Virtual Private Networks

Expounded Casually for the Novice Computer User

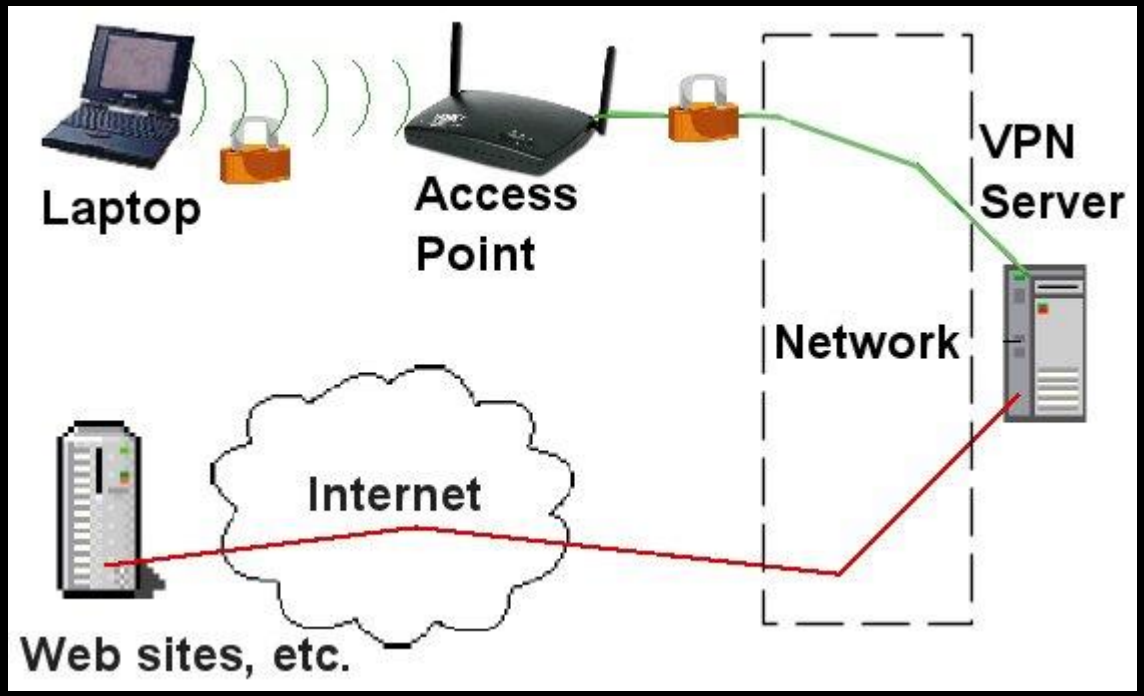
Disclaimer

Any opinions presented in this talk by the presenter do not in any way represent an official endorsement of these opinions by Freeside Technology Spaces, Inc., nor is intended to reflect the views of Freeside and its membership.

Freeside does not encourage or promote any illegal activity, including but not limited to downloading content protected by copyright.

"*Content theft is no victimless crime*," says former US Senator Chris Dodd, now CEO of the MPAA who earns a salary of $2.4 million (2011) as a lobbyist.

What is this so-called "VPN"?



