

Dear student,

The goal of this lab assignment is to give you practical experience in security. The assignment consists of the following parts:

1. Hands-on exercises in penetration testing.
 - a) Physical penetration testing
 - b) Digital penetration testing
2. Writing, reviewing and presenting a research paper.

The easiest way for an adversary to get the data is through social engineering. During the first exercise (1a), you will need to gain possession of a specific locked notebook somewhere on the University of Twente campus. The goal of the physical penetration testing exercise is to make you aware of the social engineering skills and physical activities an attacker can use to get sensitive data. After this exercise you should have a clear overview of social engineering and physical security, and know the threats that arise from them. This exercise is assessed on a group basis and contributes 24% to the overall grade of the course.

During the digital penetration testing exercise (1b), you will need to get access to remote servers. The goal of the exercise is to give you an overview of the current techniques in compromising a system. After the exercise, you should be able to use the most common tools used in penetration testing, and their capabilities. The exercise is assessed on a group basis and contributes 1% of the overall grade of the course.

During the coming weeks you will choose a paper topic from a list (2). The goal of the exercise is to improve your professional and academic skills in critical reading, problem solving, writing, reviewing, and presenting a research paper. After the assignment, you should be able to approach a problem, systematically, search for literature, find a solution, validate the solution, and formally represent it in a scientific paper. At the end of the course you will present the paper at a mini conference where the paper will be marked by your the peers. The paper is assessed on a group basis and contributes 25% to the overall grade of the course.

We hope you will enjoy the course as much as we enjoyed preparing it.

List of paper topics:

1. Ranking Attack Scenarios
2. Ethics in Physical Penetration Testing
3. The Personal Chief Security Officer
4. Efficient Implementation of Searchable Encryption
5. Data-based Access Control
6. Privacy Breach from Inter-OSN Inferences
7. Security and Privacy in Body Sensor Networks
8. Tracking Insiders
9. Presenting Soft Policies
10. Alternate Password Entry Methods for Mobile Devices

Time scale:

- 30 August: Choose team, team name, laptop target.
Scout the target.
- 6 September: Generate attack scenarios, Hand in abstract.
Get the scenarios approved and start executing them.
- 13 September: Execute the attacks. Hand in introduction and table of contents.
Execute the attacks.
- 20 September: Get second target.
Scout the target.
- 27 September: Generate attack scenarios and get them approved.
- 4 October: Penetration test on UT servers.
Penetration test on UT servers.
- 11 October: Penetration test on UT servers.
- 18 October: Execute the attacks. Paper draft.
Execute the attacks.
- 25 October: Execute the attacks.
Execute the attacks.
- 8 November: Paper submission
- 15 November: Reviews
- 29 November: Slides

Overall grading:

Stage I and III	24%	Graded by assistant, students
Stage II:	1%	Graded by assistant
Paper:	25%	Graded by professor, assistant, students
Written exam:	50%	Graded by professor

Grading of stage I and stage III (0 to 100 points):

1. Well written attack scenarios 30 points
2. Gain possession of notebook 50 points
3. Well written traces 10 points
4. Take recording of the attacks 10 points
5. "Innovative attacks" extra credit 10 points

Grading of stage II (0 to 100 points):

1. Captured flag 50 points
2. Well written traces 50 points
3. First team to finish extra credit 10 points

Grading of paper (peer review):

1. To be defined with Prof. Hartel.

Motivation

Insiders are people that have initial knowledge and credentials from the organization. When malicious, these people can cause much more damage than unauthorized adversaries. Moreover, malicious insiders are hard to detect, because they already have knowledge of the logs and which actions are logged, and which not.

Problem

We developed a tool, Portunes, which generates attack scenarios for a given configuration. However, a single configuration can have even a hundred potential attack scenarios. How to rank these scenarios?

Solution

1. Define criteria for ranking the attacks.
2. Implement the ranking in Portunes.

Needed skills

1. Knowledge in Java.
2. Good scientific writing skills

Related work

Dimkov, T. and Pieters, W. and Hartel, P., Portunes: representing attack scenarios spanning through the physical, digital and social domain *ARSPA-WITS*, **2010**

Motivation

Digital penetration testing is taught in many colleges as part of master programs. But there are no classes for physical penetration testing and using social engineering as a method in penetration testing. We believe the main reason for this is the ethical issues that rise from the activities

Problem (knowledge problem)

Is it beneficial to teach physical pen-testing and social engineering at a University?

Solution

This is just one approach. Please use your own intuition how you would like to solve the problem.

