ECE590
Computer and Information Security

Fall 2020

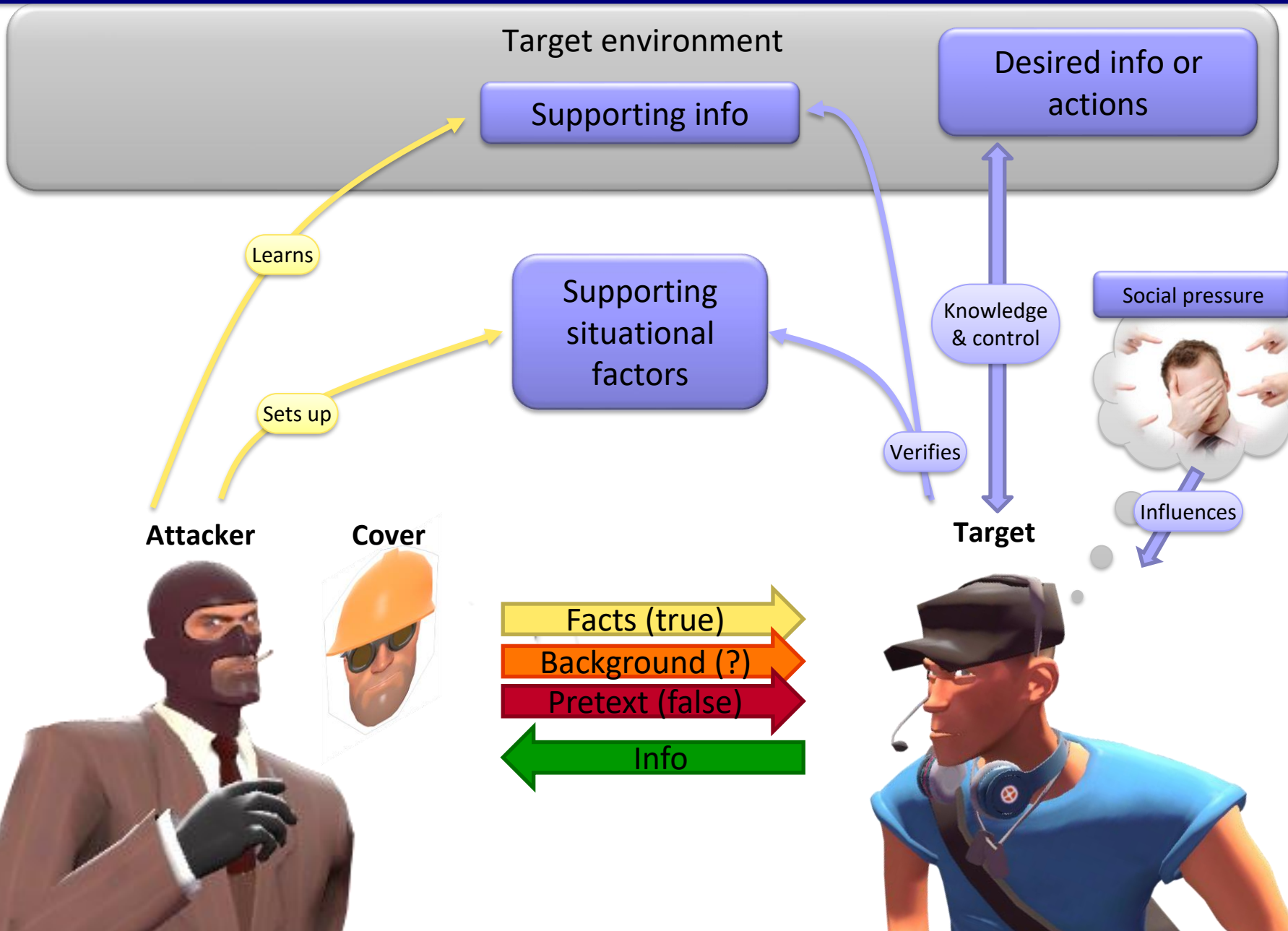
Human Factors and Social Engineering

Tyler Bletsch
Duke University

Definition

- What is non-social engineering?
  - Manipulating objects to achieve an end
- What is social engineering?
  - Manipulating *humans* to achieve an end
- Why?
  - The humans are almost always the weakest point in any system!

