UNIVERSITAS TERBUKA

MSIM4304
DASAR INFRASTRUKTUR TI

Inisiasi 8
Keamanan Informasi

Program Studi Sistem Informasi
Fakultas Sains dan Teknologi
Universitas Terbuka

PENGERTIAN KEAMANAN INFORMASI

- Menurut Sarno dan Iffano keamanan informasi adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kesinambungan bisnis, mengurangi risiko-risiko yang terjadi, dan mengoptimalkan pengembalian investasi (return on investment).

PENGERTIAN KEAMANAN INFORMASI

- Berdasarkan dokumen standar ISO/IEC 17799:2005 tentang *information security management system* bahwa keamanan informasi adalah upaya perlindungan dari berbagai macam ancaman untuk memastikan keberlanjutan bisnis, meminimalisir risiko bisnis, dan meningkatkan investasi dan peluang bisnis.

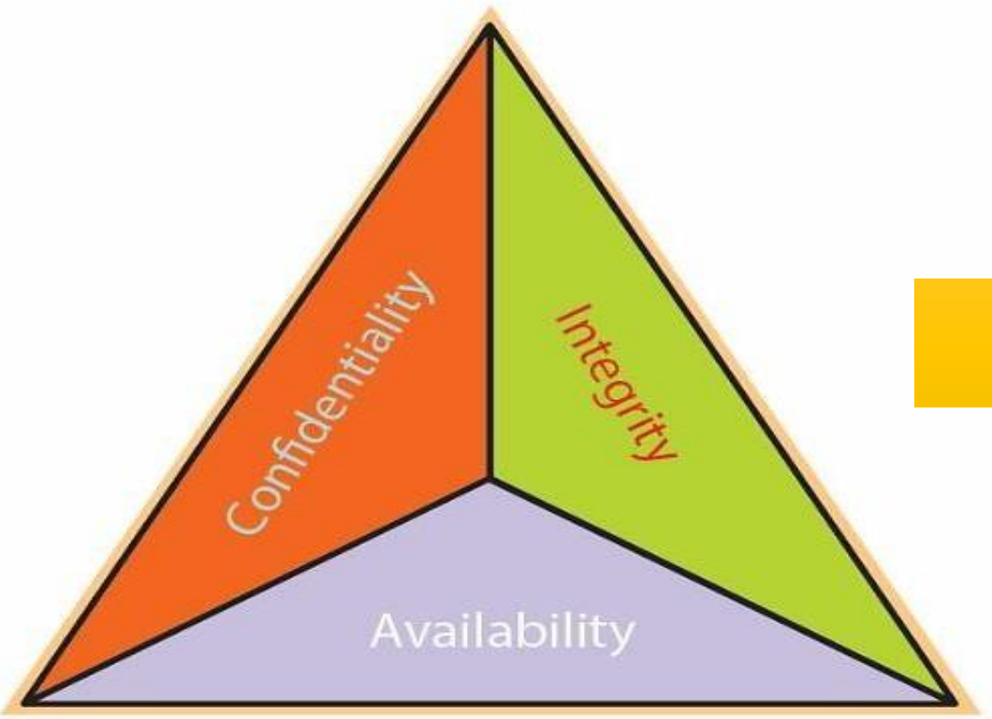
PENGERTIAN KEAMANAN INFORMASI

- Keamanan informasi menurut G. J. Simons adalah bagaimana usaha untuk dapat mencegah penipuan (cheating) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Aspek-aspek yang harus dipenuhi dalam suatu sistem untuk menjamin keamanan informasi adalah informasi yang diberikan akurat dan lengkap, informasi dipegang dan dikuasai oleh orang yang berwenang, dapat diakses dan digunakan sesuai dengan kebutuhan, dan memberikan informasi pada format yang tepat.

PENGERTIAN KEAMANAN INFORMASI

- Menurut Whitman & Mattord, keamanan secara umum dapat diartikan sebagai ‘quality or state of being secure-to be free from danger’.

