CYBER SECURITY - 182

Wednesday, 22 July 2020 1:45 PM

INTRODUCTION

Objectives of the Unit

•Describe approaches to computer security including access control, identity verification and authentication in order to minimize the cyber-attacks on a system.

•Work as a team to assess the impact of social engineering attacks in various organisations and analyse the effectiveness of its countermeasures.

•Improve the level of security of systems with remote control by using proper access control, authentication, privilege management and encryption methods.

•Apply the appropriate use of tools to facilitate network security to prevent various types of computer and network attacks, and malicious software that exists.

Code of Ethics and Agreement

•In this unit, we teach you a lot about the potential miss-use of the Internet and of computer networks.

•All software used is accessible to the knowledgeable general public.

•As a security professional, you need to know what others are capable of so that you can predict and secure vulnerabilities.

•Thus, we ask you to read the Code of Ethics statement in Moodle and to sign and submit the Agreement also posted there.

•This is a requirement of the unit. Anyone not signing will be dis-enrolled.

WEEKS 1/2

Describe approaches to computer security including access control, identity verification and authentication in order to minimize the cyber-attacks on a system.
•Work as a team to assess the impact of social engineering attacks in various organisations and analyse the effectiveness of its countermeasures.
•Improve the level of security of systems with remote control by using proper access control, authentication, privilege management and encryption methods.
•Apply the appropriate use of tools to facilitate network security to prevent various types of computer and network attacks, and malicious software that exists.

Today's Attacks

•Attacks directed at point-of-sale (PoS) systems
  •Resulted in over 1.02 billion records of consumers' payment card information being stolen in a year
  •Called "memory-scrapers", steal user's payment card numbers as card is being swiped
•Healthcare industry
  •Medical and financial information about the patient and patient's family can be used to steal identities
  •Also used for billing fraud and for purchasing drugs for resale
•Vulnerability in home wireless networking equipment
  •Would allow attackers to launch malicious software against any device connected to the home network
•Vulnerability in 1.4 million vehicles
  •Attackers could remotely control the cars
•A researcher was able to connect his laptop to an aircraft's in-flight entertainment system (IFE)
  •Once connected to IFE he could access other systems on the plane
•Personal medical devices could be next target for attackers
•Belgium credit provider had customer information stolen
  •Attackers threatened to publish information if company did not pay
•E-mail account compromised
  •Attacker sent bogus emails to account owner's contacts asking them to wire money
•Car hacking
  •Breaking into car's electronic systems
•Vulnerabilities in Apple devices
  •Continue to be exposed and manipulated by attackers
•From January 2005 through July 2015, over 853 million electronic data records in the US were breached
  •Exposing attackers to personal electronic data

Organization	Description of Security Breach	Number of identities exposed
Office of Personnel Management	Current and former federal employees exposed employees' job assignments, performance, and training, and may have exposed Social Security information and/or financial information.	4,000,000
CareFirst BlueCross BlueShield	The breach of a single database exposed names, birth dates, email addresses, and insurance identification numbers.	1,100,000
Penn State's College of Engineering	In two different intrusions attackers accessed "sensitive data" of all College of Engineering students, faculty, and staff.	18,000
Salley Beauty	"Unusual activity of payment cards at some stores" followed a similar attack 60 days before in which information on over 25,000 customer payment cards was stolen.	Unknown
AT&T	In three separate incidents employees accessed customer names and Social Security numbers, which were then sold to outsiders who used that information to unlock stolen cell phones.	280,000
Anthem BlueCross BlueShield	Names, birthdays, medical IDs, Social Security numbers, street addresses, email addresses, employment and income information were stolen in an attack that may have gone undetected for ten months.	80,000,000

Table 1-1 Selected security breaches involving personal information in a one-month period

Defining Cyber Security

•**Cybersecurity**
  •Task of securing information in a digital format
  •Ensures protective measures are properly implemented
  •Protects information with value to people and organizations

•**Three protections that must be extended (CIA)**
  •Confidentiality
  •Integrity
  •Availability

•**In addition to the CIA triad, another set of protections must be implemented:**
  •Authentication
  •Authorization
  •Accounting

•**Cybersecurity must protect devices that store, process, and transmit**

Difficulties in Defending Against attacks.

•Universally connected devices
•Increased speed of attacks
•Greater sophistication of attacks
•Availability and simplicity of attack tools
•Faster detection of vulnerabilities
•Delays in security updating
•Weak security updates distribution
•Distributed attacks
•User confusion

Reason	Description
Universally connected devices	Attackers from anywhere in the world can attack.
Increased speed of attacks	Attackers can launch attacks against millions of computers within minutes.
Greater sophistication of attacks	Attack tools vary their behavior so the same attack appears differently each time.
Availability and simplicity of attack tools	Attacks are no longer limited to highly skilled attackers.
Faster detection of vulnerabilities	Attackers can discover security holes in hardware or software more quickly.
Delays in security updating	Vendors are overwhelmed trying to keep pace updating their products against the latest attacks.
Weak security update distribution	Many software products lack a means to distribute security updates in a timely fashion.
Distributed attacks	Attackers use thousands of computers in an attack against a single computer or network.
User confusion	Users are required to make difficult security decisions with little or no instruction.

OBJECTIVES

➢ **Describe the challenges of cybersecurity**
1) Employees using non-company devices to access the company network
2) Risk from third-party service providers
3) Funding
4) Struggle to find GOOD cybersecurity providers and vendors & qualified cybersecurity professionals

➢ **Define cybersecurity and explain why it is important**
Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. It is important because it encompasses everything that pertains to protecting our sensitive data like personal information, data form either theft or damage.

➢ **Identify the types of attackers that are common today**
1) DOS/DDOS Attacks. (Denial of service)
2) Man-in-the-middle (MitM) Attack.
3) Phishing.
4) Password attacks
5) Malicious Software (Malware; spyware, ransomware, viruses and worms.)

➢ **Describe Attacks and Defences**
6) **Attacks -**

7) **Defences -**

Challenges of cybersecurity

•No single simple solution exists for protecting computers and securing information
•Different types of attacks that computers face
•Difficulties in defending against these attacks

What is Cyber Security?

•Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
•Application; Information; Network; Operational Security
•End-user education; Business continuity planning; Disaster recovery

Understanding Security

•Security
  •Necessary steps to protect a person or property from harm
  •Example: security for a home
    •Protection from burglary
    •Protection from natural forces (storms, etc.
  •Security is inversely proportional to convenience
    •As security increases, convenience decreases

- Authentication
- Authorization
- Accounting

•Cybersecurity must protect devices that store, process, and transmit information

- Information protected in three layers
  - Products
  - People
  - Policies and procedures

Cyber Security Terminology

- Asset
  - Something of value
- Threat
  - Type of action with potential to cause harm
- Threat agent
  - Person or element with power to carry out a threat
- Vulnerability
  - Flaw or weakness that allows a threat agent to bypass security

- Exploit the vulnerability through a threat vector
  - The means by which an attack can occur, such as an attacker stealing user passwords
- Risk
  - The likelihood that a threat agent will exploit a vulnerability
  - Some degree of risk must always be assumed

•Options for dealing with risk
- Risk avoidance
- Risk acceptance
- Risk mitigation
- Risk deterrence

Understanding/Importance of Cybersecurity

- Goals of cybersecurity
  - Preventing data theft
  - Thwarting identity theft
  - Avoiding legal consequences of not securing data
  - Maintaining productivity
  - Foiling cyberterrorism

- Data theft examples
  - Stealing business information
  - Stealing personal credit card number

- Identity theft
  - Stealing a person's information
  - Using information to impersonate the victim
  - Usually motivated by financial gain
  - Thieves can:
    - Create new bank or credit card accounts under the victim's name
    - File fictitious income tax returns in order to receive the victim's tax refund

- Avoiding legal consequences
  - Laws protecting electronic data privacy
    - The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    - The Sarbanes-Oxley Act of 2002 (Sarbox)
    - The Gramm-Leach-Bliley Act (GLBA)
    - Payment Card Industry Data Security Standard
    - The California Database Security Breach Act (2003)

- Maintaining productivity
  - Cleaning up after an attack diverts resources

- Foiling Cyberterrorism
  - Premeditated, politically motivated attacks against information, computer systems, programs and data
  - Intended to cause panic, provoke violence, or cause financial catastrophe
- Possible cyberterrorist targets
  - Banking industry
  - Military installations
  - Air traffic control centres
  - Water systems

Building a Comprehensive Security Strategy

- Four key elements to creating a practical security strategy:
  - Block attacks
  - Update defences
  - Minimize losses
  - Stay alert
- These are tactics used since Middle Ages

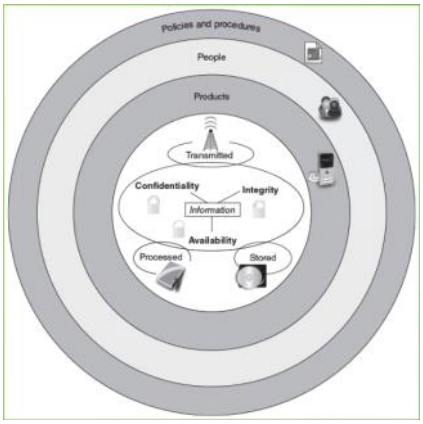
➢ Block Attacks

- Medieval castle designed to block attacks
  - High, protective stone wall
  - Moat filled with water
  - Objective: create a security perimeter

- Strong security perimeter
  - Part of the computer network
  - Data to be secured resides on personal computers

- Security is inversely proportional to convenience
  - As security increases, convenience decreases

INFORMATION SECURITY LAYERS



Layer	Description
Products	Forms the security around the data. May be as basic as door locks or as complicated as network security equipment.
People	Those who implement and properly use security products to protect data.
Policies and procedures	Plans and policies established by an organization to ensure that people correctly use the products.

