Emerging Threats in the Battle Against Cybercrime

Erez Liebermann, Assistant United States Attorney
Deputy Chief, Economic Crimes Unit
Chief, Computer Hacking and IP Section
District of New Jersey

Laws and Penalties

- Computer Fraud and Abuse Act
- Identity Theft
- Access Device Fraud
- Intellectual Property Laws

Where Are We Now?

Case Studies

U.S. v. Albert Gonzalez

- Where we meet Albert Gonzalez?
  - Arrested for ATM Fraud
  - 2003
- Shadowcrew
  - Landmark Carding Case
  - Indictment October 2004
  - 21 Arrested in U.S.; Others Overseas

ShadowCrew

http://www.shadowcrew.com/

Google

Design News ...cture news The Lair of t... will to live Publisher Unabashed U...shing Tool BUDGET News

United States Secret Service

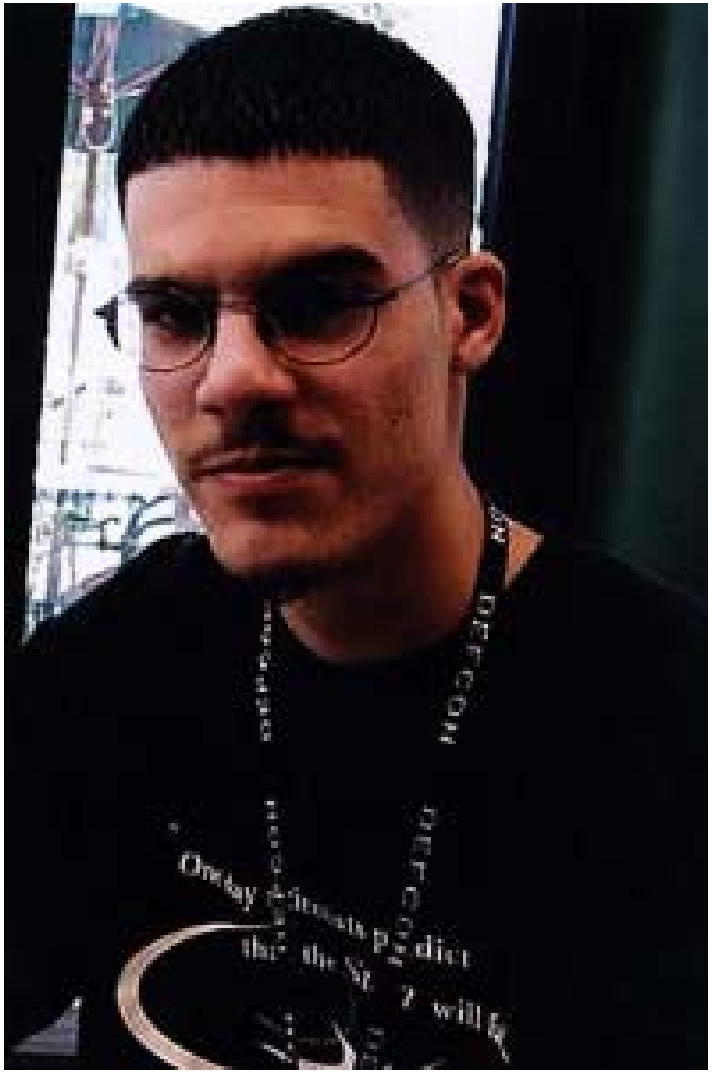
WWW.SECRETSERVICE.GOV

SHADOWCREW

"FOR THOSE WHO HAVE TO PLAY IN THE SHADOWS....."

ACTIVITIES BY SHADOWCREW MEMBERS ARE BEING INVESTIGATED BY THE

UNITED STATES SECRET SERVICE



TJX Hacking Investigation

- 2003 to 2008:
  - TJX
  - BJ's Wholesale Club
  - OfficeMax
  - Boston Market
  - Barnes & Noble
  - Sports Authority
  - Forever 21
  - DSW
- USSS & D. Massachusetts

Heartland and Others

- Continuing investigation…
- More Victims:
  - Heartland Payment Systems
  - 7-Eleven / Citi
  - Hannaford / Food Lion
  - JCPenney
  - Wetseal

Indictments

- Gonzalez Indicted
  - 3 Districs
- Longest Sentence for a Hacker:
  - 20 years.

PBX Hacking

Role of PBX

Caller

Public Network

e.g., AT&T, Sprint, Etc.

