“A Fool Gets Beaten Even ~~at Church~~” in Internet

Starting thoughts on security

Kaido Kikkas

Some thoughts for starters

- „The biggest security risk is always located between the keyboard and the chair“ - an IT maxim
- „It is not possible to create a foolproof machine, because fools are so clever“ - an Amish farmer to Howard Rheingold
- „The question is not IF a system gets compromised but WHEN.” - Kevin Mitnick
- „We are Samurai... the Keyboard Cowboys... and all those other people who have no idea what's going on are the cattle... Moooo.“ - The Plague @ Hackers

Broom at the door

- A custom still used in remote corners of the country (compare it to some modern insurance contract!)
- Sometimes, security makes weird twists – e.g. the nature of West Estonian islands has been rather well preserved “thanks” to Soviet occupation (border zone => no visitors allowed)
- Also seen in tech history (<== mindquake by Theobald?), data security included

Long time ago...

- ..., the situation was like described in “Hackers” by Steven Levy:
  - The original hacker community at MIT sensed the introduction of passwords not as a security measure but a violation of freedom
  - Reaction: recommended to use blanks (done by 1/5 of users)
  - Nowadays, we have a radically different situation (and even Richard Stallman endorses passwords...)

The grass was greener

- In times of old, computers were elitary – few people, high levels of education, practically no business involved
- In today's Western world, even a homeless person can own a computer (see https://thehomelessguy.wordpress.com/)
- Result: on the one hand, used by everyone, supports the development of society, on the other hand,
  - Weird kinds of business
  - Many bad guys
  - Even more well-equipped fools

“Password? What for?”

- MS-DOS and early Windowses were single-user systems with no native networking (Unix was a 'network native' but was mostly accessible for experts only)
- Win 95 made things much worse by introducing a primitive password system that protected nothing and could be bypassed by pressing Esc
- When NT and 2000 came with actual password protection, the mindset of average users was already busted
- Results visible even now (XP, Vista, 7, 8 – 10 is even worse due to mandatory MS account for login)

Why Windows?

- Microsoft refers to the largest market share
- Somewhat true – but much more important is the largest share of clueless users (by far). Bugs can be bad, but often they are even not needed
- Educating users might become a priority compared even to patching the systems
- Jarno Niemelä of F-Secure: “There is no patch for stupidity”

Karl Marx and Freddie Mercury

- WTF...? What are those dudes doing HERE?
  - Marx: “Unity and struggle of opposites”
  - Mercury: “I can't live with you, I can't live without you....”
- Point: a large problem is that data security is a big business with conflicting interests. **Would McAfee or Symantec rejoice if one day there was no malware in the whole world?**

Malware industry

- The biggest perdition of 21st century IT: perverted business models allowing bad behaviour to be profitable
- A very wide area from nosy marketing (I know that you always visit fishing sites so I advertise you fishing rods and rubber boots) to direct crime (identity theft, scams)
- The main problem still not solved: how to cut the stimuli for creating malware?

...and security industry

- A Jewish story tells of two doctors, father and son:
  - “Dad, you worked on Mr Smith for seven years with no result, I cured him in two months!”
  - “Son, I used his money to pay for your education.”’
- From ancient times, people have paid for security. And it was understood that
  - Security means selling the safe feeling
  - To keep the job, it is wise to keep the dangers at bay but not eliminate them
  - Sometimes, playing the “good cop, bad cop” works best

Big Brother

- State interference is growing, especially in the “democratic” Western world. E.g.:
  - Carnivore packet sniffer
  - FBI Magic Lantern keylogger
- Sometimes the Brother orders the industry not to mess with him – e.g. an antivirus must ignore a “virus-like” program
- A growing problem

...and his nasty henchmen

- Politically motivated breaches of security and privacy (East)
- Economically motivated breaches by “public” entities that are actually businesses – e.g. BSA, MPAA, RIAA (West)

Early pranks

- 1969 – Joe Engressia uses free calls by whistling
- 1971 – John “Cap'n Crunch” Draper, 2600Hz. Later builds the first blue box
- Young Kevin Mitnick (his books, e.g. *The Art of Deception*, are strongly recommended!):
  - Bus hack
  - Fooling the payphone with coin sound
- Main motive: slightly misguided curiosity and independence

Milestone: 1994

- Preceded by the Stanley Mark Rifkin case in 1976 – not actually a ‘computer crime’ but social engineering on wire transfer
- First spam in Usenet
- Vladimir Levin vs Citibank – 10M USD
- Kevin Mitnick caught with about 20 000 credit card numbers
- Opening the Net to business shows its dark side

Some common things

- Used in variations for a long time
- Skilful use of human weaknesses
- Adapt much faster than related legislation

Spam

- In 1978, Greg Thuerk sends a DEC event advertisement to about 600 users of ARPAnet
- In 1991, bad guys get up first
- In heyday, about 200 bln spam messages per day, 75-90% of all traffic
- In 2014, about 54 bln and 57% of traffic
- Medicines and complements, sex stuff, fake diplomas...
- The biggest problem: it is inexpensive (~0,00001 cents)
- Earlier ruled by the US, China and Russia, recently added Western Europe and Spanish-speaking countries

