Introduction to Hacking

Sean-Philip Oriyano

About Me

- Over twenty years in IT Security
- Author of research articles and six books
- CISSP, CNDA, CEH and others
- Consultant for US Military and Private corporations

Agenda

- Elements of Information Security
- Security Challenges
- Effects of Hacking
- Who is a Hacker?

What is Security?

- Security – *A state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable*

Points to Ponder…

- The Cyber Security Enhancement Act of 2002 mandates life sentences for hackers who recklessly endanger the lives of others
- According to research 90 percent companies acknowledge security breaches, but only 34 percent reported the crime
- The FBI estimates that 85 to 97 percent of computer intrusions are not even detected

Core Concepts

Putting it Together

Motivations for Security

- Technology improvements
  - Reaches consumers before maturity
- Networks are more common and complex
- Users are much more savvy
- Budgets have decreased
  - No or poor training
- Improved attacks and smarter attackers

In the News...

Posted in Security News - IT and Computer Security - Crime and Fraud Prevention - on 23/06/2006 RSS

Companies are not vigilant enough against the growing menace of professional hackers

The latest Deloitte Global Security Survey has shown that more than three-quarters of the world's leading 150 finance groups suffered a serious security breach in the last 12 months. 78% of these companies have experienced a breach from outside their organisation (up from 26%), while 49% have seen them come from inside the company, up 14% from the previous year.

George Lungley, managi
one year and shows how
landscape. The majority
teenagers in their bedro
and tools coupled with fu
succeed in gaining unlaw
sums of money from fina
personal data.

"It is imperative that firm
that they have to be con
small they think it is, som
backing, they have the k
Deloitte Global Security S
companies must not let u

ATM passwords found online

Up to 70,000 US cash machines vulnerable

Andrew Charlesworth, vnunet.com 22 Sep 2006

The manufacturers' passwords for cash machines used widely across the US are available online in an installation manual.

New York-based security researcher Dave Goldsmith, founder and president of penetration testing outfit Matasano Security, pieced together clues from a CNN broadcast and the website of Tranax Technologies, the ATM's manufacturer.

Then he searched for the ATM's installation and maintenance manual online which he said gave him enough information to hijack a Tranax Mini-bank 1500 series ATM if the manufacturer's default passwords had been left unchanged.

"My guess is that most of these mini-bank terminals are sitting around with default passwords untouched," Goldsmith told eWeek.

According to the Tranax website, around 70,000 1500 series ATMs are installed in the US.

