CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

INSTITUTE : UIE

DEPARTMENT : CSE

Bachelor of Engineering (Computer Science & Engineering)

WEB AND MOBILE SECURITY (Professional Elective-I)

(20CST/IT-333)

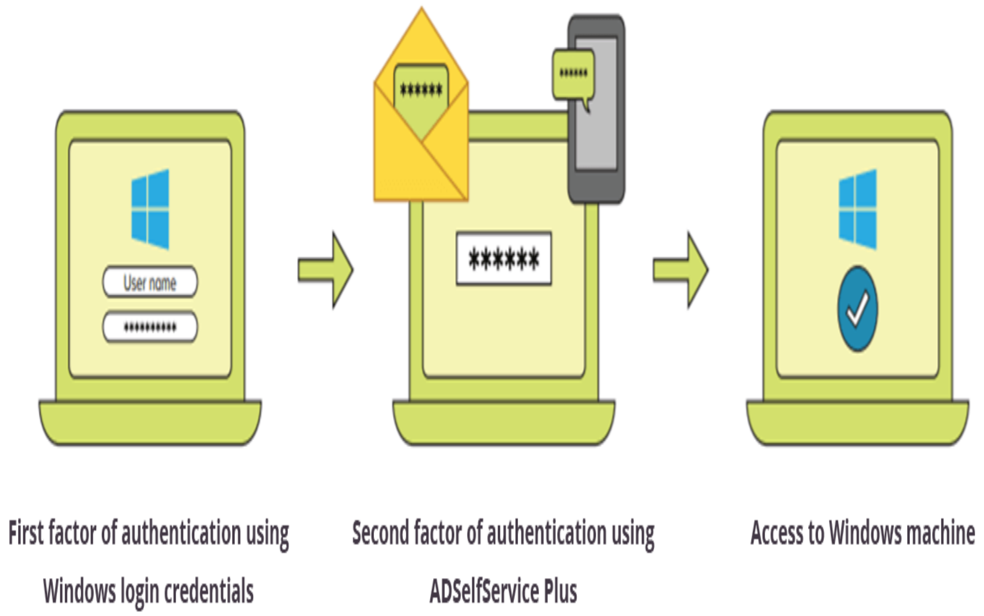
TOPIC OF PRESENTATION:

Web authentication services

DISCOVER . LEARN . EMPOWER

Lecture Objectives

In this lecture, we will discuss: attacks and countermeasures for common web authentication mechanisms, including password-based, multifactor (e.g., CAPTCHA), and online authentication services like Windows Live ID.


User name
****
******
******
******
First factor of authentication using Windows login credentials
Second factor of authentication using ADSelfService Plus
Access to Windows machine

Multi-factor authentication

Multi-factor authentication (MFA) is a method of logon verification where at least two different factors of proof are required. MFA is also referred to as 2FA, which stands for two-factor authentication. MFA helps keep protect your data (email, financial accounts, health records, etc.) or assets by adding an extra layer of security.

Multi-factor authentication

- There are generally three recognized types of authentication factors:
- Type 1 – Something You Know – includes passwords, PINs, combinations, code words, or secret handshakes. Anything that you can remember and then type, say, do, perform, or otherwise recall when needed falls into this category.
- Type 2 – Something You Have – includes all items that are physical objects, such as keys, smart phones, smart cards, USB drives, and token devices. (A token device produces a time-based PIN or can compute a response from a challenge number issued by the server.).

Multi-factor authentication

- Type 3 – Something You Are – includes any part of the human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification.

CAPTCHA:

- "reCAPTCHA is a free service from Google that helps protect websites from spam and abuse. A “CAPTCHA” is a Turing test to tell humans and bots apart. It is easy for humans to solve, but hard for “bots” and other malicious software to figure out. By adding reCAPTCHA to a site, you can block automated software while helping your welcome users to enter with ease.

