TIM158
Business Information Strategy

Instructor: Safwan Shah

Teaching Assistant: Paul Vroomen
Lecture 10

• News Presentation
  – Group 1
  – Group 2

• Discuss Quiz

• Discuss Project Assignment
A Short History On:

Hacking

Hacking has been around as long as computers as a way to reconfigure or reprogram a system to give access to someone who otherwise shouldn’t have that access. In the media, any electronics manipulation is often referred to as hacking, though “cracking” may often be more appropriate. Thanks to hacking, computer geeks can be cool and dangerous.

1. The term hacker was coined by John Nash, the famous mathematician. (Russell Crowe from A Beautiful Mind).
   - Nash
   - Crowe
   - It was an insult, meant to describe someone who used a quick, elaborate solution to sidestep a problem.

2. One of the first technology hacks was discovered in 1972.
   - A whistle from a Cap n’ Crunch box was used to make free long distance phone calls.
   - The whistle’s frequency allowed access the phone company’s internal authorization system.

3. Ian Murphy was the first hacker to be convicted on felony charges.
   - He hacked AT&T in 1981 and changed the clocks, allowing people to get late-night discounts during midday and higher rates when they called at night.

4. Kevin Mitnick was at one time the most wanted hacker in the US.
   - Hacked into: DEC, IBM, Pacific Bell
   - Prosecutors believed he could launch a nuclear weapon by whistling into a pay phone.
5. GARY MCKINNON PERFORMED THE LARGEST MILITARY HACK OF ALL TIME. 

He says he was looking for evidence of a UFO cover up.


6. ALBERT GONZALEZ RECEIVED THE LARGEST JAIL SENTENCE FOR HACKING IN US HISTORY.

Prison Term: 20 YEARS

He stole 200 million credit and debit card numbers.

$200 million in damages.

7. THE US HAS THE MOST HACKED COMPUTERS THAT SPREAD SPAM.

13.1% of the world’s spam originates here.

Brazil is 3rd with 6.8%.

India is 2nd with 7.3%.

8. VIRTUAL HACKING SCHOOLS IN CHINA GENERATE $40 MILLION EACH YEAR IN REVENUE.

Students pay less than $100 to learn.

The schools have been linked to attacks against Google and the US government.

9. WORLDWIDE, HACKERS HAVE STOLEN AN ESTIMATED $1 TRILLION IN INTELLECTUAL PROPERTY.

Hacking costs the US $4 billion a year in damages.

It costs China $1 billion a year.
10. In 2009, 43% of 2,100 businesses surveyed by Symantec had lost proprietary info to hackers.

11. A survey of IT professionals revealed 1/3 of companies deal with hacking on a daily basis.

81% of professionals admit their systems are vulnerable.

17% of those hacks are successful.

12. The average power plant receives thousands of hack attempts a year.

13. The Department of Defense hires 250 hackers per year to help defend the US from cyber threats.

Hackers attempt to commit acts of terrorism and extort money. Millions are extorted every year.


15. Social networking sites like Facebook are some of the most commonly hacked in the world.

It will be $15-$30 billion per year within the next 5 years.

Hackers target personal information, like phone numbers, from profiles.
1. Denial of Service –
   • DoS attacks give hackers a way to bring down a network without gaining internal access. DoS attacks work by flooding the access routers with bogus traffic.

2. Distributed DoS –
   • Coordinated DoS attacks from multiple sources. A DDoS is more difficult to block because it uses multiple, changing, source IP addresses.

3. Sniffing –
   • Intercepting TCP packets. This interception can happen through simple eavesdropping or something more sinister.

4. Spoofing –
   • Sending an illegitimate packet with an expected acknowledgment (ACK), which a hacker can guess, predict, or obtain by snooping.

5. SQL injection –
   • A code injection technique that exploits a security vulnerability occurring in the database layer of an application. It uses normal SQL commands.

