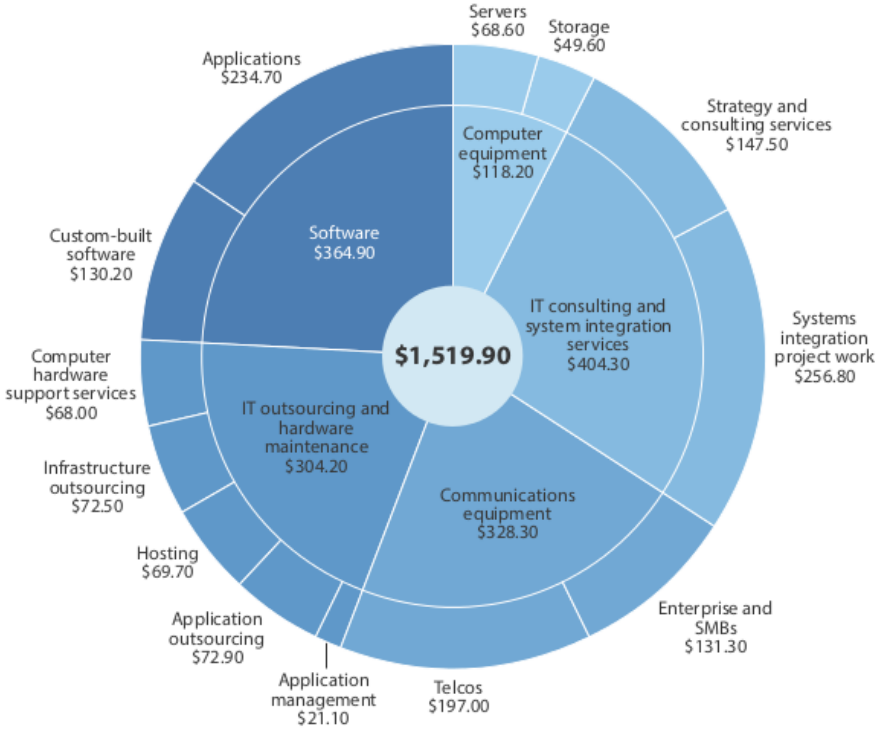
Two Factor Authentication: Security in an Age of Zero Trust

Jon Oberheide, CTO, Duo Security

Not-so-surprising trends

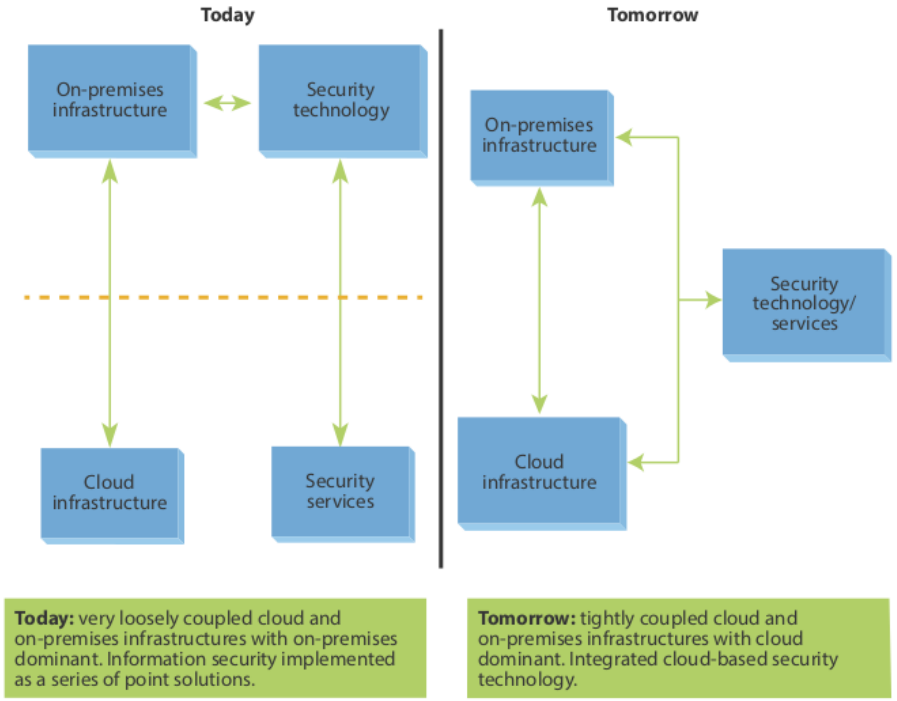
- Cloud
  - 1.5 trillion in IT spending
  - 2009: 3% implemented, 9% planning
  - 2013: 36% implemented, 46% planning
- Mobile
  - BYOD: > 286 million workers
  - >83% chose their own device