Hacking Cookies

- Cookies commonly contain sensitive data associated with authentication. If the cookie contains passwords or session identifiers, stealing the cookie can be a very successful attack against a web site.
- There are several common techniques used to steal cookies, with the most popular being script injection and eavesdropping. Reverse engineering the cookie offline can also prove to be a very lucrative attack.
- The best approach is to gather a sample of cookies using different input to see how the cookie changes. You can do this by using different accounts to authenticate at different times.
- The idea is to see how the cookie changes based on time, username, access privileges, and so on. Bit-flipping attacks adopt the brute-force approach, methodically modifying bits to see if the cookie is still valid and whether different access is gained.

Multi factor authentication

Something you have + Something you are + Something you know

Web Authentication Services

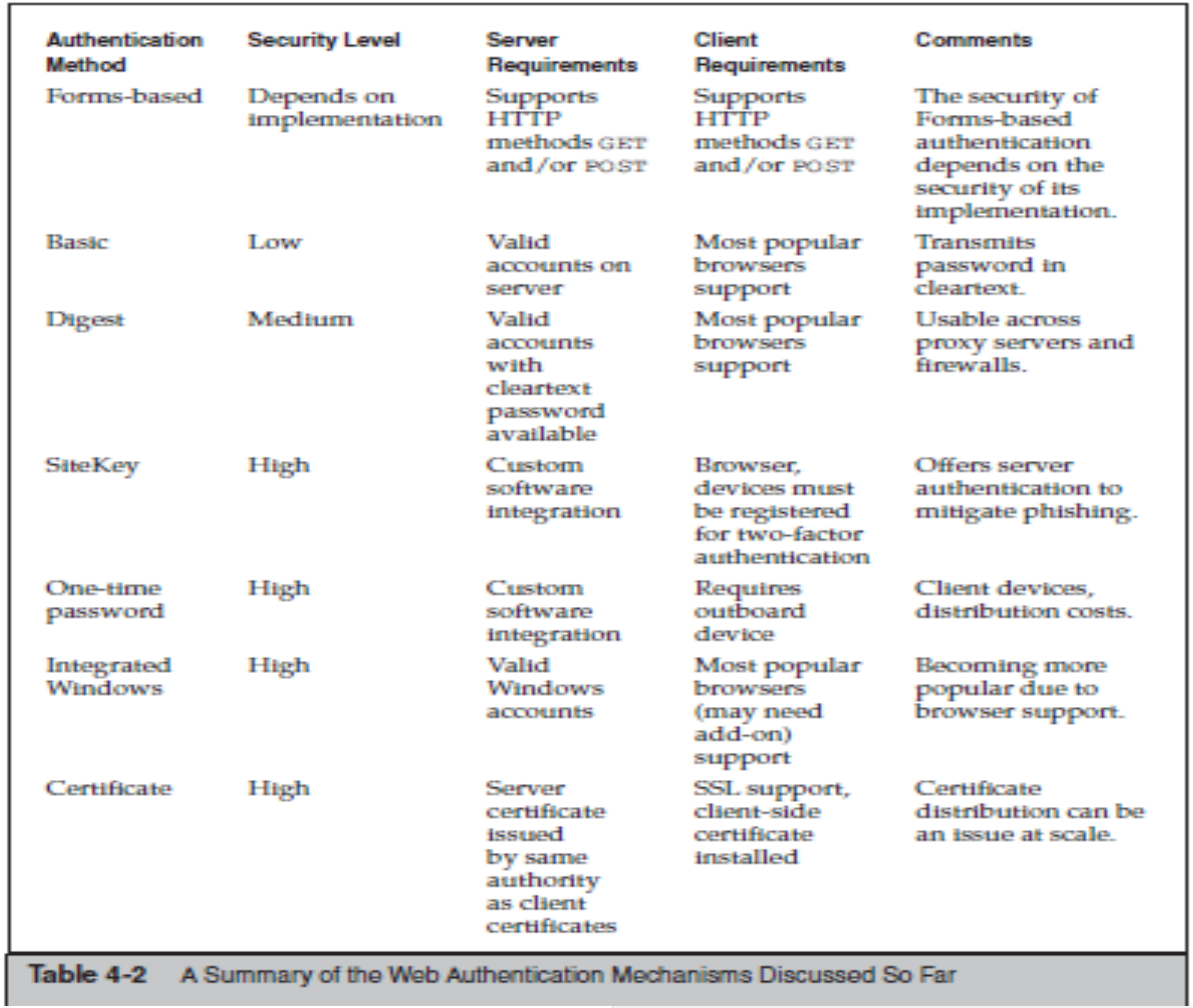
- Microsoft Passport (now known as *Windows Live ID*), which could be used by other sites to manage and authenticate customer identities.
- Originally, Windows Live ID was planned to handle authentication for sites outside of Microsoft and at one point could even boast of heavy hitters such as eBay.com as one of its members. However, the service was never widely adopted outside of Microsoft web properties and is now primarily restricted to web applications managed by Microsoft or closely integrated with Microsoft services

