Security: It's Everyone's Business!

Keith Yorkston

Abstract Security isn't only a bit of software that can be bought, installed and forgotten with the occasional upgrade thrown in. Security isn't only that set of password rules we are supposed to follow. Security isn't only that locked filing cabinet, or a guard and a scan card reader at the front door. It includes all those things, and many, many more. We all need to think about security differently. Every organisation has thousands of vulnerabilities—weaknesses that could be exploited by a malicious attacker. And, as a malicious attacker, I only need to find one vulnerability to exploit. It could be a helpful staff member holding the door open for a "fellow smoker", or a person in Finance who believed that last phone call asking them to process "that important invoice". It might be an open comms port on the production web server, or the unpatched server in the test environment. Or it could be the report listing last week's customer contacts that is mailed to the sales staff each Monday (including the sales staff who have left the organisation). I mention these because my colleagues and I have used all these techniques (and many more) to test organisations. We are security testers.

Keywords Software security · Software quality · Security testing · Security tester

1 Introduction

Your organisation has been hacked. Think for a minute—who might have instigated this attack? What type of person springs into your mind?

Did you have an image of a darkened room, with a faint green glow showing empty energy drink cans and a young, angry guy furiously pounding a keyboard? Did you imagine a vast room full of people in the strange uniforms of a totalitarian

K. Yorkston
Expleo Group, London, UK

S. Goericke (ed.), *The Future of Software Quality Assurance*,
https://doi.org/10.1007/978-3-030-29509-7_19

regime? Both could be true. Or did you think of that strange phone call that a colleague answered yesterday? Or the last invoice of the thirty that Finance processed in their last payment run? Or the guy who just took your secure waste "for disposal"? Or did you think of a workmate who always attaches a USB drive to machines at work and takes it home with them each afternoon? Or the office worker who printed an extra copy of the confidential report to pop into the outgoing mail?

Security isn't only a bit of software that can be bought, installed and forgotten with the occasional upgrade thrown in. Security isn't only that set of password rules we are supposed to follow. Security isn't only that locked filing cabinet, or a guard and a scan card reader at the front door. It includes all those things, and many, many more. We all need to think about security differently. Every organisation has thousands of vulnerabilities—weaknesses that could be exploited by a malicious attacker. And, as a malicious attacker, I only need to find one vulnerability to exploit. It could be a helpful staff member holding the door open for a "fellow smoker", or a person in Finance who believed that last phone call asking them to process "that important invoice". It might be an open comms port on the production web server, or the unpatched server in the test environment. Or it could be the report listing last week's customer contacts that is mailed to the sales staff each Monday (including the sales staff who have left the organisation). I mention these because my colleagues and I have used all these techniques (and many more) to test organisations. We are security testers.

But wait, you say. Don't testers sit at a desk in an office and write and run tests against software? Yes we do. But we also dress up as delivery drivers or people in the waste disposal industry, or wear suits after making fake company passes. What good is a fake badge? You say it won't open the security gates in reception?

You're right—on its own it won't. It would take about 10 min to create a fake ID card, as they all tend to have a photo, name and company logo on them (check your badge—am I right?) I have visited organisations and walked into reception purely to see the ID card design. Have a slightly confused look, map in hand, "Could you please tell me how to get to [any address nearby]?"

Or just wait for staff filing out at lunchtime. Then, into Microsoft Paint (yes, the big budget hacking tool), print out onto paper, and with some sticky-back plastic over an old card, I now have a freshly made organisation ID card. Of course, it won't pass close scrutiny, but when was the last time anyone checked an ID card? It gets a glance at best. Next trick, how to get through the gate?

Carry something. Literally, a big armful of paper/books/boxes/whatever. As you approach the gate (and the guard casually glances at your freshly made card) you ask, "Could you please open the barrier for me? I'm late for a meeting . . . "

And the organisation has been hacked.

