

CSE 484 / CSE M 584: Computer Security and Privacy

Usable Security

Fall 2016

Ada (Adam) Lerner

lerner@cs.washington.edu

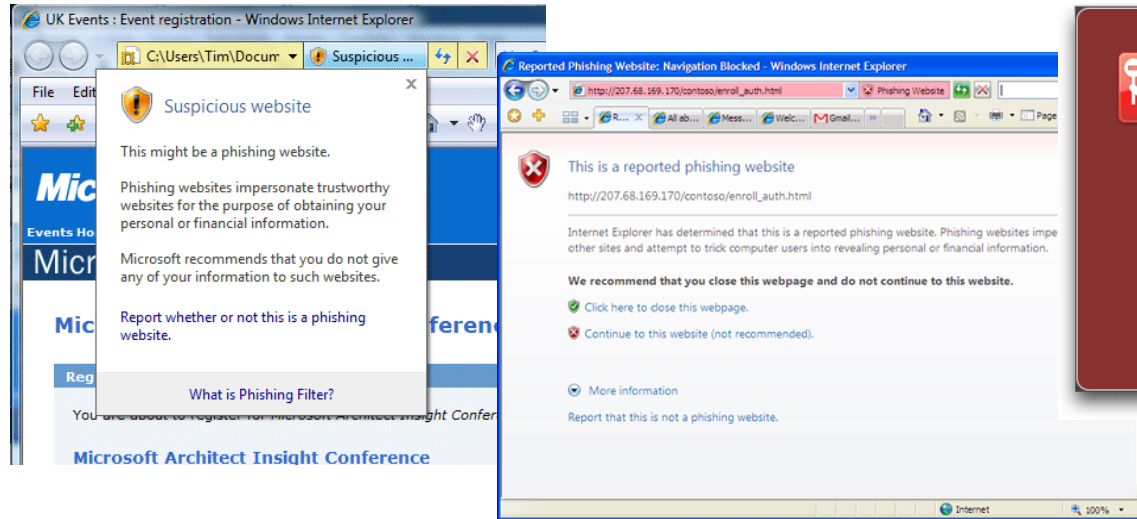
Thanks to Franz Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Safe to Type Your Password?



Active vs. Passive Warnings

- Active warnings significantly more effective
 - Passive (IE): 100% clicked, 90% phished
 - Active (IE): 95% clicked, 45% phished
 - Active (Firefox): 100% clicked, 0% phished



Passive (IE)

Active (IE)

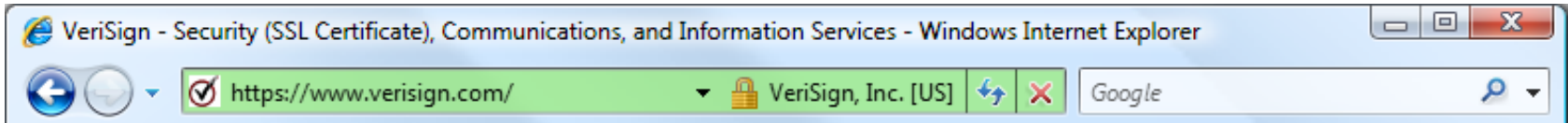


Active (Firefox)

Why Do Users Ignore Warnings?

- Don't trust the warning
 - “Since it gave me the option of still proceeding to the website, I figured it couldn't be that bad”
- Ignore warning because it's familiar (IE users)
 - “Oh, I always ignore those”
 - “Looked like warnings I see at work which I know to ignore”
 - “I thought that the warnings were some usual ones displayed by IE”
 - “My own PC constantly bombards me with similar messages”

The Lock Icon



- Goal: identify secure connection
 - SSL/TLS is being used between client and server to protect against active network attacker
- Lock icon should only be shown when the page is secure against **network attacker**
 - Semantics subtle and not widely understood by users
 - Whose certificate is it??
 - Problem in user interface design

Site Authentication Image (SiteKey)

Bank of America | Online Banking | SiteKey | Verify SiteKey - Windows Internet Explorer

https://sitekey.bankofamerica.com/sas/signonSetup.do

Bank of America | Online Banking | ...


Bank of America Higher Standards Online Banking

Confirm that your SiteKey is correct

If you recognize your SiteKey, you'll know for sure that you are at the valid Bank of America site. Confirming your SiteKey is also how you'll know that it's safe to enter your Passcode and click the **Sign In** button.

An asterisk (*) indicates a required field.

Your SiteKey:
pelicans



If you don't recognize your personalized SiteKey, don't enter your Passcode.

* Passcode:
(4 - 20 Characters, case sensitive)

Sign In

If you don't recognize your personalized SiteKey, don't enter your Passcode

Do These Indicators Help?

- “The Emperor’s New Security Indicators”
 - <http://www.usablesecurity.org/emperor/emperor.pdf>

Score	First chose not to enter password...	Group				Total
		1	2	3	1 ∪ 2	
0	upon noticing HTTPS absent	0 0%	0 0%	0 0%	0 0%	0 0%
1	after site-authentication image removed	0 0%	0 0%	2 9%	0 0%	2 4%
2	after warning page	8 47%	5 29%	12 55%	13 37%	25 44%
3	never (always logged in)	10 53%	12 71%	8 36%	22 63%	30 53%
<i>Total</i>		18	17	22	35	57

Users don't notice the **absence** of indicators!

Case Study #2: Browser SSL Warnings

- Design question: How to alert the user if a site's SSL certificate is untrusted?

Firefox vs. Chrome Warning

33% vs. 70% clickthrough rate



This Connection is Untrusted

You have asked Chrome to connect securely to **reddit.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**



This is probably not the site you are looking for!

You attempted to reach **reddit.com**, but instead you actually reached a server identifying itself as **a248.e.akamai.net**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **reddit.com**.

You should not proceed, **especially** if you have never seen this warning before for this site.

