Authentication Without Keys for Users And 'Things'

November 2017
Authentication today is a conflict of security and user experience
Today’s Authentication Factors

User dependent, Theft-prone Secret Single Point of Weakness

- USER/PASSWORD
- SMS
- TOKENS
- BIOMETRICS
Who's behind the breaches?

- 75% perpetrated by outsiders.
- 25% involved internal actors.
- 18% conducted by state-affiliated actors.
- 3% featured multiple parties.
- 2% involved partners.
- 51% involved organized criminal groups.

What tactics do they use?

- 62% of breaches featured hacking.
- 51% over half of breaches included malware.
- 81% of hacking-related breaches leveraged either stolen and/or weak passwords.
- 43% were social attacks.
- 14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.
- 8% Physical actions were present in 8% of breaches.
MFA Traditional Approach - OTP Over SMS

- Complex user experience
- SMS = single point of failure for security
- Browser MITM
“SMS is deprecated, and may no longer be allowed in future releases of this guidance.”

Digital Authentication Guidelines – March 2017
MFA Traditional Approach - OTP using Soft Token

- Complex user experience
- Theft-prone seed (server/end-point)
- Browser MITM
...Biometrics SHALL be used with another authentication factor (something you know or something you have).”

“Biometric False Match Rates (FMR) and False Non-Match Rates (FNMR) do not provide confidence in the authentication of the subscriber by themselves....

Digital Authentication Guidelines – March 2017
Octopus Authenticator

Turning the mobile device into the authentication factor of the future
Originally used to prevent accidental or malicious launch of nuclear weapons
Secret Sharing Scheme

“Distribute **Secret** into **N** useless shares so that any **K** shares can reconstruct it”

Based on proven crypto: established in 1979 separately by A. Shamir, G. Blakley

“...these cryptosystems are considered **cryptanalytically unbreakable.**”

Wikipedia/Information-theoretic-security
Example:

Secret = 3
N = 4
K = 2

Select random linear line that crosses the Y axis @ number 3
Generate 4 random points on the selected line
Exposing a single point → infinite line possibilities → useless
Any two points together expose the secret
Device authentication - no single point of security failure

- SSL (Pinned)
- PUSH
- SECURE MEMORY
- OTHER

No SMS, no tokens, not even passwords
Octopus Authenticator - Multi-shield protection

- No need to type anything
- Multiple routes with independent protection

Login (no password) / Transaction

Authenticated

Trust & Encryption

OK!

Octopus Authentication Server

OK!

salesforce
VPN
Office 365

APPROVE?

YES  NO

ACCEPT?
Password-free Active Directory Authentication

Windows Login
Outlook Web App
Office 365
Email Native Client

Octopus Servers
Active Directory
Password-free Active Directory

Octopus Authentication Server

Authentication
- Device factor
- User factor

Temporary password

Active Directory

Windows Login
User: user@domain.com

Temporary password
Octopus Authenticator

› One solution fits all
› Seamless user experience
› Ultra Security - No single point of failure
› User independent
› Scalable - “0” false positives
› Reduce TCO (CAPEX & OPEX, support)
Gartner
Cool Vendor 2016

Top 5 cyber security innovators 2016

citibank

Distribution Agreement
21 countries in Europe

TechData
June 2017

Global Partnership (JBR)
Game changer FinTech
157 countries Globally

pwc
July 2017

Gartner’s recommended IoT security platform

Some Selected Partners

AIRBUS
DEFENCE & SPACE

WIND

BAYSHORE

DEVICE AUTHORITY
IoT Security Simplified

SECRET DOUBLE OCTOPUS

Boeing

TD Bank

bank hapoalim

© 2017 Secret Double Octopus | All Rights Reserved
We’re a Multi-Disciplinary Team of Veterans

Raz Rafaeli
CEO

Prof. Shlomi Dolev
CSO

Dr. Shimrit Tzur
CTO

Chen Tetelman
VP R&D

Amit Rahav
VP Marketing & BD

Amit Lavi
VP Product

With over 100 Years Combined Experience

Backed by Top Global Investors
Thank You!

www.doubleoctopus.com