2 Training Security Testers

This example is a security test. Security testing needs to consider what is known as the "iron triangle" of:

- Technology
- Processes
- People

The testing we do is not, and should never be, limited to technology alone. Many people today still think you can "buy security", or that security is limited to a technical solution. Hackers use computers, we will be hacked, therefore hackers attacking the organisation will use computers.

But consider the example above. The only technology involved was a programme first released in 1985. This hack relied on people vulnerability—the guard wanting to be helpful. It showed a weakness in the process—I didn't scan my card (the process) because the guard scanned their own card in trying to be helpful. How could this be stopped? Could the organisation hire meaner guards? Think on this for a second . . .

A number of things could be suggested. The process could be changed, but unless it is enforced, incidents like this could continue to happen. Awareness is key—if the guards know that someone might try this, they can be aware of the situation. We have all heard of the "mystery shopper"—what we need is a "mystery hacker". Or in other words, a security tester. The organisation must train the guards and staff to recognise social engineering—the science of skilfully manoeuvring people to take some desired action. Why would a guard open the gate for me? Because I presented a situation to them that appealed to their good manners. You know, those things your parents told you, "Wash your hands, say please, and *hold the door open for others* . . . " (I was also told to add "Clean up your room!"—thanks for proof-reading, Dad).

But this training should never stop at the staff in reception. Upper management also need to not only sponsor initiatives on security, they themselves need to participate in security training. They are a huge, visible target—it's easier to find details of an organisation's CEO than the name of a person in Accounts Payable. Look at the organisation's annual report, or your country's company register (Companies House in the UK). Then, using sites like Google or LinkedIn, look them up. Even going further, using a data mining tool such as Maltego can uncover a malicious user's treasure trove of publicly available information. Much has been written about spear phishing—targeting an individual for a specific phishing attack. It's vitally important for senior staff to understand the threats posed against the organisation and the possible vulnerabilities that could be targeted. But only not in general terms, the specific attacks focussed on just them.

Business email compromise (BEC) has, for a number of years, relied on a simple fact:

No one questions the Boss!

In 2018, the US FBI estimated global losses between October 2013 and May 2018 from *this attack alone* cost organisations US$12.5 billion.[1] This attack uses spear phishing. Find out details of the senior staff, then send an email to accountspayable@[insert organisation name]. Spoof it to come from that senior staff member, with a message like "An invoice is coming from Acme Corp, can you please process this payment quickly, as it is part of Project Merlin". It's especially useful if the attacker knows a project name within the organisation, but it's also surprising how many "Project Merlins" actually happen. Then, a call comes through to the general organisation phone number—"Can I please speak to Accounts Payable?"

The call is put through, and it's Tom Jefferson[2] from Acme Corp, asking about the invoice. He seems such a nice chap, and is very apologetic about the rush for payment. He's also very helpful, giving Acme Corp's bank details to the Accounts Payable staff. The call adds legitimacy to the spoofed email, and that $12 billion loss just got a bit bigger.

Once again, there are most probably processes that should be followed by staff. The senior staff member's email was spoofed. And, the account staff were convinced to be helpful to solve a problem by the email "from the Boss", and the call they received.

But, says you, don't we know the account the money was paid to? Surely if this information was passed to the Local Constabulary, they could stake out the bank branch, looking for the suspicious individual who, while wearing sunglasses and a false moustache, withdraws the money from the account? Perhaps, but another aspect of the attack is another vulnerable victim. A lonely person who struck up a conversation with a social media connection, and due to [an unexpected tax bill/a sick relative/a windfall from a recently departed relative] they require a bank account in the target's country. And, if the target opens this account on the basis that "Afta this is dun, I cn get my viza to meat my luv", the attacker now has an account that bears a striking resemblance to the Acme account number (so close, in fact, it's the same). Or the attacker might identify a like-minded person in that country who opens the account for a percentage of the money passing through it. And the consequence? Maybe a possibly innocent (or not so innocent) person could be charged with money laundering. And the hunt goes on for the money.