Source: January 3, 2013, "Global Tech Market Outlook 2013 To 2014" Forrester report

Changes in IT infrastructure

- Cloud
  - On-prem no more
  - No app, server, infra control
- Mobile
  - Unmanaged devices
  - Heterogeneous platforms, networks, and access



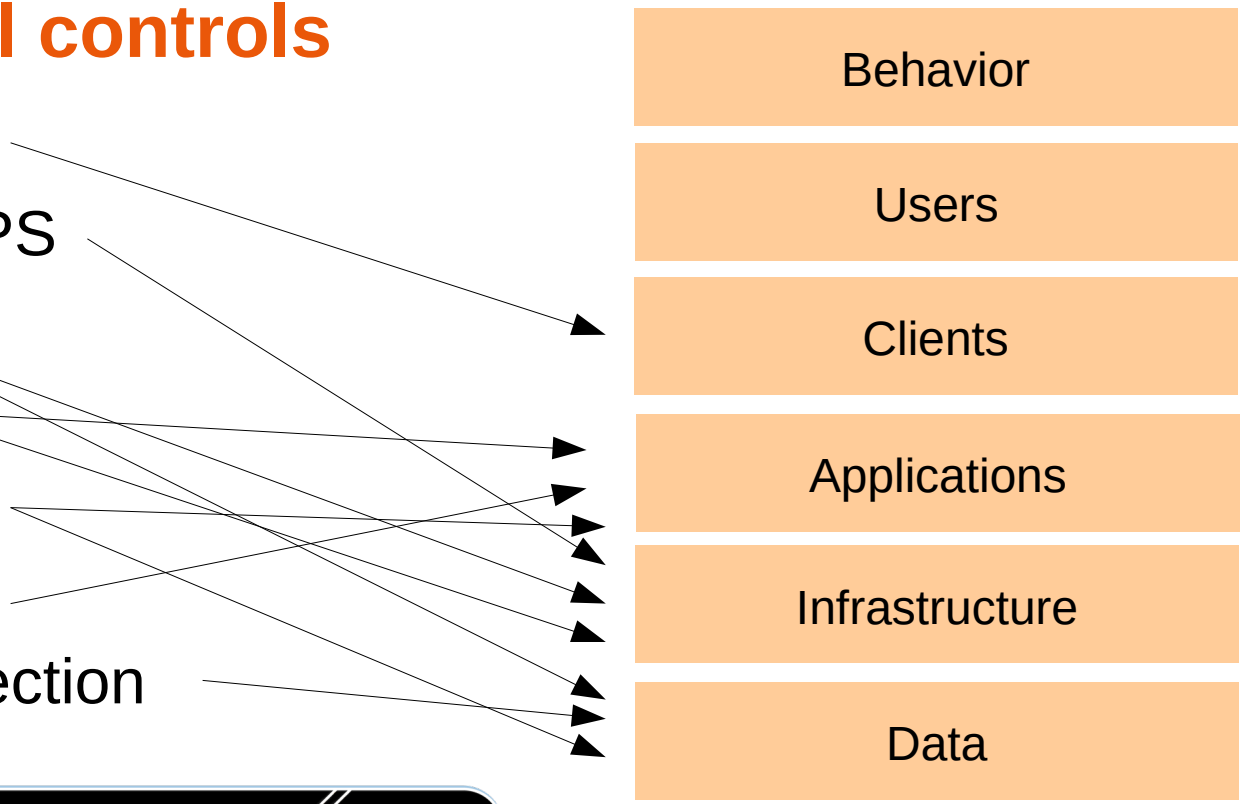
A “Zero Trust” architecture

- Forrester hinted at this with “zero trust” architecture
  - Access from anyone, anywhere, anyhow
- De-perimeterisation of clients, networks, and services
- Loss of infrastructure control
- Reduced visibility and interposition

