

SECURITY AND PRIVACY

1

Definitions

- What is security?
 - Protection of information and property from theft, corruption, or natural disaster
 - Allowing the information and property to remain accessible and productive to its intended users.
- What is privacy?
 - The desire of personal privacy concerning the storing, repurposing, providing to third-parties
 - Displaying of information via the Internet.

2

Why do we need security?

- To protect money
 - Banks, Financial transactions
- To protect information
 - Government agencies
- To ensure personal safety
 - Airlines, trains, bridges
- To keep the bad guys out
 - Or just the nosy...

3

What is the price of security?



Ease of use

- With more security comes:
 - More checks
 - Is what you are doing legit?
 - More chances for error
 - Entering wrong password
 - Differing rules
 - One site wants letters and numbers
 - Another wants a special character
 - More frustration

Performance

- The more security you have in place
 - The more activities your computer is doing to check things
 - These activities take resources
 - And your computer slows down...
- You are entering more information to authorize
 - And your performance slows down...

Inability to act

- Sometimes you just can't do what you are entitled to do,
 - Forgotten password
 - System imposed restrictions
 - 3 times enter incorrect password
- Security servers are often different than content servers
 - Differing point of failure

7

Who are the bad guys?



8

Malware

- Short for malicious software
- Programs designed to
 - Disrupt or deny operation
 - Gather information
 - Gain unauthorized access
- Software is considered malware based on the intent of the programmer

9

Virus

- A computer virus attaches itself to a program or file
- Enables it to spread from one computer to another, leaving infections as it travels.
- Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer

10

Worm

- Similar to a virus by design and is considered to be a sub-class of a virus.
- Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.
- A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

11

Trojan Horse

- At first glance will appear to be useful software
 - Do damage once installed or run on your computer.
- Results vary
 - From the merely annoying to causing serious damage
 - Can also create a backdoor on your system
 - Backdoors used to create botnets
- Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

12

Spyware

- **Collects** small pieces of information about users without their knowledge.
 - Surfing habits
- Can install additional software
 - Keyloggers
- Change web browser activity
 - Home page
- **SLOWS DOWN YOUR SYSTEM**
 - Additional activity
 - Change computer settings

13

Adware

- Software which displays advertisements
- User-consented
 - Alternative to registration fees.
- The other kind...
 - Displays advertisements related to what it finds from spying on users.
 - Example is Gator from Claria Systems.
 - Visited Web sites frequently install Gator on clients
 - It directs revenue to the installing site and to Claria by displaying advertisements to the user.
 - You get pop-up advertisements

14

Back to security..



15

How do we achieve security?

- Physical
 - Lock it down
- Authentication
 - Are you who you say you are?
- Authorization
 - Are you allowed to do what you are trying to do?

16

Physical security

- Armed guards, gates, etc.
 - Not so good
- Possession
 - Adequate for most of us
- Lock and keys, badges
 - Good for large things
 - Computer lab

17

Authentication

- Badges, passports
 - Physical possession
- Passwords
 - Differing degrees of difficulty
- Biometrics
 - Fingerprints, retinal scans
- Captcha keys
 - Are you a bot?
- Digital certificates
 - Am I talking to the real site?

18

Authorization

- Access control
 - Tying an object to permissions
 - Can be done individually or to a role
 - Can be logical or physical
- Role-based access control
 - Person is assigned "roles"
 - The roles are assigned permissions
 - Much easier to administer

19

Privacy



20

What is privacy?

- The ability to keeping information from being shared without your approval
 - Personally Identifying Information (PII)
 - Name
 - Social Security number
 - Bank account number
 - Non-PII information
 - Surfing habits
 - Purchasing habits

21

What type of info?

- Healthcare records
- Criminal justice investigations and proceedings
- Financial institutions and transactions
- Biological traits, such as genetic material
- Residence and geographic records
- Ethnicity, gender, sexual preference
- Many, many more

22

Does privacy exist anymore?

- Unfortunately, the horses have left
 - We can close the barn door, but...
 - We were in such a rush to make the data available, privacy was short-circuited
- A lot of factors are not under your control
 - Other people's data
- Significant number of experts believe that privacy no longer exists

23

Why has privacy disappeared?

- On-line shopping, surfing
 - Habits are recorded
- Identifying information
 - IP addresses, PIP
- Public surveillance
 - Cameras, facial recognition software
- Legislation
 - Terrorism, public right to know

24

Is it hopeless?

- Small subset of people with access
 - Like to believe those people require authorization
- Keep that subset small
 - Keep your info out of the bad guys hands
 - Guard your personal information
 - Don't be afraid to question someone's right to know
- Information on the net is permanent

25

How to fight back...



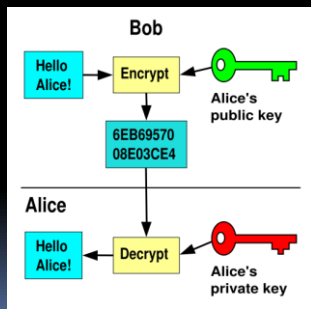
26

Passwords

- Social engineering
 - Have differing degrees of passwords
 - Don't share your important passwords
- Passwords guessers
 - Combine numbers, letters, special characters
 - Use the phrase method
 - Michelle Took Bobby Out For 4 Beers
 - MTBOF4B

27

Encryption



Backups

- Back your systems up regularly
 - Automated software
 - Built into Macs, Windows
- Can backup to portable hard drive
 - Very inexpensive these days
- If a virus attacks you, you can recover
 - Reload from backups

Personal habits

- Be careful about posting PII
 - Who can see it?
 - What is their privacy policy?
- Use differing levels of e-mail addresses
 - Keep one for shopping, surveys
 - Keep one for professional
 - Keep one for personal

Personal habits

- Change your passwords regularly
 - Every 90 days or so
 - Do NOT use your birthday...
- Watch your bank accounts
 - Easy to log in and verify transactions
 - Programs like Quicken will download
- Use encryption
 - https://

34

Personal habits

- Verify on-line sites
 - Don't give your CC# unnecessarily
 - Ensure it is a legitimate business
- NEVER respond to phishing
 - They will clean out your account in seconds
- Run virus checkers
 - Norton, MacAfee, ClamXav
- Backup your system regularly

35

References

1. http://en.wikipedia.org/wiki/Computer_security
2. <http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp>
3. http://en.wikipedia.org/wiki/Internet_privacy
4. <http://en.wikipedia.org/wiki/Malware>
5. <http://en.wikipedia.org/wiki/Spyware>
6. <http://www.buzzle.com/articles/computer-security-authentication.html>

36
