Computer Security

Stories of Social Engineering and No-Tech Hacking

Harrison, Ruzzo, and Ullman have **mathematically proven** why security is hard.

Security is hard for another reason: the **human element**.

Bruce Schneier offers further,

"It's is not natural for engineers. Good engineering involves thinking about how things can be **made to work**; the security mindset involves thinking about how things can be **made to fail**."

Attacking a system isn't always about deciphering an encrypted message with "128 bits of encryption" like on the TV shows.

Sometimes it's much easier. Sometimes, it involves **no technology** at all.

Vignette 1

Johnny Long
vulnerability assessment
testing of physical security.

Vince and Johnny are asked to emulate an external threat.

Image provided by Wikimedia Commons.

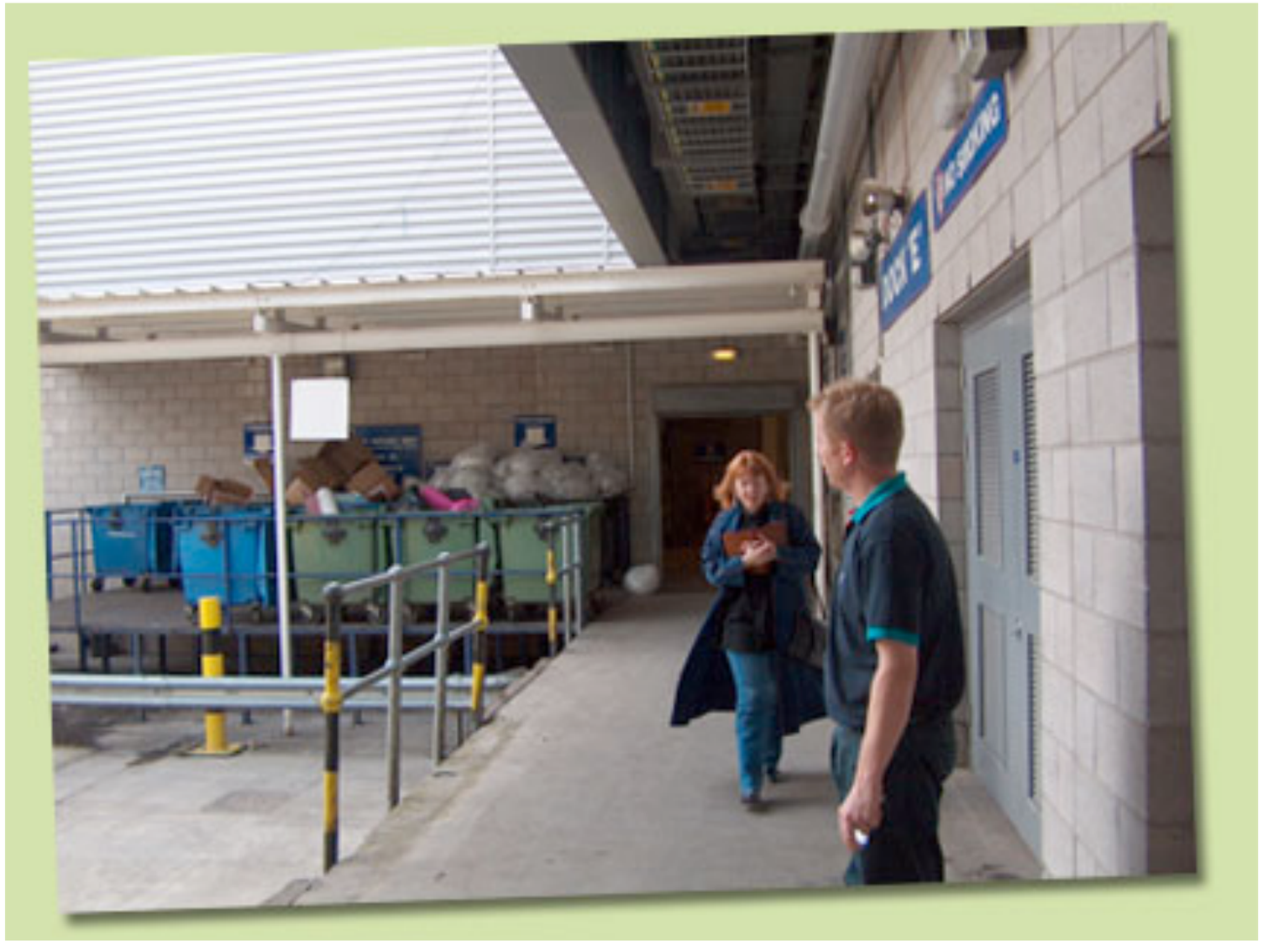
"They had poured a ton of money into expensive locks, sensors and survelliance gear"

