

I-SECURIT

The Ultimate Network and Data Security Training System

The total losses for 639 survey respondents came to just over \$130 million*

And, that's just the figure for a random sample of 639 companies in one country. The total loss due to network security lapses probably cannot even be estimated. Moreover, these losses are not due to outright theft so much as a result of networks being compromised, DoS attacks, virus contamination, and so on. All of which go to show that in today's world, computer networks and the information stored on them are under constant threat. Today, distributed computing is facing a growing number of network security threats that have, in the last few years, evolved in virulence and sophistication.

The result? Governments, corporate entities and individuals are increasingly focusing on securing their IT Assets. In addition, there are regulatory requirements for corporate entities to certify the confidentiality of customer information with them.

It is estimated that today, 13% of a company's IT budget is allocated for information security expenses – up from just 4% three years ago. However, the industry suffers from a lack of suitably trained network administrators to protect, detect and respond to network security threats. Moreover, the teaching community is constrained by the lack of a proper 'platform' which can create a real-life environment to work on network and data security issues.

* Source: CSI/FBI Computer Crime and Security Survey

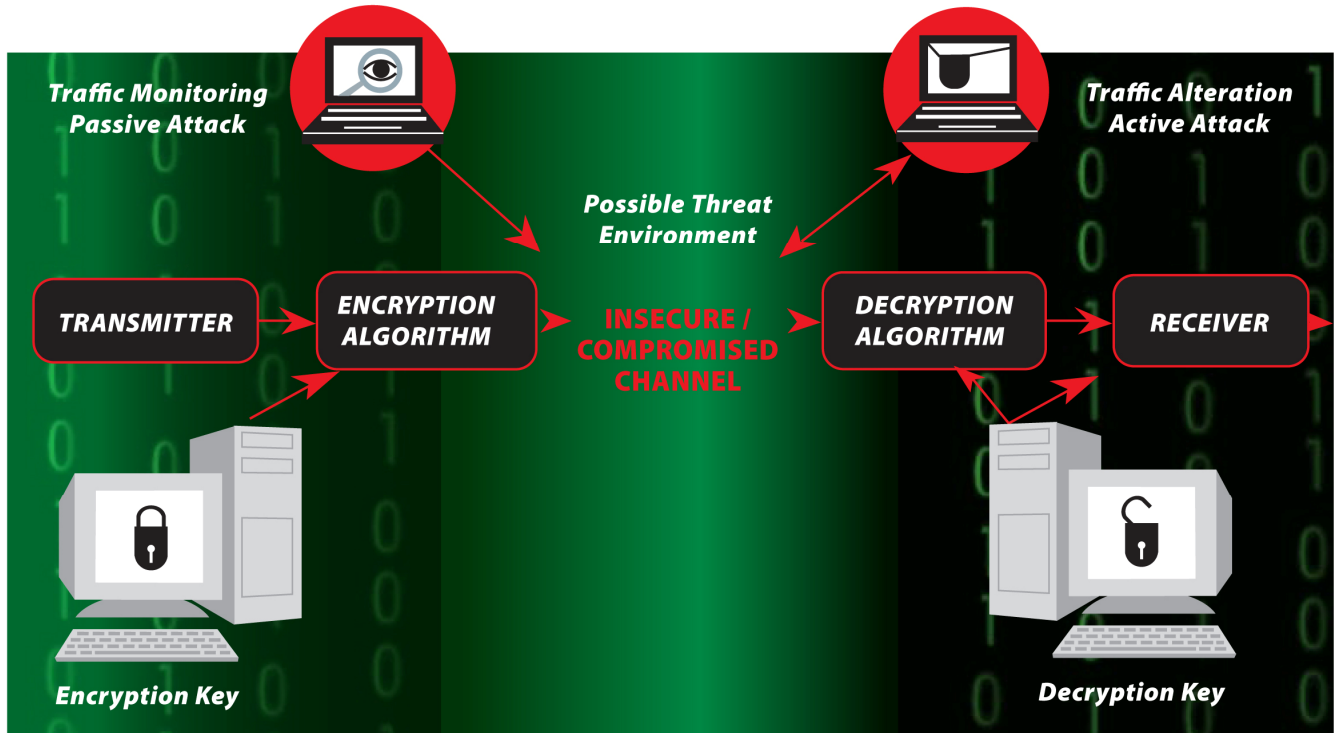


– A ONE STOP SOLUTION

- Training for Network Administrators and Security Experts
- Emulates a real-life network to give hands on training on live security threats
- Complete courseware for classroom or self-paced learning

The Benchmark i-SECURIT is a network and data security training system, that has been jointly developed by Benchmark Electronic Systems and AU-KBC Research Centre, Anna University to educate and train users on different real world network security threats and data encryption methods





Developed with AU-KBC Research Centre, Anna University, Chennai

Innovative Design Allows Real Life Training

The i-SECURIT is a complete system with two interconnected real life networks – the “Trusted Network” and the “Black Network”. These networks are isolated from the real world i.e. any corporate or campus LAN and the Internet. The i-SECURIT Central Control Unit (CCU) runs the network services, administration and control methods. The Black Network users attempt to compromise the services by different attacks, such as Intrusions, Password Cracking, and Denial of Service. The trusted network users simultaneously work on, and are trained to deploy, suitable counter measures to keep network services running properly.

