

Usable Security and User Training

KAMI VANIEA
JANUARY 25

KAMI VANIEA

1

Think about it:

Is the Doodle link to the right secure?

Sign up for tutorial sessions

<http://doodle.com/poll/t7ia4mbv9vk8ekek>

Link is also available on the website, which is at:

<http://www.inf.ed.ac.uk/teaching/courses/cs/>

KAMI VANIEA

2

First, the news...

- And someone messes up SSL certs again...
 - <http://arstechnica.co.uk/security/2016/09/firefox-ready-to-block-certificate-authority-that-threatened-web-security/>
 - http://www.theregister.co.uk/2011/08/29/fraudulent_google_ssl_certificate/
 - <http://arstechnica.com/security/2015/10/still-fuming-over-https-mishap-google-gives-symantec-an-offer-it-cant-refuse/>
 - <http://arstechnica.com/security/2015/02/lenovo-pcs-ship-with-man-in-the-middle-advare-that-breaks-https-connections/>

KAMI VANIEA

3

Quick explanation of SSL

We will cover this in more detail later

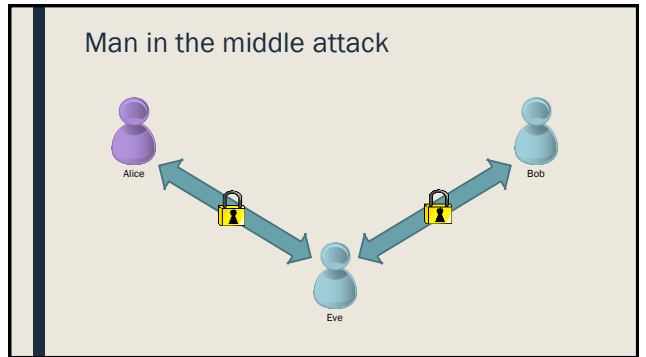
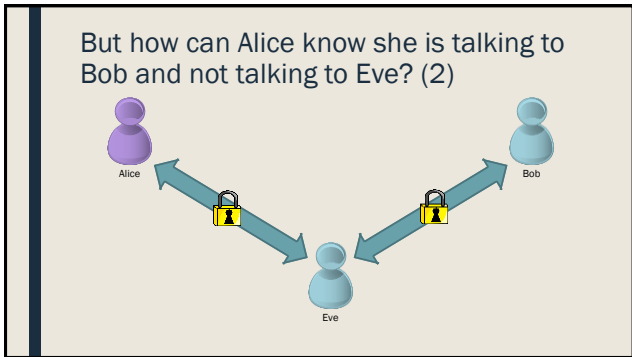
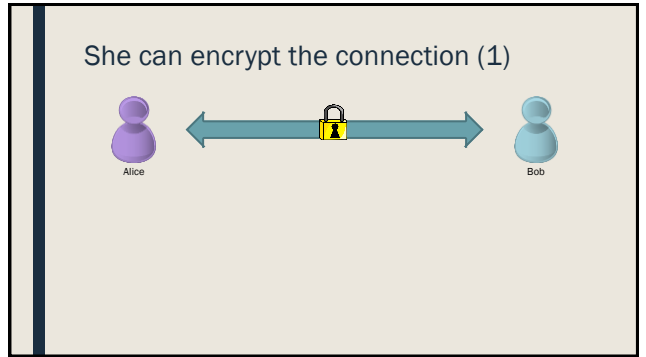
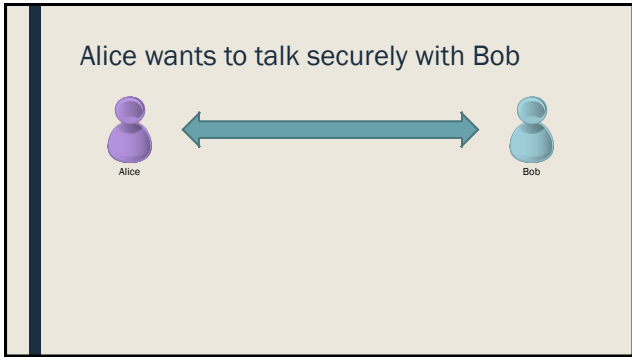
KAMI VANIEA

