OWASP Passfault

Speaker: Cam Morris
- Creator and Project Lead
- Software Security Specialist
- 10+ years development+security
- cam@passfault.com

Why?

Passwords Can Be Better

How?

Identify Patterns 1

Find Weakest Combination 3

Tie Policy to Strength 5

Measure Pattern Size 2

Estimate Time to Crack 4

Results

Accurate

Informative

Simple

Powerful

Next

OWASP Passfault

Speaker: Cam Morris
- Creator and Project Lead
- Software Security Specialist
- 10+ years development+security
- cam@passfault.com

Why?

Passwords Can Be Better

How?

Identify Patterns 1

Find Weakest Combination 3

Tie Policy to Strength 5

Measure Pattern Size 2

Estimate Time to Crack 4

Results

Accurate

Informative

Simple

Powerful

Next

Why?

Why Not Use Password Strength?

How do you measure password strength?

Passwords Can Be Better

Examples

Policies don't measure password strength

They test for compliance with good advice

You can follow the advice, and still make weak passwords

Password Policies Stink!

Of People and Passwords:

- "successfully creating a password is signficantly more difficult under stricter password policies"
- Password length was the only significant predictor of password strength

- Komanduri et. al., Carnegie Mellon & NIST

Are passwords policies in your organization effective?

"No"

*Why do companies, despite poorly training for passwords, / their password policies are rendering?

passwords are the weakest link

passwords are the **weakest link**

About 71,100 results (0.03 seconds)

Past year

Password Security Remains the **Weakest Link** Even After Big Data ...
www.eweek.com/.../**Password**-Security-Remains-the-**Weakest-Link**-E...
Jun 19, 2011 - Organizations should be implementing several measures to prevent cyber-attackers from stealing sensitive, confidential data.

ZoneAlarm Survey Reveals That **Passwords are the Weakest Link** in ...
blog.zonealarm.com/.../zonealarm-survey-reveals-that-**passwords-are**...
Dec 20, 2010 - ZoneAlarm Survey Reveals That **Passwords are the Weakest Link** in Online Security. By the ZoneAlarm Team. We've got new and interesting survey results ...

Passwords are the weakest link in online security
www.net-security.org/secworld.php?id=10353
Dec 22, 2010 - **Passwords are the weakest link** in online security. Posted on 22 December 2010. Bookmark and Share. A ZoneAlarm survey showed that 79% of consumers use ...

Passwords Are the Weakest Link In Online Security - Slashdot
tech.slashdot.org/.../**passwords-are-the-weakest-link**-in-online-securit...
Dec 22, 2010 - Orome1 writes "It's not surprising to find that 79% of consumers use risky **password** construction practices, such as including personal information and words.

Sony's **Weakest Link** Hijack | OpenID
openid.net/2011/10/13/sony's-**weakest-link**-hijack/
6 days ago - These attacks are referred to as "**weakest link** hijackings" because the hackers attack websites with the weakest security, and then collect user **passwords**. ...

Cyber Experts Point to Computer **Passwords** as **Weakest Link** in ...
www.defenceiq.com › Defence Technology › Articles

Policies don't measure password strength

They test for compliance
with good advice

You can follow the advice,
and still make weak passwords

Password Policies Stink!

Of People and Passwords:

- "successfully creating a password is signficantly more difficult under stricter password policies"
- Password length was the only significant predictor of password strength

