

EECS 3482

Introduction to Computer Security

Risk Based Authentication (RBA)

Learning Objectives



By the end of this presentation, you should be able to:

- Understand what RBA is and why it was introduced
- Know how RBA works
- Understand the balance between Fraud-mitigation and User convenience



Why was RBA introduced?

50 million Evernote users forced to change passwords³

The Financial Times' Twitter account attacked⁴

The Guardian reports on intelligence leaked by Edward Snowden⁵

CNN's, The Washington Post's and *The New York Times'* Twitter accounts hijacked⁶

5 million Gmail usernames, passwords hacked and posted to Russian Bitcoin forum⁷

Hackers breach security of HealthCare.gov⁸

EBay asks 145 million users to change passwords after cyber attack⁹

Hackers steal more than \$1 million from 1,600 StubHub users¹⁰

Russian crime ring amasses over a billion stolen Internet credentials¹¹

³2014, Data Breach Investigations Report, Verizon. ⁴ibid. ⁵ibid. ⁶ibid. ⁷5 Million Gmail Usernames, Passwords Hacked and Posted to Russian Bitcoin Forum: Report, Stone, Jeff, International Business Times, September 10, 2014. ⁸Hackers Breach Security of HealthCare.gov, Pear Robert Perlooth, Nicole, The New York Times, September 4, 2014. ⁹EBay Asks 145 Million Users to Change Passwords After Cyber Attack, Charlotte, Soham, Finkle, Jim, Mass, Labor Politics, May, 2014. ¹⁰Here's How Hackers Stole Over \$1 Million From 1,600 StubHub Users, Fitzell, Sam, Time Magazine, July, 2014. ¹¹Russian Hackers Amass Over a Billion Internet Passwords, Gelles, David, Perlooth, Nicole, The New York Times, August 5, 2014.

What is RBA?

An **Authentication system** that takes into account the **profile** of the agent requesting access to the system to determine the **risk**



Recall:

C.I.A. of Information Security

- **C.I.A. Triangle** - 3 key characteristics of information that must be protected by information security:

- ◆ **confidentiality** - only authorized parties can view private information
- ◆ **integrity** - information is changed only in a specified and authorized manner
- ◆ **availability** - information is accessible to authorized users whenever needed



But why are our passwords susceptible to hacking?

Weak Passwords: (bad Policy)

A **password policy** is a set of rules designed to enhance computer security by encouraging users to employ strong **passwords** and use them properly.

▼  **Change Password**

* Old password

New password

Confirm new password

▼ **Password Policy**

- Password must not match or contain first name.
- Password must not match or contain last name.
- Password must contain at least 2 alphabetic character(s).
- Password must be at least 6 character(s) long.
- Password must contain at least 1 lowercase letter(s).
- Password must contain at least 1 numeric character(s).
- Password must contain at least 1 uppercase letter(s).
- Password must start with an alphabetic character.
- Password must not match or contain user ID.

But why are our passwords susceptible to hacking? (cont'd)

Weak Passwords: (bad Policy)

By using a dictionary attack of the most used passwords, the hacker can easily break the password hash.

Look familiar?

