Linus Fulton

Task 1A: Browsers and Banking Security

- What does the “Not Secure” warning mean in the first picture and what risks does visiting site with the warning pose?

“Not Secure” means that the website you’re connecting to isn’t using HTTPS (HyperText Transfer Protocol Secure). Instead, you are using HTTP, an insecure version of the protocol. This version sends data over plaintext, making it readable if intercepted by an attacker (man-in-the-middle)

- Why does the second site show up as “trusted” to the browser?

The site is using HTTPS. This means any traffic between you and the website is encrypted, so only you two can unencrypted that traffic. You always have to check however, if the URL you’re visiting is the correct one. It’s possible for an attacker to set up a fake (but similar looking) website URL and secure that with HTTPS. Your data will be encrypted, but the website itself (and the attacker behind it) can still read your information.

- What other ways are there to detect a phishing/scam site?
  - Are there any tools available online?

There are a couple of ways to detect scam sites. The first is by double-checking the URL you entered. A fake URL will often look similar but with small differences (ex: facebook.com to facebo0k.com). Of course, you should also check if the site has a HTTPS connection in the first place. Once you’re on the site, any obvious misspellings or grammar mistakes can point to a fake website. Sometimes, some browsers also automatically warn the user if they enter a fake website. A combination of all the methods should make you pretty safe. Websites like “Web of Trust” can also help protect you by warning you of common scam sites.

- What is typosquatting and how does it relate to the pictures?
  - What is UDRP and how does it help with combatting typosquatting?
  - If you were to own the domain ouspg.org and would be running your crypto banking application around bank.ouspg.org, what domains could you monitor for warning signing of possible phishing attempts against your customers?

Typosquatting is a type of attack in which small misspellings of the URL are used to trick users into entering the wrong website (see the facebo0k example above). If the real URL is “danksebank.io", an attacker might set up “danksebank.fi", in hopes of tricking an unsuspecting user. UDRP is a legal system in which a website owner can challenge other domain name registrations which are confusingly similar to their own URL. If i owned “ouspg.org" and “bank.ouspg.org", I would monitor other similar URLS (bank-ouspg.org or ouspgbank.org), common misspellings (bank.osupg.org) and URLS with swapped characters (bank.0usog.org).

Task 2: Cards and Payments

- Why do modern payment cars use and chip and not a magnetic stripe?

Chip-based cared are more secure than magnetic stripe cards because the use dynamic data with each transaction. This makes them more difficult to clone or skim.

- What are EMV Certificates and why are they relevant for payment protection?

EMV certificates are used to authenticate transactions, making sure the card and the terminal are both legitimate. This prevents fraud by making sure the card is authentic during transactions-

- What attacks exist again payment cards?
  - Card-not-present?
  - Contactless payment?

Linus Fulton

Card-not-present attacks are the ones in which the card is not physically present during the transaction, such as during online shopping. Contactless payment includes attacks such as relay attacks. For these, attacks signal is intercepted between the card and the terminal.

- How is multi-factor authentication (MFA) used in banking?

MFA is used in banking to makes sure banking transactions are more secure. They combine something the user knows, such as a password or PIN, with something the user has (a phone) or are (biometrics such as fingerprints or face ID).

- How does multi-factor authentication increase payment security?

An attacker would need both access to your phone as well as knowledge of your password.

- What MFA methods are you using in your daily life?

The most common methods are SMS codes, e-mail codes, authenticator apps, and biometric authentication. I use an app where possible (which is protected with face ID), and e-mail or SMS if it’s not available.

- What attacks exist against different forms of 2FA?
  - Time-based-one-time-password?
  - Text message?

The time-based form is vulnerable to phishing or man-in-the-middle attacks, where the attacker can intercept the code. SMS codes can be gained through SIM swapping, where an attacker gains access the the victims phone number and intercepts the SMS message when it arrives.

Task 3: Card Fraud

Card fraud is generally divided into two categories: card-present fraud (CP) and card-not-present fraud (CNP). Card-present fraud includes attacks in which the actual physical card is present, so for example card skimming or at a vulnerable payment terminal. Card-not-present fraud occurs mainly during online banking. Within the EU, domestic fraud is much less common (93% of transactions but only 47% of fraud), with cross-border fraud being much more common (5% of transactions with 27% of fraud.

Between 2008 and 2019, the amount of card-present fraud has decreased while card-not-present fraud rose. This can partially be attributed to the introduction of the EMV chip, which makes card-present fraud harder to pull off. At the same time, card-not-present fraud has become much more common, mainly due to the increase in online payments over the last 2 decades. Technologies like the EMV chip, but also 3D Secure protocols and the Revised Payment Service Directive have impacted the card fraud landscape.

From the late 2000s to late 2010s, the number of card transactions, and specifically the number of online transactions has greatly risen. Despite many technological advancements, it is still the most vulnerable area for card fraud. Cross-border transactions in particular have a higher chance of being fraudulent.

The internet and e-commerce have made card-not-present fraud much more common.

Data breaches are used by attackers to collect sensitive data such as credit card numbers and other personal details. This allows them to make fraudulent transactions, specifically in the card-not-present space. The process of tokenisation is the process of replacing some card information with the unique identifier. By making sure that sensitive data is not exposed during a transaction, it makes the overall payment industry much more safe.

Linus Fulton