Proposta para Grupo de Trabalho

GT-AMPTo – Autenticação multi-fator para Todos

Programa de P&D em Serviços Avançados: Gestão de Identidade

Emerson Ribeiro de Mello

14 de março de 2017

1. Título

GT-AMPTo – Autenticação multi-fator para Todos

2. Coordenador

Emerson Ribeiro de Mello Instituto Federal
de Santa Catarina
http://lattes.cnpq.br/1478274711167428

3. Programa de P&D

Serviços Avançados: Gestão de Identidade

4. Resumo

A facilidade de autenticação única, presente nas implementações do modelo de gestão de identidade federada, trouxe benefícios no ponto de vista da usabilidade. Porém, também foram introduzidas novas vulnerabilidades, pois bastaria ao atacante descobrir um único par usuário e senha para ter acesso a todos os serviços da federação. O objetivo desse trabalho é desenvolver uma solução de autenticação com múltiplos fatores que possa ser implantada na federação CAFe, além de permitir a transposição dessa autenticação para a Internet física. Pretende-se combinar os dispositivos que o usuário carrega, como telefones e relógios inteligentes, com uma infraestrutura de Internet das Coisas (IoT). Como resultado, espera-se que os dispositivos que o usuário carrega possam ser usados como fatores extras de autenticação em serviços online e também como componente de autenticação para interação com a Internet das Coisas.

5. Abstract

The single sign-on feature included in federated identity frameworks has introduced usability benefits. However, a new set of vulnerabilities has also been introduced and if an attacker discovered the username/password pair he will be able to act on behalf of user and he will gain access to all federation services where the user is able to access. The main goal of this work is to develop a multi-factor authentication solution suitable to CAFe federation, as well as allowing the transposition of CAFe authentication to the Internet of Things. We intend to combine users devices, such as smartphone and smartwatch, with infrastructure of IoT. As a result, users' devices will act as an extra authentication factors to online services and also to physical components of IoT.

6. Parcerias

Executora principal

Instituto Federal de Santa Catarina – IFSC
Campus São José
Núcleo de Telecomunicações

Co-executora

Universidade do Vale do Itajaí – UNIVALI
Centro de Ciências Tecnológicas da Terra e do Mar
Mestrado em Computação Aplicada

Co-executora

Universidade Federal do Rio Grande do Norte Instituto
Metrópole Digital

7. Sumário

O modelo de gerenciamento de identidade federada (*Federated Identity Management* – FIM) apresentou uma solução para o problema da proliferação de credenciais de acesso. Nesse modelo, cada usuário só precisa gerenciar uma única credencial de acesso e essa o permite acessar diferentes provedores de serviço, desde que autorizado pelas políticas de controle de acesso de cada provedor de serviço.

Protocolos e *frameworks* de autenticação e autorização para FIM, como SAML 2.0 [Committee et al., 2012], OAuth2.0 [Hardt, 2012] e OpenId Connect[1] [Sakimura et al., 2014] são usados para permitir a troca de dados pessoais dos usuários entre provedores de identidade (*Identity Provider* – IdP) e provedores de serviços (*Service Provider* – SP). Essas soluções também oferecem a facilidade de autenticação única (*Single Sign-On* – SSO). Nesse caso, o usuário só precisa passar pelo processo de autenticação uma única vez, junto ao seu provedor de identidade, independente de quantos provedores de serviço ele for acessar.

Provedores de identidade são responsáveis por armazenar atributos de seus usuários e os provedores de serviço podem requisitar ao IdP atributos de um usuário que esteja pleiteando acesso aos seus serviços. Interfaces de consentimento do usuário, como o uApproveJP [Orawiwattanakul et al., 2010] do Shibboleth [Cantor, 2005] IdPv2 e Shibboleth IdPv3[2], são apresentadas como uma funcionalidade dos IdPs para dar ao real detentor dos atributos, no caso o usuário, o poder de decisão sobre o compartilhamento de seus atributos com os provedores de serviço. Ou seja, assume-se que o usuário é o único capaz de decidir quais dados pessoais seriam compartilhados e com quem.

