Dr. Raimund K. Ege
Northern Illinois University, USA

**Cyber-Security:**
*Current Practice and Future Trends*

---

**Overview of presentation**

- Introduction
- Basic concepts
- Tools and practices
- Outlook
Introduction

- me: researcher & teacher
  - object orientation
  - software architecture
  - computer and information security

- you?

Basic concepts: Overview

- the security problem today
- security incidents
- types of security threats
- avenues of attack
Comparisons indicate that:
- Average bank robbery amounts to $2,500
- Average bank fraud amounts to $25,000
- Average computer crime amounts to $500,000

**Annual computer crime loss: $5 - $10 billion**

**but:**
- large aspects of business life are conducted online
- significant aspects of personal life involve online activities

**Incident categories**

- Crimes in which the computer is the target of the attack
- Incidents in which the computer is a means of perpetrating a criminal act
- combination of both:
  - attack one computer to gain access to it
  - use this computer to launch DOS attack against other
**Attack consequences**

- A loss of **confidentiality** where information is disclosed to unauthorized individuals
- A loss of **integrity** where information is modified by unauthorized individuals
- A loss of **availability** where information or the systems processing it are not available for authorized users

**Types of attacks**

- viruses, worms and phishing
- intruders
  - hacker: script kiddy vs. elite hacker
- insider
  - most harmful
- criminal organization
  - structured attack
- terrorist and information warfare
  - targets critical infrastructure
History of security incidents

- Morris Worm
- Melissa
- ILOVEYOU
- Code Red
- Slammer

Morris Worm (November 1988)

- released by graduate student Robert Morris
  - exploited sendmail, finger, rsh
  - accident: excessive replication

- purpose: gauge size of Internet
  - infected 10 percent of machines (approximately 6,000) connected to the Internet at that time

- caused an estimated $100 million in damage
  - loss of computing resources
Melissa (March 1999)

- spread via email
- has MS Word attachment (.doc)
  - macro examines user’s address book
  - sends email via MS Outlook to first 50
- no harm intended (originally)
- clogged email services

ILOVEYOU (May 2000)

- spread via email
- has VisualBasic attachment (.vbs)
  - examines MS Outlook email
  - sends email to contacts
- clogged email services
- overwrote files
**Code Red (July 2001)**

- buffer overflow attack on MS IIS web servers
- defaced website as:
  
  HELLO! Welcome to http://www.worm.com! Hacked By Chinese!

- replicated itself to other IIS servers

- waited 20-27 days for DoS attack on fixed set of IP addresses

---

**Slammer (January 2003)**

- buffer overflow attack on MS SQL Server

- sent itself out to random IP addresses

- caused Internet traffic congestion
as Internet became more prevalent, it became vehicle for malicious exploits

- recent threats:
  - email → spam
  - websites
Email attachments: file formats

- executables
  - .exe .cmd .bat .com .dll .pif .vbs ...
- hidden extensions
- hidden double extensions
  - .gif .exe ...

moreover:
- file type associations

Email attachments: file formats

- even seemingly innocent file types:
  - .gif
  - .pdf
  - .wmf
  - .zip
Threat: SPAM

- 120 billion spam emails per day world-wide
- 77% of emails are spam on average
- modern delivery vehicle for
  - email attachments

Example: storm worm

- discovered January 2007
- backdoor Trojan horse
  - email that reports on storm in Europe
  - has executable attachment
  - opens infected host to remote control
- world’s most powerful supercomputer
  - peer-to-peer botnet
Storm email subjects:
“230 dead as storm batters Europe”

- A killer at 11, he's free at 21 and kill again!
- U.S. Secretary of State Condoleezza Rice has kicked German Chancellor Angela Merkel
- British Muslims Genocide
- Naked teens attack home director
- Radical Muslim drinking enemies's blood
- Chinese/Russian missile shot down Russian/Chinese satellite/aircraft
- Saddam Hussein safe and sound!
- Venezuelan leader: "Let's the War beginning"
- Fidel Castro dead
- FBI vs. Facebook

Storm email attachments

ATTACHMENT TYPES: .EXE .PDF .ZIP ...

