OPSEC and defense against social engineering for devels, execs, and start-ups

@KirilsSolovjovs on twitter

http://kirils.org for more

Mg.sc.comp. Kirils Solovjovs

Possible Security

Contents

- Problem: Social Engineering
  - concepts
  - attacks
- Solution: OPSEC
  - theory
  - practice

[video]

This is how hackers hack you using simple social engineering

https://www.youtube.com/watch?v=lc7scxvKQOo

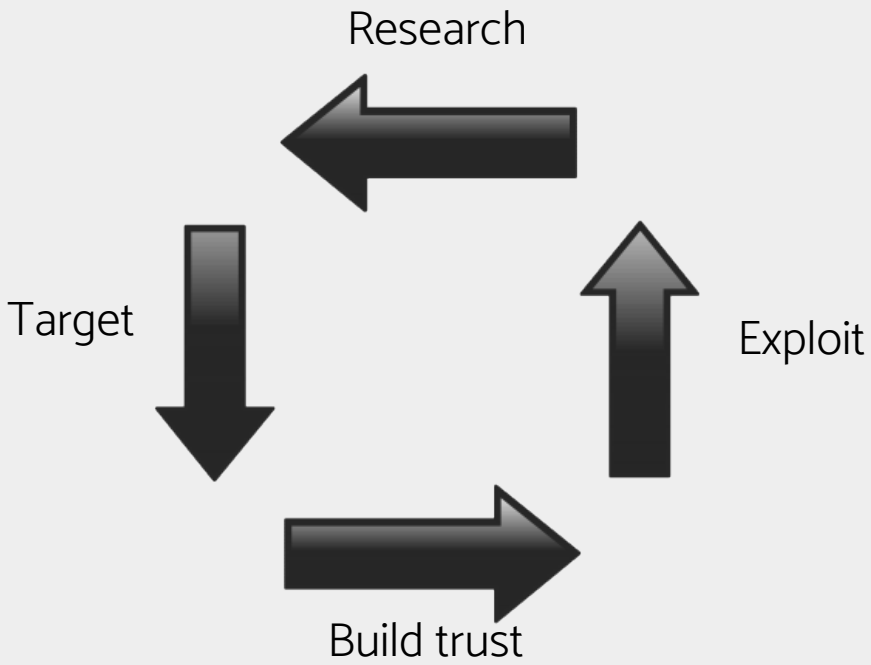
Social Engineering

Social Engineering (SE)

is the use of deception to manipulate individuals into divulging sensitive information that may be used for illegitimate or fraudulent purposes or to further attacks on a larger entity

SE attack cycle for organisations

- Research
- Target
- Build trust
- Exploit



SE attack types (in person)

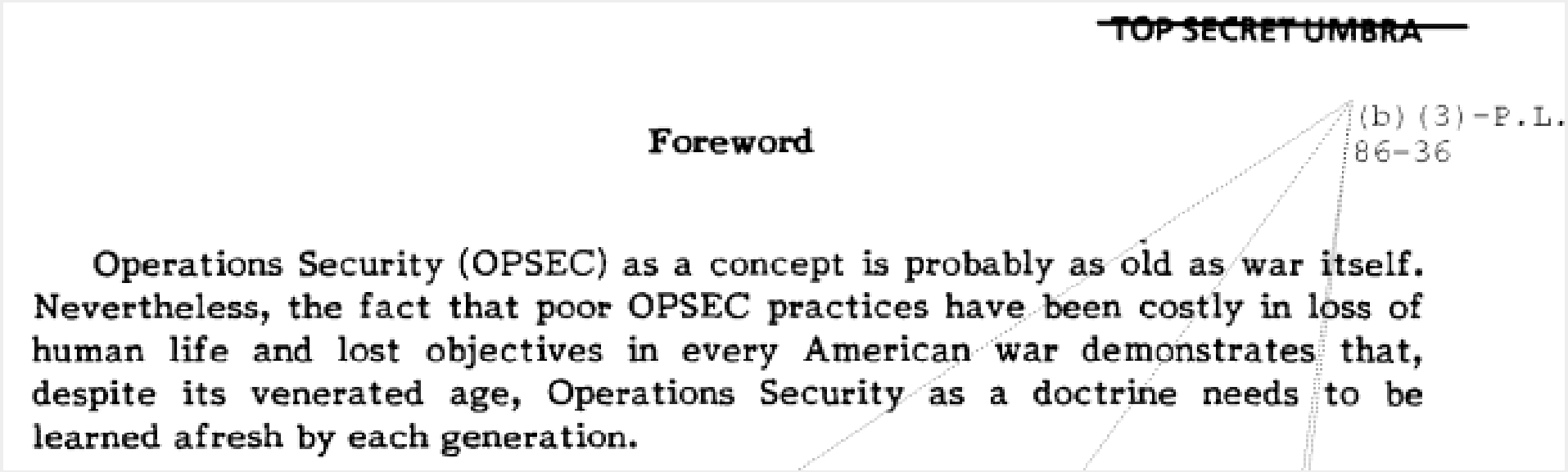
- Impersonation
  - VIP, user, tech
  - appeal to authority
  - reverse social engineering
  - identity theft
- Access
  - tailgating
  - key duplication
- Acquisition
  - eavesdropping
  - shoulder-surfing
  - dumpster-diving