Term	Example in Ellie's scenario	Example in information security
Asset	Scooter	Employee database
Threat	Steal scooter	Steal data
Threat agent	Thief	Attacker, hurricane
Vulnerability	Hole in fence	Software defect
Threat vector	Climb through hole in fence	Access web server passwords through software flaw
Threat likelihood	Probability of scooter stolen	Likelihood of virus infection
Risk	Not purchase scooter	Not install wireless network

Different Variations of Attackers

•Attackers are divided into several categories
- Cybercriminals
- Script kiddies
- Brokers
- Insiders
- Cyberterrorists
- Hacktivists
- State-sponsored

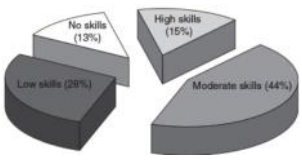
➢ Cybercriminals

•Generic definition
- People who launch attacks against other users and their computers

- Specific definition
  - Loose network of highly motivated attackers, identity thieves, and financial fraudsters
  - Many belong to organized gangs of attackers
- Targets
  - Individuals and businesses
  - Businesses and governments

➢ Script Kiddies

- Attackers who lack knowledge necessary to perform attack on their own
- Use automated attack software
- Can purchase "exploit kit" for a fee from other attackers
- Over 40 percent of attacks require low or no skills



➢ Brokers

- Attackers sell their knowledge of a vulnerability to other attackers or governments
  - Sell to highest bidder
  - Goal
- Break into computer or system
  - Take information without drawing attention to their actions
- Generally possess excellent computer skills

- Moat filled with water
- Objective: create a security perimeter

- Strong security perimeter
  - Part of the computer network
  - Data to be secured resides on personal computers attached to the network
  - Local security on all computers important
  - To foil attacks that breach the perimeter

- Goal
- Break into computer or system
  - Take information without drawing attention to their actions
- Generally possess excellent computer skills

➢ **Insiders**
- An organization's own employees, contractors, and business partners
- One study showed 48 percent of data breaches are caused by insiders accessing information
- Most insider attacks: sabotage or theft of intellectual property
- Most sabotage comes from employees who have recently been demoted, reprimanded, or left the company

➢ **Update Defences**
- Medieval example: leather shields were an adequate defense until flaming arrows were invented
- Continually update defenses to protect information against new types of attacks
  - New attacks appear daily
  - Update defensive hardware and software
  - Apply operating system security updates regularly

➢ **Minimize Losses**
- Medieval example: having a bucket of water available to put out fire started by flaming arrow
- Some attacks will get through security perimeters and local defences
- Actions must be taken in advance to minimize loss
  - Make backup copies of important data
  - Institute a business recovery policy
  - Details what to do in the event of a successful attack

◆ **STAY ALERT**
- Medieval example: defenders of the castle had to stay alert and be vigilant to join the fight
- Today, cybersecurity is the responsibility of all users
  - Users must have the knowledge of what to do
  - As well as the proper motivation to stay secure

➢ SUMMARY
- Attacks against cybersecurity have grown exponentially in recent years
- Difficult to defend against today's attacks
- cybersecurity definition
  - Protecting the integrity, confidentiality, and availability of information on devices that store, transmit, and process info rmation
- cybersecurity goals
  - Prevent data theft, thwart identity theft, avoid legal consequences, maintain productivity, and foil cyberterrorism
- Attackers fall into several categories
  - Different motivations, targets, and skill levels
- Elements of a comprehensive security strategy
  - Block attacks
  - Update defences
  - Minimize losses
  - Stay alert to attacks

WEEKS 3/4

Used wireshark to capture packets | telnet is not secure due to not being encrypted

NETCAT

Ncat is a general-purpose command-line tool for reading, writing, redirecting, and encrypting data across a network. It aims to be your network Swiss Army knife, handling a wide variety of security testing and administration tasks. Ncat is suitable for interactive use or as a network-connected back end for other tools.

2 ways to attempt windows computer hashing.

Port 21 - FTP
Port 22 -SSH
Port 23 - Telnet
Port 80 - HTTP
Port 443 - HTTPS | 0 - 65 535 is the amount of available ports.

We'll connect through port 443 due to it being 'open'

Netstat shows all connections. (In Kali)
Ifconfig shows the IP-address
The shadow file stores all encrypted passwords if applicable.
Passfile.wd stores all the user information.

If being able to establish a connection from Kali to DVL, you can run commands from Kali.

What is Hashcat?

Hashcat is a well-known password cracker. It is designed to break even the most complex passwords. To do this, it enables the cracking of a specific password in multiple ways, combined with versatility and speed. Password representations are primarily associated with hash keys, such as MD5, SHA, WHIRLPOOL, RipeMD,

What is /bin/bash?

/bin/bash is a terminal, it is the most common shell used as default shell for user login of the Linux system. The shell's name is an acronym for Bourne-again shell. Bash can execute the vast majority of scripts and thus is widely used because it has more features, is well developed and better syntax

What does the command 'grep' do?

- **Simply displays 1 line.**

It is one of the most widely used and powerful commands on Linux and Unix-like operating systems. The 'grep' command is used to search a given file for patterns specified by the user. Basically 'grep' lets you enter a pattern of text and then it searches for this pattern within the text that you provide it.

Adds a password user accounts.

Adding and manipulating users/groups

```
elmo:x:1000:1001::/home/elmo:/bin/sh
```

```
root@Kali-Attacker:~# passwd elmo
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

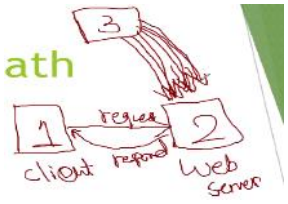
LECTURE 5/WEEK 5

Protecting personal computers is challenging due to multiple forms of attack.

Many Different attacks exist today
  Attackers are constantly modifying attacks and creating new ones.
No Single defensive program exists
  Several different defence's must be in place

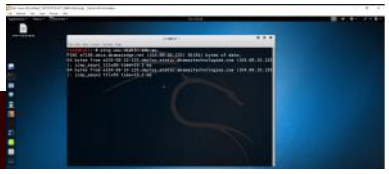
Remote Host Attacks
- DOS (Denial of Service attack)
  - Means: if a computer is provided a service, and if it denies providing a service, it is a DOS attack..
  - Being able to deny that service.
  - It's a main type of attack
  - Plenty of ways to perform DOS attack.

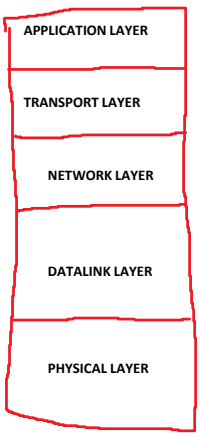
Computer No. 3 is the attacker, it is making
Computer No. 2 very busy.
It's done purely out of satisfaction



PING
- **This sends ICMP packets - (ICMP) - Internet Control Message Protocol which works on the application layer.**

- Used by network devices including routers
- send error messages and operational information e.g.
  - a requested service is not available or that a host or router could not be reached





text that you provide it.

Adding and manipulating users/groups