- Komanduri et. al., Carnegie Mellon & NIST

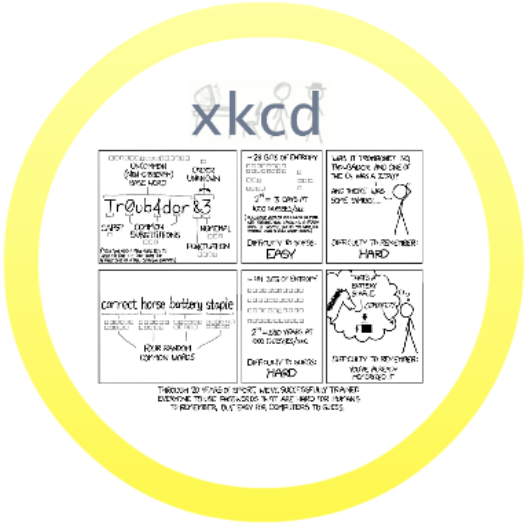
Examples

#1Eagles

- Special Chars
- Number
- Upper and Lower
- Eight Characters
- But still weak

qwerQWER1234!@#$

- Long! Looks strong
- Passes any policy
- But very guessable



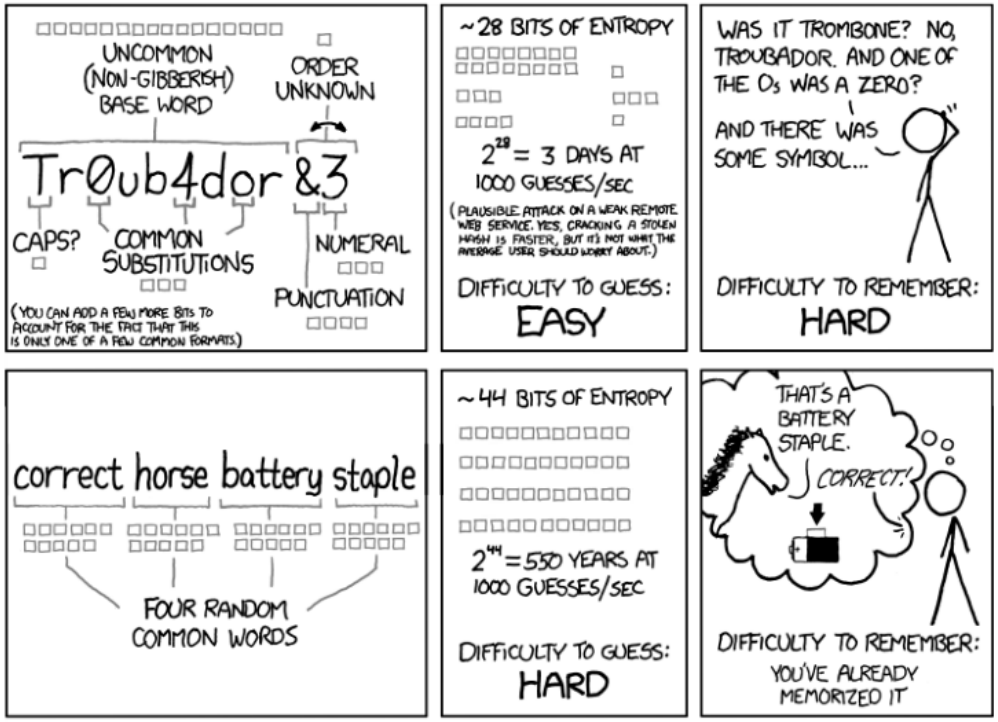
#1Eagles

- Special Chars
- Number
- Upper and Lower
- Eight Characters
- But still weak

qwerQWER1234!@#$

- Long! Looks strong
- Passes any policy
- But very guessable

xkcd



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Are passwords policies in your organization effective?

"No"

*Why do companies create yearly training for passwords if their password policies are working?

Why Not Use Password Strength?

How do you measure password strength?

How?

Identify Patterns

1

In the password

Find Weakest Combination

3

Combined size of the patterns is the measurement of strength.

Worst Case Scenario:

- Hacker knows what patterns you used.

Tie Policy to Strength

5

Set the policy to an acceptable level of risk

- Simpler configuration
- Better manage risk

Measure Pattern Size

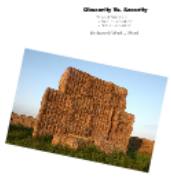
2

How many passwords fit in the Pattern

- More Accurate
- More Meaningful

Like a needle in a hay stack. How big is the hay stack*

"Cream Research Center, "Password Measures"



Estimate Time to Crack

4

- Represents current hardware
- Communicates the risk
- Enables self-training

Identify Patterns

In the password

Random Cyrillic Characters
Horizontal Keyboard Sequence
Repeated Charaters
English Word
Spanish Word
Word with Special Character Substitution
Slang Words
Backwards Word
Leet Speak
Misspelled Word
Word with Special Character Inserted
City Names
Dates
Diagonal Keyboard Sequence
Random Latin Characters

Measure Pattern Size

2

How many passwords fit in the Pattern

- More Accurate
- More Meaningful

Like a needle in a hay stack. How big is the hay stack*

*Gibson Research Center, "Password Haystacks"

Obscurity Vs. Security

Password Pattern Size
- favors secure patterns
- Not obscure patterns

Backwards Word = Word

Obscurity Vs. Security

Password Pattern Size

- favors secure patterns
- Not obscure patterns.