PBX System

Ext. 1124

Ext. 1125

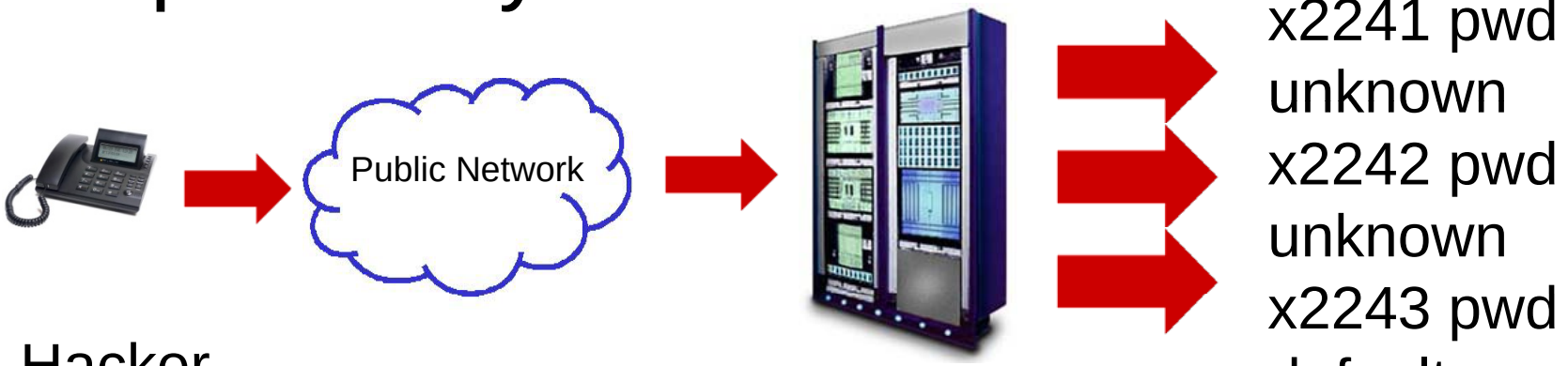
Ext. 4057

Ext. 2563

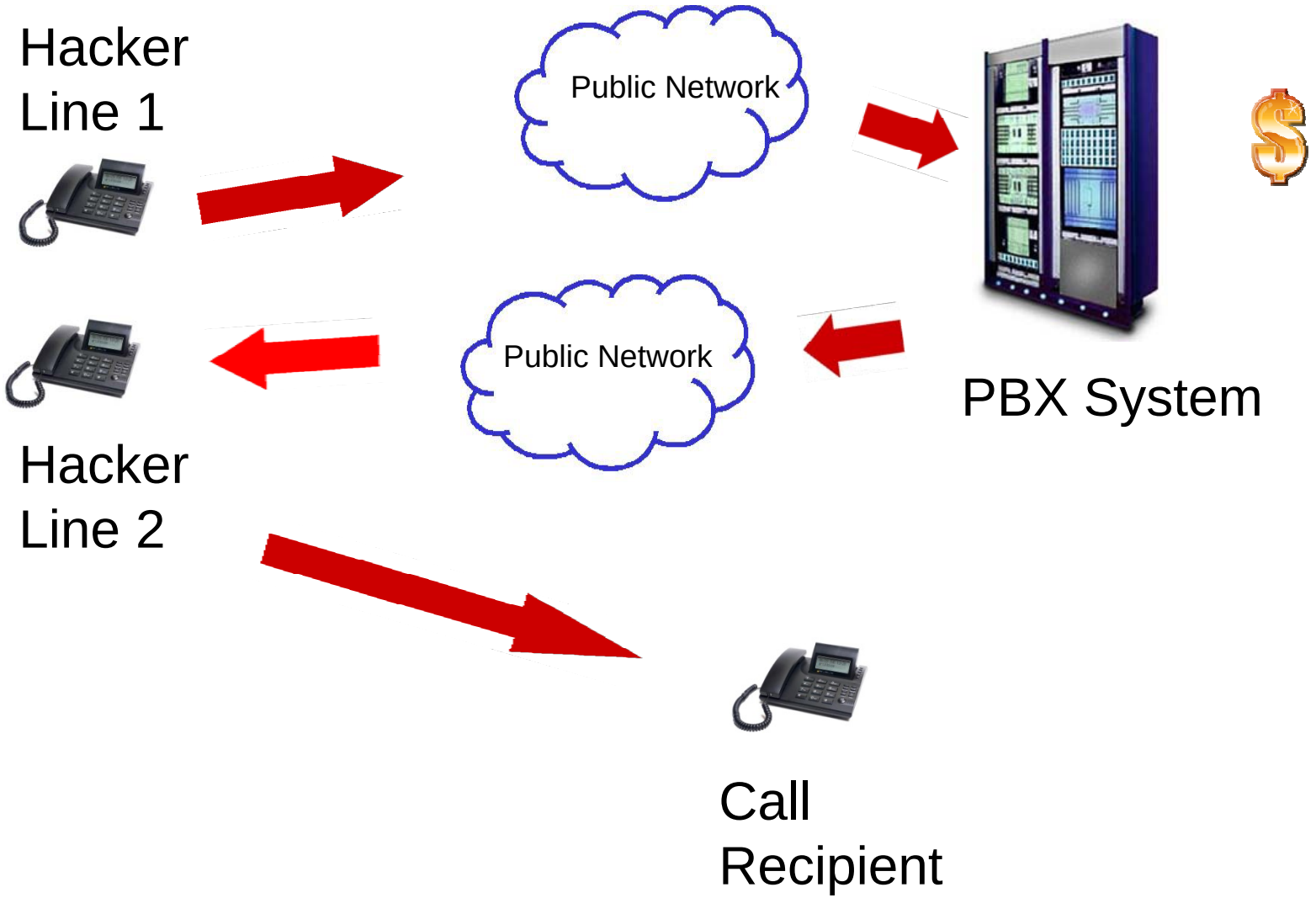