SE attack types (remote)

- Types
  - phishing, spearphishing
  - vishing
  - app impersonation
- Delivery vehicles
  - e-mails
  - usb drops
  - instant messages, sms
  - social networks
  - traffic injection
  - malware, adware

Operations Security

OPSEC or Operations Security



~~TOP SECRET UMBRA~~

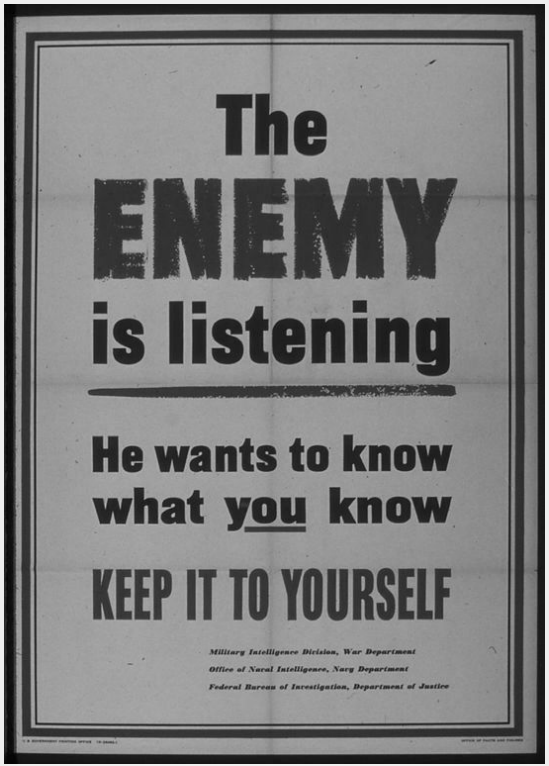
(b)(3)-P.L. 86-36

Foreword

Operations Security (OPSEC) as a concept is probably as old as war itself. Nevertheless, the fact that poor OPSEC practices have been costly in loss of human life and lost objectives in every American war demonstrates that, despite its venerated age, Operations Security as a doctrine needs to be learned afresh by each generation.

OPSEC history

- Military origins
- Has found use in today's cybersecurity
  - Why? Humans – the weakest link
  - Solution? OPSEC



OPSEC

- Identification of critical information
- Analysis of potential threats
- Analysis of your vulnerabilities
- Assessment of risk
- Application of appropriate countermeasures

Identification of critical information

- Losing which information would be detrimental to you?
- Gaining which information would be beneficial to your competitors?
- Examples:
  - passwords
  - research data
  - analytical data

Analysis of potential threats

- What are the current cybersecurity threats and exploits?
- Which threat actors should you be concerned about?
  - competitors
  - entities
- Examples:
  - Company B is developing the same product as we and is rumored to have offensive cyber capability.
  - We are travelling to China with corporate laptops and fear intercept.

Analysis of your vulnerabilities

- What are the potential deficiencies of your security process?
- What could reveal your critical information?
- Can you fix it?
- Think like the enemy! Where would you attack?
- Examples:
  - Our tech support does not properly identify callers before providing assistance
  - We don't have a firewall and do not follow secure coding practices

Assessment of risk

- What is the risk of each vulnerability?
  - Multiply every potential threat with every weakness to get the risk!
  - Risk = Impact x Probability
- What OPSEC measures can you apply for each vulnerability?
- Examples:
  - Impact of tech support not identifying callers is medium (5), because of limited tech support permissions. Interests and capabilities of Company B make it very likely (8) that they will target us, therefore risk = 5 x 8 = 40%. We can require callers to provide secret phrases when connecting over the phone.

Application of appropriate countermeasures

- Have you implemented countermeasures for the risks identified?
- What do you need to apply all the required countermeasures?
- What hinders application of the required countermeasures?
- Is it financially feasibile?
  - Prioritize by risk!
- Examples:
  - Our top risk ir rated 40% and costs 1800€ per year in extra workload and lost productivity, so we will be implementing it starting 1st of April 2018 and financing it from the IT support budget.

Tips for Operations Security

Practical OPSEC tips (everywhere)

- Secure passwords
  - create strong passwords
  - use a password manager or your head
  - don't reuse passwords
- Install latest security updates
- Do not connect unknown devices to your device or vice versa
- Mindfully decide, if you will share a piece of information (including on social media)

Practical OPSEC tips (outside the office)

- Use VPN to protect your data when using other networks
  - If using a VPN is not possible, **do not** use shared WiFi hot-spots
- Know where your stuff is
- Keep your devices and work information (e.g. printouts) with you at all times, if possible
- Be aware of your surroundings when processing sensitive information
  - talking on the phone, working on a laptop, having a face-to-face conversation

Methodological OPSEC tips (1)

- Carry out regular employee awareness trainings
  - consider reminders / posters
- Test your employees by carrying out mock social engineering attacks
- Make sure that everyone, ~~including~~ <u>especially</u> founders / exec branch commits to OPSEC

Methodological OPSEC tips (2)

- Discover your vulnerability surface as seen from the outside
- Carry out or purchase penetration tests
- Set up technical defenses and countermeasures
- Manage risk posed by contractors and suppliers

Q&A

Slides are available on http://kirils.org

Find me on twitter: @KirilsSolovjovs