^ Key elements of effective security controls have vanished ^

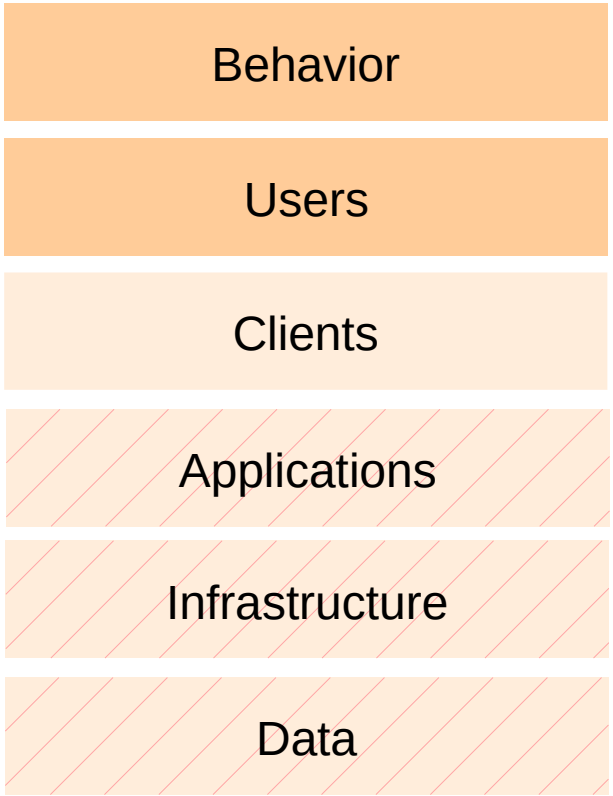
Traditional controls

- AV/HIDS
- FW/IDS/IPS
- DLP
- WAF
- SIM/SEM
- DB/DAM
- Data protection

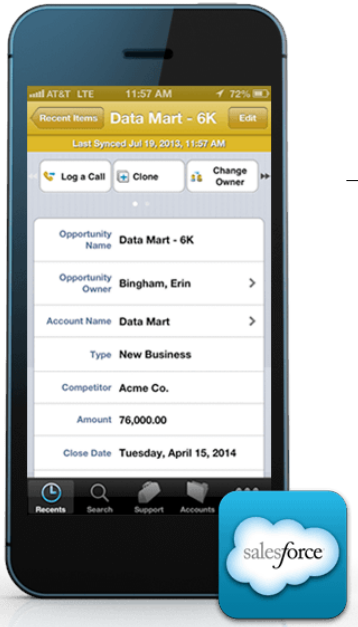


The Zero Trust stack

- With cloud/mobile, we lose the bottom half of the stack
- Data, infrastructure, apps
  - Implemented, maintained by third-party provider
- Clients
  - Unmanaged, roaming, locked mobile endpoints



Challenge: SalesForce on mobile



How do YOU protect this environment with security controls?

Techniques that won't work

- Backhaul/proxy model
  - Push down cert (MITM), cert pinning
- App instrumentation
  - Re-writing to disable pinning, MAM is a mess
- Most everything else
  - Eg. You can't ask SF to export NetFlow to your prem

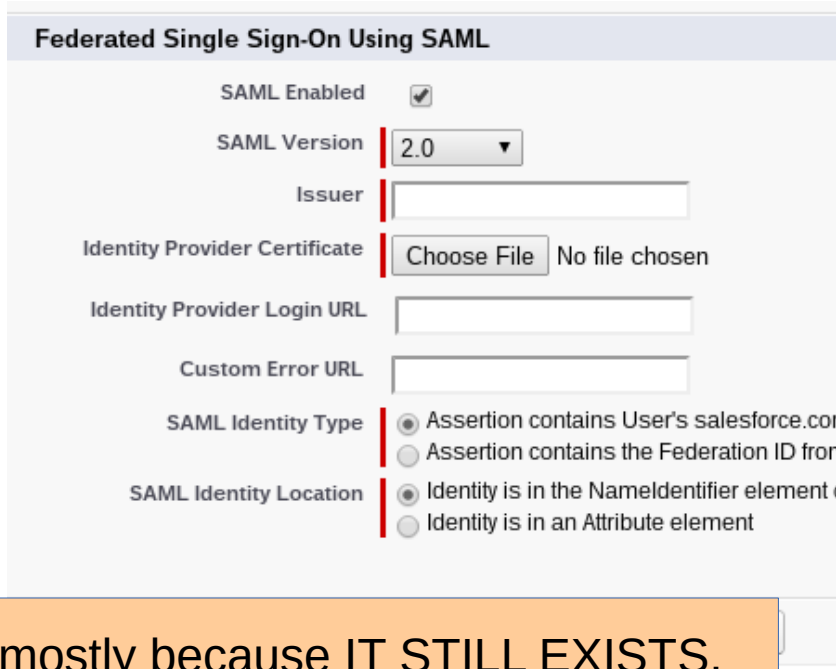
These approaches are fighting ***against*** security!