Extensions

The Hacking Method

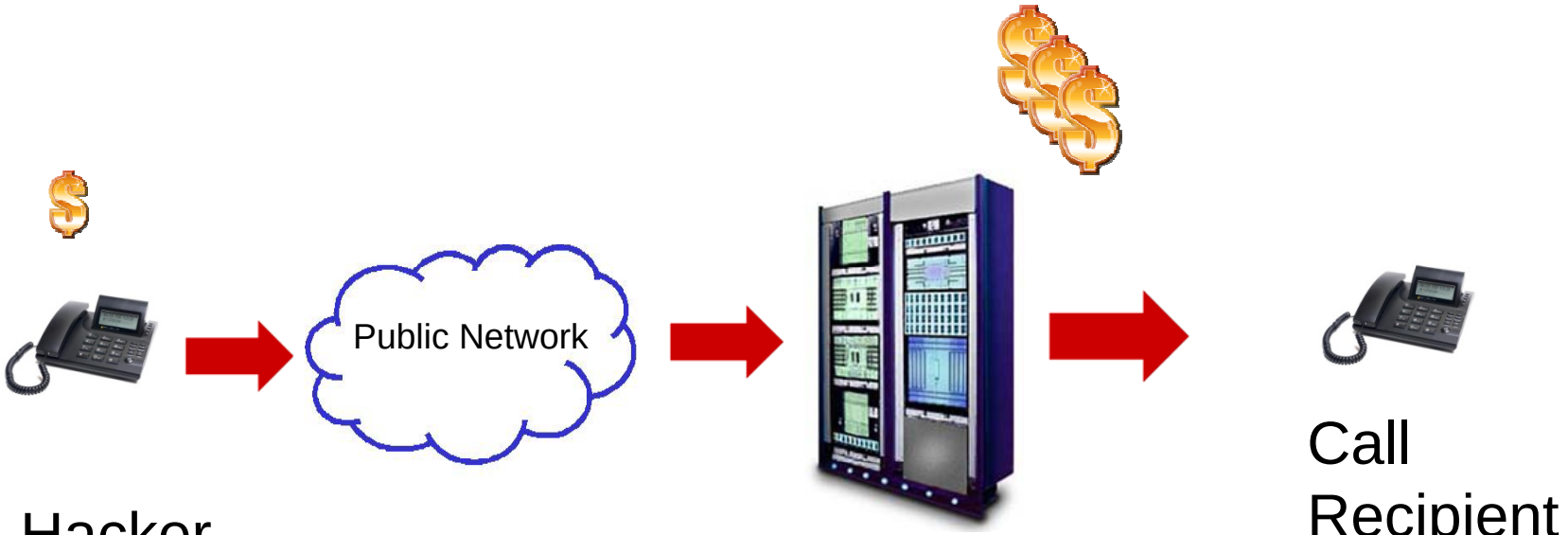
- Vulnerability = lack of security on phone systems