Packet Sniffers

tcpdump
ettercap
Wireshark
...and others

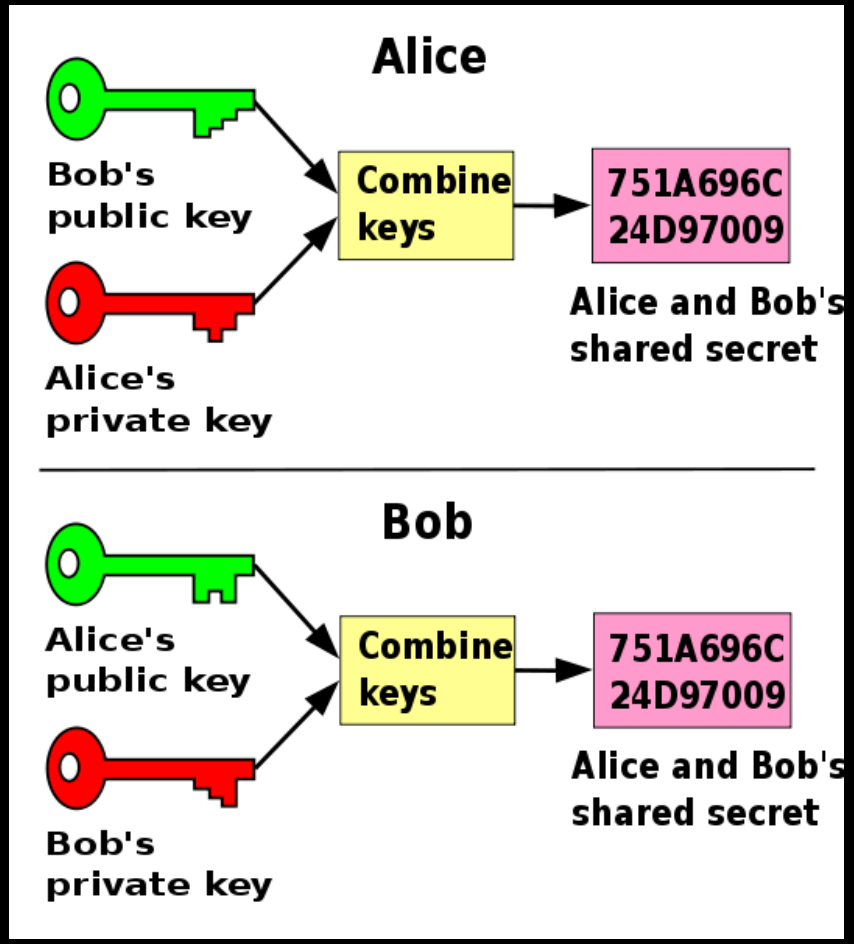
Packet sniffers (aka *analyzers*) can be used to intercept your network data, including encrypted connections!

Public-Key Cryptography

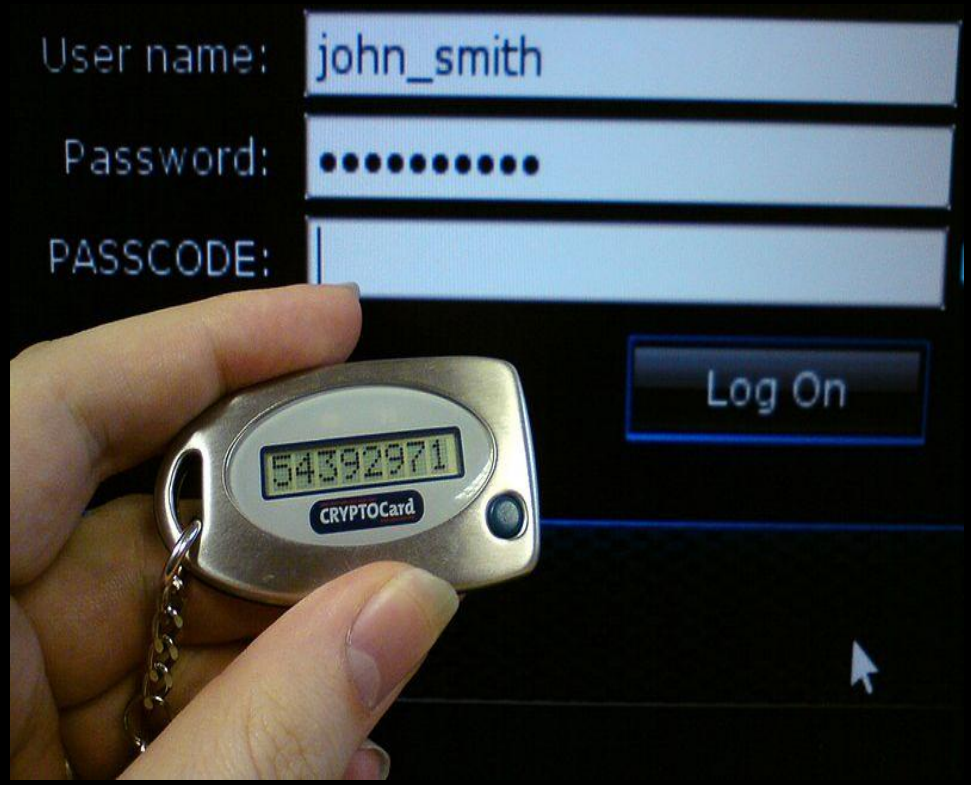
Key pairs are exchanged between Alice and Bob in this manner to encrypt and decrypt messages.