Phishing

- Interception of important information (passwords, card numbers)
- Beginning: AOL in the 90-s
- Went to the masses with the advent of social media
- From blatant stupidity to “one size fits all” to dangerous, well-targetted and manipulative spear-phishing
  - A fresh case (March 21) from Estonia: https://tech2.org/latvia/congolese-businessman-is-detained-for-fraud/

Fraud

- Classic example: the Nigerian advance free fraud (“need to smuggle out 30 mln, you will get 10%, but first I need 1200$ to grease some palms”)
- Especially nasty are the ones making use of real-life disasters
    - Some examples: http://www.fraud-magazine.com/article.aspx?id=4294967697

Simple manipulations

- “cheap offer, no delivery” or “too good to be true”
- Later, had to wander due to harassment by owners of larger online environments
- Typical goods: small but expensive items (watches, jewelry)
- Usually combined with spam

Car scams

- Examples include
  - Offering an expensive car cheap, asking for some money “for transfer costs”
  - Using a fake cheque on a larger sum, asking to return the difference
  - Offering a real car, but where from?

Dating scams

- Most social (kinda)
- A “future spouse” is asked for “some money for travel”
- Can include various manipulations, in worse cases involving the “spouse” in some criminal scheme

Techie stuff

- Direct hijacking using security holes
- Malware – classic viruses are replaced by worms
- Ransomware, e.g. CryptoLocker
- XSS (*Cross-Site Scripting*)
- DNS attacks (*pharming*)
- Fake names and homoglyph attacks

Main stages of online manipulation

- Gather as much information as possible on the mark, using innocent-looking inquiries
- Use the gathered information to play an insider, getting access to much more important information
- Use the information as you see fit

No tech

- Can also be physical:
  - **Shoulder surfing** – at terminal, code locks etc
  - **Tailgating** – to pass doors following an authorized person
  - **Dumpster diving** – to find carelessly discarded information
- Read more: *No Tech Hacking* by Johnny Long

Example 1: Martin the Auditor

- Mrs Jones, the bookkeeper of the department, receives a call from a „Martin Mint from the internal audit team“. Martin asks some questions:
  - How many employees does the department have?
  - How many of them have university degrees?
  - How often is training offered in the department?
  - What is the account number for staff costs?
  - How many employees have left during the year?
  - How is the general working atmosphere in the department?
- What is wrong here…?

Example 2: A Really Helpful Helpdesk

- Needed: a cell phone with calling card
- 1. call to Mr Smith the bookkeeper – posing as a helpdesk, asking about any problems and leaving your number. Somewhere in chat, ask for the network socket number too
- 2. call to main IT office – posing as a technician on call to Mr Smith's office, asking to switch number X socket off for repairs
- 3. Wait until Mr Smith (now offline) panics and calls that helpful guy who called him earlier

...

- 4. In an hour, the problem is solved – after calling back to the IT office and asking to reconnect socket X
- 5. „To avoid it in future“ ask Mr Smith to run a program (does not do anything visible)
- Mission complete: a sniffer/rootkit/trojan is in place
- (get rid of the phone too)

Example 3: turn the tables!

- A new sport: scambaiting (aka mugu-baiting)
- Main idea: answer to some “Dr Jones” scam letter, play a stupid white guy (inventing yourself a hilarious name like Gerald Womo Milton Glockenspiel gives style points) and try to get the “entrepreneur” to do various creative things
- The top players have received money by themselves or sent the scammer to meet in New York (alone, of course)
- Examples: whatsthebloodypoint.com, scamorama.com, 419eater.com (Warning: do not read with full bladder!)

Nigeria?

- Some factors:
- Long history of instability and corruption (rich country under unstable government, including military rule)
- Poverty and inequality still widespread – 80% of oil revenue goes to 1% of population (according to CIA Factbook)
- Large country, many tribes with old feuds
- English as *lingua franca* (about 250 local languages)
- Literacy at about 70% (various sources differ), decent overall education
- Pretty good tech infrastructure
- The scamming tradition predates Internet

Sleuth 2.0

- Most web-based social networks are actually networks of trust (people on the friend list are 'homies')
- TMI!
- Most manipulations start with establishment of trust – a social network can do a lot of initial work 'off the shelf'!
- Integrated services are a problem!
- The Gazzag.com case in 2006

Countermeasures?

- Legal steps, more flexible legislation
- Well-defined policies
- Technical awareness, esp. among 'ordinary users'
- Guerrilla measures (NB! Ethically – and sometimes legally – a grey zone!)
- ...

Some words on social media

- Make use of internal defense measures
- If possible, do not use integrated services to login (e.g. Google)
- Do not recycle passwords
- Learn some about common risks and attack types
- Create a personal security policy (what can be put up, what cannot)

Ye olde King sayest

- .."Security comes from technology, trainng and policy”
  - – Kevin Mitnick, security advisor (!)
  - see also *The Art of Deception*
- Technology: networks, firewalls, antiviruses...
- Training: awareness of different attacks
- Policy: set procedures and requirements
- https://www.sans.org/reading_room/whitepapers/engineering/a_multilevel_defense_against_social_engineering_920.

To sum it up

- The dark side of today's IT is a nasty coctail of widespread networks, poor and slow legislation, unethical business practices and human stupidity
- The main cure: learn and teach!

Thanks