ASPEK-ASPEK KEAMANAN INFORMASI



- *authentication*
- pengaturan hak akses
- *non repudiation*
- *Accountability*
- *Accountability*

TINJAUAN KEAMANAN INFORMASI

- *physical security*
- *personal security*
- *operasional security*
- *communication security*
- *network security*

Manajemen risiko

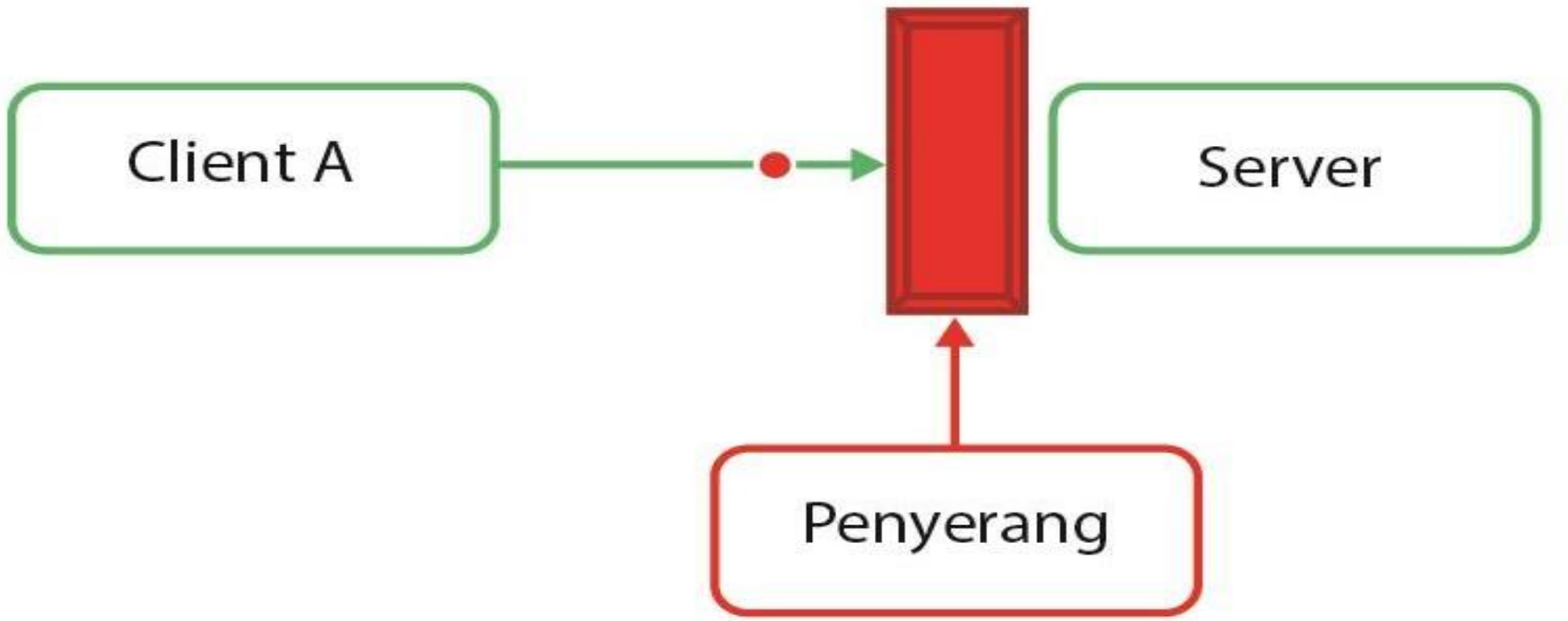
- Aset
- Ancaman
- Kelemahan

ANCAMAN DAN JENIS SERANGAN TERHADAP KEAMANAN INFORMASI

- Ancaman adalah segala sesuatu yang menyebabkan asset yang kita miliki terganggu, ancaman keamanan sistem informasi merupakan orang, organisasi, mekanisme, atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan.

