

Open Wireless Networks on University Campuses

Risk Assessment

Kjell Jørgen Hole
NoWires Research Group
Department of Informatics
University of Bergen

Last updated November 3, 2011

Outline

- Authentication vs. usability and privacy
- Open wireless networks on campuses
- Risk assessment considering
 1. illegal downloads
 2. cracker attacks
 3. negative press coverage

Authentication, usability, & privacy

definitions and trade-offs

Information system defined

- An **information system** is a collection of computers, communication networks, and storage equipment used to process, transport, and store information
- we refer to an information system offering wireless access to a wired network infrastructure as a **wireless network**

Authentication in an information system

- **Individual authentication** is the process of establishing an *understood* level of confidence that an identifier, e.g. a name, refers to a particular individual
- the authentication is **strong** if the resulting level of confidence is high

5

Usability defined

- The **usability** of an information system is mainly determined by
 1. how simple it is for users to achieve their goals the first time they use the system, and
 2. how quickly they can perform tasks after a learning period

6

Degrees of usability

- The usability is **high** if the users intuitively understand how to utilize the system to obtain the desired goals
- The usability is **low** when the users make many mistakes and have problems achieving their goals

7

Authentication vs. usability

- Authentication mechanisms reduce usability because
 - they're seen as intrusions keeping the users away from their primary tasks
 - they require users to remember secrets and/or possess authentication devices

8

Privacy defined

- We define **privacy** as the right of an individual to decide when and how *sensitive* personal information should be revealed
- People differ on what constitutes sensitive personal information
 - **examples:** credit card numbers and passwords

9

Privacy vs. authentication

- Authentication establishes a link between an individual and his or her personal information stored in an information system
- This connection can be exploited by crackers and identity thieves to do serious harm

10

Limit the use of individual authentication

Individual authentication should only be used when it is really needed because it reduces usability and introduces privacy concerns

11

Open wireless networks

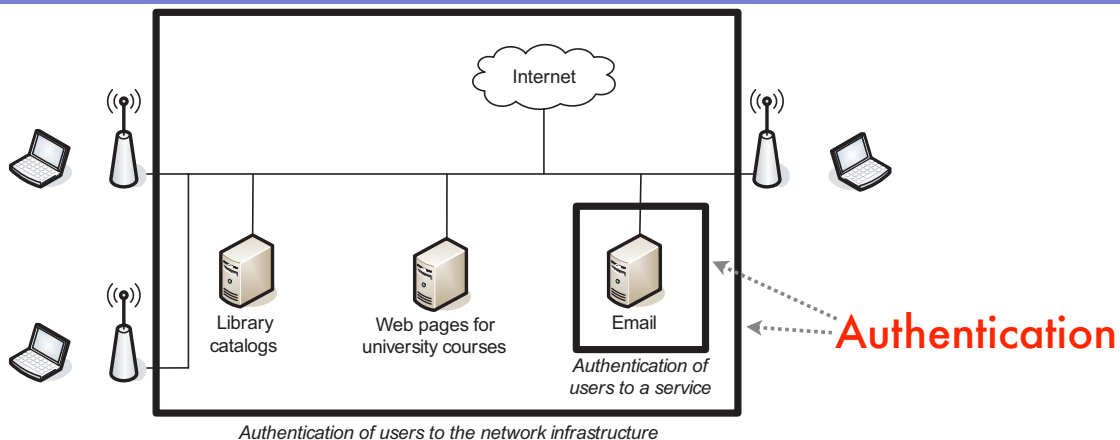
definition and advantages

Open information system

- An **open** information system grants users access to the network infrastructure without any form of authentication
- services providing sensitive information still require authentication
- In the remainder of this talk we'll study **open wireless university networks**

13

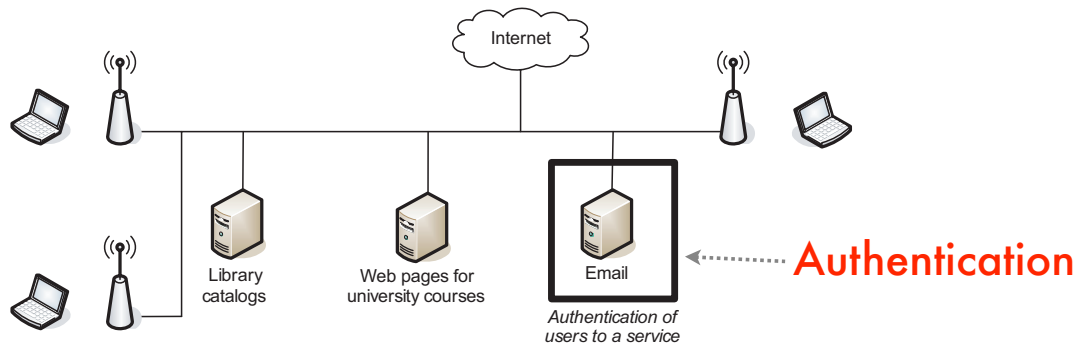
Closed network with boundary authentication