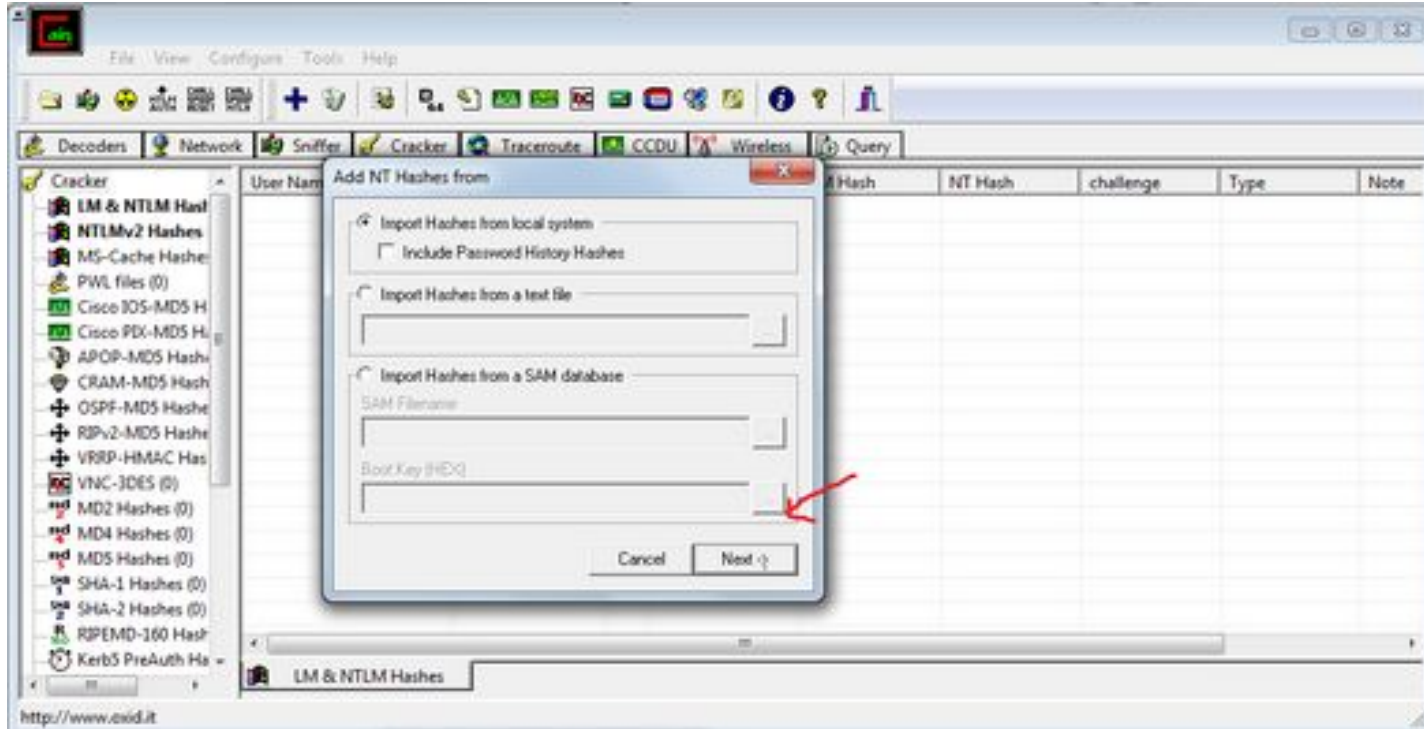
These are the top 10 most commonly used passwords of 2013:

1. 123456
2. password
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123

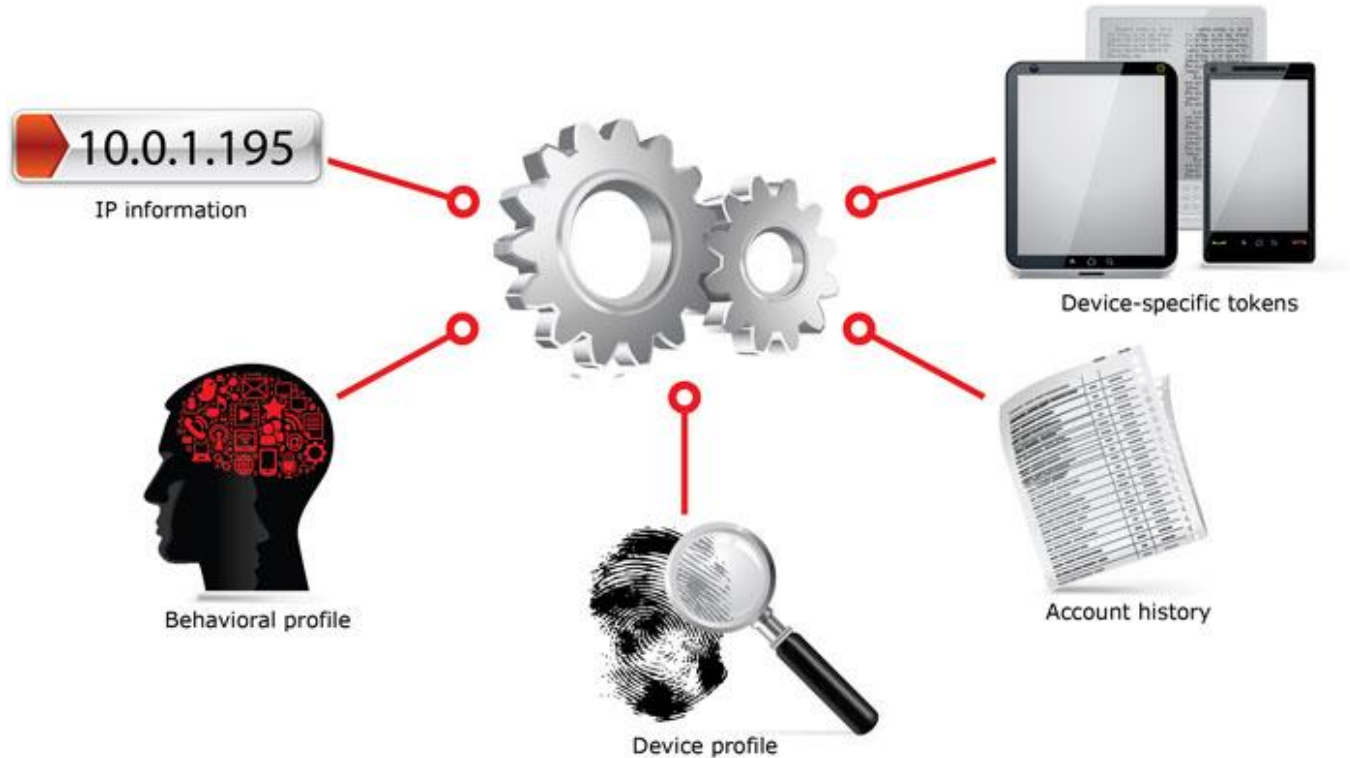
Source: Splash Data, 2014.

But why are our passwords susceptible to hacking? (cont'd)