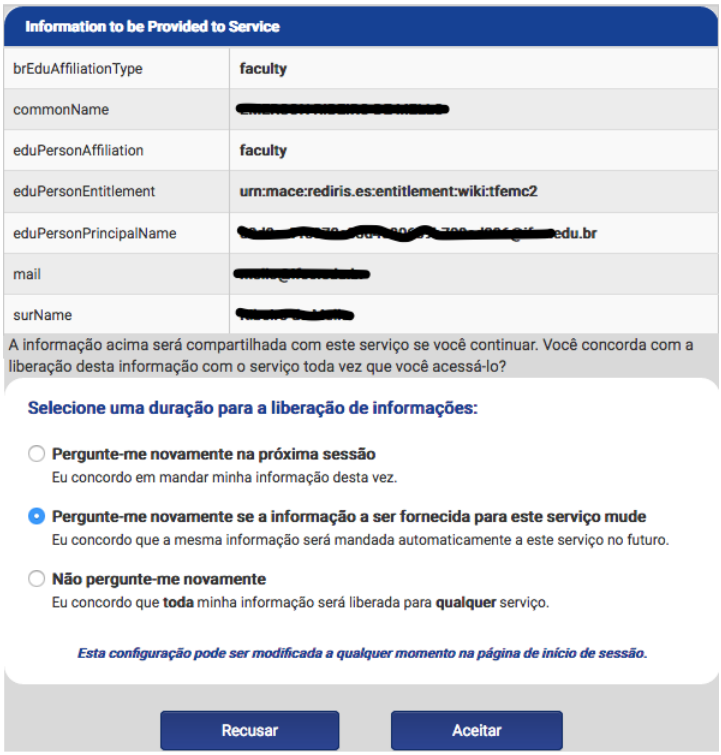

Figura 1: Interface de consentimento de usuário – provedor de identidade CAFe com Shibboleth IdPv3

Na Figura 1 é apresentada a interface de consentimento de usuário de um provedor de identidade Shibboleth IdPv3 da Comunidade Acadêmica Federada (CAFe) da RNP. Essa interface é apresentada ao usuário logo após

[1] Embora o OAuth2.0 seja um *framework* para autorização, o OpenId Connect faz uso do OAuth2.0 para prover uma solução para autenticação.

[2] https://wiki.shibboleth.net/confluence/display/IDP30/ConsentConfiguration

esse passar pelo processo de autenticação e antes dele ter acesso ao serviço oferecido pelo provedor de serviços.

Atualmente, credenciais de acesso baseadas no par nome de usuário/senha são as mais comuns usadas pelos mecanismos de autenticação. Sabe-se que essa solução possui diversas fragilidades, como por exemplo usuário escolher senhas fáceis, e suscetível a diversos ataques, como por exemplo *phishing*[3].

Credenciais de acesso são geralmente classificadas nas seguintes categorias: aquilo que você sabe – como as senhas; aquilo que você possui – como um cartão inteligente; aquilo que você é – como a biometria do usuário; e em [Brainard et al., 2006] é apresentada "alguém que você conhece" – relações humanas para intermediar a autenticação de um usuário.

Para cada uma dessas categorias, tem-se vantagens e desvantagens que podem impedir o usuário correto de ter acesso ao recurso. Por exemplo, as senhas podem ser esquecidas assim como um cartão inteligente. A biometria não pode ser esquecida, mas pode ficar indisponível temporariamente, como a falta de voz, impressão digital apagada devido a um trabalho manual, etc. Além disso, apesar da biometria apresentar maior disponibilidade, seu uso como único fator de autenticação não é considerado seguro, tendo em vista que as características de uma pessoa, apesar de serem únicas, são públicas, o que torna fácil a sua captura sem que o pessoa percebesse [Brainard et al., 2006].