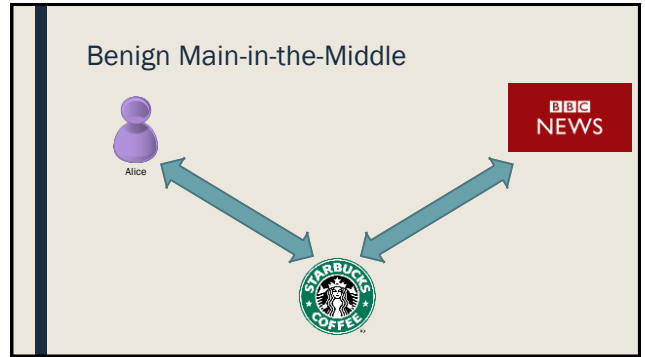
4


Slides with this background are from a talk given at the Royal Society Frontiers of Science event on why encryption is not adopted at scale

Encryption (in transit) properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed**
 - No one can read what you sent
 - No one can change what you sent
2. **Knowing who** you are communicating with
 - You are talking to who you think you are talking to and not someone else



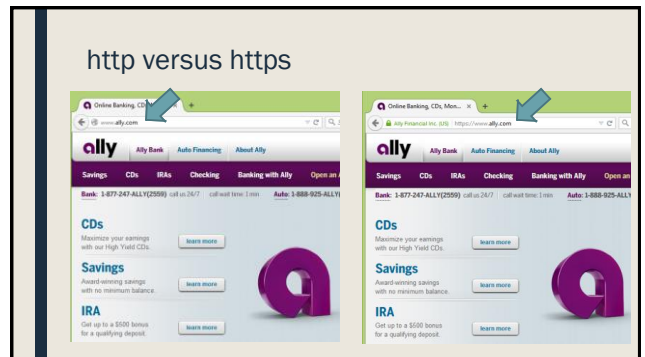




<https://ally.com>

 versus

<http://ally.com>



Encryption properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed**
 - No one can read what you sent
 - No one can change what you sent
2. **Knowing who** you are communicating with
 - You are talking to who you think you are talking to and not someone else

Key management

- Public/private key pairs
 - Give public keys to other people
 - Keep private keys private
 - Verify other people's public keys
- Keys are linked to identities
- A private key should NEVER be shared, so only one entity theoretically has access to it
- Possession of a private can be cryptographically proven when starting a communication IF you have the public key

