INTERPOL

PRIVACY AND SECURITY ON THE INTERNET

CYBER SECURUTY FORUM YAOUNDE-CAMEROON
22-26 APRIL 2013

BY ATEFOR TSEFOR Conrad, Regional Specialized Officer

OUTLINE

- Introduction
- INTERPOL global complex for innovation
- Threat assessment
- The Technology
- The Internet and Intranets
- Threats and Responses
- Conclusion

INTRODUCTION

- Why be concerned about Privacy and Security on the Internet?
- Internet is simply a way to communicate.
- It was not designed to protect the privacy of the information transmitted over it.
- Personal computers were designed to meet the needs of individual users.
- Designed to make information readily available, not to protect it.

INTERPOL GLOBAL COMPLEX FOR INNOVATION

INTERPOL

INTERPOL | GLOBAL COMPLEX FOR INNOVATION

ROLE OF INTERPOL

- **Use of I-24/7 and INTERPOL data bases**
- **International cooperation**
- **Technical assistance on request**
- **Criminal analysis on request**
- **Sharing of best practices**

INTERPOL

THREAT ASSESSMENT

- Assess accurately potential threats.
- Invest the resources needed to develop responses that neutralize them.
- Not all threats can or should be neutralized.
- Threats relating to personal computers and the Internet include;

INTERPOL

THREAT ASSESSMENT (Continuation)

- Unauthorized snooping,
- Interception of transmission over Internet as EMAIL,
- File tranfers, and www interactions,
- Impersonation (theft of identity).

INTERPOL

THE TECHNOLOGY

- ENCRYPTION
- Mathematical process of « scrambling » messages or files in a way that it can be reversed only with a specific password.
- XOR function, bit in the key is matched with a bit in the text.
- An important point about this algorithm:

  - knowing the algorithm does not help to decode the encrypted text.

THE TECHNOLOGY (continuation)

- Sufficiently long key that consist of random bits, algorithm nearly unbreakable.
- Available algorithms can be divided into two kinds:
- Weak and
- strong

INTERPOL

« SECRET KEY » ENCRYPTION

- « secret keys « are passwords that must be kept secret.
- Same key is used to encrypt and decrypt messages.
- Advantage: can be relatively small but difficult to crack.
- Disadvantage: Hard to share secret keys among all who need to know.

« Public key-Private key »Encryption

- « Public keys » and « Private keys » refer to pairs of keys derived from prime number mathematics.
- Part of assymetric encryption.
- Messages encrypted with your public key can be decrypted only with your corresponding private key.
- Messages encrypted with private key can be verified by decrypting with public key.

« Public key-Private key »Encryption(continuation)

- Advantage of assymetric encryption;
- - public key is not a secret
- - private key is secret (protected with secret password)
- Disadvantages;
- - larger keys required for adequate security
- - must be certain of public keys you use
- - You must keep your private key private

DIGITAL SIGNATURES

- Variation on encrypting a message with your private key.
- Mathematical summary of the message is created and encrypted.
- Anyone with your public key can verify that you signed the summary.
- Summary can be used to verify that the message has not been altered since it was signed.

CERTIFICATES OF AUTHORITY

- Are messages signed digitally by an independent third party.
- Verify that the person or organization that sends you the certificate really is who he/she/it says.
- They serve much like a human notary public.
- Accept certificates of authority only when you trust them.

THE INTERNET AND INTRANETS

- Consist of large numbers of interconnected computers.
- The Internet is international.
- Intranets are the same but connect only computers in a given organization.
- Computers on an Intranet are not necessarily connected to the Internet.

OPERATING SYSTEMS

- Software programs that allow users to do things with their computer hardware.
- Single-user operating systems (windows 95, Macintosh)
- Easy to use but offer little or no data security.
- Multi-user operating system (UNIX) offer considerable security

FIREWALLS

- Firewall computers have two network cards and two sets of IP addresses.
- Used to secure Intranets with protected computers behind the firewall.
- Their IP addresses are secret from the Internet.
- Computers outside the firewall cannot send packets to them and cannot « sniff » packets that they send.

NAME SERVERS

- Allow computers to have individual names.
- Names are organized into domains, sub domains, and so forth.
- Importance of concept of name servers.

INTERPOL

THREATS AND RESPONSES

- The UNIX variants are much resistant to attack by virus and penetration by amateur crackers than windows 95 or windows NT.
- « Social engineering » account information and passwords.
- Separate computers used for Internet access from computers containing vital information.
- At least 8 character passwords.

Continuation

- Java Applets and Active X controls.
- Commercial programs are available that protect user computers against malicious programs.
- « Virus » and « virus checkers »
- Download programs only from secure sites.
- Web browsers/ proxy servers (www.anonymizer.com)

CONCLUSION

« The web is a relatively young community, a neighborhood where few people lock their doors. But this community is rapidly growing into a city. Perhaps it's time you thought about installing some locks. »

INTERPOL

THANK YOU FOR YOUR KIND ATTENTION

Contacts: **c.atefor@interpol.int**

Tel: +237 77412114

+237 22640266

+237 22060262

INTERPOL