CS5285
Week 2

Weekly Reading Q1

1. Is a security vulnerability always related to technical aspects of the target? Is an attack always technical in nature? In the article, find an example of a technical and non-technical weakness exploited by attackers.

Technical: Denial of Service (DoS), SQL Injection, poor firewall, web server with known security vulnerabilities

Non-technical: Phishing

Weekly Reading Q2

2. What types of adversaries are mentioned in the article?

Mostly hacktivists (Anonymous and LulzSec)

Weekly Reading Q3

3. Which security service and associated mechanism is said to be capable of making this data breach less serious?

- Confidentiality (Encryption) – would not prevent data physically being ‘taken’ but it would be useless to the attacker. Not implemented due to cost concerns…

- Real issue – was not even security but poor procedure (failing to patch/update and configure) allowing well known vulnerabilities to remain

Weekly Reading

Quick Additional Question!

Security in e-commerce is very important these days. Why do you think this is? Who is harmed by weak security and what type of damage does security breaches cause?

- Important as we are all connected – More attackers! More customers (money/revenue is at risk)!
- Breaches harms our business (money and reputation), our customers (money, loss of privacy), and other businesses (money, reputation)

CS5285
Tutorial 1

Security Services and Mechanisms

- A security threat is a possible means by which your security goals may be breached (e.g. loss of integrity or confidentiality).
- A security **service** is a measure which can be put in place to address a threat (e.g. provision of confidentiality).
- A security **mechanism** is a means to provide a service (e.g. encryption, digital signature).

Data Confidentiality, Integrity and Availability

- **Confidentiality** is protection against unauthorised disclosure of information.
- **Integrity** is protection against unauthorised modification of data
- **Availability** is the prevention of unauthorised withholding of information or resources.

Authentication and Access Control

- **Entity authentication** provides checking of a claimed identity at a point in time.
- **Origin authentication** provides verification of source of data.
- **Access Control** provides protection against unauthorised use of resource
  - Is the entity allowed to use this resource?

Non-repudiation

- Protects against a sender of data denying that data was sent (**non-repudiation of origin**).
- Protects against a receiver of data denying that data was received (**non-repudiation of delivery**).

Mechanisms

- A *security mechanism* is a means to provide a service .
- Examples of Services/Mechanisms
  - Confidentiality (encryption)
  - Integrity (MAC/digital signature)
  - Availability (redundancy)
  - Entity Authentication (authentication protocol)
  - Origin Authentication(MAC/digital signature)
  - Non-repudation (digital signature)
  - Access Control (Access control model)

Tutorial Q1

Service	Mechanism	Algorithm	Threat
Confidentiality	Encryption	DES/3DES/AES	Data disclosure
Integrity	MAC	HMAC	Modification
Non-repudiation	Digital Signature	RSA/DSA	Repudiation

Tutorial Q2

2.a) Availability is seen as a basic security service. Briefly explain what this service does and give an example of the type of behavior it prevents in e-commerce.

It tries to preserves authorised access to services.

The main threat here is Denial of Service (DoS)

Tutorial Q2

2.b) Availability was not seen as a security service in the late 1980s when network/communication security services were written in prominent standards – but it is today. What do you think changed?

In the 1980s there was no Internet, there were limited public networks – the idea that you would connect and receive content over the Internet (and that someone would try to deny you this) was not foreseen…

Tutorial Q3

Explain to your new employer what authentication, confidentiality and integrity are and tell them which of these concepts apply to each of the problems they are having.

- Authentication – entity authentication prevents unauthorised viewers
- Confidentiality – prevent unauthorised disclosure of payment data
- Integrity – prevent unauthorised modification of news between your server and clients.

Tutorial Q4

4.a) Customers say it is possible that hackers could change the software after it is sent from your server and that they need proof that the software they received has not been modified. What security service do you need? What mechanism could you use?

Integrity/Data origin authentication – be sure where it came from.

Can use digital signature of vendor, or MAC.

(Integrity/data origin authentication can both be considered correct).

Tutorial Q4

4.b) Customers start to falsely claim that they have not received software and want their money back! What security service do you need? What mechanism could you use?

Non-repudiation of delivery. No easy answer for mechanism – client downloads encrypted file. Upon receiving a correct digital signature computed over the downloaded filed you provide them with decryption key (the signature proves they have the entire file)

Tutorial Q5

- 5.a) You are asked to implement a new security mechanism to provided confidentiality for online-chat messages. How could you use standards in building your solution?
- 5.b) What reason would you give your boss/client when asked why you are using existing standards and not developing your own solution from the beginning?

How to use standards?

- Three common ways in use a standard.
- Certification is when a neutral third-party attests to a claim of compliance.
- Compliance may be declared without recourse to third-party certification.
- Use as the basis for new design (use the parts you need)
- Most security standards do not really “require” certification.

Why standards?

"Standards are essential to trade in increasingly competitive markets. They ensure any business offering products, services or processes is:

- cost-effective and time efficient
- commercially viable
- credible
- safe."

The end!

Any questions…