Hacking Tips & Tricks

M.Ananthakrishnan
CEH LPT ECSA CCSA CPISI ITIL
Manager – Infosec Governance
Hexaware Technologies Limited
m.aananth@gmail.com
+91 8939913933

OWASP
May 7, 2011

The OWASP Foundation
http://www.owasp.org

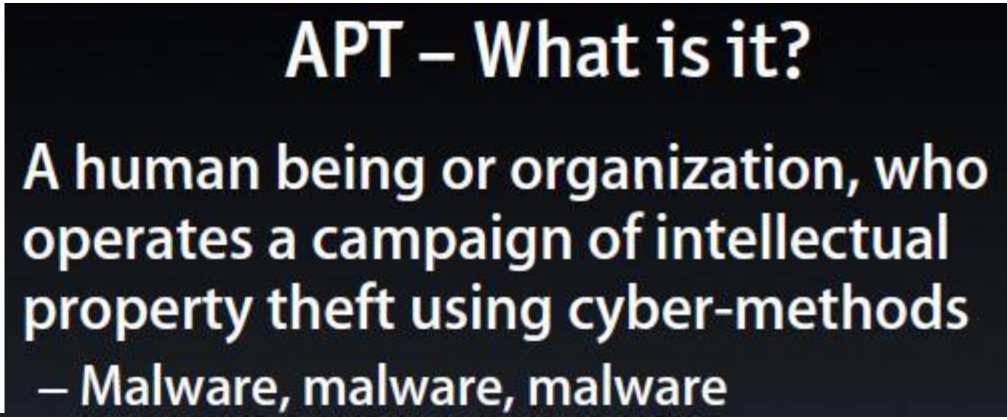
Agenda

- ❑ Security Incidents
- ❑ Vulnerability Assessment
- ❑ Wireless Hacking
- ❑ Bluetooth Hacking
- ❑ Advance password hacking