And the most targeted business sector for BEC? Which do you think? Sometimes the target can be unexpected. You must think like an attacker. With the prevalence and reliance on online services today, we can do almost anything online. Including finalising the purchase of property. The real estate sector is a lucrative area targeted by the attackers. Think of all those involved in purchasing a home—solicitors, surveyors, real estate agents, buyers and sellers. How many of these could be vulnerable? If you're buying a home and get a mail for the final purchase from the "real estate" giving the account details for the transfer. Or from the "solicitor"

[1] https://www.ic3.gov/media/2018/180712.aspx

[2] No relation to the third President of the United States.

stating there's a problem which will require a small fee to clear up. Or the real estate receives a mail from a "buyer" to list a property. Were I to turn to the "Dark Side", I would get a greater return attacking the local florist than I would attacking Amazon. The reason? Amazon spend a large amount of money hiring some of the world's experts in security, implementing top-line technology and robust processes to reduce vulnerabilities. The local florist/solicitor/real estate/surveyor cannot.

3 Reasons for (Cyber) Attacks

Why would people conduct these attacks? As mentioned previously, these attacks can obtain a large amount of money quite quickly. Years ago, motivation for the attackers was covered with MICE:

- *Money*—this is very much the motivation in the case of BEC. Money can be a multi-faceted motivator. I once was "called by Microsoft" to have the person on the call tell me about the "viruses" on my machine. After showing a little empathy ("You're job must be very difficult . . . ") and expressing how this call was a waste of time, they opened up to me, telling me they knew they were doing wrong, but it's a job to feed their family (or, were they trying to socially engineer me?). But they also felt safe, in that the chances of being caught were much less than getting fired for not "making enough successful calls". Some people can make a lot of money from malicious attacks,[3] while others do it to "pay the bills".
- *Ideology*—as before, ideology can encompass a vast array of views. This motivation could be a lone person who lost their business "to the bank", a small group supporting animal rights, or a large group with a particular secular belief. And, based on this motivation, the targets will be different. Then, there's the morally ambiguous groups of hackers, whose ideology can shift. And sometimes even this can be muddied—I enjoy when occasionally people attending demonstrations against capitalism/global corporate domination ,etc. wear the white Guy Fawkes mask from the movie *V for Vendetta*. You know, that trade-marked thing owned by Warner Brothers[4] . . .
- *Compromise*—you may have received the latest phishing mail floating around the world, a version of which I received is below:

```
Hello!
I'm a member of an international hacker
group.
As you could probably have guessed, your ac-
```

[3] "Black-hat sextortionists required: Competitive salary and dental plan"—listed on https://www.theregister.co.uk/2019/02/21/black_hats_sextortion_275k_salaries_helpers/

[4] "The irony of the Anonymous mask" listed on https://www.theguardian.com/technology/2011/aug/30/irony-of-anonymous-mask

```
count [email removed] was hacked, because I
sent message you from it.
Now I have access to you accounts!
For example, your password for [email re-
moved] is [password removed]
Within a period from July 7, 2018 to Septem-
ber 23, 2018, you were infected by the virus
we've created, through an adult website
you've visited.
So far, we have access to your messages, so-
cial media accounts, and messengers.
Moreover, we've gotten full damps of these
data.
We are aware of your little and big se-
crets...yeah, you do have them. We saw and
recorded your doings on porn websites. Your
tastes are so weird, you know..
But the key thing is that sometimes we rec-
orded you with your webcam, syncing the re-
cordings with what you watched!
I think you are not interested show this
video to your friends, relatives, and your
intimate one...
Transfer $700 to our Bitcoin wallet:
[Bitcoin wallet removed]
If you don't know about Bitcoin please input
in Google "buy BTC". It's really easy.
I guarantee that after that, we'll erase all
your "data" :D
A timer will start once you read this mes-
sage. You have 48 hours to pay the above-
mentioned amount.
```

I wonder if the author had a competitive salary and dental plan? Compromise allows the attackers to control the situation. I have something you don't want released (your photos from your phone/compromising browsing history/bank account details) and for some consideration (cash/a confidential report from your organisation) the problem *might* go away.

