Trust & Security

The department Trust & Security within SURF is responsible for both operations and innovation for Trust & Identity and Security domains. We are running the identity federation SURFconext for Dutch Research & Education, incident response team SURFcert, the DNS and mailfilter infrastructure for SURF and its members, as well as a number of other services.

Within the team there is a lot of expertise on basic internet technology (like DNS(SEC), mail), identity management and identity federations (single sign-on, SAML, OpenId Connect, etc), cryptography, information security, compliance and privacy.

If you're interested in an assignment, internship and/or stage, please get in touch with us. Preferably, send us an email stating which assignment you would like to do, and what makes you fit for the job! You'll find the main contact person for each assignment in the table below. If you think you have a great idea of your own and it seems to fit with subjects on this page, please get into contact with Joost Gadellaa (Security) or Michiel Schok (Identity) and we will assess if we can accommodate your assignment.

Many of these assignments can be approached either practical or from a more scientific perspective, to suit your assignment's requirements.

Student assignments

Title	Duration	Contact	Description	Study direction
Make MFA mandatory for SURFconext IdPs	1 - 3 months	Thijs Kinkhorst	SURFconext is the Dutch national research and education federation, which allows students, teachers, employees and researchers to use their institutional account for logging in to hundreds of online services. On a yearly basis, SURFconext processes more than 250 million logins. Institutions (universities, schools) are Identity Providers to SURFconext and connect their login system (Entra ID, ADFS, NetIQ, SimpleSAML...) to enable login by their users to these services. There are several options to enable MFA for specific SURFconext connected services. However, the default for logins to SURFconext is still first factor only. We want to investigate if it's achievable to require all 150 institutions to enable (some form of) MFA (possibly with SSO) to protect each SURFconext login. Talk with institutions about their ideas about this proposal, what are the hard cases, what could be proposed solutions so we can change the default to be secure?	
Strong authentication: RADIUS, SAML 2.0 and SURFsecureID	3 months	Pieter van der Meulen	SURFsecureID is the SURF service that adds second factor authentication to the authentication provided by SURFconext. SURFsecureID and SURFconext authentication uses the SAML 2.0 web-SSO protocol, which is a web based protocol. This means that authentication requires the presense of a web browser. We want to enable as much as applications as possible to use the (second factor) authentication of SURFsecureID. Previous efforts resulted in adding "second factor only" (SFO) authentication to SURFsecureID and developing a multi-factor-authentication (MFA) extension for Microsoft AD FS. As a next step we want you to research and build a proof-of-concept for adding a RADIUS server to SURFsecureID. RADIUS is typically used by VPN services and other remote access services. Adding a RADIUS server to SURFsecureID means creating some sort of bridge between the web based SAML 2.0 world and the decidedly non-web server-to-server authentication workd of RADIUS. A solution could be building a website where a user can login using their web-based two-factor authentication provided by SURFsecureID where you could get a ont-time-password (OTP) to authenticate using the RADIUS client. The idea is simple, but leads to many questions for you to research. E.g. - How do the applications that SURFsecureID customers want to use, use RADIUS? - What is the security of the solution? How resistant is it against e.g. phising - How to make the solutions as user friendly as possible - Can we optimise the user experience for common second factor types that are used in SURFsecureID, like Tiqr, to completely/partly skip the web based part of the solution? SURFsecureID is uses the opensource software OpenConext-Stepup.	