[Proceed anyway](#) [Back to safety](#)

▶ [Help me understand](#)

Experimenting w/ Warning Design

#	Condition	CTR	N
1	Control (default Chrome warning)		
2	Chrome warning with policeman		
3	Chrome warning with criminal		
4	Chrome warning with traffic light		
5	Mock Firefox		
6	Mock Firefox, no image		
7	Mock Firefox with corporate styling		

Table 1. Click-through rates and sample size for conditions.

Experimenting w/ Warning Design

#	Condition	CTR	N
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman		
3	Chrome warning with criminal		
4	Chrome warning with traffic light		
5	Mock Firefox		
6	Mock Firefox, no image		
7	Mock Firefox with corporate styling		

Table 1. Click-through rates and sample size for conditions.

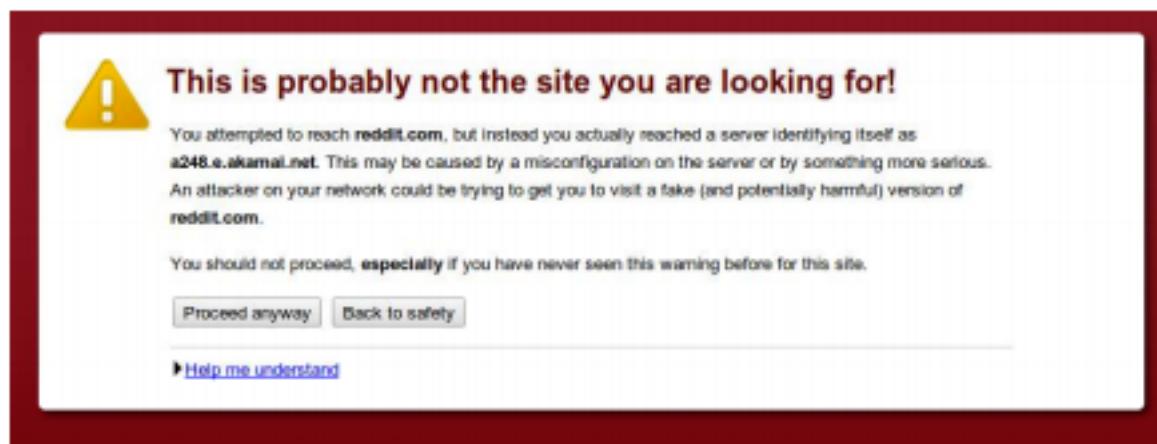


Figure 1. The default Chrome SSL warning (Condition 1).

Experimenting w/ Warning Design

#	Condition	CTR	N
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman	68.9%	17,977
3	Chrome warning with criminal	66.5%	18,049
4	Chrome warning with traffic light	68.8%	18,084
5	Mock Firefox		
6	Mock Firefox, no image		
7	Mock Firefox with corporate styling		

Table 1. Click-through rates and sample size for conditions.



Figure 1. The default Chrome SSL warning (Condition 1).



Figure 4. The three images used in Conditions 2-4.

Experimenting w/ Warning Design

#	Condition	CTR	N
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman	68.9%	17,977
3	Chrome warning with criminal	66.5%	18,049
4	Chrome warning with traffic light	68.8%	18,084
5	Mock Firefox	56.1%	20,023
6	Mock Firefox, no image	55.9%	19,297
7	Mock Firefox with corporate styling		

Table 1. Click-through rates and sample size for conditions.

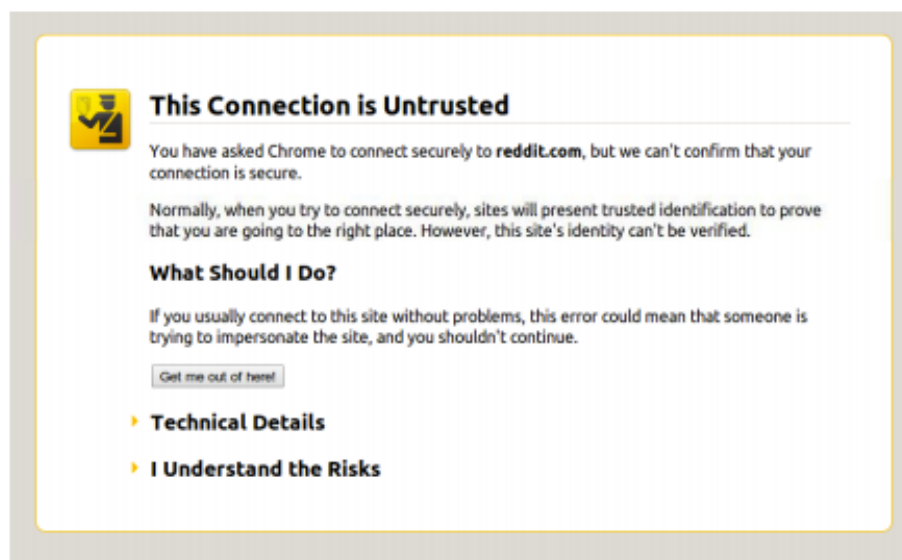
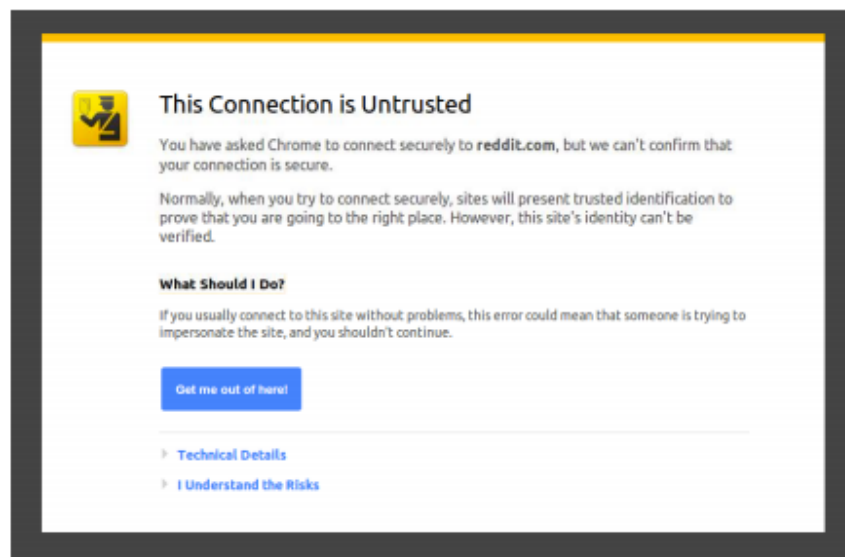


Figure 2. The mock Firefox SSL warning (Condition 5).