- Postcard
- ecard
- FullVideo
- Full Story
- Video
- Read More
- FullClip
- GreetingPostcard
- MoreHere
- FlashPostcard
- GreetingCard
- ClickHere
- ReadMore
- FlashPostcard
- FullNews
- NflStatTracker
- ArcadeWorld
- ArcadeWorldGame
Storm worm behavior

- patience: has active and inactive periods
- separation of duties:
  - small number of hosts spread worm further
  - smaller number of hosts serve as control
  - large number of hosts wait for tasks
- no damage, little impact on host
- constant change
  - delivery mechanism, payload
  - DNS manipulations: “fast flux”

Storm worm summary

- scale: 1 to 10 million infected hosts
  - billions of spam per day
  - estimate: running at only 10-20% of capacity
- commercial purpose
  - reports of partitioning
  - reports of stock manipulation
- rumors of being leased to criminal groups
- who controls storm?
**Perspectives on protection**

- provide user education
  - as simple as strong password
- provide physical protection
  - don’t lose your laptop
- provide host protection
  - patch, patch and patch
- provide network protection
  - watch and examine traffic

**Poor Security Practices**

- Password selection
  - harder passwords are harder to remember
- e-mail and web-surfing practices
- Installing unauthorized hardware and software
Human Attacks

- Piggybacking and shoulder surfing
- Dumpster diving

- Social engineering
  - gain trust of insider
    - people generally want to help somebody who is requesting help
    - people generally want to avoid confrontation
  - Reverse social engineering

Perspectives on protection

- provide user education
  - as simple as strong password
- provide physical protection
  - don’t loose your laptop
- provide host protection
  - patch, patch and patch
- provide network protection
  - watch and examine traffic
Access control

- Protect infrastructure
  - access to building
  - access to computer
  - access to network equipment

- Authentication
  - Discretionary vs. mandatory access control
  - Role-based access control

 Perspectives on protection

- provide user education
  - as simple as strong password
- provide physical protection
  - don’t loose your laptop
- provide host protection
  - patch, patch and patch
- provide network protection
  - watch and examine traffic
Security Principles

- Least privilege
- Layered security
- Diversity of Defense
- Security through obscurity
- Keep it simple

Security Operations

- Policies
  - Management statements of what the organization wants to accomplish
- Procedures
  - Step-by-step instructions on how employees are expected to act in a given situation or to accomplish a specific task
- Standards
  - Mandatory elements regarding the implementation of a policy
- Guidelines
  - Recommendations relating to a policy
Every security technique and technology falls into at least one of the three elements of the equation.

- Access controls
- Firewalls
- Encryption
- Audit logs
- Intrusion detection systems
- Honey pots
- Backups
- Incident response teams
- Computer forensics

Summary of concepts

- Cyber security is a real concern
- Human element is large

- Protection is possible
  - Education
  - Tools and practices
Part II: overview of presentation

- Introduction
- Basic concepts
- Tools and practices
- Outlook

Tools and Practices

- Encryption
  - types
  - algorithms
- Public Key Cryptography
  - PKI
  - PGP
Encryption concepts

- plain-text vs. cypher-text
- encryption algorithm: public
  - convert plain-text into cypher-text
- encryption key: secret
  - additional input to encryption algorithm

Encryption history

- Spartans used a ribbon wrapped around a specific gauge cylinder and then wrote on the ribbon
  - when unwrapped, the ribbon appeared to hold a strange string of letters
  - message could be read only when someone wrapped the ribbon back around the same gauge cylinder
- Romans used shift cipher
  - One letter of the alphabet is shifted a set number of places in the alphabet for another letter
Encryption Modes

- Computers enable more complex encryption algorithms

- Modes of encryption include:
  - Symmetric
  - Asymmetric
  - Hash functions

Key Complexity

- Key complexity = degree of security of the system
  - Key complexity = number of possible key values
  - Keyspace depends on size of key value
    - 48bit vs. 64bit vs. 128bit vs. 192bit vs. 256bit

- Brute-force attack: attempting every possible key
Sender and the receiver use same key
- requires key management
- key must be exchanged by other means

**Symmetric Encryption Algorithms**

- **DES**: Data Encryption Standard
  - 54bit shared key, judged as weak
- **3DES (Triple DES)**
  - uses three keys instead of the single key
  - spins through the DES algorithm three times
- **AES (Advanced Encryption Standard)**
  - key sizes: 128, 192, 256 bits
  - no known successful attacks
- **others**:
  - CAST, Rivest Cipher (RC)
  - Blowfish, IDEA (International Data Encryption Algorithm)
Asymmetric Encryption

- Sender and receiver use different keys
  - algorithm involves difficult math problems
  - also known as public key cryptography

- RSA
  - uses product of two large prime numbers (100 to 200 digits) to generate one key for decryption and another for encryption
  - used for 20 years, but much slower than DES
- Diffie-Hellman
  - also uses large prime numbers
  - used in SSL, SSH and IPsec protocols to establish session key
- others:
  - ElGamal: used by US government
  - ECC: uses elliptic curve function
Encryption Mode: Hashing

