Security and Network Management

Tommaso Pecorella
tommaso.pecorella@unifi.it

Corso di Studi in Ingegneria delle Telecomunicazioni
Corso di Studi in Ingegneria Informatica
Scuola di Ingegneria
Università degli Studi di Firenze

02 – Security Basics
aa. 2016/17

Security ?

Security is simple to define. *Right ?*
Security properties are usually listed as:

- **Confidentiality** – Ensuring that information is not accessed by unauthorized persons
- **Integrity** – Ensuring that information is not altered by unauthorized persons in a way that is not detectable by authorized users
- **Authentication** – Ensuring that users are the persons they claim to be

However, reaching these goals is not *that* simple.
Moreover, one should not mistake *Security* for *Safety* (or viceversa).

Security and Safety

Security

1. the quality or state of being secure: as
   a. freedom from danger : safety
   b. freedom from fear or anxiety
   c. freedom from the prospect of being laid off (job security)
2. something given, deposited, or pledged to make certain the fulfillment of an obligation
3. an instrument of investment in the form of a document (as a stock certificate or bond) providing evidence of its ownership
4. something that secures : protection
   a. measures taken to guard against espionage or sabotage, crime, attack, or escape
   b. an organization or department whose task is security

Safety

1. the condition of being safe from undergoing or causing hurt, injury, or loss
2. a device (as on a weapon or a machine) designed to prevent inadvertent or hazardous operation

`http://www.merriam-webster.com/dictionary/safety`

Security costs

Security is not free of charge:

1. The system is more complex.
2. Implementation and operational costs.
3. Workflow is changed (some stuff can not be done, or with limitations).

Before planning the system security, we need to know *what* have to be made secure, *why*, and *against who*.

When the security policies are too limiting (or they are not understood), the user will find a way to violate them. Security policies, if not followed, are *useless*.

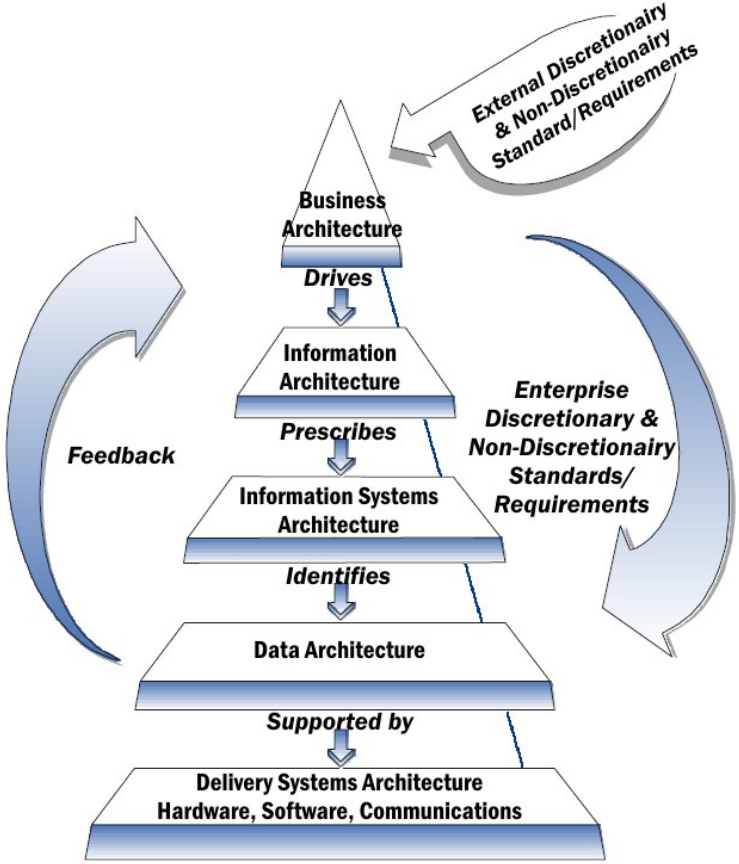
Bottom line: we need a way to describe *what*, *why*, and *against who*

Enterprise Architecture Framework

"An Enterprise Architecture Framework (EA Framework) is a framework for an Enterprise Architecture which defines how to organize the structure and views associated with an Enterprise Architecture."