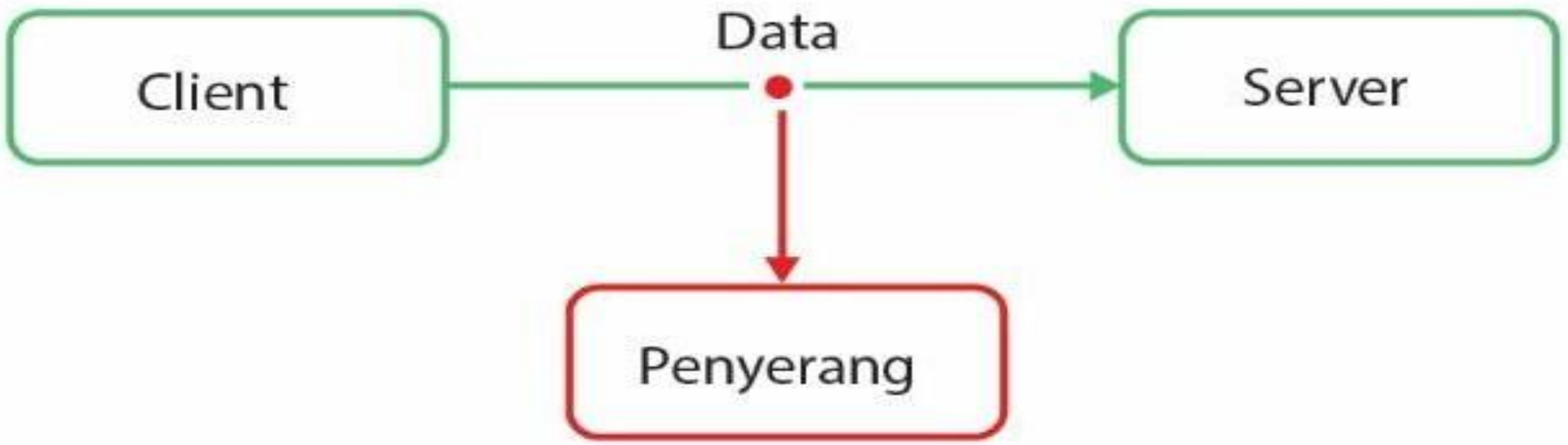
Bentuk Serangan

- *Interruption,* merupakan ancaman terhadap *availability*, yaitu data dan informasi yang berada dalam sistem komputer dibuang atau dirusak, sehingga menjadi tidak ada atau tidak berguna. Contohnya, *hard disk* yang dirusak, memotong jalur komunikasi, *denial of service* (*DoS*).