A autenticação multi-fator, as vezes chamada de autenticação com dois fatores (*two factor authentication*) surge como uma solução para aumentar a robustez dos processos de autenticação e, geralmente, combina fatores das diferentes categorias apresentadas anteriormente, ou poderiam ainda combinar dois ou mais fatores de uma mesma categoria, como é o caso das senhas descartáveis (*One Time Password* – OTP) [Haller et al., 1998]. Nesse caso, parte-se do pressuposto que um atacante conseguiria comprometer um desses fatores, porém o grau dificuldade aumentaria muito se fosse necessário comprometer dois ou mais fatores.

Atualmente, diversos provedores de serviços públicos (e.g. Google, Github, Dropbox, etc.) na Internet oferecem formas de autenticação com múltiplos fatores. Há ainda algumas iniciativas específicas para o framework Shibboleth (usado na Federação CAFe), na academia [da Silva and de Mello, 2015], na indústria[4] e alguns projetos de código aberto[5]. O *Research and Education FEDerations group* (REFEDS) está com uma consulta pública até o final de março de 2017 para construção do documento *Multi-Factor Authentication (MFA) Profile Recommendation*[6], o qual especificará como o contexto de autenticação multi-fator deverá ser expresso nas asserções SAML e utilizado por provedores de identidade e provedores de serviços.

Em [Weiser, 1991], foi apresentada a visão de um mundo no qual a computação do século 21 seria móvel e onipresente. Pode-se concluir que isso tornou-se realidade principalmente por causa dos telefones inteligentes (*smartphones*), que levaram a computação para o ambiente do usuário, ou seja, para o seu dia-a-dia. Deste modo, os *smartphones* se tornaram um dos candidatos a dispositivo de suporte a autenticação multi-fator, como de fato já é usado por soluções comerciais, seja para recebimento de mensagens de texto (SMS) ou para executar algum aplicativo que permita o uso de senhas descartáveis [NIST, 2016].

Outra vertente para confirmar a visão de Weiser está na Internet das Coisas (*Internet of Things* – IoT) e na computação ubíqua. Com a IoT as coisas ao redor das pessoas além de estarem disponíveis através da Internet, podem também colaborar entre si para oferecer serviços ou informações para as pessoas de acordo com o contexto e localização das mesmas [Atzori et al., 2010]. Por exemplo, um termostato inteligente pode observar a rotina de chegada e saída das pessoas em uma residência, bem como suas preferências de temperatura, e ajustar automaticamente a temperatura visando gerar economia, diminuindo a potência ou mesmo desligando o condicionador de ar, quando as pessoas estão fora e ligar instantes antes das pessoas chegaram, podendo aqui comunicar com os *smartphones*. Segundo [Saha and Mukherjee, 2003], a

[3] Atacante poderia induzir o usuário correto fornecer suas credenciais de acesso em uma página *web* maliciosa.

[4] https://duo.com/docs/shibboleth

[5] https://github.com/Ratler/shibboleth-mfa-u2f-auth

[6] https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+MFA+Profile

computação ubíqua requer que suas aplicações se integrem com o ambiente do usuário de tal forma que passem despercebidas. A escalabilidade, integração, heterogeneidade e invisibilidade são os principais desafios na construção deste tipo de aplicação, que se relacionam fortemente com a IoT.

A IoT apresenta requisitos singulares que demandam abordagens diferenciadas acerca da segurança [Atzori et al., 2010], sendo a gestão de identidade de usuários e dispositivos uma destas. Em ambientes federados, a autenticação para dispositivos da IoT ainda é um problema em aberto.

7.1. Problematização e Justificativa

A Internet hoje é mais inclusiva que a Internet da década de 90 e os usuários fazem uso de uma diversidade maior de dispositivos para acessá-la, estando os telefones inteligentes em grande evidência. Diariamente pessoas com diferentes níveis de habilidades com informática usam a Internet para consumir conteúdo digital, fazer compras, compartilhar informações em redes sociais, etc. Para esse tipo de público, que inclui até mesmo estudantes e funcionários de instituições de ensino usuárias da federação CAFe, interações complexas com sítios web, como redirecionamentos HTTP entre provedor de identidade e provedor de serviço, podem ser suficientes para fazer com essas pessoas compartilhem mais dados pessoais do que deveriam ou mesmo fornecer dados pessoais em sítios maliciosos.

