CE876 - Information Security Mng. & Eng.

Lecture 7: Identity & Access Management

Seyedeh Atefeh Musavi / Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology
Spring 1400

S4Lab

Acknowledgments: Some of the slides are fully or partially obtained from other sources. A reference is noted on the bottom of each slide to acknowledge the full slide or partial slide content.

Threat evolution is accelerating

S4Lab

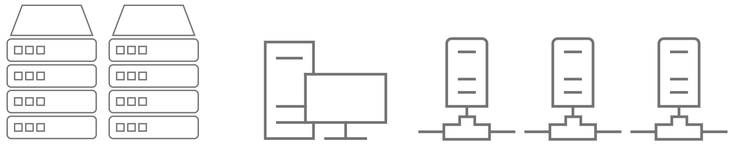
Malware-Less Attacks

‘File-less’ Malware

Tailored/Targeted Malware

Mass Distribution Malware

THREAT AGES



Malware and Infrastructure

Identity and Apps

Your enterprise in transformation

S4Lab

Requires a modern identity and access security perimeter

Cloud Technology

SaaS adoption

Office 365

Modern Enterprise Perimeter

Infrastructure as a Service

Platform as a Service

[Microsoft CISO Workshop]

Internet of Things

1st class mobile experience

ENGAGE YOUR CUSTOMERS

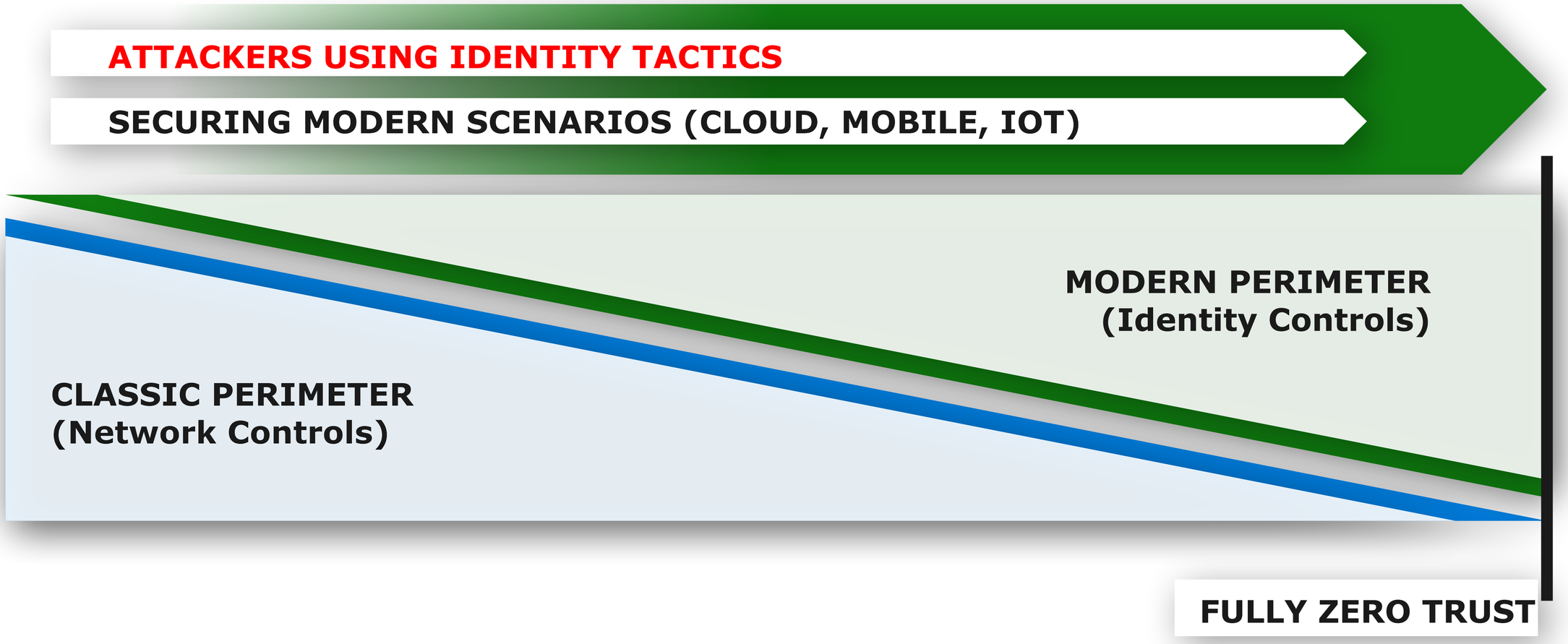
EMPOWER YOUR EMPLOYEES

OPTIMIZE YOUR OPERATIONS

TRANSFORM YOUR PRODUCTS

Running Dual Perimeters

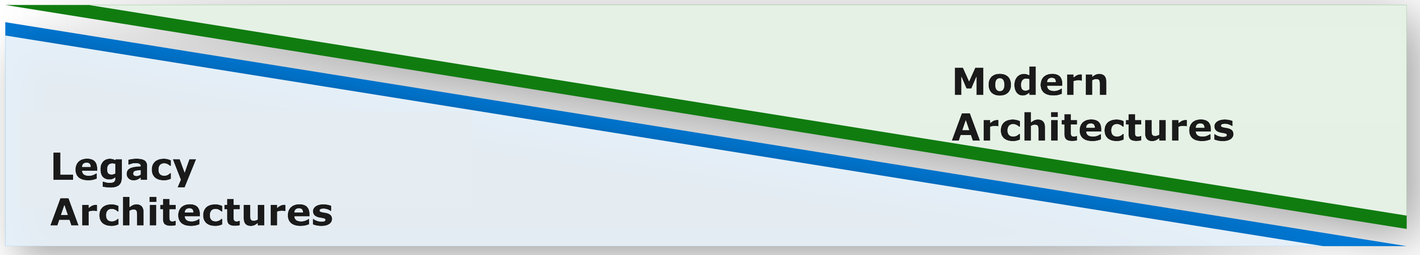
S4Lab



[Microsoft CISO Workshop]

Evolution of Roles and Responsibilities

S4Lab



"STOP THE PRESSES!" → CONTINUOUS VALIDATION

Security roles will change with architectural/operational models

Manual Resource Administration	**Administration**	Author & Govern Automation
Containment with Network	**Network → Containment**	Containment at all layers (Net, App, ID, Data, etc.)
Quality Check Before Release	**Development**	Security SME in DevOps process
Project based Engagement	**Architecture**	Continuous Engagement & Improvement

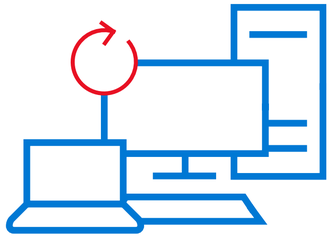
[Microsoft CISO Workshop]

Designing for Failure – The Mindshift

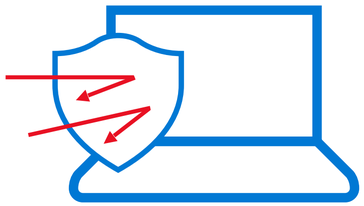
S4Lab

THEN

Reliability:
Designed not to fail

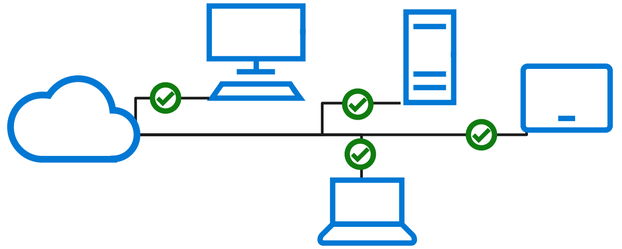


Prevent:
Every possible attack

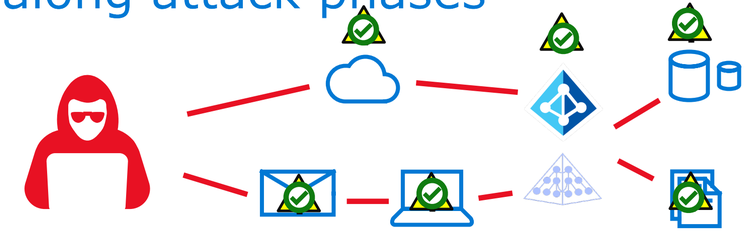


NOW

Resilience:
Designed to recover quickly



Assume Compromise:
Protect, detect, and respond along attack phases



What is IAM?

S4Lab

- Identity and Access Management
- Traditionally considered just the internal face of an enterprise, but has been evolved to cover CIAM (Customer Identity and Access Management).
- Include:
  - Authentication of users and system
  - Authorization of those users and systems
  - User provisioning
  - Audit of identity systems
  - User repository management
  - Password policies, and other concerns
- In this session we will focus on authentication/authorization.
  - So do we talk only about users?

[Authentication vs. Federation vs. SSO, Robert Broeckelmann, 2017]

What is the IAM?

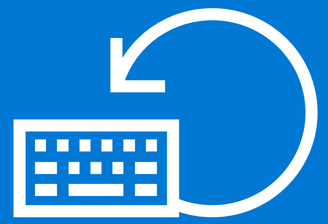
S4Lab

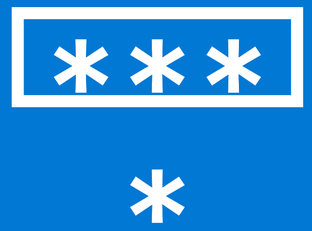
- So do we talk only about users?
- No, machines also should be authorized too.
  - Internal Server2Server communication
  - B2B relationships
  - Enterprises may have APIs

[Authentication vs. Federation vs. SSO, Robert Broeckelmann, 2017]

Trends and challenges

S4Lab





Attackers using identity to bypass network controls

Phishing allow attackers to impersonate valid user Identities

Credential theft allows attackers to expand access by impersonating identities

Passwords aren't enough to protect identities

Single factor authentication (Passwords) without context isn't enough assurance

Attacks on credentials circumvent software assurances (without hardware isolation)

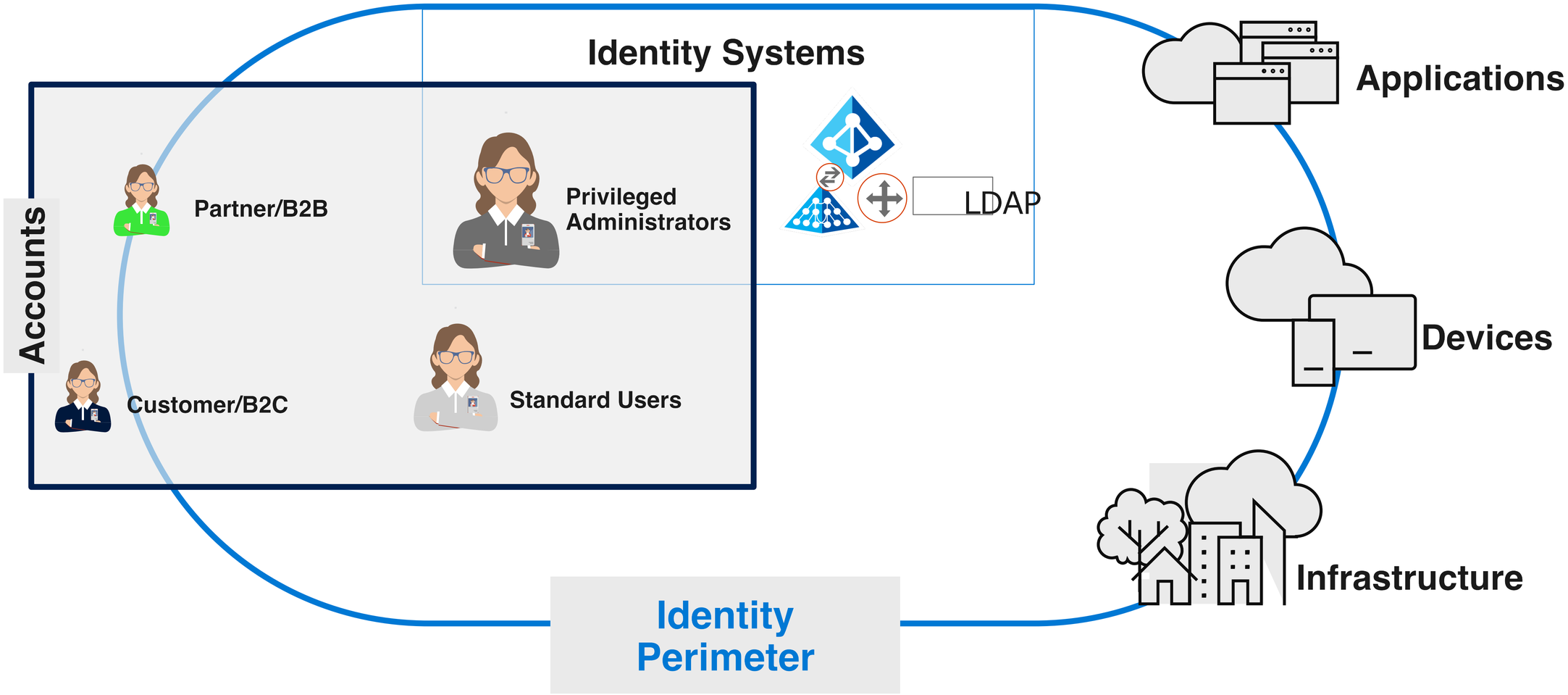
Identities being used outside network

Cloud, Mobile, and IoT assets are frequently beyond reach of enterprise firewalls