Windows Live ID

- Windows Live ID is the latest stage in the evolution of Microsoft's Passport service and is used to authenticate to Microsoft's core web applications, including MSN, Hotmail, Messenger, Xbox Live, Channel9, among others. A Windows Live ID is a digital identity consisting of one or more claims that are used to authenticate users to the Windows Live ID authentication service.
- These claims may be comprised of information such as a user's e-mail address, the organization(s) that user belongs to, and the roles, relationships, and other authorization-related data associated with the user.
- Authentication is accomplished through the use of a username/password pair, strong passwords and security PIN combinations, smart cards, or self-issued Windows CardSpace cards. The Windows Live ID service also supports specialized mechanisms such as RADIUS protocol to authenticate nonstandard devices including cell phones and the Xbox 360

OpenID

- OpenID is a user-centric, decentralized authentication system providing services identical to that of Windows Live ID. The key difference is that in OpenID, there is no central authentication provider. Any number of organizations can become providers, allowing for greater choice and flexibility.
- The process of authenticating to a site, referred to as a *relying party* (previously OpenID consumer), is simple. First, a nonauthenticated user visits a web site supporting OpenID—for this example, let's say slashdot.com— and selects OpenID as his method of authentication.



Authentication Method	Security Level	Server Requirements	Client Requirements	Comments
Forms-based	Depends on implementation	Supports HTTP methods GET and/or POST	Supports HTTP methods GET and/or POST	The security of Forms-based authentication depends on the security of its implementation.
Basic	Low	Valid accounts on server	Most popular browsers support	Transmits password in cleartext.
Digest	Medium	Valid accounts with cleartext password available	Most popular browsers support	Usable across proxy servers and firewalls.
SiteKey	High	Custom software integration	Browser, devices must be registered for two-factor authentication	Offers server authentication to mitigate phishing.
One-time password	High	Custom software integration	Requires outboard device	Client devices, distribution costs.
Integrated Windows	High	Valid Windows accounts	Most popular browsers (may need add-on) support	Becoming more popular due to browser support.
Certificate	High	Server certificate issued by same authority as client certificates	SSL support, client-side certificate installed	Certificate distribution can be an issue at scale.

Table 4-2 A Summary of the Web Authentication Mechanisms Discussed So Far

References:

Books:

1. Hacking Exposed Mobile: Security Secrets & Solutions 1st Edition, Kindle Edition, by Neil Bergman, Mike Stanfield, Jason Rouse, and Joel Scambray
2. Hacking Exposed Web Applications, 3rd edition, Joel Scambray, Vincent Liu, Caleb Sima, Released October 2010, Publisher(s): McGraw-Hill

Reference Links:

https://www.globalknowledge.com/us-en/resources/resource-library/articles/the-three-types-of-multi-factor-authentication-mfa/#gref

https://www.manageengine.com/products/self-service-password/windows-logon-two-factor-authentication.html

Relevant Videos:

https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661

https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA

THANK YOU