Network Security

Epilogue, Social Engineering

Marcus Bendtsen, Andrei Gurtov

Institutionen för Datavetenskap (IDA)

Avdelningen för Databas- och Informationsteknik (ADIT)

People are people

The biggest threat to any security system…

Social Engineering

- Network security is not only about technology.

- Social engineering plays on the ignorance, **insecurities** and **fear** of people.
- The social engineer uses ***psychological techniques*** to trick others into doing things for them that they should not do.
- They exploit personal knowledge about the subject, systems, organisation, etc. that they want to attack.

- A good social engineer is a **friend** from the moment they start talking to you, they *make you feel good* … most of the time. When it does not work, they *make you feel scared*…

(Office phone rings)

Hi, this is Bob from support services. We show that there is a problem with your network. Are you having problems at the moment?

No, everything is fine

Just to make sure, could you log off and just log back on for me? Don't tell me your password.

Sure (Clickety click) everything's working

That's strange. I should have seen something when you did that. Could you try again please?

No problem (clickety click) Still working

Odd. Oh well, thanks for your help

(Hangs up)

The social engineer could be using electronic surveillance to get keystrokes, could have planted a key-logger, or could simply be listening to what the user is typing (you can recover text fairly accurately from the sound of a keyboard).

(Phone rings in the middle of the night)

This is Tiny in corporate security. Why are you transferring confidential files from our systems?

What? I just woke up! What files?

Our logs show that you're transferring company confidential files from your account to a cracked FTP server in Bulgaria. You'll go to jail for this.

I've been sleeping! It has to be someone else! Can't you do something?

OK. Give me your account name and password. We need to sign on as you to track this one down.

It's kmc and password fred.

We'll be contacting you first thing in the morning. Don't tell anyone else about this until we track down the spy.

Plays on surprise and fear, and can be very successful.

Give up password for a cheap pen

- Infosec 2003 organizers:
    - Interviewed travellers in London Waterloo station.
    - 75% gave up password when asked; 15% more after a follow-up question.

    - Common passwords: “password”, name, age, birthdate, etc.

    - 2/3 had told their passwords to a co-worker
    - 3/4 knew a co-workers password
    - 2/3 used the same password for everything

Usability

- Underestimated part of security.
- Problem is that security is extremely complex, and asking users and developers to know about security may be to big a task.
- Just knowing about certificates seems to be a big problem, where users and developers accept certificates that are easily forged.
- Security products on offer are most likely to complex, built by engineers that do not ***appreciate that end-users are not experts***.

USB Threats

- **Half of people plug in USB drives they find in the parking lot**
- Researchers from Google, the University of Illinois Urbana-Champaign, and the University of Michigan, spread 297 USB sticks around the Urbana-Champaign campus
- 48 percent of the drives were picked up and plugged into a computer, some within minutes of being dropped
- Just 16% of users bothered to scan the drives with anti-virus software before loading the files; 68% said they took no precautions
- 68% of the users said they were only accessing the drive in order to find its owner

Summary of Network security

Network security

- Network security starts with good network design:
  - Segmentation
  - Perimeter defence
  - Containment

- The main focus of network design is to reduce ***exposure***.
- Do so by segmenting your networks and defend these perimeters with firewalls.
- Firewalls are not an excuse for bad security elsewhere.

- ***Wireless*** carries with it concerns that need to be taken seriously, even by those who decide on wired networks (rouge access points).

Network security

- Securing communications is important to make sure that you have:
  - Confidentiality
  - Integrity
  - Authentication
  - Typical techniques include TLS/SSL and IPSec.

- There are examples of protocols that are not designed with *security awareness* (ICMP, DNS, etc.)
- Scanning is a useful for both good and bad, and requires very good understanding of network protocols.
- IDS are critical, but require a lot of knowledge and consideration.
- Humans pose the biggest threat against security, not all security has to do with technology.

Literature

- **Important for exam**
- Slides
- D. Smith, “Improving Computer Security through Network Design”.
- Matta Security Limited, “An introduction to Internet Attack and Penetration”.
- Ptacek and Newsham, “Insertion Evasion and Denial of Service: Eluding Network Intrusion Detection”.
- IPSec and SSL/TLS (There is an RFC and book chapters). *Focus on learning what I presented on the slides*.

- **Less important for exam**
- Security Flaws in 802.11 Data Link Protocols
- DNSSEC
- *IDN whitepaper*

- **Not important for exam**
- DNS Cache Poisoning – The Next Generation
- Remote OS detection via TCP/IP stack fingerprinting

Linköpings universitet

expanding reality

www.liu.se