It is something related to the *enterprise management*.

We need to *understand* it and use it.



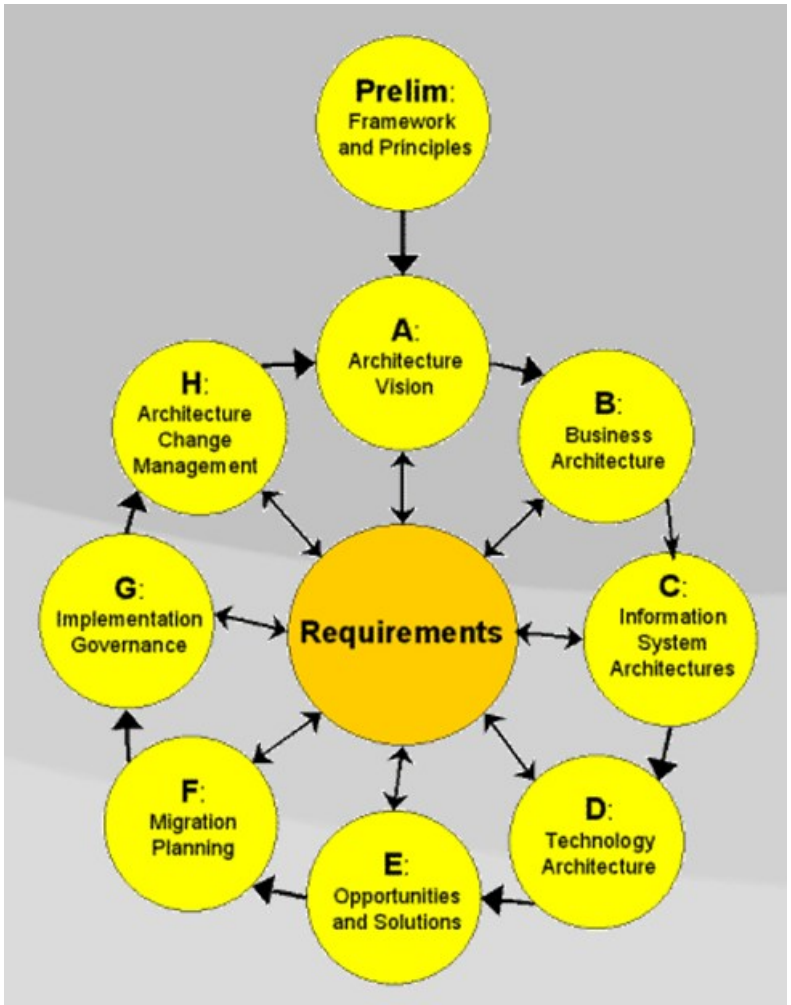
Enterprise Architecture Framework

The most used EAFs are:

- COBIT - Framework for IT Governance and Control
- TOGAF - the Open Group Architecture Framework
- DoDAF - United States Department of Defense Architectural Framework.
- MODAF - United Kingdom Ministry of Defence Architectural Framework.
- NAF - the NATO Architecture Framework
- SABSA a comprehensive framework for Enterprise Security Architecture and Service Management.

TOGAF and COBIT are the most used ones for non-military enterprise.

Enterprise Architecture Framework



Tutti gli EAF (quasi) adottano modelli "iterativi" in cui ad ogni fase si raffinano e precisano i concetti precedenti.

Quasi tutti i Framework pongono l'accento sui dati piuttosto che sulle applicazioni e/o la tecnologia.

Si introduce quindi il concetto di *Asset*.