1. Define criteria which define the advantages and disadvantages of teaching physical penetration testing.
For example:
 - a. Advantage: Makes the students aware of threats that originate from social engineering and physical intrusions which will help them in future to better combat adversaries.
 - b. Disadvantage: The students might turn into adversaries with will use the knowledge in social engineering and physical intrusions to achieve malicious goals.
2. Provide information why the criteria are good and what are its weaknesses.
3. Based on these criteria, come to a conclusion why teaching physical penetration testing / social engineering is good or bad.
4. Use the same criteria to measure cost/benefits of teaching digital penetration testing and compare the results.
5. Validation:
 - a. Ex: Do questioners on the other students before and after the penetration testing exercises (physical and digital) and use the scale to see if it reflects the reality.

Needed skills

1. Some background in ethics.
2. Excellent skills in writing scientific papers.

Related work

Barrett, N. Penetration testing and social engineering Hacking the weakest link *Information Security Technical Report, Elsevier*, **2003**, 8, 56-64 DOI: [10.1016/S1363-4127\(03\)00007-4](https://doi.org/10.1016/S1363-4127(03)00007-4)

Logan, P. & Clarkson, A. Teaching students to hack: curriculum issues in information security *SIGCSE, ACM*, **2005**, 37, 157-161 DOI: [10.1145/1047124.1047405](https://doi.org/10.1145/1047124.1047405)

Pashel, B. Teaching students to hack: ethical implications in teaching students to hack at the university level *InfoSecCD '06: Proceedings of the 3rd annual conference on Information security curriculum development, ACM*, **2006**, 197-200 DOI: [10.1145/1231047.1231088](https://doi.org/10.1145/1231047.1231088)

Endicott-Popovski, B. & Lockwood, D A Social Engineering Project in a Computer Security Course *Academy of Information and Management Sciences Journal*, **2006**, 9

Background

As consumers' lives are revolving more and more around IT, they are facing serious security and privacy risks. But in spite of this, consumers are incapable of securing themselves. They forget to make regular backups, do not check their online banks statements and put very sensitive data on social networking sites.

At the same time, consumers are overwhelmed by well-intended advice and tools that can supposedly remedy their problems. Microsoft offers free anti-virus, the New York Times offers a three-step remedy for Facebook privacy, governments spend a great amount of money on increasing consumer 'awareness', Apple sells dedicated devices for backups, and the open source community develops software to help consumers manage their passwords.

Unfortunately, implementing, or even finding all such advice and tools would likely take more time every day than the average person is on-line. Worse, there is no proof that these 'solutions' actually work, and they will certainly not work in the near future, as consumers' use different systems and applications from day to day, and new threats emerge. As a consequence, consumers will either spend too much or too little time on security, erring on the side of too little, and their effort is ill-focused, as they do not oversee the entire range of options and do not understand the tradeoffs involved.

Problem analysis

What consumers need most urgently is a security process: they need a structured way of dealing with the security risks they face. Executing this process is something that a government cannot do, and a government cannot make it unnecessary either by privacy legislation or consumer protection. Neither can businesses automate it completely, as the process starts with the consumer's own objectives. Ultimately responsibility for security should be placed into the hands of the consumers themselves: they must be 'in control' of their own IT devices, services and data.

Assignment

You will design and build the 'personal Chief Security Officer', which helps consumers to stay in control. The tool allows consumer to define their goals, enter the devices and data they have and informs them about the threats they face, and the mitigations they can take.

Related work

Bits of Freedom. [Online Zelfverdediging in 5 Clicks](#).

Cleeff, A. van (2010) *A Risk Management Process for Consumers*. Technical Report TR-CTIT-10-25, Centre for Telematics and Information Technology, University of Twente, Enschede. ISSN 1381-3625

International Organization for Standardization (ISO/IEC). ISO/IEC 27001:2005 Information technology {Security techniques { Code of Practice for Information Security Management, 2005.

ISACA. [Cobit V4.1 and V5.0](#).

Motivation

It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. This makes it impossible for unauthorized users or attackers to access the data but at the same time an authorized user cannot search for specific data, so one has to sacrifice functionality for security. It is desired to support searching functionality without any loss of data confidentiality.

We developed a new search scheme based on Bloom filters and want an efficient implementation for real life usage.

Task

We aim to implement our Searchable Encryption Scheme, based on Bloom filters, in a very efficient way, where efficiency is measured in speed.

1. Implement our Searchable Encryption Scheme in an efficient way
2. Performance tests on small amount of data
3. Test different data structures and databases

Related work

Bloom, B. H. Space/Time Trade-offs in Hash Coding with Allowable Errors *Commun. ACM*, 13(7):422-426, 1970

Eu-Jin Goh. Secure indexes. Cryptology ePrint Archive, Report 2003/216, 2003.

