BÀI TẬP LỚN

Học phần: Nhập môn An toàn thông tin (IT4015)

Đề tài: Giải pháp thay thế mật khẩu truyền thống - Sử dụng câu hỏi bí mật

Sinh viên thực hiện:

- **Nguyễn Đình Đạt** - 20173011
- **Lê Hà Hưng** - 20183757
- **Nguyễn Duy Khai** - 20183771

Giảng viên hướng dẫn: TS. Trần Vĩnh Đức

---

1. Đặt vấn đề

Thời đại mà chúng ta đang sống thường có thể được nhắc đến với từ khóa là "thòi đại công nghệ". Đúng như vậy, khoa học - kỹ thuật và công nghệ không những phổ biến vì vốn dĩ nó thực sự gần như tồn tại ở mọi nơi của Việt Nam và trên thế giới rồi, mà hơn như thế, công nghệ đang dần ăn nhập vào cuộc sống mỗi người với mọi hoạt động, mọi sinh hoạt trong xã hội. Đi liền với đó là việc liên lạc, trao đổi, lưu trữ thông tin thông qua các nền tảng "cloud" và mạng Internet đã trở nên một thói quen sinh hoạt của mọi người trong đời sống và cả trong công việc, gần như ai cũng có cho mình một tài khoản cá nhân ở một hệ thống nào đó và gần như các đơn vị cung cấp dịch vụ dù lớn, dù nhỏ cũng có cho mình những hệ thống để quảng há, quản lý thông tin và tương tác với người dùng, họ cung cấp hoặc cho phép người dùng tạo tài khoản cá nhân để đăng nhập vào và sử dụng hệ thống của họ.

Tất cả sự phát triển của công nghệ, Internet mạng xã hội và các dịch vụ trực tuyến mang đến rất nhiều những sự tiện lợi cho con người - tất nhiên, đó là lý do để "chúng" ra đời - hướng đến phục vụ công việc và đời sống cá nhân mỗi người hay các cơ

quan, đơn vị, tập thể. Và hiển nhiên cái gì cũng có 2 mặt, đi liền với thuận lợi là những thách thức, một trong số đó mà chúng ta có thể rất quan tâm ở đây là an toàn, bảo mật thông tin người dùng, tài khoản không bị giả mạo, không bị kẻ gian tấn công, sử dụng trái phép để lừa đảo, lấy dữ liệu bí mật hay bất kỳ mục đích xấu nào, đây luôn là vấn đề mà thế giới số chưa bao giờ ngừng quan tâm. Giải pháp cho việc quản lý và bảo mật tài khoản người dùng phổ biến nhất hiện nay vẫn là sử dụng mật khẩu, chúng em xin tạm gọi giải pháp này xuyên suốt nội dung báo cáo là "mật khẩu truyền thống". Nhiều năm qua, việc sử dụng thao tác đăng nhập với mật khẩu vẫn đang khá thuận lợi, có thể nhìn chung là vậy, nhưng để nói an toàn, muốn tránh đến mức tối đa những hiểm họa xoay quanh thông tin đăng nhập tài khoản, liệu "mật khẩu truyền thống" có thực sự an toàn?

Chỉ cần tìm kiếm trên Internet với từ khóa "tấn công tài khoản", "mật khẩu tệ" hay "mật khẩu phổ biến",…. (kết quả tìm kiếm sẽ tốt hơn nếu dùng các từ khóa bằng Tiếng Anh), chúng ta sẽ được thấy ngay rất nhiều những kết quả là mình chứng khá rõ cho thấy rằng: Mật khẩu truyền thống chưa thực sự là giải pháp an toàn. Hằng năm, những vụ tấn công tài khoản người dùng đặc biệt là những tài khoản quan trọng như tài khoản ngân hàng, tài khoản quản trị hệ thống các doanh nghiệp, cơ quan, đơn vị, hay những tài khoản rất phổ biến như các nền tảng mạng xã hội Zalo, Facebook, ... và cả việc quét mật khẩu wifi nhà hàng xóm nữa. Việc bị tấn công, bị xâm nhập, bị mất tài khoản, để lộ mật khẩu vẫn còn rất nhiều, cho dù đội ngũ phát triển của các hãng đã không ngừng khắc phục nhưng việc thất thoát thông tin đăng nhập vẫn chưa bao giờ dừng lại. Hay điển hình là một công bố của hãng NordPass cùng các đối tác vào năm 2020 mà ai quan tâm chắc hẳn đều đã biết, khi mà, hầu hết các tải khoản, mật khẩu bị rò rỉ, bị xâm phạm không hẳn đến từ lỗi nhà phát triển mà nằm ở thói quen của người dùng, hãng đã có thống kê cho thấy rằng, những mật khẩu kém an toàn lại vô cùng phổ biến - được người dùng ưa chuộng để đặt cho tài khoản của mình điển hình là: 123456, 12345678, một dãy các số 1 – số 0, hay đơn cử là mật khẩu đậm chất Việt như "anhyeuem" cũng lọt top 200 thế giới về mật khẩu phổ biến. Kẻ tấn công hoàn toàn có thể thử nghiệm việc xâm nhập các tài khoản với những mật khẩu này, hay đơn giản là tấn công vét cạn với những mật khẩu chỉ toàn chữ thường, toàn số, như vậy, mật khẩu trở nên thiếu an toàn và mang đến nhiều hiểm hoạ về bảo mật thông tin.