Complexity

Networks

Laws

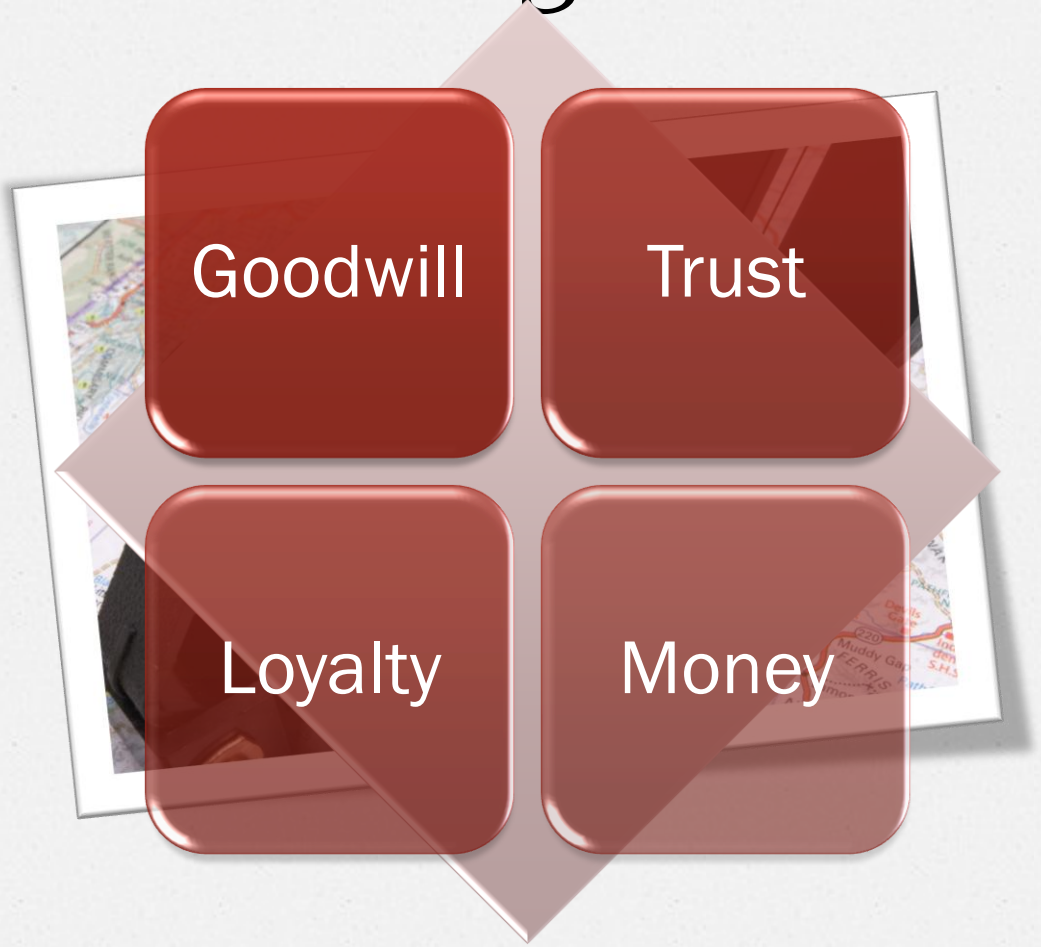
Software

Management

Users

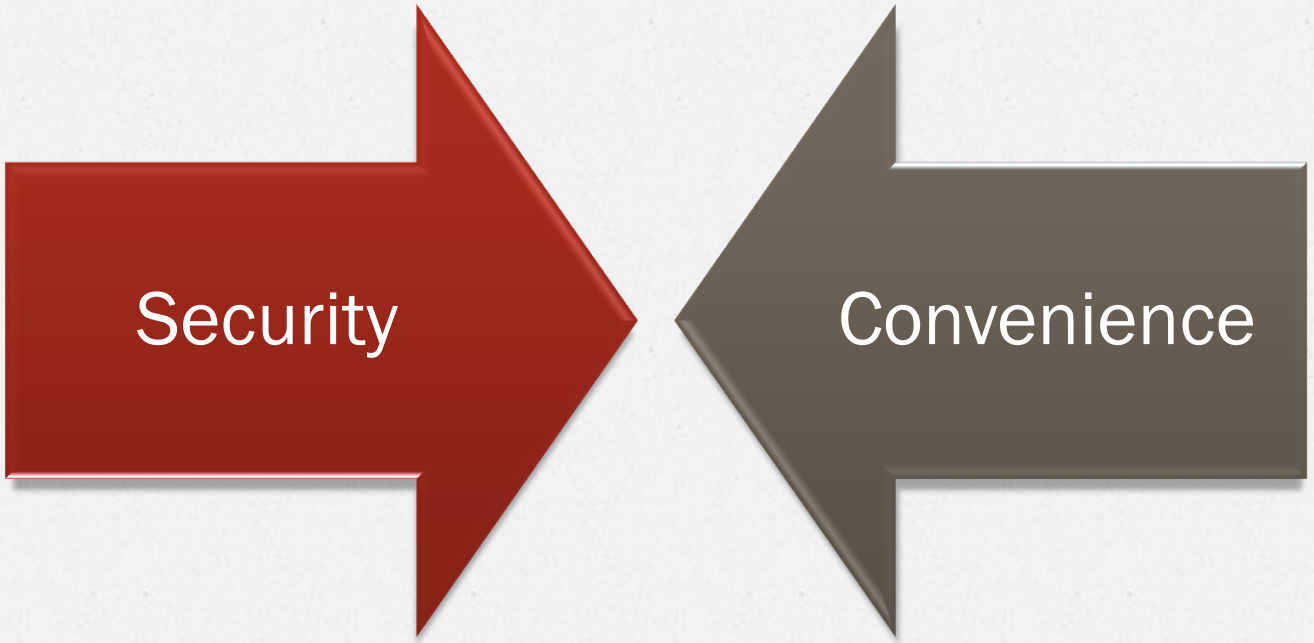
Demands

Intangibles



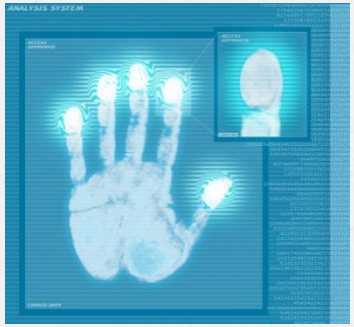
Polls

