18 June 2006

Social Engineering for Penetration Testers

Sharon Conheady

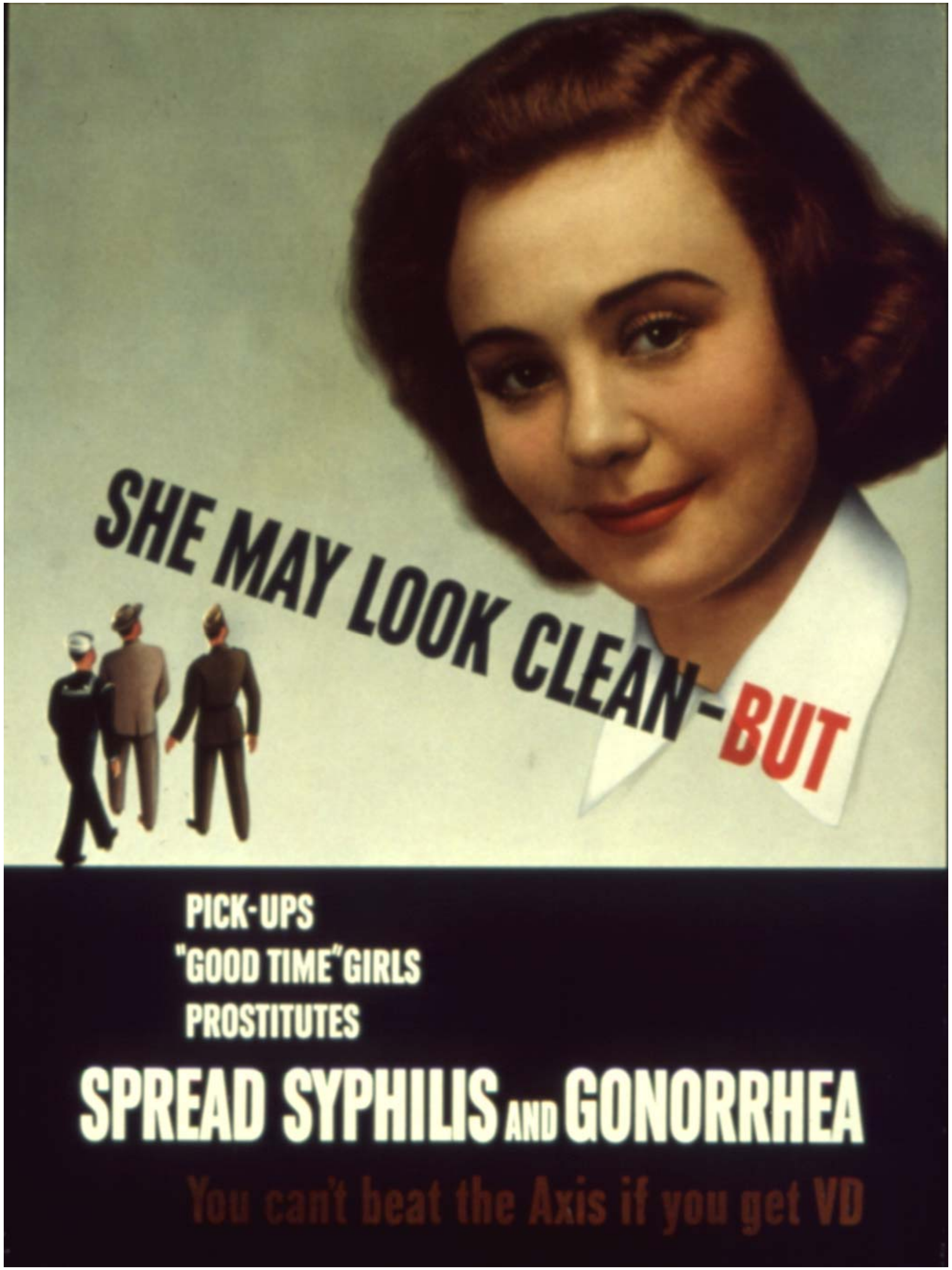
sconheady@uk.ey.com / evil@smokinggnu.org