```
elmo:x:1000:1001::/home/elmo:/bin/sh
oscar:x:1001:1001::/home/oscar:/bin/sh
lisa:x:1002:1002::/home/lisa:/bin/sh
homer:x:1003:1002::/home/homer:/bin/sh
root@Kali-Attacker:~#
```

Adds a password user accounts.

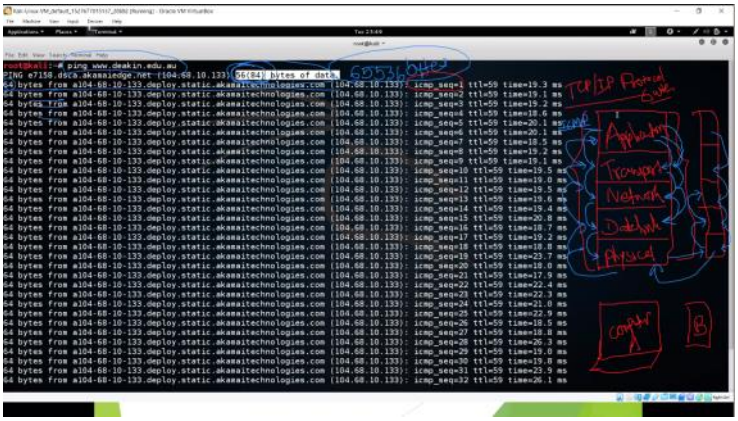
```
root@Kali-Attacker:~# passwd elmo
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@Kali-Attacker:~#
```

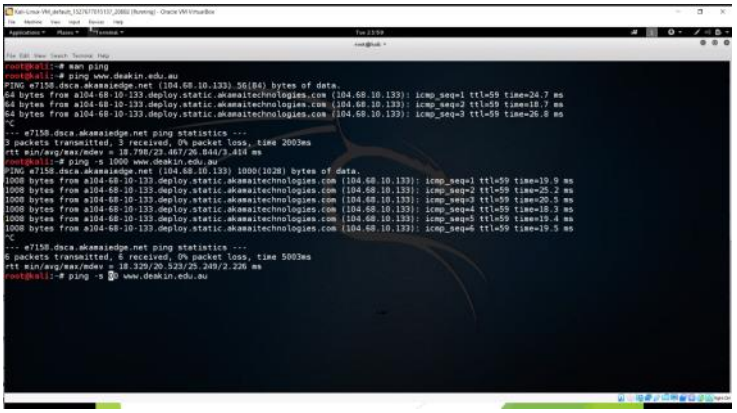
PHYSICAL LAYER

:XXXX:0000: = the user account identifier
:0000:XXXX: = the group it is linked to in the system

Define the internet: something the connects device all over the world/ a place where people can connect
A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols
A huge network, which is a collection of smaller area networks.

- Internet is something to establish a connection from a router to a an ISP.
- Is a way to connect to other devices.





Review: how the Internet Works

3

- Internet
  - A global network that allows devices connected to it to exchange information
  - Composed of networks to which devices are attached
  - Not owned or regulated by any organization or government entity
  - Computers loosely cooperate to make the Internet a global information resource
  - Two main Internet tools:
    - World Wide Web and email

Information on the WWW (World Wide Web)
- We use the internet as a infrastructure to grab information on servers
- Can be classified as a 'spiders web'

Emails
- Different tools we use over the internet

HTML
- is a language we use to communicate over the internet, it allows us to send text, graphic, images, audio, video and hyperlinks (Also to exchange data over the internet)
- The role of a web browser is to communicate html coding which is converting data into a human-readable language

The World Wide Web (Cont)

- World Wide Web (WWW)
  - Better known as the *web*
  - Internet server computers that provide online information in a specific format
- Hypertext Markup Language (HTML)
  - Allows Web authors to combine text, graphic images, audio, video, and hyperlinks
- Web browser
  - Displays the words, pictures, and other elements on a user's screen

The World Wide Web (Cont)

- Hypertext Transport Protocol (HTTP)
  - Standards or protocols used by Web servers to distribute HTML documents
  - Subset of Transmission Control Protocol/Internet Protocol standards (TCP/IP)
- Web browser on the user's computer sends a request to a remote web server
  - Web server responds by sending the HTML document to the user's local computer

➢ **SSH (Secure Shell)**

- Cryptographic network protocol for operating network services securely over an unsecured network - replacement for Telnet
- Best known for remote login and command execution on computer systems by users.
- Access to shell accounts on Unix-like operating systems
- The encryption used by SSH is intended to provide confidentiality and integrity.

•11

- Files leaked by Edward Snowden indicate that the National Security Agency can sometimes decrypt SSH, allowing them to read the contents of SSH sessions.
- On 6 July 2017 WikiLeaks confirmed that the US Central Intelligence Agency had developed hacking tools to crack the SSH protocols

NOTORIOUS PING OF DEATH

Attacker can achieve, in 1996 all the computers were affected by the notorious ping of death attack.
In 1997, it was obsolete.

Notorious ping of death attack

- denial of service (DoS) attack - 1996
- caused by an attacker deliberately sending an IP packet larger than the 65,536
- One of the features of TCP/IP is fragmentation; it allows a single IP packet to be broken down into smaller segments
- a packet broken down into fragments could add up to

- Web browser on the user's computer sends a request to a remote web server
  - Web server responds by sending the HTML document to the user's local computer
  - User's web browser displays the document

4 Most common web app threats:
XSS, SQL

Why they occur? From flawed coding, if they had properly written the code this attack wouldn't happen. If we fail to sanitize the input and output from a browser, these 2 attacks can occur.

Web application attacks

- Client-server software application
  - Client (or user interface) runs a web browser
- 4 most common web app threats include:
  - Cross site scripting (XSS), SQL injections, DDoS and Cookie poisoning
- Majority of web attacks occur through:
  - SQL injection and XSS
    - Result from flawed coding
    - Failure to sanitize input to and output from the web app

SQL Injection attack and defense

10

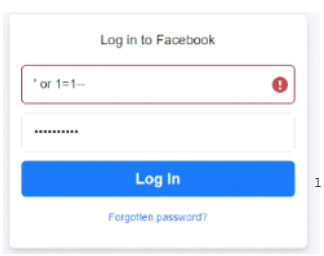
- attackers gain access to Web apps
- adding Structured Query Language (SQL) code or statements to a Web forum input box in the form of an SQL query
- request for a specific action to be performed on a database e.g. dump the database contents to the attacker
- Example
  - during user authentication a username and password are entered and inserted into a query.
  - user is then either granted or denied access, depending on if the correct information was submitted. Web forums typically don't have any means to block input other then usernames and passwords
  - an attacker can perform an SQL injection attack by using input boxes to send requests to the database, possibly granting them access.

SQL Injection attack

11

- SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.
- SQL injection attacks allow attackers to:
  - spoof identity
  - tamper with existing data
  - cause repudiation issues such as voiding transactions or changing balances
  - allow the complete disclosure of all data on the system
  - destroy the data or make it otherwise unavailable
  - become administrators of the database server.

This attack is possible where username and password is applicable



DVL - Damn Vulnerable Linux.
Damn Vulnerable Linux is a discontinued Linux distribution geared toward computer security students. It functioned as a tool for observing and studying vulnerabilities in the Linux kernel and popular user space software

< Can work with Linux SQL injections (A2)

WEBGOAT on DVL

1. What is Damn Vulnerable Linux?
   - Damn Vulnerable Linux (DVL) is everything a good Linux distribution isn't. Its developers have spent hours stuffing it with broken, ill-configured, outdated, and exploitable software that makes it vulnerable to attacks.
   - DVL isn't built to run on your desktop -- it's a learning tool for security students. DVL is a live CD available as a 150MB ISO.

- One of the features of TCP/IP is fragmentation; it allows a single IP packet to be broken down into smaller segments
- a packet broken down into fragments could add up to more than the allowed 65,536 bytes
- Many operating systems didn't know what to do when they received an oversized packet, so they froze, crashed, or rebooted.

Notorious ping of death attack

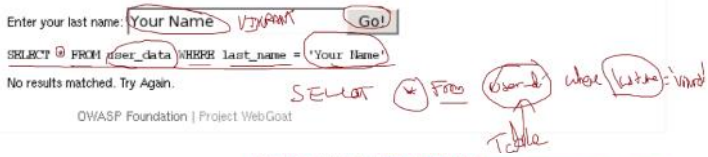
- Ping of death attacks were particularly malicious
- the identity of the attacker sending the oversized packet could be easily spoofed
- the attacker didn't need to know anything about the machine they were attacking except for its IP address.
- 1997, operating system vendors had made patches available to avoid the ping of death.
- Still, many Web sites continue to block Internet Control Message Protocol (ICMP) ping messages at their firewalls to prevent any future variations of this kind of denial of service attack.

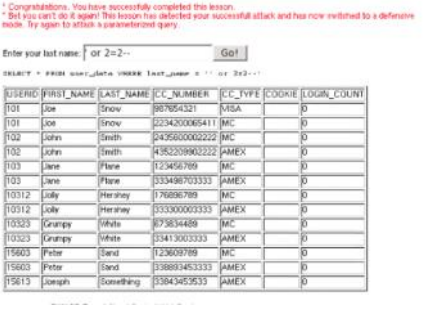
- Protecting personal computers is challenging
- Many different types of attacks exist today
  - Attackers are constantly modifying attacks and creating new ones
- No single defensive program exists
  - Several different defenses must be in place