Password Hash File



Factors for Profile Compilation



Authentication Methods



Something you know



Something you have



Something you are



Authentication Methods



Where you are



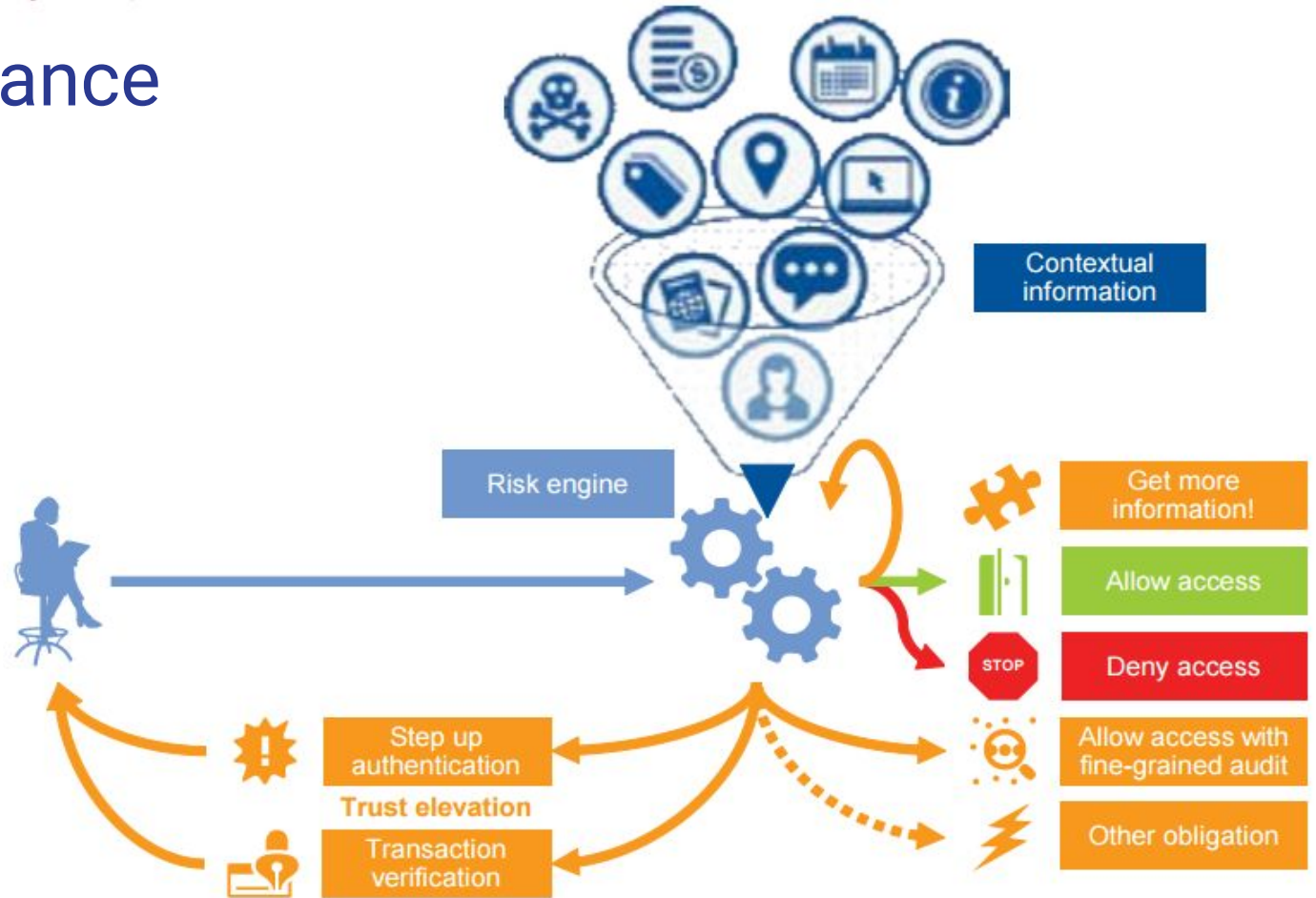
Who you know



What you're doing



RBA at a Glance



Risk Engine: Determining Risk



Where is the user?



Which system or device is being used?

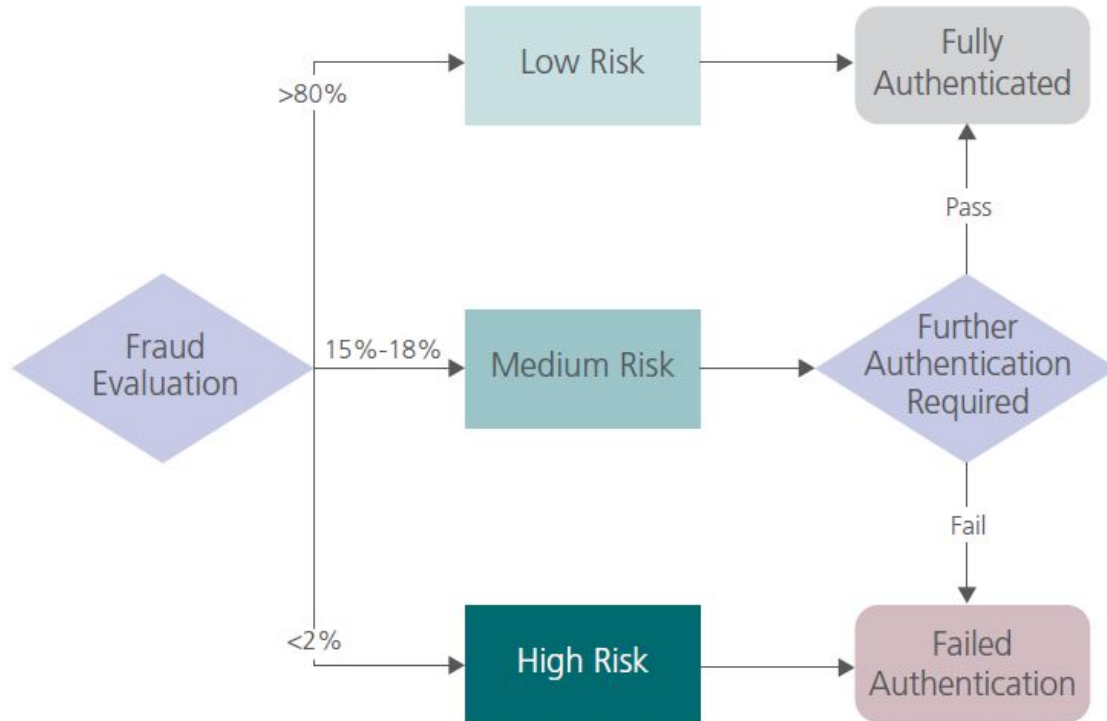


What is the user trying to do?