Cash is not the only motive

A99 Operation Empire State Rebellion - Communication #

by AmpedStatus

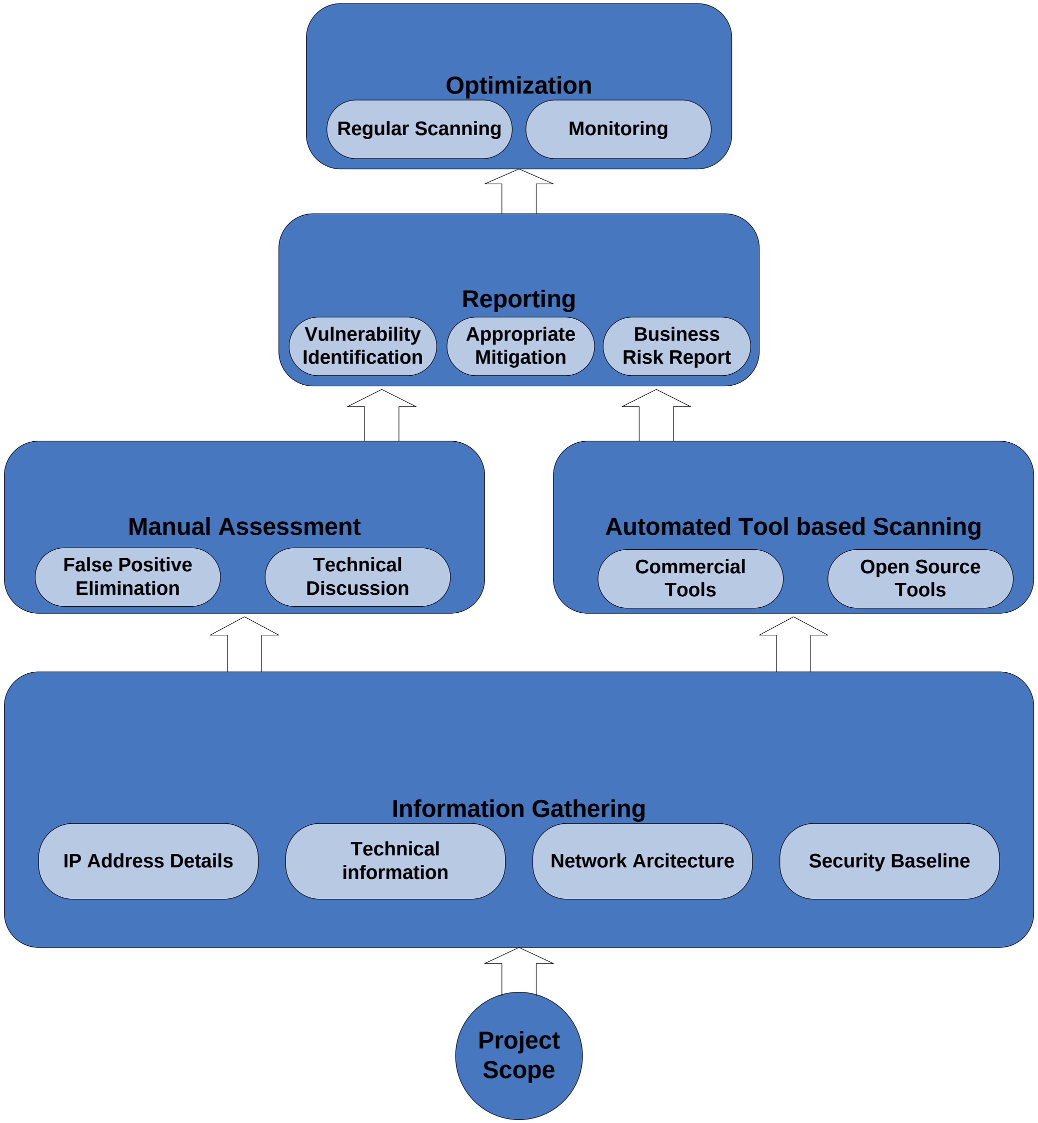

APT – What is it?

A human being or organization, who operates a campaign of intellectual property theft using cyber-methods