Social Engineering Model



Pretext, support, and cover

- **Pretext**: The false pretense on which the interaction is based
  - Supporting **information**:

	Verifiable during attack	Non-verifiable during attack
True	Fact	Background
False	Pretext	

    - **Fact**: "Bob was recently hired."
    - **Background**: "I look/sound like Bob."
    - **Pretext:** "I'm Bob."
  - Supporting **situational factors**
- **Cover**: The identity used in the pretext ("Bob")

Verifiable support for the pretext

- **Facts**: Stated support for the pretext, e.g.:
  - "This site was just opened, so everything's nuts."
  - "Your boss's name is Susan."
  - "I know we need a code number to clear this error."
- **Situational factors**: Implied support for the pretext, e.g.:
  - Caller ID says it's a call from inside the office
  - The guy is standing in front of me in a nice suit
  - He has an employee badge

“Facts” are more than you think

- **Terminology**
- Simple **public information**
  - Office locations
  - Public phone numbers
  - Public employee data (e.g. “meet our staff” page)
  - Public records (tax info, building info, patents, etc.)
  - Documentation
- Info from **social networks**
- Subtle **mannerisms** of your cover
  - If a specific person, their writing or speaking style
- Stuff obtained from **dumpster diving**!

Social norms and social pressure

Thought	Exploit
I want people to like me	“Could you be a pal and help me login?”
I don’t want to make someone angry (Especially if they have power over me)	“I’m the CFO, and your badgering about security codes is going to make me miss our earnings call!”
I don’t want to hurt people (Especially colleagues)	“If you don’t open this firewall port, the product demo will fail and I could be fired!”
I want to appear confident and competent	“Don’t you know how to admin a Cisco BXQ9458? Just type ‘grant everyone all’ and it will work!”
I want power/money	*picks up thumbdrive labeled ‘salaries’*
I want the admiration of my peers	“Can you help us save the product launch? All you have to do is click ‘allow’!”

Teller's Psychology of Magic

1. **Exploit pattern recognition.**
2. Make the secret a lot more trouble than the trick seems worth.
3. It's hard to think critically if you're laughing.
4. Keep the trickery outside the frame.
5. To fool the mind, combine at least two tricks.
6. Nothing fools you better than the lie you tell yourself.
7. **If you are given a choice, you believe you have acted freely.**

From "Teller Reveals His Secrets".

Kevin Mitnick - Art of Deception

- "People inherently want to be helpful and therefore are easily duped"
- "They assume a level of trust in order to avoid conflict"
- "It's all about gaining access to information that people think is innocuous when it isn't"
- Here a nice voice on the phone, we want to be helpful
- Social engineering cannot be blocked by technology alone

Adapted from "Social Engineering: The Art of Social Hacking" by Christopher Stowe

Attacker goals

- May just want info for the next conversation:
  - “Can you look up an employee ID number for me?”
  - “Can you give me the extension for so-and-so?”
- Logins, passwords, or connection info
  - Including password reset questions that may come up in conversation (first pet’s name, street you grew up on, parent’s birthplace, etc.)
- Permissions:
  - “Can you give me access to such-and-such?”
  - “Can you unblock myhackedsite.com?”
  - “Can you open port 22?”
- Actions:
  - “Can you visit this link for me?”
  - “Can you set this DVD on my desk?”
  - “Can you put the DVD on my desk into the drive?”
  - “Can you click ‘yes’ on my screen?”

Defense fundamentals

Education

- Explain the danger
- Present realistic examples
- Don’t talk down to people
- Make clear who has responsibilities to support others and provide information

Culture

- Security must be taken seriously (but not excessively)
- Need to avoid cry-wolf effect
- Individuals must be confident to check credentials without fear of reprisal