Apesar do modelo de gestão federada apresentar a facilidade de um único nome de usuário e senha para acessar todos os serviços da federação, usuários da federação também possuem contas em serviços externos a ela. Por exemplo, contas em serviços de e-mail, de compartilhamento de arquivos, redes sociais, etc. Dessa forma, usuários poderiam fazer uso de uma estratégia leiga e nada ideal, onde fariam uso da mesma senha para todos os serviços, estratégia essa também definida como "*Poor man SSO*" em [Arias et al., 2014].

Atualmente, a federação CAFe está fundamentada sobre o *framework* Shibboleth e a maioria dos provedores de identidade estão na versão 3 (Shibboleth IdPv3). As orientações gerais da RNP para as instituições participantes da CAFe indicam a necessidade do uso da interface de consentimento do usuário (Veja Figura 1), porém, não indicam a obrigatoriedade do uso de múltiplos fatores para autenticação. Apesar da RNP ter iniciado o piloto para emissão de certificados digitais para pessoas com a ICPEdu[7], esses certificados não são usados pelos provedores de identidade como um fator de autenticação para seus usuários. Na prática, usuários da CAFe fazem uso dos seus pares usuário/senha no processo de autenticação em seus IdPs para assim solicitar ao provedor de serviço da ICPEdu a emissão de certificado digital para pessoa.

De acordo com [Schaar, 2010], é essencial projetar sistemas destinados a processar dados pessoais considerando a privacidade por padrão (*Privacy by Design*). Sistemas precisam criar mecanismos para proteger dados pessoais e dar poder aos usuários para que esses possam indicar como seus dados serão processados ou compartilhados. Contudo, a atual interface de consentimento do usuário no Shibboleth IdPv3, usado pela CAFe (Veja Figura 1) , assume que o usuário é plenamente capaz de entender os termos técnicos ali expostos e as implicações da decisão a ser tomada. Nesse caso, o usuário não tem de fato o poder de decidir, pois a única alternativa é aceitar ou ele será impedido de acessar o serviço desejado. O usuário também não tem a opção de consentir parcialmente a lista de atributos solicitados.

Dessa forma, para usuários leigos, tais interfaces de consentimento do usuário podem ser entendidas com um passo extra e sem sentido entre eles e o recurso desejado. Então para esse tipo de usuário o comportamento padrão ao ver tal interface é aceitar sem ao menos ler o que está sendo apresentado ou mesmo escolher a opção: "*Não me pergunte novamente e eu concordo que meus dados pessoais sejam compartilhados com qualquer serviço da federação*"[8].

[7] https://www.rnp.br/servicos/servicos-avancados/icpedu/certificado-pessoa-icpedu [8]Texto presente na atual interface dos IdPs da CAFe.

A gestão de identidades federadas de usuários é um tema quem vem sendo bem discutido na literatura, entretanto, a gestão de identidades federadas de dispositivos não é bem caracterizada e, segundo [Miorandi et al., 2012], há um grande desafio de pesquisa neste cenário. A autenticação de objetos e de usuários em uma mesma infraestrutura federada, como por exemplo, uma federação baseada no framework Shibboleth não é tratada na literatura.