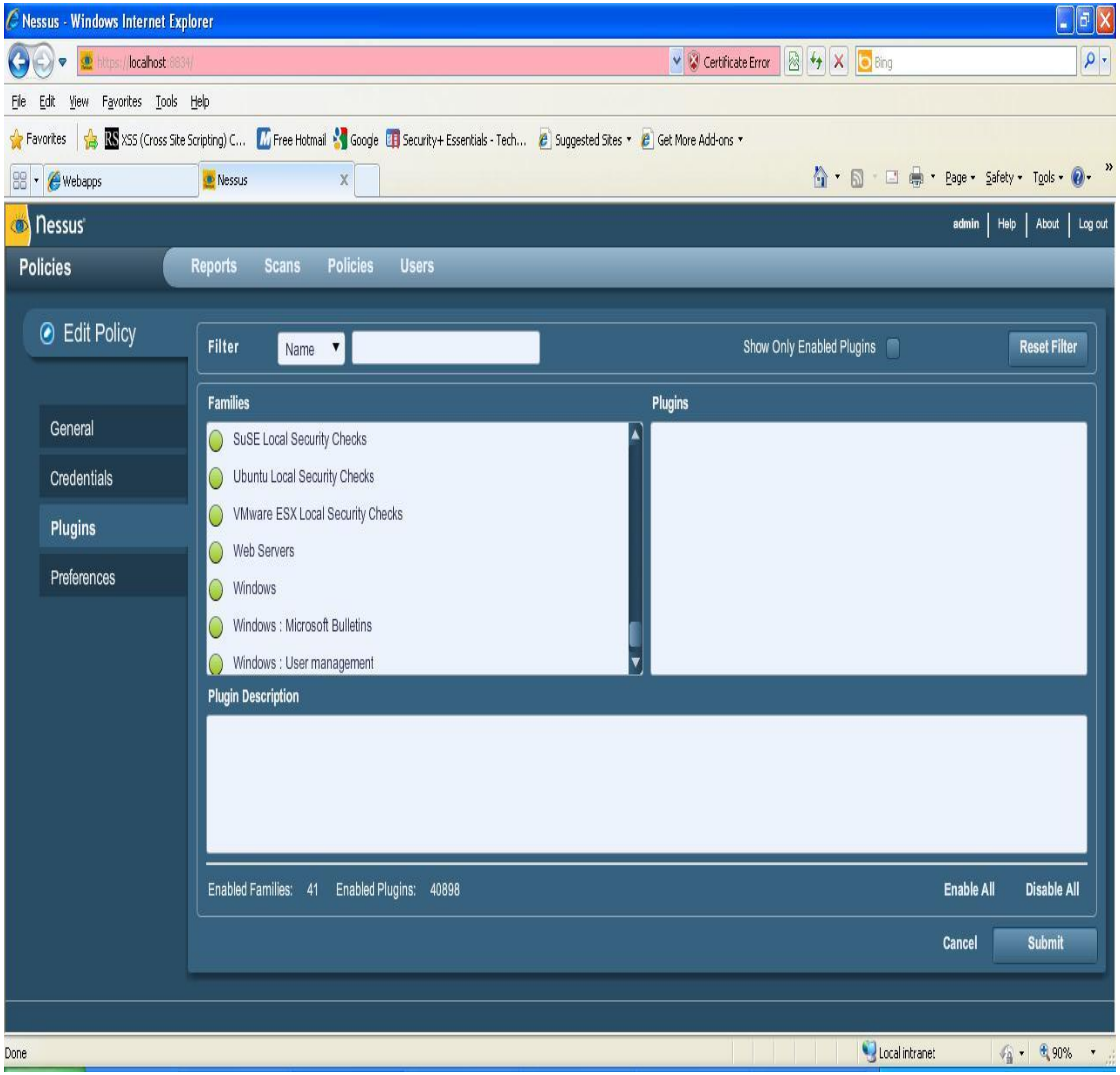
– Malware, malware, malware

The bad guys STILL HAVE their zero day, STILL HAVE their vectors, and STILL HAVE their malware

Vulnerability Assessment Methodology & Tools



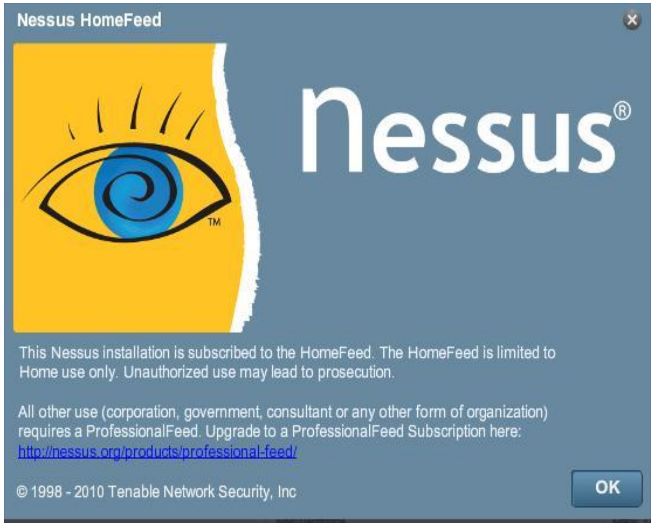
Vulnerability Assessment Methodology & Tools



Families:

- SuSE Local Security Checks
- Ubuntu Local Security Checks
- VMware ESX Local Security Checks
- Web Servers
- Windows
- Windows : Microsoft Bulletins
- Windows : User management

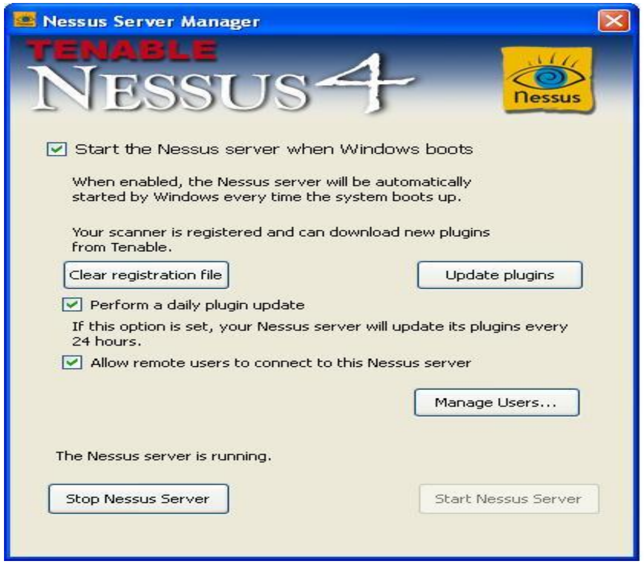
Enabled Families: 41 Enabled Plugins: 40898



This Nessus installation is subscribed to the HomeFeed. The HomeFeed is limited to Home use only. Unauthorized use may lead to prosecution.

