Keeping Yourself *and Your Customers* Secure

Gihan Dias

LK Domain Registry

Security is Important to a Network Operator

- True
- False

What is Security?

- A system is secure if you can rely on it to behave as it should
  - Not practically achievable
- Any system may be attacked by someone
  - or something

- You can never be *sure* your system is secure
  - But you can increase its likelihood

Why are Systems Insecure?

- Systems are not designed and built with security in mind
- People (we) are not aware (or don't care) of security implications of their acts
- Believe "It won't happen to me"
- So what if something happens?

What Can be Attacked?

- Your own systems
- Your customers
- The whole world

so what if your Customers are Attacked?

- Your responsibility to protect customers
- You may have to spend significant resources to deal with an attack on a customer
  - e.g. Bandwidth usage
- An unhappy customer is bad for you
- Good protection attracts better customers

so what if Someone Else is Attacked?

- If the attack come from your network, you will be blacklisted
- Your bandwidth will be used up
- An unsafe internet is bad for everyone

Who (or What) Could Attack?

- Hardware
- Systems Software
- Applications Software
  - Off-the-shelf
  - Made to order
  - In-house
  - User written
- Administrators and Operators
- Users
- Outsiders

Why would they Attack?

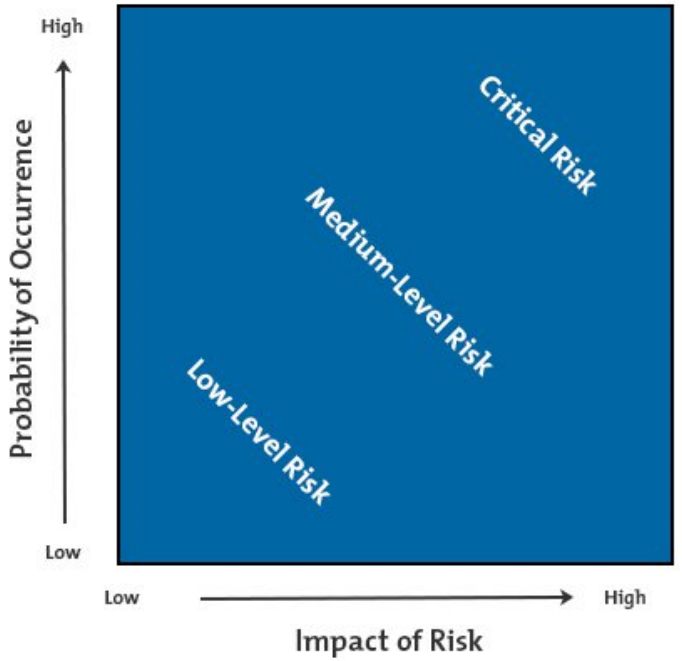
- For fun
- To gain points
- To make money
- For political or ideological reasons

What's needed for an Attack?

1. A Vulnerability
   - Some way to get in to your system
2. Threat Agent
   - Someone (or something) which wants to attack
   - Needs something from you
     - Maybe just CPU or IP address
3. For an attack to occur, some vulnerability must be exploited by some threat agent

Risk caused by a Threat

- Not all threats have the same impact
  - e.g. checking to see if a service is open
- Some threats are less likely to happen
  - e.g. Tsunami in Kandy
- Risk = Likelihood * Impact
- Don't worry about low-level risks
- Concentrate on critical ones



Risk Mitigation

- Reduce the likelihood
  - e.g. code securely
- Reduce the impact
  - e.g. hash your passwords

Some Types of Attack

- Attacks on Websites
- E-Mail attacks
- DDoS
- Ransomware
- Advanced Persistent Threats (APT)

Web Security

- Web is the most visible public-facing system of an organisation
- Often commercially valuable
- Most web designers and administrators unaware of security issues

OWASP Top 10 Most Critical Web Application Security Risks (2013)

A1 Injection

A2 Broken Authentication and Session Management

A3 Cross-Site Scripting (XSS)

A4 Insecure Direct Object References

A5 Security Misconfiguration

A6 Sensitive Data Exposure

A7 Missing Function Level Access Control

A8 Cross-Site Request Forgery (CSRF)

A9 Using Components with Known Vulnerabilities

A10 Unvalidated Redirects and Forwards

E-Mail based Attacks

- Still one of the most common vectors

- Spam
- Phishing
- Social engineering
- Hoaxes
- Malware

DDoS

- Using a large number of compromised devices to attack
- Easy, due to large number of devices with easily exploitable weaknesses
  - Now people have high-bandwidth connections
  - all the better to attack you with
- Now we have millions of IoT devices
- Remember:
- People will use you – and your customers – to launch attacks

Ransomware

- Encrypt you files and ask for Bitcoin
- Range from nuisance to major disaster
- Both clients and servers can be attacked

- Ensure your data is backed up frequently
- Ensure your backups are protected
  - Keep multiple backups
  - Keep off-line backups

Advanced Persistent Threats (APT)

- An attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time
- Has specific Objectives and Targets
- Willing to spend time and effort to achieve the targets
- Takes care to remain unobserved and progresses step-by-step towards the objective

Stages of an Attack

- Reconnaissance
- Scanning
- Access
- Escalation
- Exfiltration
- Sustainment
- Obfuscation

When do you need Security?

- Before
- During
- After
  the attack

When (cont.)

- Planning stage
- Programming
- Policy
- Operations
- Incident Response
- Audit

Planning

- Security must be designed into the system
  - not an “add on” or option
- Security features often cause
  - inconvenience to the user
  - affect system performance
  - add to cost
- Manager must balance security vs utility

Incident Response

- What do you do when you are hit?
- How do I get help?
- Who do you tell?
- What are your corporate and legal obligations?

Questions?

gihan@uom.lk