Exercise: Risk & Trust

ACME Water are working with Bournemouth University Cyber Security Unit (BUCSU) to improve the security of some of its business customers.

BUCSU is a consultancy practice that is part of Bournemouth University, primarily targeting SMEs in the Bournemouth & Poole areas. They will expand their website by providing a free online vulnerability test for SMEs. The service will identify IT security issues that place many SMEs at risk. SMEs using this service may then wish to receive guidance from BUCSU consultants on how to mitigate these risks.

ACME Water have asked you to provide advice on the site's design from a trust perspective, and identify any potential risks associated with potential idea.

Questions

1. How might potential customers assess the trustworthiness of the site?

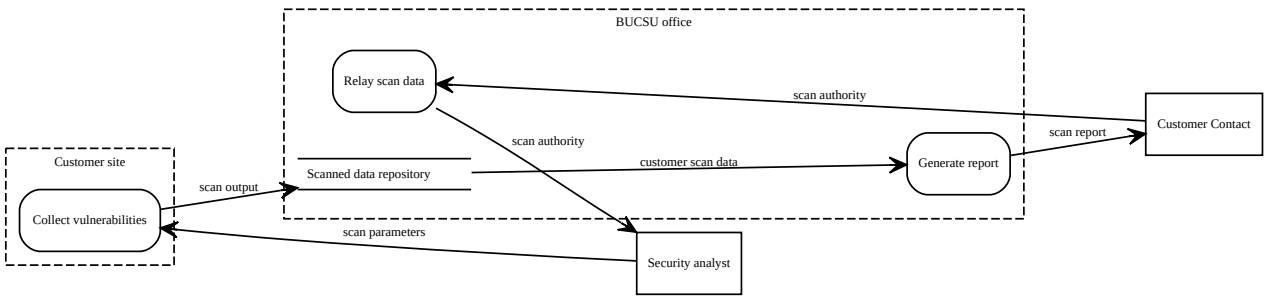
1. Website layout. Is this site similar to other legitimate websites they know?
2. Logos and certifications. Do they check and understand them? What are 'CREST academic partner' and 'Cyber Essentials' really signalling? Being a CREST academic partners says nothing about the service being offered, although the link to Cyber Essentials might help potential consumers see the point of such scans.
3. Do potential customers believe they can find feedback on BUCSU's past behaviour, e.g. by relevant forums or social media. Are there incentives for contributing reputation information?
4. Inclusion of charity names, or other public organisations (e.g. the police) - exploits benevolence.
5. Amount of information given – scammers would not take the time to put all that information in the site.
6. Company information – scammers would not share that much information on who they are.
7. Who sanctions BUCSU if things go wrong?

<u>Other comments</u>

To support 'Temporal Embeddedness' it might be useful to use a more stable identity than just taking the company name. This necessitates taking further information before scanning takes place. By doing so both the truster and trustee (BUCSU) will appreciate the potential for future interactions.

2. Model the data flows between SME and the relevant BUCSU systems. You should note trust boundaries, and any possible threats and vulnerability associated with these data flows.

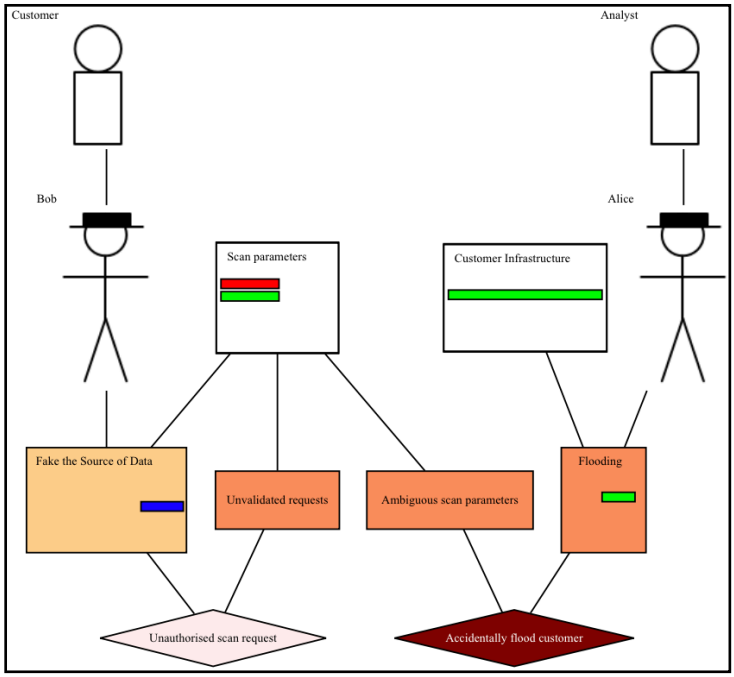
Here is one permutation of a DFD based on the brief.



There are clearly trust boundaries between the Customer and BUCSU office. If you think the scan parameters are held elsewhere, there might be a trust boundary encompassing the 'Relay scan data' process too. Note that the entities are not within any trust boundaries; as these are 'external' actors, we have no control over them.

3. Specify TWO risks based on one of the data flows modelled? You should specify the threat and vulnerability underpinning each risk, the assets underpinning each risk, and provide some indication of the risk's validity.

There are a slew of possible vulnerabilities and threats associated with this DFD. These can be considered on an element-by-element basis, but looking at the flows crossing trust boundaries is a good place to start as there are all sorts of spoofing, tampering, and non-repudiation threats associated with these - particularly based on your interpretation of the entities!



One possible risk is an 'unauthorised scan request', i.e. the person making the request doesn't have the authority to carry out there scan, or this scan doesn't actually come from the customer. This is effectively spoofing the 'scan authority' data flow between the Customer Contact entity and the Relay scan data process. The threat (False source of data) has been drawn from CAPEC-151, and the vulnerability (Unvalidated requests) is drawn from the assumption that scan requests are received via email without any form of verification of the sender's identity.

Another potential risk - 'Accidentally flood customer' results from the denial of service on the scan parameters data flow between the Security analyst entity and the Collect vulnerabilities process. The threat (Flooding) is again drawn from CAPEC [CAPEC-125], but the vulnerability is based on a security analyst (Alice) who is unintentionally carrying out the threat due to ambiguous scan parameters.