SOCIAL ENGINEERING

Dress = $300. Rented Tux = $200.
Bypassing Secret Service to meet the president inside the White House = Priceless!
“Stratagem 1 "Deceiving the heavens to cross the sea”
瞒天过海
(Using the the 36 stratagems for Social Engineering)

Jayson E. Street, CISSP, C|EH, GSEC, GCIH, GCFA, IEM, IAM, ETC…
Let go of my EGO

Who Am I?

defcon18@f0rb1dd3n.com
Hacker/Social Engineer

INFOSEC talk = slide like this ;-) 

- Sun Wu (Tzu) “Ping-fa”(The Art of War)
- All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near. Hold out baits to entice the enemy. Feign disorder, and crush him.
Contents

• INTRO
• History of the 36 Stratagems
• History of Social Engineering
• How S.E. differs between cultures
• The new OSI model
• Top 5 Stratagems relating to S.E.
• Discussion
The History of the 36 Stratagems

Cooking = France

Painting = Italy

Military Strategy = China
The History of Social Engineering

From the beginning of time before it had a name it was being used as an effective form of attack.

Amenhotep III

The first Trojan attack

Bards masters of the (S.E.) craft
How S.E. differs between cultures

Asia: Save face = Losing secrets

Europe: Command = Control

North America: Do unto others = Before they do to you

South America: Mutual benefit = An uneven outcome
The new OSI model

Layer 1-6 is over used time for a new vector. Layer 7 good but getting better defended. Layer 8 less guarded and can’t be patched ;(-)
Why use Layer 8?

---

Credit to @jcran
3. "Killing with a borrowed knife"
借刀杀人

Turn an enemies asset against him
(Let the employee be the attack vector)
3. "Killing with a borrowed knife"

借刀杀人

Cont...
3. "Killing with a borrowed knife"
借刀杀人
Cont…
3. "Killing with a borrowed knife"
借刀杀人
Cont…
3. "Killing with a borrowed knife"
借刀杀人
Cont…
3. "Killing with a borrowed knife"
借刀杀人

Cont...
3. "Killing with a borrowed knife"

借刀杀人

Cont...
3. "Killing with a borrowed knife"
借刀杀人
Cont...

Realtime results for "headed to"

JaybirdGSU: Headed to Savannah at 4
less than 20 seconds ago from bit - Reply - View Tweet

smedaris: Starbucks, then headed to work to start an experiment. Not my ideal saturday.
half a minute ago from UberTwitter - Reply - View Tweet

KaramatFabrics: Headed to the first meeting of the Houston Modern Quilt Guild
half a minute ago from UberTwitter - Reply - View Tweet

lostintranslatn: Headed to Beaufort, SC.
half a minute ago from Twitterific - Reply - View Tweet

banamatt: headed to work, then to the sisters for my nieces birthday.
half a minute ago from web - Reply - View Tweet

iratlee: just had one of my better business ideas, must research. was headed to get my hair cut. "u don't know" jay-z remix was on the radio.
hal a minute ago from Tweetie - Reply - View Tweet

gordyfisher: What de gwan twedren mi headed to de festivities hyah den a coconut tree burn fya
less than a minute ago from UberTwitter - Reply - ViewTweet

kilnichfactor: @GUBLERNATION if you're headed to Times Square, go to the Sanno store across from AMC theaters. They got sick threads bro!!
less than a minute ago from web - Reply - ViewTweet

vachtladyk: is headed to Tn to visit w/family. Still sporting my UK hoodie. Go Cats
3. "Killing with a borrowed knife"
借刀杀人
Cont…

Thanks @jonoberheide
3. "Killing with a borrowed knife"

借刀杀人

Cont...

Thanks @jonoberheide
5. "Looting a house on fire"

Lay offs / acquisitions create the proper kind of chaos for a subtle attack.
15. "Luring a tiger from its lair in the mountain" 调虎离山

Wait for the worker to take his network (laptop) to you.
15. "Luring a tiger from its lair in the mountain"

调虎离山
15. "Luring a tiger from its lair in the mountain”
17. "Tossing out a brick to get a jade"

$15.00 USB could return an investment of $5,000,000. If cast out to the right “lucky” person
36. "Escape - the best scheme"

走为上

Every plan should have an exit strategy in case the attack fails (especially if you are doing it in the “real world”).

Chance

THIS CARD MAY BE KEPT UNTIL NEEDED OR SOLD

GET OUT OF JAIL FREE

©1935 Hasbro
Okay now what can we do?
Okay now what can we do?

SECURITY AWARENESS
I'm tired of these Motha FSCKing Users!
With Motha FSKing easy to guess passwords!
Okay now what can we do?

PHYSICAL COMPROMISE

Yeah it's just like them.
Okay now what can we do?

APT

There are people smarter than you, they have more resources than you, and they are coming for you. Good luck with that.

Thanks to @0ph3lia
Okay now what can we do?

• Without understanding where the opponent's weaknesses are you cannot borrow their strength to use against them. (Cheng Man Ching)

• http://www.dissectingthehack.com
• http://f0rb1dd3n.com
• http://headhacker.net
• http://www.social-engineer.org/
• http://netragard.com
• http://isc.sans.org

• @jaysonstreet on Twitter
Now let’s learn from others

• Discussion and Questions?????

• Or several minutes of uncomfortable silence it is your choice.

• This concludes my presentation Thank You
Those Links Again

- http://www.dissectingthehack.com
- http://f0rb1dd3n.com
- http://headhacker.net
- http://www.social-engineer.org/
- http://netragard.com
- http://isc.sans.org
- @jaysonstreet on Twitter