

Guaracabuya  
169, 158, 17  
November  
Revolutionary  
Organization  
206, 49, 67  
212, 44, 100, 0/127  
212, 44, 101, 0/175  
212, 44, 102  
212, 44, 96  
212, 44, 97  
212, 44, 98, 0/199  
212, 44, 99, 0/207  
216, 72, 216, 72, 24  
216, 72, 25  
216, 72, 26  
216, 72, 27  
63, 170, 172  
63, 170, 173  
63, 170, 174  
63, 170, 175  
Abortion Abu  
Nidal  
Organisation Abu  
Qatada Abu  
Zubaydah  
Admiral Tom  
Wilson AFGS  
ships Afintoxin  
Air Expeditionary  
Force AKSISU Al  
Hakim Aladdin  
Knowledge  
Systems Internet  
Security Unit  
Alamar  
Aleksander Lebed  
Alexander  
Vladimirov Al-  
Gama'a al-  
Islamiya Alik  
Galiyev Al-Qaida  
American  
Enterprise  
Institute  
American Society  
for Industrial  
Security Anatoli  
Leffronov Anatoli  
Khorechko  
Andrew  
Kreptinevich  
ANGOL ANET  
Anthrax 836  
Antibiotics  
Antilivestock  
agent Arabel  
Elias Archbishop  
Achille Silvestrin  
Area 51 Armed  
Forces  
Radiobiological  
Research  
Institute (Medical  
Radiological  
Defense) Armed  
Islamic Group  
Armed Services  
Committee  
Research and  
Development  
Panel Army  
Technical Escort  
Unit ASIS Aspin-  
Brown

## WHAT CAN BE DONE FROM THE BEJUCAL BASE BESIDES ELECTRONIC ESPIONAGE?

MANUEL CEREIJO

JUNE 2001

From the Bejucal base in Cuba, besides the listening to telecommunication channels in the United States, they can also produce attacks on the security of the United States' computer systems or networks. The general categories of attack are:

- **Interruption:** An asset of the system is destroyed or becomes unavailable or unusable. This is referred to as an attack on availability. Examples include destruction of a piece of hardware, such as a hard disk, the cutting of a communication line, or the disabling of the file management system.
- **Interception:** They get access to an asset. This is referred to as an attack on confidentiality. Example is the unauthorized copying of files or programs
- **Modification:** The attacker tampers with an asset. This is referred to as an attack on integrity. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network
- **Fabrication:** The attacker inserts counterfeit objects into the system. This is referred to as an attack on authenticity. Examples include the insertion of spurious messages in a network or the addition of records to a file.

### CATEGORIES OF ATTACKS

A useful categorization of these attacks is in terms of passive attacks and active attacks. Passive attacks are in the nature of monitoring of transmissions. The goal of the attacker is to obtain information that is being transmitted. Two types of passive attacks are (1) release of message content; (2) traffic analysis. A release of message content is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.

The second passive attack, traffic analysis, is more subtle. Suppose that we had a way of masking the contents of a message or other

Hizbollah External  
Security  
Organization  
Hollinger  
International  
Hoover Institution  
Human Intelligence  
HUMINT ICANN  
Igor Domaradsky  
Igor Rodionov  
Infoglide  
Information Warfare  
Immunology In-O-  
Tel In-O-Tel  
Interface Center  
International Sikh  
Youth Federation  
Internet Corporation  
for Assigned Names  
and Numbers  
Investigative Group  
International IRA  
Isaac Cohen Isaac  
Levi Islamic Army  
of Aden Islamic  
Jihad Islamic Jihad  
Israeli Defense  
Forces Israeli  
Division 5 Izz el-  
Din al-Qassam  
Brigades Jarsh-e-  
Mohammed Jiang  
Zemin JIMAD John  
Gannon John  
Hopkins University  
John Jay College  
Joint Program  
Office for  
Biological Defense  
Joint Service  
Chemical Biological  
Information  
Systems (JSCBIS)  
Joint Strike Fighter  
Joint Vaccine  
Acquisition  
Program Jose Cause  
Jose Ramon  
Cabañas Journal of  
Immunology Junin  
John Kasteo Chase  
Ken Alibek Kevin  
Ziege Khalid Deek  
Khattab Kurdistan  
Workers' Party  
Larry Press  
Lashkar-e-Taiba  
Lassa fever  
Lawrence  
Livermore National  
Laboratory Lev  
Telegin Li Hongzhi  
Li Ka-Shing Li  
Peng Liberation  
Figers of Tamil  
Belam Library of  
Congress Los  
Alamos Nuclear  
Weapons Lab Los  
Palacios Lourdes Ly  
Tong Machupo  
Main Intelligence  
Directorate of the  
General Staff  
Marburg Marine