-- Long

Image provided by Wikimedia Commons.

The Outer Gate. The site is enclosed entirely by a fence. Employees and visitors enter the site through a gate. Which is opened.

The Loading Dock: "Just look like you belong. Say hello to the employees. Be friendly. Comment on the weather"



The Exit Door: "Vince had seen that the bar on the exit door is touch sensitive. 'It doesn't operate by pressure; it operates when it senses it has been touched. Very handy in a fire.'"

--Long

They hack the door with a washcloth and a wire hanger.

Image taken from “The Simpsons”

Johnny keeps hacking.

These days he's working for "HackersForCharity".

But that's **physical security**. It's not as easy to no-tech hack computer security.

Right?

Human Psychology

"Consistently over 60% of people will do downright immoral things if they are told to"

--Ross Anderson paraphrasing Stanley Milgram

Stanley Milgram, 1961

"Randomly" choose a teacher and a learner. Put them in separate rooms.

The teacher, in a room with a "scientist" in a white lab coat asks the learner multiple choice questions.

If the learner is wrong, the teacher must shock him.

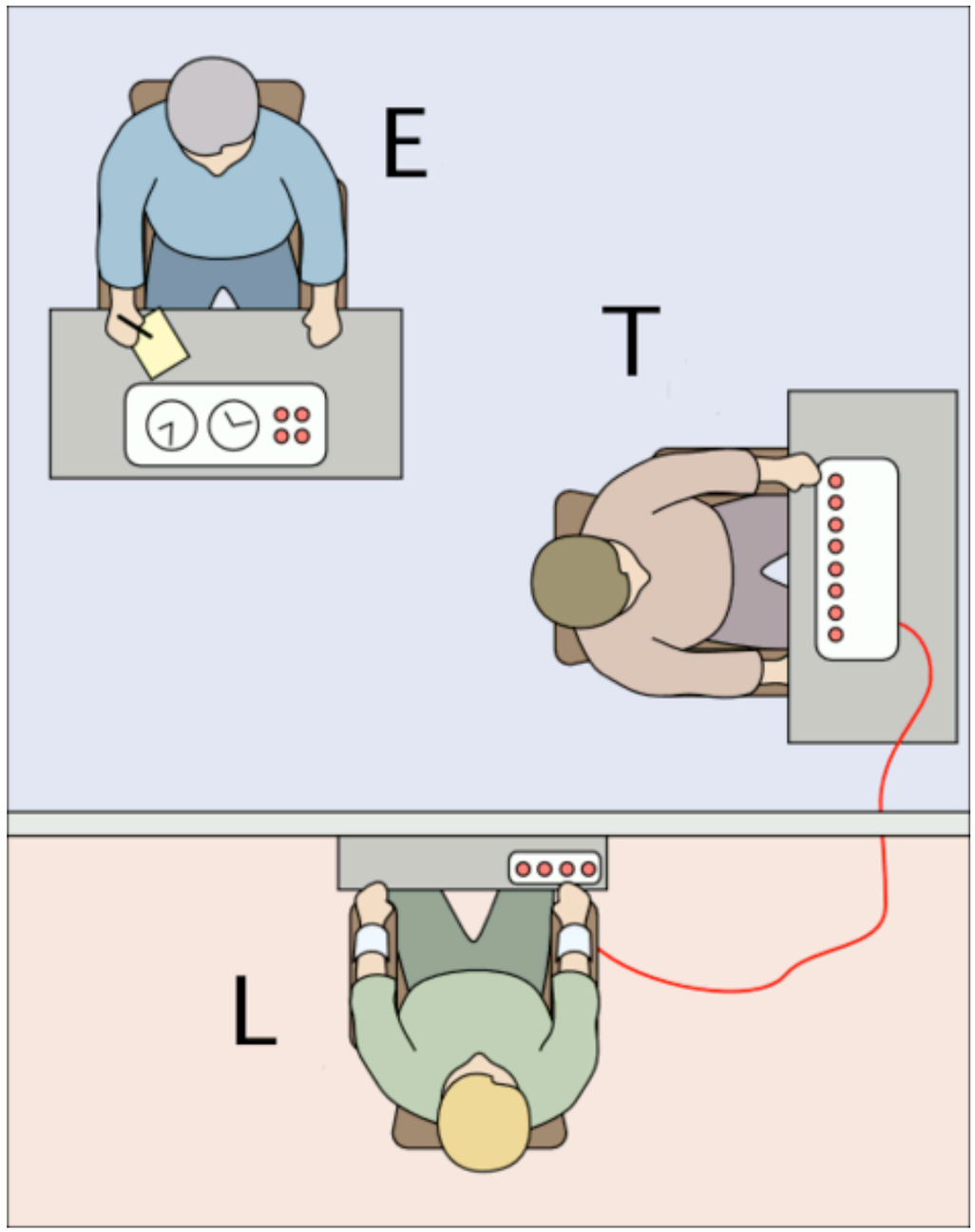


Image provided by Wikimedia Commons.

Vignette 2

Hacking Paris Hilton's Phone

In 2005, Paris Hilton's phone was hacked. The contents of her T-Mobile Sidekick were posted to illmob.org, including the phone numbers of Eminem, Vin Diesel, Lindsay Lohan, and Anna Kournikova.

Step 1.

The attackers learn of a programming glitch on the T-Mobile website. They figure out how to reset the password of any user whose phone was a sidekick. They just needed the user's phone number.

Step 2.

Get Paris Hilton's phone number.

The attackers get a caller-ID spoofer and call a T-Mobile sales store in California.

The conversation goes something like this:

“This is [invented name] from T-Mobile Headquarters in Washington. We heard you’ve been having problems with your customer account tools?”

