The Future of Wiretapping

Susan Landau
Privacyink.org

The Future of Wiretapping

- Once upon a time … phones stayed fixed and wiretapping was easy.

The Future of Wiretapping

- Once upon a time … phones stayed fixed and wiretapping was easy.

- Then phones began to move.

The Future of Wiretapping

- Once upon a time … phones stayed fixed and wiretapping was easy.

- Then phones began to move.
- And then voice comms got more complicated.

The Future of Wiretapping

The Future of Wiretapping

- The FBI solution: new laws.

The Future of Wiretapping

- The FBI solution: new laws.

  Require that services and apps be tappable.

The Future of Wiretapping

- The FBI solution: new laws.

  Require that services and apps be tappable.

This creates security risks, threatens innovation.

The Future of Wiretapping

- The FBI solution: new laws.

  Require that services and apps be tappable.

This creates security risks, threatens innovation.

- There is another way.

The Future of Wiretapping

- The FBI solution: new laws.

  Require that services and apps be tappable.

This creates security risks, threatens innovation.

- The Vulnerability Solution:

  No added risks --- and it has to be done anyway.

Why is IP Wiretapping Difficult?

- Infrastructure provider is not the service provider.
- New services all the time.
- Peer to Peer.
- Encryption.
- Mobility.

Building Wiretapping Capabilities into Communications Infrastructure Creates Risk

- Ripe, rich target.
- Central point of failure.

These risks are not hypothetical: Vodafone Greece

These risks are not hypothetical: Vodafone Greece

These risks are not hypothetical: Telecom Italia

These risks are not hypothetical: the NSA experience

- **All** CALEA-compliant switches tested by NSA had security risks.

The risks are not hypothetical: CALEA applied to IP networks

- Cisco wiretapping architecture for IP-networks based on European standards for law-enforcement interception;
- If recommended cryptography is not used, it is easy to spoof; unauthorized parties receive interception.

The risks are not hypothetical: CALEA applied to IP networks

- Probes into Google from China discovered which Google users were the subject of wiretap orders.

Building Wiretapping Capabilities into Communications Apps Creates Risk

- Either the developer puts the capability in, and responds to each access request …

- Or the developer enables remote access to the device by other parties.

Building Wiretapping Capabilities into Communications Apps Creates Risk

- Either the developer puts the capability in, and responds to each access request …

- Or the developer enables remote access to the device by other parties.

- Furthermore, it won't work.

Crypto, open-source software, off-shore services are problems.

Bottom Line:

- CALEA applied to PSTN risky.

- CALEA applied to IP networks much more so.

Internet Apps

- The Internet encourages lightweight applications.
- Built quickly.
- And consequently hard to secure.

Internet Apps

- The Internet encourages lightweight apps.
- Built quickly.
- And consequently hard to secure.

That's BAD.

Internet Apps

- The Internet encourages lightweight apps.
- Built quickly.
- And consequently hard to secure.

Another way to look at it: Easy to Exploit.

Wiretapping The Target (the IP Way):

- No alligator clips, no headset.
- No wiretapping while standing in the dark basement.

Wiretapping the Target: The IP Way

- Instead we must use the tools we have.

Wiretapping the Target: The IP Way

- Get a warrant.

Wiretapping the Target: The IP Way

- Get a warrant.

- Probe the target's device to discover OS, version, applications, versions.

Wiretapping the Target: The IP Way

- Get a warrant.
- Probe the target's device to discover OS, version, applications, versions.
- Get a warrant.

Wiretapping the Target: The IP Way

- Get a warrant.

- Probe the target's device to discover OS, version, applications, versions.

- Get a warrant.

- Download the wiretap apps using a vulnerability tailored to the OS or apps on the target device.

Wiretapping the Target: The IP Way

WHAT ?

Wiretapping the Target: The IP Way

- Get a warrant.
- Probe the target's device to discover OS, version, applications, versions.
- Get a warrant.
- Download the wiretap using a vulnerability tailored to the OS or apps on the target device.

Wiretapping the Target: The IP Way

Can This Really Work?

- A stable of working vulnerabilities.

- A careful policy to protect targets and the public.

Wiretapping the Target: The IP Way

Can This Really Work?

- A stable of working vulnerabilities.
- A careful policy to protect targets and the public.
- State and local law enforcement use FBI tools.

The Vulnerabilities Market

- Common Vulnerabilities Enumeration (CVE): weekly listing of newly published vulnerabilities. Authoritative, though not necessarily up to date.
- Private companies: Vupen, VulnerabilityLab, Secunia.
- Private dealers.