Identity and Access controls are inconsistent on different cloud services and devices

Identity and access management

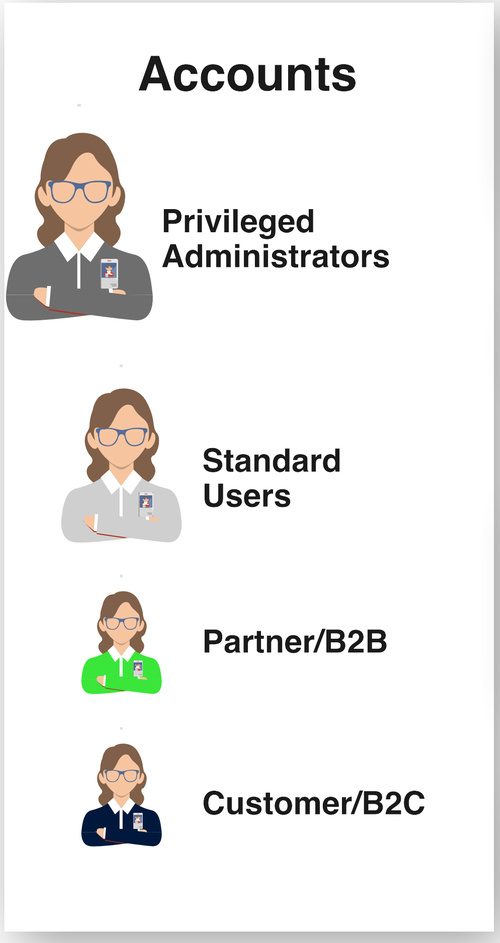
S4Lab



Account security
Success factors to increase attack cost

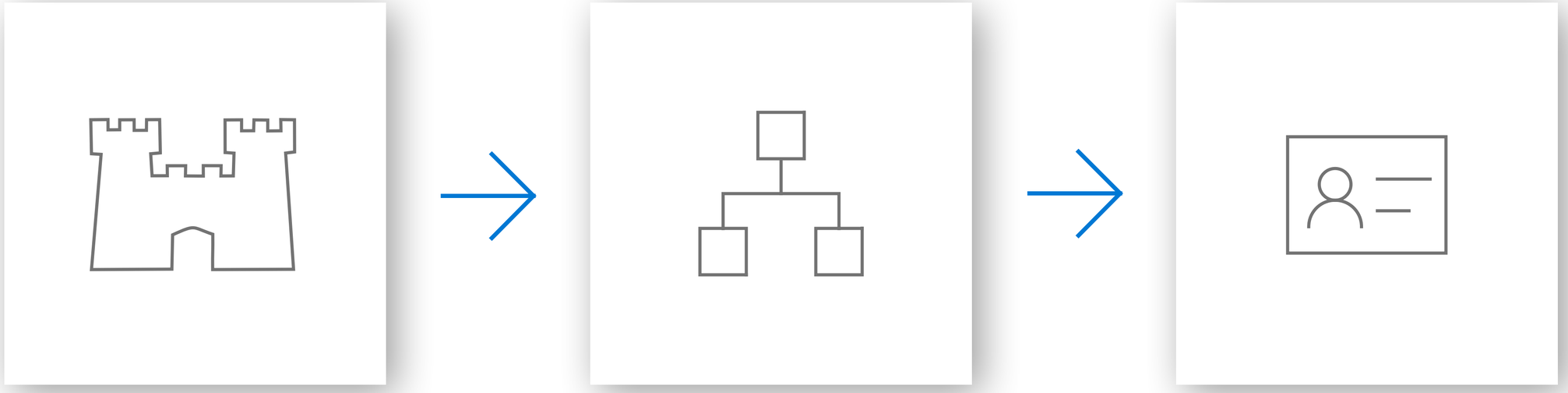
S4Lab

- Great experience
  - For users, identity managers, and security
  - Single Identity and Single Sign On (SSO)
- Strong assurances
  - Additional Factors like biometrics and others
  - Increase context in authentication / authorization decisions
    - Time, date, geolocation
    - Device integrity and compliance
    - Known Bad sources from threat intelligence
  - Behavior Analytics to understand normal profile for that user/entity
  - Hardware assurance for credentials stored on devices
- Flexible Access Levels
  - Allow for Low Risk
  - Increase Assurance (add MFA) based on risk factors
  - Decrease Access (Block download) based on risk factors
  - Force Remediation for high risks (compromised devices and accounts)



Evolution of security perimeters

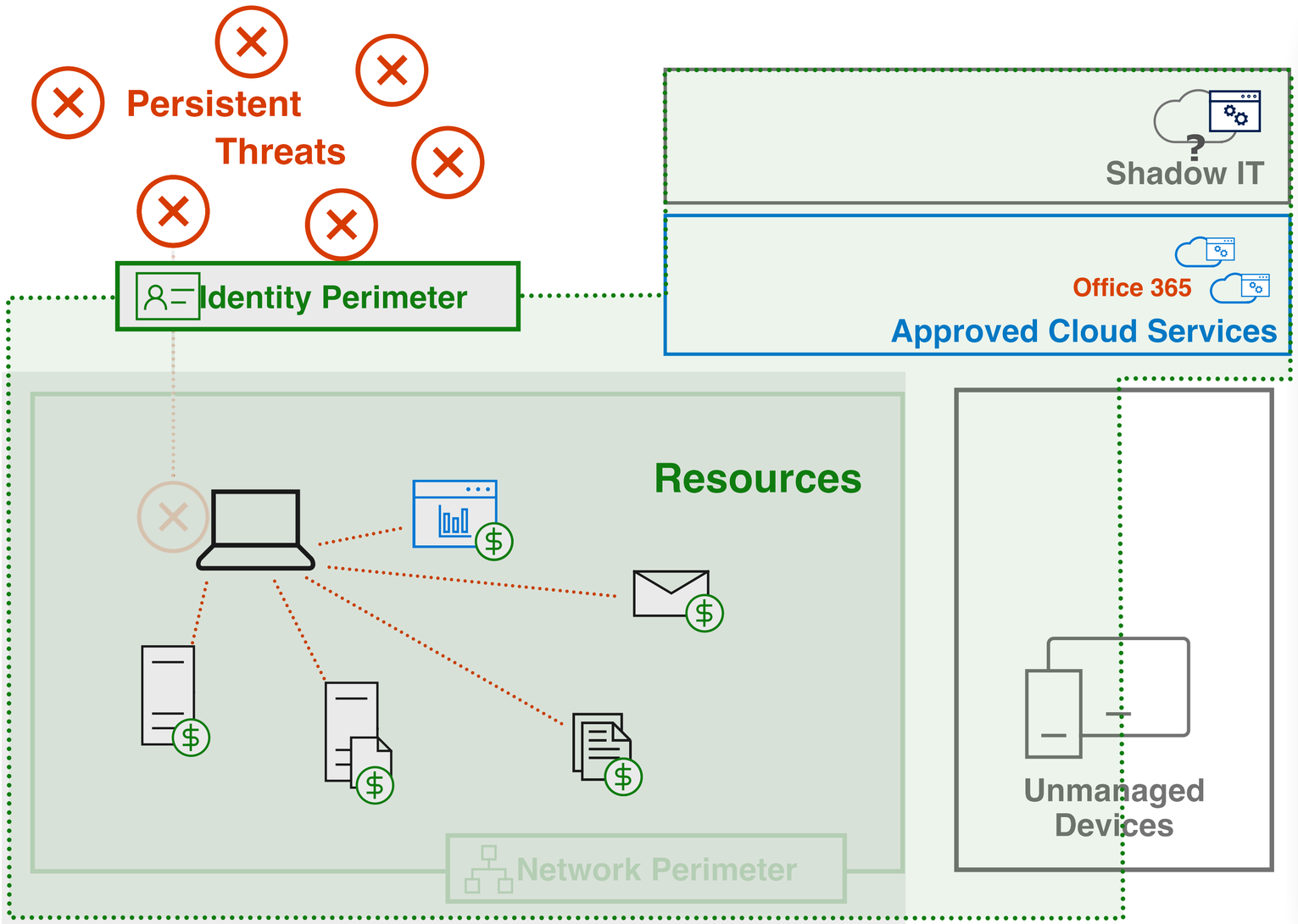
S4Lab



Physical **Network** **Identity**

Modernizing the security perimeter

S4Lab



Network protects against classic attacks…

…but bypassed reliably with

- Phishing
- Credential theft

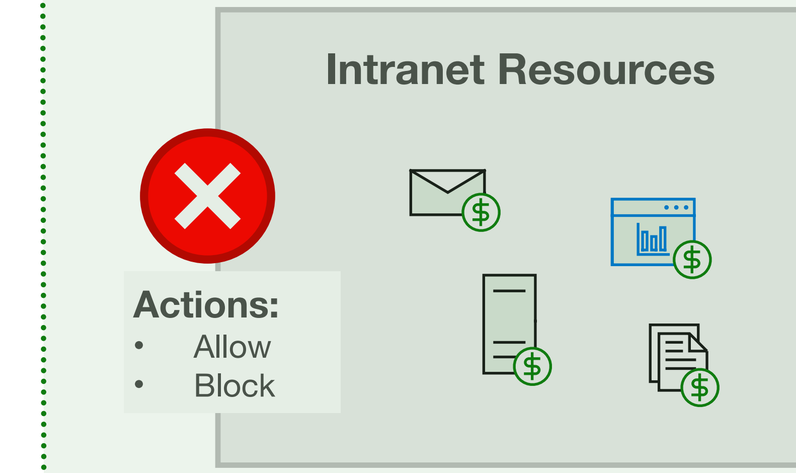
\+ Data moving out of the network

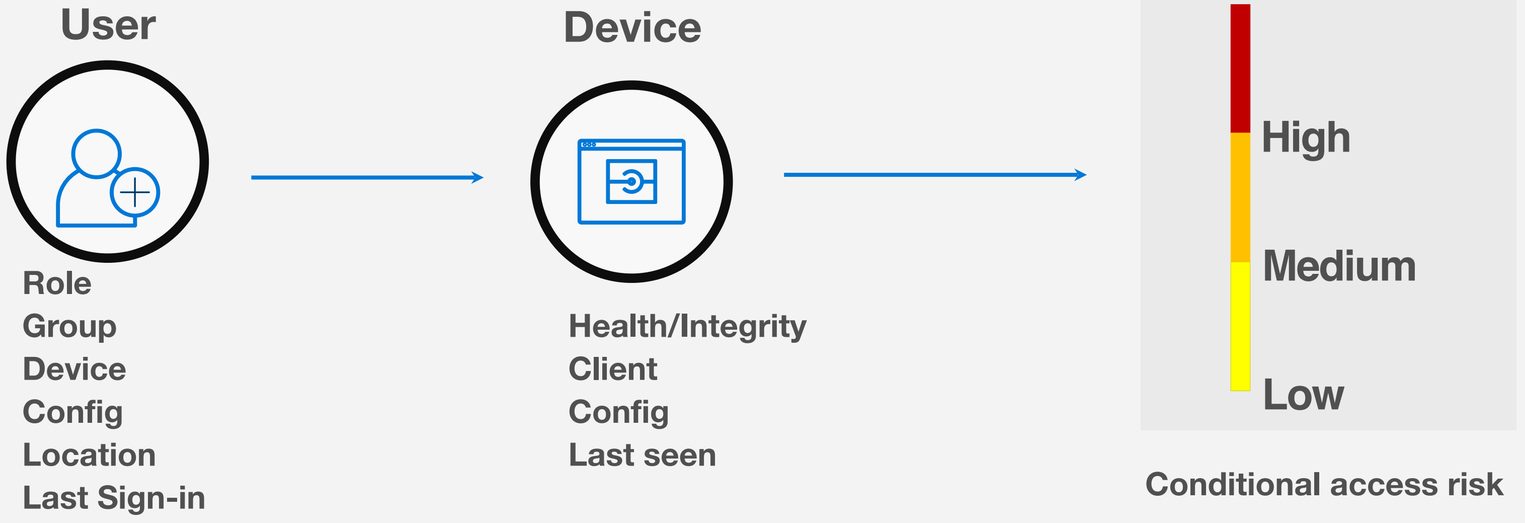
= Critical to build modern security perimeter based on Identity