The public keys (in green) can be freely posted on the Internet.

The private keys (in red) must be kept secret (ex. stored on an encrypted USB drive).



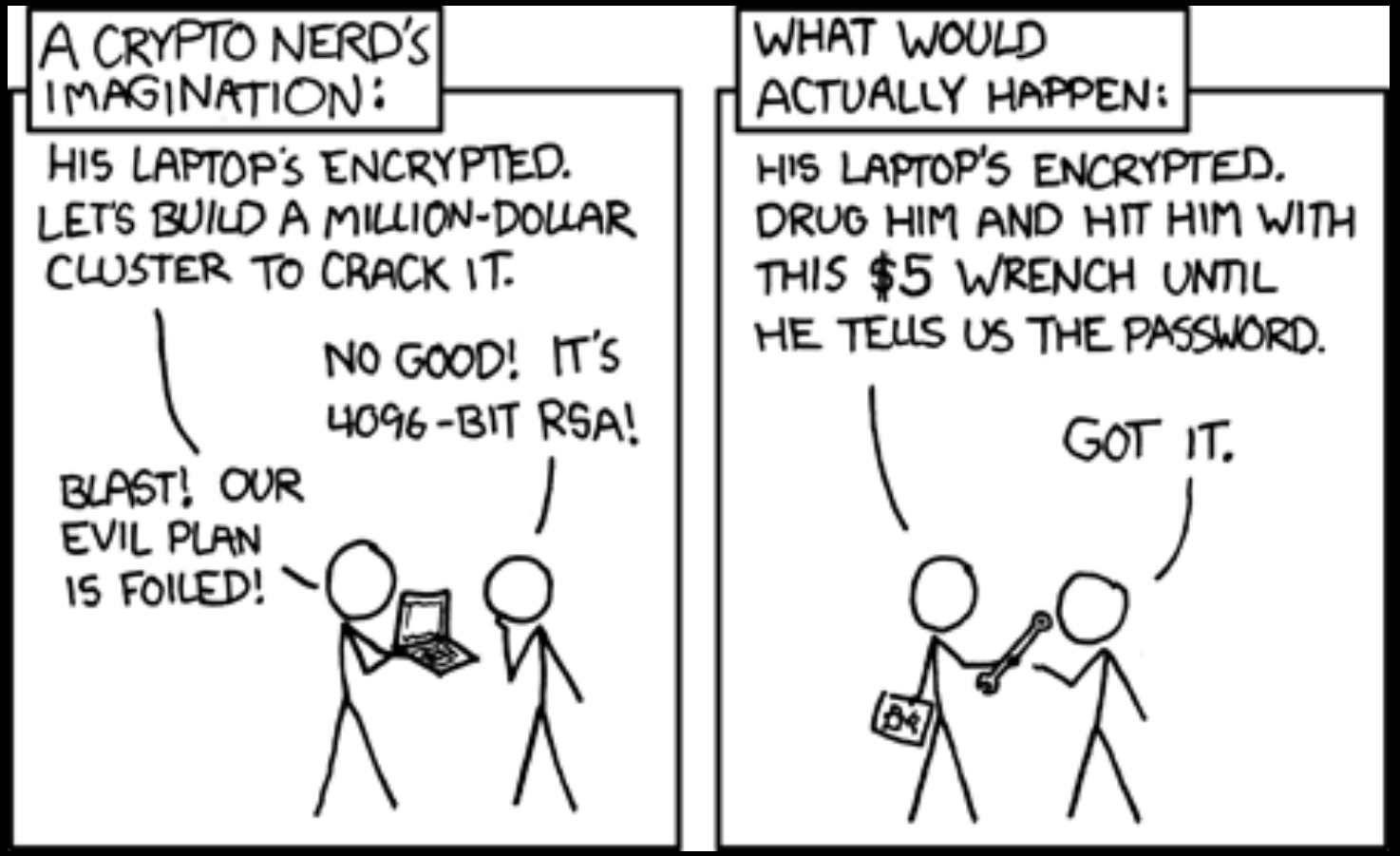
Two-Factor Authentication



In some cases, tokens with codes are issued that provide a secondary means of verifying your identity.

The thinking goes, an attacker needs both your password and token to pass as you.

Rubber Hose Cryptanalysis



Our your token can be easily pick-pocketed...