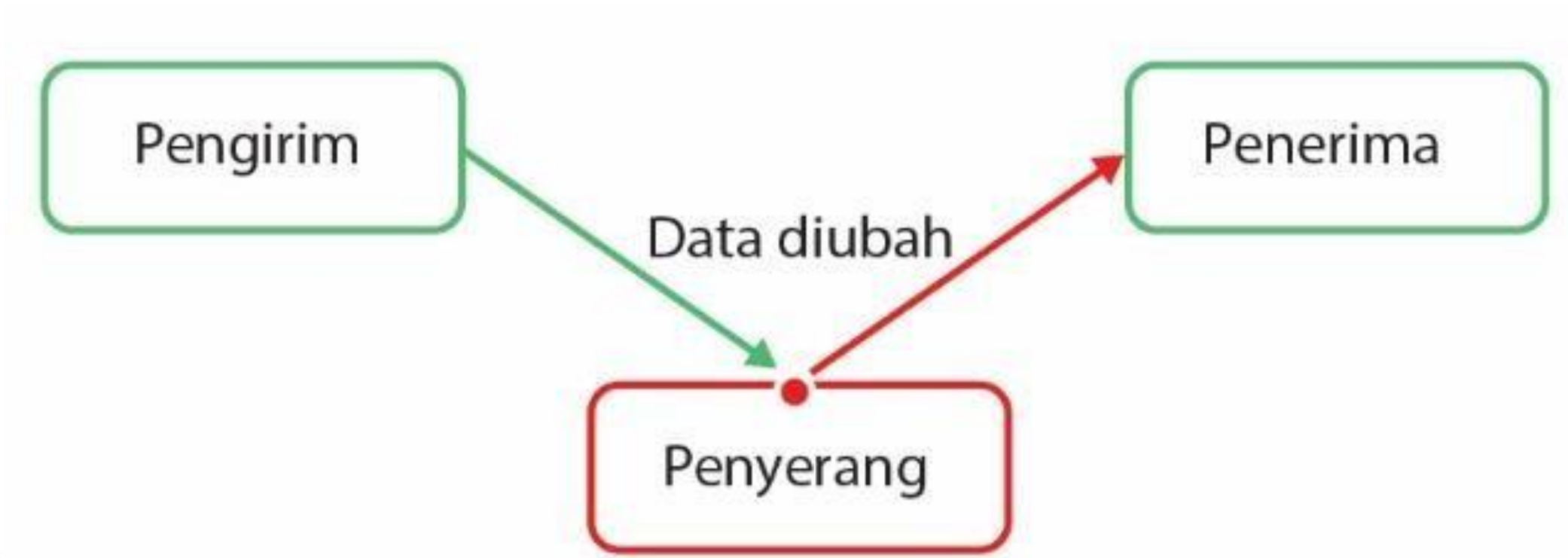
Bentuk Serangan

- *Interception,* pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contohnya dengan menyadap data yang melalui jaringan publik atau menyalin data secara tidak sah.



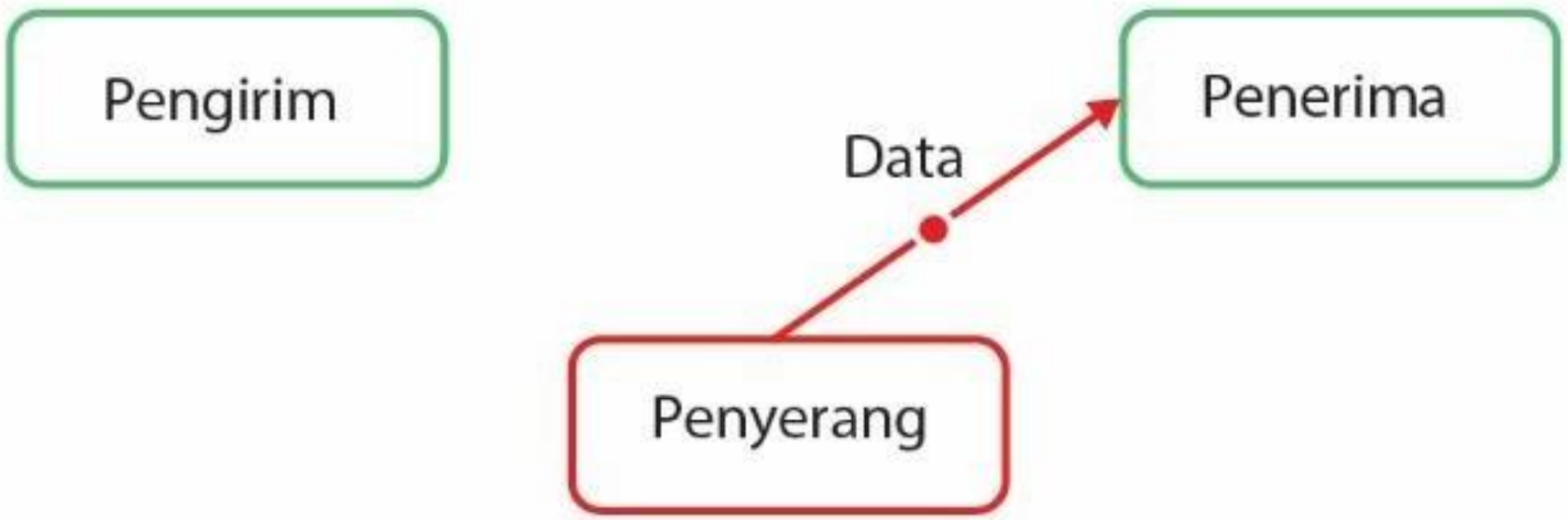
Bentuk Serangan

- *Modification,* pihak yang tidak berwenang berhasil mengakses dan merubah informasi. Contoh, mengubah isi dari website dengan pesan-pesan yang merugikan pemilik *website* (*defacing*).