- The resources inside the network perimeter are only made available to a user after a successful authentication

14

Service level authentication



- An open network gives the users unrestricted access to the Internet, library catalogs, and web pages with course information
- The email server with sensitive information still requires individual authentication

15

Increased usability

- Open wireless networks can
 1. increase the usability because students and faculty do not need to remember passwords and/or carry authentication devices
 2. give short-term guests easy Internet access without the need for new user accounts
 3. provide the public with effortless access to online catalogs maintained by university libraries

16

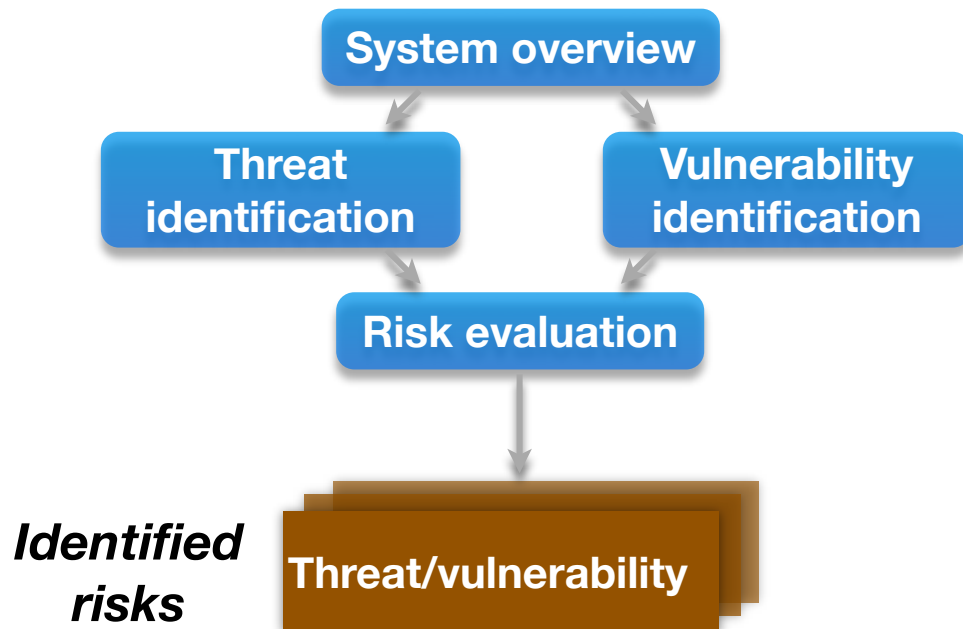
Increased privacy

- If users authenticate to a wireless university network, then the IT department can track users' movements and activities on campus
- Data from many network sessions can be combined to build **user profiles** including the users' preferred whereabouts
- An open wireless network reduces these privacy concerns

17

Risk assessment

with examples



19

Vulnerabilities and threats

- A **vulnerability** is a flaw in the design or a bug in the implementation of an information system
- A **threat** is an adversary with the capabilities and the intentions to exploit a vulnerability

20

Risk

- A **risk** is the negative impact of a vulnerability exploited by a threat, considering **likelihood** and **impact** of occurrence

21

Likelihood defined

Likelihood level	Likelihood definition
High	Very motivated and skilled threats. Controls are inefficient.
Medium	Motivated and competent threats. Controls slow down attacks.
Low	Threats lack motivation or skills. Efficient controls exist.

