



UNIVERSITY
OF TRENTO - Italy




Cyber Security Risk Assessment
Fall 2016

Lecture 02 – Terminology
Fabio Massacci

9/19/16 Fabio Massacci - Cyber Security Risk Assessment 1




UNIVERSITY
OF TRENTO - Italy




Lecture Outline

- **What is Computer Security about?**
 - Security Properties
- **Basic Security Terminology**
 - Asset, Risk, Vulnerability, Threat, Security Policy, Countermeasure....
- **What assets do we need to protect?**
 - Hardware, Software, Data Communication Lines
- **How are those assets threatened?**
 - Threats, Attacks Types
- **What can we do to counter those threats?**
 - Countermeasures, Security Controls Types
- **Putting all together**
 - An example: Online Payment
- **A little exercise**
 - Mother, Father, and Child

9/19/16 Fabio Massacci - Cyber Security Risk Assessment ▶ 2



UNIVERSITY
OF TRENTO - Italy




What is a tangible asset?

- **Hardware**
 - computer systems, data storage, data communication devices
- **Software**
 - operating systems, system utilities, applications, services
- **Data**
 - files and databases
- **Communication Lines**
 - local and wide area network communication links, router, gateways and so on

9/19/16 Fabio Massacci - Cyber Security Risk Assessment ▶ 3



UNIVERSITY
OF TRENTO - Italy



What are “intangible” assets?

- **What is really of value**
 - Information and Values
 - Business Processes
 - Company Reputation
- ***In most cases the “tangible” assets by themselves are not really what you care about***
 - Customer DB of 10M Records → priceless
 - DBMS managing the DB → buy & install new for 20K
 - 1TB Hard disk storing DBMS files → buy new for 2K

9/19/16 Fabio Massacci - Cyber Security Risk Assessment 4

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

What Properties of Assets?

- ***The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, the availability and confidentiality of information systems resources (=Assets),***
 - NIST Computer Security Handbook
- ***Lots of other definition about “cyber” security***

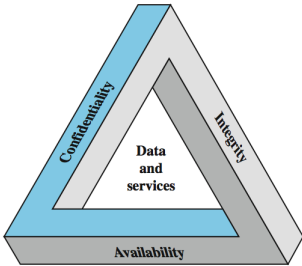
9/19/16 Fabio Massacci - Cyber Security Risk Assessment ▶ 5

UNIVERSITY OF TRENTO - Italy


eit Digital MASTER SCHOOL

The CIA Triad


- ***Confidentiality***
 - preventing unauthorized disclosure of information
- ***Integrity***
 - preventing unauthorized modification of information
- ***Availability***
 - preventing of unauthorized withholding of information or resources



9/19/16 Fabio Massacci - Cyber Security Risk Assessment ▶ 6



UNIVERSITY
OF TRENTO - Italy



A “Pre-requisite” property

- **Authenticity**
 - the property of an entity of being “genuine” and to be verified
 - origin authenticity, data authenticity
- **Authenticity is a pre-requisite property of all three properties**
 - If you cannot tell who is Fabio Massacci, how can your system ever assure that data is only read by him (confidentiality), only modified by him (integrity) or accessible to him (availability)?

9/19/16 7
Fabio Massacci - Cyber Security Risk Assessment




UNIVERSITY
OF TRENTO - Italy




A question?

- **Identity theft in the US (2012)**
 - Population: 314.100.000
 - Identity Theft: 16.600.000
- **Identity theft in Italy (2012)**
 - Population: 59.500.000
 - Identify Theft: 24.000
- **Why so few Italian frauds?**
 - After all Italy invented the mafia and exported it to the world

9/19/16 8
Fabio Massacci - Cyber Security Risk Assessment




UNIVERSITY OF TRENTO - Italy




A question... cont

- **Identity theft in the US (2012)**
 - Population: 314.100.000
 - Credit cards: 600.000.000
 - Identity Thefts: 16.600.000
- **Identity theft in Italy (2012)**
 - Population: 59.500.000
 - Credit cards: 61.000.000
 - Identify Thefts: 24.000
- **So there are**
 - 5 USA residents vs 1 Italian resident
 - 10 USA credit cards vs 1 Italian credit card
 - 691 USA id frauds vs 1 Italian id fraud
- **Why no 10 US frauds vs 1 Italian fraud or even more?**