- We will look at how the design of an underlying protocol has been used for an attack and how this can be defended

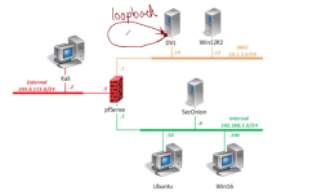
FIREWALLS

- Software-based personal firewall
  - Designed to prevent malware from entering a computer
  - Examines incoming data from the Internet or local network
  - Blocks (filters) certain content
- Configuration
  - User can grant or deny permission for specific programs to communicate across network
  - See Figure 3-8
- Hardware-based network firewall
  - Designed to protect an entire network
  - Usually located at the "edge" of the network as the first line of defense

Function	Personal firewall	Network firewall
Location	Runs on a single computer	Located on edge of the network
Scope of protection	Protects only computer on which it is installed	Protects all devices connected to the network
Type	Software that runs on computer	Separate hardware device
Filtering	Based on programs running on the computer	Provides sophisticated range of filtering mechanisms







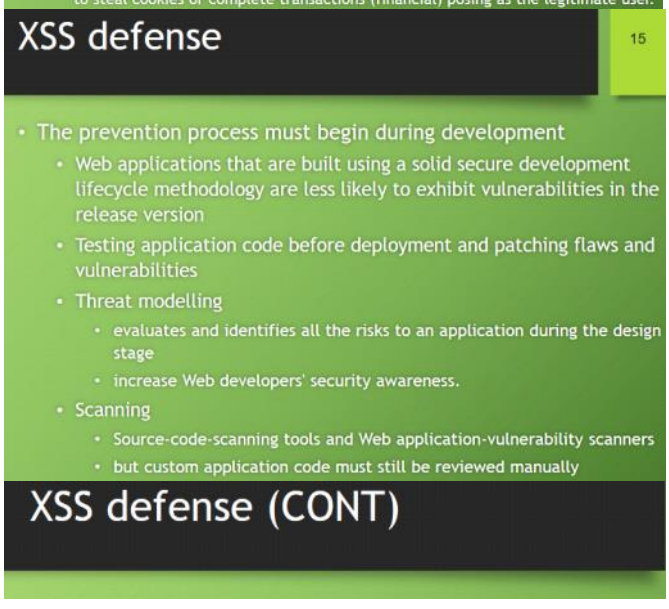
LOOP BACK INTERFACE
Connecting to the same device.

exploitable software that makes it vulnerable to attacks.

- DVL isn't built to run on your desktop -- it's a learning tool for security students. DVL is a live CD available as a 150MB ISO.
- It's based on the popular mini-Linux distribution Damn Small Linux (DSL), not only for its minimal size, but also for the fact that DSL uses a 2.4 kernel, which makes it easier to offer vulnerable elements that might not work under the 2.6 kernel.
- It contains older, easily breakable versions of Apache, MySQL, PHP, and FTP and SSH daemons, as well as several tools available to help you compile, debug, and break applications running on these services, including GCC, GDB, NASM, strace, ELF Shell, DDD, LDasm, LIDa, and more.
- DVL was initiated by Thorsten Schneider of the International Institute for Training, Assessment, and Certification (IITAC) and Secure Software Engineering (S[illegible]) in cooperation with Kryshaam from the French Reverse Engineering Team. "The main idea behind DVL," says Schneider, "was to build up a training system that I could use for my university lectures." His goal was to design a Linux system that was as vulnerable as possible, to teach topics such as reverse code engineering, buffer overflows, shellcode development, Web exploitation, and SQL injection.

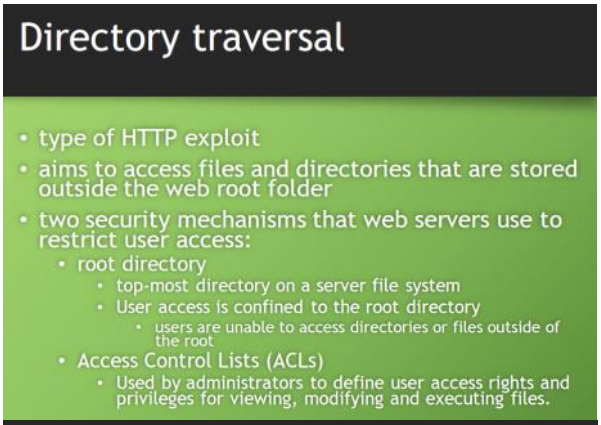
2. What is WebGoat SQL Injection?
   - SQL injection is a common web application attack that focuses on the database backend.
   - WebGoat is a deliberately insecure J2EE web application maintained by OWASP designed to teach web application security lessons.

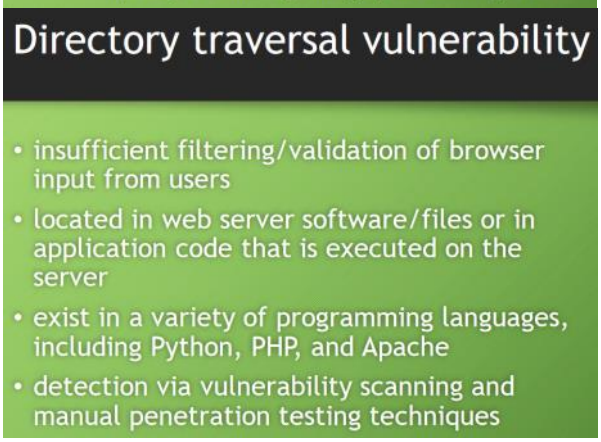
XSS Attack and Defence



SQL Injection -
If any website allows a user to input credentials, it will allow you to write a command. This will translate HTML into a

WEEK 8 -





Directory Traversal - changing things in the URL, to give access to files not only inside the file, but things outside the file. (Information)

- **Can access shadow files and other important files through web browser on the hard drive.**
- ../ Method : Using this method can use a terminal to direct itself through to parent directory's.
  It takes us back to the 'parent directory'
-

Emails -

Web-browser vulnerabilities -

|| EXAMPLE OF ../ METHOD || - DIDN'T HAVE PERMISSION'S

XSS defense (CONT)

- Web developers should filter user input to:
  - Remove possible malicious characters and browser scripts
  - Install user-input-filtering code to remove malicious characters.
- Administrators can also configure browsers to only accept scripts from trusted sites or disable browser scripting
  - can result in a website with limited functionality.

WEEK 8 -

Directory Traversal examples

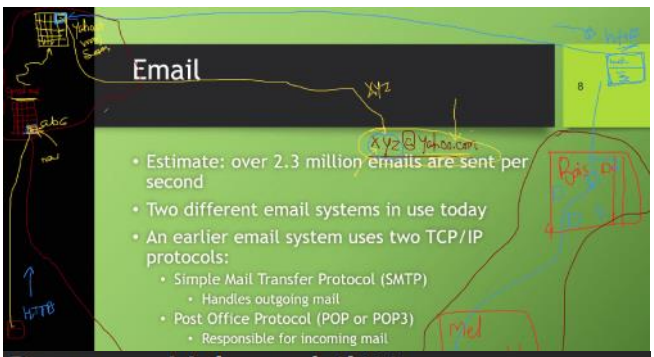
- two basic groups:
- 1. attacks that target directory traversal vulnerabilities in the web server
  - typically exploited to execute files
  - sending URLs to the web server that contain the name of the targeted file and have been modified with commands and web server escape codes
  - an attacker might use the "%2e%2e/" escape code if the "../" command is blocked
  - requires trial-and-error from the attacker

Directory Traversal examples

2. attacks that target vulnerabilities in application code
   - find a URL in which an application retrieves a file from the web server
   - modify the URL string with commands for the server and the name of the file they seek to access
   - The "../" directive is commonly used, as it instructs the web server to retrieve a file from one directory up.
   - use trial-and-error to access a specific file by determining how many ".../" commands it takes to locate the correct directory and retrieve the file via the application.

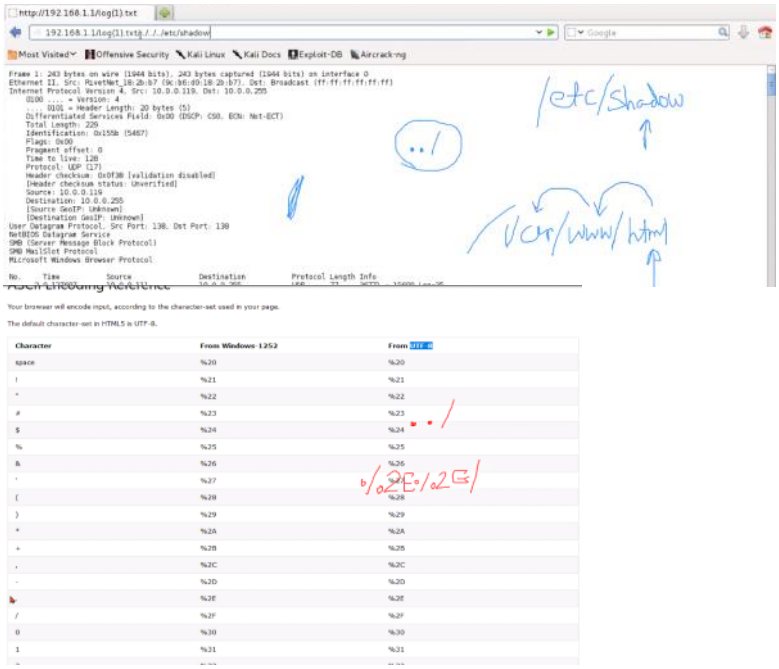
How Email Works -
In postal system, Melbourne --> Brisbane;

BROWSER VULNERASBILITIES



Browser Vulnerabilities

- In early days of web, users viewed static content
  - Information that does not change



Directory Traversal prevention

- programmers should be trained to validate user input from browsers
  - Input validation ensures that attackers cannot use commands that leave the root directory or violate other access privileges.
- filters can be used to block certain user input
  - Enterprises typically employ filters to block URLs containing commands and escape codes that are commonly used by attackers.
- web server software (and any software that is used) should be kept up-to-date with current patches

Email

- Estimate: over 2.3 million emails are sent per second
- Two different email systems in use today
- An earlier email system uses two TCP/IP protocols:
  - Simple Mail Transfer Protocol (SMTP)
    - Handles outgoing mail
  - Post Office Protocol (POP or POP3)
    - Responsible for incoming mail

Internet Security Risks

- Variety of risks from using the Internet
  - Browser vulnerabilities
  - Malvertising
  - Drive-by-downloads
  - Cookies
  - Email risks

Browser Vulnerabilities (cont)

- JavaScript
  - Embedded in HTML document
  - Executed by browser

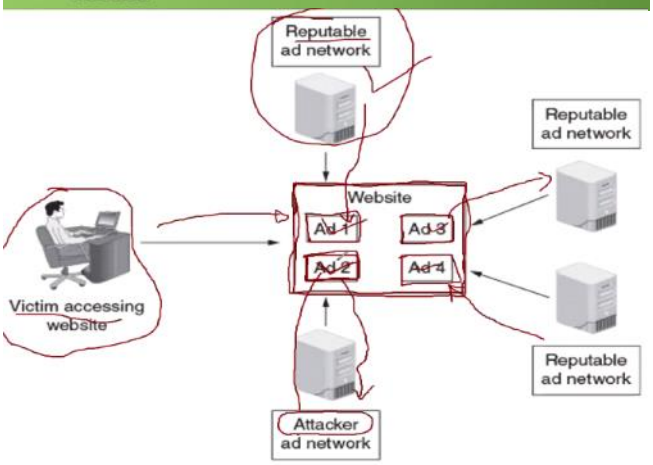
content
- Information that does not change

- Today, users demand dynamic content
  - Content that changes (animation or customized info)
- Scripting code
  - Computer code that commands the browser to perform specific actions
  - JavaScript is the most popular scripting code

- Extensions
  - Expand the normal capabilities of a web browser for a specific webpage
  - Most are written in JavaScript
  - Generally have wider access privileges than JavaScript running in a webpage
  - Browser-dependent
    - Extensions that work in Google Chrome will not function in Microsoft Edge

Browser Vulnerabilities (cont)

- Plug-in
  - Adds new functionality to the browser so users can play music, view videos, or display special graphic images
- Java
  - Complete programming language
  - Used to create small applications called applets
- Efforts being made to minimize risks associated with extensions, plug-ins, and add-ons
  - Some web browsers block plug-ins
  - Other browsers use a "Click to Play" feature that enables a plug-in only after the user gives approval
  - HTML5 (most recent version) standardizes sound and video formats so that plug-ins like Flash are not needed



COOKIES

Cookies (cont)

- User-specific information file created by server
- Stored on local computer
- First-party cookie
  - Created by the Web site the user is currently viewing

- JavaScript
  - Embedded in HTML document
  - Executed by browser
  - Defense mechanisms in place to prevent JavaScript programs from causing serious harm