Is the user's behavior consistent?

Risk Engine: Risk Assessment



RBA Use Case: Scenario 1

Scenario 1

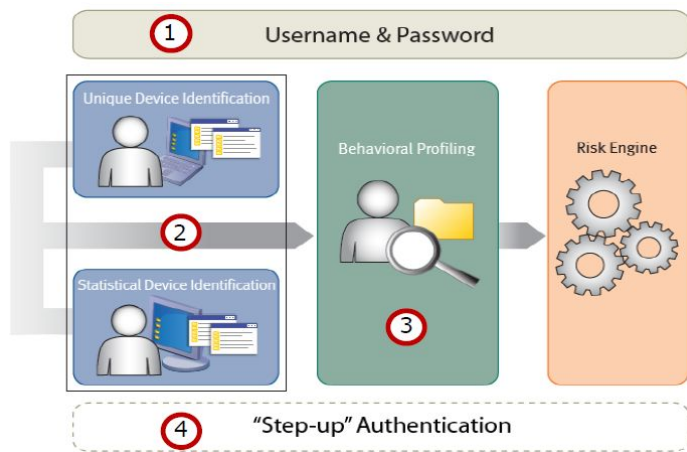


Legitimate employee attempts to log in to access corporate data from office in Toronto using a work laptop at 9:00 a.m. EST

Risk-based authentication analyzes:

User ID Password Device Fingerprint Location Geo-velocity IP Address Login History

Traditional Pattern



RBA Use Case: Scenario 2

Scenario 2










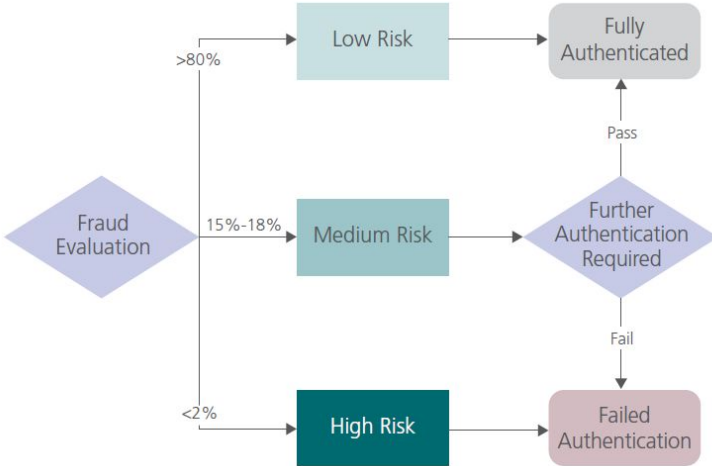
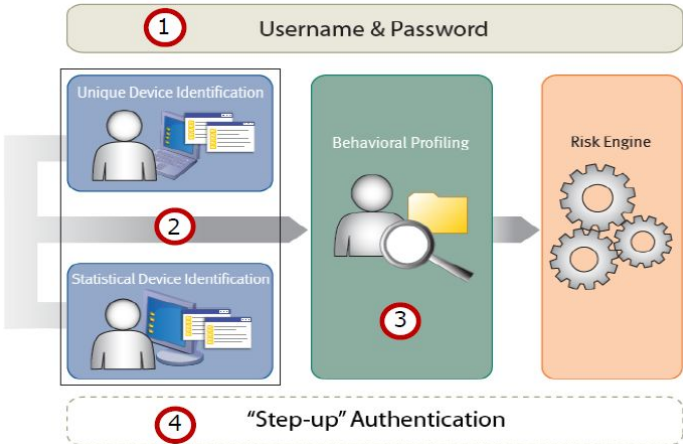
Legitimate employee attempts to log into corporate email in New York on a smartphone at 8:30 p.m. EST

Risk-based authentication analyzes:

User ID Password Device Fingerprint Location Geo-velocity IP Address Login History


Traditional Pattern

						
Valid	Valid	Recognized device associated with user	Not normal location, but near enough geographically	Distance traveled appropriate for user's last login time	Valid	During abnormal working hours



RBA Use Case: Scenario 3

Scenario 3



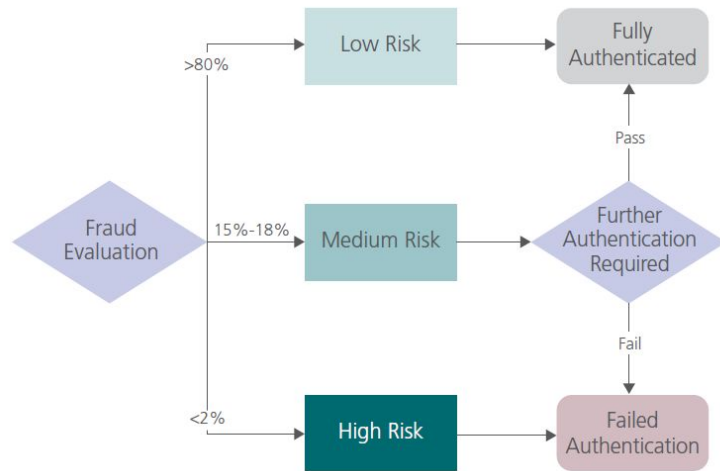
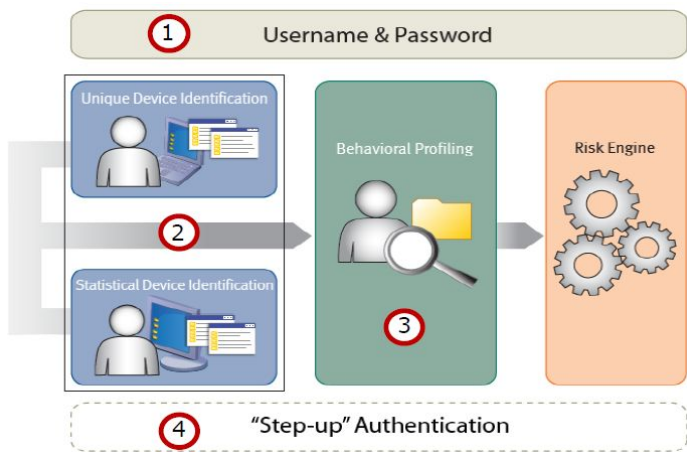
Attacker attempts to log in to access corporate data from the Philippines using a computer at 2:30 a.m. EST


Risk-based authentication analyzes:

User ID Password Device Fingerprint Location Geo-velocity IP Address Login History