The Vulnerabilities Market

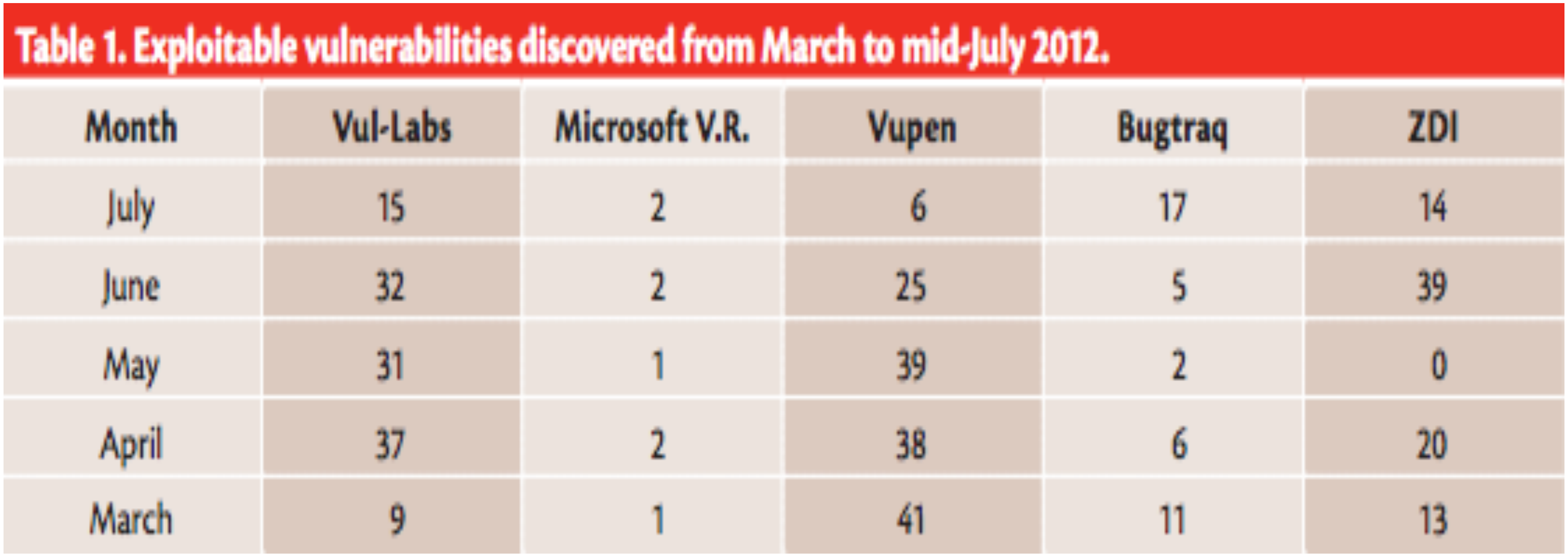

Table 1. Exploitable vulnerabilities discovered from March to mid-July 2012.

Month	Vul-Labs	Microsoft V.R.	Vupen	Bugtraq	ZDI
July	15	2	6	17	14
June	32	2	25	5	39
May	31	1	39	2	0
April	37	2	38	6	20
March	9	1	41	11	13

Law Enforcement and the Vulnerabilities Market

- Law enforcement must discover --- or purchase --- a vulnerabliity.

- Zero-day exploit.

Law Enforcement and the Vulnerabilities Market

- Law enforcement must discover --- or purchase --- a vulnerability.

- Zero-day exploit.

- Will there be enough vulnerabilities?

Law Enforcement and the Vulnerabilities Market

- Law enforcement must discover --- or purchase --- a vulnerability.

- Zero-day exploit.

- Will there be enough vulnerabilities?

Unfortunately yes.

Law Enforcement and the Vulnerabilities Market

- Law enforcement must discover --- or purchase --- a vulnerability.
- Zero-day exploit.
- Exploit it? Report it?

Law Enforcement and the Vulnerabilities Market

- Law enforcement must discover --- or purchase --- a vulnerabliity.
- Zero-day exploit.
- Exploit it? Report it? --- Do Both.

Law Enforcement and the Vulnerabilities Market

- Report and exploit?

Time to patch is slow.

Monthly or bimonthly patch releases, delays, etc.

Law Enforcement and Using Vulnerabilities

- Is this legitimate?

Law Enforcement and Using Vulnerabilities

- Is this legitimate?

- By reporting, increasing security.

Law Enforcement and Using Vulnerabilities

- Is this legitimate?
- By reporting, increasing security.
- Only exploiting when there is a wiretap order.

Law Enforcement and Using Vulnerabilities

- Is this legitimate?

- Could this be increasing the vulnerabilities market?

Law Enforcement and Using Vulnerabilities

- Is this legitimate?

- Could this be increasing the vulnerabilities market?

No, the vulnerabilities market is dominated by national-security organizations, not law enforcement.

Preventing Dirty Play

Preventing Dirty Play

- Enforce reporting of vulnerabilities.

- Ensure that only the targeted material is accessed, and not other material.

What We're Proposing

- Use precisely targeted vulnerabilities to accomplish legally authorized wiretaps.

- Do this instead of building wiretap capabilities into all infrastructure and applications.

Two Final Points

- Better to use vulnerabilities present in communications infrastructure and apps than to introduce new ones to ensure wiretapping capability.

- Law enforcement will **not** be introducing new vulnerabilities, only exploiting those already present.

Further Reading

- Bellovin, Blaze, Clark, and Landau, “Going Bright: Wiretapping without Weakening Communications Infrastructure,” *IEEE Security and Privacy*, Jan/Feb 2013.

- “CALEA II: Risks of Wiretap Modifications to Endpoints,” May 17, 2013, https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf

- “Eavesdropping on Internet Communications,” editorial board, *New York Times*, May 20, 2013, https://www.nytimes.com/2013/05/20/opinion/eavesdropping-on-internet-communications.html

Further Reading

- Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, MIT Press, 2011.
- Schneier, “The FBI's New Wiretapping Plan is Great News for Criminals,” *Foreign Policy*, May 29, 2013.