Zichtbaarheid	3 months	Wim Biemolt	SURFcert is voor de zichtbaarheid van incidenten grootdeels afhankelijk van "betrouwbare bronnen". Bijvoorbeeld een sinkhole waar naartoe een besmet systeem verbinding maakt. Waarschijnlijk missen we door deze wijze wel de nodige incidenten. Het zou mooi zijn als we daar enig inzicht in kunnen krijgen. Door het maken van een vergelijking van een besmet systeem versus de meldingen die daarvoor binnen komen. Is er via die weg een beeld te krijgen wat we zoal kunnen missen en zijn er alternatieven om ook de gemiste incidenten bij SURFcert op de radar te krijgen.	
Federated Appstore	3-6 months	Arnout Terpstra	SURFconext is the Dutch national research and education federation, which allows students, teachers, employees and researchers to use their institutional account for logging in to hundreds of online services. On a yearly basis, SURFconext processes more than 100 million logins. Worldwide, eduGAIN interconnects 66 federations with more than 3000 Identity Providers and 2600 services. A (big) problem for eduGAIN and its federations isthe discoverability of services. Both end-users and Identity Provider administrators are often unable to find services that might be of interest for them. For one, this is because there is no single point where these services can be found in a user-friendly manner. There is a technical interface, however, the services' metadata is often out of date: contact information, service descriptions, logos, etc. Due to the sheer amount of services, it is impossible for SURF to keep this information up to date. It would be better if the Service Providers themselves supply this information and regularly update this. However, the incentive to do so is currently missing. To (artificially) create such an incentive, we can borrow ideas from Apple and Google, who've demontrated how to run a succesful Appstore. Wouldn't it be nice to have something like that for federations as well? But how should we build it? What should it look like? Would it actually work? For this assignment, there is plenty of room for students with different backgrounds. If you have any ideas, do not hesitate to contact us and inquire about the possibilities!	
Honest design for privacy	3-6 months	Arnout Terpstra	Privacy is a very hot and relevant topic. Increasingly our lives are supported by digital technologies, and the number of sensors in those technologies keeps on growing. This generates a lot of data, in which companies and governments are very interested, as it an be used to predict us and our behaviour. Looking at how eager people are to use new technologies and make their lives a little bit more convenient, one could conclude people do not care about privacy at all. This is absolutely not the case. People *do* care, but they often feel powerless to do something about it or they are simply not aware of the consequences of certain technologies. Did you know Amazon's "smart" speaker Alexa is constantly recording everything that is being said and sends it to servers in the US? Most people have no clue. We can solve this by designing products and interfaces which cause "friction": deliberately do something unexpected. What if Alexa would start talking to you by itself, for instance asking you how your workday was (since it probably knows when you work, where you work, etc.)? Are you a creative designer with an above average interest in privacy? This assignment is perfect for you.	
Real time SURFconext login analysis	3-6 months	Bart Geesink	SURFconext is our federated authentication service. It is implemented as a central hub, performing more than 100M authentications a year. At busy times, 20 logins a second are handled by the proxy. More than 1000 services are connected to around 200 Identity Providers. Real time logs are available of all authentications passing through. For this assignment, we'd like you to develop a tool to perform real time analysis of the logins, in order to detect anomalies. The login patterns are very predictable, which makes this project suitable to use machine learning techniques to predict the login statistics. Some of the public statistics can be found here.	
Mapping and Integration of Information Security and Privacy Maturity Models with SURFaudit Frameworks	3-6 months	Abdul Altawekji	This project emphasizes the theoretical exploration and understanding of relevant information security and privacy maturity models. The key objective is to analyze and document existing models these maturity-based models, while focusing on integrating such models with SURFaudit assessment frameworks for information security and privacy. By doing so, we aim to cohesively integrate these models with our existing assessment frameworks. Understanding the intersections, gaps, and potential improvements within these frameworks are among the primary goals of this work. The research will provide insights into the current standards, best practices, and potential enhancements for our assessment frameworks, ensuring a robust, updated, and holistic approach to information security and privacy for the education and research sectors.	