Techniques that *might* work

- Identity as a security control
  - Strong authentication and access control
  - Who, what, when, where, why how accesses your data
- Why identity?
  - Interposition
  - Survivable
  - Threat mitigation

Interposition

- Security depends on interposition and visibility
- Interposition depends on compatibility, interoperability, standards
- SF: SAML delegation to IdP



Identity is a key interposition point...mostly because IT STILL EXISTS.

Survivability

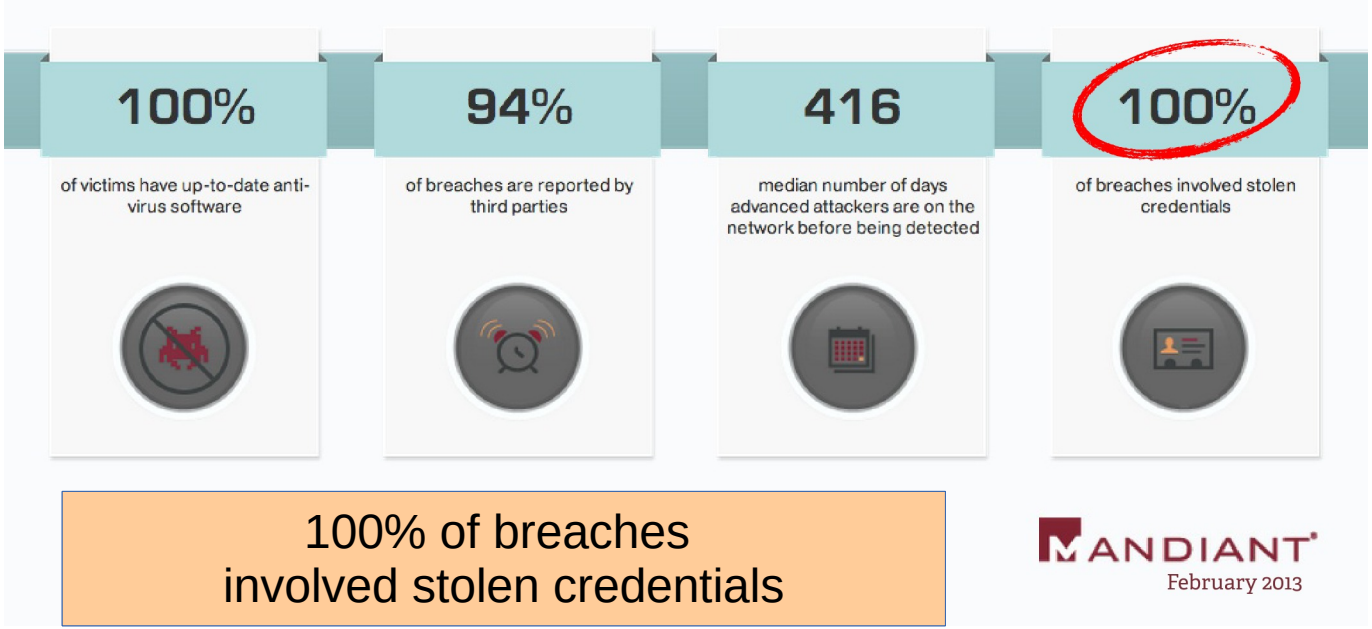
- Other controls evaporated, what about identity?
- Service-owned identity
  - User identity is a PITA to outsource
- User-owned identity (BOYI)
  - Maybe some day?
- Migration towards ***more*** interoperability
  - For current enterprise SaaS: SAML or die.