6. Viruses and Worms –
   • Self-replicating programs or code fragments that attach themselves to other programs (viruses) or machines (worms). Both viruses and worms attempt to shut down networks by flooding them with massive amounts of bogus traffic, usually through e-mail.
7. Back Doors -
Hackers can gain access to a network by exploiting back doors administrative shortcuts, configuration errors, easily deciphered passwords, and unsecured dial-ups. With the aid of computerized searchers (bots), hackers can probably find any weakness in the network.

8. Trojan Horses -
Trojan horses, which are attached to other programs, are the leading cause of all break-ins. When a user downloads and activates a Trojan horse, the software can take the full control over the system and you can remotely control the whole system.. great..!!! They are also reffered as RATs(Remote Administration tools). I've written about them here.
9. **Keyloggers**
Consider the situation, everything you type in the system is mailed to the hacker..!!
Wouldn't it be easy to track your password from that.. Keyloggers perform similar functionalities.. So next time you type anything.. Beware..!! Have already posted about keyloggers and ways to protect yourself from them.. read it here.

10. **BruteForcing**
The longest and most tiring job.. don't even consider this if you don't know the SET of password for your victim..

11. **Secret Question**
According to a survey done by security companies, it is found that rather than helping the legitimate users the security questions are more useful to the hackers.. So if you know the victim well try this..

12. **Social Engineering** –
Gains your trust ... con job.
13. Phishing –
You have to bring the user to a webpage created by you resembling the legitimate one and get him to enter his password, to get the same in your mail box.

14. Fake Messengers -
So its a form of phishing in the application format.. getting user, to enter the login info in the software.

15. Cookie Stealer -
Here the cookie saved by the sites are taken and decoded and if you get lucky.. You have the password..!!!

16. DNS Poisoning or PHARMING –
Redirecting automatically to a malicious page and get user data.

17. Whaling -
This method gets you the password of the accounts which are used by the hackers to receive the passwords.. So you just have to hack one ID, which is simplest method( Easy then hacking any other account, will tell you how in coming posts..) and you will have loads of passwords and so loads of accounts at your mercy..!!!
iPremier

• A case on crisis management
• How could iPremier have managed better
  – Procedures of crisis management
    • Who to call, when to call, ...
    • Doing failover testing, rehearsal, ..
    • Making sure logging is possible
    • Latest equipment
    • Maintaining a pre-emptive culture
    • ..
Questions

• What is like being woken up at 430 AM with a crisis in the making?
• What are iPremier’s priorities?
• How did iPremier perform in crisis? What could they have done differently?
• What information should iPremier share with the customers?
Lecture 11
8 May 2014

Reliability and Security in IT infrastructure
Agenda

- Presentations
- Feedback on Business Case Analysis
- Presentation format for Finals
Final Business Analysis Project

- May 15: Proposal
- May 24: Optional Draft
- June 7: Final paper
Format of Final Presentation

- Slide 0
  - Who are we? Why we chose the company? What is the main conclusion? This surprised us?

- Slide 1
  - Our analysis model

- Slide 2

- Slide 3

- Slide 4

- Slide 5

- Slide 6

- Slide 7
Reliability vs. Security

• What is the difference?

• What different scenarios need to be considered?
Reliability Basics

• Redundancy
  – Multiple paths through a network make the network robust to failing links

• Individual components are not so reliable
  – Buying backup equipment is possible, but sometimes expensive

• Redundancy can make more complex management challenges
Math of Availability

• Difference between 2% down in one business vs another
  – When might it go down?
  – Who is affected

• FRAMES ...
  – Flexible
  – Reliable
  – Available
  – Monitored
  – Extensible
  – Securely scalable
Fig 6.1 Five Components in Series

- Total availability of components in series requires all components to be available

\[
.98 \times .98 \times .98 \times .98 \times .98 = \text{service availability of 90%}
\]
Fig 6.2 Combining components in series decreases overall availability exponentially

- Increased number of components increases the likelihood that one of them is out