- Apply hash function to plain-text
  - is a special mathematical function that performs one-way encryption to produce cipher-text

- Common uses of hashing:
  - storing computer passwords
  - ensuring message integrity

Example: Message Digest (MD)

- Message Digest (MD) is the generic version of one of the three algorithms
  - MD2
    - digest length: 124 bits, optimized for 8-bit machines
    - successful attacks are known
  - MD4
    - 124 bits digest, optimized for 32-bit computers
    - collision attack successful in under 1 minute on PC
  - MD5
    - 124 bits digest, slower but improved algorithm
    - no known successful attacks
Public Key Cryptography

- Goal: ensure secure communication
- Each party has public/private key pair
- Encryption used to ensure
  - confidentiality of communication
  - identity of parties

Example scenario

- Alice and Bob want to exchange email
- Step 1: Alice and Bob each create key pair
- Step 2: Alice and Bob publish their public keys (and keep their private keys private)
Example scenario:  
Bob sends email to Alice

- Bob encrypts email with Alice’s public key

  - Observations:
    - email is confidential
    - only Alice can read email
    - but:
      - Alice is not assured that Bob sent email

- Alice decrypts email with her private key

Example scenario:  
secure emails between Alice & Bob

- Bob encrypts email with Alice’s public key
- Bob signs email with his private key
  - Alice authenticates email with Bob’s public key
  - Alice decrypts email with her private key
Facit: can we trust a public key?

- need public key repository
- protocols to ensure integrity of keys
- approaches:
  - PGP
  - PKI

Public Key Infrastructure

- framework to enable secure communication

- via
  - key management for encryption
  - certification of identities
PKI elements

- **Keys**: public and private
- **Certificates**: to hold keys
- **Authorities**: to register & verify

For:
- E-mail clients
- Virtual private network products
- Web server components
- Domain controllers

Example: email from Diane to John

1. Diane signs the message.
2. Diane encrypts John’s public key.
3. Diane uses John’s public key for encryption purpose.
Basics of Public Key Infrastructures

- PKI involves registration & certificate authorities
  - individual requests registration
    - requires proof of identity
    - identity information is validated
  - registration authority (RA) tells certificate authority (CA) to generate a certificate
  - certificate authority signs certificate with its private key

Obtaining a Digital Certificate

1. The user requests a digital certificate
2. Some requests to issue a certificate are denied
3. The user's information, such as name and email, is validated
4. The information is stored in a database and a verification
5. Once verified, the user provides a public key and certificate information is sent to the CA
6. The CA generates a digital certificate containing the public key and the user's identifying information
7. The certificate is sent to the user
Registration Authority

- RA accepts a request for digital certificate
- RA perform the necessary steps of registering and authenticating the person requesting a certificate
- Certificate classes:
  - I: encrypt and sign email
  - II: sign software
  - III: become CA
- classes require different authentication levels

Certificate Authority

- CA is trusted authority for certifying an individual's identity
- CA issues digital certificate
  - certifies association between subject's identity and a public key
  - private key that is paired with the public key in the certificate is stored separately
  - certificate is signed with CA's private key
**Certificate Example**


**PKI example: email from Joyce to Maynard**

[Diagram showing the process of sending an email using PKI.]
Trust and Certificate Verification

- Browsers have a long list of CAs configured to be trusted by default

![Certificate Manager](image)

Revocation

- Certificates are revoked when the certificate's validity needs to be ended before its actual expiration date:
  - private key has been exposed
    - ex.: social engineering attack, laptop lost, ...
  - data in certificate no longer applies to subject
    - ex.: employee left a company
- CA maintains certificate revocation list (CRL)
  - CRL must be secured:
    - signed with CAs private key
  - CRL should be distributed
PKI Standards and Protocols

- Business processes
- Applications
- Standards & Protocols
- PKI implementation level

PKIX & PKCS
X.509, ISAKMP, CMP, XKMS

SSL, TLS, S/MIME
WTLS, WEP, IPsec

March 1, 2009

Example: SSL/TLS

- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
  - most common means of interacting with a PKI and certificates
- ensures privacy between communicating applications and their users on the Internet
**Illustration: TLS handshake**

- Client hello, random value, and algorithm list
- Server hello, server's random value, certificate, and optional certificate request
- Client certificate (optional)
- Pre-master secret (encrypted)
- Client and server generate master secret
- Change cipher spec (start using encryption)
- Server changes record layer security state
- Client finished
- Server finished
- Exchange application data

