Enhanced User Authentication with UAuth

Risk Management & Push Notification in a Single Sign-On Environment

Agenda

- MFA - Why ?
- UAuth - Push Notifications
- Risk Management

Multi-Factor Authentication (MFA)

- **Widely adopted** security mechanism
- Multiple Layers of Authentication
- **Prevention** of Phishing - Stolen passwords

Methods

- Already existing methods of MFA in Universities’ SSO
    - OTP (One Time Password) via SMS
    - TOTP (Time-based One Time Password)

Methods

- Already existing methods of MFA in Universities’ SSO
  - OTP (One Time Password) via SMS
  - TOTP (Time-based One Time Password)
- **New Method**
  - **UAuth Push Notification App by GUnet**

Methods - UAuth

- Advantages of Push Notification over SMS / TOTP
  - **More Secure**, eIDAS higher level of assurance
  - **User familiarity**
  - **User friendly**
  - **Cost-free**

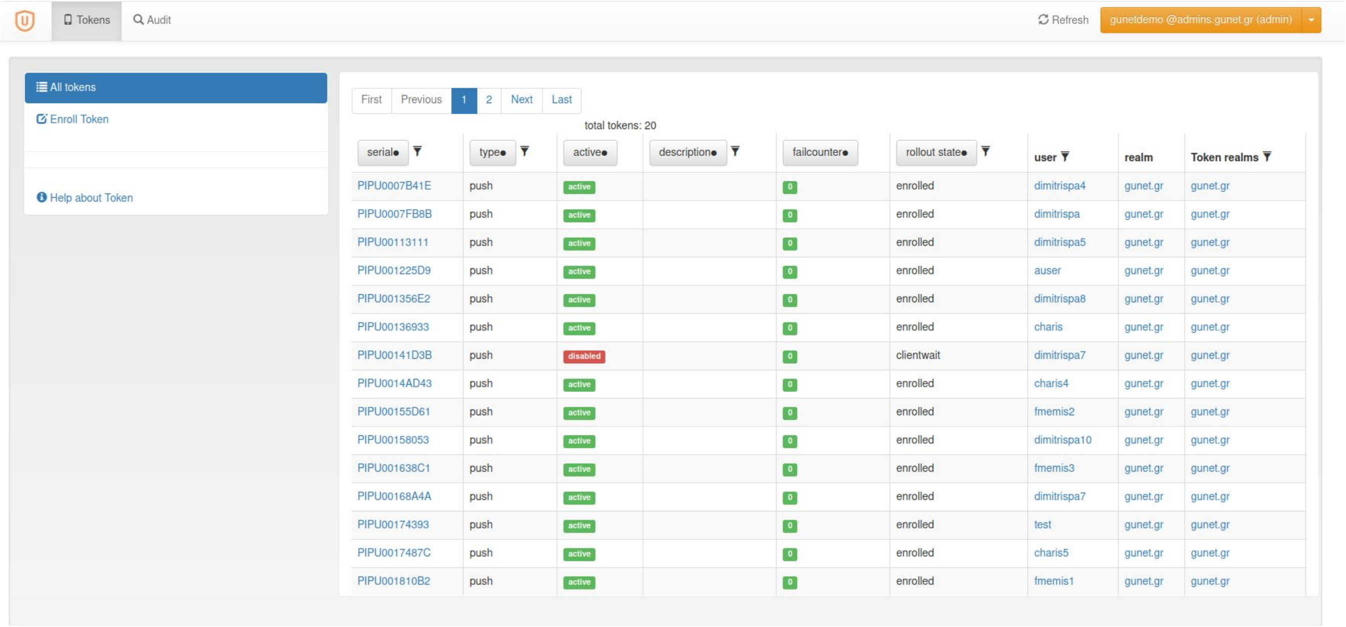
LIVE DEMO

Prerequisites

- **Mobile Device Dependency**
  - Requires smartphone devices

- **Reliance on Mobile Networks**
  - Functionality dependent on the availability and stability of mobile networks