Backwards Word = Word

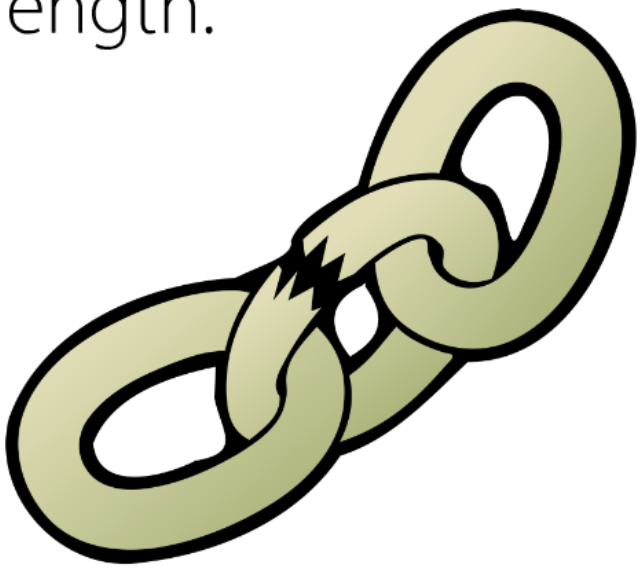
Find Weakest Combination

3

Combined size of the patterns is the measurement of strength.

Worst Case Scenario:

- Hacker knows what patterns you used.



Estimate Time to Crack

4

- Represents current hardware
- Communicates the risk
- Enables self-training

Tie Policy to Strength

5

Set the policy to an acceptable level of risk

- Simpler configuration
- Better manage risk

Results

Accurate

Identifies more weak passwords, yet allows strong passwords that don't pass traditional policies

Informative

Provides detailed analysis of the password so users quickly learn how to create strong passwords without training

Simple

Communicates the risk of poor passwords with the "time to crack"

Powerful

Empowers administrators to know and control the strength of passwords for the organization

Current Password Advice

- is not wrong...
- but it's not exactly right
- it encourages one type of pattern

Length is King

- 12 random characters
- 4 random words
- 2 misspelled words

esu

Accurate

Identifies more weak passwords, yet allows strong passwords that don't pass traditional policies

Informative

Provides detailed analysis of the passw
learn how to create strong passwords

curate

ntifies more weak passwords, yet allows strong
swords that don't pass traditional policies

Informative

Provides detailed analysis of the password so users quickly
learn how to create strong passwords without training

Simple

Communicates the risk of poor password
"time to crack"

Powerfu

ord A

pass traditional policies

rmative

es detailed analysis of the password so users quickly
ow to create strong passwords without training

Simple

Communicates the risk of poor passwords with the "time to crack"

Powerful

Empowers administrators to know and
strength of passwords for the organiz

ble

unicates the risk of poor passwords with the
o crack"

Powerful

Empowers administrators to know and control the strength of passwords for the organization