The Loopback Method



The Pass-code Method



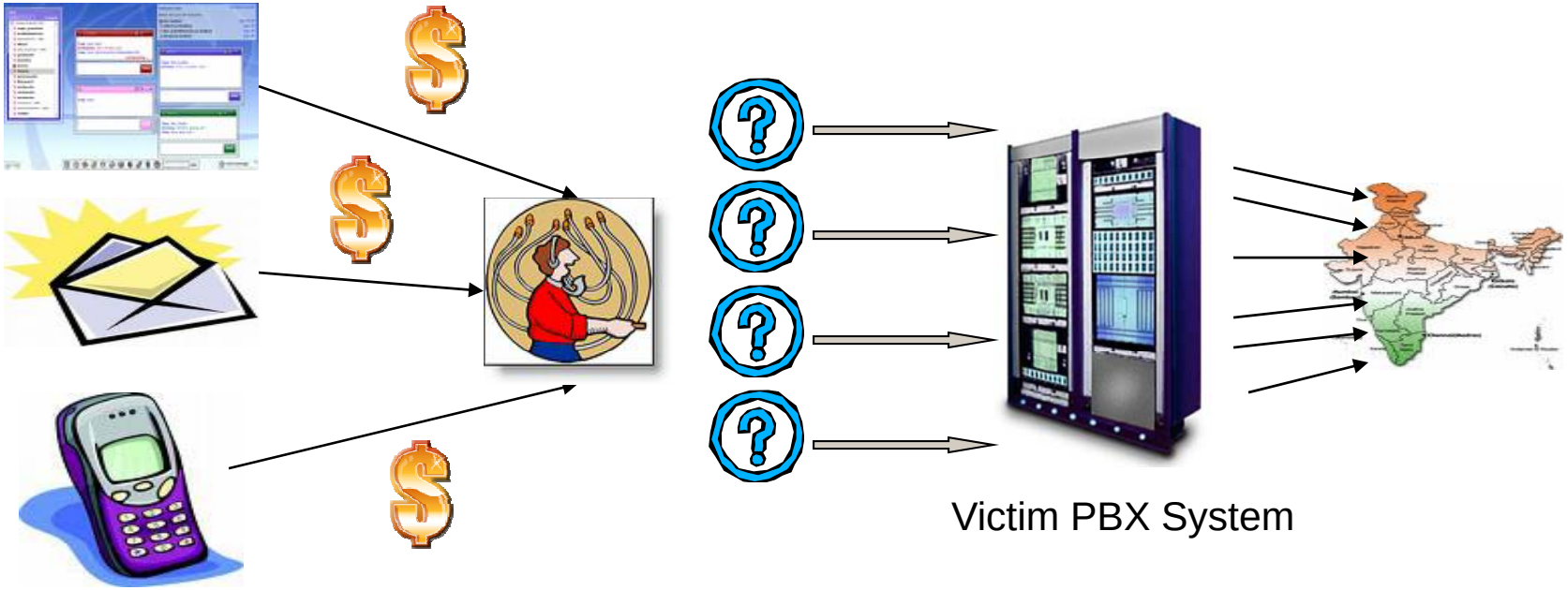
Hacker

PBX System

Call Recipient

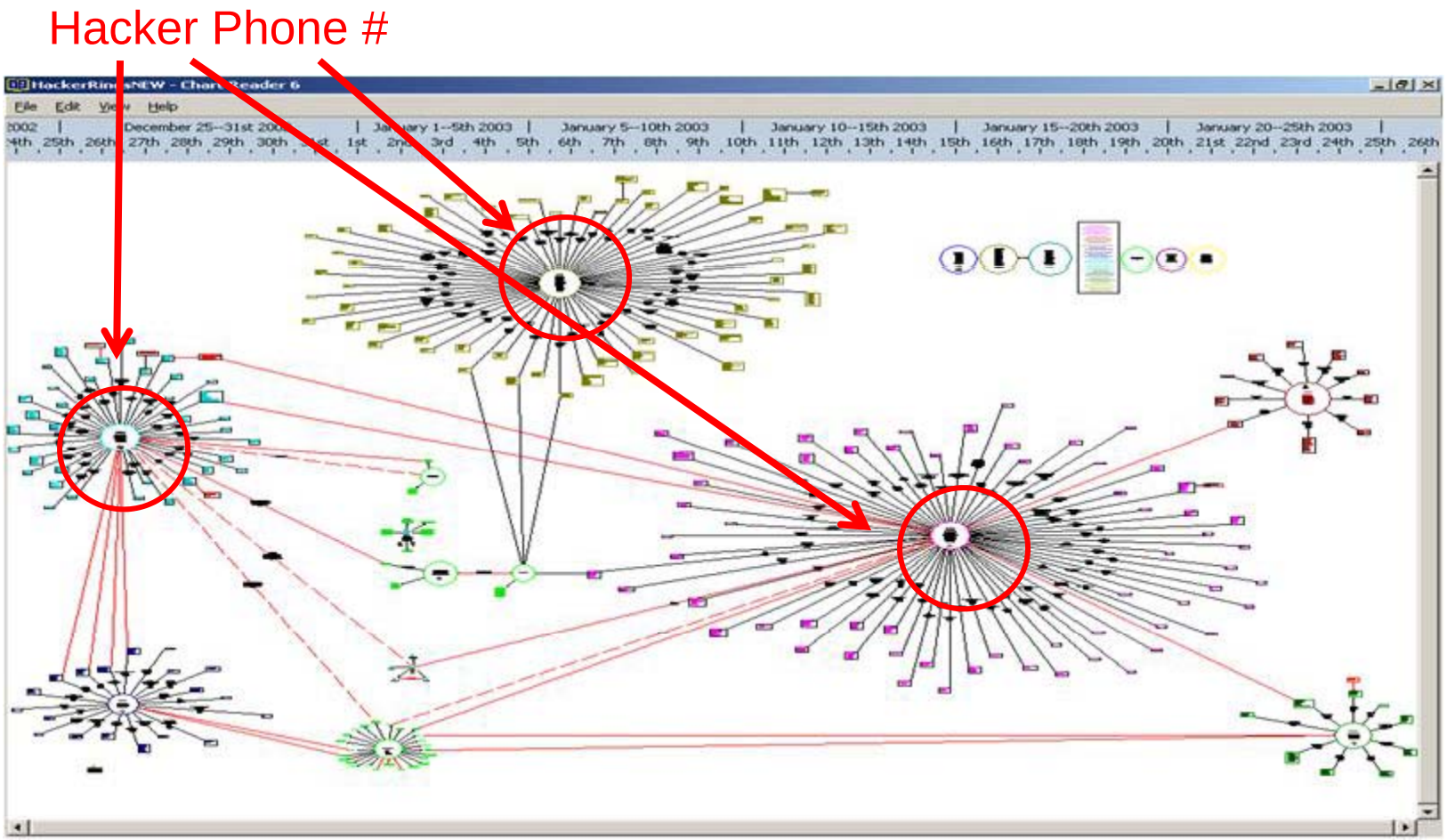
Why Hack?