Ego—sometimes, the urge to be "the smartest person in the room" can take over. It could be childhood dreams (such as reading of the exploits of Kevin Mitnick or Kevin Poulsen, both security experts arrested for hacking) and imagining "If only . . . ", or it could be the need to, like many conspiracy theorists, be the only person "who knows the truth".

Some of the tools the attacker will use are fear, greed and even empathy. Chris Hadnagy and Michelle Fincher wrote the book *Phishing Dark Waters* [1] where they took an in-depth study of phishing. An attacker can use fear, such as the example above, or the alert from "your bank" saying your account has been hacked, and you should click the link below to "verify your password". They can use greed—the Spanish prisoner/Nigerian 419 scam—where the victim is asked to "please make a small payment/give me access to your account to release the

millions held offshore, for a substantial fee". And the most insidious is empathy—my grandmother/mother/child/cute puppy is dying, and I need money to save them (photo attached). All these attack the person—and our technology and processes must be in place to combat these.

4 What Security Testers Need to Understand

Let's be clear. We have looked at elements of criminal offenses. All the attacks mentioned above are crimes in the UK according to the Fraud Act and Computer Misuse Act amongst others. These crimes fall into two categories—cyber dependant (hacking an online account, where without IT, the crime wouldn't exist) and cyber-enabled (where the number of victims of a criminal act can be increased—an organisation I worked for used to receive snail-mail letters from "Nigerian Princes").

This is something that is absolutely vital for a security tester to understand. You might be running a legitimate test within your organisation, but unless you have documented permission from a person of relevant authority, you could be charged and even found guilty of an offence. Remember, a malicious user might be an employee of the organisation. If you do not have specific permission, how do we know that your test isn't an actual attempt at malicious harm? Something as benign as clearing your browser cache could be interpreted by authorities in the USA as destroying evidence. Any work conducted as a security tester must be covered by legal indemnity—the basis for which is supplied by the Open Web Application Security Project (OWASP).[5] If you have ever played Monopoly, this is the security tester's "Get Out of Jail Free" card. Literally. It provides evidence that the work security testers are undertaking IS AUTHORISED, and isn't cover for an internal malicious user.

As said, even if you are testing your own organisation's systems, you absolutely need this permission. Never let someone else (e.g. a hypothetical project manager) convince you this is not required. If this isn't in place, you are breaking the law, and could be subject to prosecution.

Another interesting threat that has grown since 2014 is a method called "account stuffing". Let's say a hypothetical user has multiple online accounts. The user cannot remember unique passwords for all the accounts, and uses the same password for a number of accounts. Now, let's say they have the same password for both the local florist AND their Amazon account. So, if I steal the local florist usernames and passwords (remember, their security policy might not be best practice), I could now access many more accounts with that credential set.

What's more disturbing is the marketplace for stolen credentials has been "automated". Stolen credentials are fed into an automated process checking these against sites like Amazon, PayPal or E-bay (amongst others). A successfully stolen and checked account can then be sold to interested parties for between $0.50 USD

[5] https://www.owasp.org/index.php/Authorization_form

and $3.50 USD, with the potential for the purchaser to make up to 20 times the cost price.[6] This is why we are continuously told not to replicate passwords over multiple sites. Account stuffing relies on a people-based weakness, we cannot remember long, complex, unique passwords, so we cheat! And inadvertently, create a vulnerability.