+44 (0)20 7951 8936

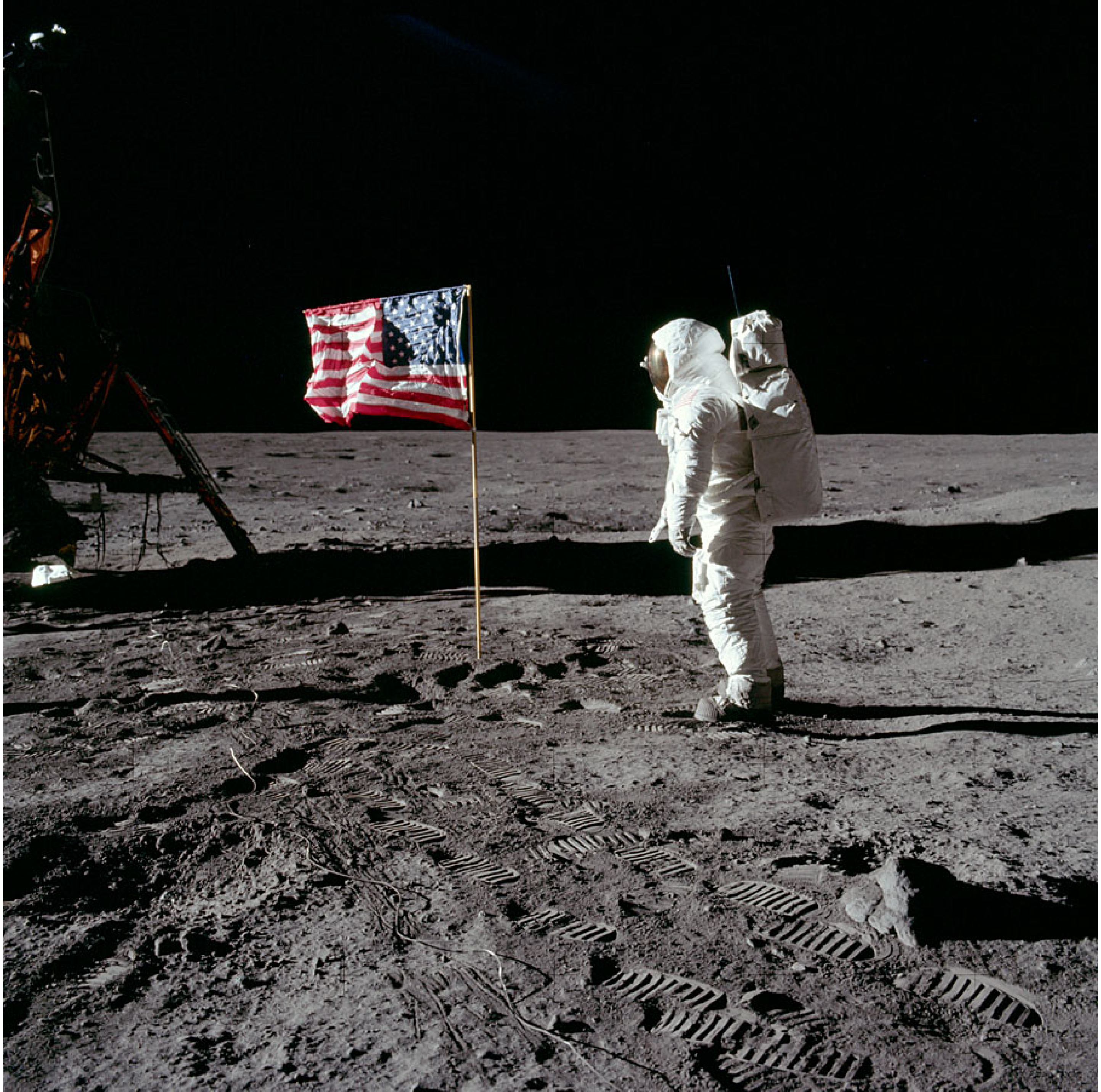
What is Social Engineering?

efforts to influence popular attitudes and social behaviour on a large scale, whether by governments or private groups

- Wikipedia definition


SHE MAY LOOK CLEAN-BUT
PICK-UPS
"GOOD TIME"GIRLS
PROSTITUTES
SPREAD SYPHILIS AND GONORRHEA
You can't beat the Axis if you get VD

Join the Fight to be Fit!