All other use (corporation, government, consultant or any other form of organization) requires a ProfessionalFeed. Upgrade to a ProfessionalFeed Subscription here: http://nessus.org/products/professional-feed/

© 1998 - 2010 Tenable Network Security, Inc



☑ Start the Nessus server when Windows boots

When enabled, the Nessus server will be automatically started by Windows every time the system boots up.

Your scanner is registered and can download new plugins from Tenable.

☑ Perform a daily plugin update

If this option is set, your Nessus server will update its plugins every 24 hours.

☑ Allow remote users to connect to this Nessus server

The Nessus server is running.

Wireless Usages & vulnerabilities

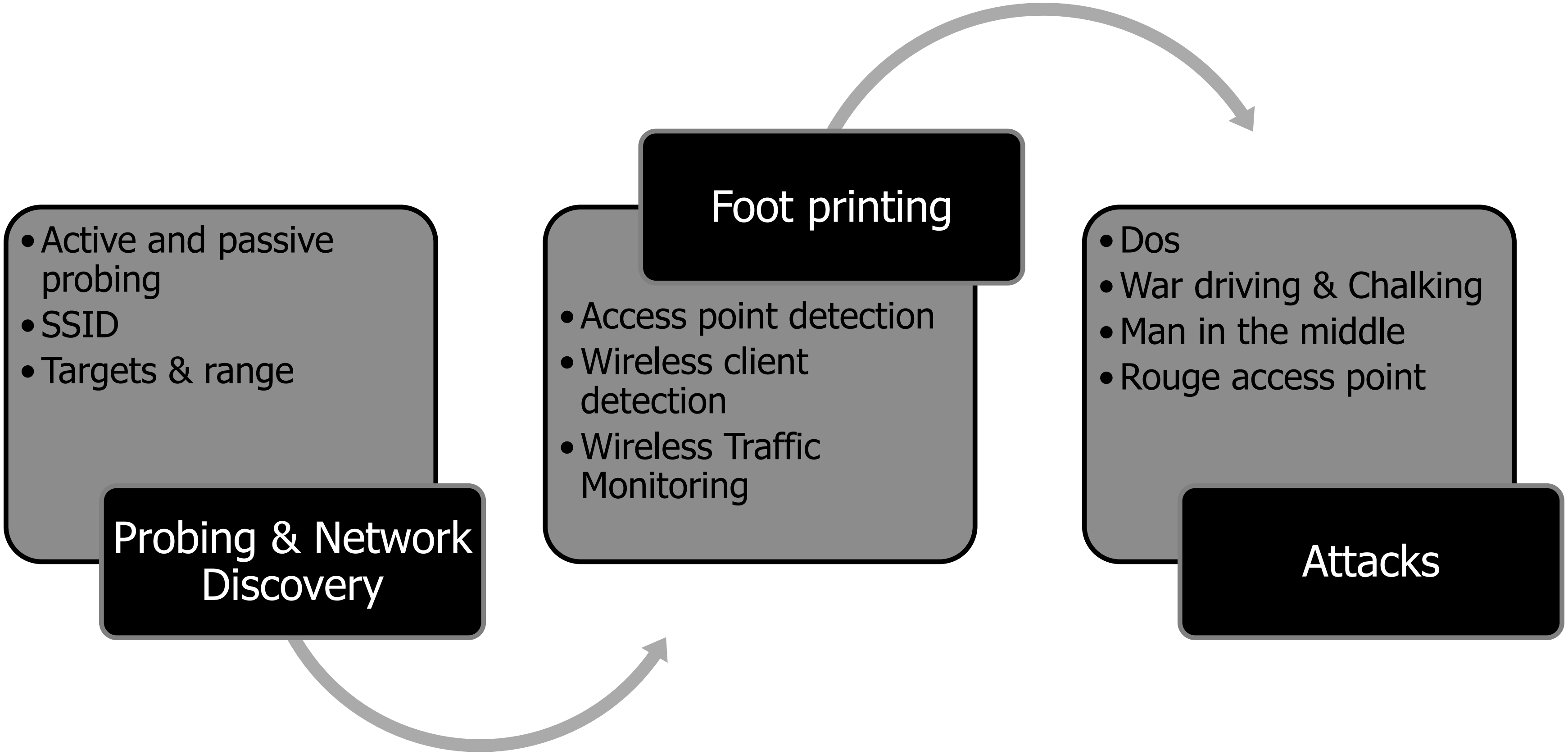
Wireless technology is becoming popular and at the same time has introduced several security issues. It’s a cost effective solution and mobility ,Easy sharing, the same advantages turned to be the security threats.