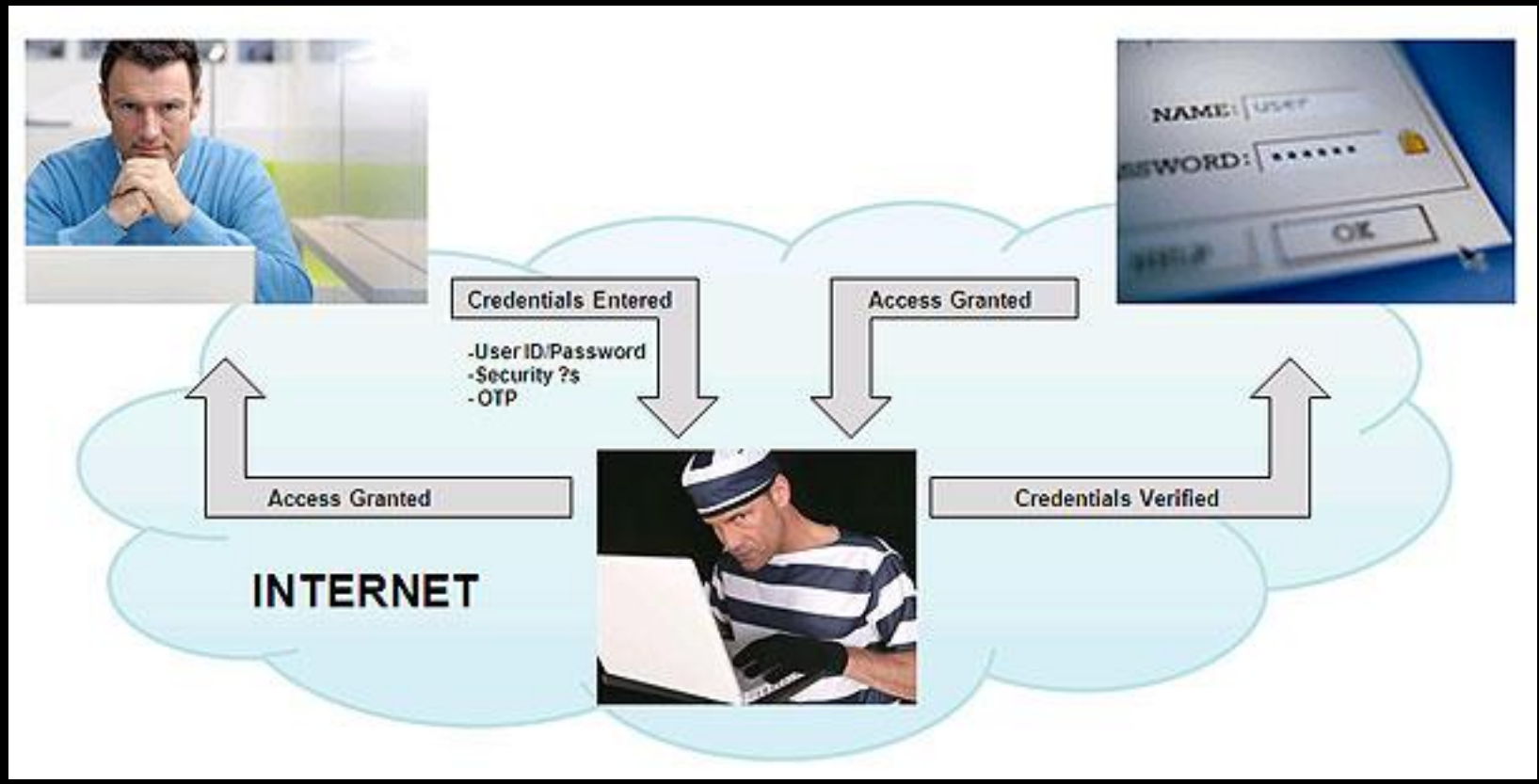
VPN without Borders

Reasons to use a VPN service:

- Access content restricted by region (ex. BBC iPlayer)
- Access paid content in your home country from another (ex. Hulu Plus)
- Securely access business resources when traveling abroad
- Anonymously perform competitive analysis at home and abroad
- Additional layer of security and privacy when using "free" wifi
- Bypass government surveillance, censorship, or firewalls (ex. Great Firewall of China)
- Anonymous communication for whistleblowing or releasing information to journalists
- Privacy Protests, or using cryptography as a form of non-violent resistance
- Safe access to support forums and resources for people living under hostile regimes (ex. women in Saudi Arabia, LGTBQ persons in Gambia)

Man-in-the-Middle (MITM) Attack

Illustrated by stock photography:



Government-in-the-Middle Attack

Illustrated by released top-secret NSA slides:

Legal Considerations

Copyright trolls want you to settle quickly and quietly, so they can continue to abuse the legal system.

In many cases, copyright trolls don't even own the copyrights to the work they are threatening to sue you for.

Corporations and Governments: Super Friends

- Fan-created Subtitle Site Raided by Swedish Police (July 2013)
- Microsoft Sued over 'Mafia-Like' Anti-Piracy Raid (June 2013)
- Five Undercover Police Cars Sent To Arrest Single Alleged Movie Pirate (May 2013)
- Japanese Police Arrest 27 File-Sharers in Nationwide Show of Force (February 2013)
- Men Face Deportation [from South Africa] for Running World's Least-Visited Torrent Site (December 2012)
- Police Raid 9-Year-Old Pirate Bay Girl, Confiscate Winnie the Pooh Laptop (November 2012)
- Wikileaks: MPAA collaboration with ICE

Opinions on legal and moral issues surrounding copyright may vary, but there are two undeniable facts from the past few years:

- Police are increasingly becoming militarized; and
- Corporations are using government to a far greater degree to protect their business interests, in unprecedented ways

Open Wireless Movement

When running an open wifi, it's probably best if you route the "public" traffic through a VPN.

Next time on CryptoParty...

How to turn a Raspberry Pi into an Open Wifi hotspot, with VPN out!

VPN Provider Policies

- Provider Logging
  - origin IP address
  - exit IP address
  - unencrypted internet traffic
  - don't forget to consider national/supra-national policies on data retention (ex. EU directives)
- Payment Options
  - cash or bitcoin?
  - paypal accepted?
  - credit cards? pre-paid cards?

How anonymous do you need to be?

Anonymity Considerations

- Transmitting information reveals parts of your identity (bits)
- Researchers found that **four data points** could uniquely identify 95% of cell phone
- Stay anonymous: don't visit your bank accounts or check your email
- VPN service providers can be subpoenaed for information, logs
- **Whistleblower's paradox**: don't reveal information if you're one of a very small set of people with private knowledge

Panopticlick Demo

Summary: VPN Strengths

Changes your IP address
Routes your internet traffic through an encrypted tunnel
Destination IP could enable access to restricted internet resources

- Strong **supplement** to your privacy on the internet

Summary: VPN Weaknesses

Typically user is unable to verify VPN service provider identity and policies

Faulty configurations could compromise user identity and anonymity

VPN service provider also subject to subpoena and other legal pressures

- Compromises of certificate authorities and MITM attack on VPN providers by government agencies

Thanks!

"They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."

Benjamin Franklin