Bentuk Serangan

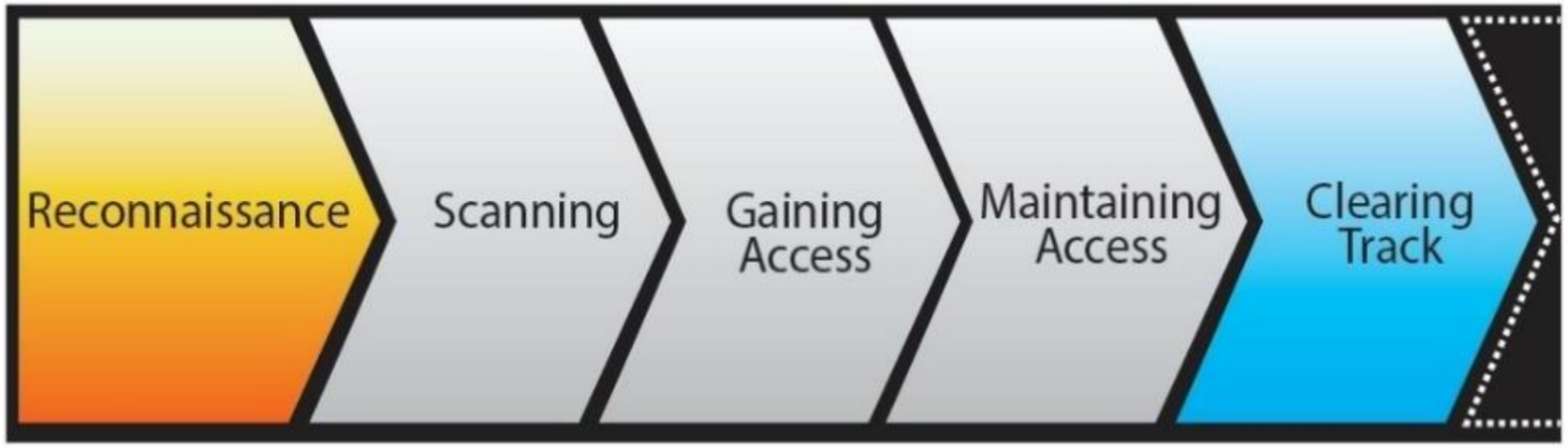
- *Fabrication,* merupakan ancaman terhadap informasi yang dilakukan oleh orang yang tidak berwenang dengan cara menyisipkan objek palsu ke dalam sistem. Contohnya, memasukkan pesan-pesan palsu seperti email palsu ke dalam jaringan komputer.