Code Vulnerability Analysis and Strengthening of the SURFdomains Backend API-Server and design	3-6 months	Abdul Altawekji	In light of the ongoing development of a new codebase and the redesigned structure for SURFdomains, this project is geared towards a hands-on approach. This project seeks to employ various code analysis methods to identify potential vulnerabilities within the new codebase. One could think of using static and dynamic testing, as well as various fuzzing techniques to name a few techniques. The objective is to assess, challenge, and "break" the code to its limits, with the ultimate goal of reinforcing the robustness of our backend API-server. As a possible complementary pursuit, an exploration into the new architecture of SURFdomains from a security standpoint can be undertaken.	
Development and Enhancement of the DNS-Firewall for SURFdomains	3-6 months	Abdul Altawekji	The DNS firewall (also known as protected DNS or pDNS) project is intended as an extension of SURFdomains and embodies a collaborative and development-oriented approach. Its aim is to engage in setting up a DNS-firewall similar to that of SWITCH: https://www.switch.ch/dns-firewall/ As well as collecting additional data from various sources to optimize its operation. As we move forward, a collaboration with SWITCH in September 2023 will guide and shape this initiative. This project provides an opportunity to understand the intricacies of DNS-based security measures and contribute to strengthening the cyber defence mechanisms of SURFdomains.	
Management of Cyber Risks in the context of Organizations with Decentralized IT in	3-6 months	Joost Gadellaa	One specific challenge when assessing and mitigating cyber risks in large institutions, is dealing with decentral IT departments. The direct motivation for this research is the case of Faculties and Institutes within Universities in the Netherlands. Historically, these have done most of their IT themselves, but this can cause challenges when dealing with IT security and when the organization wants to make progress in gaining more control of their security risks. It can be very beneficial to have part of the IT organization close to the end-users, but what implications does it have for cybersecurity risks? Possible research questions include: • What are the characteristics of decentral IT departments in Dutch higher education? • What kind of security challenges emerge because of this decentralization? • What are possible technical ways to deal with these challenges? • What organisational/governance solutions can be found? • What processes does an organization need to think about in order to profit from decentral IT?	
Usability of Mobile Device Management solutions for Organizational Information Security	3-6 months	Joost Gadellaa	With the rise of remote work and BYOD, mobile devices such as phones, tablets and laptops used for work have become an inherent part of organization’s IT landscape. They are vital tools for productivity and availability. However, these devices often access sensitive organization data, and they can be a serious threat to security if hacked, stolen or lost. There are many technical measures already known to combat these security threats, known as ‘Mobile Device Management’ (MDM). They take a certain level of control over (private or organization) devices to ensure security. Although the technical possibilities and solutions are well-understood, there seems to be a gap between the technical and the user perception. Employees often misunderstand what these solutions do, why it is important, contributing to resistance and non-compliance. This project aims to better understand experience of employees with and their perception of MDM solutions, with the goal of identifying ways to improve: • MDM tools and configuration • Risk communication around these issues and MDM solutions • User acceptance and adoption of them	
Cybersecurity dialoog (NL only)	3-6 months	Nicole van Deursen	Dialoog over risico’s tussen cybersecurity experts en hun hiërarchisch meerderen (directeuren, decanen en bestuurders) is soms lastig. Dit geldt ook voor gesprekken van cybersecurity experts met experts in andere veiligheidsdomeinen (fysieke veiligheid, kennisveiligheid, sociale veiligheid etc.). Ze spreken elkaars taal niet goed en hebben niet altijd begrip voor de beslissingen van de ander. Er zijn diverse bronnen te vinden die dialoogvragen voorstellen om die gesprekken te stimuleren. Maar hoe pas je die vragen toe in een gespek? En zijn deze dialogen effectief? Leiden ze tot verhoging van wederzijds begrip en verbeterde relaties? Ontwikkel een spelvorm of een workshop waarmee gesprekken over cybersecurity tussen integrale veiligheidsdisciplines en tussen hiërarchische lagen kan worden gefaciliteerd. Hierbij kan gebruik worden gemaakt van bestaande bronnen met dialoogvragen. Meet het effect van de dialoog op de deelnemers.	Interaction design, multimedia design, human factors, communication, security studies

Cybersecurity atlas	3-6 months	Nicole van Deursen	The famous Dutch: De Bosatlas van de Veiligheid (https://view.publitas.com/noordhoff-atlassen-and-additionals/bladertool-bosatlas-van-de-veiligheid/page/1) visualizes a variety of safety and security information. Is it feasible to create a book of safety & security maps for the education sector? Create 5 maps of relevant safety & security topics in higher eduction in The Netherlands. Topcis may include cybersecurity, internet safety, cybercrime, physical security and so on. Generic data is available from public sources such as https://basisbeveiliging.nl/#/maps, https://www.cbs.nl/nl-nl/publicatie/2023/31/cybersecuritymonitor-2022, https://www.risicokaart.nl and so on. We also have specific data at SURF. The challenge is to relate such data to the geographical locations, demographics, and environment of universities, hbo's and mbo's in The Netherlands. Find and relate data, tell the story and visualise it in maps!	data science, information science, Geographical Information Systems, social geography
Toolwheel for (SaaS) applications	3-6 months	Joost Gadellaa	Educational institutions have developed various tool guides to help users navigate online tools responsibly, outlining recommended tools, potential risks, and official alternatives. This project aims to assess the effectiveness of these guides and explore the possibility of a centralized approach through an organization like SURF. Depending on student background, the project could have a design, product or technical focus. Both practical and academic approaches ar possible, although the latter would include design science to get to something tangiable. By the end of the study, we aim to offer practical recommendations for educational institutions to enhance their tool guides, potentially through a centralized approach or even have a prototype of a tool that leverages collective knowledge.	
Open Source tooling for Attack Surface Monitoring	3-6 months	Joost Gadellaa	Within a number of our members there is a need to be facilitated in their efforts on Attack Surface Mapping. For many institutions, SURF runs the network, DNS ánd PKI infrastructure, putting us in an information position where we could help. A large number of tools, scans and frameworks exists online and can be used, but a shared approach could be beneficial. This project aims to look into existing tools, analyse user needs for this kind of tooling, and build a Proof of Concept or pilot closely integrated with other SURF services.	
DDoS mitigation	1, 3 or 6 months	Wim Biemolt	The network of SURF currently uses various techniques to protect the network and the connected institutions against various kinds of (DDoS) attacks. But as attacks and/or networks evolve we need to investigate different solutions. For a wide range of attacks.	

pingback:

- https://www.sos.cs.ru.nl/applications/master/main.html
- TODO: update https://rp.os3.nl/2021-2022/index.html