Policies

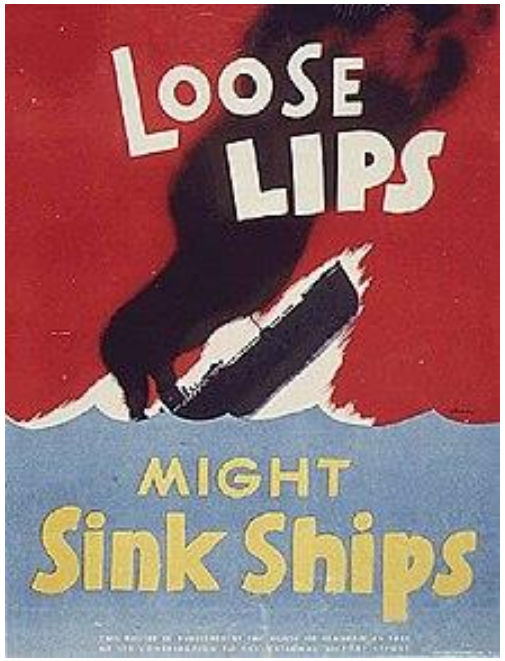
- Explicitly state what information can be made public; rest is confidential
- Establish procedures for identity verification, even for exceptional situations

Deeper defense through auditing

- Periodic **auditing**
  - Try to solicit employees to reveal confidential information, make config changes, etc.
  - Provide reporting mechanisms and reward employees who report attacks (both fake and real)
  - Follow up technical anomalies (e.g. IDS/logwatch results) with human investigation
- Exploit the “cry wolf” effect
  - If your auditors are always trying to catch employees, they will develop an immunity to actual attackers

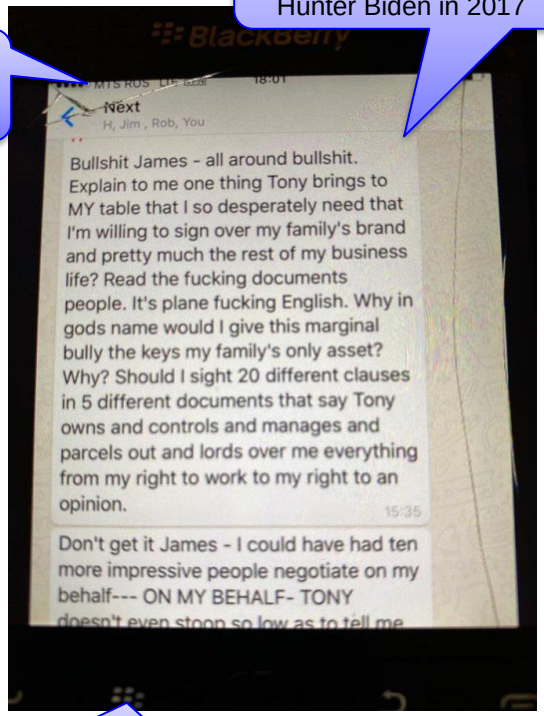
OPSEC: Operations Security

- **OPSEC**: Actions to prevent adversaries from learning useful information through inadvertent leaks
- Applies to attackers and defenders:
  - Poor OPSEC for attacker:
    - Attacking from actual IP address
    - Letting attack tools fall into defender hands
    - Failing to hide method of infiltration, allowing exploit to be discovered
    - Leaving evidence in logs
  - Poor OPSEC for defender:
    - Leaving internal info accessible to public (e.g. network map, countermeasures deployed)
    - Posting credentials to public repos
    - Letting attacker under investigation know they're being tracked
    - Announcing weaknesses and vulnerabilities