Motivation

In social networking sites, people want to share more information with people who know them well. Following this logic, users could then grant access to their profile based on what others already know about the profile. Recently, the DIES group published a paper on what we call data-based access control. In this approach, access to information is protected by the information itself. This has also been termed self-encryption.

Assignment

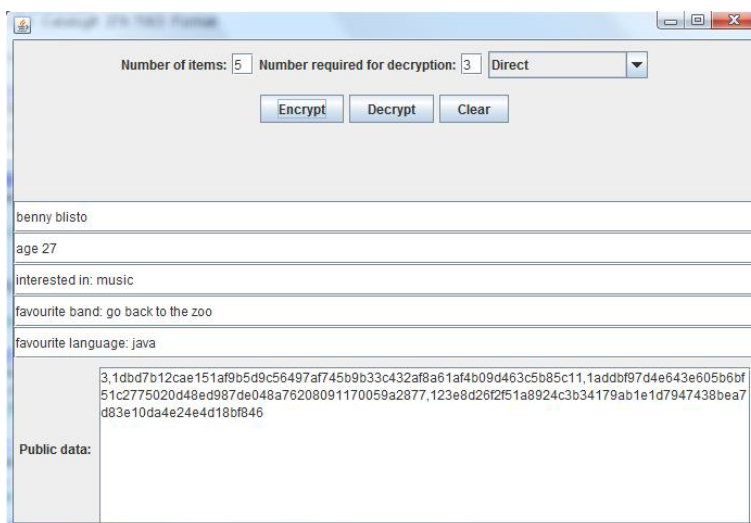
In this project, you will investigate the possibilities of applying data-based access control in social networking sites. The assignment consists of two parts:

1. First, you will specify types of policies that are suitable for social networking sites. In a very simple policy, we may have three pieces of information a, b and c, and one can access the third one if one already knows the other two, but more complicated policies are possible.
2. Secondly, you will build a prototype system for social networking based on the Java code for encryption techniques that we will make available. The user interface should mimic a simple social networking site.

Required knowledge and skills:

- basic understanding of various encryption techniques;
- programming in Java, including user interface design.

Implementation



A snapshot of the current Java implementation. Turn this into a “real” social networking application!

Related work

Paper on data-based access control by Pieters and Tang:
<http://eprints.eemcs.utwente.nl/15728/>

Motivation

Online social networks have become an important communication platform for internet users to advertise selves, share information, and find kindred spirits. Though they share the same basic theme, OSNs may have quite different focuses. For example, LinkedIn mainly aims at professionals, while Match.com mainly aims at dating services for singles. There are also OSNs, such as Facebook, Bebo, and Myspace, which are general-purpose instead of having a specific focus.

Researchers have shown that users' privacy may be in danger because of their information disclosure in OSNs. Service providers of OSNs have adopted a variety of measures to improve the privacy situation. However, it is widely believed that the existing measures are far from adequate from providing a satisfactory privacy guarantee. As an example, both Jop's work in analyzing Hyves and Arjan's work in analyzing Facebook demonstrate that sensitive information leaks from current OSNs even if the users have attempted to apply the privacy protection measures offered by the service providers.

Goal

Validate the hypothesis that, for users, more sensitive information can be revealed by inferences among different OSNs. The main rationale behind this is that many users in fact participate in multiple OSNs, where they will disclose different sets of personal information and their profiles are inter-connected, and some information considered sensitive in one OSN may be considered as public in another OSN. An additional reason is that human users are not consistent in enforcing their privacy policies in the sense that they may indirectly disclose sensitive information in their OSN activities.

Solution

1. Select the candidate OSNs for our analysis. Facebook and Hyves are two obvious choices, but it is also necessary to consider others to find the most suitable targets for our purposes.
2. Extract users' information from the selected OSNs either through the APIs provided by the service providers or by any other possible means.
3. Correlate the harvested information from the different OSNs, and construct inferences from there.
4. Apply some data mining algorithms to the harvested data to figure out more interesting information.