    - JavaScript cannot read, write, or delete files from a local computer
  - A malicious JavaScript program can capture and send user information without the user's knowledge or authorization

Defense	Explanation
Limit capabilities	JavaScript does not support certain capabilities. For example, JavaScript running on a local computer cannot read, write, create, delete, or list the files on that computer.
Sandboxing	By only permitting JavaScript to run in a restricted environment ("sandbox") this can limit what computer resources it can access or actions it can take.
Same origin	This defense restricts a JavaScript downloaded from Site A from accessing data that came from Site B.

Name	Description	Location	Browser Support	Examples
Extension	Written in JavaScript and has wider access to privileges	Part of web browser	Only works with a specific browser	Download selective links on webpage, display specific fonts
Plug-in	Links to external programs	Outside of web browser	Compatible with many different browsers	Audio, video, PDF file display
Add-on	Adds functionality to browser itself	Part of web browser	Only works with a specific browser	Dictionary and language packs

- Add-Ons
  - Add a greater degree of functionality to the entire browser; not just a single webpage as with a plug-in
  - Add-ons can do the following:
    - Create additional web browser toolbars
    - Change browser menus
    - Be aware of other tabs open in the same browser process
    - Process the content of every webpage that is loaded

Malvertising (cont)

- Attackers use third-party advertising networks to distribute malware
  - Through ads sent to users' web browsers
- Advantages for the attacker:
  - Occurs on "big-name" websites
  - Usually website owners are unaware malware is being distributed through their website ads
  - Ad network rotate content quickly, making it difficult to determine if malvertising was the culprit of attack
  - Attackers can narrowly target victims

DRIVE BYS -

Drive-By Downloads

- Drive-by downloads
  - Attack attempting to infect the website directly
  - Can result in a user's computer becoming infected just from viewing the website
  - Attackers attempt to inject malicious content by exploiting it through a vulnerability in the web server
  - Injected content is virtually invisible to the naked eye

Email Risks -
Very cheap to send spam emails, an attacker will access botnet to send spam emails so
No one will know who the spam attacker is
SPAM FILTERS

- They will scan the content of each and every email and check if the email has a specific word 'attack' and flag it as a spam email.
- Instead of adding the text in the email, they will add the content in an image. Spam filters will not be able to detect this.

E-Mail Risks (cont)

- Stored on local computer
- First-party cookie
  - Created by the Web site the user is currently viewing
- Third-party cookie
  - Often come from Web site advertisers
  - Used to tailor advertising to a user
- Locally shared object (LSO) also called a flash cookie
  - Store data more complex than in a regular cookie
- Security and privacy risks of cookies
  - First-party cookies can be stolen and used to impersonate user
  - Third-party cookies can be used to track user's browsing and buying habits

Is user specific information which is created by a web server.

MORE INTERNET DEFENCES -

- Defending against Internet-based attacks begins with having the computer properly secured
  - Manage patches, configure firewalls, install anti-malware software, monitor User Account Control, create data backups, and know how to recover from an attack
- Once computer is secured, additional steps to resist Internet-based attacks include:
  - Securing the web browser
  - Maintaining email defenses
  - Follow Internet security best practices

What is Privacy?

Privacy is if we have control of our private information

What is Privacy?

- Privacy
  - The state or condition of being free from public attention to the degree that you determine
- Today
  - Data is collected on almost all actions and transactions that individuals perform
- Collected through:
  - Web surfing, purchases, user surveys and questionnaires, and other sources
- Data is then aggregated by data brokers

Why are we worried about privacy?

Due to being able to share information on public domains and the data can be collected and ANYONE can use that shared data and take advantage of this information;

- **To impersonate**
- **To incriminate**
- **To gain financial information**

3 Catergoiries of Private Data (Risk Associated)

- Risks fall into three categories:
  - Individual inconveniences and identity theft
    - Used to direct ad marketing campaigns and to impersonate the victim for personal gain
  - Associations with groups
    - Use of personal data to place individuals in groups based on similar interests
  - Statistical inferences
    - More in-depth than groupings

Can make a complete picture basis on what you do online.

Issue	Explanation

- They will scan the content of each and every email and check if the email has a specific word 'attack' and flag it as a spam email.
- Instead of adding the text in the email, they will add the content in an image. Spam filters will not be able to detect this.

E-Mail Risks (cont)

- Spam
  - Unsolicited email
  - Lucrative business - costs very little to send
  - Almost all spam is sent from botnets
- Spam filters
  - Block email containing specific words
- Image spam
  - Uses graphical images of text to circumvent text-based filters

IMAGE SPAM -

EFFECTS OF SPAM -

- Effects of spam
  - Lost productivity
  - Money spent on spam-filtering software
  - Wide distribution of malware
- Malicious attachments
  - Files sent with email
  - When attachment is opened, computer is infected
  - Replicate by sending themselves in an email message to entire list of contacts in infected computer
- Embedded hyperlinks
  - Hyperlink contained within email message body
  - Directs users to attacker's Web site
  - Hyperlink may display only words
    - Hides address of actual site
- Attacker's site may look like a legitimate site
  - Tricks user into entering personal information

PRIVACY PROTECTIONS - 3 SOLUTIONS

- Protections may be implemented to reduce the risks associated with private data
  - Cryptography
  - Following best practices **PRIVACY BASED PRACTICES**
  - Organizations that collect private data have responsibilities

CRYPTOTOGRAPHY -

- **Can achieve privacy with the 5 basic protections**
  - **Confidentiality - Something we wont to keep private unless it is authenticated to be accessed by a friend.**
  - **Integrity - Resistant to changes or attack. Holding the same value one has sent to someone else.**
  - **Availability - Data that belongs to us is accessible to us all the time.**
  - **Authentication - Providing appropriate authentication for a user by verifying ones identity.**
  - **Nonrepudiation - is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated**

- Cryptography can provide five basic protections:
  - Confidentiality

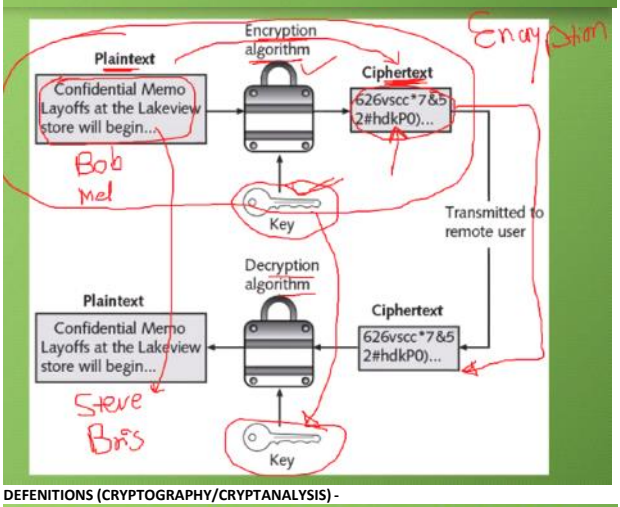
Can make a complete picture basis on what you do online.

Issue	Explanation
The data is gathered and kept in secret.	Users have no formal rights to find out what private information is being gathered, who gathers it, or how it is being used.
The accuracy of the data cannot be verified.	Because users do not have the right to correct or control what personal information is gathered, its accuracy may be suspect. In some cases, inaccurate or incomplete data may lead to erroneous decisions made about individuals without any verification.