“No, we haven’t had any problems really, just a couple of slow downs.”

“Yes, that is what is described here in the report. We’re going to have to look into this for a quick second.”

Step 2 (continued).

The T-Mobile rep gave out the URL of the internal T-Mobile site used to manage customer accounts. **Also**: username and password used by employees to login.

Step 3.

With Hilton's phone number, they could use the glitch to reset her password. A text message was sent to her phone. So the attackers called her, using their caller-ID spoofer.

“There are some network difficulties.

Have you been getting any SMS about a password reset?

What were the contents of the message?”

Step 3 (continued).

With the contents of her text message, they were able to change her password and lock her out of her phone.

Since videos and data on the Sidekick are stored on T-Mobile's central servers, they could download all of Hilton's info to their own phones.

I was like, HOLY [expletive], DUDE...SHES GOT NUDES."

“The average $10-an-hour sales clerk will tell you anything you want...these people are not usually well-trained, and they tend to be more customer friendly and cooperative.”

-- Kevin Mitnick

Vignette 3

Patricia Dunn and the HP spying scandal

Carly Fiorina

In 2005, CNET publishes an article about how Carly clashes with the Hewlett Packard Board.

Clearly there's a leak. She's gonna find it.

Except she gets fired.

Image provided by Wikimedia Commons.

Patricia Dunn

Dunn becomes "Non Executive Chairman of HP" and assumes head of the search.

Private detectives, subcontractors of HP, are told to **get phone records** of journalists, HP board members, and employees.

They use pretexting. A social engineering term referring to impersonating the target victim to get others to divulge information.

August 11, 2006: Letter from AT&T to Thomas Perkins, a HP board member who resigned when George Keyworth was found and accused of being the leak.