Related work

Bachelor thesis about inferring information from Hyves:
<http://referaat.cs.utwente.nl/new/paper.php?paperID=604>

Motivation

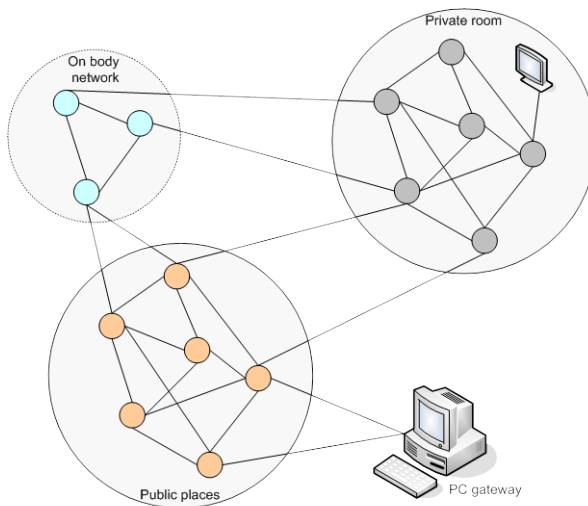
The Body Sensor Network (BSN) field is an interdisciplinary area, which could allow inexpensive and continuous health monitoring with real-time updates of medical records via Internet. A number of intelligent physiological sensors can be integrated into a wearable wireless body area network, which can be used for computer assisted rehabilitation or early detection of medical conditions.

Challenge

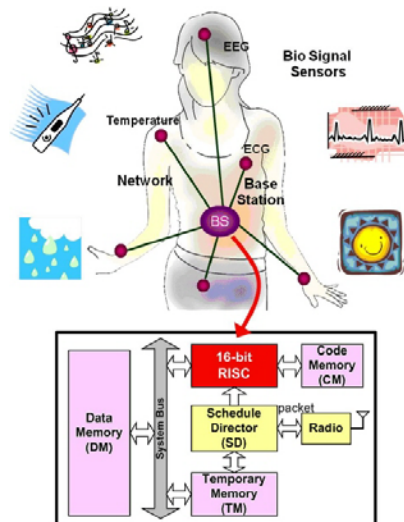
As a typical e-Health application, security problems with the use of BSNs could include:

- Interoperability.
- System and device-level security.
- Patient Privacy.
- Sensor validation.
- Data consistency.

Example



a) BSN Network Model



b) Body Sensors

Evaluation

1. Build up an interoperable BSN use case which is close to practice.
2. By considering related e-Health regulations and best practice, define proper interoperability, security and privacy for the defined use case.
3. By following the use case and the definitions, analyze the implications of its interoperability, security and privacy. How can we balance them under the current (security) infrastructure? Moreover, how can we achieve them by improving the current infrastructure?

Related work

KALwEN: A New Practical and Interoperable Key Management Scheme for Body Sensor Networks
<http://eprints.eemcs.utwente.nl/14573/>

Motivation

Insiders are people that have initial knowledge and credentials from the organization. When malicious, these people can cause much more damage than unauthorized adversaries. Moreover, malicious insiders are hard to detect, because they already have knowledge of the logs and which actions are logged, and which not.

Problem (knowledge problem)

How to formally present logging of insider actions?

Solution

In DIES we developed a framework for representing insider actions. We want to expand the framework with logging capabilities.

1. Formally define the logging capabilities of the system.
2. Implement the logging capabilities in Portunes.

Needed skills

1. Knowledge in Java.
2. Good background in formal methods.

Related work

Probst, C. & Hansen, R. An extensible analyzable system model *Information Security Technical Report, Elsevier*, **2008**, *13*, 235-246

Dimkov, T. and Pieters, W. and Hartel, P. Portunes: representing attack scenarios spanning through the physical, digital and social domain *ARSPA-WITS*, **2010**

Motivation

Insiders are people that have initial knowledge and credentials from the organization. When malicious, these people can cause much more damage than unauthorized adversaries. Moreover, malicious insiders are hard to detect, because they already have knowledge of the logs and which actions are logged and which not.

Problem

In Portunes, all policies are either completely enforced or not. This is not always true for soft policies on people, who sometimes might break a policy, and other times faithfully follow it. How to present these soft policies on people?

Solution

1. Add weight on policies in Portunes.
2. Rank the attack scenarios based on the probability of the scenario happening.

Needed skills

1. Knowledge in Java.
2. Good formal methods

Related work

Dimkov, T. and Pieters, W. and Hartel, P. Portunes: representing attack scenarios spanning through the physical, digital and social domain *ARSPA-WITS*, **2010**.