- Two reasons:
  - *Income*
  - *Anonymity*



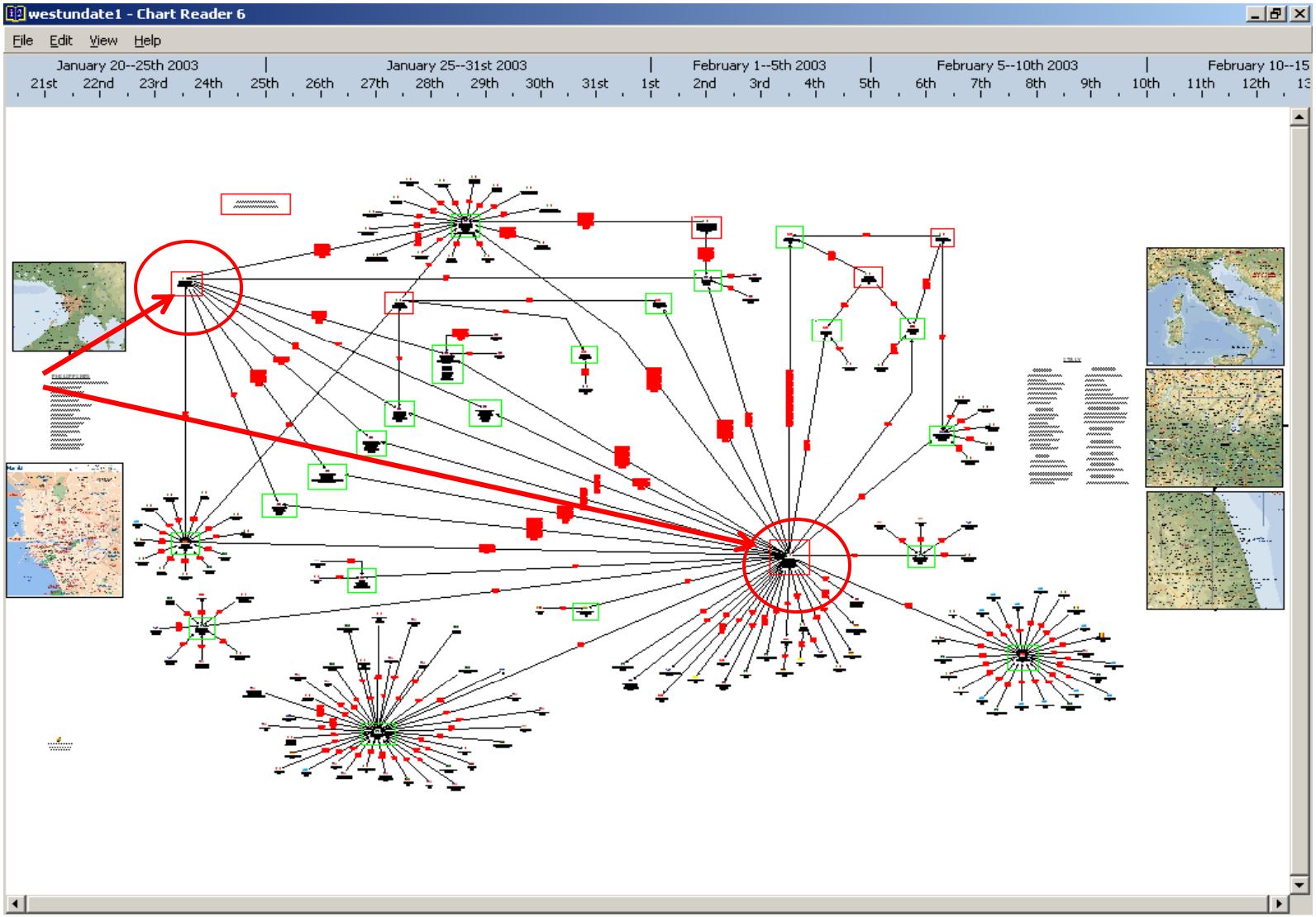
Victim PBX System

Telecommunication Traffic Analysis



Financial Analysis

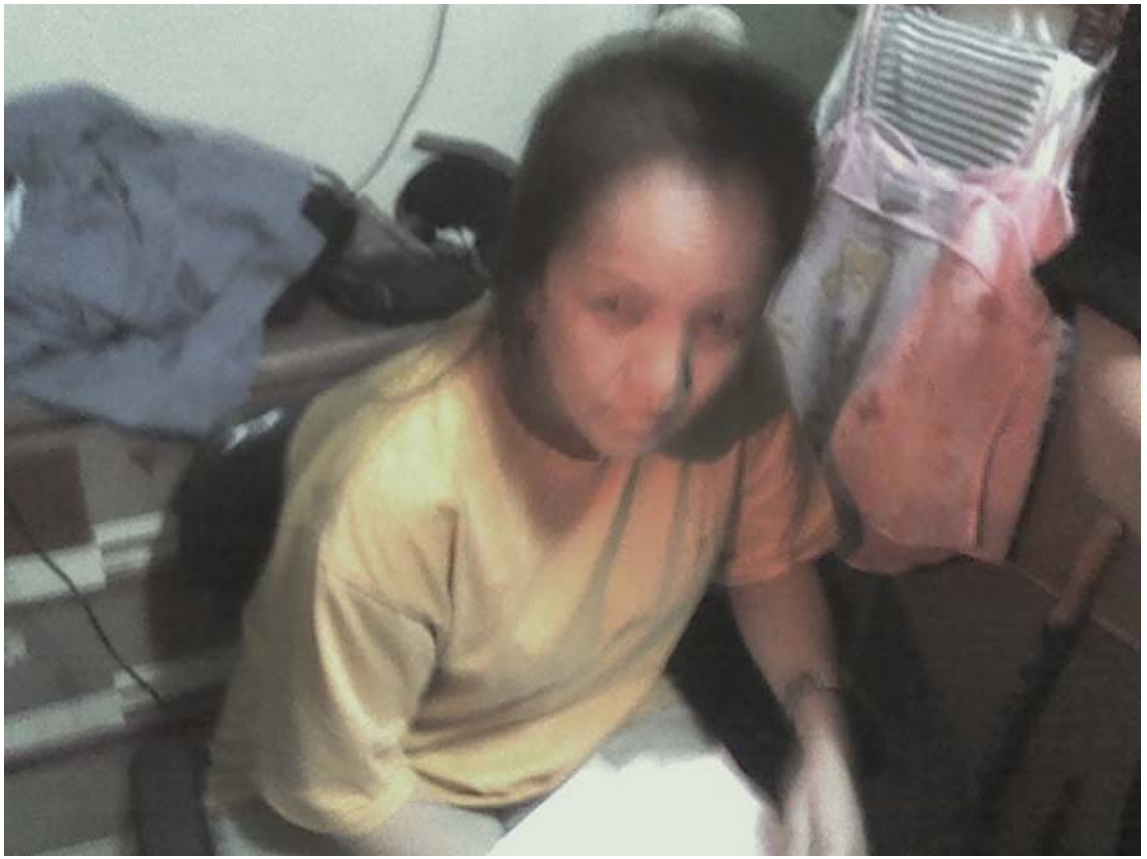
FINANCIERS



Operation March 9-10th, 2007

Suspect Michael Kwan

Nancy M Gomez - Malolos Avenue Metro Manila



