Computer Security

02r. Assignment 1 Review

Paul Krzyzanowski

Rutgers University

Spring 2018

Question 1

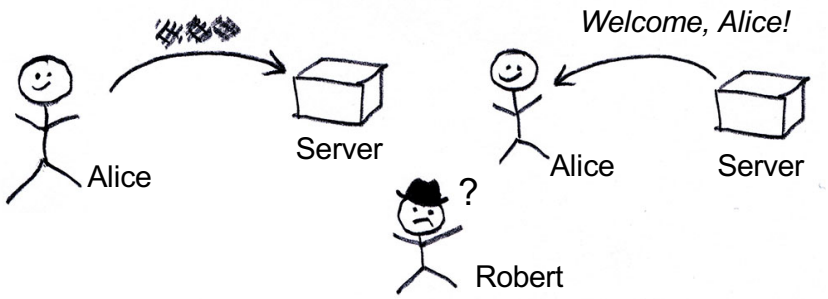
How does *authenticity* differ from *integrity* in computer security?

- Subtle difference. The terms are often used interchangeably.
  - Integrity means that a message is genuine – not forged
  - Authenticity adds a concept of "freshness" – that the message is not a valid message that redelivered
- "Authenticity means integrity plus freshness: you have established that you are speaking to a genuine principal, not a replay of previous messages."

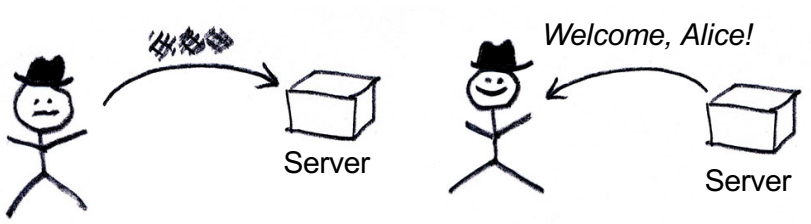
Discussion: replay attacks

- An adversary may not always have the ability to alter – or even decrypt – a message
- However, capturing the message and transmitting it at a later time may create desired outcomes
- This is called a **replay attack**

Example



Robert observes the network messages when Alice logs onto a system … but cannot decipher Alice's message



Robert plays back the same message Alice sent … and gets logged in as Alice

Question 2

Briefly, what is *pretexting*?

pre·text
/ˈprēˌtekst/

noun

a reason given in justification of a course of action that is not the real reason.
"the rebels had the perfect pretext for making their move"
synonyms: excuse, false excuse, ostensible reason, alleged reason; guise, ploy, pretense, ruse
"he used the pretext of looking for his dog to come into our yard"

- Pretexting means using a pretext, lying
  - pretending to be somebody else, usually a person authorized to do something or be privileged to have information that you want.
- Pretexting is often used in social engineering
  - Using deception to obtain get individuals to divulge information

Question 2 [Social Engineering Discussion]

- Social engineering is the most common attack technique for computers
  - Beats out exploits by hardware and software vulnerabilities
- Outsiders want to become insiders to get access to what they need
  - They use social engineering to get insiders to help them
- Phishing emails are the most common way to get account information from insiders
- Social engineering is often a first step to other attacks
  - Account compromise
  - Client-side attacks & compromising personal devices
  - Physical intrusion
  - Destruction

http://www.computerweekly.com/news/4500272941/Social-engineering-is-top-hacking-method-survey-shows

Question 2

Define each of these concisely
(a) What is *policy*?
(b) What is *mechanism*?
(c) What is *assurance*?

- What is policy?
  - A definition of ***what*** you're supposed to achieve
- What is mechanism?
  - The ciphers, access controls, hardware tamper-resistance and other machinery that you assemble in order to implement the policy
- What is assurance?
  - "the amount of reliance you can place on each particular mechanism.

Question 3

What is meant by *assurance* in the context of security?

"The amount of reliance you can place on each particular mechanism."

- Assurance determines how much we can trust a system
- Achieving it involves steps to ensure the system is trustworthy and functioning properly
  - Detailed specifications of behavior
  - Analysis of all components of the design (hardware, software, and any other components)
  - Testing that the implementation will produce the desired behavior in all cases

Question 4

What is meant by *security theater*?

- Measures designed to produce a feeling of security rather than the reality
  - Term created by *Bruce Schneier* in his book *Beyond Fear*
- "Security theater refers to security measures that make people feel more secure without doing anything to actually improve their security."