Bad OPSEC examples in the news

- Bad attacker OPSEC: Russian misinformation operation



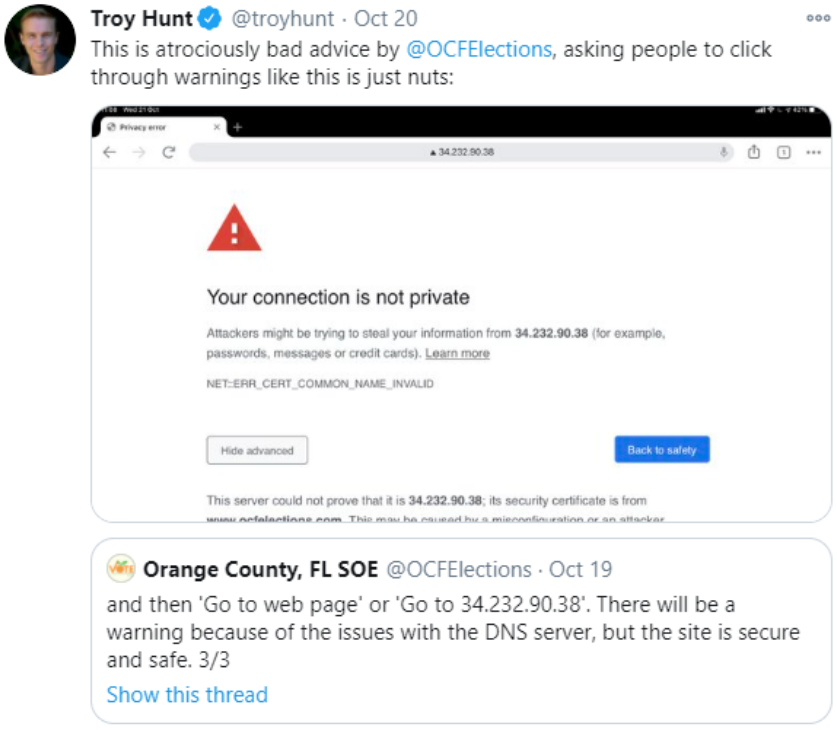
WhatsApp text purported to be sent by Hunter Biden in 2017

Cell provider that only operates in Russia

It's a Blackberry, which discontinued WhatsApp support in 2016

https://www.rawstory.com/2020/10/rudy-is-so-bad-at-this-giuliani-mocked-after-photo-of-alleged-hunter-biden-text-is-linked-to-russia/

- Bad defender OPSEC: Florida election board



https://twitter.com/troyhunt/status/1318721481765908480

Exercise examples

"Due to the rise in inclement weather, we're committed to our employee's safety and are in the process of upgrading our remote access gateway so that everybody has the opportunity to work from home. Please click the link below to install the new software. You will be asked to enter your credentials before continuing."

- Fit it to the model:
  - Supporting info/situational factors?
  - Pretext?
  - Social pressures?
  - Goal?
- How could it be prevented?

Source. From a successful email phishing campaign.

Exercise examples

Unauthorized person glides in behind someone at card-locked door and wanders halls of a company looking for information or objects to steal.

- Fit it to the model:
  - Supporting info/situational factors?
  - Pretext?
  - Social pressures?
  - Goal?
- How could it be prevented?

Exercise examples

Contractor shows up at front desk, says he's there to top up the fire suppression system. Once inside, he does a costume change into a suit, tells a random worker he's an executive from out of town and needs a desk to work at for the day.

- Fit it to the model:
  - Supporting info/situational factors?
  - Pretext?
  - Social pressures?
  - Goal?
- How could it be prevented?

Exercise examples

A call to a remote Walmart from "a newly hired manager of government logistics" seeking "a complete picture of the store's operations" for a "a multi-million-dollar opportunity to win a major government contract".

- Fit it to the model:
  - Supporting info/situational factors?
  - Pretext?
  - Social pressures?
  - Goal?
- How could it be prevented?

Source. From a successful social engineering competition at DefCon 2012.

Exercise examples

Email selling a stock advice service includes some non-trivial stock market predictions. The predictions turn out correct! A follow-up comes in with another batch of predictions, and they turn out to be right, too! One more set of predictions arrive, and again they're right! They predicted the market three times in a row…must be legit, right?

- **What's the trick?**
- Fit it to the model:
  - Supporting info/situational factors?
  - Pretext?
  - Social pressures?
  - Goal?
- How could it be prevented?

Source: John Huggard's personal finance course at NC State

Exercise examples

Video

Attacker and friend break into a secure telco datacenter for a self-guided tour. Is apprehended, pretends to be visiting engineer, the guard calls VP for the site in the middle of the night, attacker gets on and talks over her confused questions with "yes, I'm here as planned", hangs up before handing the phone back, and leaves before she can find the number to call back.

- Fit it to the model:
  - Supporting info/situational factors?
  - Pretext?
  - Social pressures?
  - Goal?
- How could it be prevented?

Source. Story from Kevin Mitnick circa 1993.

Conclusion

- Human factors can be the weakest links
- Pretexting:
  - Provide enough facts and unverifiable, plausible background information that the lie isn't questioned
- Defense:
  - Education
  - Culture
  - Policies
  - Auditing