Philippine National Police CSI Squad

Maria Lopez Residence -Burgus St. Cubao

Suspect - Maria Isabel Lopez

Evidence

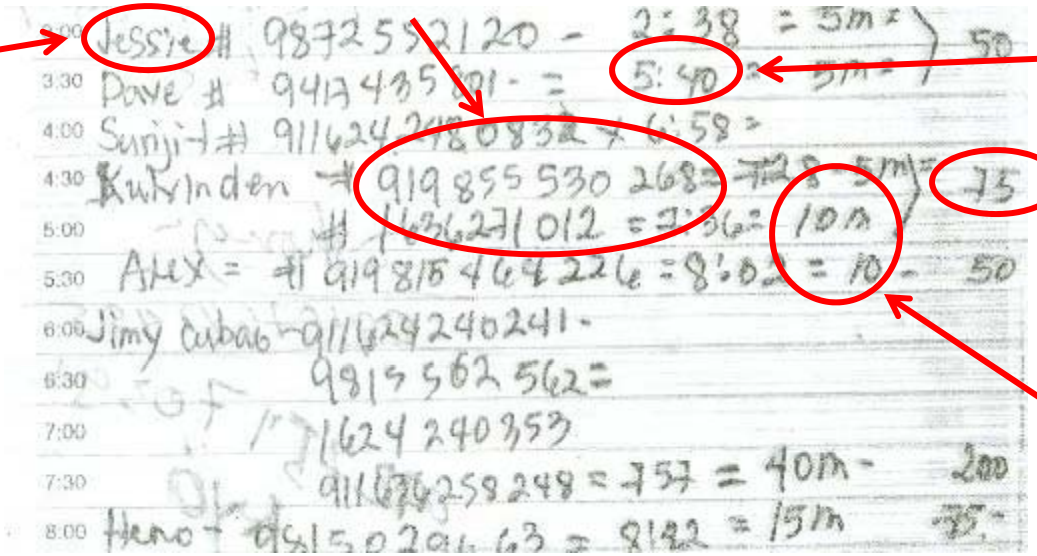
Lair of the hacker Maria Isabel Lopez

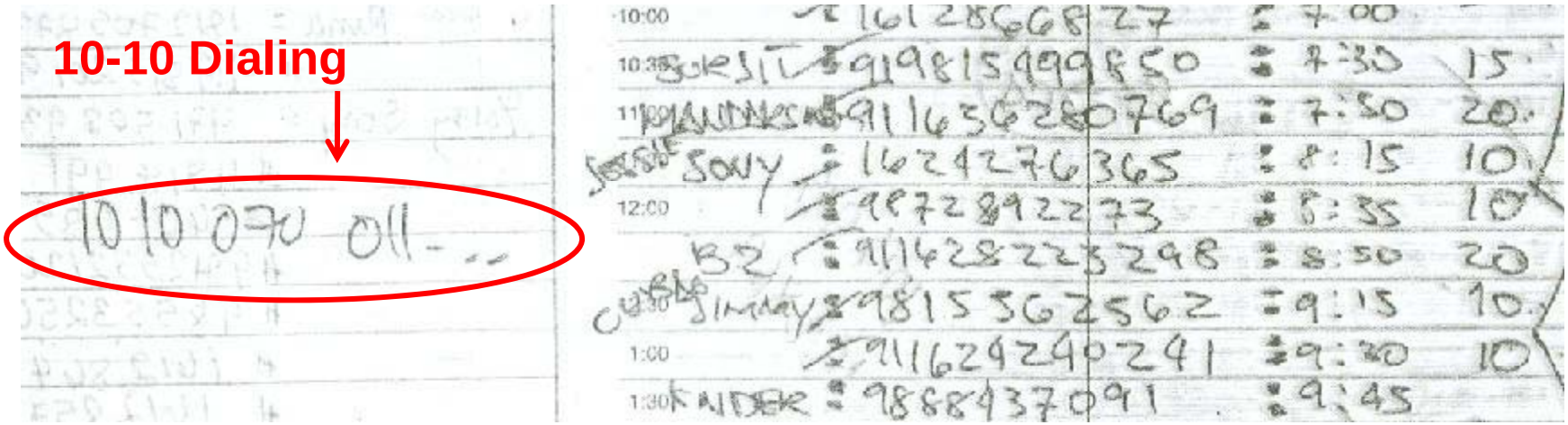
Juffer Virgo residence Benitez , Quezon City