Asset

Si definisce *asset* una qualsiasi risorsa dell'Enterprise che abbia o rappresenti un valore importante per l'Enterprise stesso.

Un asset può essere rappresentato da:

- Dati
- Componenti tecnologici (hardware)
- Componenti applicativi (applicazioni)

Un asset ha anche delle proprietà intrinseche e/o desiderate e/o imposte dalla legge (e.g., i dati personali sono sottoposti alla legge sulla Privacy).
Tali proprietà sono "esportate" agli asset che interagiscono con l'asset in questione.

Lo scopo della sicurezza è quello di proteggere gli asset.

Risk management

Il Risk Management è un processo composto da:

1. identificazione
2. valutazione
3. riduzione del rischio a livelli accettabili
4. implementazione di contromisure per mantenere il livello di rischio definito

Quello che siamo abituati a pensare come “sicurezza” è svolto ai punti 3 e 4.

Risk assessment methodologies

Il Risk assessment può essere qualitativo o quantitativo.

Qualitativo

Esempio: matrici importanza (influenza) / probabilità di occorrenza
Danno una visione semplice e sintetica dei possibili rischi

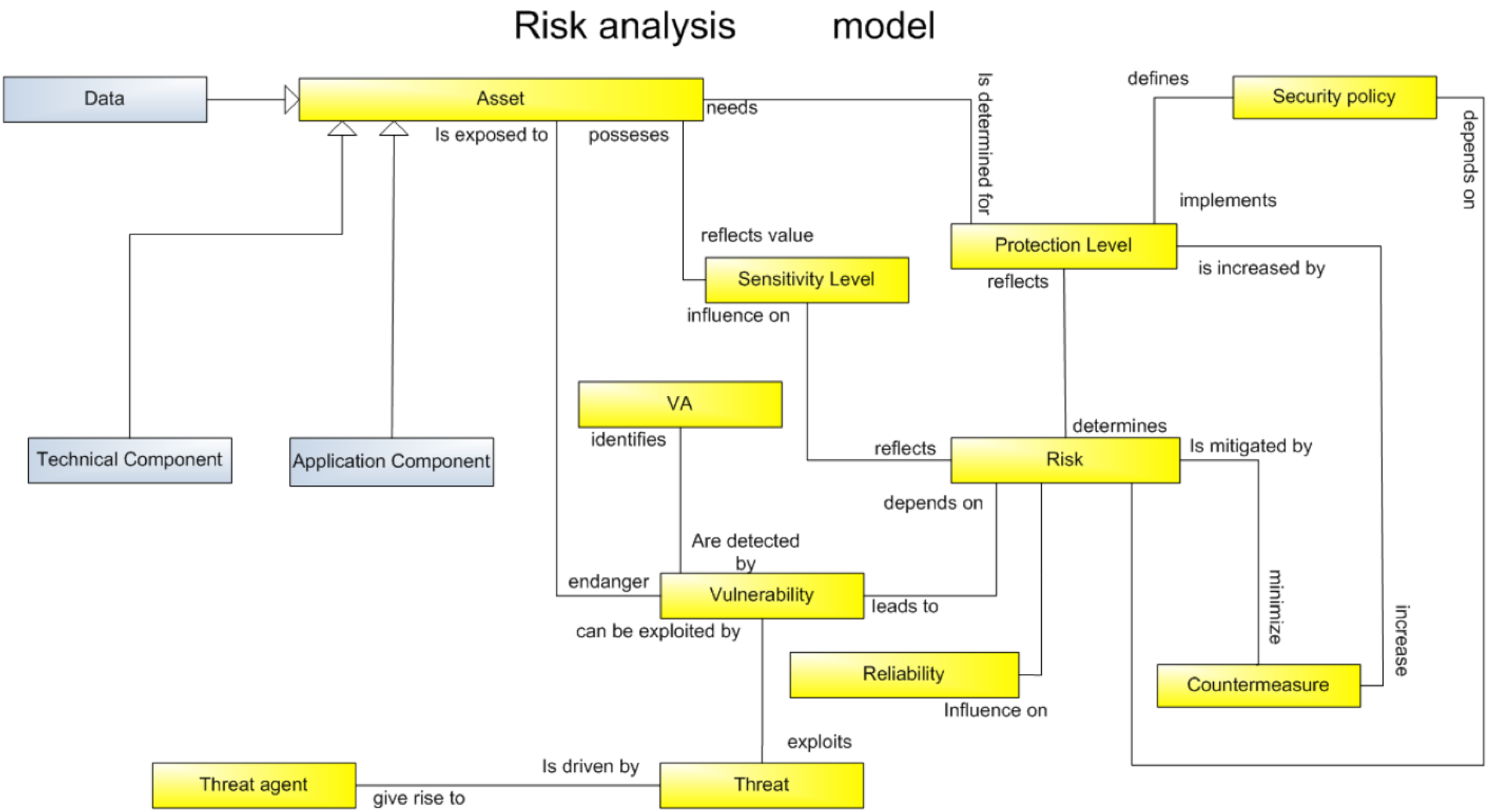
Quantitativo

Esempio:

- Asset value (AV)
- Annual rate of occurrence (ARO)
- Exposure factor (EF) (percentage)
- Single loss expectancy (SLE) = AV x EF
- Annual loss expectancy (ALE) = ALE = SLE x ARO

Quasi sempre sono stime troppo grossolane.

Risk analysis model



Il Vulnerability Assessment è una parte chiave nel processo.

Threat model

Per definire in modo completo la “sicurezza” è infine indispensabile il Threat Model.

RFC 3552

A THREAT MODEL describes the capabilities that an attacker is assumed to be able to deploy against a resource.
It should contain such information as the resources available to an attacker in terms of

- information,
- computing capability, and
- control of the system.