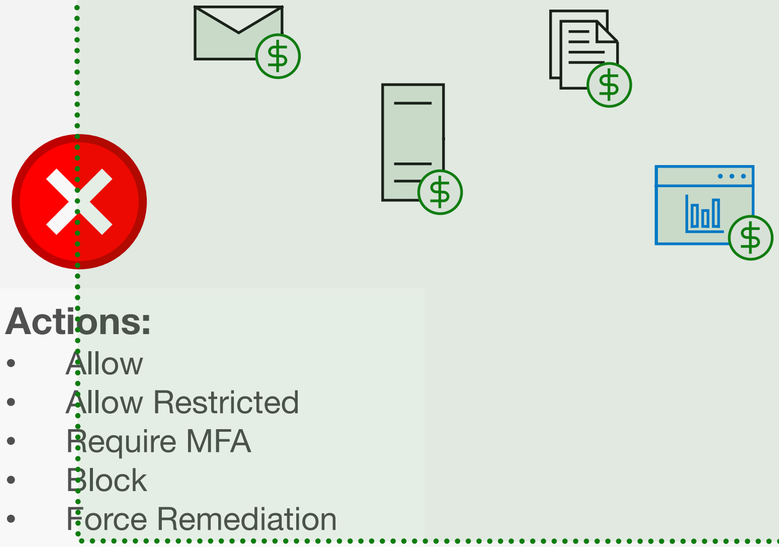
- *Identity and Access Management* Strong Authentication + Monitoring and enforcement of policies
- *Strength from Hardware & Intelligence*– Auth & Access should consider device status, compromised credentials, & other threat intelligence

VISIBILITY AND CONTROL AT THE PERIMETER

S4Lab

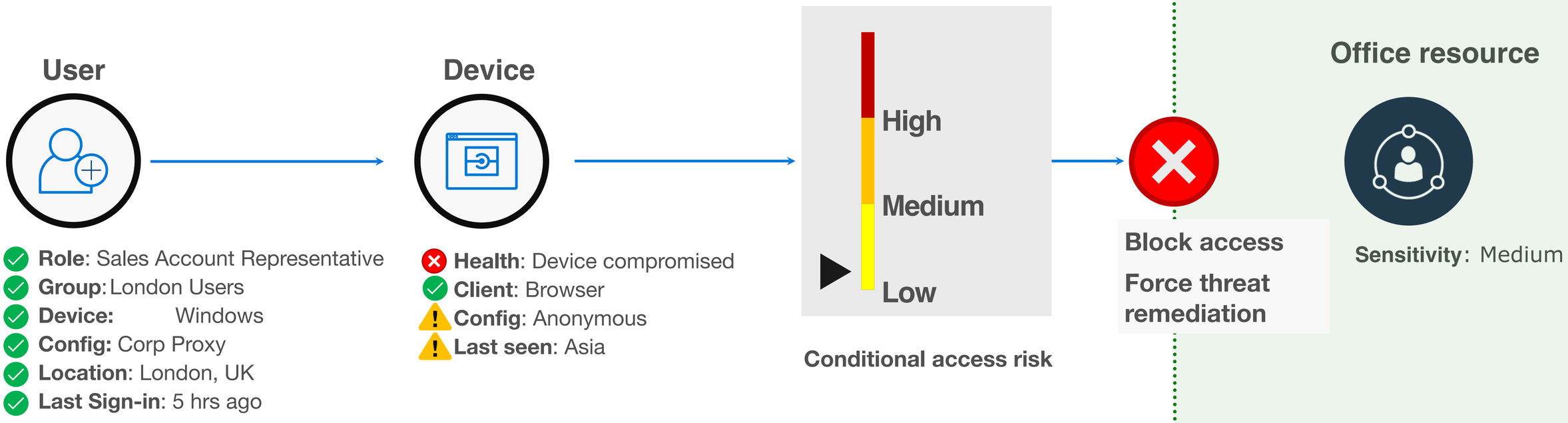






Conditional Access Example

S4Lab



For insights into password spray and other modern attack patterns, see https://channel9.msdn.com/events/Ignite/Microsoft-Ignite-Orlando-2017/BRK3016

Malicious activity detected on device

Anonymous IP

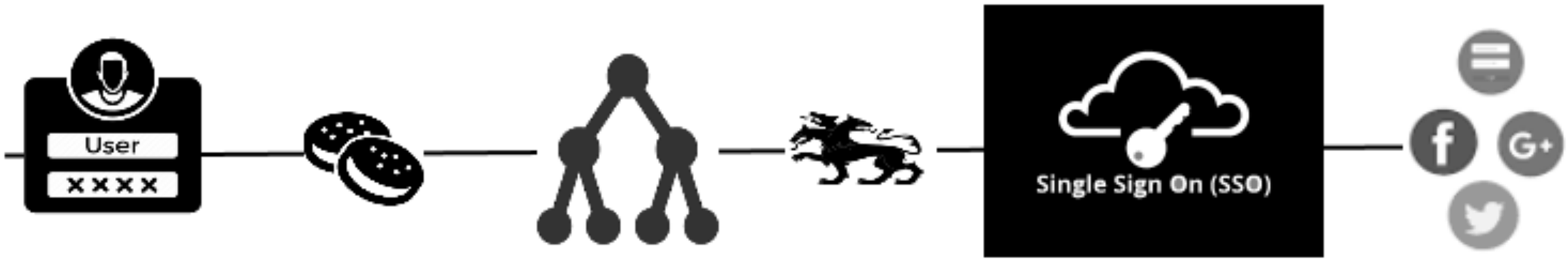
Unfamiliar sign-in location for this user

Authentication/authorization in an enterprise

Password-based authentication management

S4Lab

- Multiple choices to implement authentication/authorization in an enterprise
- Different devices which support specific authentication methods/protocols



Password-based IAM choices

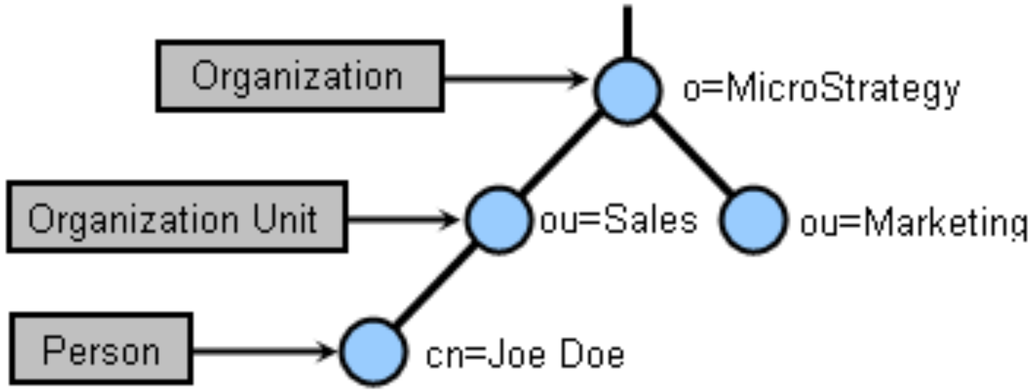
S4Lab

- One way is to use traditional login for each service. Not scalable.
- Another is to use a third party trusted authentication server to manage all authentication/authorization decisions.
- Often assume having a server which includes identity information and some applications which query the server to check identities.
- This application can be internal(employees), external (partners/customers).
- Can you provide a well-known example?

LDAP approach

S4Lab

- A layer 7 standard protocol for apps like email clients, browsers, networked systems
- Central repository server (LDAP server)
  - Not in relational way but in attribute and value pair
  - Can be public, or organization-specific
- Optimized protocol for info which often read, rare update, e.g user info
- It can be implemented open (open-ldap for Linux) Or proprietary (active-directory in Windows)



[Image:https://doc-archives.microstrategy.com/]

Case Study

- Take Sharif for example:
  - Each service/organization operates it’s own authentication service (e.g. ldap)
  - edu, email, restaurant, department email, etc.
- Two issues:
  - If same password for all services, then if one gets compromised, all your access are compromised.
    - Having different passwords for each service, really messy!
  - Have to keep re-entering passwords for the different services at Sharif.

Single Sign On (SSO)

S4Lab

- The idea is to use single sign-on among all software resources.
- So can LDAP be an SSO?

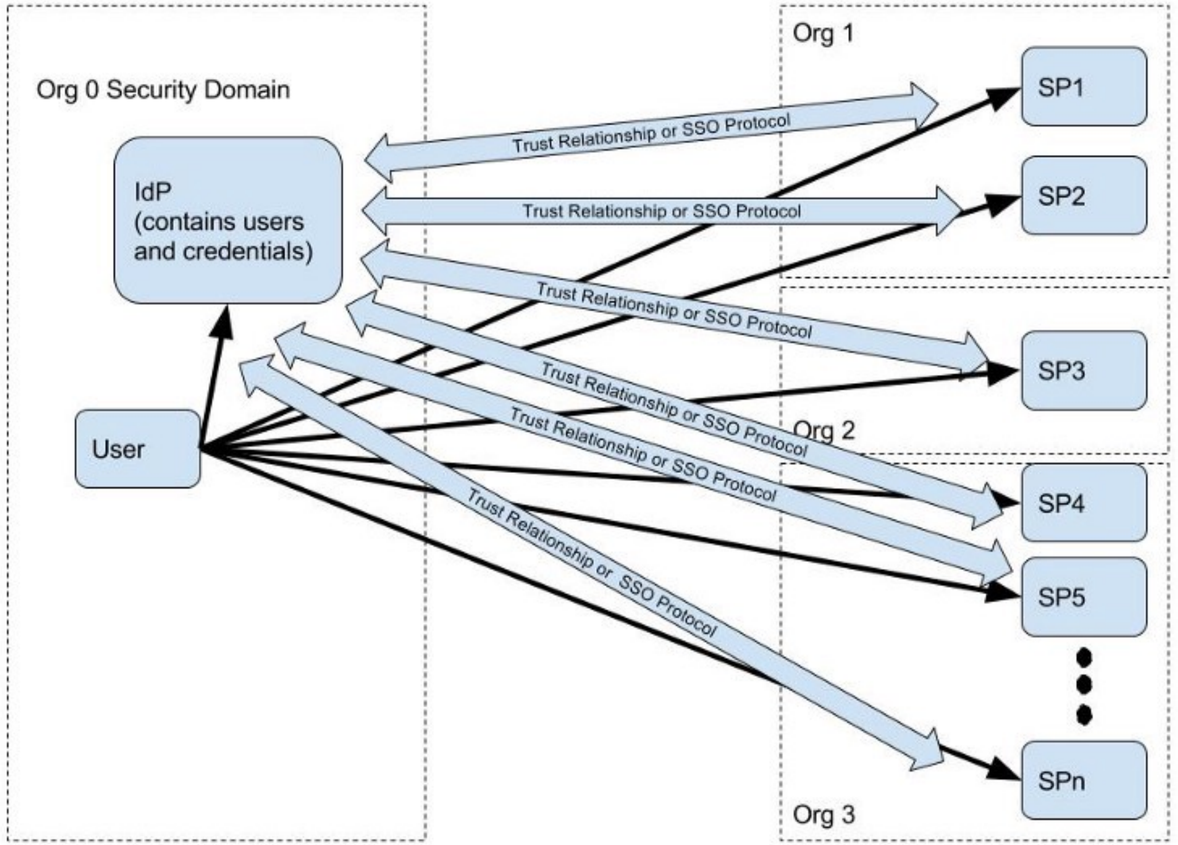
Single Sign On (SSO)

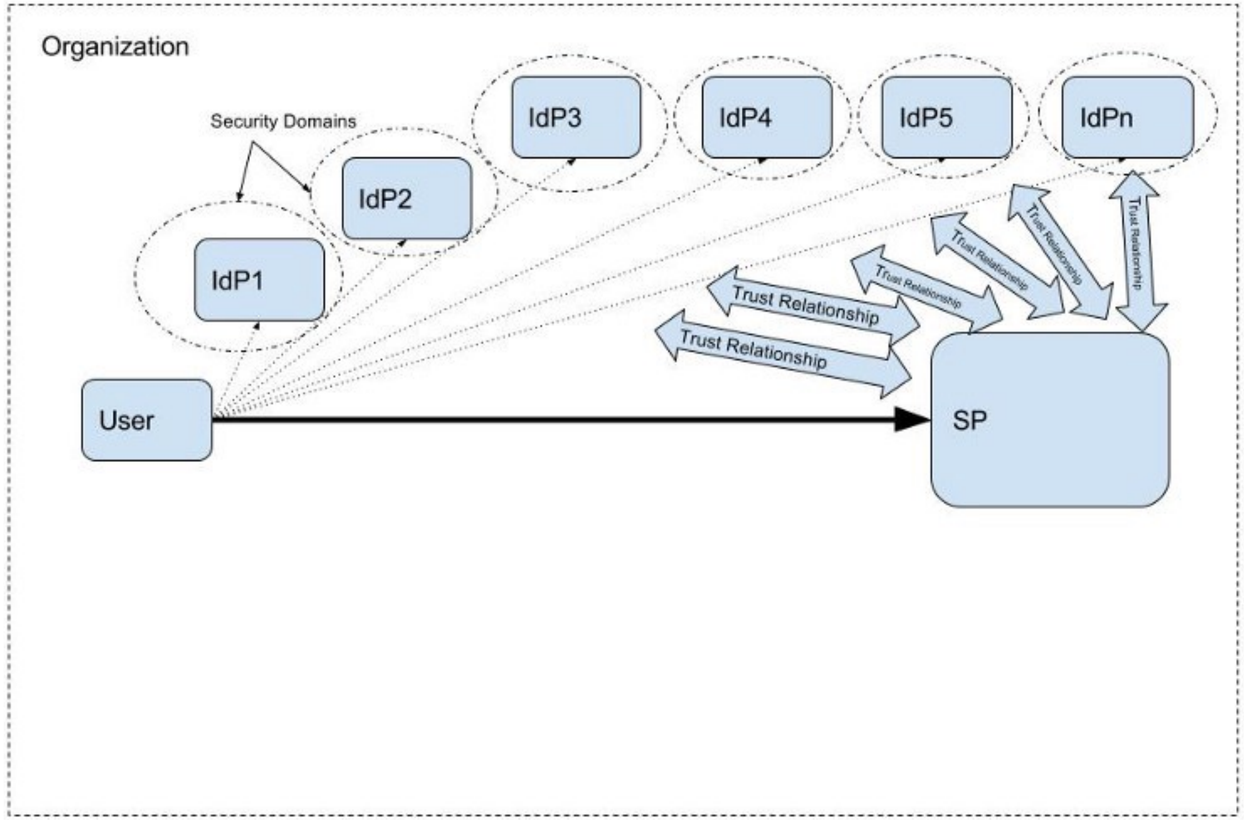
S4Lab

- The idea is to use single sign-on among all software resources.
- So can LDAP be an SSO?
- For each new login, although a same account, is queried from the LDAP server.
- So if we need more scalability we can think of an approach which a user can be authenticated multiple time by passing tokens to the apps?
- Assuming a trust relationship between the service providers and the identity provider.