Various Wireless standards : 802.11a , 802.11b , 802.11g , 802.11i , 802.16

Vulnerabilities :

- Default Configuration
- Weak passwords
- Physically insecure locations
- Rogue access points
- Lack of network monitoring
- Insufficient network performance
- MAC address filtering
- Inadequate encryption standards
- War Driving
- Easy to eavesdrop
- Unsecured holes in the Network

Wireless Attacking Methodology



- Active and passive probing
- SSID
- Targets & range

Probing & Network Discovery

Foot printing

- Access point detection
- Wireless client detection
- Wireless Traffic Monitoring

- Dos
- War driving & Chalking
- Man in the middle
- Rouge access point

Attacks

How to Prevent Wireless Hacks

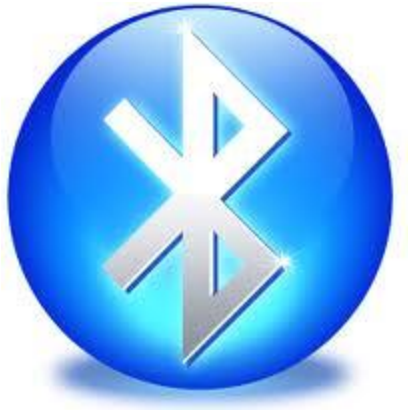
- ❑ Access Point Monitoring
- ❑ Wireless Client Monitoring
- ❑ General Wireless Traffic Monitoring
- ❑ Wireless IDS
- ❑ Frequent security testing

Bluetooth Usages & Vulnerabilities

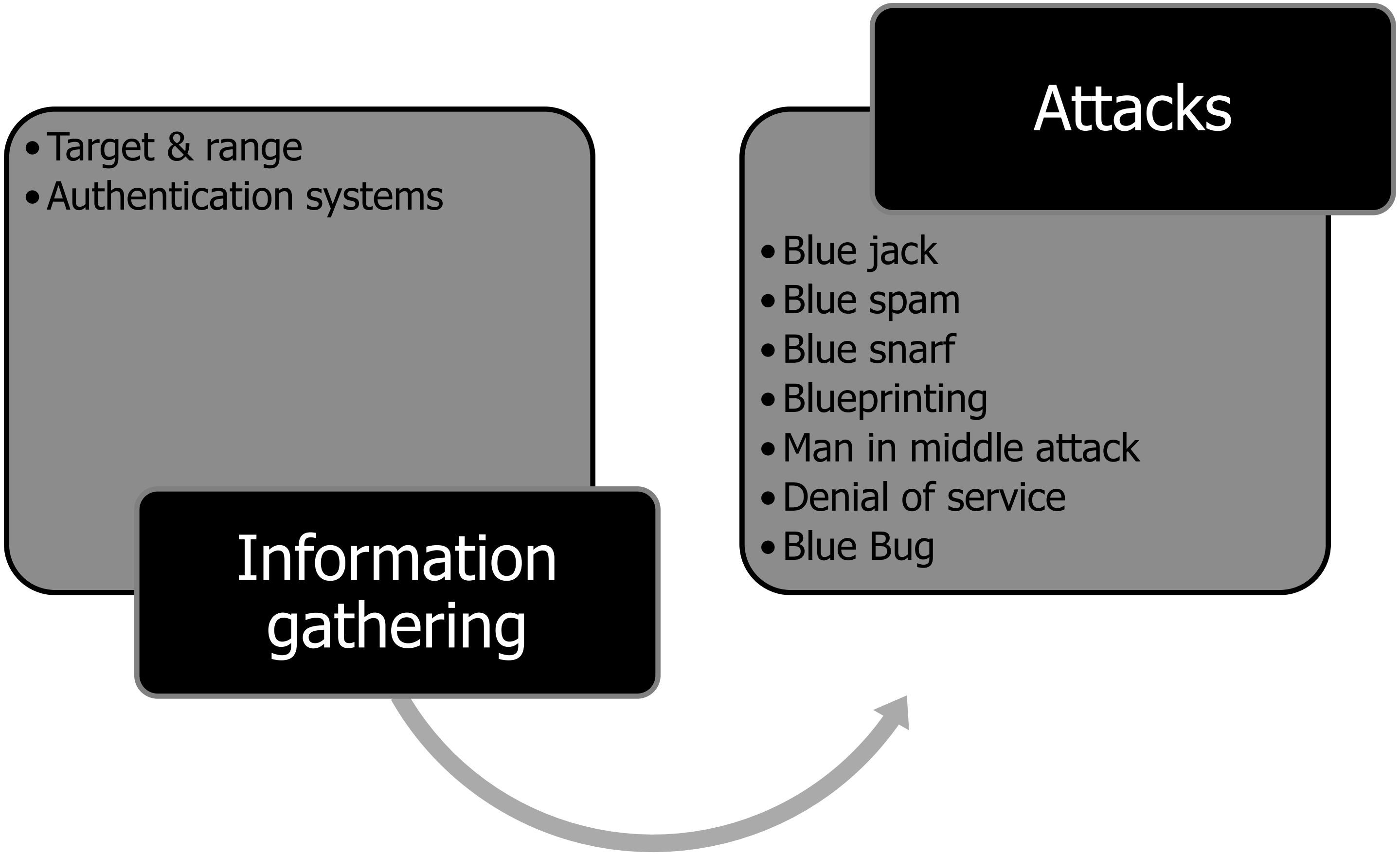
Bluetooth technology is becoming popular short-range radio link designed to connect portable and/or fixed electronic devices. Bluetooth specification defines security at the link level, allowing flexibility in the application security design. Bluetooth system provides for three basic security services: 1) Confidentiality 2) Authentication 3) Authorization