Suspect Juffer Virgo from Benitez Street Location

Other Hacker's Documents

Examples of documents seized from hacker's home





MR Luna Street, Paranaque

Mastermind Mahmoud Nusier

Suspects at Police Headquarters

PBX Phase II: Italy

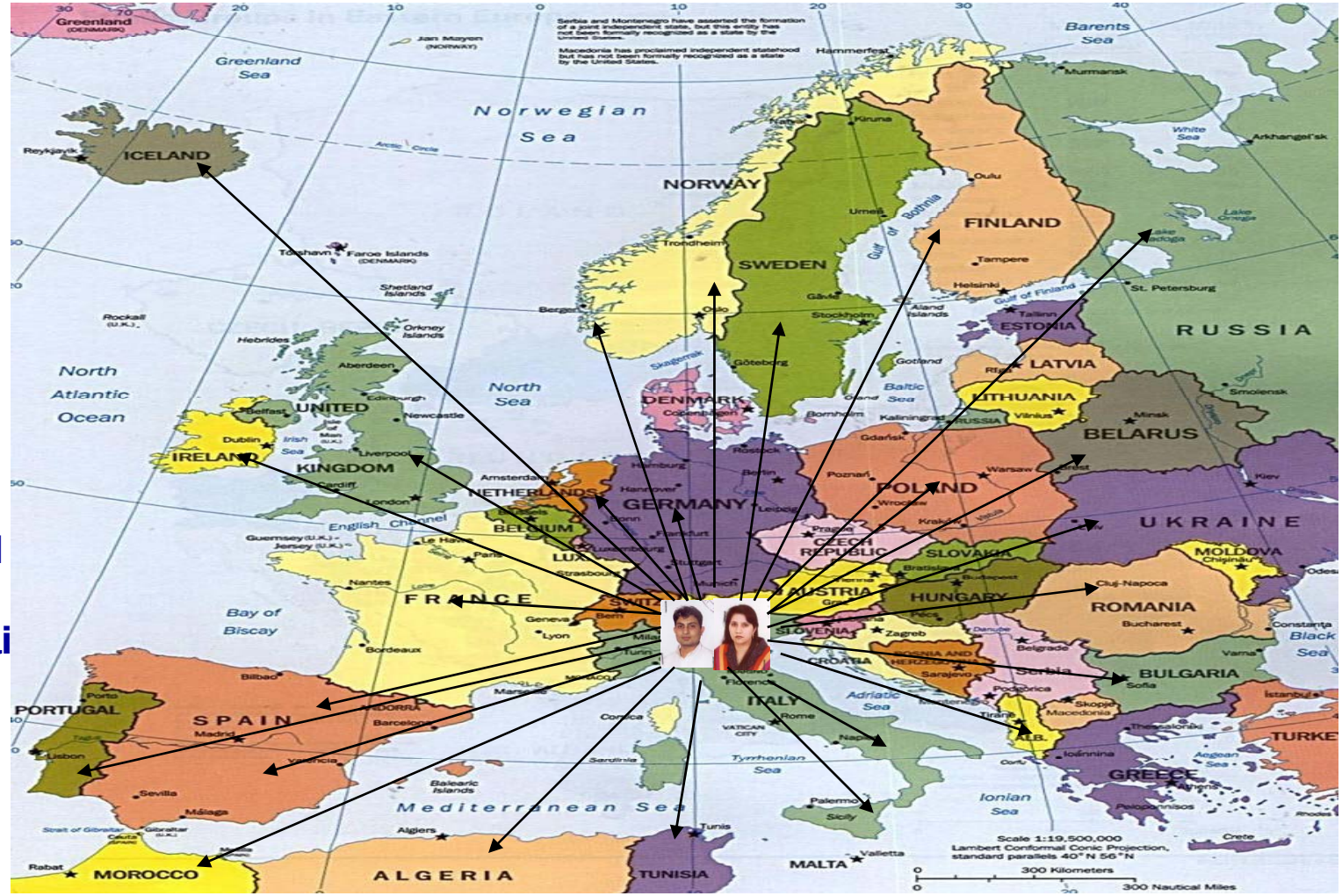
Italy Search and Arrests – June 12, 2009

Questura di Brescia - D.I.G.O.S.

Vendita dei codici PBX

In tal modo il sistema violato ed il numero delle intrusioni ai PBX si amplia con proporzioni geometriche.

Il manager fornisce le informazioni sul centralino compromesso ai Phone Center.