SSO vs federated identity

S4Lab



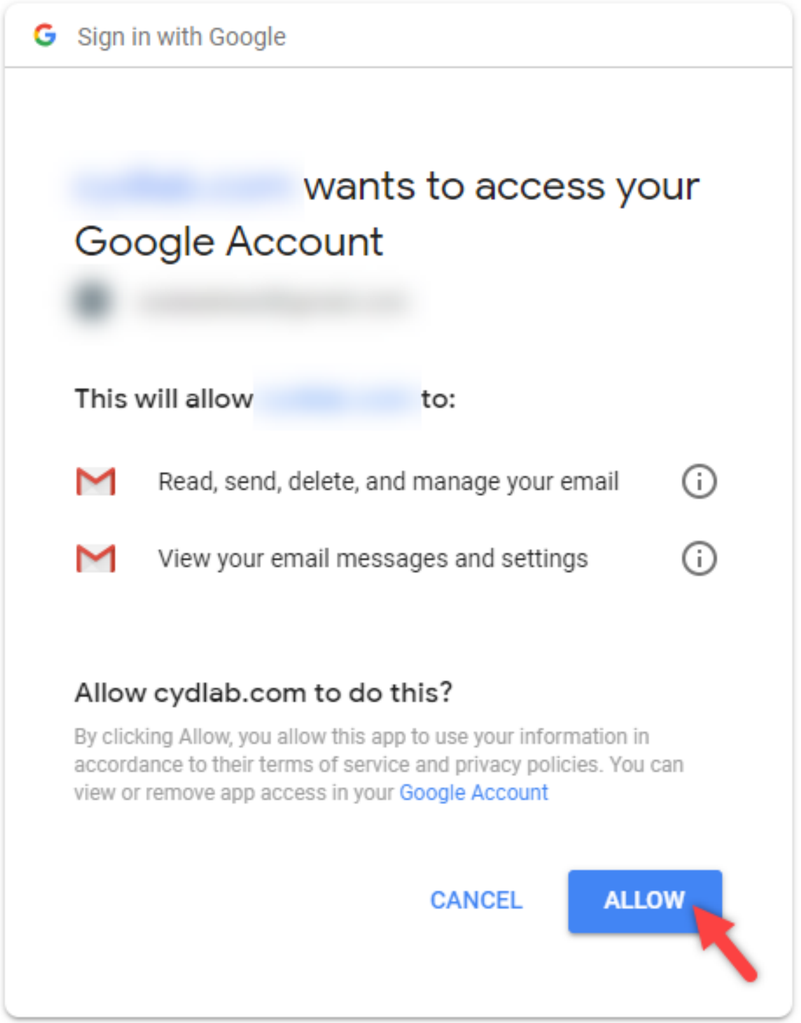


[Authentication vs. Federation vs. SSO, Robert Broeckelmann, 2017]

Oauth2

S4Lab

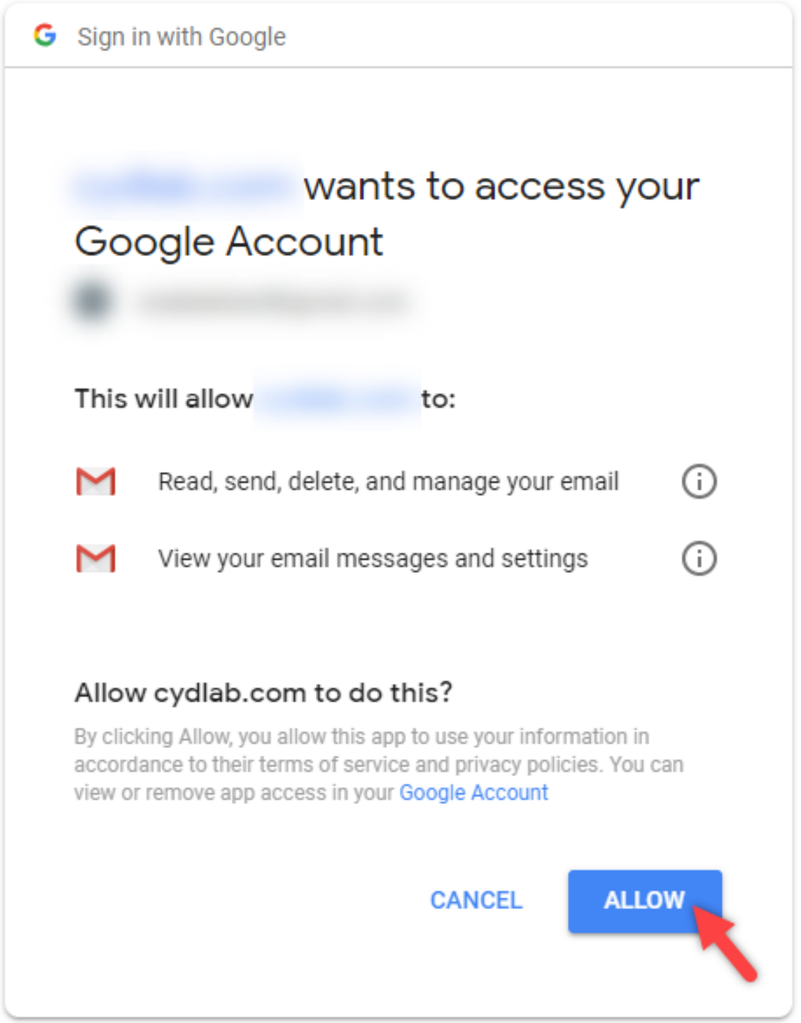
- Have you ever logged into a third-party web site with your Google, Facebook, or Twitter account, by granting permission to your account?
  - You've used Oauth.
- Is OAuth (pronounced “oh-auth”) an authentication protocol?



Oauth2

S4Lab

- Have you ever logged into a third-party web site with your Google, Facebook, or Twitter account, by granting permission to your account?
  - You've used Oauth.
- Is OAuth (pronounced “oh-auth”) an authentication protocol?
  - NO
  - Open authorization
  - Open id is a protocol for authentication on top of oauth.
  - OAuth decouples your authorization policy decisions from authentication



Before Oauth days…

S4Lab

- LinkedIn has a feature that imports your Google contacts and invites them to connect with you. Back in the day, LinkedIn would ask you to give them your Google username and password.
  - They would use it to log in on your behalf, download your contacts and log out.
  - You can only hope that they don’t do anything else with your credentials.

[OAuth and OpenID explained with real life examples, A. Starreveld, 2018]

With Oauth

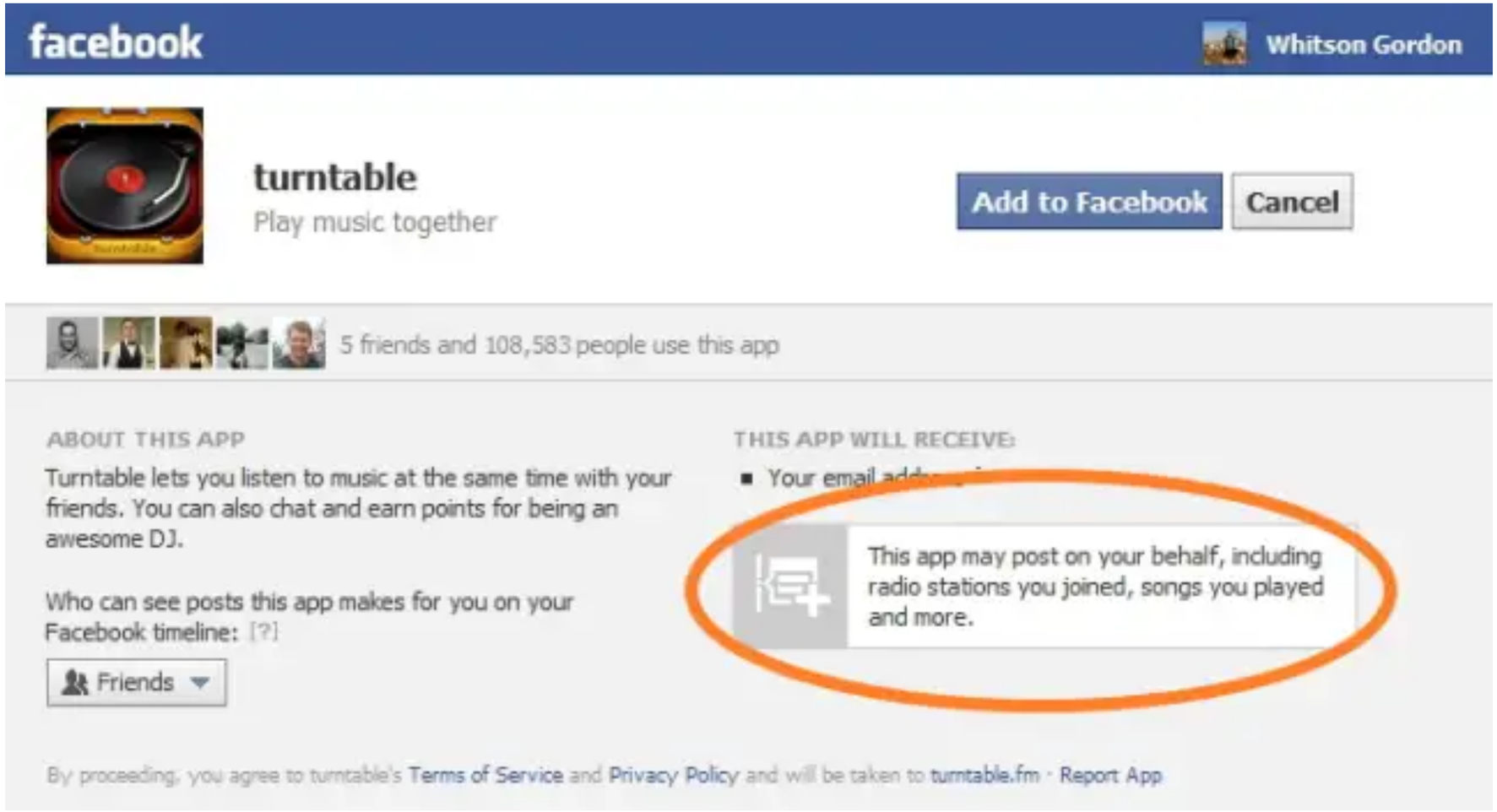
S4Lab

- Oauth idea is to only giving them access to the stuff you want them to access.
  - Instead of asking you for your password!!
  - Remember, you're giving your username and password to Gmail/Twitter not the app.
  - When you click the "Authorize" button, Gmail/Twitter creates an "Access Token" and an "Access Token Secret". These are like passwords, but they only allow the app to access your account and do the things you've allowed it to do.
- What if the app get hacked?
  - Your password is still safe.
    - The hackers would still be able to post on your behalf, follow people, or do whatever else you've given access to do, but all you need to do is go to your account settings and revoke access to that app

[Understanding OAuth: What Happens When You Log Into a Site with Google, Twitter, or Facebook whitsongordon W. Gordon, 2012]

On your behalf!