Vulnerabilities :

- Default Configuration
- Weak PINS
- Eavesdropping and Impersonation
- No user authentication
- Unsecure Master keys
- Physically insecure locations



Bluetooth Attacking & Methodology



Information gathering

- Target & range
- Authentication systems

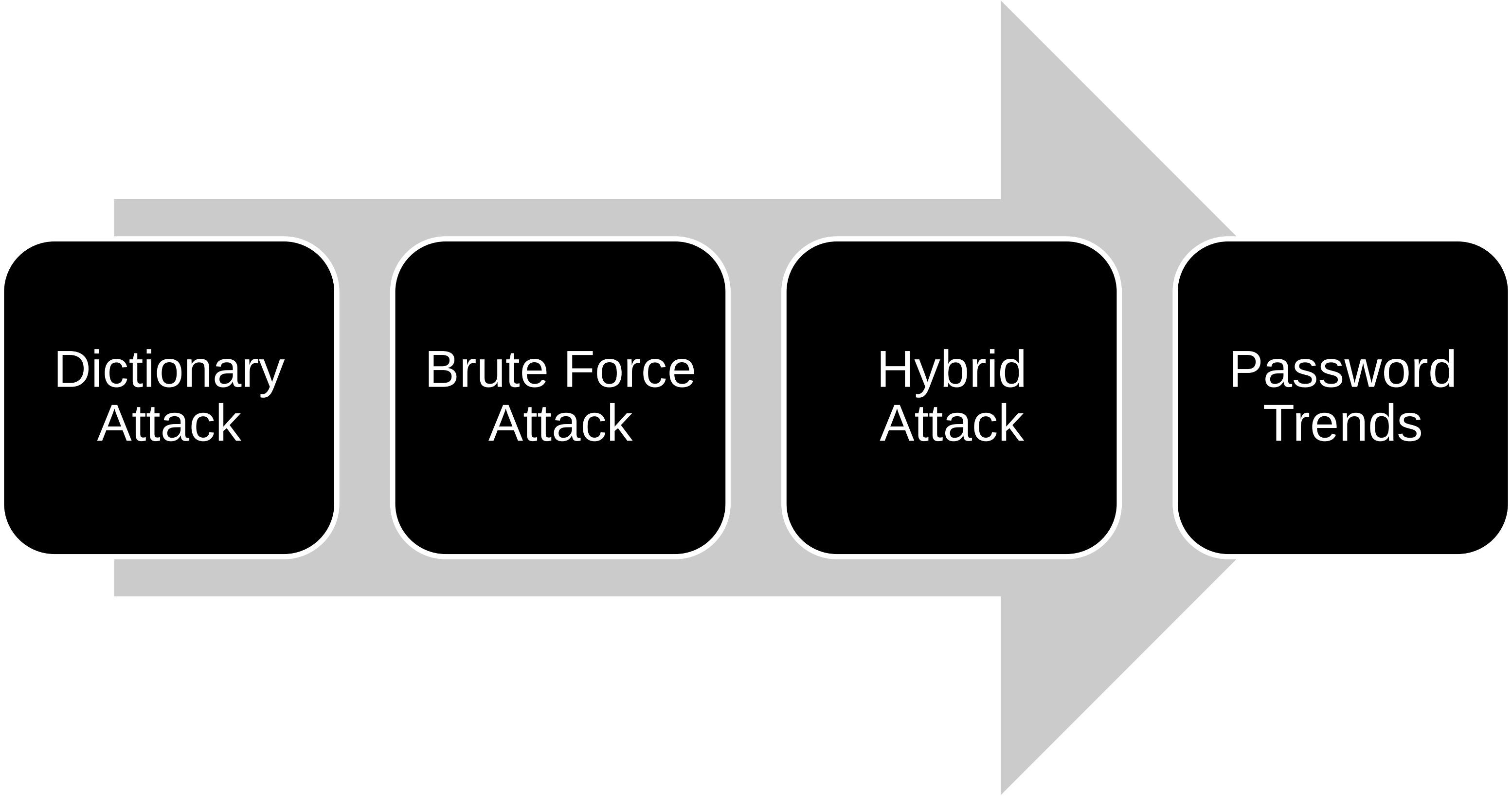
Attacks

- Blue jack
- Blue spam
- Blue snarf
- Blueprinting
- Man in middle attack
- Denial of service
- Blue Bug

How to Prevent Bluetooth Hacks

- ❑ Switch off blue tooth when not in use
- ❑ Strong PIN codes – long & dynamic
- ❑ Vendor configuration removal
- ❑ Non – Discoverable Mode after paring
- ❑ Switch off – unnecessary SCO/eSCO links

Password Hacking



Dictionary Attack

Brute Force Attack

Hybrid Attack