Experimenting w/ Warning Design

#	Condition	CTR	N
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman	68.9%	17,977
3	Chrome warning with criminal	66.5%	18,049
4	Chrome warning with traffic light	68.8%	18,084
5	Mock Firefox	56.1%	20,023
6	Mock Firefox, no image	55.9%	19,297
7	Mock Firefox with corporate styling	55.8%	19,845

Table 1. Click-through rates and sample size for conditions.



Opinionated Design Helps!



The site's security certificate is not trusted!

You attempted to reach **192.168.17.129**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

[▶ Help me understand](#)

Adherence	N
30.9%	4,551

Opinionated Design Helps!



The site's security certificate is not trusted!

You attempted to reach **192.168.17.129**, but the server presented a certificate not trusted by your computer's operating system. This may mean that the server's credentials, which Chrome cannot rely on for identity information, or an attacker intercepted your communications.

You should not proceed, **especially** if you have never seen this warning.

Proceed anyway

Back to safety

▶ [Help me understand](#)



Your connection is not private

Attackers might be trying to steal your information from **reddit.com** (for example, passwords, messages, or credit cards).

Proceed to the site (unsafe)

Back to safety

▶ [Advanced](#)



Your connection is not private

Attackers might be trying to steal your information from **www.example.com** (for example, passwords, messages, or credit cards).

[Advanced](#)

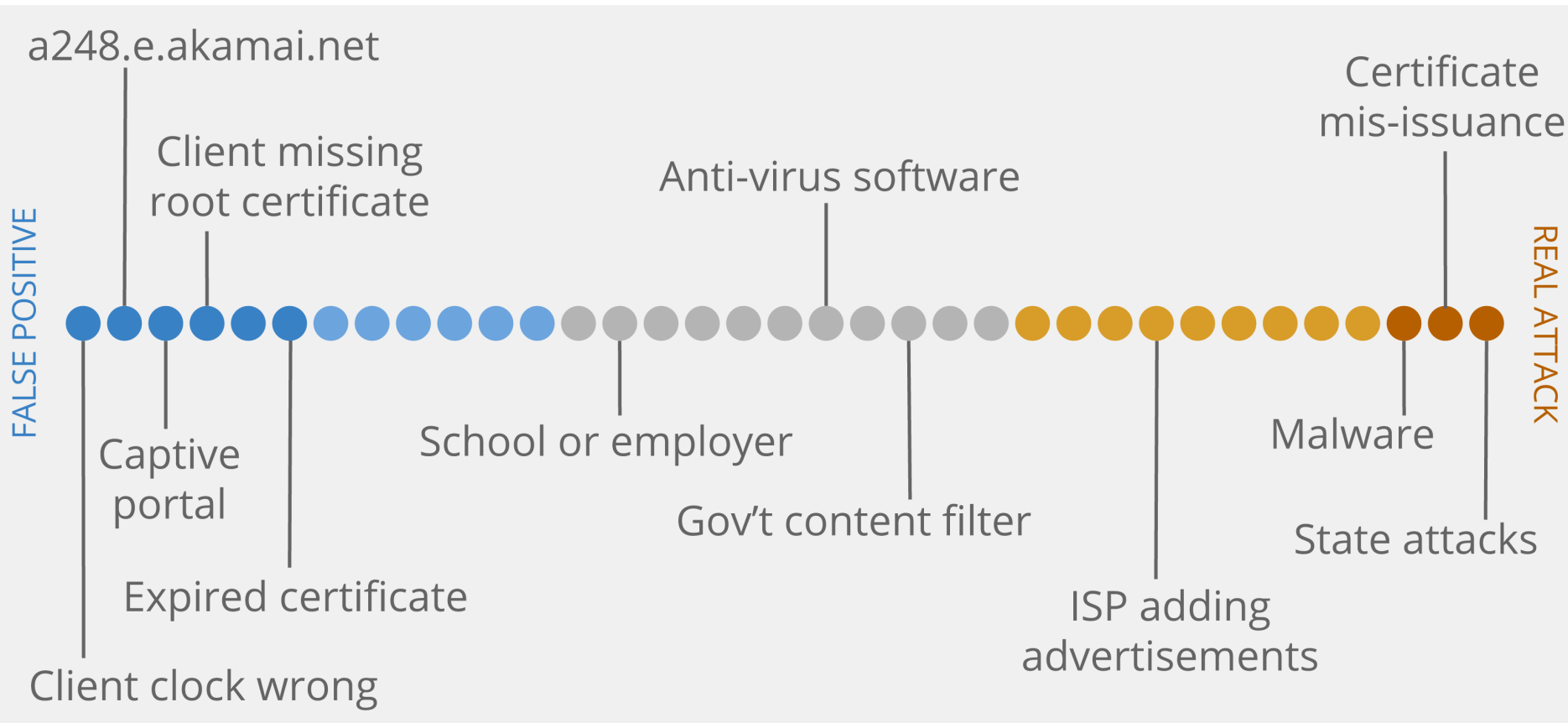
Back to safety

Adherence	N
30.9%	4,551
32.1%	4,075
58.3%	4,644

Challenge: Meaningful Warnings

- In an ideal world, we would only show a warning when there was a real attack!
- Q1: What are some cases where you would get false alarm SSL warnings?