Threat mitigation

	Attacker			Defender
	Access	**Control**	**Technique**	**Response**
Remote	App/Server	*Passive/Offline*	Guess/SQLi	Password hashing, Password proof, Weak Biometric
	Database		Crack	
	Network		Sniff	
	Conversation		Phish/Forge	One-Time Passwords
		Active/Online	MITM	PKI/Strong Biometric
	Endpoint		Trojan/Keylog	Out-of-Band Call/SMS
		Real-Time	Sidejack/MITB	Anomaly Detection
	Transaction	*Persistent*	Modify	Transaction Verification
User	Multi-channel	*Coordinated*	MITMobile	Fraud Detection/RBA

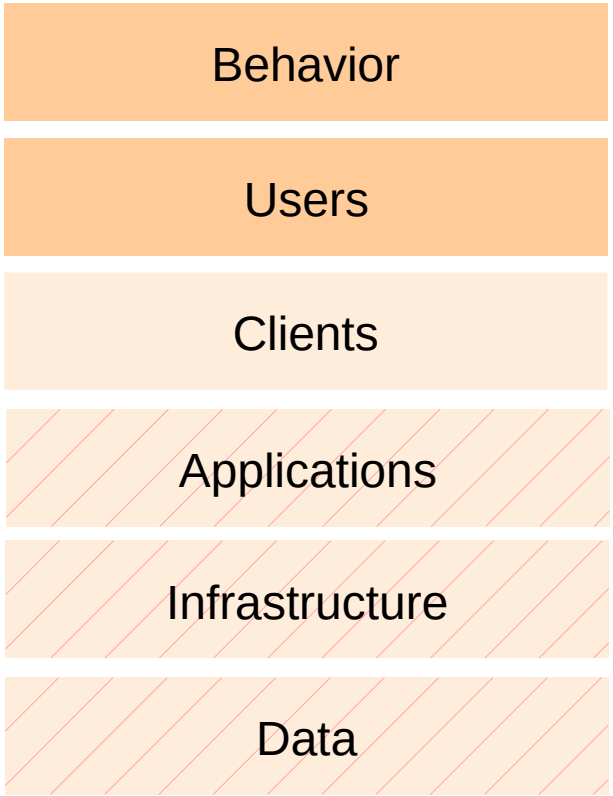
The evolution of threats towards users has driven new authentication requirements

Stolen credentials



Mapping identity on the stack

- How does identity provide control at upper layers of the stack?
  - User identities
  - Client devices
  - User behaviors
- How can we mitigate the threats with such a limited wedge into applications?



Securing users

- User authentication is our primary wedge
- Strong authentication → two-factor

Best way to authenticate logins or transactions:
ask the users themselves!

- Leveraging smartphones can increase security AND usability of two-factor
- BONUS: tangible control for users

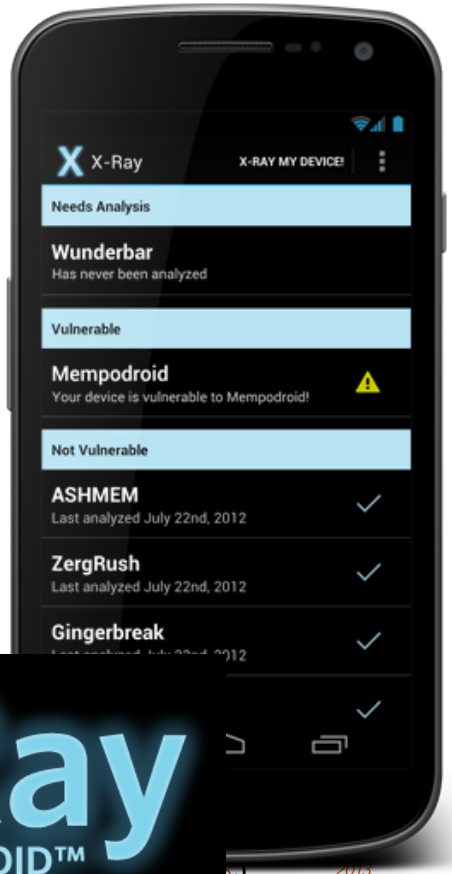
Securing clients

- Mobile devices as trusted authenticators
  - Mobile security, eh?
- Protecting unmanaged, locked devices is non-trivial
- On-going research projects at Duo
  - X-Ray vuln assessment
  - ReKey “Master Key” hot-patching
  - Hardware-backed credentials on mobile devices