Jenis serangan yang dapat dilakukan oleh cracker

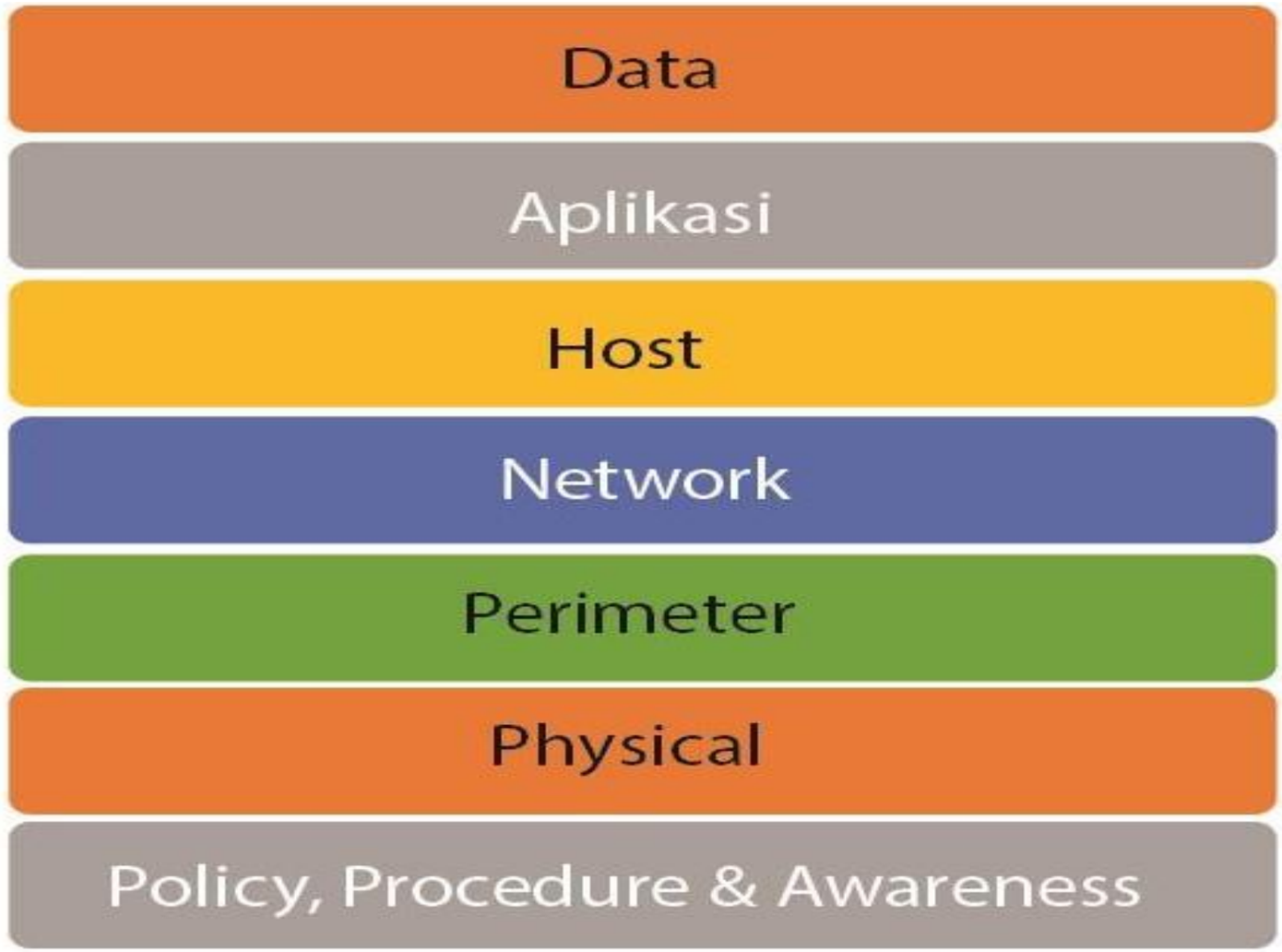
- *Web deface*
- *DoS* (*Denial of Service*) dan *DDoS* (*Distributed Denial of Service*)
- *Spoofing*
- *Sniffing*
- *DNS poisoning*
- *Trojan*
- *SQL injection*
- *Phising*

METODOLOGI SERANGAN TERHADAP KEAMANAN INFORMASI



ARSITEKTUR PENGAMANAN SISTEM

- Mekanisme pendekatan pengamanan berlapis dapat meningkatkan kemampuan untuk mendeteksi *cracker* dan mengurangi tingkat keberhasilan seorang *cracker*. *Defense-in-depth* terdiri dari serangkaian lapisan yang saling terhubung



ARSITEKTUR PENGAMANAN SISTEM

- Dalam penerapan mekanisme pengamanan perlu diperhatikan konsep segitiga keamanan, fungsionalitas dan kemudahan penggunaan. Secara umum, seiring dengan upaya peningkatan keamanan, maka tingkat fungsionalitas sistem dan kemudahan penggunaan akan berkurang bagi pengguna. Begitupula sebaliknya semakin tinggi tingkat kemudahan penggunaan maka semakin rendah pula tingkat keamanan sistem.