![Graph showing the decrease in availability with increasing number of components in series. The x-axis represents the number of components in series (each 98% available), and the y-axis represents availability. The curve shows a significant decrease as the number of components increases.]
Redundancy through parallel components

- All components have to fail in order for the link to fail

\[
\begin{align*}
\text{Component 1} & : 98\% \\
\text{Availability} & \\
\text{Component 2} & : 98\% \\
\text{Availability} & \\
\text{Component 3} & : 98\% \\
\text{Availability} & \\
\text{Component 4} & : 98\% \\
\text{Availability} & \\
\text{Component 5} & : 98\% \\
\text{Availability} & \\
.02 \times .02 \times .02 \times .02 \times .02 & = .0000000032 \\
\text{Probability of Failure} &
\end{align*}
\]
Fig 6.4 Redundancy increases availability
More general networks

- How do we calculate probability of failure in network?
- How do we recognize the critical vulnerabilities?
Calculating Reliability

• Combine parallel components first

\[
\text{Reliability(parallel)} = 1 - (\text{failprob})^k
\]

• Then combine series elements

\[
\text{Reliability(series)} = \text{product of individual reliabilities}
\]
High Availability Facilities

- Redundant power supply
- Physical security
- Climate Control
- Fire suppression
- Network connectivity
N+1 vs. N+N redundancy

• N+1 means one backup per type
• N+N means one backup per component
Security
Fig 6.5 Typical E-commerce Infrastructure

- Most components have redundancy
- Why not all?
Security against malicious threats

- Multiple different types of threats

**Normal Handshake**
- SYN: User’s PC says “hello”
- ACK-SYN: Server says “Do you want to talk?”
- ACK: User’s PC says “Yes, let’s talk”

**DoS Handshake**
- SYN: User’s PC says “hello” repeatedly
- ACK-SYN: Server says “Do you want to talk?” repeatedly
- No Response: User’s PC waits for server to “timeout”
Fig 6.7 distributed Denial of service attack
Fig 6.8 Spoofing

- Packets look like they came from another source
Intrusion

• Attacker gains access to internal IT structure
  – Usernames/passwords
  – Hacking using sniffer software

• Once inside, intruder can
  – Steal information
  – Alter data
  – Delete data
  – Deface programs/websites

• Detecting what someone has actually done is difficult
Viruses and worms

• Malicious software programs that replicate and spread to other computers
• Large range of potential damage
• Usually, viruses require user execution, whereas worms move automatically
• Recent examples target vulnerabilities, trigger cascade of events
Internal security threats

• Employees responding to phishing
• Laptop loss
• Access to previous employees not blocked
• Missing patches
• Forwarded emails with hidden threats
Malware (Malicious Software)

- Adware
  - Spyware collecting cookie information of personal web habits
- Browser Hijacker
  - Alter browser settings, redirect homepage, tell you your computer is infected etc.
- Internet Dialer
  - Making calls to -900 numbers on a dialup connection
- Keylogger
  - Monitor keystrokes
- Rootkit
  - Install malicious code, disable security features etc.
Defensive Measures

• Access and security policies
  – Who can read what?
  – Who can have an account?
  – Who is allowed to change what?
  – How is policy enforced?

• Firewalls
  – Collection of hardware, software to prevent unauthorized access of internal computer resources
  – Act like a security gate to check legitimate employees trying to use network
  – Filtering vs. relaying
Defensive Measures

• Authentication
  – Various levels (host, network etc.)
  – Any granularity possible (files, directories etc.)
  – Strong authentication requires complex passwords, often changing
  – Digital certificates
  – Biometric data

• Encryption
  – Uses a key to decode and decode message
  – Public/private combination
  – Only person with private key can decrypt
Defensive Measures

• Patching
  – Exploiting weaknesses in system is a primary strategy for attack
  – Knowing what has been patched is critical

• Intrusion detection and network monitoring
  – Automatically filtering out attacks is best
  – Logging and diagnostic systems help improve and detect what has actually happened
Security Management Framework