Challenge: Meaningful Warnings



Client Clocks & HSTS

- HSTS: A protocol for websites to tell their clients “always access me over HTTPS”
- 20% of all HSTS warnings are caused by the client machine’s clock being wrong.

Password Managers

- Separate application and/or extension in your browser.
- Remembers and automatically enters passwords on your behalf.
- Seems possibly **easier** than remembering all your passwords. Is it **more secure**?

A Typical Phishing Page

PayPal - Welcome

http://www.ipaypal.szm.sk/login.html

Google

Najít na stránce Najít další Hlas Autorský mód Všechny obrázky Přizpůsobit šířce 100%

PayPal [Sign Up](#) | [Log In](#) | [Help](#)

Welcome Send Auction Tools

Member Log-In [Forgot your email address?](#)
[Forgot your password?](#)

Email Address

Password

Join PayPal Today
Now Over 100 million accounts

Learn more about [PayPal Worldwide](#)

Shop Without Sharing
Your Financial Information
PayPal. Privacy is built in. [Learn more](#)

How PayPal works.
[Learn more](#)

Text To Buy
X-Men 2
for only \$5.98
[Buy Now](#)

PayPal Mobile
[Learn more](#)

Buyers **eBay Sellers** **Merchants**

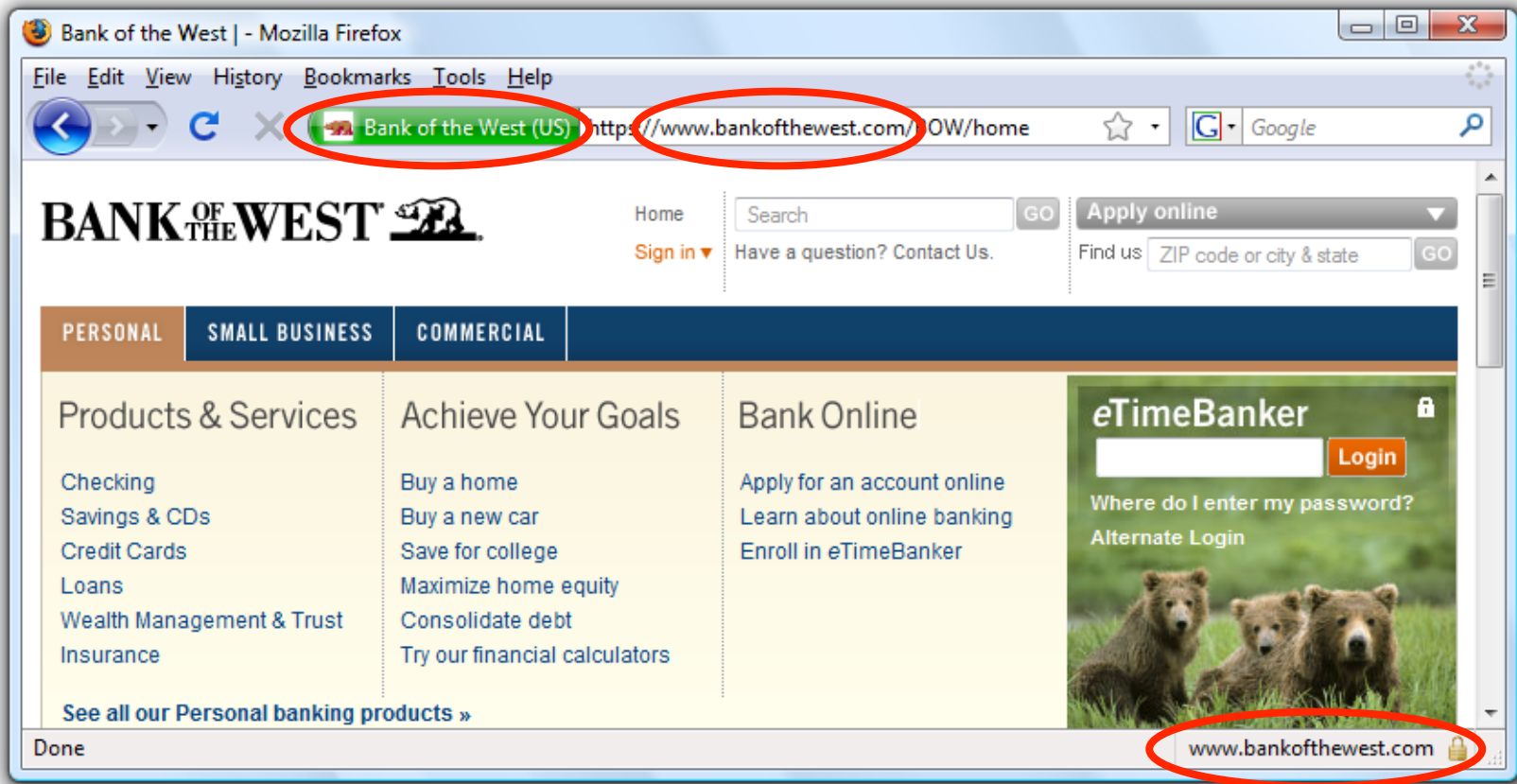
[Send money](#) to anyone with an email address in 55 countries and regions.
PayPal is [free](#) for

[Free eBay tools](#) make selling easier.
PayPal works hard to help [protect sellers](#).