Polizia di Stato **F.B.I.**

Arrestati ed Indagati nel procedimento penale

Kanwal Shabina
nata in Pakistan il 11.12.1971

Mohammad Zamir
nato in Pakistan il 30.01.1969

SHAH Zahir
nato in Pakistan il 01.01.1970

WASEEM Ahmed
nato in Pakistan il 01.03.1969

IQBAL Khurram

nato in Pakistan il 04.04.1980

Outsider Attack

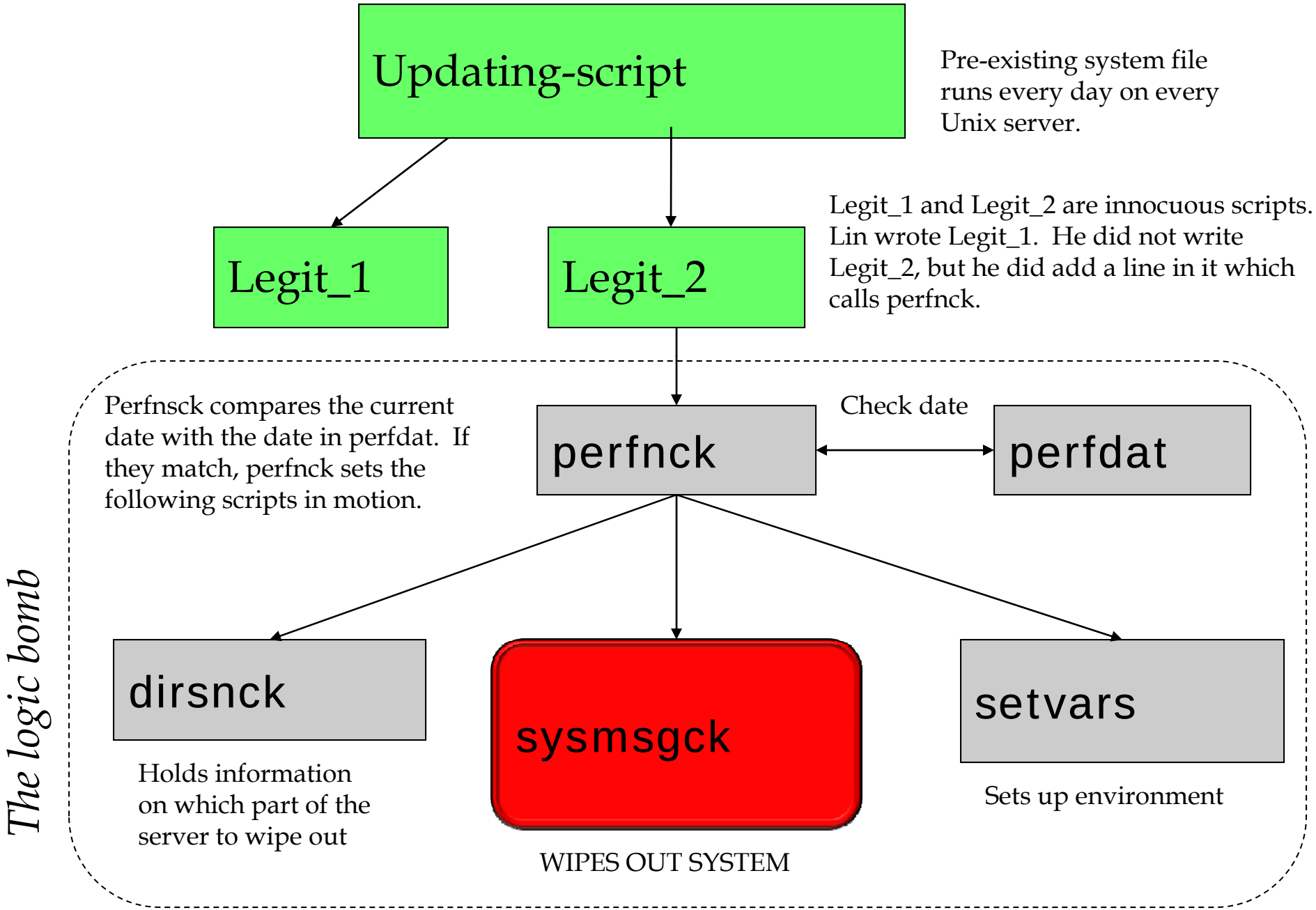
- Voice Over Internet Protocol (VOIP)
  - Edwin Pena and co-conspirators hack into VOIP companies and unsuspecting intermediaries.
  - Brute Force Attacks.
  - Millions made.


POWER
G-WEST
MAY 20 2006

Insider Attack

- Medco Health Solutions, Inc.
  - Andy Lin Feared he would be fired when rumors of layoffs spread.
  - Planted logic bomb in Medco's system.
  - Had it been triggered:
    - Financial Damage
    - Health implications

The Operation of Lin's Logic Bomb



- Medco Health Solutions, Inc. – Cont'd
  - Pleaded Guilty
  - Employee

Cyber Extortion

- Actual breach into computer systems
- Threatened breach into computer system

Military Hack

- **United States v. Gary McKinnon**
  - Weapons Station Earle
  - NASA
  - Pentagon
- Searching for info on UFO's?

"US foreign policy is akin to government sponsored terrorism these days... It was not a mistake that there was a huge security stand-down on September 11 last year... I am SOLO. I will continue to disrupt at the highest levels."


FREE
GARY
http://FreeGary.org.uk

Data Breaches: To Report or Not to Report?

- Data breach notification laws
- Cooperate with authorities
- Avoid aggravating factors in a lawsuit

What if it Happens?

- Call Law Enforcement.
- But...

Myth:

"If I call law enforcement, they won't care."

Myth:

"Law enforcement won't be able to catch the bad guys."

Myth:

"I can handle the situation myself."

Myth:

"If I just patch the security hole, restore my data, and fire the dirty insider, then I don't need to tell anyone."

Myth:

"If I call law enforcement, they'll come and take my servers away."

Myth:

"If I report to law enforcement, I'll lose control of my proprietary data."

Best Practices

- Protect the rights of the victim.
- Consult with senior management.
- Consult with IT staff.
- Minimize disruption to the company.
- Coordinate media releases.
- Keep the company informed.
- Build relationships before an intrusion.

Steps to Protect

- Logs, Logs and more Logs.
- Separation of Powers.
- Click-Through Banners.
- Extra vigilance.
- Immediate cut-off.

Questions?

My contact info:

erez.liebermann@usdoj.gov

973.645.2874