Để giải quyết vấn dề này, các thành viên của nhóm em với 3 bạn Đạt, Hưng và Khai đã cùng nhau lên ý tưởng xây dựng một giải pháp thay thế, giảm thiểu những

nguy cơ mà mật khẩu truyền thống để lại, giải quyết những tồn tại xoay quanh mật khẩu thiếu an toàn. Giải pháp mà chúng em muốn đề xuất là thay thế mật khẩu truyền thống trong thao tác đăng nhập bằng việc sử dụng câu hỏi bí mật, những nội dung mang tính cá nhân hóa hơn và chứa bên trong câu trả lời là cả một tính cách – không đơn thuần là một dãy ký tự, dãy số vô hại mà có nguy cơ bị tấn công vét cạn.

2. Mô tả ý tưởng giải pháp

Với giải pháp đăng nhập tài khoản xoay quanh các câu hỏi bí mật, theo một cách nghĩ đơn thuần, hệ thống sẽ đưa ra những câu hỏi bí mật cho người dùng lựa chọn khi tạo tài khoản và người dùng điền câu trả lời cho câu hỏi này vào, lúc đăng nhập, người dùng sẽ chỉ cần điền câu trả lời và họ cần nhớ câu hỏi họ đã chọn, nhờ đó câu hỏi được đảm bảo là "bí mật". Nhưng với giải pháp chúng em muốn xây dựng, chúng em còn muốn nhiều hơn như thế, chúng em muốn tài khoản người dùng được quản lý (riêng với thao tác đăng nhập) sẽ đi liền với một tính cách, một sở thích, một thói quen và một lối hành văn, cách nói, cách hỏi, cách trả lời rất riêng, nhờ đó tài khoản mang tính cá nhân rất cao và gần như theo chúng em là an toàn tuyệt đối.

Để làm được điều này, chúng em muốn xây dựng hệ thống với lớp đăng nhập như sau:

- Bên nhà phát triển đã tạo sẵn các nhóm chủ đề, các từ khóa và cung cấp cho người dùng khi họ tiến hành tạo tài khoản cá nhân, thay vì cung cấp luôn một danh sách các câu hỏi.
- Người dùng tạo tài khoản sẽ chọn chủ đề, từ khóa cho mình và dựa vào đó để đặt các câu hỏi tùy ý liên quan đến chủ đề, từ khóa, đồng thời điền câu trả lời cho mình. Lúc này với mỗi chủ đề, từ khóa, mỗi người sẽ có cách gợi nhớ, cách nghĩ, cách hỏi của riêng mình và qua đó thao tác đăng nhập đi kèm được đảm bảo tính cá nhân gần như ở mức tối đa.
- Khi đăng nhập, hệ thống sẽ không bắt người dùng phải tự giác điền câu trả lời một cách cứng nhắc nữa, vì lâu dần nó trở nên như mật khẩu vậy, thay vào đó, hệ thống sẵn sàng cung cấp các câu hỏi, nhưng thực tế là những câu hỏi gây nhiễu xoay quanh chủ đề, từ khóa người dùng đã chọn khi đăng nhập. Việc của người dùng là nhận thấy chủ đề trên câu hỏi thì không cần quan tâm đến câu hỏi gây nhiễu mà chỉ việc trả lời như những gì mình đã trả lời cho câu hỏi mà bản thân đã đặt khi tạo tài khoản, hệ thống kiểm tra nếu câu trả lời là chính xác với những thông tin người dùng đã cung cấp sẵn từ trước trên hệ thống thì

thao tác đăng nhập là thành công (hệ thống có dòng thông báo nhắc nhở ở trang đăng nhập để lưu ý người dùng chỉ trả lời theo đúng những gì mà họ đã lựa chọn lúc tạo tài khoản)

Như vậy, với giải pháp này, so sánh với mật khẩu truyền thống chúng ta có những ưu điểm và hạn chế như sau:

Ưu điểm:

- An toàn gần như là tuyệt đối, việc bảo mật thông tin tài khoản đi liền với tính cách, phong cách cá nhân riêng mà không máy móc nào có thể "quét" được.

