Social Engineering

Humans: The Good and the Bad
“Trusted people—people who must be trusted in order for the system to function—are part of any security system. They are a critical element, perhaps the critical element, because they’re the most resilient part of the system, the most able to improvise, the best equipped to make on-the-spot decisions, and the most skilled at detecting the presence of attackers. But of course human beings, when considered as components of a security system, are a double-edged sword. They can fall asleep, get distracted, and be tricked. They can turn against a security system. A good security system leverages the benefits of trusted people, while building counter-measures to prevent them from abusing that trust.”

- Bruce Schneier, Beyond Fear
Lecture Overview

● Core idea: humans are complex and less rigid than computers
● This can be either a good thing or a bad thing, depending on what the circumstances are
Human Security is Hard

- Humans are put in the position of making more subtle decisions than computers
  - They’re good at it! (way better than computers)
  - They’re bad at it (we didn’t evolve for this…)
  - Examples?
Human Security is Hard

- Humans are put in the position of making more subtle decisions than computers
  - They’re good at it! (way better than computers)
  - They’re bad at it (we didn’t evolve for this…)
  - Examples?
    - Should this person be let into the CIT?
    - Should I trust this person to sleep on my couch?
    - Should I trust this email from the prince of Nigeria?
Part 1: The Bad
Why target humans?

a. As we all know, software and hardware are immune to attack
b. It’s amusing
c. Humans are even more poorly designed than computer systems
Why target humans?

**A Crypto Nerd's Imagination:**

His laptop's encrypted. Let's build a million-dollar cluster to crack it.

No good! It's 4096-bit RSA!

Blast! Our evil plan is foiled!

**What Would Actually Happen:**

His laptop's encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.
Psychology!

- “Disease to please”
- Social proof
- Low self-confidence
- Greedy
- Trusting by default
- Easily pressured by time
ATTENTION: THE MANAGING DIRECTOR

DEAR SIR,

URGENT BUSINESS PROPOSAL

WE HAVE THIRTY MILLION U.S. DOLLARS WHICH WE GOT FROM OVER INFLATED CONTRACT FROM CRUDE OIL CONTRACT AWARDED TO FOREIGN CONTRACTORS IN THE NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC). WE ARE SEEKING YOUR ASSISTANCE AND PERMISSION TO REMIT THIS AMOUNT INTO YOUR ACCOUNT. YOUR COMMISSION IS THIRTY PERCENT OF THE MONEY.

PLEASE NOTIFY ME YOUR ACCEPTANCE TO DO THIS BUSINESS URGENTLY. THE MEN INVOLVED ARE MEN IN GOVERNMENT. MORE DETAILS WILL BE SENT TO YOU BY FAX AS SOON AS WE HEAR FROM YOU. FOR THE PURPOSE OF COMMUNICATION IN THIS MATTER, MAY WE HAVE YOUR TELEFAX, TELEX AND TELEPHONE NUMBERS INCLUDING YOUR PRIVATE HOME TELEPHONE NUMBER.

CONTACT ME URGENTLY THROUGH THE FAX NUMBER ABOVE.

PLEASE TREAT AS MOST CONFIDENTIAL, ALL REPLIES STRICTLY BY DHL COURIER, OR THROUGH ABOVE FAX NUMBER.

THANKS FOR YOUR CO-OPERATION.

YOURS FAITHFULLY,

PRINCE JONES DIMKA
3-4-95
Dear Manager,

(If you are not the person who is in charge of this, please forward this to your CEO, Thanks)

We are the organization of trademark intellectual property protection in China. Here we have something to confirm with you. We received a formal application on 24/07/2013. A company named "TianHui Import & Export Co. Ltd" was applying to register [redacted] as its Trademark and the following domain names:

- asia.cn
- com.cn
- com.tw
- hk.net.cn
- org.cn
- tw

After our initial checking, we found the names were similar to your company's, so we need to check with you whether "TianHui Import & Export Co. Ltd" has any relationship with you and whether the registration of the listed domains by "TianHui Import & Export Co. Ltd" would bring any impact on you. If no impact on you, we will go on with the registration at once. If you have no relationship with that company and the registration would bring some impact on you, please inform us within 10 workdays. Out of the time prescribed we will unconditionally finish the registration for "TianHui Import & Export Co. Ltd"

Please contact us in time in order that we can handle this issue better.