My public key

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA...
-----END PUBLIC KEY-----
```

Idea: Certificate Authorities can do the verification instead of users

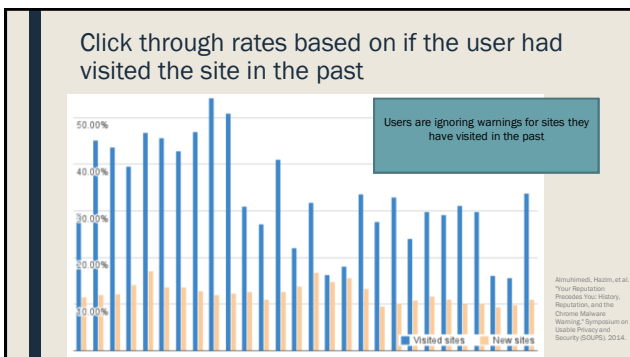
Adrienne Porter Felt @apf_

hey @Gogo, why are you issuing *.google.com certificates on your planes?

Real world click-through rates

- Studied the click-through rate for malware and HTTPS warnings
- Malware
 - Firefox 7.2%
 - Chrome 23.2%
- Phishing
 - Firefox 9.1%
 - Chrome 18.0%
- HTTPS
 - Firefox 33.0%
 - Chrome 70.2%

Almuhamed, Hazim, et al. "Your Reputation Precedes Your History, Reputation, and the Chrome Malware Warning." Symposium on Usable Privacy and Security (SOUPS), 2014.



Why do people click through the warnings?

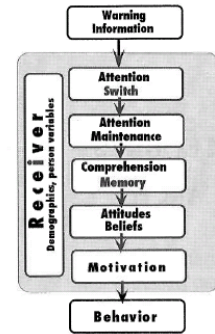
- The site is used often and trusted
 - "YouTube is a well known website. I'd assume that the malware block is in error."
- The person who posted the link is trusted
 - "I find it harder to believe [the warning] when my facebook friend just posted it and had no problems."
- The site where the link is assumed to have good security
 - "I presume that visiting youtube from a facebook link would be safe."
- They think they are safe
 - "I use Linux I'm not afraid of anything."
 - "I have an anti virus"

Why people don't use privacy protections

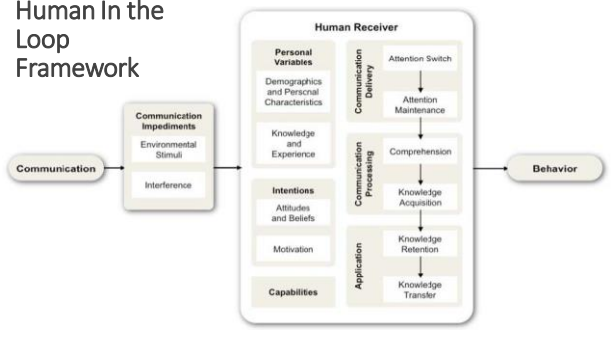
1. People don't really care about privacy
2. People are not aware of the privacy issues
3. People are not aware of how to protect themselves
4. People are aware, but are unable to use the privacy protections

Communication-Human Information Processing Model (C-HIP)

- Developed to model why people do or don't understand road signs
- We adapted it to computer security

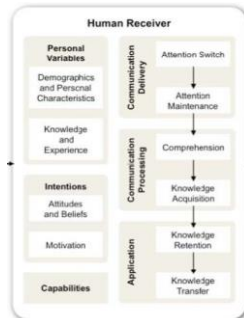


Human in the Loop Framework

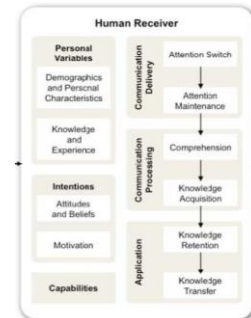
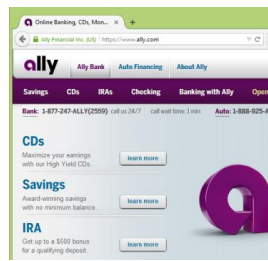


We are now going to use the framework to figure out why people are ignoring SSL warnings...

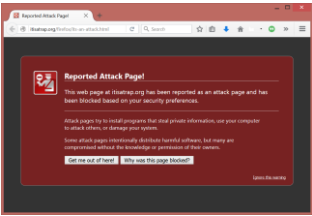
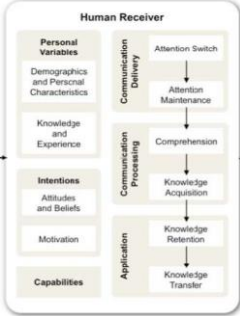
What level of the framework does this fail at?



And this one?


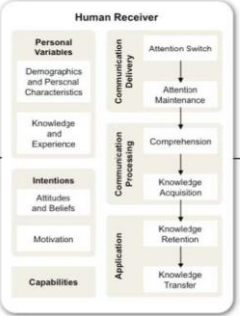


And this one?

The diagram illustrates the Human Receiver model, which is a vertical flowchart. On the left, it lists five categories: Personal Variables (Demographics and Personal Characteristics), Knowledge and Experience, Intentions (Attitudes and Beliefs), Motivation, and Capabilities. On the right, it shows a sequence of cognitive processes: Attention Switch, Attention Maintenance, Comprehension, Knowledge Acquisition, Knowledge Retention, and Knowledge Transfer. A central column labeled 'Communication Processing' connects these stages, with 'Communication Delivery' at the top and 'Application' at the bottom.

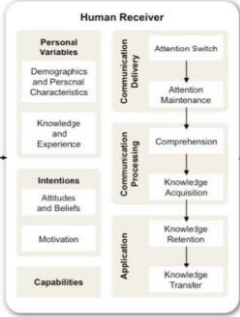
Any better?

This slide is identical in layout to the previous one, but the screenshot shows a Chrome browser warning page with a blue and red design, indicating a malware warning.

And this one?

- The site is used often and trusted
 - “YouTube is a well known website. I’d assume that the malware block is in error.”
- The person who posted the link is trusted
 - “I find it harder to believe [the warning] when my facebook friend just posted it and had no problems.”
