What are threats?

• What threats can you think of to your home?
• To your money (including bank accounts, checks, credit and debit cards)?
• To your home computer?

Digital Threats: More of the Same

• Theft
• Vandalism
• Extortion
• Con Games
• Fraud
• Stalking
• Voyeurism
Digital Threats: What’s Different

Automation
- Salami Attack from Office Space.

Action at a Distance
- Volodya Levin, from St. Petersburg, Russia, stole over $10 million from US Citibank. Arrested in London.
- Operators of CA BBS tried and convicted in TN court because TN had d/led pornography f/ CA.

Technique Propagation
- Criminals share techniques rapidly and globally.

Classes of Threats

Disclosure
- unauthorized access to data
  - Examples
  - copyright infringement
  - unauthorized CC use

Deception
- acceptance of false data
  - Examples
  - Anti-spam filter techniques
  - “Social engineering”

Disruption
- interruption of correct system operation
  - Examples:
  - DDOS attacks

Usurpation
- unauthorized control of system component
  - Example: Nicholas Jacobsen
  - Controlled T-mobile’s systems in 2004
  - Monitored e-mail, downloaded web-cam photos
  - Sold customer records (incl SSN, voicemail pw, etc)
Classes of Threats

Snooping
- interception of data
- Examples:
  - Reading email, or intercepting cleartext passwords.
  - ECHELON.

Modification
- Examples:
  - Changing student grades in War Games.
  - Website defacing (>1500/month recorded at attrition.org in 2005)

Spoofing
- impersonation
- Examples:
  - Spam emails almost always spoof source address.
  - The many Citibank phishing scams.

Classes of Threats

Repudiation of Origin
- Deny ordering goods.

Denial of Receipt
- Deny receipt of payment or goods.
- Examples
  - eBay
  - Credit card payments.

Denial of Service
- Examples:
  - Filling up disk with spam, unauthorized copies of files.

Types of Attacks Experienced

By Percent of Respondents

- Network Denial
- DoS/DDoS
- Malware
- Phishing
- Hacking
-钓鱼攻击
- 网络攻击
Survival Time 2010

Vulnerabilities
To realize a threat, attackers must exploit a vulnerability. Vulnerabilities can be in the:
- Virtualization system
- Operating system
- Networking stack of OS
- Web browser
- Applications
- User

Evolution of Vulnerabilities
Threat Information

- SANS Internet Storm Center (blog + statistics)
- Bugtraq (current mailing list)
- CERT (authoritative slow reports)
- IBM X-Force (semi-annual threat reports)
- Malware Domain List (dangerous DNS domains)
- Risks Digest (discussion)
- Symantec (monthly threat reports)

Who are the Attackers?

- Hackers vs Crackers
- Levels of attackers
  - Developer
    - Finds new security vulnerabilities
    - Writes tools and exploits
  - User
    - Understands tools; modifies tools/exploits
  - Script Kiddie

Who are the Attackers?

- Criminals.
  - 1993: Thieves installed bogus ATM at Manchester Mall. Saved account#s + PINs.
- Organized crime.
  - 2000: Mafia-led organization members arrested for attempt to steal $680 million from Bank of Sicily.
- Malicious insiders.
  - 2001: Mike Ventimiglia deletes files of his employer, GTE. $200,000 damage.
- Industrial espionage.
  - 2001: Verdicts in Cadence Design Systems vs. Avant against 7 employees incl CEO. 5 sentenced to jail.
Who are the Attackers?

Press.
- 1998: Cincinnati Enquirer reporter Michael Gallagher breaks into Chiquita Fruits voicemail to expose illegal activities.

Police.

Terrorists.
- 1999: DOS attacks and web defacements against NATO country computers during Kosovo bombings.

National Intelligence.
- 2000: Former CIA Director Woolsey admitted to using ECHELON information to help US companies win foreign contracts.

Two Types of Attackers

Targeted attackers focus on victims with more than a minimum value since to make their attacks worthwhile, they need:
- Concentration of value
- Visibility of extractable value

Automated attacks are scalable across millions of users and are worthwhile for the long tail of typical targets.

What Are Our Defences?

- Firewalls
- Virus Scanners
- Spyware Scanners
- Patches
- Backups

Prevent
Detect
Respond
Recover
What Are The Attacks?