Com base na contextualização apresentada é possível formular as seguintes questões de pesquisa e desafios a serem tratados por essa proposta de grupo de trabalho:

1. Como aumentar a robustez do processo de autenticação dos usuários na CAFe sem que isso tenha um grande impacto na usabilidade?
2. Como a CAFe poderia ser moldada para oferecer uma melhor experiência de uso em dispositivos móveis, como os telefones inteligentes?
3. Como melhorar as interfaces de consentimento do usuário de forma que protejam a privacidade do usuário, de forma que o usuário não precise conhecer termos técnicos ou relacionados a privacidade?
4. Como os certificados digitais de pessoa da ICPEdu poderiam ser usados como mais um fator de autenticação dos provedores de identidade?
5. Como dispositivos poderiam usufruir dos provedores de identidade da CAFe para permitir a autenticação usuário-dispositivo e dispositivo-dispositivo?

7.2. Objetivos

O objetivo geral desta proposta é desenvolver uma solução que permita aos provedores de identidade da CAFe operarem com múltiplos fatores de autenticação, tratar da privacidade dos dados de seus usuários de forma implícita e transpor a autenticação para dispositivos físicos da Internet das Coisas. Com a solução proposta, espera-se que usuários da CAFe possam usufruir da autenticação com múltiplos fatores, usando seus dispositivos pessoais ou mesmo contas pessoais em provedores de serviços comerciais e que essa autenticação na CAFe possa ajudá-los a passar por mecanismos de controle de acesso físico para ter acesso a ambientes, como prédios, laboratórios, etc.

Essa proposta apresenta os seguintes objetivos específicos:

1. Analisar especificações, soluções e implementações de múltiplos fatores de autenticação que possam ser empregados nos principais protocolos e *frameworks* que implementam o modelo de gestão de identidade federada, o que inclui Shibboleth e OAuth2.0;
2. Analisar especificações, soluções e implementações de interfaces de consentimento de usuário dos principais protocolos e *frameworks* que implementam o modelo de gestão de identidade federada, o que inclui Shibboleth e OAuth2.0;
3. Analisar especificações, soluções e implementações que permitiriam aos dispositivos da Internet das Coisas usufruir dos benefícios do modelo de gestão de identidade federada, além de contribuir para o processo de autenticação de seus usuários;
4. Desenvolver uma solução para provedores de identidade da CAFe para possibilitar a autenticação com múltiplos fatores, bem como a gestão de todo o ciclo de vida desses fatores extras, como a emissão, renovação e revogação, podendo aqui ser aproveitado o conhecimento prévio desse grupo de pesquisa [da Silva and de Mello, 2015];
5. Demonstrar a solução desenvolvida no contexto de um estudo de caso que permitiria aos dispositivos da Internet das Coisas usufruir dos benefícios da CAFe para o fornecimento de soluções de autenticação e autorização para ambientes físicos, podendo aqui ser aproveitado a experiência prévia desse grupo de pesquisa [de Mello, 2017a, de Mello, 2017b, de Mello, 2017c], onde foram combinados

criptografia de chave pública, padrão FIDO UAF [Machani et al., 2014] e *smartphones* como fatores de autenticação.

A solução a ser proposta terá como base os seguintes componentes de *software* e *hardware*:

- **Autenticação com múltiplos fatores e controle de acesso à ambientes físicos**
  - **Software:** Shibboleth IdPv3; FreeOTP[8], aplicativo para o sistema operacional Android que possibilita o uso de senhas descartáveis baseadas nas especificações OATH/TOTP [M'Raihi et al., 2011] e OATH/HTOP [M'Raihi et al., 2005]; Dummy UAF Client [de Mello, 2017a], aplicativo para Android que implementa um cliente da especificação FIDO UAF [Machani et al., 2014]; FIDO UAF Demo Server[9] que implementa o servidor da especificação FIDO UAF.
  - **Hardware:** Para os dispositivos móveis, como telefones e relógios inteligentes: leitores biométricos para capturar impressão digital, voz e face; interfaces de comunicação como NFC, BLE e WiFi. Para dispositivos na Internet das Coisas pretende-se aproveitar as interfaces de comunicação como NFC, BLE e WiFi.
- **Interface de consentimento do usuário**
  - **Software:** Códigos do Shibboleth IdPv3 e Shibboleth SP.