Commission  
Asymmetric  
tactics Atlantis  
Babbar Khalsa  
Bejucal BEMMA  
Inc BIDS Bill  
Patrick Bill  
Richardson  
Biohazard  
Biological  
Integrated  
Detection System  
Biopreparat  
Biosafety  
Bioweaponer  
Bioweapons Bluff  
Arsenal Bonfire  
Botonin  
Botulinum Brem  
Serovertrot  
Brucellosis  
Cadmium  
Caribbean  
Radiation Early  
Warning Systems  
Carnegie Moscow  
Center Carnivore  
CBIAC  
(Chemical  
Warfare/Chemical  
Biological  
Defense  
(CW/CBD)  
Information  
Analysis Center)  
CBIRF CCBS  
CDC Cellular  
immunity Council  
Information  
Coordination  
Center Center for  
Civilian  
Biodefense  
Studies Center for  
Defense  
information  
Center for  
Democracy and  
Technology  
Center for  
Disease Control  
of Atlanta Center  
for Strategic and  
Budgetary  
Assessments  
Center for  
Strategic and  
International  
Studies Center for  
the Study of  
Intelligence  
Centers for  
Disease Control  
and Prevention  
Central Incident  
Response Group  
Charles Bailey  
Chechnya  
Cheltenham  
Government  
Communications  
Headquarters  
Surveillance  
Network  
Chemical and  
Biological  
Weapons  
Nonproliferation

information traffic so that Cuba, even if they capture the information, could not extract the real information because of the use of encryption. The attacker could after a period of time extract the information and messages, defeating the encryption process.

The second major category of attack is active attacks. These attacks involve some modification of the data stream or the creation of a false stream. It can be subdivided into four categories: masquerade, replay, modification of message, denial of service.

A masquerade takes place when the attacker, under certain entity, pretends to be a different entity, and therefore enabling an authorized entity to obtain extra privileges. Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Modification of service simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. The denial of service prevents or inhibits the normal use or management of communications facilities. This is a very important and serious possible attack. It could disrupt an entire network, either by disabling the network or by overloading it with messages so as to degrade performance. The attacker could target airports, financial centers, power companies, dams control centers, etc. It is quite difficult to prevent active attacks. The goal is to detect them and to recover from any disruption or delays caused by them.

## INTRUDERS

There are three classes of intruders:

- **Masquerader:** the intruder is not authorized to use the computer and penetrates a system's access controls to get inside. This can be done from the Bejucal base
- **Misfeasor:** A legitimate user who access data, programs, or resources for which is not authorized. This can be done by an insider, not from the Bejucal base
- **Clandestine:** the intruder seizes supervisory control of the system. Can be done from inside or from the Bejucal base

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. The intruder must acquired information that should have been protected. In most cases, this information is in the form of a password. The password file can be protected by one way encryption or by limiting the access control to the file. What are the most common techniques used so far to try to break

Corps Response  
Force Marine  
general Charles  
Wilhelm MASINT  
Mass casualty  
weapons  
Measurement and  
Signature  
Intelligence Media  
Most Mediasnap  
Medical Chemical  
and Biological  
Defense  
Medstatistika  
MEMS Menwith  
Hill Michael  
Sheehan Micro-  
electromechanical  
systems Mikhail  
Kasyanov Mikhail  
Kolesnik MINRIX  
Mirzabekov  
Molecular biology  
Mosaic Group  
Muons Mustafa  
Labsi Myelin toxin  
NASA X-43  
National Center for  
Infectious Disease  
National Foreign  
Intelligence  
Program National  
Intelligence Council  
National  
Photographic  
Interpretation  
Center National  
Security Adviser  
NCID NEST  
netLaser Network  
Security Solutions  
NFIIP Nikolai  
Leonov Nikolai  
Vashtel Nikolai  
Petrov Nikolai  
Stolyrov Nikolai  
Urakov NPC NSS  
NTI NTV Nuclear  
Emergency Search  
Team Obolensk  
Oleg Ignatiev Open  
Source Intelligence  
Osama bin Laden  
OSI OSINT FOSS Inc  
Oswaldo Sanchez  
Cabrera Palestinian  
Islamic Jihad  
Pasechnik  
Pathogenic agents  
Pathothogeb  
Countermeasures  
program Patrick  
Kellay Paul D  
Woltowitz PC -SPES  
People's Mujahideen  
Peptides PGIS  
Pinkerton Global  
Intelligence Services  
PKK Plum island  
Program for  
monitoring  
Emerging Diseases  
Program Manager  
for Chemical  
Demilitarization  
PROMED Q fever  
QIC Radiation  
poisoning Radio