Subjective

22

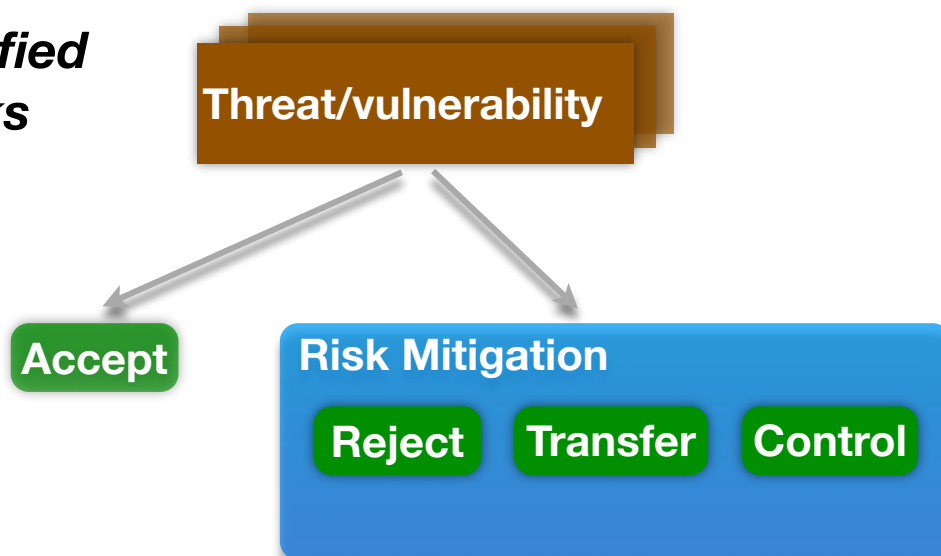
Impact defined

Subjective

Magnitude of impact	Impact definition
High	Very costly loss of major assets or highly priced damage to a stakeholder's interests.
Medium	Considerable losses of assets or significant damage to a stakeholder's interests.
Low	Minor losses of tangible assets or small damages to a stakeholder's interests.

23

Identified risks



We do not discuss risk mitigation. However, we consider open networks with and without controls

24

Illegal downloads

Threat and vulnerability discussion

- Illegal downloading of music and movies goes on in student dorms
 - employees also misuse university networks
- When individual authentication is removed from the network perimeter, the temptation to use the network for illegal downloads may increase

Efficient controls

- A university introducing an open wireless network must create rules to govern network usage
- The rules must reserve the right to prosecute any user who causes economic loss or damage to the university's reputation
- The rules will limit misuse from students and employees, but not eliminate it

27

Additional controls

- Possible to monitor and log network traffic to stop unwanted activity
 - monitor traffic, not users
- Many illegal downloads can be "filtered out" by only allowing traffic on certain network ports
- Special filters maintained by the police can be used to stop child pornography

28

Risk assessment

The likelihood vary in different open networks. We consider the likelihood and impact to stakeholder in two university networks, with (and without) controls.

Stakeholder: *large international recording company*

Vulnerability	Threat	Likelihood	Impact
Illegal downloads	regular users	Medium (High)	Low (Low)

Example only

Terminal-to-terminal attacks

T & V discussion

- When students and faculty utilize mobile terminals, it's possible for a cracker to attack a terminal via an access point or directly via a wireless link
- A cracker may also attack from the wired infrastructure. He could for example
 - install rogue access point running malware, or
 - exploit access point installed by a user

31

Efficient controls

- Run personal firewalls and up-to-date antivirus programs on mobile terminals
- While regular users are less likely to install rogue access points in open networks, the IT staff must continue to watch for rogue access points
- There exist software tools to help finding rogue access points

32

Risk assessment

The likelihood vary in different open networks. We consider terminals with (and without) efficient controls.

Stakeholder: *owner of terminal*

Example only

Vulnerability	Threat	Likelihood	Impact
terminal attack	cracker	Low (Medium)	Medium (Medium)

Attacks on local networks

T & V discussion: non-sensitive services

- When users don't have to authenticate to the network infrastructure, a cracker may be able to introduce false services such as
 - fake lecture notes
 - bogus research papers
 - forged university web pages

35

Efficient controls for non-sensitive services

- Install anti-virus software and firewalls on servers
- run auditing programs to record the activities of users and carry out regular reviews of logs to detect illegal activity
- Be prepared to quickly reinstall and secure web servers

36

Risk assessment

The likelihood vary in different open networks. We consider two networks, with (and without) controls.