Internet Threat model

Genericamente si assume che l'attaccante:

- sia a conoscenza di tutte le informazioni possibili (non segretezza)
- abbia sufficiente capacità computazionale (nei limiti dei sistemi commerciali)
- abbia un totale controllo del sistema di comunicazioni (send/receive), ma NON abbia il controllo degli endpoints.

In alcuni casi è plausibile parlare di attacchi "limitati", dove l'attaccante può alternativamente:

- inviare ma non ricevere [tutto] (active attacks, blind o meno)
- ricevere ma non inviare (passive attacks)

Esempi di attacchi

Passive Attacks

- Confidentiality Violations
- Password Sniffing
- Offline Cryptographic Attacks

Active Attacks

- Replay Attacks
- Message Insertion
- Message Deletion
- Message Modification
- Man-In-The-Middle

Topologia !

Attenzione alla topologia della rete.

Assumere che l'attaccante possa inviare e ricevere pacchetti con la stessa facilità è *falso*.

Quindi gli attacchi si possono dividere in:

- On-path - di solito solo un gateway o un router sono on-path,
- Off-path - il caso normale,
- Link-local - caso speciale, l'attaccante è sulla stessa subnet di uno degli endpoints.

Non si deve mai assumere che l'attacco sia off-path, ma certamente è più difficile (meno probabile) che sia on-path. Inoltre per "diventare" on-path necessario portare un attacco alla topologia (routing), possibile ma non semplice.

Ricordarsi che...

Un Attacco:

1. non è mai fine a sé stesso,
2. sfrutta una vulnerabilità,
3. è rivolto ad un *asset*.

Un Asset:

1. ha sempre delle vulnerabilità,
2. ha un protection level e un sensitivity level,
3. si può proteggere con delle *countermeasures*.

Le contromisure non sono le protezioni contro le vulnerabilità (quelle sono tese ad eliminare le vulnerabilità), sono... contromisure.
E.g.: se mi bloccano la mail mi faccio mandare un fax.