9/19/16 Fabio Massacci - Cyber Security Risk Assessment 9



UNIVERSITY OF TRENTO - Italy




The BIG US mistake: Auth vs Ident


- **Identification (Oxford dictionary)**
 - “The action or process of identifying someone or something or the fact of being identified.”
- **Authentication (ibidem)**
 - “The process or action of proving or showing something to be true, genuine, or valid”
- **Can you discover my social security number?**
 - Very easy
- **What can you do with it?**
 - Very little
- **Why?**
 - It is just an unique identifier, not a unique authenticator.

VALUTAZIONE COMPARATIVA PUBBLICA PER N
web.poliba.it/.../k05a10... ▼ Translate this page Polytechnic University of Bari ▼
 Mar 20, 2000 - Massacci Fabio. 12. Milano Michela. 13. ... Massacci Fabio. 10. Milano Michela ... Massacci Fabio nato a Cagliari il 19/6/1967; Milano Michela ...

9/19/16 Fabio Massacci - Cyber Security Risk Assessment 10




UNIVERSITY
OF TRENTO - Italy




The CIA Triad: Confidentiality

- **Data Confidentiality**
 - protecting private and sensitive data from access and disclosure by unauthorized individuals
- **Unlinkability**
 - Two items of interest are unlinkable if an attacker can't determine that they are related to each other
- **Anonymity**
 - A subject (a user) is anonymous if an attacker cannot be distinguish him/her in the anonymity set of subjects

9/19/16 Fabio Massacci - Cyber Security Risk Assessment ▶ 11




UNIVERSITY
OF TRENTO - Italy




The CIA Triad: Integrity

- **Data Integrity:**
 - data are not modified by unauthorized individuals
- **System Integrity:**
 - system performs its intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

9/19/16 Fabio Massacci - Cyber Security Risk Assessment ▶ 12




UNIVERSITY
OF TRENTO - Italy




The CIA Triad: Availability

- **Availability**
 - ensuring that a resource is accessible and usable by an authorized entity
 - It concerns intentional failures caused by a human
- **Reliability**
 - It concerns accidental software, hardware, communication failures

9/19/16 Fabio Massacci - Cyber Security Risk Assessment ▶ 13




UNIVERSITY
OF TRENTO - Italy




Other Properties

- **Accountability**
 - the property of tracing security related actions/events to the responsible entity
- **Non-repudiation**
 - the property of having unforgeable evidence that an event/action has occurred
 - non-repudiation of origin, non repudiation of delivery
- **“Privacy” (Often grouped with confidentiality)**
 - the right of an individual to control what data are collected and stored by who and to whom are disclosed

9/19/16 Fabio Massacci - Cyber Security Risk Assessment ▶ 14



UNIVERSITY OF TRENTO - Italy



What can you do without...

	Confidentiality	Integrity	Availability	Accountability	Non-repudiation	Privacy
No Confidentiality	X	10	15	6	6	Not really
No Integrity	12	X	Kind of	x	x	Kind not
No Availability	Yes	Yes	X	Kind of	Same	

9/19/16 Fabio Massacci - Cyber Security Risk Assessment 15




UNIVERSITY OF TRENTO - Italy




What can you do without... (2015)

	Confidentiality	Integrity	Availability	Accountability	Non-repudiation	Privacy
No Confidentiality	x	10	8	7	4	no
No Integrity	2	x	7	2 - no	no	"Ni"
No Availability			x			

9/19/16 Fabio Massacci - Cyber Security Risk Assessment 16



UNIVERSITY
OF TRENTO - Italy



Suggested Readings

- **Textbook -- Chapter 1.**
- **Additional Readings**
 - Chapter 1, Ross Anderson. Security Engineering
 - Chapter 2, Dieter Gollmann. Computer Security
- **Insight**
 - D. Sterne: On the Buzzword 'Security Policy', IEEE Symposium on Research in Security and Privacy 1991
 - K. Thomson. Reflection on trusting trust. Turing Award Lecture.
- **Fact finding**
 - Reports on ID Theft in the US and Italy

9/19/16

Fabio Massacci - Cyber Security Risk
Assessment

► 17