Stakeholder: *university owning network*

Example only

Vulnerability	Threat	Likelihood	Impact
false services	cracker	Low (Medium)	Low (Low)

37

T & V discussion: sensitive services

- Services with sensitive information must authenticate all users
- Since it is easy to “sniff” passwords on unencrypted wireless links, password-based authentication also requires the use of end-to-end encryption

38

Efficient controls for sensitive services

- Authentication and end-to-end encryption can be obtained using
 - VPN (Virtual Private Network)
 - SSH (Secure Shell)
 - SSL (Secure Sockets Layer)
- The steps suggested for non-sensitive services should also be applied

39

Anonymous attacks on remote networks

T & V discussion

- Removing the authentication from the network perimeter can make it possible for a cracker to carry out anonymous attacks on information assets anywhere on the Internet
- these attacks include music and software piracy, identity theft, denial-of-service attacks, spam, phishing, and attacks on remote machines

41

Spoofing of MAC addresses

- A cracker can spoof the MAC address of his mobile terminal to get anonymous Internet access via an open network
- However, an open campus network doesn't represent a major new attack vector because there already exist many open Wi-Fi networks

42

Existing open networks

- A Wi-Fi network is said to be open if the WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) security protocols aren't used
- Roughly 40% of the Wi-Fi networks in the city of Bergen, Norway were open in 2006

43

Tor

- Tor, tor.eff.org, also enables crackers to carry out anonymous attacks over Internet
- Tor consists of a network of computers, or proxies, used to reroute people's Internet traffic
- Multiple layers of encryption inside the Tor network protect the traffic from eavesdropping

44

Open network and Tor (1)

1. The owner of a wireless network cannot determine what remote system a cracker is accessing
2. The wireless network owner cannot determine the content of communication between the cracker and the remote system
3. The owner of the remote system cannot determine the originating network of the cracker

45

Open network and Tor (2)

4. If a cracker reveals his identity to someone on the Internet, then that someone can still not determine the cracker's home network
5. It is hard for the IT department to determine which mobile terminal the cracker is using on a campus with many active terminals

46

Efficient controls

- The risk associated with anonymous Internet access from an open university network can be reduced, but not eliminated, by introducing network monitoring
- The remaining risk is limited because a cracker is more likely to choose an open network owned by a private party rather than attempt to exploit an open network monitored by a large IT department

47

Ethical dilemma?

- While Tor was created to anonymize web browsing and publishing, instant messaging, and other applications using the TCP protocol, Tor may also be used by crackers
- Hence, the decision to install an open campus network is somewhat of an ethical dilemma

48

Risk assessment

The likelihood vary in different open networks. We consider two networks, with (and without) controls.

Stakeholder: *university owning network*

Example only

Vulnerability	Threat	Likelihood	Impact
anonymous attacks	cracker	Low (Medium)	Medium (Medium)

Negative press coverage

T & V discussion

- A university may worry that security breaches on an open network will lead to negative press
- Mandatory authentication of all users is therefore introduced to
 - make successful attacks less likely, and
 - deflect criticism away from the IT department to the users
- Bad news are kept secret from the press

51

Efficient controls

- In the long run it is better to build trust by being honest and open than to try to hide bad news. The IT department should
 - cooperate with the press to reduce the negative impact of an incident
 - explain what happened and outline the steps it'll take to improve the security in the future

52

T & V discussion

- A university information system contains **personal information** such as
 - medical information
 - social security numbers
 - annual salaries
 - student grades
 - disciplinary actions

53

Efficient controls

- Very sensitive personal information should not be available on open wireless network at all
- Services providing sensitive information must use strong authentication

54

Risk assessment

The likelihood vary in different open networks. We consider two networks, with (and without) procedures to inform the press.

Stakeholder: *university owning network*

Example only

Vulnerability	Threat	Likelihood	Impact
bad press	journalists	Low (Medium)	Low (Medium)

55

Final discussion

Discussion (1)

- There is no absolutely correct answer to the question about whether or not to install an open wireless network on a university campus
- To make a decision on whether to deploy an open wireless network, the associated risks must be weighted against the advantages

57

Discussion (2)

- An open network can improve the education of students and make important information easily available to both faculty and the general public
- Further, the legitimate privacy requirements of guests, students, and faculty make a strong case for for allowing an open network

58

Discussion (3)

- An IT department worried about the risks associated with an open network can monitor and filter the traffic
- Telling the truth, and thus building trust, can reduce the impact of negative press reports
- Experience with an open wireless network at the Department of Informatics, University of Bergen, indicates that the overall risk is acceptable in some cases

59

References

- K. J. Hole, L.-H. Netland, Y. Espelid, A. N. Klingsheim, H. Hellesteth, and J. B. Henriksen, "Open Wireless Networks on University Campuses," *IEEE Security & Privacy*, July / August 2008
- G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems," NIST Special publication 800-30, July 2002