Identity theft can impact the accuracy of data.	Victims of identity theft will often have information added to their profile that was the result of actions by the identity thieves, and even this vulnerable group has no right to see or correct the information.
Unknown factors can impact overall ratings.	Ratings are often created from combining thousands of individual factors or data streams, including race, religion, age, gender, household income, zip code, presence of medical conditions, transactional purchase information from retailers, and hundreds more data points about individual consumers. How these different factors impact a person's overall rating is unknown.
Informed consent is usually missing or is misunderstood.	Statements in a privacy policy such as "We may share your information for marketing purposes with third parties" are not clearly informed consent to freely allow the use of personal data. Often users are not even asked for permission to gather their information.
Data is being used for increasingly important decisions.	Private data is being used on an ever-increasing basis to determine eligibility in significant life opportunities, such as jobs, consumer credit, insurance, and identity verification.

CRYPTOGRAPHY CONSISTS OF AND CAN BE APPLIED BY -

- **Involves ENCRYPTION AND DECRYPTION**

- Basic Terms and the Encryption/Decryption Process
- Types of Ciphers
- Hashes
- Symmetric Encryption
- Asymmetric Encryption
- Cryptography Algorithm Use
  - Steganography



DEFENITIONS (CRYPTOGRAPHY/CRYPTANALYSIS) -

Cryptography is the art and science of secret writing, *encrypting*, or hiding of information from all but the intended recipient.

Cryptanalysis is the process of attempting to break a cryptographic system and return the encrypted message to its original form.

MORE DEFENITIONS -

- Plaintext – a piece of data that is not encrypted
- Ciphertext – the output of an encryption algorithm
- Cipher – a cryptographic algorithm
- Algorithm – a step-by-step, recursive computational procedure
- Key – a sequence of characters or bits used by an algorithm to encrypt or decrypt a message
- Encryption – changing plaintext to ciphertext
- Decryption – changing ciphertext to plaintext

CRYPTOGRAPHIC ALGORITHMS -

- Every current encryption scheme is based

- Cryptography can provide five basic protections:
  - Confidentiality
  - Integrity
  - Availability
  - Authentication
  - Nonrepudiation

Characteristic	Description	Protection
Confidentiality	Ensures that only authorized parties can view the information	Encrypted information can only be viewed by those who have been provided the key.
Integrity	Ensures that the information is correct and no unauthorized person or malicious software has altered that data	Encrypted information cannot be changed except by authorized users who have the key.
Availability	Ensures that data is accessible to authorized users	Authorized users are provided the decryption key to access the information.
Authentication	Provides proof of the genuineness of the user	Proof that the sender was legitimate and not an imposter can be obtained.
Nonrepudiation	Proves that a user performed an action	Individuals are prevented from fraudulently denying that they were involved in a transaction.

TYPES OF CIPHERS

- Shift
- Substitution
- Transposition
- Affine Ciphers
- Vigenère

SHIFT -
If you have a message you want to transmit securely, you can encrypt it (translate it into a secret code). One of the simplest ways to do this is with a shift cipher. ... A shift cipher involves replacing each letter in the message by a letter that is some fixed number of positions further along in the alphabet.

SUBSTITUTION -
In cryptography, a substitution cipher is a method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth

TRANSPOSTION -
In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext

AFFINE CIPHERS -
The Affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter

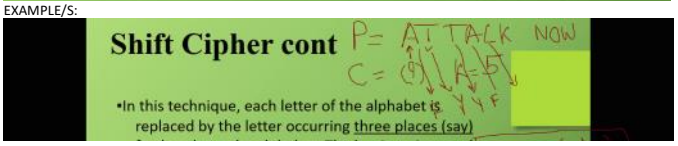
VIGENERE -
Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets

SLIDES FOR CIPHERS -

SHIFT CIPHER - was the first cipher used to hide data

- A classic example of this is the early shift cipher, known as *Caesar's cipher*.
- Caesar's cipher uses an algorithm and a key: the algorithm specifies that you offset the alphabet either to the right (forward) or to the left (backward), and the key specifies how many letters the offset should be.
- The Caesar's cipher is also known as a shift cipher.

EXAMPLE/S:



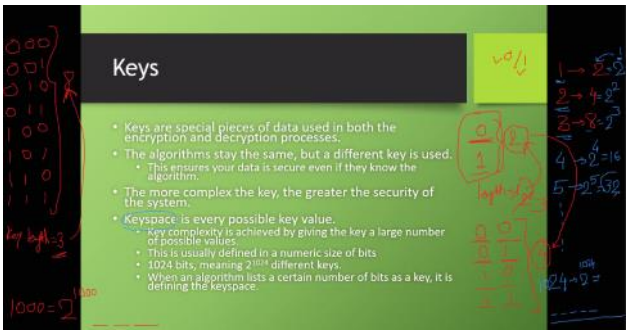
Decryption – changing ciphertext to plaintext

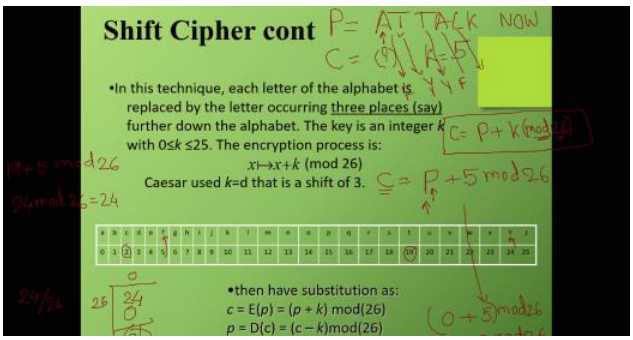
CRYPTOGRAPHIC ALGORITHMS -

- Every current encryption scheme is based upon an algorithm.
- The cryptographic algorithm—what is commonly called the encryption algorithm or cipher—is made up of mathematical steps for encrypting and decrypting information.

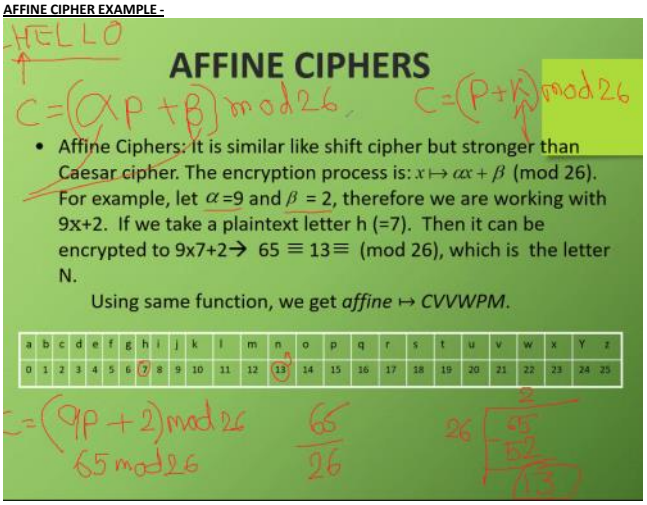
KEYS - 'To lock and unlock.'

- Keys are special pieces of data used in both the encryption and decryption processes.
- The algorithms stay the same, but a different key is used.
  - This ensures your data is secure even if they know the algorithm.
- The more complex the key, the greater the security of the system.
- Keyspace is every possible key value.
  - Key complexity is achieved by giving the key a large number of possible values.
  - This is usually defined in a numeric size of bits
  - 1024 bits, meaning 2^{1024} different keys.
  - When an algorithm lists a certain number of bits as a key, it is defining the keyspace.



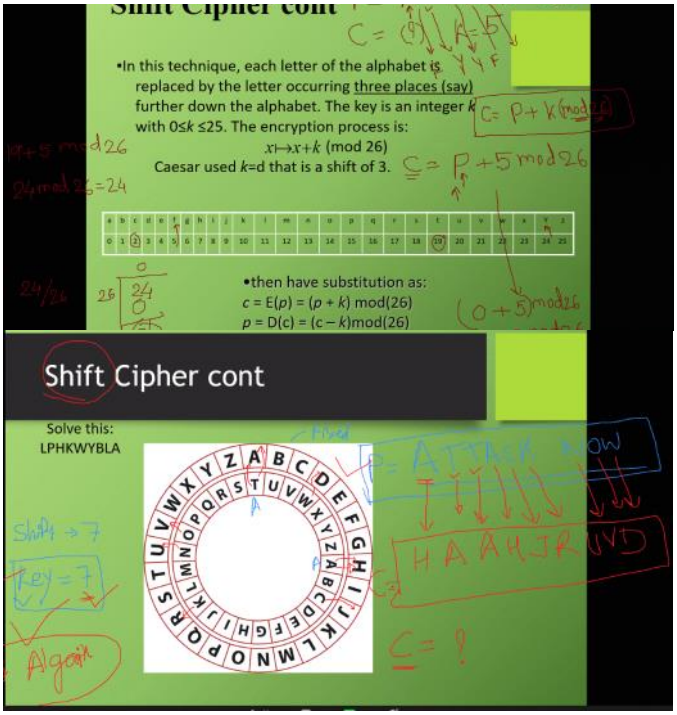


AFFINE CIPHER EXAMPLE -



What is a Vigenere Cipher?

- The Vigenère cipher is a much more complex cipher.
- It corrects the issues with more simplistic keys.
- It works as a polyalphabetic substitution cipher that



SUBSTITUTION CIPHER

- Shift ciphers are easy to crack.
  - Simply figure out the number of rotations.
- *Substitution ciphers* were developed because they are more complex.
- Substitution ciphers work on the principle of substituting a different letter for every letter.
  - *a* becomes *g*, *b* becomes *d*, and so on.
  - The letters are not in order as they are in shift ciphers.

TRANSPOSITION

- Transposition method:

READ COLUMN BY COLUMN

WRITE ROW BY ROW

1	2	3	4
G	O	O	D
M	O	R	N
I	N	G	I
N	D	I	A

- Transposition ciphers also *fail* to *mask* the characteristics of the language being encrypted.

- Decipher the following:
- EEATX_N_CI_AESA_L_CHLNTAEO_BNTBIC_UT
- Hint: The key is between 3 and 7

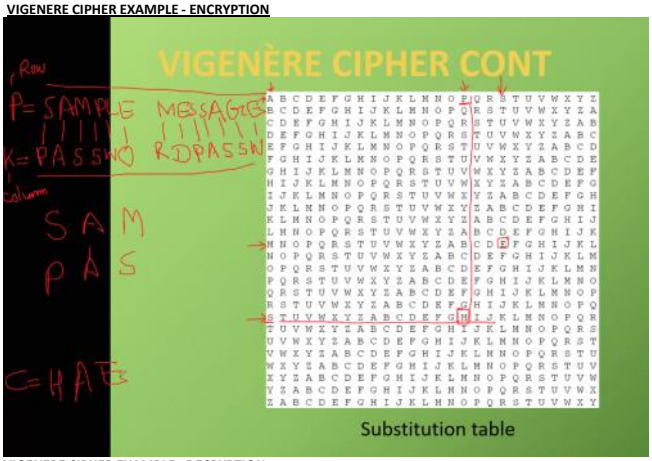
P = EXCELLENCL

Shift Cipher cont

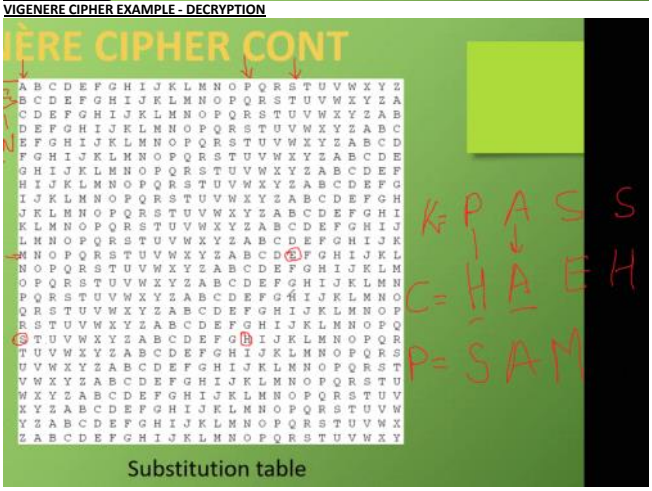
•In this technique, each letter of the alphabet is

- The Vigenère cipher is a much more complex cipher.
- It corrects the issues with more simplistic keys.
- It works as a polyalphabetic substitution cipher that depends on a password.
- The Vigenère cipher system and systems like it.
- Makes the algorithms rather simple
- But the key rather complex, with the best keys comprising very long and very random data

VIGENERE CIPHER EXAMPLE - ENCRYPTION



VIGENERE CIPHER EXAMPLE - DECRYPTION



| SHADOW FILE IS THE FILE WHICH STORES PASSWORDS ON LINUX |

BLOCKMETHOD - ?

A **block cipher** is an **encryption method** that applies a deterministic **algorithm** along with a symmetric key to encrypt a **block** of text, rather than encrypting one bit at a time as in stream **ciphers**. For **example**, a common **block cipher**, AES, encrypts 128 bit **blocks** with a key of predetermined length: 128, 192, or 256 bits

- Most algorithms use block mode to process data to create the hash.
- They break the data into sets of bits (blocks) such as 512.