S4Lab

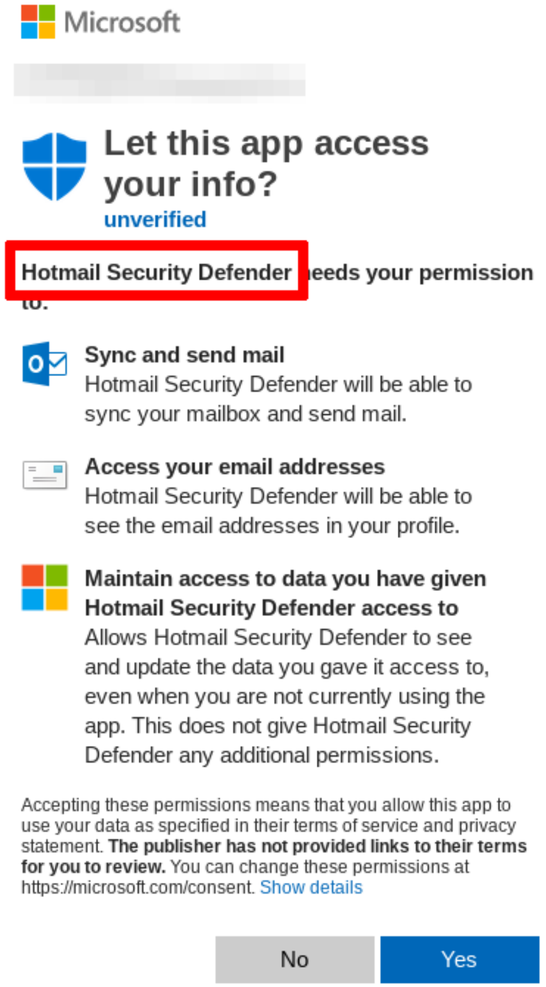


[Understanding OAuth: What Happens When You Log Into a Site with Google, Twitter, or Facebook whitsongordon W. Gordon, 2012]

OAuth2 Phishing: A real story

S4Lab

- Instead of creating fake login pages or fake password reset forms and grabbing the credentials to the targets' accounts, attackers make use of "OAuth Phishing".
- Attackers do not need to steal credentials!
  - Create malicious third-party applications and lure the targets into granting the applications access to their accounts.
  - Simply abuse legitimate functionality that online platforms provide.
- Authentication to the account happens on the legitimate site, no form of two-factor authentication - including Security Keys - can mitigate against this.
- In December 2018, Amnesty International documented widespread targeted phishing attacks.

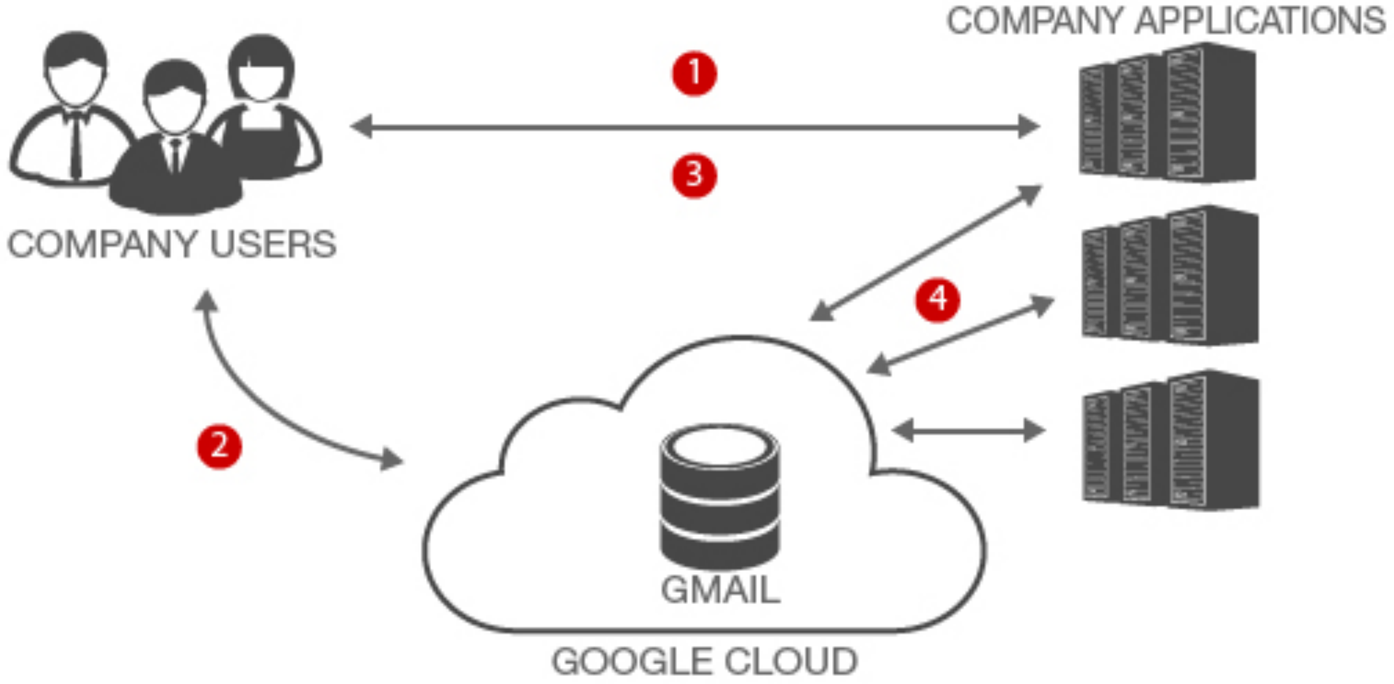


[Evolving Phishing Attacks Targeting Journalists and Human Rights Defenders from the Middle-East and North Africa, 2019]

Oauth2 in an enterprise (1)

S4Lab

- A prime example of this adoption is based on a use case where a company's email system is hosted in the Google cloud.
- Google cloud is the identity repository for the company's users.
- What's the problem with this cloud-based access control architecture?

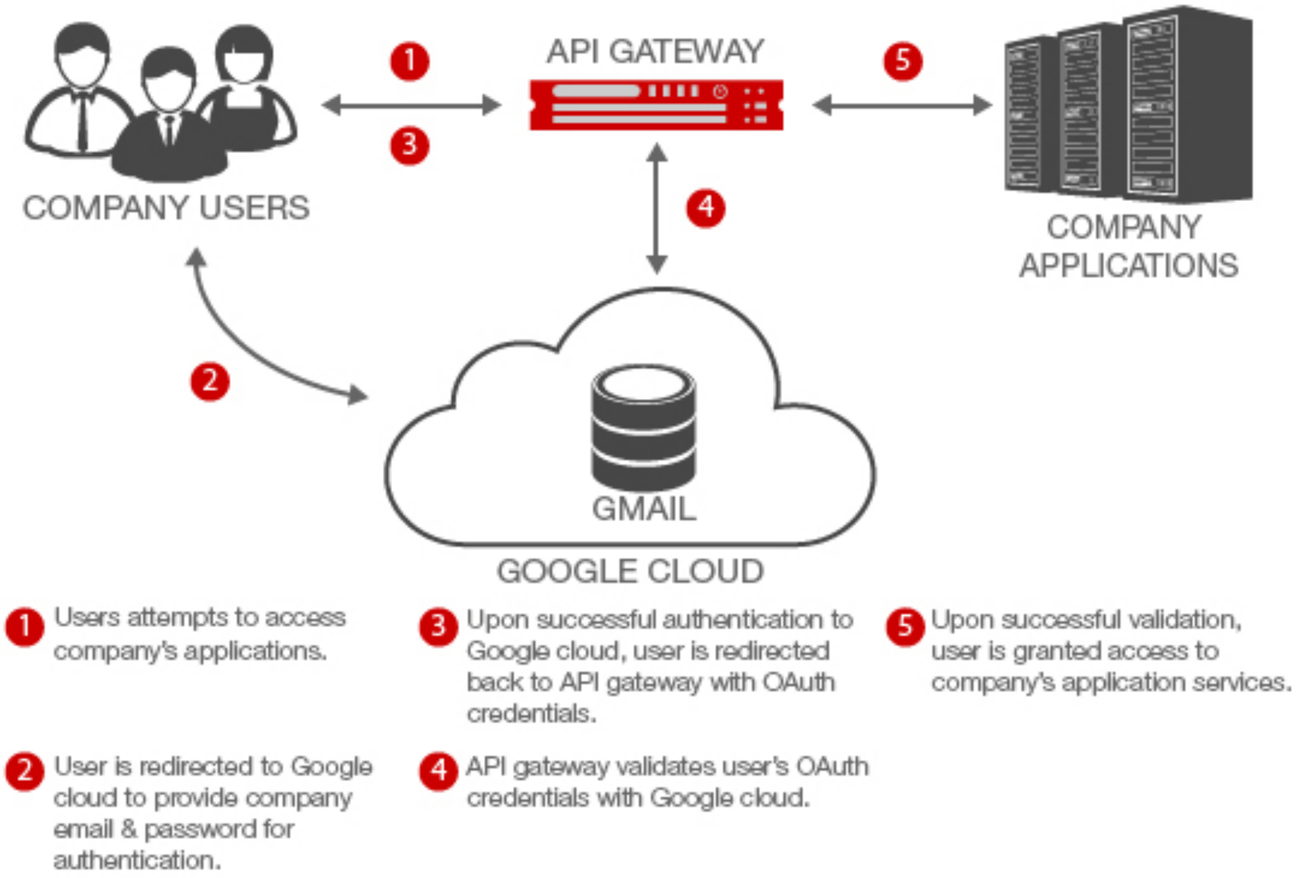


[How to Use OAuth for Enterprise Identity Management, Ona Blanchette, 2014]

Oauth2 in an enterprise (2)

S4Lab

- By adding an api gateway:
  - No modifications are required to company applications. Applications are OAuth agnostic.
  - Integration and testing of OAuth is no longer required with applications
  - Centralized monitoring and enforcement is easier with an API Gateway.
  - An API gateway accelerates SSL traffic that contains OAuth credentials.
- Is this always better?



[How to Use OAuth for Enterprise Identity Management, Ona Blanchette, 2014]

Why openID?

- What did we see with Oauth?
- A web app can receive a delegated access token to some resources of a user.
  - This is an authorization service.
- In many cases web apps only require an authentication service.
- They can use Oauth as authentication service
  - However Google may implement Oauth differently from Twitter.
  - Oauth is just a specification.
  - There were no authentication concern.
- OpenID is a unified authentication layer implemented on Oauth.

OpenID

Corporate Board Members

- Google – Adam Dawes
- Janrain – Jim Kaskade
- Microsoft – Anthony Nadalin
- Oracle – Prateek Mishra
- Ping Identity – Pam Dingle
- Symantec – Brian Berliner
- US Department of Health & Human Services, Office of the National Coordinator – Debbie Bucci
- Verizon – Bjorn Hjelm
- VMware – Ashish Jain

[Image: https://openid.net/]

OAuth2 Tokens

S4Lab

- Tokens in Oauth make authentication/authorization stateless and hence scalable.
  - The user state is never saved in the server’s memory
- OAuth spec doesn’t define the token type.
- What are token types and which is better?

Different exiting Tokens

S4Lab

- What are token types and which is better?
  - Session cookies: used extensively in server-based authentication.
    - Not self-contained, requires some state.
  - Authentication tokens: authentication tokens usually are used instead of the username/password combinations.
  - Authorization tokens: decoded to review the user's contents, domain, authorization levels (admin, user, read, write).
  - Access tokens: only provided to an authenticated and authorized user and to access a specific API.

[Demystifying Tokens for Securing Enterprise APIs, Jayashankar S. and Kandy S. T., ISSA Journal, 2020]

An Example

S4Lab

- The user logs into https://banka.com and is redirected to the login page.
  - As he doesn't have a session identifier or a session cookie.
- The user enters username/password and is logged into the application.
- Bank A allocates a session identifier and stores it in a session cookie, which is stored in the user's browser.
- If this was a mobile app, and if a user chooses to authenticate using the phone's biometrics, the server would send back an authentication token, which is stored in the phone.
  - Next time the user logs in, he uses the authentication token instead of entering his username/password combination.

[Demystifying Tokens for Securing Enterprise APIs, Jayashankar S. and Kandy S. T., ISSA Journal, 2020]

An Example

- Once authenticated, the authorization server in enterprise environment checks its backend about the user, whether he is the primary member of the account or an authorized manager of the account.
- Depending upon the user details, an authorization token is sent back to the user, with the details embedded in as a token.
- During each transaction, the user forwards the authorization token to the server, which is then exchanged with an access token.
- When the user requests to access the BalanceAPI, the server sends the user an access token through which he can log in to the BalanceAPI and check his balance.

[Demystifying Tokens for Securing Enterprise APIs, Jayashankar S. and Kandy S. T., ISSA Journal, 2020]

Scope-based authorization

S4Lab

- A common approach to authorization is to use scopes (permissions).
- Access tokens are built up with scopes.
- A user requests the scopes he intends to use.
  - Based on a policy, this is either granted or denied.
- That means the authorization server implements policies and that an authorization server may decide not to include a certain scope into an access token.
  - E.g. you give your identity to a gatekeeper to enter a critical scope, he checks the list and give you an access.
- Server should know all identities and the policy which related these identities to scopes.