**PGP: Pretty Good Privacy**

- alternative to PKI
- based on: Web of trust
- decentralized grass-roots model
- created by Philip Zimmermann in 1991
- implemented by
  - PGP
  - OpenPGP
  - GnuPG
**PGP setup**

- PGP program is installed locally
- PGP program creates public/private key pair for user
- Public key is deposited in public key server
- Keys of other parties can be retrieved from public key server(s)

**Sending email with PGP**

- Message is encrypted using symmetric encryption and chosen session key
- Session key is encrypted with user’s private key
- Session key is encrypted with recipient’s public key
Receiving email with PGP

- Session key is decrypted with user’s private key
- Session key is decrypted with sender’s public key
- Message is decrypted using session key

PGP uses RSA or Diffie-Hellman

- RSA version
  - IDEA algorithm to encrypt with short symmetric key
  - RSA to encrypt IDEA key
  - Diffie-Hellman version
    - CAST algorithm to encrypt the message
    - Diffie-Hellman algorithm to encrypt the CAST key
PGP Digital Signature

- digital signature created by hash function on user's name and other signature information
  - hash value is encrypted with the sender's private key
  - receiver uses the sender's public key to decrypt the hash value
  - decrypted hash value must match hash value sent as the digital signature for the message

PGP example: GnuPG

- Open source software
- Gnu Privacy Guard
  - gnupg.org

- Thunderbird email client plugin
  - EnigMail
  - enigmail.mozdev.org
**Generate Key pair**

![Key generation interface](image1)

Note: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Activating or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.

**Look up public key**

![Public key lookup interface](image2)
Look up public key

Key Management

March 1, 2009  GlobeNet 2009 - Tutorial T1: Ege - CyberSecurity
Upload public key

Compose email
Send email

Receive email
Summary

- Encryption
- Public Key Cryptography
- PKI
- PGP

Part III: overview

- Introduction
- Basic concepts
- Tools and practices
- Outlook
Security landscape

- Current attacks and their effectiveness
- Best practices to mitigate
  - threat level
  - attack impact
- to keep Internet usage useful!

Modern attacks

- Email
  - attachments
  - phishing
  - html
- Browser
  - security holes
  - spoofing
  - malicious code
- OS
**Protection plan**

- Establish secure baseline
- Increase security
- Hardening operating systems
- Hardening network
- Hardening applications

**Secure baseline**

- be wary of default configurations
  - installation's goal is to ensure positive user experience
  - huge variety in installation environment
- security is becoming more prevalent
- need secure baseline
  - ease of administration
  - speed of recovery
Guidelines for OS Baseline

- apply all service packs and patches
  - install anti-virus software
  - install anti-spyware software
  - install spam filter
  - configure automatic notification and update

- create and enforce password policy
  - password aging
  - password audits
  - no password recycling

Guidelines for OS Baseline

- restrict permissions on files and directories
  - remove all unnecessary file shares
  - possible remove File And Printer Sharing protocol
  - set appropriate ACLs on all necessary file shares
  - disable unnecessary services
  - remove unnecessary users
  - disable or remove unnecessary programs
  - enable security event auditing
Network Hardening

- routers, switches, and access points
  - remove defaults: ID/user/password
  - control network access
  - apply updates and patches

- traffic filtering: firewall
  - elements: rules that accept vs. deny traffic
  - bandwidth/throughput sensitive
  - advanced rules to control traffic:
    - port/service specific
    - stateful traffic analysis
    - intelligent decisions

Application Hardening

- Secure applications against local and Internet-based attacks
  - Remove unneeded functions or components
  - Restrict access where you can
  - Make sure application is kept up-to-date with patches
**Web Servers**

- most common targets for attack
  - IIS vs. Apache
- web server hardening
  - apply all updates and patches
  - remove all unnecessary files: sample files
  - set permissions for all files and directories
  - only enable required components

**Mail Servers**

- mail server is also common target
  - reconnaissance: VRFY, EXPN
  - relaying
  - buffer overflows
- apply all updates and patches
  - MS Exchange, sendmail
  - others: postfix, qmail, Exim
  - system-wide virus, malware & spam scan
FTP Servers

- Enables remote access to files
- Hardening
  - Apply updates patches
  - Control permissions
    - Files/directories
    - Users
    - Hosts

DNS Servers

- Translation between FQDN and IP address
- Hierarchical lookup model
- Common implementation: Berkeley BIND
- Common attacks
  - Reconnaissance, zone transfer
  - Spooﬁng
- Hardening
  - Apply updates and patches
  - Zone keys
**File and Print Services**

- restricted to authorized, authenticated users
  - users may stop, pause, or delete their own print jobs
- spool queue access only for administrators