Traditional Pattern

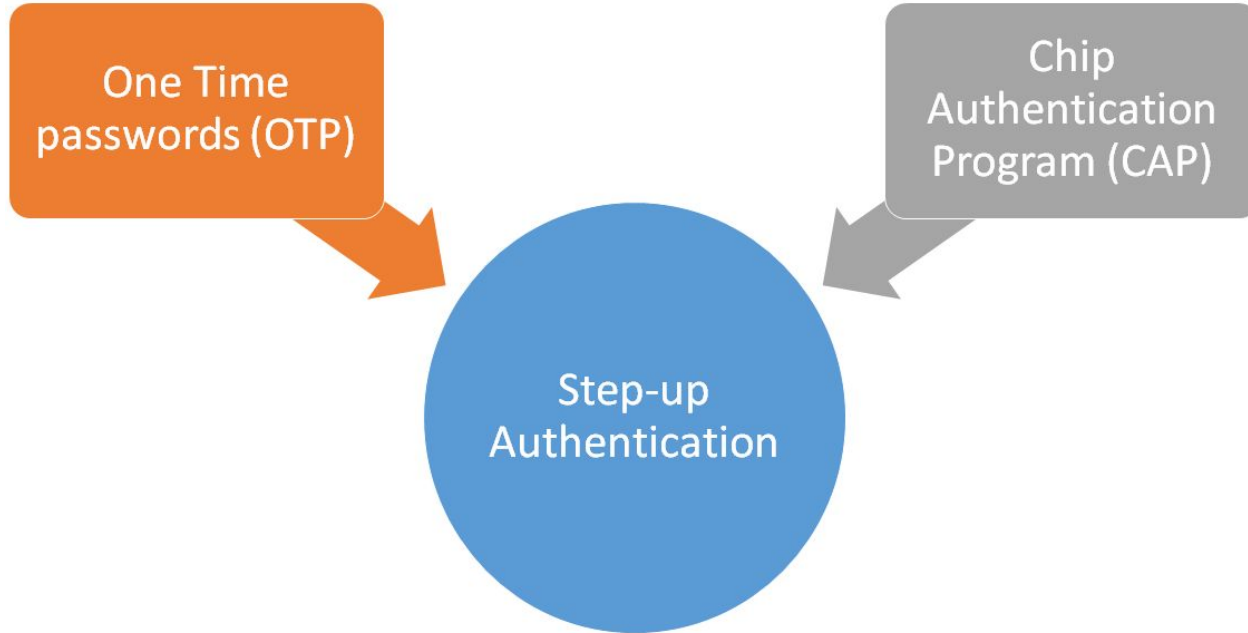
						
Valid	Valid	Unknown device, no association to user	Abnormal Location and not near to standard location	Distance travel inappropriate for user's last login time	Valid	During very abnormal working hours





By determining risk, the system
minimizes the false positive and false
negative transactions

“Step-up” Authentication



One Time Passwords (OTP)



OTP
one time password



OTP Example



Verify it's you

To sign in to your Google Account, choose a task from the list below.



Get a text message with a verification code at (•••) •••••45 >



Get a phone call with a verification code at (•••) •••••45 >



Ask Google for help getting back into your account >

ittbyan@gmail.com

[Use a different account](#)





Verify it's you

There's something unusual about how you're signing in. To show that it's really you, complete the task below.



Enter a verification code

A text message with a verification code was just sent to **(...)****45**

Done



WIND Home 10:10 PM 45%

[Back](#) +1 (716) 274-0398 [Details](#)

Text Message
Today 10:10 PM

G-356893 is your
Google verification code.



Text Message

Send

← Recently used devices



Notice anything suspicious? [Secure your account](#)



Windows

Toronto, ON, Canada **CURRENT DEVICE**



Windows

Moldova - 2 minutes ago **NEW**



CRAZYYY

Canada - 3 hours ago



严平华的 iPad

Canada - 3 hours ago



Windows

Toronto, ON, Canada - 4 hours ago **NEW**



Windows

Toronto, ON, Canada - 11 March, 14:19 **NEW**

← Recently used devices



Windows

Current device



This is a new device. If you don't recognise it, someone may have your password. We recommend that you [secure your account](#) now.