Não foi encontrado na literatura, bem como em repositórios de projetos de código aberto, soluções que possibilitem o que está sendo proposto neste projeto. Dessa forma, entende-se que o trabalho a ser desenvolvidopode ser considerado como um aprimoramento da infraestrutura de autenticação e autorização usada como base pela Comunidade Acadêmica Federada (CAFe) e por outras federações acadêmicas baseadas no *framework* Shibboleth. A proposta ainda permitirá demonstrar um possível uso para os certificados pessoais ICPEdu e o desenvolvimento de uma solução de controle de acesso físico compatível com as tecnologias da CAFe.

8. Duração do projeto e marcos

	1			2			3			4		
	1	2	3	4	5	6	7	8	9	10	11	12
	05/17	06/17	07/17	08/17	09/17	10/17	11/17	12/17	01/18	02/18	03/18	04/18
Estado da arte		**M1**		**M3**								
Proposta do protótipo		**M2**			**M4**							
Desenvolvimento do protótipo						**M5**				**M7**		
Avaliação do protótipo									**M6**			
Documentação e divulgação dos resultados			**RA1**			**RA2**			**RA3**			**M8**

Tabela 1: Cronograma de atividades

Abaixo é apresentado o detalhamento dos marcos do projeto citados na Tabela 1:

[8] https://freeotp.github.io

[9] https://github.com/emersonmello/UAF

- **M1:** Versão inicial do Relatório Técnico 1 (RT1) com a revisão bibliográfica sobre interfaces de consentimento de usuário, autenticação com múltiplos fatores e autenticação e autorização no contexto da Internet das Coisas;
- **M2:** Versão inicial do Relatório Técnico 2 (RT2) indicando uma proposta de arquitetura para o protótipo a ser desenvolvido, bem com os componentes de software e hardware que serão usados;
- **M3:** Versão final do Relatório Técnico 1 (RT1) sobre a revisão da literatura.
- **M4:** Versão final do Relatório Técnico 2 (RT2) indicando a arquitetura escolhida para o desenvolvimento do protótipo;
- **M5:** Implementação inicial e funcional do protótipo a ser desenvolvido;
- **M6:** Entrega do plano de testes, bem como os resultados dos testes executados;
- **M7:** Entrega do protótipo finalizado;
- **M8:** Entrega da versão final da documentação técnica, manual de instalação e uso e apresentação dos resultados gerados. Também terá como entrega o último Relatório de Atividades (RA4).

A atividade **Documentação e divulgação dos resultados**, apresentada na Tabela 1, terá entregas parciais respeitando o edital da RNP. Ou seja, ao final de cada pacote de trabalho será entregue um relatório de acompanhamento (RA1, RA2, RA3 e RA4).

9. Recursos financeiros

9.1. Equipamentos e software

Descrição	Qtde	Valor unitário	Total
Telefone inteligente com Android 6 ou superior com NFC e leitor de impressão digital compatível com Google Imprint	2	R$ 2.500,00	R$ 5.000,00
Relógio inteligente com Android Wear 2.0 ou superior com BLE, NFC e WiFi	2	R$ 2.000,00	R$ 4.000,00
Raspberry Pi 3 Premium Kit	3	R$ 500,00	R$ 1.500,00
PN532 Adafruit NFC/RFID Controller Shield	3	R$ 300,00	R$ 900,00
Leitor de cartão NFC/RFID ACR122U USB	3	R$ 300,00	R$ 900,00
Kit com 02 breadbord, capacitor, resistor, transistor, led, jumpers para breadboard	3	R$ 150,00	R$ 450,00
Estimote Long Range Location Beacons – Dev Kit (3 unidades por kit)	3	R$ 700,00	R$ 2.100,00
Notebook 14” - especificação padrão RNP	2	R$ 4.087,00	R$ 8.174,00
Total			R$ 23.024,00

10. Ambiente para testes do protótipo

Pretende-se fazer uso do laboratório de experimentação em gestão de identidade da RNP, o GidLab[10], para validar a parte do protótipo que depende das entidades e relações presentes em uma federação Shibboleth, bem como a integração com soluções como o OAuth2.0 e OpenId Connect. Contudo, parte do

[10] https://gidlab.rnp.br

desenvolvimento e experimentos serão realizados com os kits de prototipagem para IoT e computadores a serem adquiridos dentro do contexto dessa proposta.