**Directory Services**

- Enable single login
  - multiple applications, data sources, and systems
  - certificate and encryption capabilities
- Domain-based hierarchy
  - schemas for multiple purposes
- Common systems
  - MS Active Directory
  - OpenLDAP
  - Novel eDirectory
**User level precautions: email**

- attachments, phishing, html

- protection:
  - use latest version of email client
    - hide embedded images
    - alert to phishing attack
      (displayed URL differs from actual URL in html tag)
  - educate users
  - execute attachment in secure sandbox

**User level precautions: browser**

- Symptoms of a browser hijacking:
  - different homepage, search page or favorites
  - options in Internet settings have been changed
  - access is blocked to certain functions
  - redirection of incorrectly typed URLs

- protection:
  - use latest version of browser
  - disable scripting: ActiveX, JavaScript
    - don’t trust any browser pop-up
  - run browser in sandbox
**Browsers Trends**

- control web navigation
  - via search engine, e.g. Google SafeSearch
  - via URL parsing tools:
    - Web of Trust
    - OpenDNS

**Google SafeSearch**

- Blocks web pages containing explicit sexual content from appearing in search results:
  - Use strict filtering (Filter both explicit text and explicit images)
  - Use moderate filtering (Filter explicit images only - default behavior)
  - Do not filter my search results
  - Labels “harmful sites” in search results
Safe Browsing
Diagnostic page for www.cull.com

What is the current listing status for www.cull.com?
This site is not currently listed as suspicious.

What happened when Google visited this site?
Of the 4 pages we tested on the site over the past 90 days, 8 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2019-02-15, and suspicious content was never found on this site within the past 90 days.
This site was hosted on 2 network(s) including ASEPST (TDS), AS19475 (APPLEDPS).

Has this site acted as an intermediary resulting in further distribution of malware?
Over the past 90 days, www.cull.com did not appear to function as an intermediary for the infection of any sites.

Has this site hosted malware?
No, this site has not hosted malicious software over the past 90 days.

March 1, 2009
GlobeNet 2009 - Tutorial T1: Ege - CyberSecurity

Safe Browsing
Diagnostic page for blog.jimnry.com

What is the current listing status for blog.jimnry.com?
This site is not currently listed as suspicious.

Part of this site was listed for suspicious activity 1 time(s) over the past 90 days.

What happened when Google visited this site?
Of the 98 pages we tested on the site over the past 90 days, 1 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2009-02-22, and the last time suspicious content was found on this site was on 2009-01-27.
Malicious software includes 1 scripting exploit(s). Successful infection resulted in an average of 1 new process on the target machine.
Malicious software is hosted on 1 domain(s), including 93.133.136.16.
This site was hosted on 1 network(s) including AS14700 (PEOPLE)

Has this site acted as an intermediary resulting in further distribution of malware?
Over the past 90 days, blog.jimnry.com did not appear to function as an intermediary for the infection of any sites.

Has this site hosted malware?
No, this site has not hosted malicious software over the past 90 days.

March 1, 2009
GlobeNet 2009 - Tutorial T1: Ege - CyberSecurity
If you did a Google search between 6:30 a.m. PST and 7:25 a.m. PST this morning, you likely saw that the message "This site may harm your computer" accompanied each and every search result. This was clearly an error, and we are very sorry for the inconvenience caused to our users.

What happened? Very simply, human error. Google flags search results with the message "This site may harm your computer" if the site is known to install malicious software in the background or otherwise surreptitiously. We do this to protect our users against visiting sites that could harm their computers. We maintain a list of such sites through both manual and automated methods. We work with a non-profit called StopBadware.org to come up with criteria for maintaining this list, and to provide simple processes for webmasters to remove their site from the list.

www.OpenDNS.com

- customized DNS lookup
  - modify name server setting
- filters FQDN translation to IP address

- provides:
  - anti phishing
  - parental controls
  - useful shortcuts
  - type correction
- setup via DNS server setting at:
  - individual workstation IP connection settings
  - router for whole network

- control via account at www.opendns.com
Web of Trust

- www.mywot.com
- community rating of websites
- implemented as browser add-on
  - Firefox or Internet Explorer
- as of February 2009:
  - Number of rated sites: 21,625,169
  - New this month: 275,365
  - Number of dangerous sites: 1,534,704

www.mywot.com

- annotates search results
- rates website

- controls hyperlinks on page
- demo at www.mywot.com/demo
Summary

- Threats are ever present
  - increasing sophistication
- Tools and practices
  - education of users is key
  - safety via encryption
  - peace of mind via modern tools
- Internet is here to stay!