Turning to your inquiry, this is what we know. First, with respect to your "local" residential telephone account with the former SBC (now AT&T), an online account was established on January 30, 2006. Notably, that appears to be the only date of access to this account - i.e., it appears this was a one-time attempt to obtain information and, although your billing records for December 2005 and January 2006 would have been accessible, it appears that the person reviewed only your bill for the January 2006 billing period. The person registering the online account did so through the Internet and provided your telephone number and the last four digits of your Social Security Number to identify himself/herself as the authorized account holder. We have no way of determining how the person obtained this Social Security Number information.

The attackers used his SSN and phone number to open an online account to his local telephone account. HP had provided this information to the attacker.

August 11, 2006: Letter continues.

Second, with respect to the AT&T long distance account associated with the above-referenced phone number, a separate online account was established January 29, 2006. The background on this account is slightly more complex. Initially, an attempt was made to register this account over the Internet. It appears that this failed because the person attempted to utilize the last four digits of your Social Security Number for authentication, but our account records for this long distance account did not contain that information and thus the authentication failed.

Subsequently, a call was made to the AT&T Customer Care Unit for assistance. Although our records do not contain specific details of the call, it appears the caller represented himself as the customer of record, provided identifying information to the service representatives satisfaction, and sought assistance because of the inability to complete the online registration. The AT&T service representative then apparently established the online account while the person was on the phone. Our records indicate that the online account was subsequently accessed on February 2, 2006. Again, that appears to have been the only date of access for this online account, and our records indicate that although the November 2005 to January 2006 billing records were available for review, the person viewed only your bill for the January 2006 billing period.

The attackers tried the same approach with his long-distance account, but had to call customer service to get assistance opening the online account.

September 2006: Patricia Dunn is asked to resign.

"I have resigned today **at the request of the board**. The unauthorized disclosure of confidential information was a serious violation of our code of conduct. I followed the proper processes by seeking the assistance of HP security personnel. I did not select the people who conducted the investigation, which was undertaken after consultation with board members. I accepted the responsibility to identify the sources of those leaks, but **I did not propose the specific methods of the investigation**."

--Patricia Dunn's public statement from HP website

In 2007, the FCC strengthened privacy rules to protect against pre-texting.

Carriers are now required to notify the customer immediately when the following are created or changed:

- a password
- a back-up for forgotten passwords
- an online account
- the address of record

Vignette 4

Jonathan Lebed hacks Wall Street

In 1996, Jonathon Lebed was 12 years old.

In a nationwide stocking picking contest hosted by CNBC, Lebed's team "Triple Threat" placed fourth.

On September 20, 2000, the Securities and Exchange Commission (SEC) settled its case against Jonathon Lebed, age 15.

Why?

He sent a lot of e-mails.

Subj: THE MOST UNDERVALUED STOCK EVER

Date: 2/03/00 3:43 pm Pacific Standard Time

From: LebedTGI

FTEC is starting to break out! Next week, this thing will EXPLODE...

Currently FTEC is trading for just $2 1/2! I am expecting to see FTEC at $20 VERY SOON.

Let me explain why...

Revenues for the year should very conservatively be around $20 million. The average company in the industry trades with a price/sales ratio of 3.45. With 1.57 million shares oustanding, this will value FTEC at ... $44.

It is very possible that FTEC will see $44, but since I would like to remain very conservative...my short term target price on FTEC is still $20!

The FTEC offices are extremely busy...I am hearing that a number of HUGE deals are being worked on. Once we get some news from FTEC and the word gets out about the company...it will take off to MUCH HIGHER LEVELS!

Starting in September 1999, Lebed would pick and buy a stock. He would write a single message about it. Then he would post it as many times as possible to Yahoo! Finance message boards.

He learned how to write his messages from watching the home shopping show “Shop at Home!”

He found limitations on how many messages he could post. He rotated through AOL screen names and Yahoo logins to post around 200 messages before he went to school.

Next message, he found his Yahoo accounts deleted, so he just made new ones.

It’s called a pump-and-dump.

It’s illegal.

As his lawyer comments, “what little Jon seemingly wasn’t aware of was that only chartered financial analysts are legally entitled to engage in the practice.”

In four years, Lebed made $800,000.

He settled with the SEC for $285,000.

Lesson: It doesn't matter if you are using 4 zillion bits of encryption if someone can just as easily bribe your ex-spouse to get your password.