[OAuth and OpenID explained with real life examples, Albert Starreveld, 2018]

Claim-based authorization

S4Lab

- Policies may change, but the identities do not.
- What if we can change our policies, without such coupling to the authorization server?
- Think of a hotel key which authorize you to enter a specific room.
  - What we ask the server:
    - This user claims to be X.
    - Check if he is X, an access to Y should be provided for him.
  - We need a self contained token which include these all.
  - So the decision about the authorization has been made in the app.
  - Claim-based authorization is a better fit for fine-grained authorization.

[OAuth and OpenID explained with real life examples, Albert Starreveld, 2018]

Claim or Scope, which to use?

S4Lab

- In practice used together.
- OpenID Connect (OIDC) scopes are used by an application during authentication to authorize access to a user's details, like name and picture.
  - Each scope returns a set of user attributes, which are called claims.
  - The scopes an application should request depend on which user attributes the application needs.
- One can see Claim/scope-based authorization as a modern alternatives to roles.
- Certain things are available to all authenticated users, some to people who have specific claims.
- Today’s there are many situations which we have so many users with same role but different identities.

[OpenID Connect Scopes, Auth0 Docs, 2021]

JWT

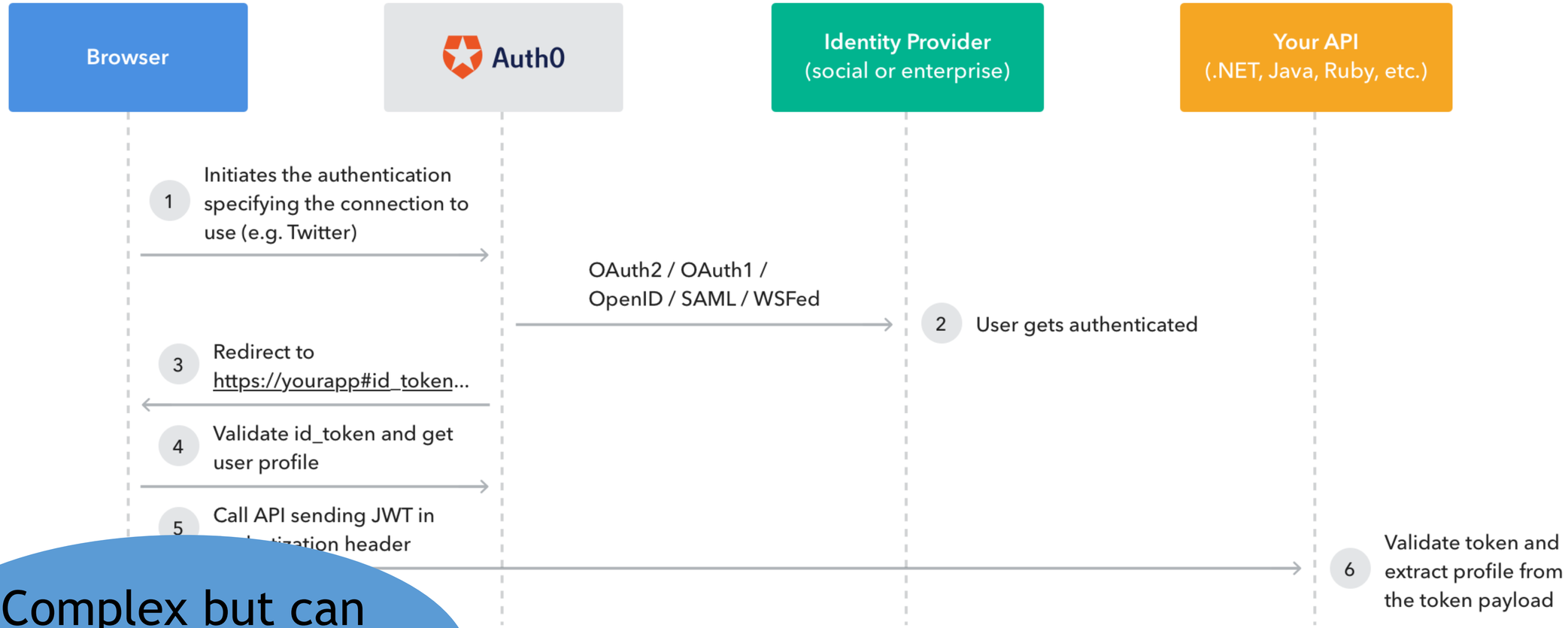
- JSON Web Token are known as Oauth tokens
- Works in claim-based manner
- The JWT specification defines seven Registered Claim Names which are the standard fields commonly included in tokens, as well as custom claims.

```
{
  "name": "John Doe",
  "iat": 1516239022
}
```

- Supports token signing to protect the integrity.
- The user takes its token from the authorization server and store it locally.
- What's the difference with sessions?
  - No need to keep state like session id or cookies.

Auth0 service

S4Lab



Complex but can be outsourced!
e.g. Auth0

[How Auth0 Uses Identity Industry Standards, auth0, 2016]

WPA2 Enterprise (802.1x)

S4Lab

- What would be a more secure wifi connection?
  - Better encryption?

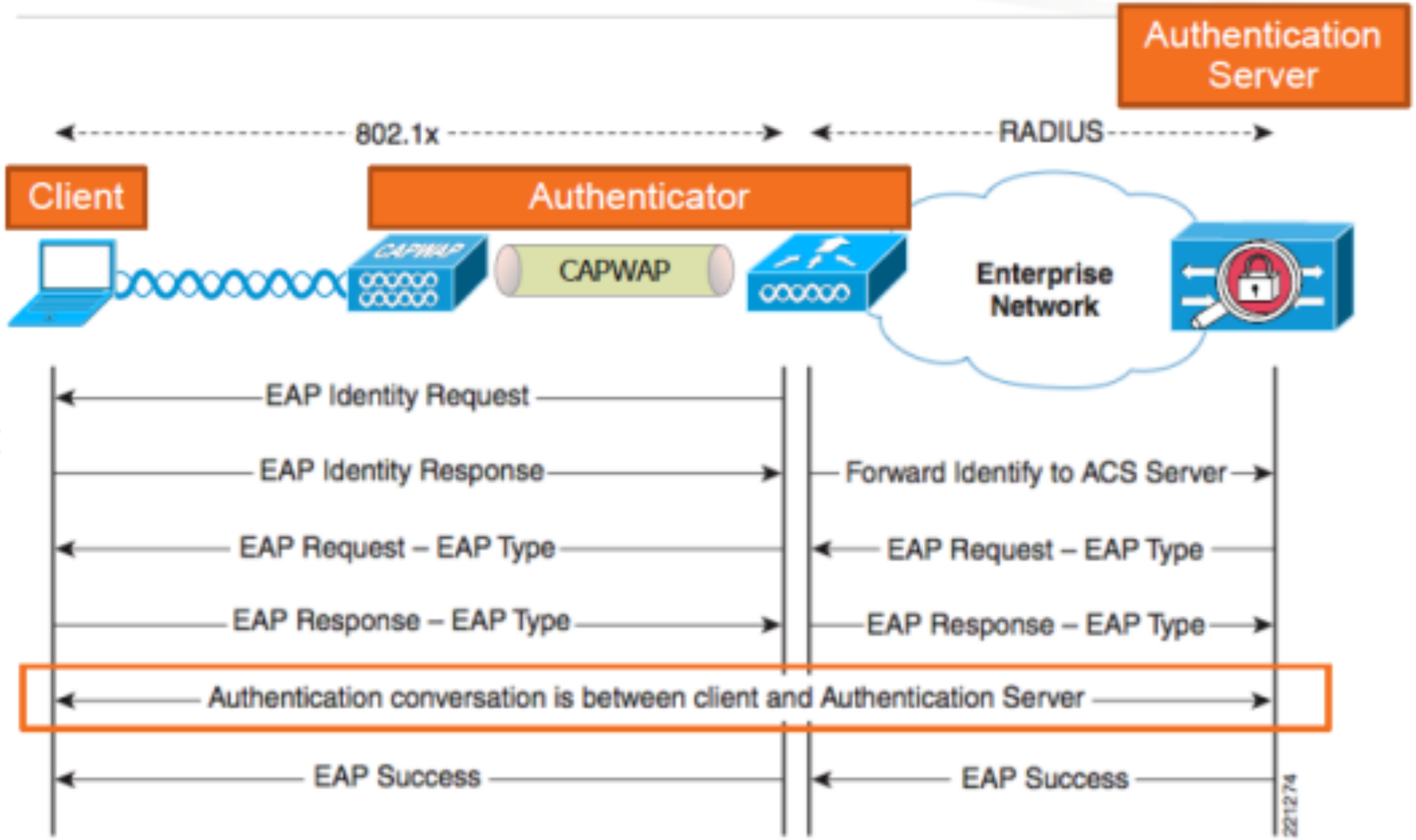
WPA2 Enterprise (802.1x)

S4Lab

- What would be a more secure wifi connection?
  - Better encryption?
  - Better authentication
- What if we don’t want to use pre-shared key authentication used in personal schemes?
  - E.g. WPA2 personal (PSK) vs WPA2-enterprise
    - RADIUS server authenticate the user.
    - Build a master key for this user’s traffic encryption.
- Your implementation choices:
  - Some access points come with built-in software that can operate 802.1x (though only for the smallest of small deployments).
  - Have a server yourself (e.g. your LDAP server).
  - Outsource the RADIUS service (e.g. SecureW2).
  - Go for a unified solution.

[Simplifying WPA2-Enterprise and 802.1x, SecureW2, 2021]

EAP — Protocol Flow



- htt

[EAP Overview, Nayarasi, 2013]

Toward Password-less IAM

Why password-less

S4Lab

- The first motivation is on the server side.
- Why store secrets from users?
- Public keys are not secret and hence require less cost to protect.
- So the most common password-less schemes are based on key pairs.

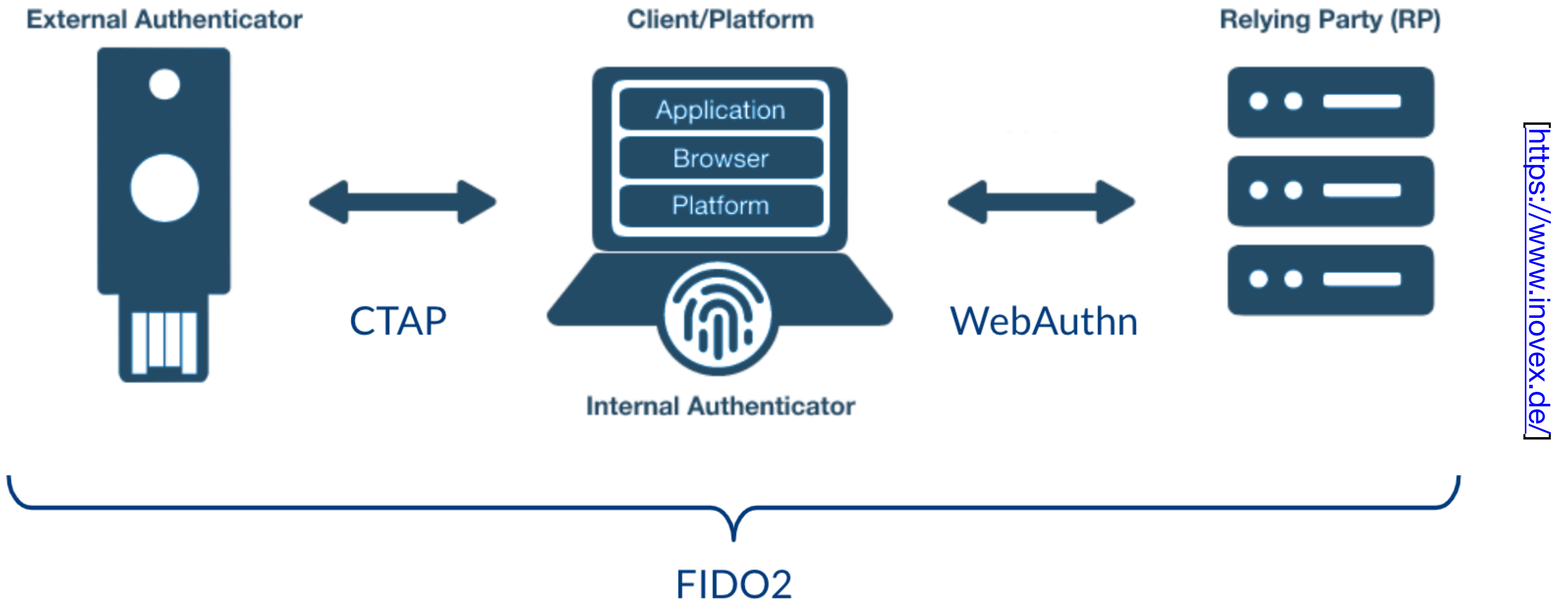
Why password-less?