- The site where the link is assumed to have good security
 - “I presume that visiting youtube from a facebook link would be safe.”
- They think they are safe
 - “I use Linux I’m not afraid of anything.”
 - “I have an anti virus”



The diagram is identical to the previous ones, showing the Human Receiver model.

Users

DAVE LINCOLN 34

Users are not the enemy

- Malicious actors are the enemy
- Users are a partner in keeping the system secure
- Like any partner:
 - They have skills you don’t have
 - They are missing skills you do have
- Think about what skills they have that you need
- Use the skills you have to make good decisions on users’ behalf

DAVE LINCOLN 35

Phishing attacks and training

DAVE LINCOLN 35

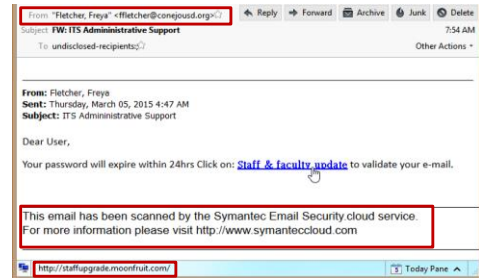
Phishing

- Phishing – Attempting to trick someone into taking the “bait” and interacting in a way they should not.
 - Typically involves the impersonator pretending to be someone else that the person trusts
 - Interactions: Clicking a link, opening a file, replying with information, transferring money, ect.
- Spear phishing – Phishing, but with a small number of targets and each email is crafted for that individual
- Whaling – Phishing for people with a lot of money, i.e. CEO
- QRishing – Phishing attacks through QR codes

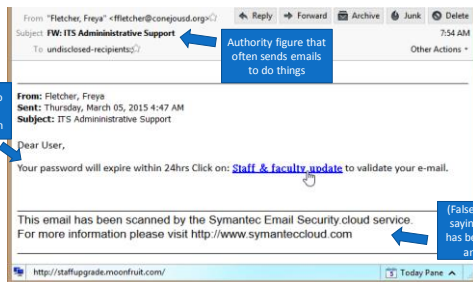
KARL WINKEL

37

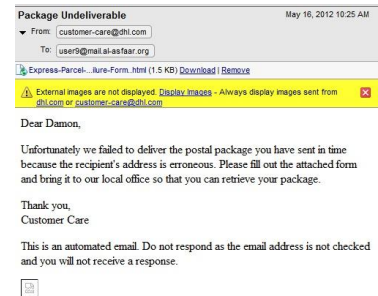
What on this email can be trusted?



(Wrong) Trust indicators



Sneaky email to get the recipient to open the attachment, which is an html document



Problem: Users click on links and attachments

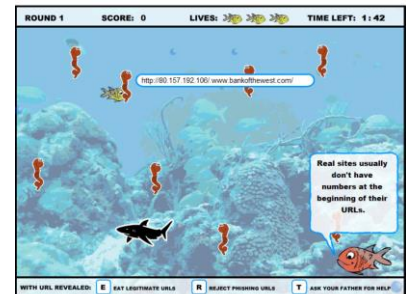
- Scan all incoming attachments and links for blacklisted content
- Teach users
 - Only click if you are expecting the email
 - Do not open attachments unless you are expecting them
 - If you are not sure, contact the person or company separately and ask if they sent the email
 - If you are not sure, contact the IT department
 - Banks and credit card companies will never contact you this way

KARL WINKEL

41

Anti-Phishing Phill

- Serious game to help people learn to spot dangerous URLs
- Training sometimes works
- But it takes time
- And people forget



KARL WINKEL

42

PhishGuru

- Comic to train people to spot phishing attacks
- Best time to train is after a users has already fallen for an attack
- Send out fake attacks and train those who click on them

Give users options that make sense and work for them

PhishGuru

- Users know what they are expecting
- Users know who the email looks like it is from
- Users can do an out-of-band contact (phone call)
- Users do not want to ignore a serious issue

In Summary...

- Academics say in-the-moment training works
- Chief Security Officers (CSOs) have mixed opinions
- Everybody thinks that users clicking on links and attachments is a big problem

Why show warnings at all?

- Determined users might disable Safe Browsing. Which would prevent future warnings.
- User could also open the website in another browser that is less safe and does not block the website.
 - America Online users used to go to a friend's house to open malicious sites because the ISP blocked malicious sites.
 - Different browsers block different sets of sites, we don't want to teach users to use less safe browsers.

Questions