Assessing mobile vulnerabilities

- First mobile vulnerability assessment tool
- Scan for privesc vulns on Android devices that go unpatched for months & years
- United 2012: > 50% devices vulnerable

http://xray.io

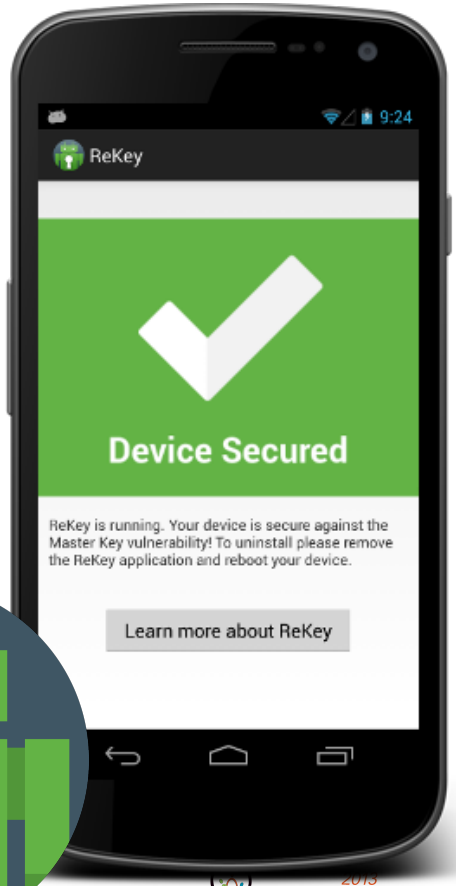


X-Ray FOR ANDROID™

Hot-patching mobile vulnerabilities

- Android “Master Key” vulnerabilities
- Affected over 99.9% of Android devices
- ReKey hot-patches the vulns in-memory without Google, OEMs, carriers

http://rekey.io



Hardware-backed credentials

- HSM/SE/TEE/TrustZone/M-Shield
  - Acronym soup!
- Smartcard in your smartphone
  - Crypto engine, tamper-proof key store, etc
- Unclonable credential
  - Even if phone is completely rooted!

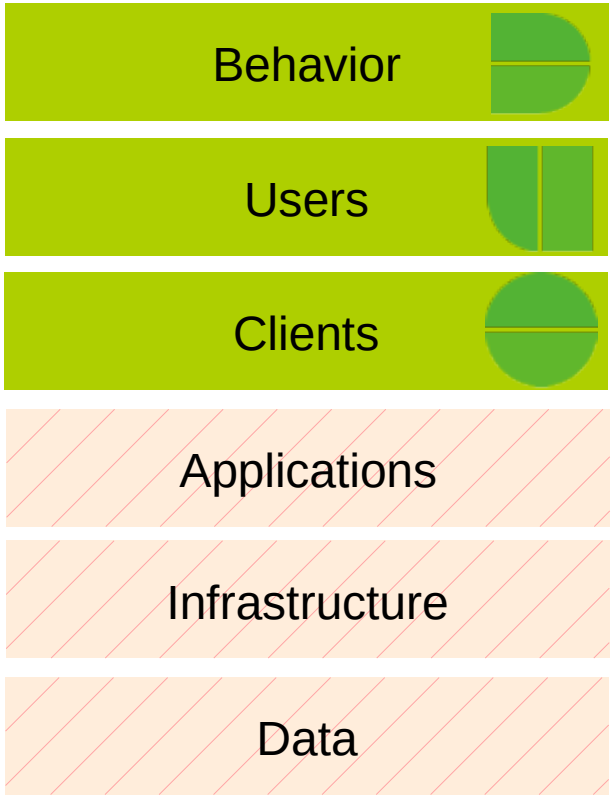
Google wallet

Analyzing behaviors

- We can have ***strong*** device-based identity
  - But...security is never infallible
- User behaviors provide a higher-order analysis target
- Anomaly detection and behavioral controls
  - Geofencing
  - Geo-impossible logins
  - Account sharing
  - Multi-account credential theft

Future: a bigger, better wedge?

- Reintroducing security controls into your cloud infrastructure and apps
  - Delivered via identity control plane
- Standardization and interop are key to success (yikes!)
  - A common “wedge” across services
  - XACML, CloudAuthZ, OAuth, UMA, ???



Thanks!

Jon Oberheide
Duo Security
jono@duosecurity.com
@jonoberheide / @duosec