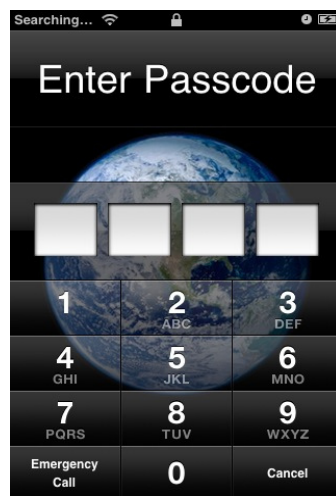
ALTERNATE PASSWORD ENTRY METHODS FOR MOBILE DEVICES

Supervisor: STEFAN DIETZEL

MOTIVATION

Mobile devices have become an integral part of our communication habits. The more we use such devices to communicate with friends and colleagues, the more sensitive information we store on them, calling for good user authentication. However, a good password entry method for mobile devices is not easy to design. Due to the constrained display size of mobile devices, users typically type slower than on regular keyboards and make more errors. That makes it easier for attackers to observe every character that is typed in. Moreover, the increased number of typing mistakes forces mobile operating system providers to lessen the obfuscation of the password that is entered, thus further increasing the risk of someone observing the typed combination.

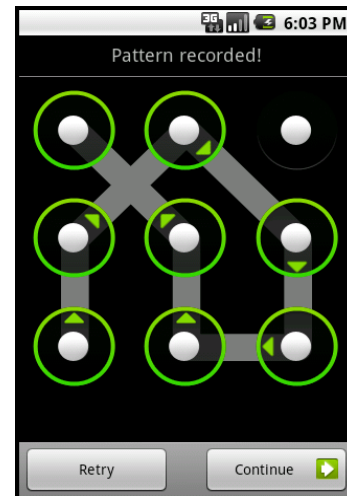
EXAMPLES



(a) iPhone unlock screen.



(b) iPhone password entry.



(c) Android unlock gesture.

(a) Many iPhone applications use a numeric pad to enter passwords, making it easy for a shoulder-surfer to follow the finger movement. (b) The standard password entry method for alphanumeric passwords on the iPhone is to hide all but the last character of the password while typing. While this approach makes it harder to observe the typed password using finger movement, an attacker can still obtain the full password using the sequence of shown last characters. (c) Newer versions of Android allow users to use a unique combination of swipes to unlock the phone.

RESEARCH TARGETS

Your goal is to assess the current state of the art in alternate password entry methods for mobile devices. You will first collect several current proposals and then compare them using a number of metrics. Possible metrics include classic password strength metrics, such as entropy, as well as the ease of use for the user and how easy it is for shouldersurfers to obtain the entered password. Finally, you can use your gained knowledge to propose an own password scheme, which is either entirely new or enhances existing ones. You can evaluate your proposed scheme using a proof-of-concept implementation. Note that, while you need to address all research targets to some extent, you are free to put your focus on an aspect that particularly interests you.

RELATED WORK

1. Paul Dunphy, Andreas Heiner and N. Asokan, "A Closer Look at Recognition-based Graphical Passwords on Mobile Devices", *Symposium on Usable Privacy and Security (SOUPS) 2010*, July 2010, Redmond, WA USA.
2. Davis, D., Monroe, F., and Reiter, M. K. 2004. "On user choice in graphical password schemes." In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13* (San Diego, CA, August 09 - 13, 2004). USENIX Security Symposium. USENIX Association, Berkeley, CA, 11-11.
3. Roth, V., Richter, K., and Freidinger, R. 2004. "A PIN-entry method resilient against shoulder surfing." In *Proceedings of the 11th ACM Conference on Computer and Communications Security* (Washington DC, USA, October 25 - 29, 2004). CCS '04. ACM, New York, NY, 236-245.
4. N.L. Clarke, S.M. Furnell, "Advanced user authentication for mobile devices," *Computers & Security*, Volume 26, Issue 2, March 2007, Pages 109-119, ISSN 0167-4048.

(You should use the given list to start your own research explorations rather than to rely on it alone.)

Appendix C:

INFORMED CONSENT

GW.07.130

I, (*name of student*)

agree to perform penetration tests for

Dimkov Trajce

I understand that the participation of is completely voluntary. At any time, I can stop my participation.

I fully oblige to the following rules of engagement:

1. I will only execute attacks that are pre-approved by the researcher and only to an assigned target.
2. I am not allowed to cause any physical damage to UTwente property, except for Kensington locks.
3. I am not allowed to physically harm any person as part of the test.
4. I will video or audio record all my activities while interacting with people during the penetration test as a proof that no excessive stress or panic is caused to anyone.
5. If I am caught by a guard of police officer, I will not show any physical resistance.

Signature of researcher:

Date:

Signature of student:

Date:

Get out of jail card

The student _____ is performing a penetration test in the period between 6th and 27th of September. The test is approved by Dimkov Trajce and the security management of UTwente. In case of being caught while executing the penetration test, please contact G.M. van Diessen tel: 0534892259 or Dimkov Trajce tel: 0624685503 at any time of the day.

Researcher signature