- If a file were 1400 bits long, it would create three blocks with the third one being padded with zeros.
  - 2x512 is 1024, the third block would be 376 bits of the message and 136 bits of zeros.

MD - Message digests

Message Digest

- Message digest (MD) is the generic version of one of several algorithms that are designed to create a message digest or hash from data input into the algorithm.
- MD algorithms work in the same manner as SHA:
  - They use a secure method to compress the file and generate a computed output of a specified number of bits.

Shift Cipher cont

- In this technique, each letter of the alphabet is replaced by the letter occurring three places (say) further down the alphabet. The key is an integer k with $0 \le k \le 25$. The encryption process is: $x \mapsto x+k \pmod{26}$
  Caesar used k=d that is a shift of 3.

$C = (P+K) \bmod 26$

$P = (C-K) \bmod 26$

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	Y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- then have substitution as:
  $c = E(p) = (p + k) \bmod(26)$
  $p = D(c) = (c - k) \bmod(26)$

HASHING IN GENERAL/FUNCTIONS -

Hashing Functions

- Special mathematical function that performs *one-way encryption to produce a fingerprint that is called a digest.*
- *Considered secure if it is has these characteristics:*
  - *Fixed size; a digest of a short set of data should produce the same size as a digest of a long set of data.*
  - *Unique; two different sets of data cannot produce the same digest, which is known as a collision*
  - *Original; should be impossible to produce a data set that has a desired or predefined hash*
  - *Secure; the resulting hash cannot be reversed in order to determine the original plaintext*
  - Once the algorithm is processed, there is no feasible way to use the ciphertext to retrieve the plaintext.

Hash algorithms

- Hashing functions
- Collision attacks
- Common hash algorithms
  - SHA
  - Message Digest

Common uses of hashing functions -

- **Websites like Facebook will store the hash, not your username/password.**

- Hashing functions are used to
  - Store computer passwords
  - Ensure message integrity
- The hash value is also reproducible by anyone else running the same algorithm against the same data.
- This means you can
  - Create a file.
  - Get its hash value.
  - Send the file and the hash to someone.
  - They can run the file and get it hash value as well.
  - If the hashes match, the file is in complete tact.

COLLISION ATTACK -

- A collision attack is used to compromise a hash algorithm.
- It occurs when an attacker finds two different messages that hash to the same value.
- This attack is very difficult and requires generating a separate algorithm that attempts to find a text that will hash to the same value of a known hash.
- This must occur faster than simply editing characters until you hash to the same value, which is a brute-force type attack.
- Hash functions that suffers from collisions lose integrity.
- An attacker that can make two different inputs hash to the same value, can trick people into running malicious

algorithm.

- MD algorithms work in the same manner as SHA:
  - They use a secure method to compress the file and generate a computed output of a specified number of bits.
- The MD algorithms were all developed by Ronald L. Rivest of MIT.
  - MD2
  - MD4
  - MD5

- MD2
  - Developed in 1989; an early version of MD5
  - It takes a data of any length and produces a hash output of 128 bits.
  - MD2 is optimized for 8-bit machines.
    - MD4, MD5 are optimized for 32-bit machines.
- MD4
  - Developed in 1990; optimized for 32-bit computers
  - It is a fast algorithm, but it is subject to more attacks than more secure algorithms such as MD5.
  - It has been shown to be vulnerable to collision.
  - As such, most people use MD5 instead.

MD5:

- Developed in 1991 and is structured with additional security to overcome the problems in MD4.
- Very similar to the MD4 algorithm, only slightly slower and more secure.
- Creates a 128-bit hash of a message of any length and segments the message into 512-bit blocks.

DES (Data Encryption Standard)

Data Encryption Standard (DES)

- Developed in 1973, adopted as a federal standard in 1976
  - Block cipher
  - The block size is 64 bits—64 bits of plaintext gives you 64 bits of ciphertext.
  - 56-bit key length
  - Performs a substitution and permutation (a form of transposition) based on the key 16 times on every 64 bit block.
- While DES has been a common business standard for 20 years, modern computing power has made the key breakable.
- NIST now certifies Advanced Encryption Standard (AES) to

3DES -

3DES

- Triple DES (3DES) is a variant of DES.
  - Depending on the variant, it uses either two or three keys.
  - Multiple encryption - goes through the DES algorithm three times.
- 3DES is stronger than DES but has similar weakness.
- The longer key length makes it more resistant to brute force attacks.
- 3DES is a good interim step before the new encryption standard, AES.

Asymmetric Encryption -

Asymmetric encryption

- Asymmetric Cryptographic Algorithms
  - Also known as public key cryptography
  - Uses two keys instead of one

type attack.

- Hash functions that suffers from collisions lose integrity.
- An attacker that can make two different inputs hash to the same value, can trick people into running malicious code.

SHA in a nutshell -

- SHA stands for **secure hash algorithm**.
- Refers to four hash algorithms published by the **National Institute of Standards and Technology (NIST)** and the **National Security Agency (NSA).**
  - Federal Information Processing Standards (FIPS) 180-2
- Applies compression function to data input.
  - Accepts up to 2^{64} bits or less and then compresses it down to a smaller number of bits
    - i.e. – 160 bits for SHA-1

- SHA-1, SHA-256, SHA-384, SHA-512
- SHA-1 was one of the more secure hash functions.
  - But it has been found to be vulnerable to a collision attack.
- These longer versions are referred to as SHA-2.
  - SHA-224, SHA-256, SHA-384, and SHA-512
  - All have longer hash results, and are more difficult to attack successfully.
- SHA-2 does require more processing power to compute the hash.
- NIST announced of winner of SHA-3 in October 2012.
- The SHA-3 algorithm will not be drawn from SHA-2.
- The SHA-3 standard was released by NIST on August 5, 2015

Symmetric Encryption -

Symmetric Encryption cont

- Symmetric algorithms are important because:
  - They are comparatively fast.
  - Have few computational requirements
- Their main weaknesses:
  - Two geographically distant parties both need to have a key that matches the other key exactly.
  - Simple keys can quickly be brute-forced.
  - Secure key exchange can be an issue.

AES (Advanced Encryption Standard) - 'is more secure'

Advanced Encryption Standard (AES)

- AES is a block cipher that separates data input into 128-bit blocks.
  - Can also be configured to use blocks of 192 or 256 bits.
- AES can have key sizes of 128, 192, and 256 bits, with the size of the key affecting the number of rounds used in the algorithm.
  - Longer key versions are known as AES-192 and AES-256, respectively.
- No efficient attacks currently exist against AES.

d0 03 c7 fe 0f 37 f2 1d d4 7f 68 63 ee 3c 6c aa

RSA ( ) -

RSA

- Ron Rivest, Adi Shamir, and Leonard Adleman (RSA)
- One of the first public key cryptosystems invented.

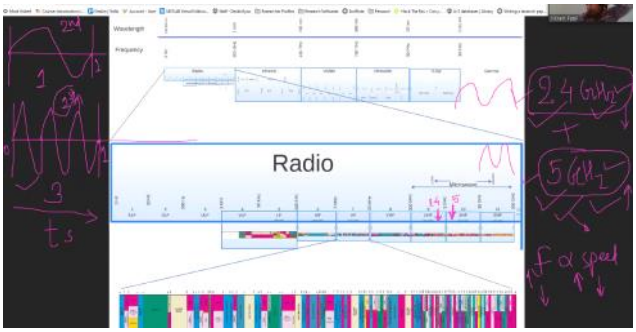
- Asymmetric Cryptographic Algorithms
  - Also known as public key cryptography
  - Uses two keys instead of one
    - One is known as public key and one is known as private key
  - Keys are mathematically related
    - Public key is known to everyone and can be freely distributed