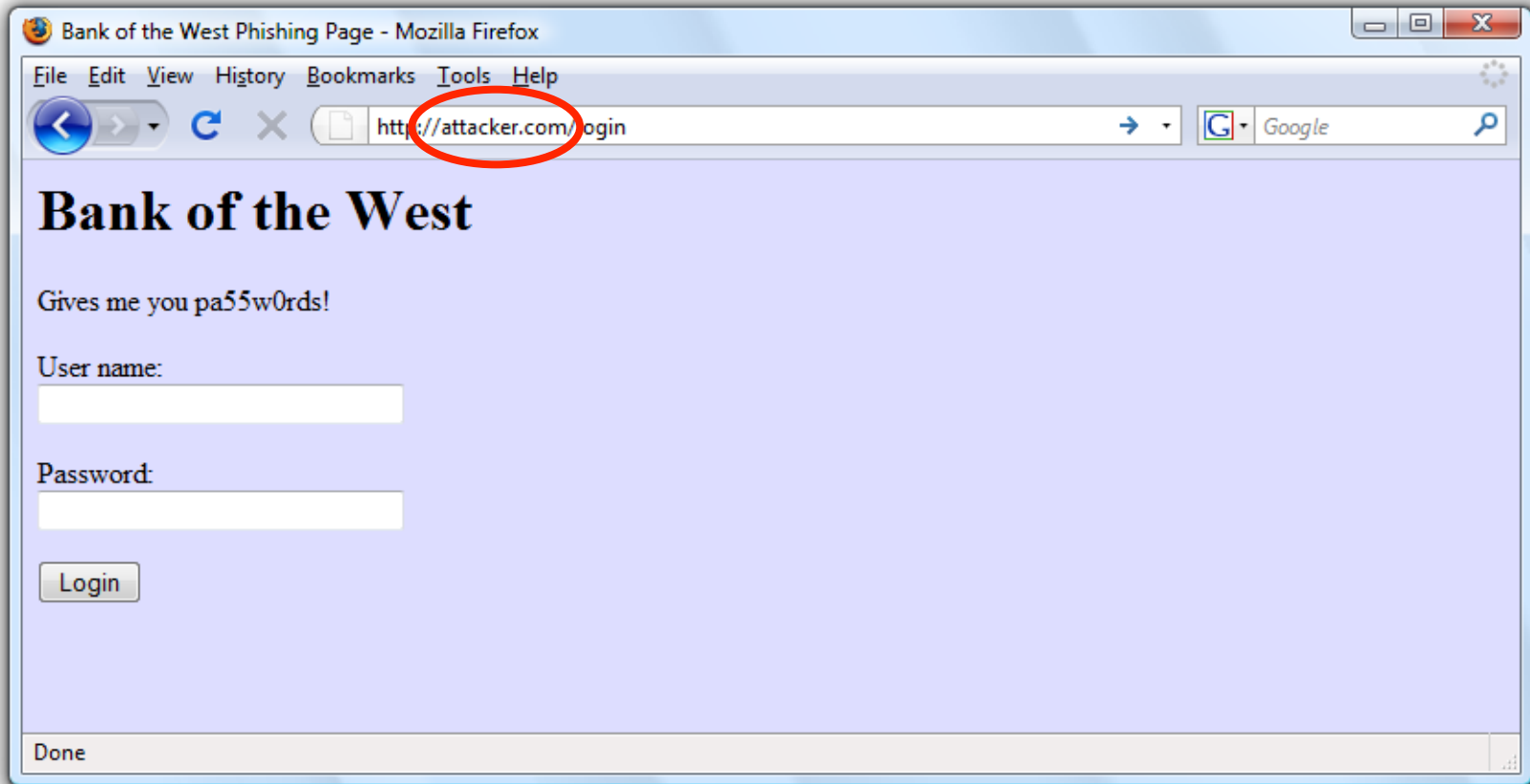
[Accept credit cards](#) on your website using PayPal.
[Compare our solutions](#) to merchant accounts

What's New

Safe to Type Your Password?



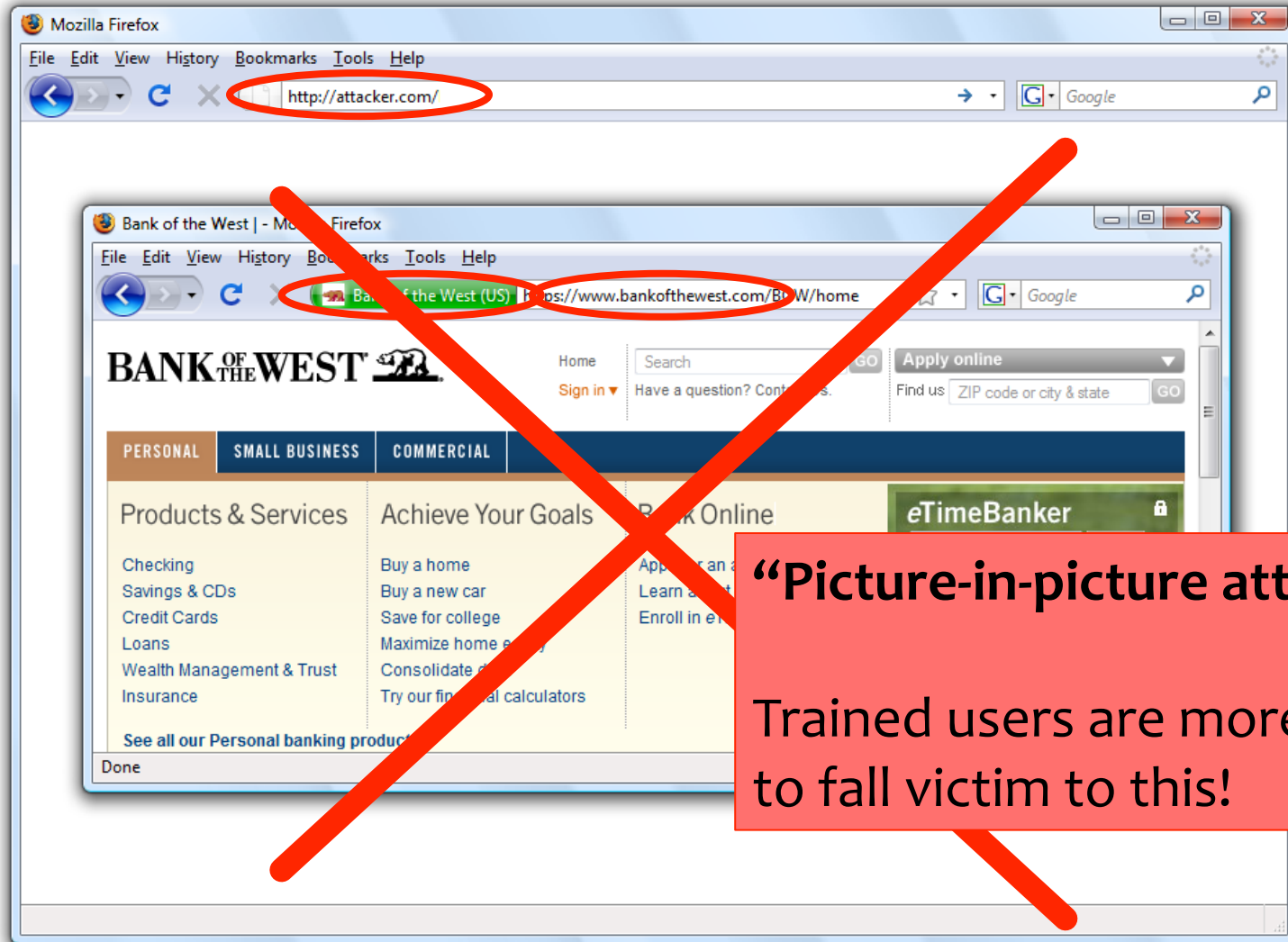
Safe to Type Your Password?