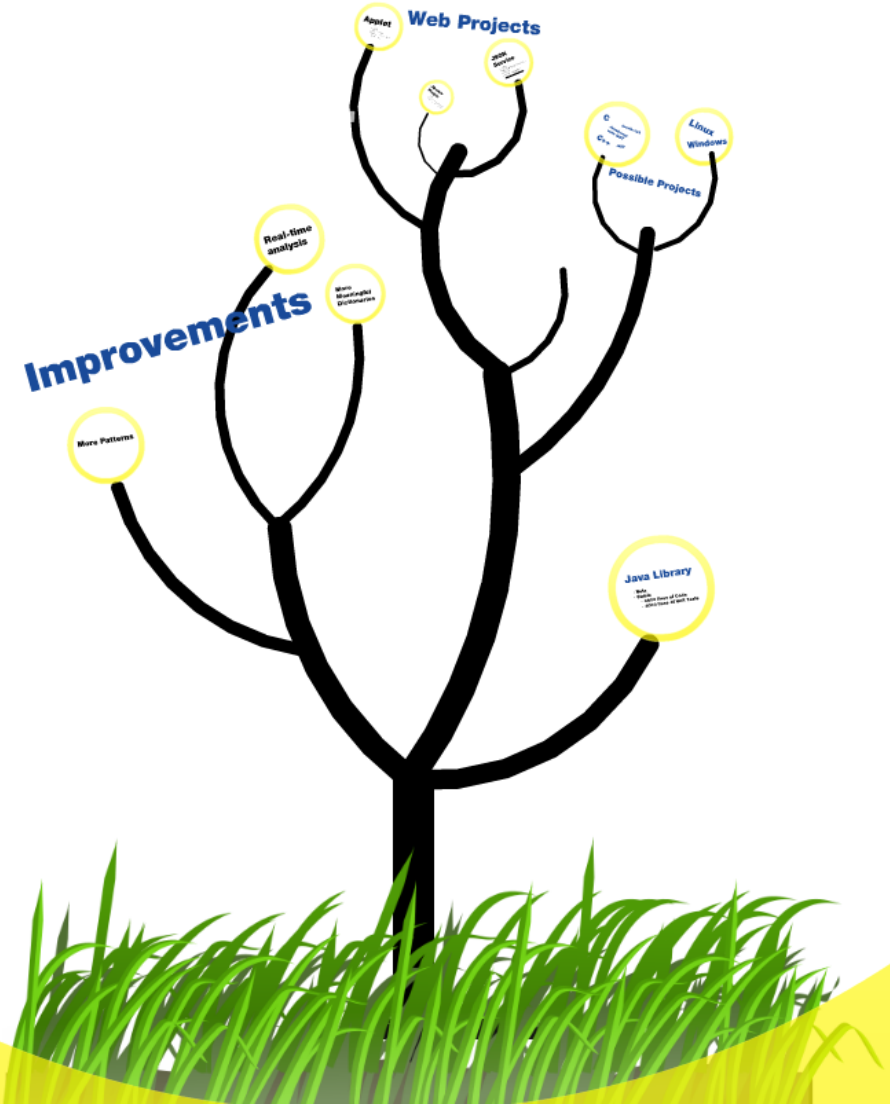
Current Password Advice

- is not wrong...
- but it's not exactly right
- it encourages one type of pattern

Length is King

- 12 random characters
- 4 random words
- 2 misspelled words

Next