• Make Deliberate Security Decisions
• Consider Security a Moving Target
• Practice Disciplined Change Management
• Educate Users
• Deploy Multilevel Technical Measures, as many as can afford
Firewall deployment

• Should be part of solution – not whole
• Can become bottleneck if not managed well
• Rules should be carefully set up
  – Allow only traffic meeting criteria X (?)
  – Allow all traffic except that meeting criteria Y (?)
Spyware Protection: Ten Rules from IT security advisory

1. Teach employees to be cautious when opening attachments, particularly those sent from unknown sources.
2. Make sure employees understand the dangers of downloading and installing unauthorized programs from the Internet.
3. Compile and enforce an enterprise-wide policy for network firewalls and proxies that will prevent unauthorized downloads from Web sites both known or suspected to harbor spyware.
4. Provide users with passwords to access desktop computers, make sure they can only access systems with those passwords, and change them regularly.
5. Make sure email spam protections are set to the highest possible levels.
6. Make sure all browser security settings are set correctly, preferably at a minimum of “medium”
7. Make sure all the latest browser and operating system patches are installed on all desktop and server systems.
8. Make sure all security software installed is up-to-date and is using the latest version of the threat database.
9. Don’t provide regular network users with administrator privileges that will allow them to download and install such things as device drivers.
10. Install spyware scanning software at both the desktop and the Web gateway to provide a layered anti-spyware defense.
Virtual Private Networks

• Let distributed organizations and business partners communicate securely using public networks such as the Internet

• Traditionally, VPNs have employed Internet Protocol Security (IPsec).

• IPsec VPNs establish a protected tunnel between two fixed points – Eg. a corporate headquarters and a branch office

• Seamless solution from user perspective
Risk Management of Availability and Security

- Cannot afford to stop every possibility
- Expected loss is one measure (prob. x cost)
Incident Management (Recall last week’s case)

• Before
  – Sound infrastructure
  – Disciplined execution of operating procedures
  – Careful Documentation
  – Established Crisis Management procedures
  – Scenario testing

• During
  – Follow the plan!
  – Avoid emotional, over-optimistic or political influences

• After
  – Detect what has happened
  – Rebuild carefully
  – Document
  – Public Announcement Decisions
Security Improvement: CIO plan after failing an audit (Hengst article)

- Prioritize
- Assign Recovery Roles
- Require Status Reports
- Run Own Assessments
- Schedule Another Audit
Lecture 12
May 2014

Ford - Dell
Case Discussion
• Can Ford emulate Dell?
• Is mass customization possible?
  – To what extent
  – With what result?
• Can automobiles be delivered like PC’s
  – It is 10 years ago ...
Differences and Similarities

• Supplier network

• Purchasing methods
  – In Ford Procurement drove product
  – In Dell Product drove procurement

• Consumer cost

• Complexity of configurations

• Organizations

• Speed of obsolescence
• Consider the experiences that you (or your friends or members of your family) have had in buying a car; compare these to the experience of buying a computer online (if you’ve never done this, go to Dell’s website—www.dell.com—and explore how online computer buying works). What do you think explains the differences?
• What advantages does Dell derive from virtual integration? How important are these advantages in the auto business?
• What challenges does Ford face that are not also faced by Dell? How should Ford deal with these challenges?
• If you were Teri Takai, what would you recommend to senior executives? To what degree should Ford emulate Dell’s business model?
Ford

- Internet site – mid ‘95 (1m/day by mid ‘97)
- Intranet in mid-’96
- Extranet (B2B) ready by Jan 1997
- Created ANX with GM/C to set standards
- Jac Nasser CEO Jan ’99 (cost cutter)
- $6.9B profit in ‘98
- $1.7K profit per vehicle
- 4th behind Honda, Toyota, Nissan
Existing Supply Chain

- Thousands of suppliers
- Emphasis on fostering long term relationships with suppliers versus creating competition to reduce component cost
- Tier 1 suppliers managed T-2 suppliers ...