Referências

[Arias et al., 2014] Arias, P., Cabarcos, F. A., Trapero, R., Díaz, D., and Sánchez, A. M. (2014). Blended identity: Pervasive idm for continuous authentication. *IEEE Security & Privacy Magazine*. [Atzori et al., 2010] Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15):2787–2805.

[Brainard et al., 2006] Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., and Yung, M. (2006). Fourthfactor authentication: somebody you know. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 168–178. ACM.

[Cantor, 2005] Cantor, S. (2005). *Shibboleth architecture: Protocols and Profiles*. Internet2.

[Committee et al., 2012] Committee, O. S. S. T. et al. (2012). Security assertion markup language (saml) 2.0.

[da Silva and de Mello, 2015] da Silva, S. N. and de Mello, E. R. (2015). O uso de um segundo fator e autenticação contínua em provedores de serviços críticos. Programa de gestão de identidade (PGID) da Rede Nacional de Ensino e Pesquisa (RNP).

[de Mello, 2017a] de Mello, E. R. (2017a). A dummy FIDO UAF Client suitable to conduct development tests on Android smartphones that are not FIDO Ready.

[de Mello, 2017b] de Mello, E. R. (2017b). A simple application to demonstrate how to use FIDO UAF protocol and NFC on physical access control (Door lock systems).

[de Mello, 2017c] de Mello, E. R. (2017c). Door lock NFC card reader for Raspberry PI - NFC, Android, RaspberryPI, Adafruit PN532.

[Haller et al., 1998] Haller, N., Metz, C., Nesser, P., and Straw, M. (1998). Rfc 2289: A one-time password system. Technical report, Technical report, IETF.

[Hardt, 2012] Hardt, D. (2012). The oauth 2.0 authorization framework. RFC 6749, RFC Editor. http://www.rfc-editor.org/rfc/rfc6749.txt.

[Machani et al., 2014] Machani, S., Philpott, R., Srinivas, S., Kemp, J., and Hodges, J. (2014). Fido uaf architectural overview. *FIDO Alliance, December*.

[Miorandi et al., 2012] Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497–1516.

[M'Raihi et al., 2005] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and Ranen, O. (2005). Rfc 4226: Hotp: An hmac-based one-time password algorithm. Technical report, Technical report, IETF.

[M'Raihi et al., 2011] M'Raihi, D., Machani, S., Pei, M., and Rydell, J. (2011). Rfc 6238-totp: Timebased one-time password algorithm. Technical report, Technical report, IETF.

[NIST, 2016] NIST (2016). Digital Authentication Guideline. *DRAFT NIST Special Publication 80063*. https://pages.nist.gov/800-63-3/sp800-63b.html.

[Orawiwattanakul et al., 2010] Orawiwattanakul, T., Yamaji, K., Nakamura, M., Kataoka, T., and Sonehara, N. (2010). User-controlled privacy protection with attribute-filter mechanism for a federated sso environment using shibboleth. In *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2010 International Conference on*, pages 243–249. IEEE.

[Saha and Mukherjee, 2003] Saha, D. and Mukherjee, A. (2003). Pervasive computing: a paradigm for the 21st century. *Computer*, 36(3):25–31.

[Sakimura et al., 2014] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and Mortimore, C. (2014). Openid connect core 1.0. *The OpenID Foundation*.

[Schaar, 2010] Schaar, P. (2010). Privacy by design. *Identity in the Information Society*, 3(2):267– 274.

[Weiser, 1991] Weiser, M. (1991). The computer for the 21st century. *Scientific american*, 265(3):94– 104.