Web Projects
Applet
Possible Projects
Linux
Windows
Improvements
Real-time analysis
More Patterns
Java Library

Java Library

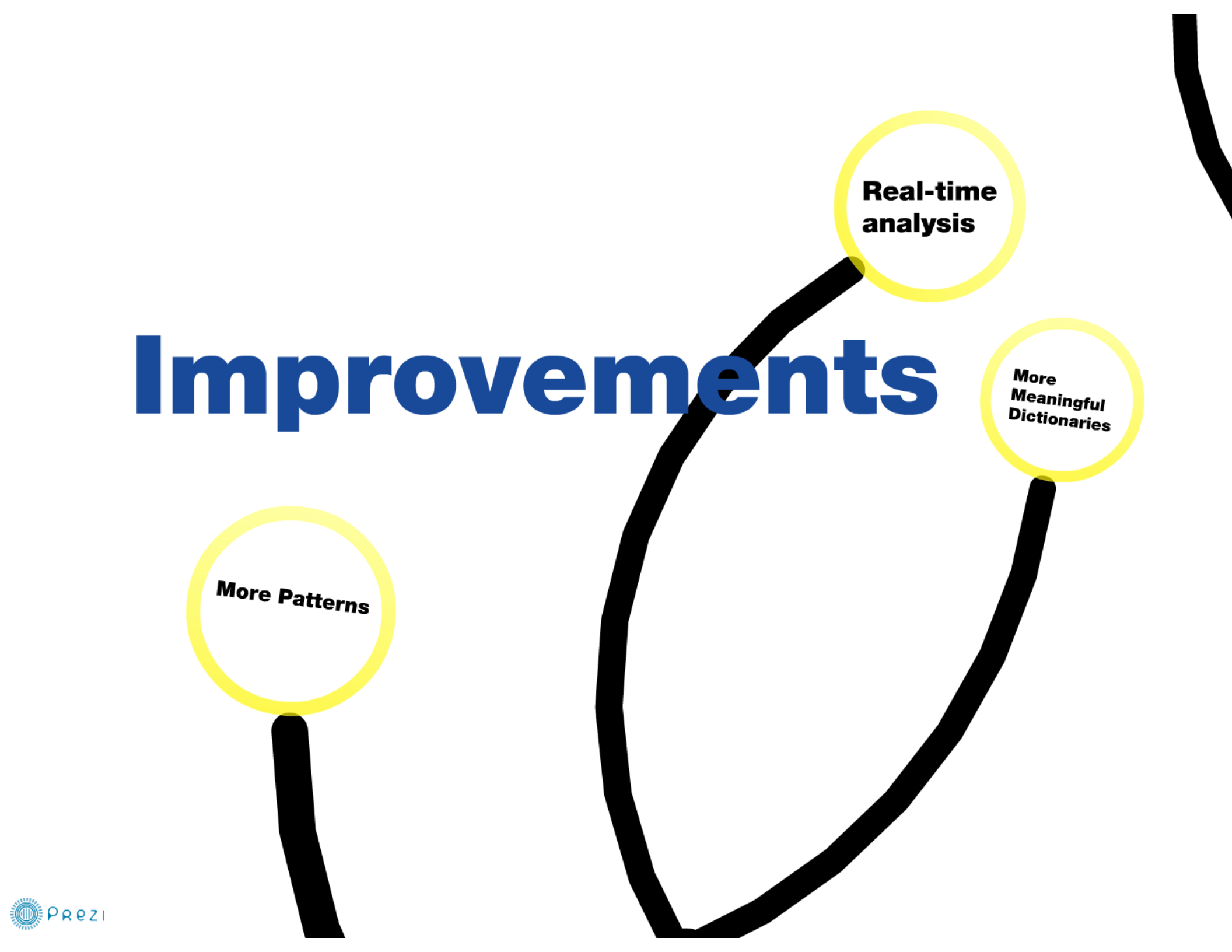
- Beta
- Stable
  - 3500 lines of Code
  - 3000 lines of Unit Tests