5 About Password Security

Passwords demonstrate the battle between security and usability. A long, complex password might be good for an organisation's security, but if security procedures become onerous in the view of users, they will find a way of subverting or avoiding them. The procedure thus becomes ineffective. Consider the following password rules (which might look familiar to many) and the subsequent passwords:

1. Must be a minimum 8 characters (12345678)
2. Must contain at least 1 upper and 1 lower case character (Qwertyui)
3. Must contain at least 1 number (Qwertyu1)
4. Must contain at least 1 special character (Qwerty1!)
5. must be changed every 30 days (Qwerty2")

These listed passwords would take at most minutes to break for tools like John the Ripper or Hashcat. Various lists exist of the "Top 25" passwords used—all of which vary slightly due to the data on which they draw, but contain many of the same passwords (and yes, "password" is in there!) But they point to a common theme—that is when we think we are being "random", we aren't. There is a reason why "qwertyuiop" isn't a good password—look at the top row of keys on a keyboard. Humans follow patterns, and those patterns can be predicted and replicated.

An interesting point is during the infamous Sony email hack relating to the release of the movie *The Interview.* The then CEO of Sony, Michael Lynton, had a password of *Sonyml3.*[7] Any prizes for guessing what his next password might have been?

We need to forget passwords. Any password of eight characters is broken very quickly, and just because the MINIMUM is eight, it doesn't mean EXACTLY eight. And even if it cannot be broken in seconds, the attacker may not mind. They would have all the time they need to crack the password, as even when an alert goes out from the attacked site, how many people actually change THAT password, let alone all the other accounts using that same one. It should be noted that the encrypted password isn't decrypted, but a known word is encrypted to see if the encrypted result matches any passwords in the stolen set. The longer the password, the exponentially more combinations could be used to create a password. And, it

[6]"The Economy of Credential Stuffing Attacks" listed on https://www.recordedfuture.com/credential-stuffing-attacks/

[7]https://twitter.com/kevinmitnick/status/545432732096946176?lang=en

doesn't need to be complex, only long. The password *dhr*$_*$*Qdfe* is much less secure than *dog* . . . , let alone a much longer *sausagedog* . . . !

6 Use Passphrases Instead of Passwords

The comedian John Oliver interviewed Edward Snowden[8] and the topic of passwords came up. We should forget about passwords, and think passphrases. Rules we can follow are:

1. Still use the mix of characters (upper/lower/numbers/special characters)
2. Use a combination of unrelated words
3. Use words from different languages—a mix is best
4. Do not rely on leetspeak/133t5p3@k alone (where letters are replaced by similar shaped numbers/special characters)
5. Do not rely on one rule alone!

As an example, let's base a passphrase on that favourite fermented curd—cheese. In using a combination of the rules above, my passphrase could be *Ch3ese&Kase&Farmaajo*. After all, who could forget cheese! At 20 characters, that would give the password crackers a run for their money.

Or, think song lyrics. Something like *4!We!Are!Young!And!Free.*[9] Even harder to crack, at 23 characters. Each character exponentially increases the number of combinations, so longer is better. Although, *MargretThatcherIs110%Sexy* still takes the prize for sheer creativeness.

What we need is time. If a breech is detected, we need time to ensure word gets out to those affected by the breech. So timely notification is key from the organisations who become the victims of attack. The longer the passphrase is, the longer it takes to crack.

We could go even further, and use a password manager. These tools will allow a secure container into which your credentials and passphrases can be stored. They are useful, in that they can allow secure passphrases to be auto-generated, stored, and most importantly made unique for every separate site or system accessed. Some also come with wallets to store payment information, and can work both in desktop and mobile environments. Both commercial and opensource tools are available.

The downsides of these tools can be:

- What password/phrase do you have to access this tool? If it's weak, it would reduce the usefulness of the tool.
- What security is built into this tool itself? Could the encryption it uses be an older, compromised version?

[8] https://www.youtube.com/watch?v=yzGzB-yYKcc—please watch this video—in 3 min you will know how simple passphrase security can be.

[9] The second line of the Australian national anthem.