Best Regards,

David Tang

**Auditing Department.**
**Registration Department Manager**

4/F, No.9 XingHui West Street,

JinNiu ChenDu, China

Office: +86 2887662861

Fax: +86 2887783286

Web: [http://www.cn-network.com](http://www.cn-network.com)
Respect for Social Norms

- Social norms are ingrained
- People are very uncomfortable breaking them
- Examples?
Respect for Social Norms

● Social norms are ingrained
● People are very uncomfortable breaking them
● Examples?
  ○ Cell phones
  ○ Door piggybacking
Deference to Authority

- People are deferential to authority
- It’s often easy to appear to have authority
- Examples?
Deference to Authority

● People are deferential to authority
● It’s often easy to appear to have authority
● Examples?
  ○ Just sound like you know what you’re doing
  ○ Wear official uniforms (bank vault case)
USB Drop

- Department of Homeland Security drops USB drives in parking lots
- 60% of people who picked them up plugged them into a computer
- What was compromised?
Availability of Information

● ‘Security’ Questions:
  ○ In what city or town does your nearest sibling live?
  ○ What is the name of the place your wedding reception was held?
  ○ What is your pet’s name?
Historical Attempts: AOL (1998)

- Man calls AOL support, pretends to be employee
- Creates rapport, tells him that he’s got a nice car for sale
- Sends him an email with car.exe
- Whoops, backdoor.
@N Takeover

- Paypal reveals last 4 digits of CC by posing as employee
- GoDaddy accepted last 4 digits + first 2 to reset account
- MX records changed, allowing email access
- Reset Twitter password via personal domain
@mat Takeover

- Amazon reveals last four digits of CC
- Treated as secure information to reset @me.com email
- Resets Gmail password
- Resets Twitter password
What went wrong?

- More importantly, who was at fault?
- Every company independently was secure.
What went wrong?

- Every company independently was secure.
- But! Different companies have different sets of ‘secret’ information to verify identity
  - Credit card verification (last 4 digits, first 2)
  - Address
  - Mother’s maiden name
Hosting Providers

- Inputs.io - compromised chain of emails, called up hosting provider, asked for server password reset…
- Poloniex - posed as repairman, got physical access to machines
Secure Systems with Humans

- Why do spies classically travel with a cyanide pill?
Secure Systems with Humans

• Why do spies classically travel with a cyanide pill?
  ○ Humans have trouble containing information
  ○ Little safe or secure way to “encrypt” or hide sensitive information
Defense against the Dark Arts

- Education.
- Notice confusion.
  - When does your model break down?
- Principle of least privilege.
- Consistency.
- Assert yourself and don’t back down.
Security Fails

• We try to design security to be perfect
• Despite this, it *will fail*
  ○ Fail open (ie, let an attacker in)
  ○ Fail closed (ie, keep out a trusted party)
• Question: How do you cope with that failure?
• Examples?
Security Fails

● Examples?
  ○ Fail open
    ■ Metal detectors fail
    ■ Electricity drops, security camera turn off, doors open
  ○ Fail closed
    ■ I forgot my password
    ■ I lost my dorm key
Security Fails

- Systems can be *brittle* or *resilient*
- Brittle - a small failure can be very bad
- Resilient - a small failure can be coped with
- Examples?
Security Fails

- Systems can be *brittle* or *resilient*
- Brittle - a small failure can be very bad
- Resilient - a small failure can be coped with
- Examples?
  - Brittle - Airport security after 9/11
  - Resilient - Credit card security
  - Brittle - Biometric authentication
  - Resilient - A guard desk in the lobby
People are Resilient

- Ahmed Ressam and Diana Dean
- Other examples?
People are Resilient

- Ahmed Ressam and Diana Dean
- Other examples?
  - I forgot my cs department password
  - We’ve been hacked!
  - Natural disasters, etc
Takehome

- People have strengths and weaknesses
  - Very resilient
  - Unpredictable and unreliable
- Key goal: design security systems that take advantage of the good and avoid the bad