Improvements

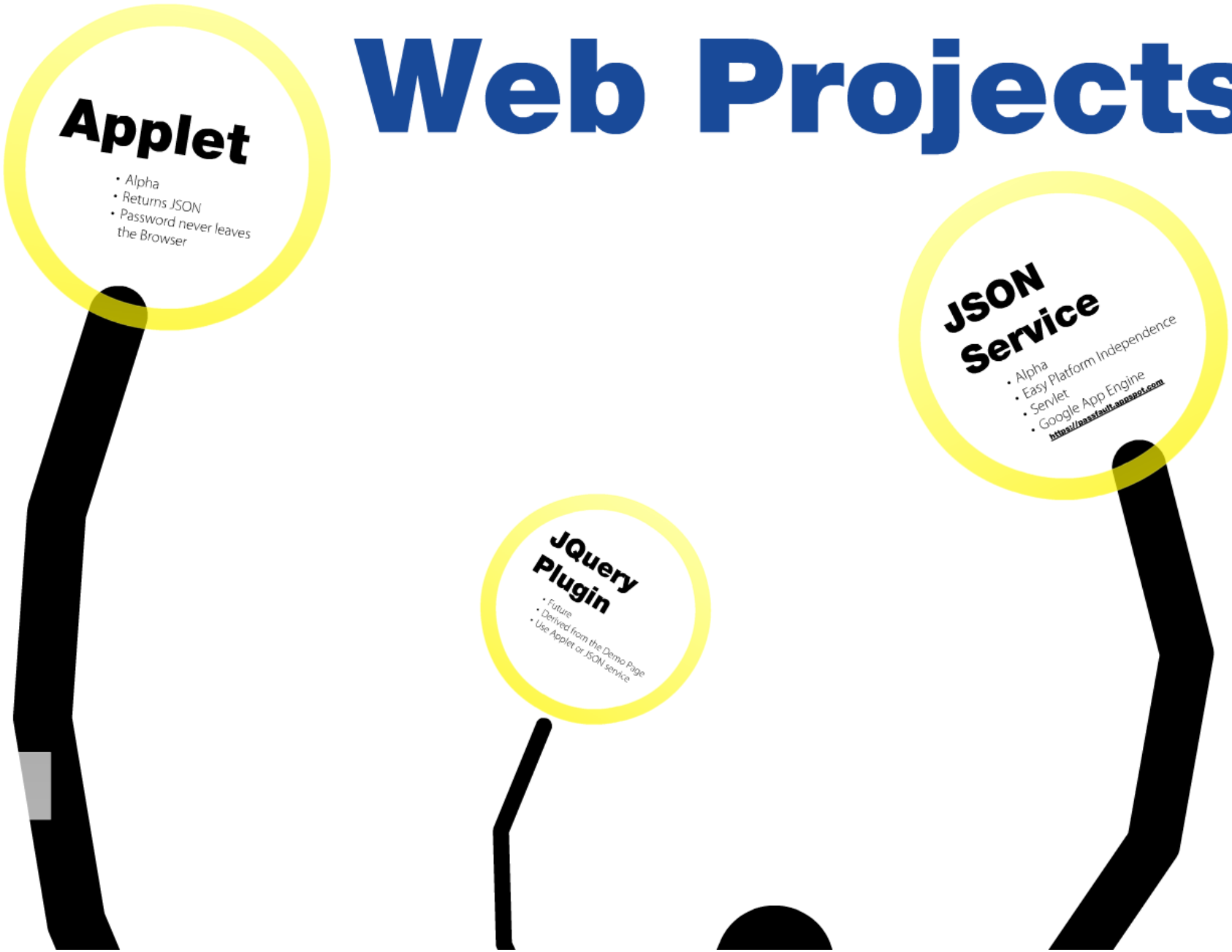
Real-time analysis

More Meaningful Dictionaries

More Patterns



Web Projects



JSON Service

- Alpha
- Easy Platform Independence
- Servlet
- Google App Engine

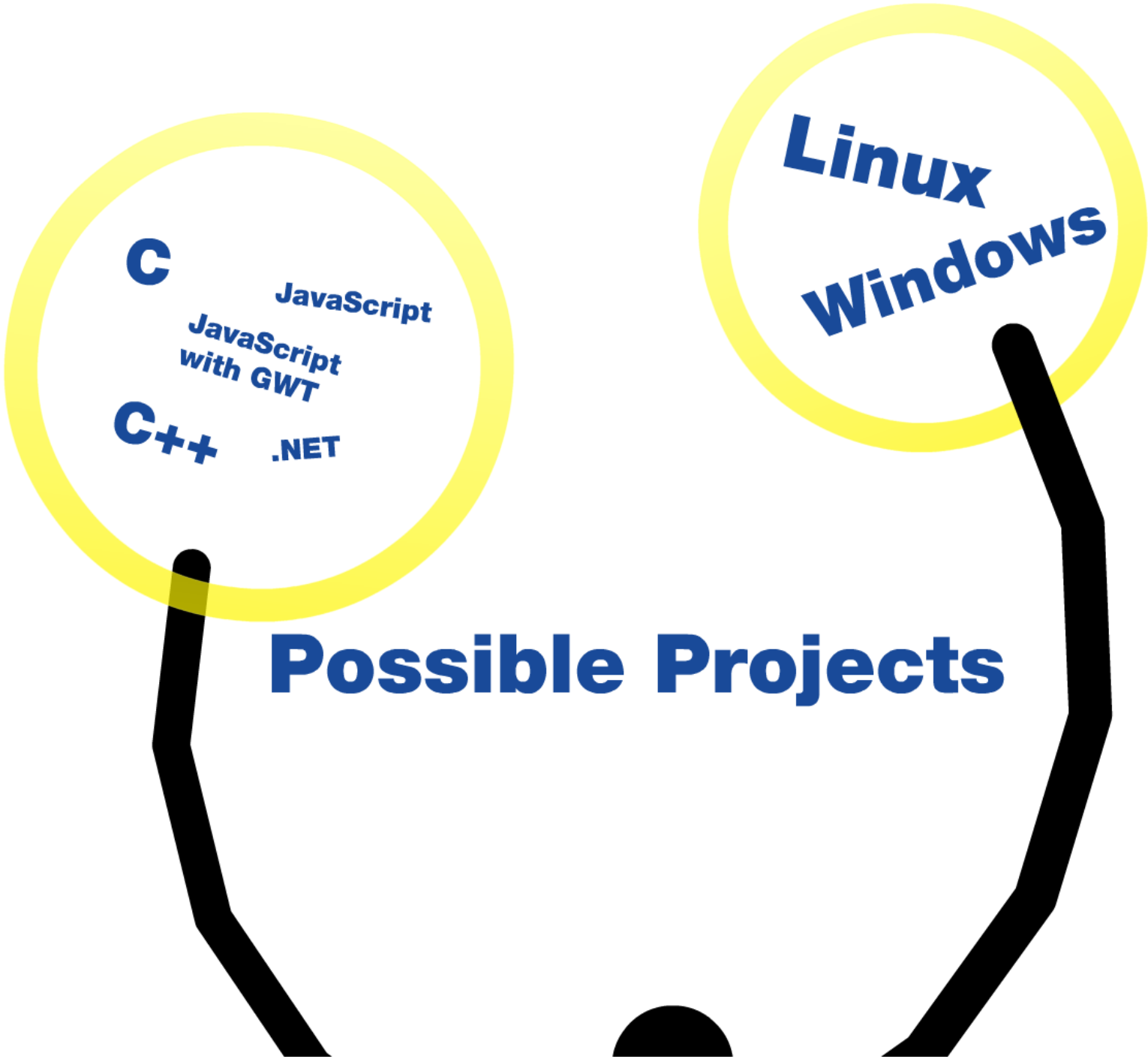
https://passfault.appspot.com

Applet

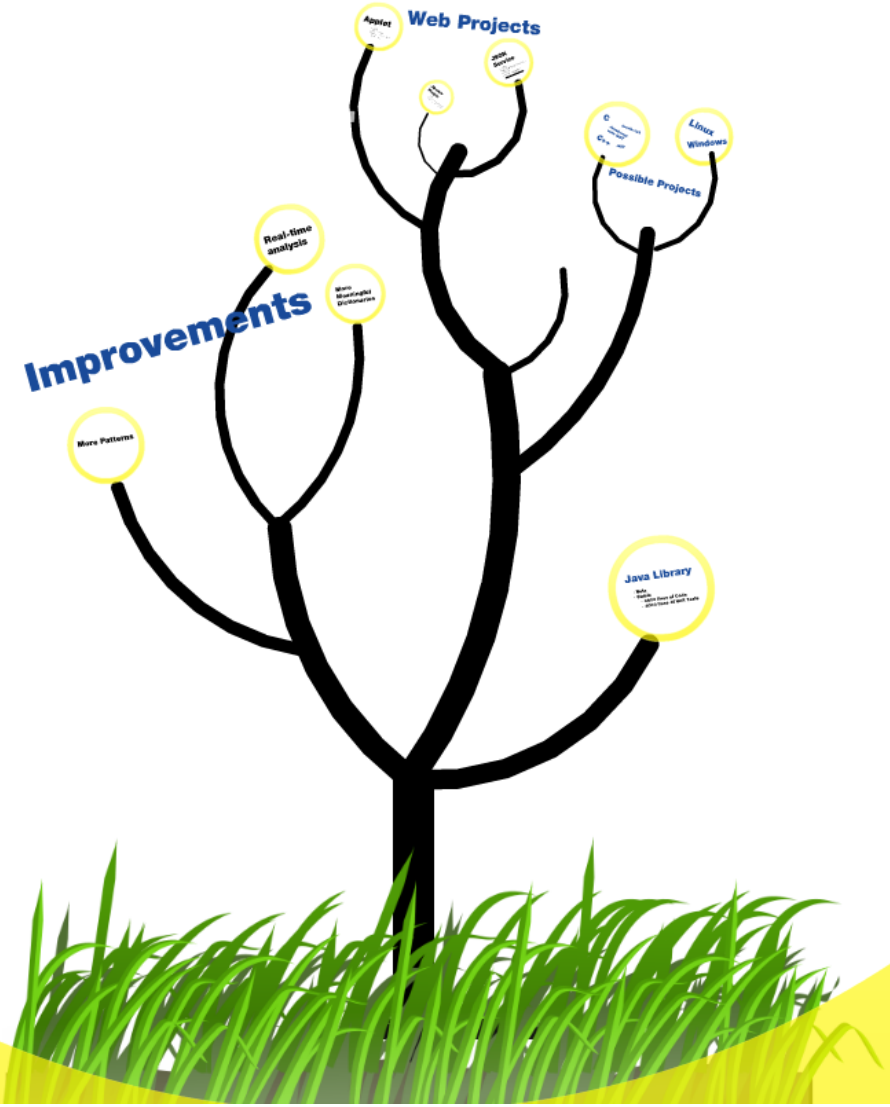
- Alpha
- Returns JSON
- Password never leaves the Browser

JQuery Plugin

- Future
- Derived from the Demo Page
- Use Applet or JSON service


C
JavaScript
JavaScript with GWT
C++
.NET
Linux
Windows
Possible Projects

Next


Web Projects
Applet
Possible Projects
Linux
Windows
Improvements
Real-time analysis
More Patterns
Java Library

OWASP Passfault

Speaker: Cam Morris
- Creator and Project Lead
- Software Security Specialist
- 10+ years development+security
- cam@passfault.com