    - Private key is known only to the individual to whom it belongs
    - Security relies upon resistance to deducing one key, given the other.
  - Symmetric encryption algorithms include:
    - RSA, Diffie-Hellman, ElGamal, ECC (Elliptic Curve Cryptography)

- Important principles regarding asymmetric cryptography:
  - Key pairs
    - Requires a pair of keys
  - Public key
    - Do not need to be protected
  - Private key
    - Should be kept confidential
  - Both directions
    - Keys can work in both directions (encryption and decryption)

- It typically works by using hard math problems.
- A common method relies on the difficulty of factoring large numbers.
- Computers can easily multiply very large primes with hundreds or thousands of digits but cannot easily factor the product.
- They also form the basis for digital signatures.

Asymmetric Encryption Summary

- Creates the possibility of digital signatures and corrects the main weakness of symmetric cryptography.
- Ability to send messages securely without senders and receivers having had prior contact.
- Digital signatures enable faster and more efficient exchange of all kinds of documents.
- With strong algorithms and good key lengths, security can be assured (in isolation).



Wi-fi Equipment
NIC Adapter - sends and gathers wireless capabilities
Runs through drivers

Modems convert analogue signal into a digital signal and digital signal into a analogue signal

- Wi-Fi equipment
  - Mobile device needs a wireless client network interface card adapter (wireless adapter)

- Ron Rivest, Adi Shamir, and Leonard Adleman (RSA)
- One of the first public key cryptosystems invented.
  - Published in 1997
  - Used for encryption and digital signatures
  - Uses the product of two very large prime numbers (between 100 and 200 digits long and of equal length)
- While a simple algorithm, it has withstood the test of more than 20 years of analysis.
- Does not replace symmetric encryption because RSA is 100 times slower than DES!
- Asymmetric encryption is used to exchange symmetric keys.

Mobile networks means wireless networks - this will cover mobile devices and related risks.

Most users, spend most of there time using wireless devices.
1 out of 4 searches are made from a wireless device.

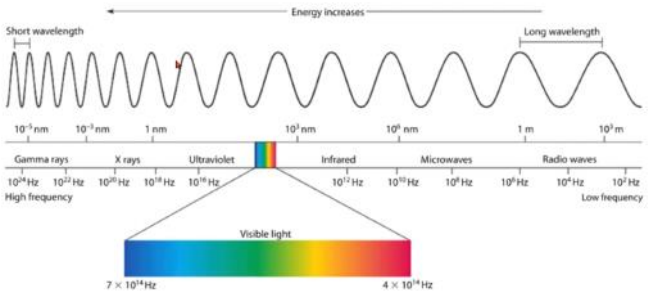
- Users now spend over half of computing time each day using a mobile device
- Four out of every five web searches today are performed on a mobile device
- Wireless networks have become a prime target for attackers
  - Attempt to capture unprotected wireless signal

Wi-fi & Bluetooth

Attacks Through Wireless Networks

- Popular types of wireless networks
  - Wi-Fi
  - Bluetooth
- Wi-Fi networks
  - Wireless local area network (WLAN)
  - Use radio frequency (RF) transmissions
  - Devices in range of a connection device can send and receive information
- Institute of Electrical and Electronics Engineers (IEEE) responsible for establishing Wi-Fi standards

Increaser Frequency > Wave length will increase



	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac
Frequency	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	2.4 & 5 GHz	5 GHz
Nonoverlapping channels	3	3	23	3	21	21
Maximum data rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	7.2 Gbps
Indoor range (feet/meters)	65/20	125/38	115/35	115/35	230/70	115/35
Outdoor range (feet/meters)	328/100	460/140	393/120	460/140	820/250	460/140
Standard ratification date	1997	1999	1999	2003	2009	2014

Mobile Device Security

- Wi-Fi equipment
  - Mobile device needs a wireless client network interface card adapter (wireless adapter)
  - Special software is needed to translate between the device and adapter
    - Included in all OSs today
  - Wireless broadband router
    - Mostly used for home-based Wi-Fi networks
    - Base station for sending and receiving signals
    - Gateway to the Internet

- Access point (AP)
  - More sophisticated than a wireless router
  - Used in a business or school setting
  - Signals can only be transmitted for several hundred feet
  - Multiple APs are used to provide "cells" or areas of coverage
  - Users move (called *roaming*) from one cell to another
    - A *handoff* occurs so that the AP user is closest to becomes the new base station

Tablet, Mobile and Laptop are mobile devices.

- Securely configure a home wireless network
  - Secure the router
  - Turn on Wi-Fi Protected Access 2 (WPA2) Personal
- Securing the Wireless Router
  - Lock it down by password protecting access to its internal configuration settings
- Router remote management settings
  - Allows configuration through the internet
- Recommendation: disallow remote management unless needed

- Device Setup
  - Disable unused features
    - Can serve as a threat vector
  - Enable lock screen
    - Prevents mobile device from being used until user enters correct passcode:
      - PIN, password, swipe pattern, fingerprint touch ID
    - Some devices can be configured with additional protections:
      - Extended lockout period
      - Reset to factory settings

Summary - discussed how Wi-Fi and wireless networks work.
Discussed different standards of Wi-Fi
What router is
What ac is
Evil twin
Attacks related to Bluetooth
Defensive techniques for mobile devices

(feet/meters)						
Standard ratification date	1997	1999	1999	2003	2009	2014

Mobile Device Security

- Best Practices
  - Do not erase built-in limitations (called jailbreaking)
  - Do not sideload unapproved apps
  - Use appropriate sanitization and disposal procedures for mobile devices
  - Back up data stored on mobile device regularly
  - Do not call phone numbers contained in unsolicited emails or text messages
  - Be aware of current threats affecting mobile devices

- Device Loss or Theft
  - Keep mobile device out of sight when traveling in high-risk area
  - Avoid becoming distracted by what is on the device
  - When holding a device, use both hands
  - Do not use the device on escalators or near transit train doors
  - White or red headphone cords may indicate they are connected to an expensive device
    - Change to less conspicuous color

- Device Loss or Theft (cont'd)
  - If theft does occur, do not resist or chase the thief
    - Contact organization or wireless carrier and change all passwords for accounts accessed on the device
  - Security features can be used to locate the device or limit damage

Security feature	Explanation
Alarm	The device can generate an alarm even if it is on mute.
Last known location	If the battery is charged to less than a specific percentage, the device's last known location can be indicated on an online map.
Locate	The current location of the device can be pinpointed on a map through the device's GPS.
Remote lockout	The mobile device can be remotely locked and a custom message sent that is displayed on the login screen.
Thief picture	A thief who enters an incorrect passcode three times will have her picture taken through the device's onboard camera and emailed to the owner.

Table 5-4 Security features for locating lost or stolen mobile devices

Security feature	Explanation
Alarm	The device can generate an alarm even if it is on mute.
Last known location	If the battery is charged to less than a specific percentage, the device's last known location can be indicated on an online map.
Locate	The current location of the device can be pinpointed on a map through the device's GPS.
Remote lockout	The mobile device can be remotely locked and a custom message sent that is displayed on the login screen.
Thief picture	A thief who enters an incorrect passcode three times will have her picture taken through the device's onboard camera and emailed to the owner.