Safe to Type Your Password?



Safe to Type Your Password?



“Picture-in-picture attacks”
Trained users are more likely to fall victim to this!

Question

- **Q.** What are the root causes of usability issues in computer security?

Issue #1: Complexities, Lack of Intuition

Real World



We can see, understand, relate to.

Electronic World



Too complex, hidden, no intuition.

Issue #1: Complexities, Lack of Intuition

- Mismatch between perception of technology and what really happens
 - Public keys?
 - Signatures?
 - Encryption?
 - Message integrity?
 - Chosen-plaintext attacks?
 - Chosen-ciphertext attacks?
 - Password management?
 - ...

Issue #2: Who's in Charge?

Real World



Electronic World



Users want to feel like they're in control.

Where analogy breaks down: *Adversaries* in the electronic world can be *intelligent, sneaky, and malicious*.

Complex, hidden, but *doctors manage*

Complex, hidden, and *users manage*

Issue #2: Who's in Charge?

- Systems developers should help protect users
 - Usable authentication systems
 - Usable privacy settings (e.g., on social media)
 - User-driven access control
- Software applications help users manage their applications
 - Anti-virus software
 - Anti-web tracking browser add-ons
 - PwdHash, Keychain for password management
 - Some say: Can we trust software for these tasks?

Issue #3: Hard to Gauge Risks

“It won’t happen to me!” (Sometimes a reasonable assumption, sometimes not.)

"I remembered hearing about it and thinking that people that click on those links are stupid," she says. "Then it happened to me." Ms. Miller says she now changes her password regularly and avoids clicking on strange links. (Open Doors, by V. Vara, The Wall Street Journal, Jan 29, 2007)

Issue #4: No Accountability

- Issue #3 is amplified when users are not held accountable for their actions
 - E.g., from employers, service providers, etc.
 - (Not all parties will perceive risks the same way)
- Also, recall that a user's poor security choices may affect **other** people
 - E.g., compromise account of user with weak password, then exploit a local (rather than remote) vulnerability to get root access

Issue #5: Annoying, Awkward, or Difficult

- Difficult

Remembering 50 different “random” passwords

Schneier on Security

A weblog covering security and security technology.

[« The Emergence of a Global Infrastructure for Mass Registration and Surveillance | Main | PDF Redacting Failure »](#)

May 02, 2005

Users Disabling Security

It's an old story: users disable a security measure because it's annoying, allowing an attacker to bypass the measure.

A [REDACTED] accused in a deadly courthouse rampage was able to enter the chambers of the judge slain in the attack and hold the occupants hostage because the door was unlocked and a buzzer entry system was not activated, a sheriff's report says.

Security doesn't work unless the users want it to work. This is true on the personal and national scale, with or without technology.

Issue #6: Social Issues



- Public opinion, self-image
 - Only “nerds” or the “super paranoid” follow security guidelines
- Unfriendly
 - Locking computers suggests distrust of co-workers
- Annoying
 - Sending encrypted emails that say, “what would you like for lunch?”

Issues with Usability

1. Lack of intuition
 - See a safe, understand threats. Not true for computers.
2. Who's in charge?
 - Doctors keep your medical records safe, you manage your passwords.
3. Hard to gauge risks
 - “It would never happen to me!”
4. No accountability
 - Asset-holder is not the only one you can lose assets.
5. Awkward, annoying, or difficult
6. Social issues

Question

- **Q.** What approaches can we take to mitigate usability issues in computer security?

Response #1: Education and Training

- Education:
 - Teaching technical concepts, risks
- Training
 - Change behavior through:
 - Drill
 - Monitoring
 - Feedback
 - Reinforcement
 - Punishment
- May be part of the solution – but not the solution

Response #2: Security Should Be Invisible

- Security should happen
 - Naturally
 - By Default
 - Without user input or understanding
- Recognize and stop bad actions
- Starting to see some invisibility
 - SSL/TLS
 - VPNs
 - Automatic Security Updates
 - User-driven access control

Response #2: Security Should Be Invisible

- “Easy” at extremes, or for simple examples
 - Don’t give everyone access to everything
- But hard to generalize
- Leads to things not working for reasons user doesn’t understand
- Users will then try to get the system to work, possibly further reducing security

Response #3: “3 Word UI”: “Are You Sure?”

- Security should be invisible
 - Except when the user tries something dangerous
 - In which case a warning is given
- But how do users evaluate the warning? Two realistic cases:
 - Always heed warning. But then you need to only give warnings when there’s a real problem.
 - Always ignore the warning. If so, then how can it be effective?