UAuth Admin Panel



total tokens: 20

serial●	type●	active●	description●	failcounter●	rollout state●	user	realm	Token realms
PIPU0007B41E	push	active		0	enrolled	dimitrispa4	gunet.gr	gunet.gr
PIPU0007FB8B	push	active		0	enrolled	dimitrispa	gunet.gr	gunet.gr
PIPU00113111	push	active		0	enrolled	dimitrispa5	gunet.gr	gunet.gr
PIPU001225D9	push	active		0	enrolled	auser	gunet.gr	gunet.gr
PIPU001356E2	push	active		0	enrolled	dimitrispa8	gunet.gr	gunet.gr
PIPU00136933	push	active		0	enrolled	charis	gunet.gr	gunet.gr
PIPU00141D3B	push	disabled		0	clientwait	dimitrispa7	gunet.gr	gunet.gr
PIPU0014AD43	push	active		0	enrolled	charis4	gunet.gr	gunet.gr
PIPU00155D61	push	active		0	enrolled	fmemis2	gunet.gr	gunet.gr
PIPU00158053	push	active		0	enrolled	dimitrispa10	gunet.gr	gunet.gr
PIPU001638C1	push	active		0	enrolled	fmemis3	gunet.gr	gunet.gr
PIPU00168A4A	push	active		0	enrolled	dimitrispa7	gunet.gr	gunet.gr
PIPU00174393	push	active		0	enrolled	test	gunet.gr	gunet.gr
PIPU0017487C	push	active		0	enrolled	charis5	gunet.gr	gunet.gr
PIPU001810B2	push	active		0	enrolled	fmemis1	gunet.gr	gunet.gr

Risk Management in SSO

MFA protection

What is SSO Risk Management ?

Detection of unusual activities

Sign-ins from **unfamiliar** IP addresses, suspicious user agents, or **unexpected** countries, and taking necessary actions to prevent security breaches

Actions

1. Blocking Login

2. Triggering MFA

Login Throttling

Throttling Based on Failed Logins

- Time window in which capacity can be allowed
- Refill Strategy
  - Greedy
  - Intervally
- IP - Limit from the same IP address.
- IP and username - Limit a specific user from the same IP address.

Predefined Mfa Triggers

Day/Time

- Trigger mfa before and after a specific hour.
- Specific Days of the week

Location - Maxmind database

- Custom Rules on specific geographical parameters
  - **cities and countries**

Custom Scenario

Custom solutions

e.g. specific account types in **LDAP**, official unit or individual

Case Study: SCH

Enabling multi-factor authentication (MFA) for specified services operating outside of Greece is a strategic security move.

Event-based Risk Management

- Detection of suspicious authentication requests based on user behavior and **collected authentication events**.
- Authentication attempts are evaluated against configurable **criteria and a risk threshold**.
- **Risk calculators** analyze past events to calculate risk scores based on IP address, browser user agent, geolocation, and date/time.

Risk Calculators ½

Date Time Risk Calculator

- Counts the number of authentication events within a time window around the current timestamp. The greater the concentration of events within this time period, the lower the overall risk.

GeoLocation Risk Calculator

- Counts the number of authentication events from the same geographical location. If a higher percentage of events originate from the same location, the risk score should be reduced.

Risk Calculators 2/2

IP Address Risk Calculator

- Counts the number of authentication events from the same IP address. As the number of events from a specific IP address increases, risk levels are lowered.

UserAgent Risk Calculator

- Counts the number of authentication events initiated from the same user agent. When a specific user agent is used more frequently, it also leads to a decrease in the risk score.

Event-based Risk Management

- Mitigation actions can be taken if the risk exceeds the **threshold**.
- Mitigation options include **blocking authentication** or enforcing **multifactor authentication.**
- Authentication attempts, evaluations, and mitigations are logged for audit purposes.
- Contingency plans can **notify** the principal and deployer via **email** and **SMS**.

IP Intelligence

CAS provides access to third party services who enable examinations of the client IP address and decide **whether access should be granted**.

Third Party Service Subscription

Given an IP address, the system will return a probabilistic value (between a value of 0 and 1) of how likely the IP is a VPN / proxy / hosting / bad IP.

By employing machine learning and probability theory techniques, the system perform dynamic checks on large datasets.

Thank You!