Project China's  
Ministry of  
Public Security  
Cholera Clinton  
has sold out  
America  
including our  
nuclear secrets  
Clinton sells to  
Communists and  
Terrorists  
Clinton  
poisoning lying  
treasonous  
Commie Bastard  
Cofer Black Colin  
L. Powell Colonel  
Abuse Colonel  
Uliyanov Colonel  
Viktor Alksnis  
Comdex Data  
Systems  
Committee on  
Overhead  
Reconnaissance  
COMOR  
Compound 19  
computer network  
attack Computer-  
security system  
Condoleza Rice  
Congressional  
Privacy Caucus  
Control Risks  
Groups Corona  
satellite photos  
Counterterrorism  
CREWS CSBA  
CSICCC Cuban  
Wasp Network  
Curie Institute  
Curt Weldon  
Cyberattack  
Cybercrime  
Cyberterrorists  
Cyberwarfare  
Cylink DACCRE  
DataScan  
Tempest  
Monitoring  
Systems Defense  
Advanced  
Research Project  
Agency - DARPA  
Dengue Denial  
and deception  
techniques  
Departamento de  
Tropas Especiales  
Department of  
Agriculture  
Exotic disease  
laboratory  
Department of  
Energy Nuclear  
Emergency  
Search Team  
Dick Cheney  
Domestic  
Preparedness  
Program Dozor  
Dugway Proving  
Ground Dugway  
Proving Ground  
Home Page  
Duncan Campbell  
E. coli bacteria  
Ebola virus  
ECHELON  
Edgewood  
Chemical  
Biological Center  
(CBC)  
Electronic  
Frontier  
Foundation  
Electronic  
Privacy  
Information  
Center Emerald

into a system?

- Try words on the system's online dictionary
- Collect information about the users. Full names, spouses' names, children's names, pictures in their offices, books in their offices, etc (Here the operating personnel in Bejucal needs inside information)
- Users' phone numbers, social security numbers, room numbers, license plate numbers, etc (inside information is also needed)
- Use a Trojan horse
- Tap the line between a remote user and the host system

## SUMMARY

Network security has assumed increasing importance. Individuals, corporations, government agencies, must heighten their awareness to protect data and messages, and to protect systems from network-based attacks. The disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security.



Electronic Station  
Cuba Ramon Garcia  
Rand Corp RASP  
Rem Petrov  
Revolutionary  
Peoples' Liberation  
Party-From Richard  
Clarke Richard  
Falkenraih  
Rickettsiae Robert  
Castell Robert  
Phillip Hauser  
Robert Steele  
Rosbusiness-  
Consulting ru  
Ru-sian Academy of  
Sciences SAIC  
Salafist Group for  
Call and Combat  
Salk Center Sandia  
National Laboratory  
Sarin Gas Caplet  
SCIF SCPS Scriabin  
Search engine to  
detect Internet  
Fraud Secure  
computing  
Professional Services  
Secured  
Compartmentalized  
Information  
Facilities Senchi  
Endo Select  
Therapeutics  
Semiotics Senate  
Intelligence  
Committee SENSEL  
Sensitive  
Compartmented  
Information Sergei  
Netyosov Shaan  
Jones Shigella  
Dysentria Bacteria  
Smallpox Society of  
Competitive  
Intelligence  
Professionals Southern  
command Soviet  
Circus Sprint  
International SRI  
International SS-23  
missiles Stanislav  
Levenko Stanton  
McCandlish Stasi  
Steganography  
Stepnogorsk  
Initiative  
Stepnogorsk  
Sverdlovsk SVR Sy  
Goodman TechJam  
TEMPEST Terje  
Rod-Larsen Terril  
Maynard Terrorism  
Task Force The  
NBC Medical  
Defense Information  
Server Thiobacillus  
Thiosidans Thomas  
H. Moore Thrips  
palm TMI  
Communications  
TNT Tomahawk  
cruise missiles  
Toronto Caving  
Group Transnet  
Electromagnetic  
Pulse Standard  
Treasury  
department's office  
of Foreign Asset  
control TFCSTS  
U.S. Army Soldier  
and Biological  
Chemical Command  
Information Server  
U.S. Interest Section  
in Havana Umberto  
Eco United States  
Army Chemical  
School United