Browser



Firefox 38.0

1 minute ago

Last location used 

Moldova - 1 minute ago

Notifications & alerts



New device signed in

Moldova - 2 minutes ago



Windows

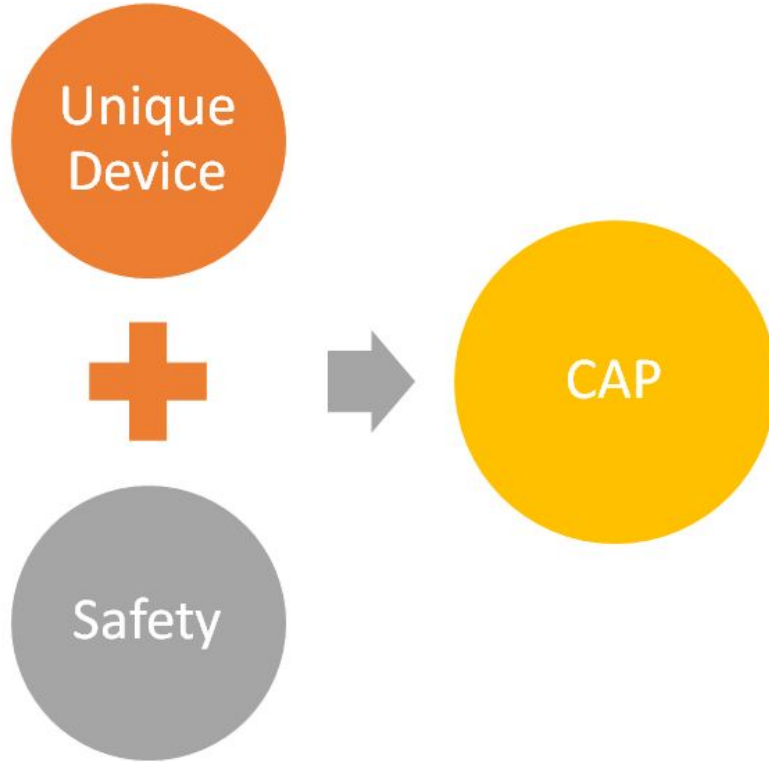
Toronto, ON, Canada - 11 minutes ago



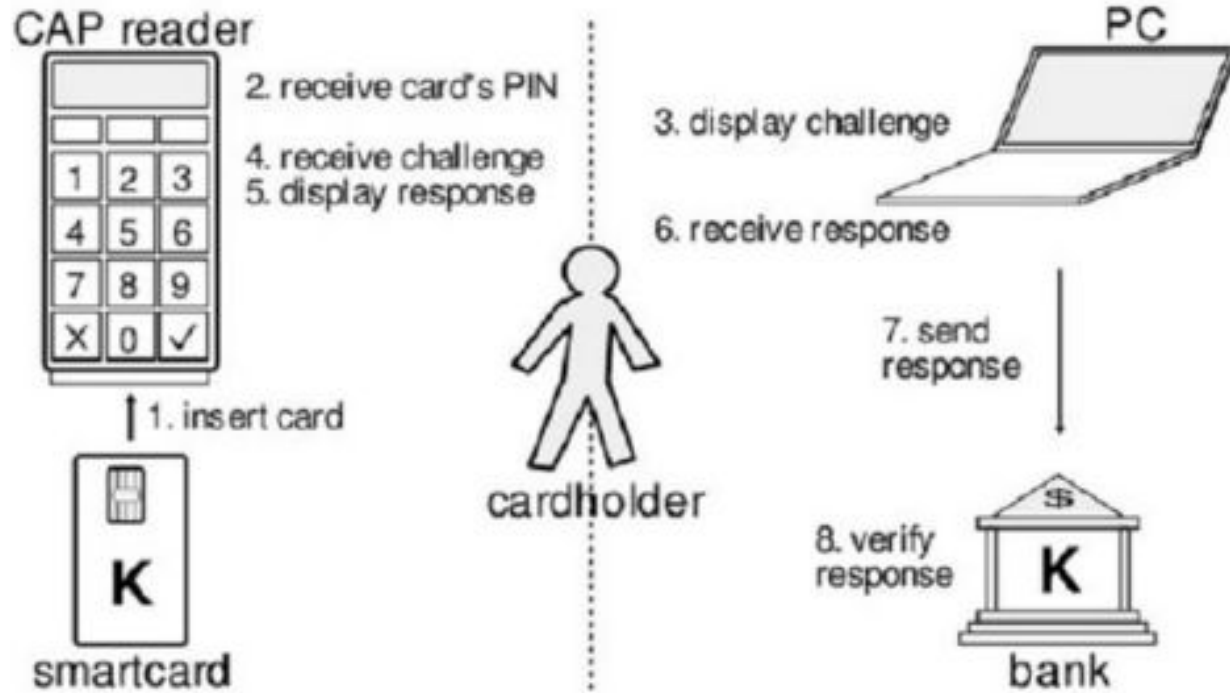
CRAZY

Canada - Yesterday, 22:59

Chip Authentication Program



How CAP Works



Q & A

Q1: How does RBA balance **strong security** and **user-convenience**?

A: By Determining risk and only requiring a small number of transactors (that are deemed risky) to further authenticate themselves.

Q2: How does RBA determine risk?

A: Through a risk engine that evaluates a risk score based on the user's behaviour in comparison to the account profile to determine if any abnormalities are present.

Q 3: What is an OTP?

A : A **one-time password (OTP)** is a random password that is valid for only one login session or transaction.



Questions?