Password Trends

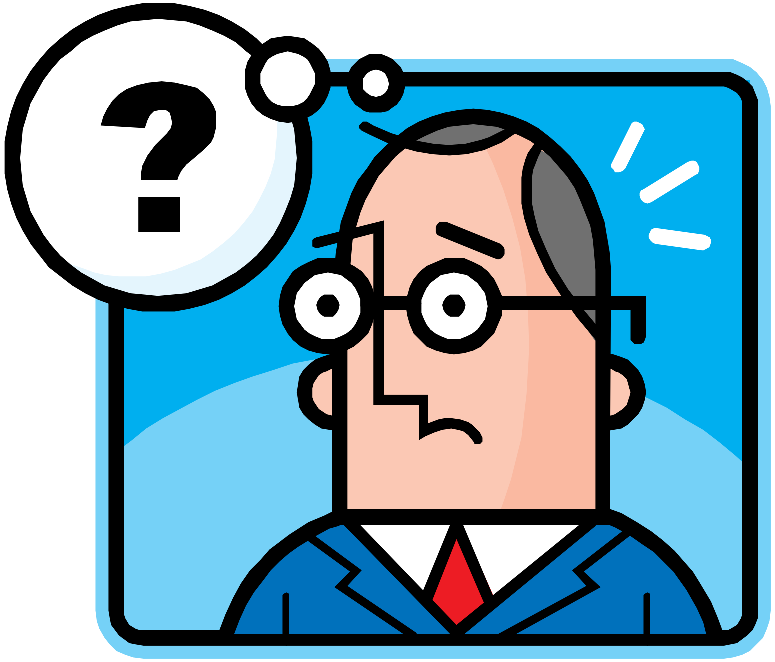
Ways to Prevent Applications from password Hacks

- ❑ Remove Guessable & vendor default
- ❑ URL String Password Disclosure
- ❑ Remove from cookies
- ❑ Account information in an Encryption database

Best practices

- ❖ Do not add a single digit or symbol before or after a word – for example, “microsoft1”
- ❖ Do not double up a single word – for example, “msoftmsoft”
- ❖ Do not simply reverse a word – for example, “tfosorcim”
- ❖ Do not remove the vowels– for example, “io”
- ❖ Key sequences that can be easily repeated - for example, “qwerty”, “asdf” etc.
- ❖ Do not garble letters– for example, converting e to 3, L to 1, o to 0, as in “z3ro – 10v3”

Q & A



THANK YOU