- Phishing
- Malware
- Ransomware
- Spyware
- Botnets

Phishing E-mail

Dear Sky Bank customer,

We recently reviewed your account and suspect that your Sky Internet Banking account may have been accessed by an unauthorized third party.

Protecting the security of your account and the Sky Financial network is our primary concern. Therefore, as a preventive measure, we have temporarily blocked access to certain account features.

To remove your access errors, please take the following steps to ensure that your account has not been compromised:

1. Log in to your Sky Internet Banking account. In case you are not familiar with Internet Banking, you will have to fill in all the required information, including your name and your account number.

2. Review your account history for any unauthorized transactions or debits, and check your account profile to ensure no changes have been made. If any unauthorized activity has taken place on your account, report it to Sky Financial Group staff immediately.

To get started, please click the link below:

[Click Here]

Note: Sky Bank Financial Group. All rights reserved.

Phishing Site

Dear Sky Bank customer,

We recently reviewed your account and suspect that your Sky Internet Banking account may have been accessed by an unauthorized third party.

Protecting the security of your account and the Sky Financial network is our primary concern. Therefore, as a preventive measure, we have temporarily blocked access to certain account features.

To remove your access errors, please take the following steps to ensure that your account has not been compromised:

1. Log in to your Sky Internet Banking account. In case you are not familiar with Internet Banking, you will have to fill in all the required information, including your name and your account number.

2. Review your account history for any unauthorized transactions or debits, and check your account profile to ensure no changes have been made. If any unauthorized activity has taken place on your account, report it to Sky Financial Group staff immediately.

To get started, please click the link below:

[Click Here]

Note: Sky Bank Financial Group. All rights reserved.
Malware

- Trojan Horses
- Viruses
- Worms

Ransomware

How to pay to get your information back.
1. Click on this link to open your eGOLD account - the input screen is the eGOLD "Transfer and withdraw" page. You need to make the payment by clicking on the "2 ADD" button on the bottom of the page.
2. On the next page is the sign-up form.
   1. "Account name": here is where you name your account - top
      note is easy to remember (as you will be asked for it and
      reasonably short, example: "Cola's eGOLD", "My Hero eGOLD"
      or package "Hello" whatever you like. Just make it easy for
      you to remember.
   2. "One form": here, just repeat the account name (from 1 above).
   3. "One form": here, you can type your address, phone number, and email address (any email address can be used
      just have to be recommended you get your E-mail address - is a
      free normal email address).
   4. "Also remember your alias": this includes a fax number.
      (don't have a fax number? This company offers free fax to email
      services). Try and make it as easy as possible for eGOLD to on
   5. "Password": this is the most important piece of information
      connected to your eGOLD account. You can not change enough
      for your password, open a new account.
   6. "Sign up": here, just click "Sign up!"

Spyware and Adware

Most Trojan Horses, some infect directly.

- Browser hijacking
- Pop-up advertisements
- Keystroke and network logging
- Steal confidential data from email and files

80% of PCs are infected with spyware
(Oct 2004 AOL/NCSA survey.)
## Rootkits

- Execution Redirection
- File Hiding
- Process Hiding
- Network Hiding

### Diagram

```
User Program
  |
  | Rootkit
  |
  | OS
```

## Botnets

A worm or direct attack usurps control of a PC, then installs control software to listen for instructions. Instructions can include:

- Attempt to infect other PCs
- Send spam message
- Launch DOS attack
- Upgrade attack and control software
- Virus writers sell botnets to spammers for $0.10/compromised PC

## Advanced Persistent Threat

**Advanced** means the attacker can conduct attacks ranging from publicly available exploits to research new vulnerabilities and develop custom exploits.

**Persistent** means the attacker has a mission; they are not opportunistic intruders and will not stop attacking and find easier targets if they counter obstacles.

**Threat** means the attacker is not a piece of mindless code. The attackers are organized, funded, and motivated.
Key Points

- Computer crimes same as pre-computer crimes.
- Differences in digital threats
  - Automation
  - Action at a distance
  - Technique propagation
- Digital threats
  - Phishing
  - Malware
  - Ransomware
  - Spyware
  - Botnets

References

9. SANS Internet Storm Center, http://isc.sans.org/survivaltimephp