Your potential. Our passion.™
Microsoft®
start something
Sonic
Start discovering new music.
Collecting the old stuff. Start recording your own.
Mixing and mashing. Taking it on the road.
Start creating your personal soundtrack.
Windows xp

With a world of software and devices that run on Windows® XP, the choice is yours. Go to **windows.com** and start anything you like.

© 2005 Microsoft Corporation. All rights reserved. Microsoft, Windows, the Windows logo, and "Your potential. Our passion." are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

What is Social Engineering?

techniques hackers use to deceive a trusted computer user within a company into revealing sensitive information, or trick an unsuspecting mark into performing actions that create a security hole for them to slip through

- Kevin Mitnick

Different types of attacks

- Mumble attack

- Reverse engineering

- 10 attack

- Phone v’s Physical

- Lots more

The social engineering problem

- Sumitomo Mitsui Bank

- Lexis-Nexis

- ChoicePoint

- Credit Union

Why perform a social engineering test?

- To test the effectiveness of physical security controls
- To test the level of security awareness among staff
- Good practice for staff

The stages of the attack

1. Target identification
2. Reconnaissance
3. Creating your scenario
4. Going in for the attack
5. Getting out again

Reconnaissance

- Passive information gathering
  - Google
  - Company website
  - Annual reports
  - Job ads / Employee resumes
  - etc
- Physical reconnaissance
  - Where are the security guards?
  - Do smokers congregate in a certain area outside?
  - Where are the CCTV cameras?
  - What time do employees go in / leave the office?
  - etc

Creating Scenarios

- Think about how sophisticated your attack needs to be
- More security focused organisations, eg, banks, will require a more complex attack
- Use props
- Keep it realistic

Going in for the attack

- Use your scenario to get in
- Gain access to network
- Prove you were there
- Think about how to get out again

A few tips

- Use a false name, but use your own first name.
- Consider using a surname that sounds like your own.
- Be a woman (preferably a foreign one)
- Flirt / use flattery
- Offer an incentive
- Get a job

Secrets of Success

- Balance of Power

- Time Travel – or how to be an effective liar

What can go wrong?

- You are recognised
- Balance of power backfires
- Overcompensate by giving too much detail
- Everything

BE PREPARED

How to prevent social engineering attacks

- Education & Awareness
- Social engineering testing
- Security policy
- Vet all your staff
- Don’t trust anyone!

Use of this Information

This presentation pack necessarily represents only part of the information which we considered in carrying out our work, being that which we considered to be most relevant to our understanding of your needs, in the light of this presentation.

The information in this presentation pack will have been supplemented by matters arising from any oral presentation by us, and should be considered in the light of this additional information.

If you require any further information or explanations of our underlying work, you should contact us.

The information in this presentation pack is confidential and contains proprietary information of Ernst & Young. It should not be provided to anyone other than the intended recipients without our written consent.

Anyone who receives a copy of this presentation pack other than in the context of our oral presentation of its contents should note the first two points above, and that we shall not have any responsibility to anyone other than our client in respect of the information contained in this document.

Questions

For more information, please contact:

Sharon Conheady	**Tony Ritlop**	**David Dunn**
Technology & Security Risk Services	Technology & Security Risk Services	Technology & Security Risk Services
Ernst & Young UK	Ernst & Young Canada	Ernst & Young Canada
London	Montreal	Toronto
UK	Quebec	Ontario
Tel #: +44 (0)20 7951 8936	Tel #: 514.879.2679	Tel #: 416.943.2597
sconheady@uk.ey.com	tony.ritlop@ca.ey.com	david.dunn@ca.ey.com