7 About Usernames

But passphrases are only half the battle. What about usernames? How many people have a common username (usually an email address) across many different websites? It's interesting, in that often we are asked to input our email address for access to a catalogue or whitepaper. Or "Join for free" to receive great discounts. Or join with your Google or Facebook account. This can spread your information far and wide. And, if one of those sites you fed your details into is attacked, and your user credentials stolen, the impact could be much wider. Now, your email could go into that list of addresses targeted for attackers to use in phishing attacks. Some methods to avoid this include using a short-term mail service like 10minutemail.com[10] for those sites that mail a link to the download you're after, or having multiple mail accounts (Gmail/Hotmail/etc.) to use for various site logins.

8 Conclusions

Am I being paranoid? My kids abound in their father's alleged paranoia, extending to my son's custom-made tinfoil hats, or my wife asking why we need multiple broadband accounts. But, as Philip K Dick[11] once said, "Strange how paranoia can link up with reality now and then . . . ".

Once an attack has been made, and data lost, there is the aftermath. The embarrassment for those who fell for the attack, and the looks they now get from colleagues around the office. Another danger present is a phenomenon called "Monday's Expert". After an event, everyone sees the mistakes that were made when pointed out. Think about that sports programme where each week the panel look at the weekend's games. Of course that player was offside/onside/committing a foul/not committing a foul/over the line/short of the line. It's blatant when we are shown the multitude of slow motion high-definition camera views, complete with added computer graphics. How did the referee miss that? We can, from a security point-of-view, fall victim to "it could never happen to me", as we roll our eyes and say knowingly to colleagues beside the water cooler "How could they ever let that happen?"

But, play the event back at regular speed. Would you make the right/same/a different decision? We must appreciate that when faced with a decision, people always have the option of choosing the right/wrong/sub-optimal/a different outcome. They may not have enough information or knowledge of the background situation, and yet are asked to make that decision RIGHT NOW. That is where training can help.

[10] https://10minutemail.com/10MinuteMail/index.html

[11] American science fiction writer, whose books were the basis for such films as *Bladerunner*, *Minority Report*, *Total Recall* and *The Man in the High Castle*.

I'm not talking about turning every employee into a security expert—that will not be a practical (or cost-effective) solution.

The basic training that's required should allow the organisation's staff:

1. To summarise the need for security to protect technology/process/people
2. To relate the motivation of a malicious user to the organisation's assets
3. To recognise potential security vulnerabilities in the day-to-day tasks of their own job role
4. To follow security processes!

There should also be a small team of people within the organisation who do specialise in security. The training for this team would go much further—allowing this group to write, test/audit, and maintain the organisation's security to the required level. It's up to them to continuously test these procedures, and ensure the people using them not only understand the steps, but the reasons behind why the steps are necessary.

Earlier, I mentioned time. It takes time for an attacker look for vulnerabilities, and to exploit them once found. It is everyone's job in the organisation (and our job for our personal lives) to reduce the possible vulnerabilities. But they will always exist. There might be a determined attacker who, based on MICE, might want to attack your organisation, or even you personally. You cannot stop all attacks, but you can make the time and resources needed to expend in the attack to be too high a price for the attacker to pay. It's like a cryptic crossword—many people look at it and don't even attempt it. A smaller number start, and might even get part way through to completing it. But a few will be either determined enough to complete it (but it takes a long time) or both determined and clever enough to do it quickly. Although these people are to be feared, they are not invincible. But, luckily, they are few in number, and the methods of defeating them are growing. But so are the methods they can use to attack. Security is a subject that if you are standing still, you are moving backwards faster than you would realise. Your aim is to make the resources needed to expend in the attack greater than the attacker is willing to put on the table. We must do this through reducing vulnerabilities contained within our organisation's technology, our processes, and, most importantly, our people.

Finally, let's hope it's not a nation state that wants your stuff. This attacker has a potentially unlimited set of resources—if they want your stuff, they will get it. The only way to stay safe is to switch off all internet connected devices, destroy them, then go and live in a cave. Putting on tinfoil hat now . . .

Reference

1. Hadnagy, C., Fincher, M.: Phishing Dark Waters. Wiley, Hoboken, NJ (2015)