Innovative Design allows Real Life Training

The i-SECURIT covers a large gamut of network security threats and its users can obtain hands-on experience with a wide variety of network security issues and cryptography methods. The course design allows the learner to read about a concept, witness a demonstration and then actually practice its execution. This meets the study flow of beginners as well as industry professionals. Through a single i-SECURIT, you can connect up to 15 PCs, with one slot reserved for the network administrator, and can start working with as little as two to three PCs.

COURSEWARE

We have worked with experts in the field of network security and cryptography to create comprehensive learning material for conducting complete network security courses. The course material has been presented by pedagogy experts for ease of learning and long term retention. Users can follow the theory and go through the exercises for a complete understanding of the concepts through self-study. This also makes it ideal for user paced learning.

TRAINING DESIGN APPROACH

i-SECURIT Experiment Topics are designed at three levels:

Level I: Running Network Services

Network services to be run and procedures to be adopted are discussed.

Level II: Attack the Trusted Network and shut down the services

The methods used in attacking network services and shutting them down are explained in this level. The manual explains the same with step-by-step instructions.

Level III: Training on Network Security Counter Measures

The user is trained on Network administration and monitoring methods used to protect a network from the cyber-attacks - as experienced in Level II - as well as on different techniques such as cryptography, honeypots, etc., to ensure data and information security.

EXPERIMENTS

Network Security Fundamentals – An Introduction

- Networking basics – Setting up and invoking network elements
- Ethics and Legality – Policy & practices that need to be followed in security practices including exploits, reporting methods, necessity of ethical hacking, social engineering practices, etc.

Network / System threats

- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Sniffing – Packet / Mail sniffing
- Spoofing – IP, MAC

Web Vulnerabilities

- Web based password capturing, SQL injection (injection discovery, form validations), and Buffer overflow
- Honeypots – Active, anti-intrusion technique

Malware

- Trojans & Backdoors
- Virus & AV methods

Network Identification

- Enumeration – TCP ping, Ping sweep, ICMP ping, NULL Scan, Fast Scan, UDP port scan, Syn Stealth, Fin Stealth
- OS detection

Cryptography

- Symmetric encryption scheme, Stream Cipher – RC4
- Symmetric encryption scheme, Block Cipher – S-DES, 3-DES
- Asymmetric encryption scheme, Block Cipher – RSA
- Hashing scheme – MD5
- Block Cipher modes – ECB, CBC, CFB, OFB

Web services using crypto techniques

- PKI
- Authentication schemes – Different authentication schemes including password based authentication, IP Based Authentication and Challenge Handshake Authentication Protocol (CHAP)
- Steganography

PRODUCT SPECIFICATIONS

Central Control Unit (CCU)

Network ports: 100 Base-T ports

- 2

- One each to connect to switches of trusted and black networks
- RJ45 interface, auto negotiating

Remote login to configure the CCU, up to 14 user logins

Power input: 220 V A.C., 50 Hz

FEATURES

- **Single Trainer solution for practicing several different Network Security & Cryptography topics**
- **Comprehensive set of exercises for different security threats and attacks**
 - System threats – Identification & hacking, Backdoors, Virus, Worms & Trojans
 - Web Vulnerabilities
 - Cryptography
 - Intrusion threats – Sniffing, Spoofing, SQL injection
- **Central Control Unit (CCU) to control and emulate real life network under study**
 - Remote login, Packet handling, routing, etc.
- **Variable network size – up to 7 nodes in each network (Trusted and Black) can be controlled**
 - Comprehensive learning material written by experts and presented by pedagogy experts
- **Instruction Manuals**
 - Technical manual emphasizing practical aspects of network and information security. Can be used as reference and for self-study
 - Experiment manual – Step-by-step instructions covering all levels of experiments

ORDERING INFORMATION

i-SECURIT – Cryptography & Network Security Assurance Laboratory, comprising:

- CCU – 1
- Manual (Technical manual and Experiment manual) – 1
- Network cable – 2

Note: Network cabling to be done by the client for the number of users intended

SYSTEM REQUIREMENTS

Minimum Setup:

No of PC's required: 3
Windows – 2 machines
Linux with FTP server – 1 machine

Full Setup:

No of PC's required: 14
Windows – 7 machines
Linux with FTP server – 1 machine
Windows / Linux – 6 machines

Windows system configuration: Windows 2000 with SP4 or Windows XP with SP2

Linux system configuration: Redhat Linux ver 7.3 or ver 9.0

Required Dependencies:

Java Runtime Environment ver 1.5 (or above), WinPCap (for Windows)

Ethereal Packet Sniffer (for Windows)

Internet Explorer 6.0 or above / Netscape Navigator 7 or above / Firefox 1.0 or above

Macromedia Flash Player 6.0 or above



Feedback Instruments

5 & 6 Warren Court
Park Road, Crowborough
East Sussex
TN6 2QX
United Kingdom
Tel: +44 1892 653322
Sales: sales@feedback-instruments.com
Website: www.feedback-instruments.com

For further information on Feedback equipment please contact ...

Feedback reserves the right to change these specifications without notice.