Factors Impacting Security



Cost of a Security Incident

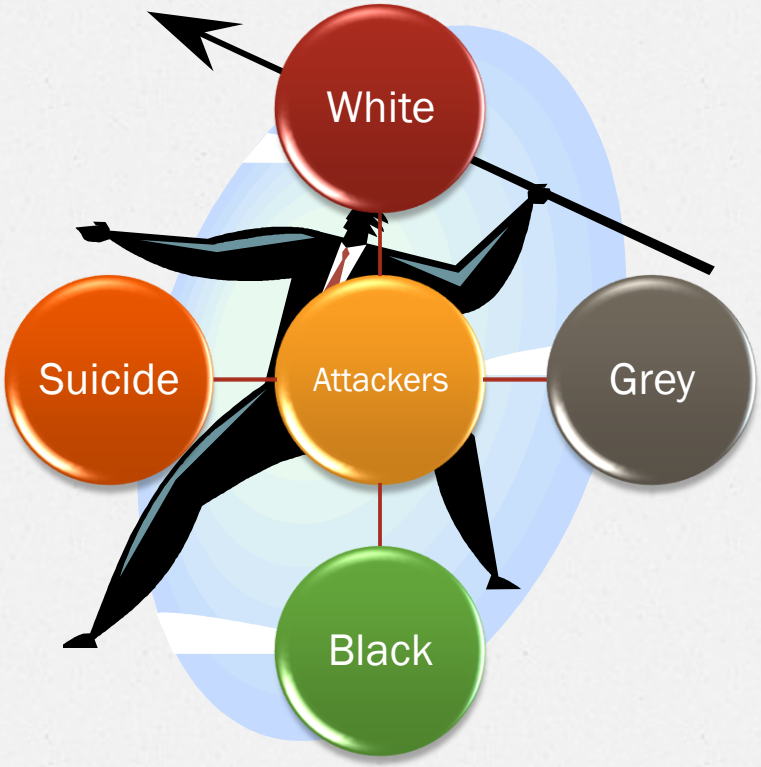
- Corporate espionage
- Identity theft
- Lost revenues
- Lost of confidence
- Lost productivity
- Legal action