S4Lab

- The second philosophy for password-less is MFA (multi-factor authentication) evolution.
- Passwords are vulnerable to phishing attacks/identity thefts.
- MFA was designed to make login with passwords more resilient.
  - E.g. SMS/authenticator apps, bio-metric factor
- However, evolution of MFA shows that passwords are not necessary!
  - If we have some sufficient parameters other than the password, why bothering user with a pass?

Password-less standards

S4Lab



[https://www.inovex.de/]

- FIDO authentication
- Now, all Azure AD users can sign in password-free using a FIDO2 security key, the Microsoft Authenticator app, or Windows Hello.

[Plan a passwordless authentication deployment in Azure Active Directory, Microsoft, 2021]

Why password-less? (con't)

S4Lab

- Another motivation is more fundamental: The Authentication problem.
- Access control is the basis for most of our security mechanisms and mostly based on identities:
  - Factor one: What you know (e.g. pass)
  - Factor two: What you have (e.g. token, OTP)
  - Factor three: What you are (e.g. biometrics)
- All these factors suffer from:
  - Single-time mediation: Once an identity is authenticated, the insider is given complete and full unlimited access.
  - Too annoying to be asked frequently from an employee.
  - Vulnerable to insider threats.
    - It is estimated that 23 to 27% percent of cyber crimes are done by insiders.
- -> why not use more contextual data for authentication?

[Choi, S., & Zage, D., Addressing insider threat using "where you are" as fourth factor authentication. IEEE International Carnahan Conference on Security Technology, 2012]

Updating the authentication

S4Lab

- Trying to upgrade the authentication concept to have more contextual information.
  - Authentication may not violate the laws of physics.
  - A person can not be in two different places at the same time.
  - There is a limit to how fast a person can move through space and time.
  - A person's identity may not be inter-changed.
- Proposing the forth factor : where you are?
- Uses Real-Time Location System (RTLS) as factor 4:
  - Provides continuous ID tracking with convenience.
  - Forces the virtual threat to physicalize the penetration attack.
  - Space-time attributes of the cyber identity is captured.

[Choi, S., & Zage, D., Addressing insider threat using "where you are" as fourth factor authentication. IEEE International Carnahan Conference on Security Technology, 2012]

Discussion on employee monitoring

S4Lab

- When you need more contextual context from your employees to authenticate them, you need to monitor them more precisely.
- Is this ethical/legal?
- Employee monitoring technologies were traditionally for preventing insider threats (and not authentication).
- Different monitoring methods:
  - Location monitoring
  - Software/email monitoring
  - Video monitoring
  - Keylogging
- Different tools:
  - Labor sync, Hubstaff, Spyera,…
- What other things an employee has which can be tracked?

Be aware of rules

S4Lab

- "As a general rule, employees have little expectation of privacy while on company grounds or using company equipment, including company computers or vehicles," Matt C. Pinsker, adjunct professor of homeland security and criminal justice at Virginia Commonwealth University.
- Different legal permissions and specific rules depending on where you are.
- An example is Electronic Communications Privacy Act of 1986 (ECPA)
  - Allows business owners to monitor all employee verbal and written communication as long as the company can present a legitimate business reason for doing so.
  - It also allows for additional monitoring if the employee gives consent.
- Monitoring computer web activity is different and can fall under different legal precedent (Privacy rules).

[Spying on Your Employees? Better Understand the Law First, Freedman M., 2020]

Surveillance or monitoring?!

S4Lab

- “Panoptic sort: The collection, processing, and sharing of information about individuals and groups that is generated through their daily lives as citizens, employees, and consumers and is used to coordinate and control their access to the goods and services that define life in the modern capitalist economy.” University of Pennsylvania law professor Oscar Gandy,1993

- What about biased and discriminatory practices?

[Schneier, B., Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company, 2015]

New employee monitoring technologies

S4Lab

- Prediction and flagging tools that aim to predict characteristics or behaviors of employees or that are designed to identify or deter perceived rule-breaking or fraud.
- Biometric and health data of workers collected through tools like wearables, fitness tracking apps, and biometric timekeeping systems as a part of employer provided health care programs, workplace wellness.
- Gamification and algorithmic management of work activities through continuous data collection.
  - Technology can take on management functions, such as sending workers automated “nudges” or adjusting performance benchmarks based on a worker’s real-time progress.

[Workplace Monitoring & Surveillance, Mateescu A., Nguyen A., Data & Society, 2019]

How can the regulations affect the scene?

S4Lab

- As surveillance fades into the background, it becomes easier to ignore.
- And the more intrusive a surveillance system is, the more likely it is to be hidden.
  - Many of us would refuse a drug test before being hired for an office job, but many companies perform invasive background checks on all potential employees.
  - Being tracked by hundreds of companies on the Internet—companies you've never interacted with or even heard of—feels much less intrusive than a hundred market researchers following us around taking notes.
- We're living in a unique time in history; many of our surveillance systems are still visible to us.
  - Identity checks are common, but they still require us to show our ID.
  - Cameras are everywhere, but we can still see them.
- In the near future, because these systems will be hidden, we may unknowingly acquiesce to even more surveillance.

[Schneier, B., Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company, 2015]

Considering the effect on compliance

S4Lab

- Sometimes regulations do not catch up with the technology.
- The first step is to segment the user population in your network. You'll have to bifurcate your users into two groups:
  - Users in a compliance boundary
    - For example, people who handle credit card/payment information
  - Everyone else
- This segmentation is necessary because there are compliance requirements in some industries that essentially require using user names and passwords.

[Preparing your enterprise to eliminate passwords, Arsenault B., Microsoft, 2019]

Bring Your Own Device

BYOD policy

S4Lab

- Improve employee satisfaction.
- Reduces device ownership cost for the companies.
- Typically no central control and management on your own device .
  - Network admin, CSO, CISO are not admin of your own device!
- Is this the only choice other than enterprise device?
  - No, there are similar concepts and concerns:
    - BYOA (Bring Your Own App)
    - CYOD (Choose Your Own Device)
    - COPE (Corporate Owned Personally Enabled)
- Static or dynamic (context-aware) BYOD policies.

What if no clear BYOD policy?

S4Lab

- Considering every thing, is not straightforward:
  - Unlike work email, most mobile text messages don't flow through the corporate network except when employees use a company-deployed texting app.
- Not only security concerns:
  - The employee is terminated and the company remote wipes his iPad, which deletes personal data. Is the company culpable?
  - IT conducts a search on a BYOD and finds out that an employee has been working on a project that potentially undermines or competes with the organization. If the employee was doing this on his own time, can the company fire the employee based solely on this potentially ill-gotten evidence?
- Companies need to craft an employee BYOD policy that keeps corporate data safe yet doesn't infringe on a person's right to privacy on their personally owned device.

[BYOD: If You Think You're Saving Money, Think Again, Tom Kaneshige, cio.com, 2012]

Where do you apply BYOD policies?

S4Lab

- Security enforcement at the server side:
  - Easier to manage and update, as the enterprise has central control over the servers.
  - Places a minimum amount of trust on the clients, as sensitive policies are maintained at the server side and their enforcement does not assume client cooperation.
- Security enforcement at the client side:
  - much of the device-specific context essential to BYOD security is only available at the client side.
  - However, delegating policy enforcement to the clients requires a strong trust in the BYOD devices
  - Policy information is completely revealed to the clients
  - Cannot easily support network-wide policies->local view.
  - Extra processing overhead to resource-constraint mobile devices
- Security enforcement at the network level:
  - only provides fixed functions specialized for packet processing.
  - lack of programmability in traditional networks.
- An ideal solution ->achieves the “best of worlds”:

[Kang, Q., et al., Programmable In-Network Security for Context-aware {BYOD} Policies, USENIX Security Symposium, 2020]

Data-related BYOD policies

S4Lab

- Data security
- Data exfiltration, e.g. Data loss prevention
- Data transfer, e.g. USB Connection limitation:
  - Only BYODs that provide FIPS 140-2 device-level encryption may be connected to [AGENCY NAME] PCs for document transfer purposes (currently only Blackberry devices are certified as 140-2 compliant)

[Bring Your Own Device, White House, 2012]

BYOD at Client Side

BYOD policy for mobile devices.

S4Lab

- BYOD is a management policy which can/might cover different mobility management scopes:
  - *Mobile Asset Management:* the focus is at device-level (e.g. OS, HW, GPS, etc.).
  - *Mobile Application Management:* Corporate App Store, Mandatory applications ,etc.
  - *Mobile Content Management:* Data management, PIM (Personal Information Management) , Data push, etc.
  - *Mobile Security Management:* Prohibit Application installation/uninstallation , Maintaining Certificates, Mobile device encryption , anti-virus, KIOSK Mode.

airwatch by vmware

CITRIX XenMobile

[Pierer, M., Mobile device management: Mobility evaluation in small and medium-sized enterprises. Springer, 2016]

Choices for BYOD at client side

S4Lab

- Desktop as a Service (DaaS). E.g. Desktone
  - Some rules are enforceable on desired services.
    - E.g. this file can be accessed by an iPad only in the enterprise not the road.
- Virtual mobile infrastructure (VMI)
  - Remote access to corporate data/services
    - Cloud (e.g. Dropbox, Do you know open source alternative?)
    - Vpn
- OS level protection (isolate corporate data/app)
  - Virtual machines to provide a dual identity device.

An example: Android Enterprise

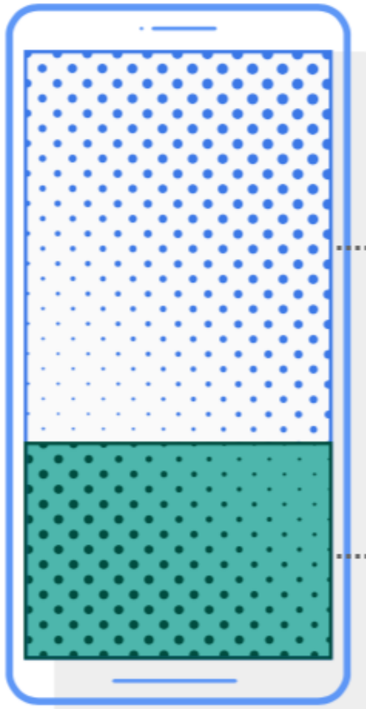
S4Lab

- An Android Enterprise solution is a combination of three components:
  - Your EMM console: A web application you develop that allows IT admins to manage their organization, devices, and apps.
  - Android Device Policy: An app supplied by Android that automatically applies the management policies set in your EMM console to devices.
  - Managed Google Play: Users can only install apps from managed Google Play that their organization approves for them.

[Android Enterprise, Overview, Google, 2021]

Android Enterprise (two profiles)

S4Lab

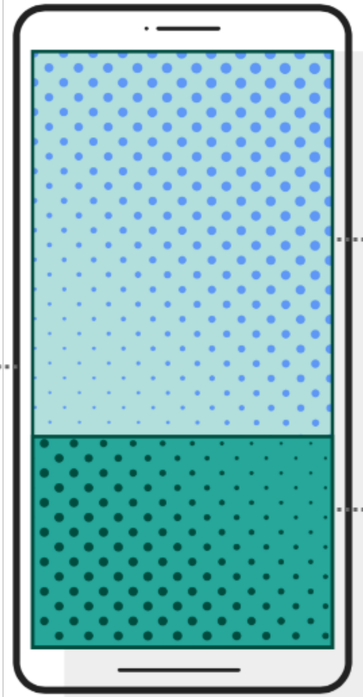


Personal profile
- Contains personal apps & data
- Not visible to organization

Work profile
- Contains work apps & data
- Visible to organization
- Managed by organization

Work profile for employee-owned devices (BYOD)

Organization can enforce most device-wide settings.