Response #4: Focus on Users, Use Metaphors

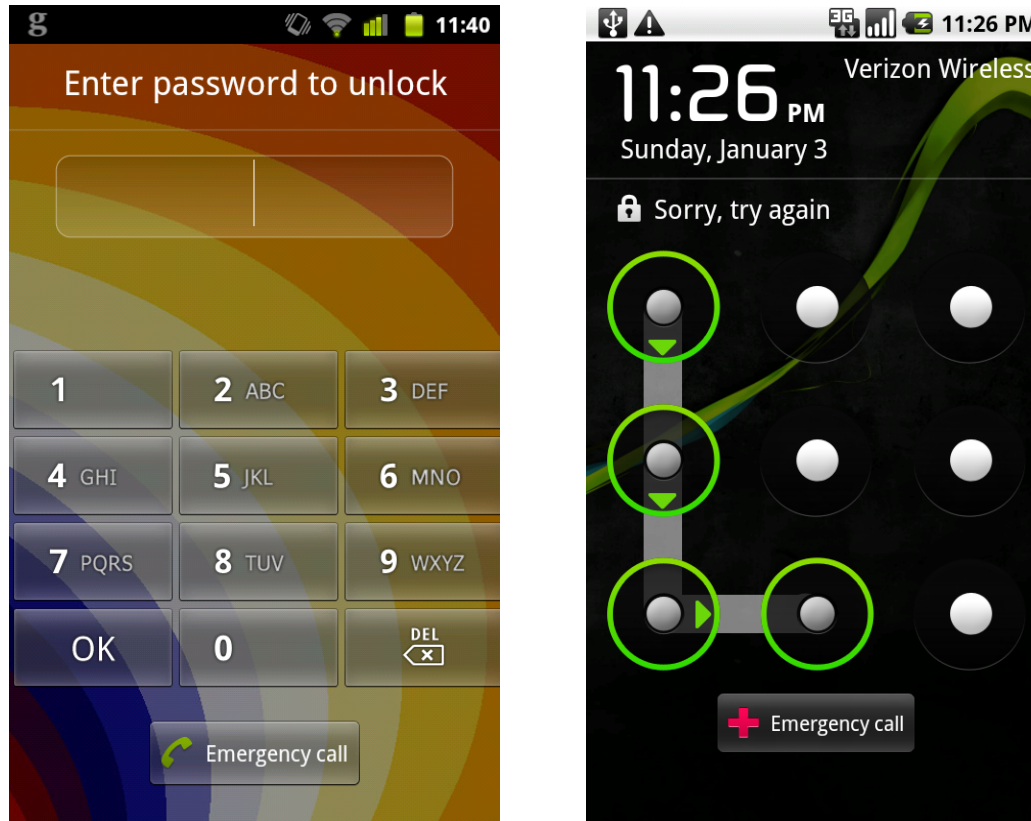
- Clear, understandable metaphors:
 - Physical analogs; e.g., red-green lights
- User-centered design: Start with user model
- Unified security model across applications
 - User doesn't need to learn many models, one for each application

Response #5: Least Resistance

- “Match the most comfortable way to do tasks with the least granting of authority”
 - Ka-Ping Yee, [Security and Usability](#)
- Should be “easy” to comply with security policy
- “Users value and want security and privacy, but they regard them only as secondary to completing the primary tasks”
 - Karat et al, [Security and Usability](#)

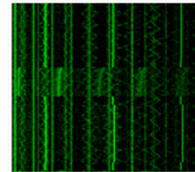
SIDE CHANNELS

Accelerometer Eavesdropping



Aviv et al. "Practicality of Accelerometer Side Channels on Smartphones" ACSAC 2012

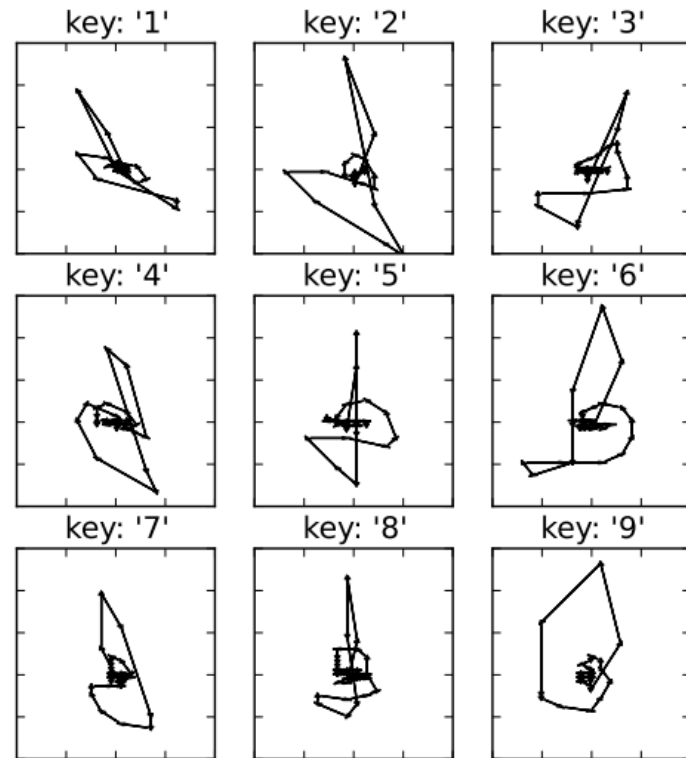
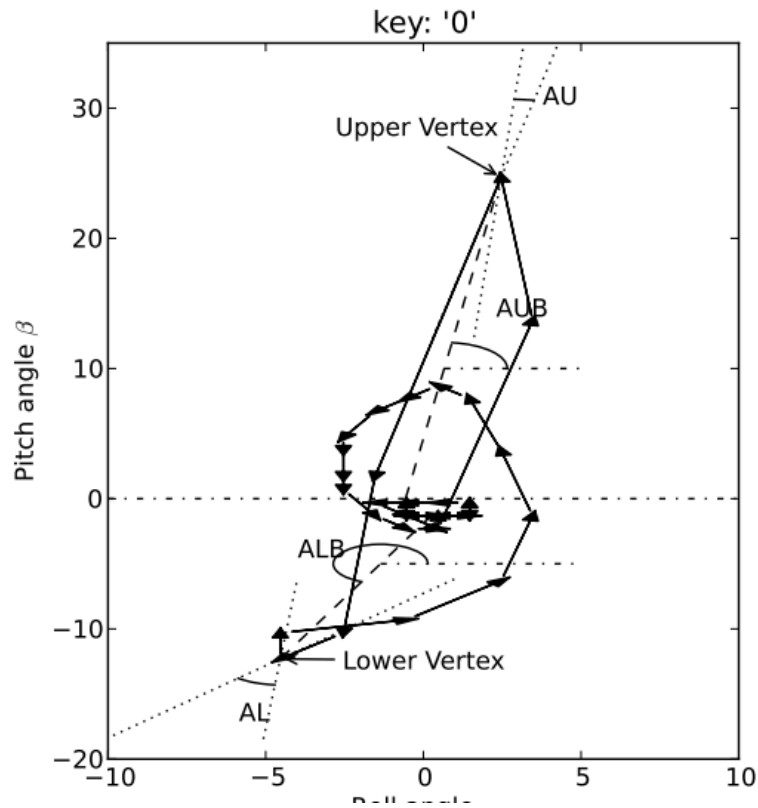
Key Extraction via Electric Potential



