Security Engineering
Fall 2015

Lecture 02 – Terminology

Fabio Massacci

Lecture Outline

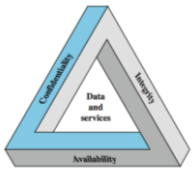
- ***What is Computer Security about?***
  - Security Properties
- ***Basic Security Terminology***
  - Asset, Risk, Vulnerability, Threat, Security Policy, Countermeasure….
- ***What assets do we need to protect?***
  - Hardware, Software, Data Communication Lines
- ***How are those assets threatened?***
  - 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

What is Computer Security About?

- ***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,***
  - NIST Computer Security Handbook

The CIA Triad

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



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)?

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?***

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 frauds vs 1 Italian fraud

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.

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
- ***Anonimity***
  - A subject (a user) is anonymous if an attacker cannot be distinguish him/her in the anonimity set of subjects

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

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 sofware, hardware, communication failures

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 occured
  - 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

What can you do without…

	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			

What is an 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 an so on

What is a vulnerability, a threat, and risk?

- ***Vulnerability***
  - A flaw or weakness in a system's design, implementation, operation, management that could be exploited by a threat
- ***Threat***
  - circumstance, capability, event, action that could breach securtity and cause harm to an asset
- ***Threat Agent***
  - the entity carrying out a threat
- ***Risk***
  - An expectation of loss expressed as the probability that a threat occurs and the harmful result

Threat Types (1)

- ***Attive Attacks***
  - Aim to modify system'assets or to affect their operation
  - Preventing them is harder than detecting them
  - e.g reply attack, SQL injection
- ***Passive Attacks***
  - Aim to learn or make use of information that not affect the system'assets
  - Detecting them is harder than preventing them
  - e.g traffic analysis

Threat Types (2)

- ***Unauthorized disclosure***
  - Exposure, Interception, Inference, Intrusion
- ***Deception***
  - Masquerade, Falsification, Repudiation
- ***Disruption***
  - Incapacitation, Corruption, Obstruction
- ***Usurpation***
  - Misappropriation, Misuse

Which threat does affect…

	Unauthorized disclosure	Disruption	Disruprion	Usurpation
Confidentiality				
Integrity				
Availability				

Threat Agents

- ***Insider Attacks***
  - The treat agent is a legitimated user of the system who oversteps his/her authorization
  - Frequent vector for large companies
- ***Outsider Attacks***
  - The threat agent is an unauthorized user of the system or illegitimate user to the system
- ***Both can be prevented and detected up to a certain level***

Assets and Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled	Hardware trojan sends data out	EM field changes data
Software	Programs are deleted	Unauthorized copy of the software	Working program is modified
Data	Files are deleted	Unauthorized read of data	Existing files are modified or new files are fabricated
Communication Lines	Messages are deleted, Communication lines make unavailable	Messages are read. The traffic pattern of messages are observed	Messages are modified or fabricated

Historic Threats to Assets

- ***Hardware***
  - Desktop computer stolen at Sutter Physicians Services and Sutter Medical Foundation, which contained about 3.3 million patients' mediacal details stored in unencrypted format in 2011
- ***Software***
  - Phishing attack to PayPal stealing customers' credit card details in 2006
- ***Data***
  - Data breaches (passwords), stemming from attacks that compromised Sony PlayStation Network, Sony Pictures in 2011, Target, OPM etc. etc.
- ***Communication Lines***
  - Kevin Poulsen was a teenage telephone hacker who hacked the phone lines to win a Porsche in a radio contest in 1990

What is a security control?

- ***an action, device, a procedure or technique that …***
- ***reduces a threat, a vulnerability, or an attack by ….***
- ***eliminating it,***
- ***minimizing the harm it causes, or***
- ***discovering and reporting it so that corrective action can be taken***

Types of Security Controls

- ***Management Controls***
  - Awareness and Training
  - Security policy and practices
  - Audit and Accountability
  - Risk-assessment
  - Contingency Planning
- ***Technical Controls***
  - Identification and authentication
  - Access and authorization
  - Encryption
  - Digital Signature
  - Privacy-enhancing technologies

When they can be applied?

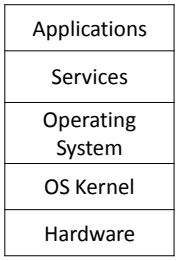
- ***Preventive***
  - Measures that prevent your assets to be affected
- ***Detective***
  - Measures that allow to detect when an assets has been affected, how it has been affected, and by who
- ***Reactive***
  - Measures that allow to recover your assets or (partially) restore operation from damage to your assets

Which control does protect…

	Preventive	Detective	Reactive
Confidentiality			
Integrity			
Availability			

Where security controls should be placed?

- ***You need to find***
  - right layer for each security control
  - right security control for each layer
- ***Usually three levels***
  - Users (Database access controls)
  - Applications
  - Infrastructure



An exercise in Security

- ***Mother, Father and Child***
  - You are a mother
  - Your asset is your child
  - You can use the father to provide some services
  - You have to balance security and cost
- ***Only one thing is possible for you***
  - Bring the child to school
  - Collect the child from school
- ***What is safer for a child?***
  - Go back home from school alone?
  - Go back with the father?

Threats

- ***Threats***
  - Going Alone:
  - Father pick-up:
- ***Threat Agents***
  - Going alone:
  - Father pick-up:

Design your controls

- ***Going Alone***
  - Preventive:
  - Detective:
  - Reactive:
- ***Father pick up***
  - Preventive:
  - Detective:
  - Reactive:

Mother, Father, and CHILD II

- ***Going alone...***
  - upon instructions on security measures
    - the child would not accept lift from unknown people (authentication + preventive)
    - He would scream if forced (reactive)
    - If he doesn't show up at planned time mother will react (detective)
  - Trust assumption: on screaming passers-by will react and act
- ***Trustworthy but very costly***
  - Persistent training of "user" (i.e. child)
    - Do not take lift for people you don't know
  - Resistance to social engineering attacks must be trained
    - It doesn't matter it was just a nice old man
  - 100% alert monitoring by mother

Mother, Father and Child III

- ***The father solution is dirty cheap***
  - Can be quickly authenticated by the child
  - No training of any kind
  - No measure against social engineering
  - No monitoring
- ***The father is trusted by the mother...***

Mother, Father and Child IV

- ***Making "Going alone" trustworty is expensive***
  - Lots of additional security measures
- ***"Father picks up" is trusted and cheap***
  - No security measure
- ***The father is trusted by the mother...***
  - But **almost all** child kidnapping, beating, and killing are done by fathers or close members of the family
  - Only few (8%) done by "maniacs" unknown to the child
    - U.N. Statistics
- ***A Trusted Component is not something that is secure. It is something against which we plan no defence***

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Suggested Readings

- ***Textbook introduction***
  - Chapter 1, Stallings and Brow. Computer Security
  - Chapter 2, Dieter Gollmann.Computer Security
  - Chapter 1, Ross Anderson. Security Engineering
- ***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