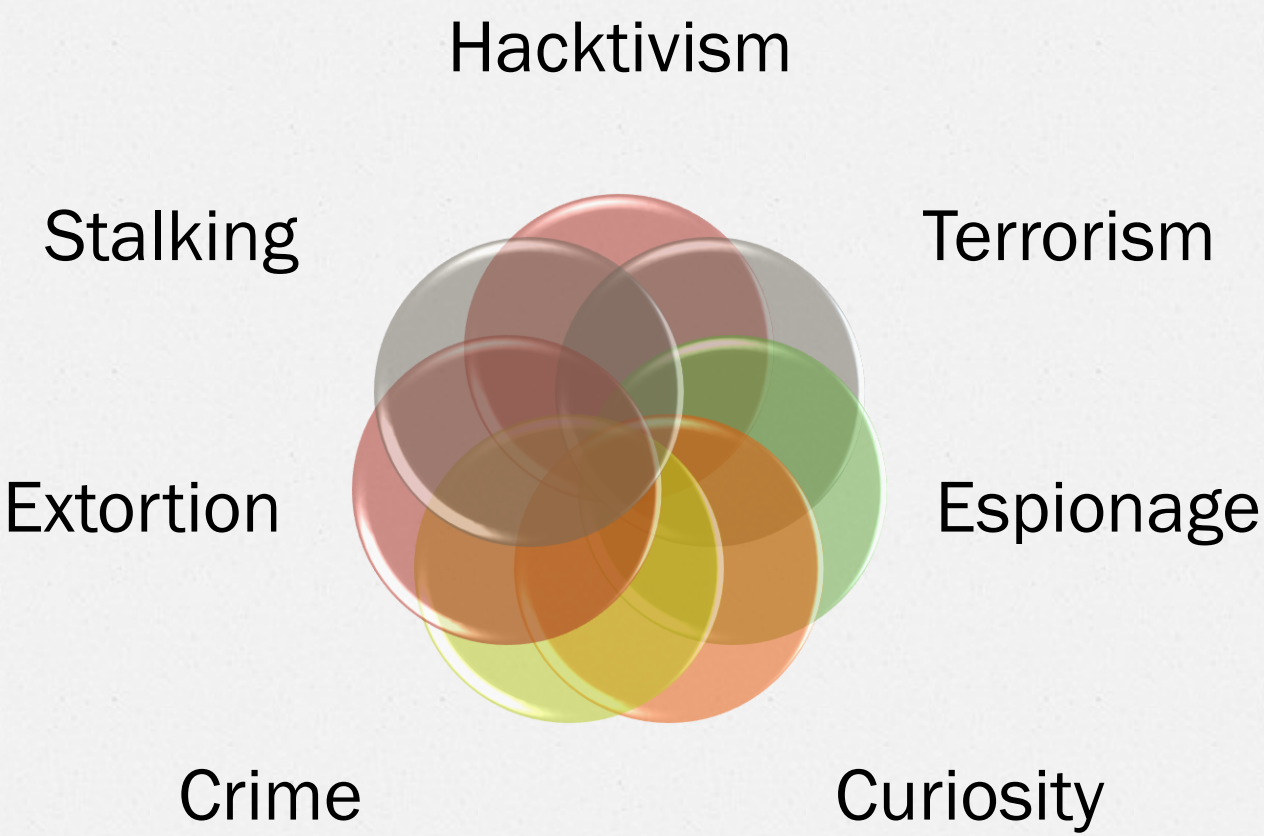
Today's Threats

- Existing weaknesses in technology
- Misconfiguration
- Poor policy and planning
- Human error
- Human malice
- Social Networking

Types of Hackers



Motivations for Hackers



What Makes it Possible?

- Ignorance
- Carelessness
- Recklessness
- Sharing of information
- Lack of training
- Smaller staff
- Social networking

What Does Security Impact?

- Security touches many diverse and seemingly unrelated systems
  - Improving security relies on knowing the “Big picture”
- Security is relevant to every system, process and person
  - Technical
  - Administrative
  - Physical

Note: In security one must understand the big picture

Penetration Testing and Ethical Hacking

- Used to test a target network
  - Target of Evaluation
- Test a network with a client's permission
- Never go outside the project scope
  - Without paperwork
- Emulate an actual attack

Why Pentest?

- Legal requirements
- Sanity check
- Part of a regular audit
- Build consumer confidence

Phases of Ethical Hacking

Approaches to Ethical Hacking

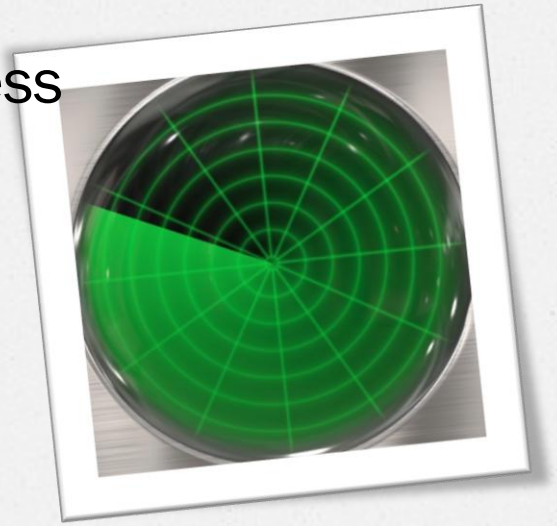
Ethical Hacking Tests

Steps in Ethical Hacking

- **Step 1:** Talk to your client on the needs of testing
- **Step 2:** Prepare NDA documents and ask the client to sign them
- **Step 3:** Prepare an ethical hacking team and draw up schedule for testing
- **Step 4:** Conduct the test
- **Step 5:** Analyze the results and prepare a report
- **Step 6:** Deliver the report to the client

Should You Pentest?

- Not a bad idea
- May be a legal requirement
- Can help validate systems
- Can find holes
- Can keep high state of readiness
- Can find outdated practices
- Yes



What We've Covered

- Elements of Information Security
- Security Challenges
- Effects of Hacking
- Who is a Hacker?