Key = 1110111011...

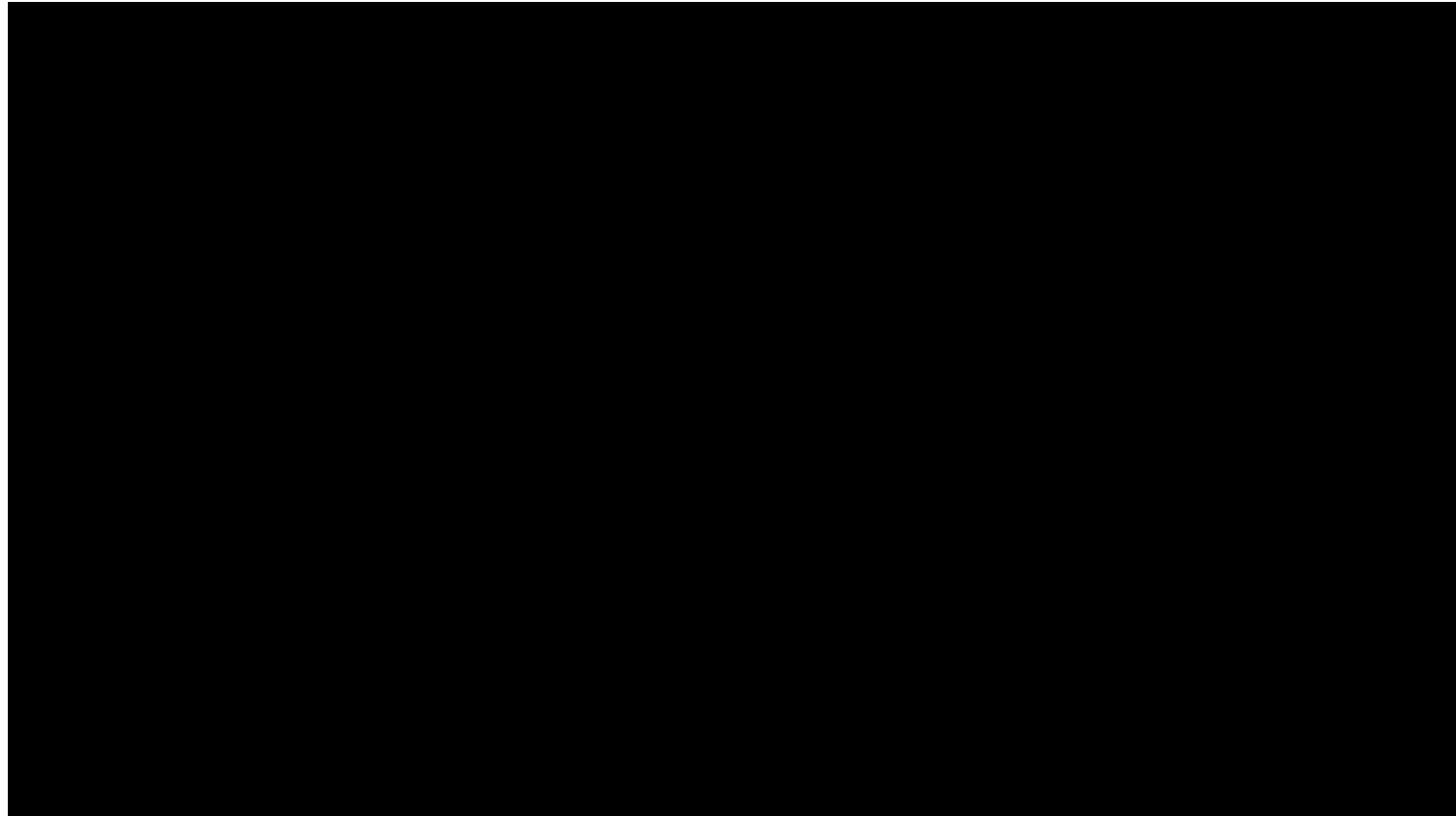
Genkin et al. "Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks On PCs" CHES 2014

More Gyroscope



Chen et al. "TouchLogger: Inferring Keystrokes On Touch Screen From Smartphone Motion" HotSec 2011

Audio from Video



Davis et al. “The Visual Microphone: Passive Recovery of Sound from Video” SIGGRAPH 2014