Personal profile
- Contains personal apps & data
- Not visible to organization
- Some usage policies can be enforced

Work profile
- Contains work apps & data
- Visible to organization
- Managed by organization

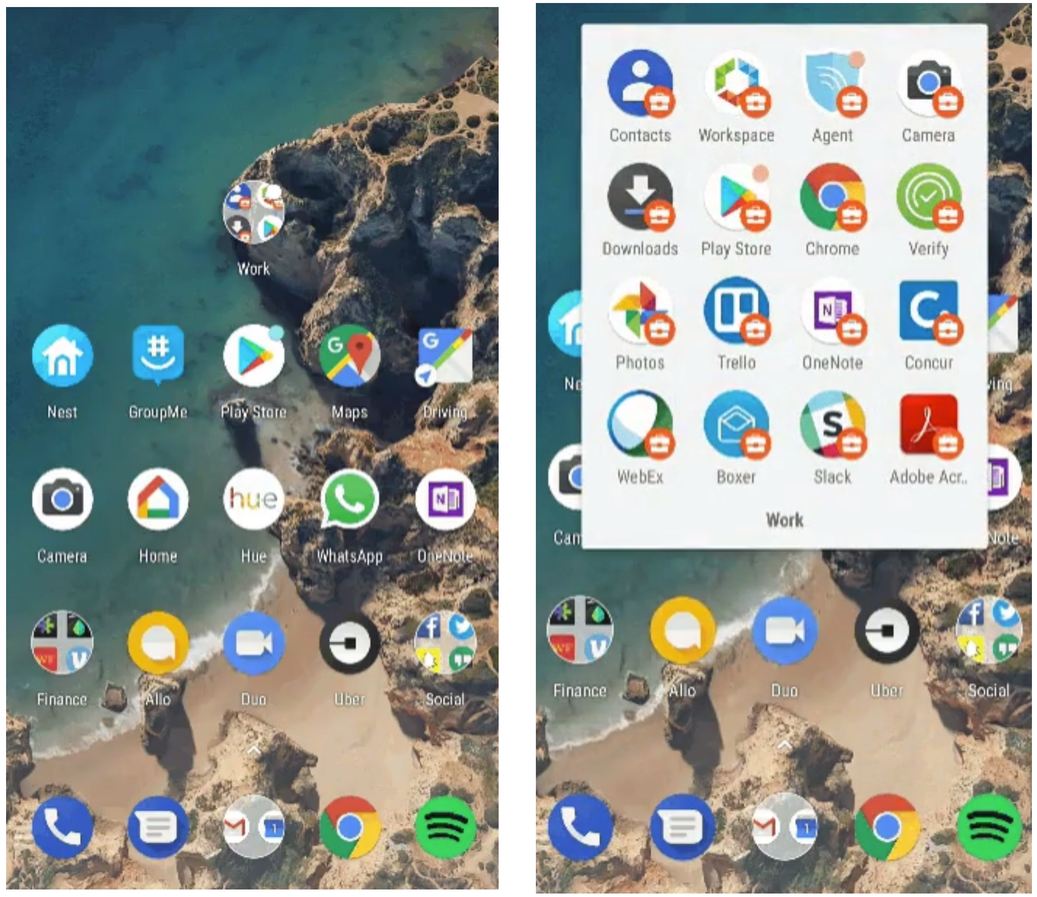
Work profile for mixed-used company-owned devices

[Android Enterprise, Overview, Google, 2021]

Android Enterprise work profile

S4Lab

- OS-level container
- Contains all corporate applications and data and ensures that the data is separated from any personal apps and data a user may have.
- The two profiles run side by side in the home screen of the device, with work apps and notifications badged with a briefcase.
  - You may have Two of the same apps which have different data!
- Separation between a user's personal data and work data is enforced at the OS kernel level across processes, memory, and storage.



[Image:https://blogs.vmware.com]

[Enabling your BYODprogram with theAndroid work profile, Android, 2016]

How policies are applied in Android enterprise?

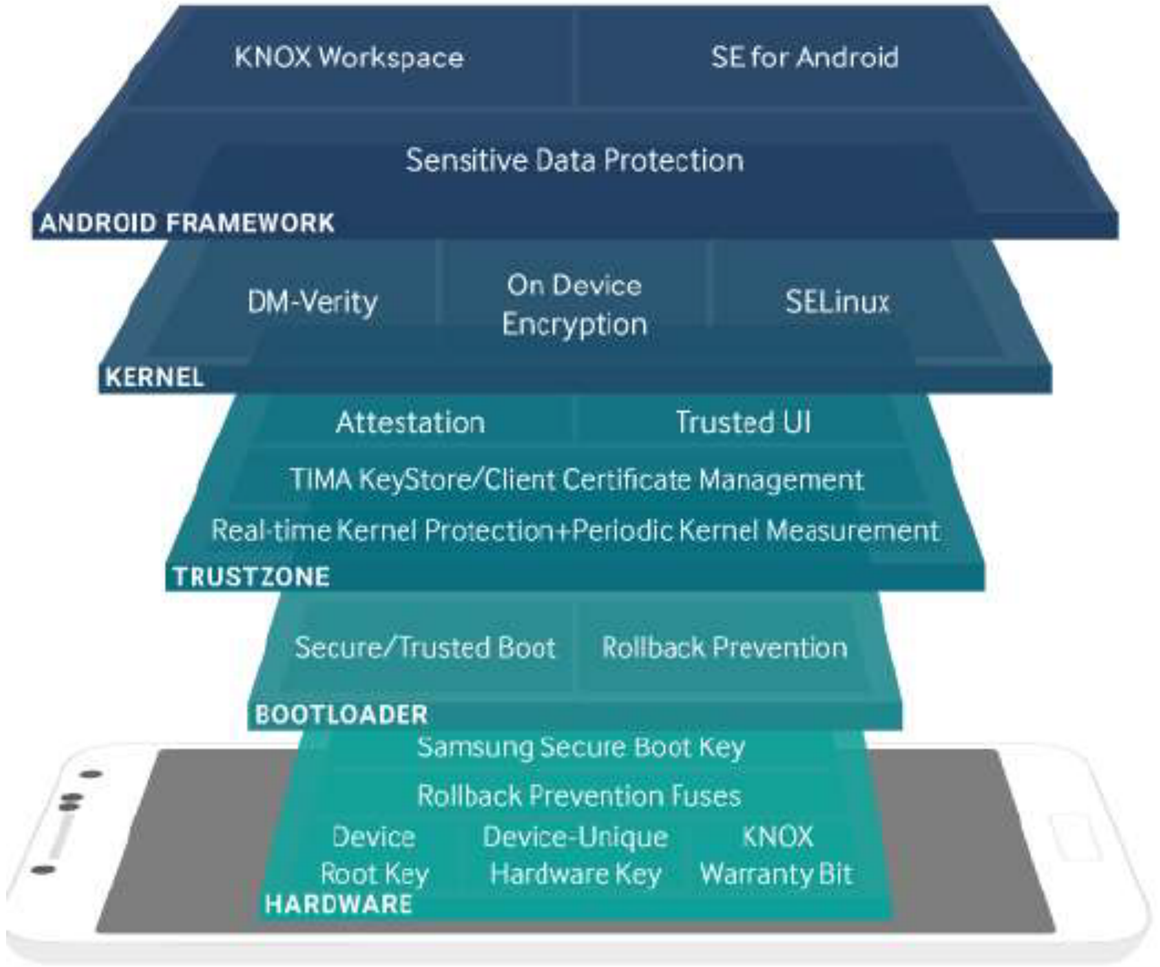
S4Lab

- OS-level access control in Android:
  - SELinux: Security-Enhanced Linux (SELinux) enforces mandatory access control (MAC) over all processes.
  - Seccomp filter: In conjunction with SELinux, Seccomp further restricts access to the kernel by blocking access to certain system calls.
- All Android devices that an organization manages through an EMM console must install a Device Policy Controller (DPC) app during setup.
  - A DPC is an agent that applies the management policies set in an EMM console to devices
- The DPC runs in one of two main modes: Device Owner. Profile Owner

How secure is the Android enterprise?

S4Lab

- Details are different in different implementations.
- Hardware TEE, Secure boot, and etc. can improve the work profile security.
- Not much discussed by security community yet.



[Samsung KnoxTMSecurity Solution, Samsung Research America, 2017]

BYOD at Network Side

Network arch. choices for BYOD (1)

S4Lab

- The Frugal Approach
- Isolating all tablets and smartphone devices to a separate VLAN outside the corporate network.
  - Where the only way to access internal resources is via VPN.
- No specific mobile management capabilities.
- Existing network management solutions to monitor network traffic inside and outside the VLAN to detect suspicious activity .
- Not Optimal but cheap.
  - You lack visibility to discover who are the top bandwidth consumers and track these trends in the long term.

[Three BYOD approaches -- and the budget impact, Ennio Carboni, Network World, 2012]

Network arch. choices for BYOD (2)

S4Lab

- The Big Brother Approach
  - Dedicated mobile management capabilities.
- Best for larger organizations or public companies that must met compliance regulations.
- For example, you can focus on the mobile endpoints and force end users to use a password.
- Another area to explore is encryption of any sensitive data, such as corporate email.
- You can select a SaaS solution that creates a so-called "dual-persona" environment where some apps and data are cordoned off for enterprise use, others for personal use.

[Three BYOD approaches -- and the budget impact, Ennio Carboni, Network World, 2012]

Network arch. choices for BYOD (3)

S4Lab

- The Wireless Pane of Glass Approach
- Managing the underlying wireless infrastructure -- like Cisco and Aruba wireless LANs -- while at the same time understanding who's using their wireless networks and for what purposes.
- Capabilities offered in this space range from live maps of controllers, LWAPs and user devices, to detection of rogue access points or reports on the encryption level and configuration of access points.
- Some solutions can track user activity on wireless networks to the point of spookiness: You can track individual employees or visitors as they move around the building -- how many meetings, where they took place, for how long -- even where they had lunch.

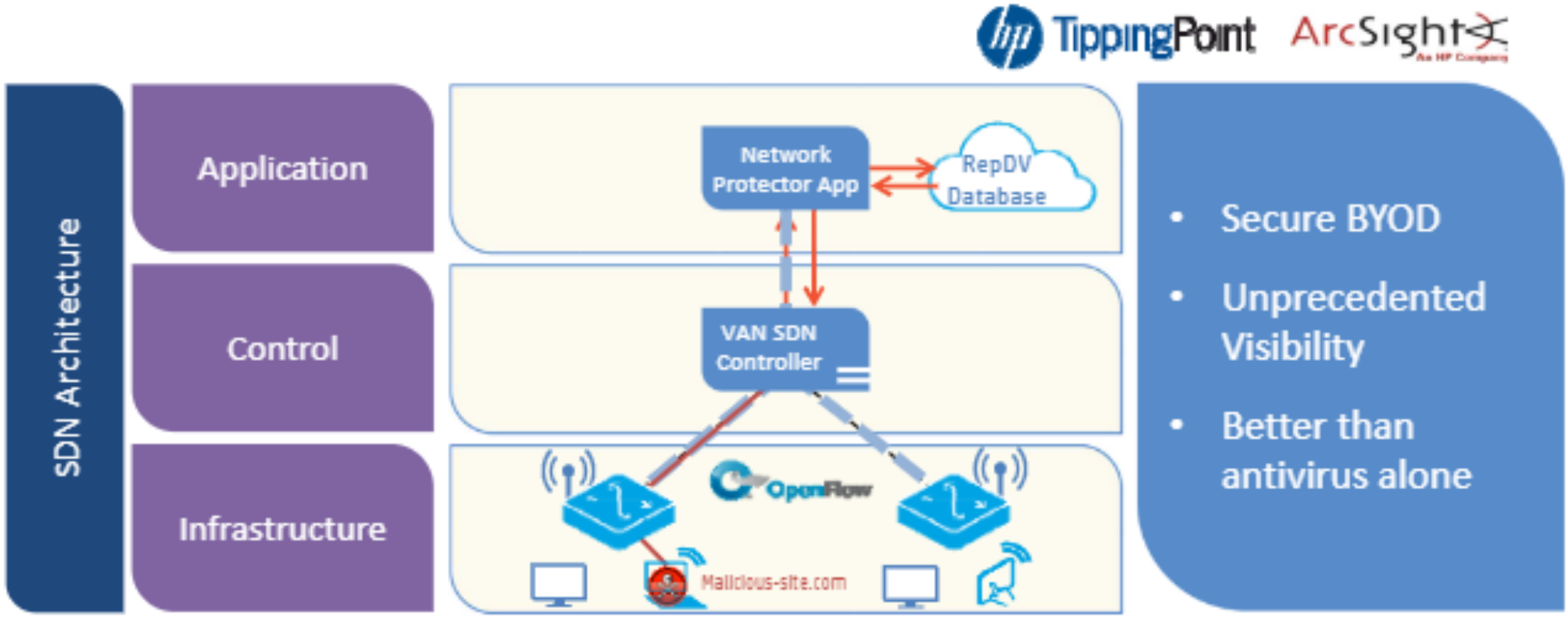
[Three BYOD approaches -- and the budget impact, Ennio Carboni, Network World, 2012]

SDN-based BYOD policies

S4Lab

- SDN idea
  - Decouple control plane (routing decisions) from data plane (networking packets).
  - A network component (SDN controller) is a brain of a network which is the central control plane.
  - Associated with Openflow protocol to communicate with other routers.
- The network does not need to have static architecture.
- Hence best fits for BYOD management.

An example



[Sikkerhet Network Protector SDN app, Leirvik G.A., HP Networking,]

Let’s again consider the costs?

S4Lab

- Is it really cost effective?
- There are hidden costs for the corporate:
  - Device repair/support
  - Security, Management, Data Loss
  - Multi-platform support (requires Unified Endpoint Management like Mobileiron)
  - Multi-department support
- And for the employee:
  - BYOD has become a matter of trust between employee and employer.
    - Should know about the trade-off between the comfortability and some levels of privacy leaks.
    - Lawyer up before signing the BYOD agreement.
  - Some limiting on device selection to be consistent with BYOD policies.

[BYOD Stirs Up Legal Problems, Tom Kaneshige, cio.com, 2012]

Further reading

S4Lab

- Kang, Q., Xue, L., Morrison, A., Tang, Y., Chen, A., & Luo, X. Programmable In-Network Security for Context-aware {BYOD} Policies. In 29th USENIX Security Symposium, 2020

QA