Elevation Of Privilege means users can gain capabilities when they don't have proper authorization

ELEVATION OF PRIVILEGE

So, for each part of the asset, think about how each STRIDE threat could have an impact

Ask “How could a particularly skilled attacker {Spoof, Tamper, Repudiate, etc.} this part of the system?”

STRIDE

- **S** - SPOOFING
- **T** - TAMPERING
- **R** - REPUDIATION
- **I** - INFORMATION DISCLOSURE
- **D** - DENIAL OF SERVICE
- **E** - ELEVATION OF PRIVILEGE ←

TO UNDERSTAND STRIDE THREAT MODELING IN MORE DETAIL, LET'S TAKE REPUDIATION FOR EXAMPLE.

The threat is “Repudiating an action”.

List actions the attacker might take. For example, in a simple payment app, an attacker might claim to have not initiated a money transfer.

Threat Example	What the attacker does ?
Repudiating an action	

Or an attacker might claim to have not received the SMS code they need to make the transfer.

Threat Example	What the attacker does ?
Repudiating an action	Claims to have not initiated a money transfer.
	Claims to have not received the SM

Or they may say they did not receive a transfer that they should've received yesterday.

Threat Example	What the attacker does ?
Repudiating an action	Claims to have not initiated a money transfer.
	Claims to have not received the SMS code
	Claims to not receive a transfer

Analyze each of those actions and provide notes. In the first example

Threat Example	What the attacker does ?	Notes
Repudiating an action	Claims to have not initiated a money transfer.	
	Claims to have not received the SMS code	
	Claims to not receive a transfer	

where the attacker claimed not to have initiated a transfer, think about what could have happened.

Threat Example	What the attacker does ?	Notes
Repudiating an action	Claims to have not initiated a money transfer.	The attacker claimed not to have initiated a transfer.
	Claims to have not received the SMS code	
	Claims to not receive a transfer	

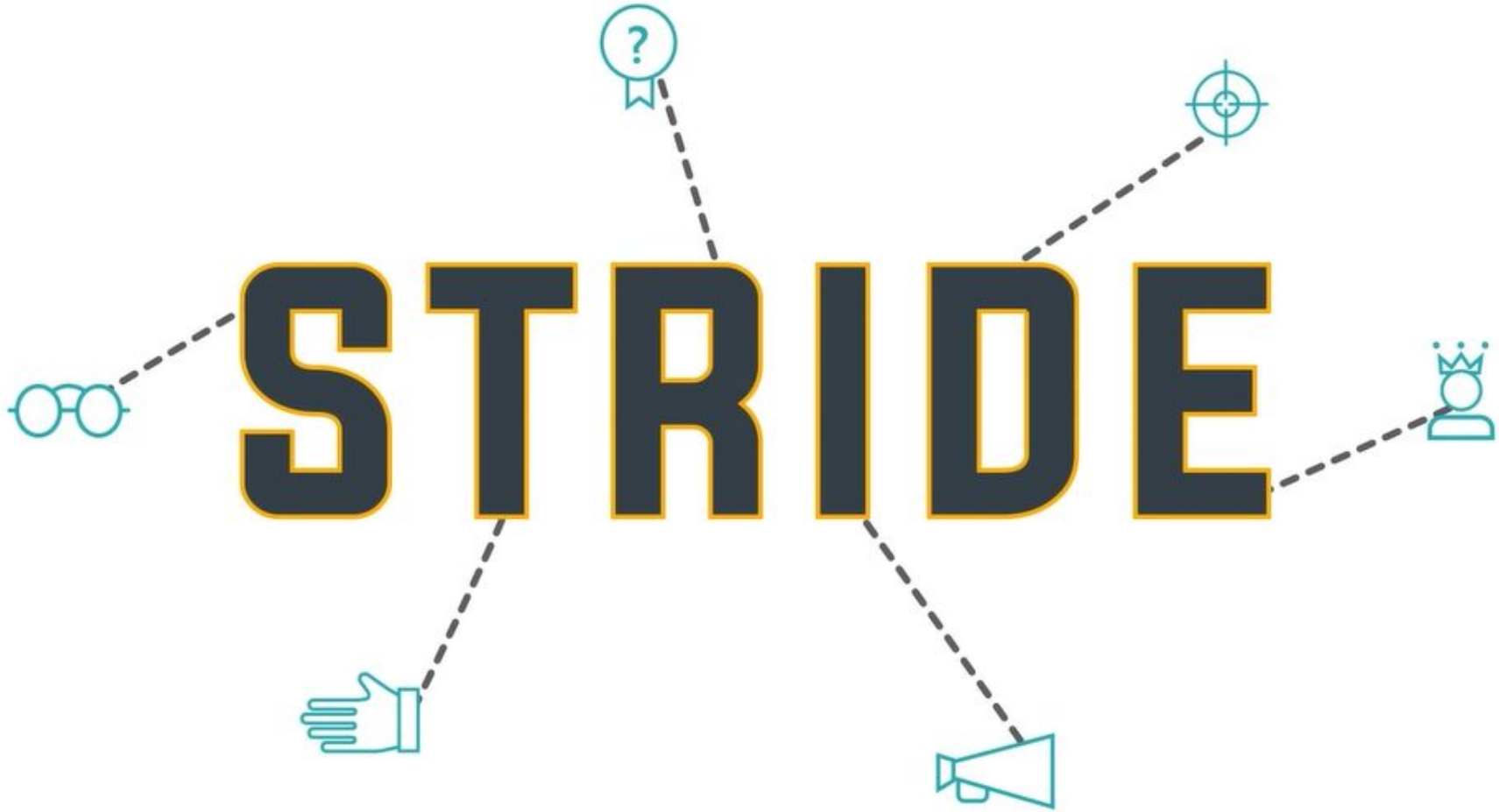
Perhaps it is an accident and the user simply forgot they sent a transfer. Maybe it is an instance of fraud.

Threat Example	What the attacker does ?	Notes
Repudiating an action	Claims to have not initiated a money transfer.	The attacker claimed not to have initiated a transfer. User simply forgot they sent a transfer.
	Claims to have not received the SMS code	Or maybe it is an instance of fraud
	Claims to not receive a transfer	

Or perhaps the attacker has exploited a specific vulnerability.

Threat Example	What the attacker does ?	Notes
Repudiating an action	Claims to have not initiated a money transfer.	The attacker claimed not to have initiated a transfer. User simply forgot they sent a transfer.
	Claims to have not received the SMS code	Or maybe it is an instance of fraud.
	Claims to not receive a transfer	Perhaps the attacker has exploited a specific vulnerability.

STRIDE helps you consider and play out various scenarios so you can prepare for each of them accordingly.



Though STRIDE is just one of many threat modeling methodologies, developers should keep in mind:

- Threat modeling is most effective when done early on in the security development lifecycle

Congratulations, you have now completed this module!


SECURE
CODE
WARRIOR