Hạn chế:

- Có thể gây phức tạp, mất thời gian hơn với người dùng trong thao tác tạo và đăng nhập tài khoản.
- Bị phụ thuộc vào thói quen và sự nghiêm túc của người dùng khi xây dựng câu hỏi và câu trả lời bí mật trên hệ thống. Điều này là chấp nhập được khi chúng ta sẵn sàng bỏ thời gian vận hành và hoàn thiện giải pháp đi liền với việc xây dựng thói quen nghiêm chỉnh của người dùng, nếu họ muốn tài khoản an toàn, họ cần ý thức nghiêm túc đặt câu hỏi và câu trả lời mang tính cá nhân cao và đi liền với bản chất bên trong con người của mình để tránh những sự cố đăng nhập về sau.

3. Giải pháp kỹ thuật xây dựng sản phẩm

Với ý tưởng trên, để cụ thể hóa giải pháp, nhóm chúng em hướng đến xây dựng một sản phẩm minh họa:

- Một trang login (trang đăng nhập, đăng ký tài khoản) đơn giản với HTML, CSS và JS để minh họa các thao tác sử dụng, đồng thời quản trị dữ liệu tài khoản với cơ sở dữ liệu SQL Server hoặc MongoDB.
- Sử dụng ngôn ngữ Python để xây dựng lõi giải pháp trong thao tác tạo câu hỏi nhiễu, cung cấp chủ đề, từ khóa và xử lý câu hỏi, câu trả lời bí mật của người dùng.

4. Ý tưởng phát triển trong tương lai

Tạm thời, với khoảng thời gian khá ngắn nên chúng em chỉ xây dựng một sản phẩ, "demo" mang mục tiêu minh họa nhưng vẫn đảm bảo các điều kiện về an toàn. Trong tương lai, nhóm hướng đến phát triển giải pháp để sẵn sàng cung cấp cho các hệ thống của các đơn vị, với mục tiêu hoàn thiện giải pháp, khắc phục các tồn tại và tạm thời nhìn chung giải pháp của chúng em cho hệ thống là an toàn, phải ít nhất qua thời gian vận hành để nhìn nhận các lỗ hổng và dần khắc phục. Đồng thời, chúng em cũng lên ý tưởng về việc xây dựng một model bên trong hệ thống, vận dụng kiến thức về trí tuệ nhân tạo và xử lý ngôn ngữ tự nhiên (NLP), hệ thống sẽ có khả năng tự cập nhật, thông qua các thao tác sử dụng (hỏi và trả lời) hằng ngày của người dùng, hệ thống sẽ xây dựng được bộ từ khóa, chủ đề phong phú hơn và tự sinh ra được nhiều các câu hỏi gây nhiễu cho mỗi tài khoản để việc đăng nhập theo thời gian lâu dài vẫn đảm bảo an toàn khi mà câu hỏi nhiễu ít bị trùng lập, đồng thời hệ thống có khả năng xử lý câu trả lời tốt hơn. Việc đặt mục tiêu vận dụng NLP cho giải pháp là hợp lý khi mà giải pháp bảo mật đi liền với tiếng nói, ngôn ngữ cá nhân của người dùng, NLP giúp hệ thống không ngừng cập nhật và nhờ đó thời gian vận hành lâu dài vẫn không bị đe dọa bởi các kỹ thuật tấn công.

Chúng em đặt kỳ vọng rằng hệ thống và giải pháp chúng em xây dựng là tốt, khả thi và sẽ được triển khai đồng thời trở nên phổ biến trong thực tế vào một ngày không xa. Chúng em xin chân thành cảm ơn những góp ý, đánh giá quý báu của thầy Trần Vĩnh Đức, chúng em vẫn mong muốn tiếp tục nhận được thêm những chỉ dẫn từ thầy để đề tài được hoàn thiện tốt hơn.