  – *Beyond Security Theater article*
- A common example is airport security
  - Extra security measures, such as removing shoes, or confiscating liquids do essentially nothing to increase security … but ended up costing huge $$$

Question 4 [Security Theater Discussion]

- A few more examples
  - Entering some buildings
    - A guard will ask to see your drivers license – even though they have no idea who you are and don't record the license
  - Fingerprint scanning
    - Gives some people the illusion of high security when it really isn't
  - Photo ID badges (rather than access cards)
  - Photo ID on credit cards (demonstrated to be completely ineffective)
  - Security guards at a stadium focused on checking for beer or food in bags
    - May blindly ignore real threats (like guns)
  - Thinking your system is safe because you installed an anti-virus program
  - Drug stores scanning your license when you buy Sudafed
    (I assume meth labs have better ways of getting Pseudoephedrine Hydrochloride)

- While security theater makes some people feel better
  - There are real costs
  - There are consequences: if people don't fly because it's more of a pain, they can drive, which is a lot more deadly
  - By focusing security inspections in a few areas, the bad guys can more easily hide things in areas that are not inpected

Question 5

Why does the FDIC recommend that bank employees take periodic vacations?

To give someone else a chance to take over and ensure that there is no ongoing fraud by a specific employee.

- It is "*one element of an institution's overall internal control system*." During the employee's time away, "*their duties and responsibilities should be assumed by other employees*."
  - *FDIC Vacation Policies* letter
- "*So other people at the firm can check out their 'book' of trades and comb them for irregularities, fraudulent trades, and in general to clear away any webs of financial deceit.*"
  - *Marketplace article*

Question 4 [Vacation Policy Discussion]

- Often, ongoing fraud requires continuous presence of the perpetrator
  - Manipulate records
  - Respond to questions

- *Think about Ponzi schemes (e.g., Bernie Madoff)*
  - *Take money from people*
  - *Pretend to invest it & produce "good" returns, thus attracting more investors*
  - *Use money from new investors to pay off old ones if necessary & keep extra money for yourself*
  - *Create fake trading records and forged accounting statements*
  - In the Bernie Madoff case, people suspected that was too much for him to do on his own:
    - James Ratley, president of the Association of Certified Fraud Examiners said, *"In order for him to have done this by himself, he would have had to have been at work night and day, no vacation and no time off. He would have had to nurture the Ponzi scheme daily. What happened when he was gone? Who handled it when somebody called in while he was on vacation and said, 'I need access to money'?"*

https://en.wikipedia.org/wiki/Participants_in_the_Madoff_investment_scandal

"Perpetration of an embezzlement of any substantial size usually requires the constant presence of the embezzler in order to manipulate records, respond to inquiries from customers or other employees, and otherwise prevent detection. It is important for examiners and bank management to recognize that the benefits of this policy may be substantially, if not totally, eroded if the duties performed by an absent individual are not assumed by someone else."

– FDIC Vacation Policies letter

Access Control Discussion

MAC vs DAC

- DAC = Discretionary Access Control
  - The user is in charge of setting file permissions
  - If you own a file, you can set any access permissions you want on it … and even give it away
  - The root user (user ID 0) has the power to change any permissions
- MAC = Mandatory Access Control
  - System owner defines security policies
  - Users cannot override them, regardless of their privilege level
- MAC takes priority over DAC

Subjects and objects

- Subjects access objects
  - They perform actions on objects
- Subjects are users and processes
  - Processes run with the ID, and hence privileges, of a user
- Objects are resources
  - Typically files and devices
  - They do not perform operations

SELinux (Security Enhanced Linux)

- Originally a kernel patch created by the NSA to add MAC to Linux
- Supports three MAC models:
  - Type Enforcement (TE)
  - Role-Based Access Controls (RBAC)
  - Multi-Level Security (MLS) – the Bell-LaPadula Model
  - Multi-Category Security (MCS)
    - Extension of MLS to define categories within a security level
- There other security models and implementations available in other distributions!

Type Enforcement (TE) on SELinux

- Every subject (e.g., user) and object (e.g., file) on a system is assigned a label
  - Processes are subjects – they run with the privileges of a user
  - A label assigned to a process is called its domain
  - A label assigned to an object (file) is called its type
- Access control rules
  - The security administrator defines what access a domain (subject) can perform on a type (object)

```
allow userdomain bin_t:file: execute;
allow user2domain bin_t:file: read;
```

    - Allows users with the label "userdomain" execute rights for files with the label "bin_t" and allows users with the label "user2domain" read rights for those files

RBAC in SELinux

- Role-Based Access Control (RBAC) is integrated with the TE model
- Role-based access is specified in terms of TE
  - Management interface
  - Manage privileges based on roles users may assume
  - Control operations that a role can perform
- Essentially the same as TE but goal is to simplify labeling
  - A "role" is a layer of indirection: it groups users and file operations
  - Easier conceptually than setting permissions between arbitrary domains and types

MAC can reduce the need for root

- Traditionally the *root* user has supreme power
  - But you need supreme power to do *any* administrative task
- Models such as TE and RSBAC allow you to define classes of users that can perform certain operations and access certain files
  - E.g., you can define a network administrators who can modify network configuration files and run network commands

The end