FRAUD DETECTION IN ONLINE BANKING

The recent shift in security model at Landsbankinn

What shift?

- In the last year we did a significant alteration of our security model in the Personal Online Bank.

- When we talk about security model we mean both the technology used (What we do) and the processes used (How we do it).

43

Nr. 43: Næsta kynslóð í netöryggi

AÐGERÐIR Í TAKT VIÐ NÝJA STEFNU

Landsbankinn tekur upp næstu kynslóð í netöryggi

Nýtt öryggiskerfi Landsbankans fyrir netbanka hámarkar öryggi notandans, gerir auðkennislykla óþarfa, eykur þægindi við notkun netbankans og dregur úr líkum á fjársvikum og annarri misnotkun.

Landsbankinn þinn er heiti á stefnu Landsbankans. Bankinn hefur mikilvægu hlutverki að gegna í samfélaginu. Landsbankinn hefur breyst mikið og mun breytast og eflast enn frekar í takt við stefnuna. Við skiptum ekki um nafn heldur hugarfar.

Kerfi í stöðugri þróun

Auðkennislykill óþarfur

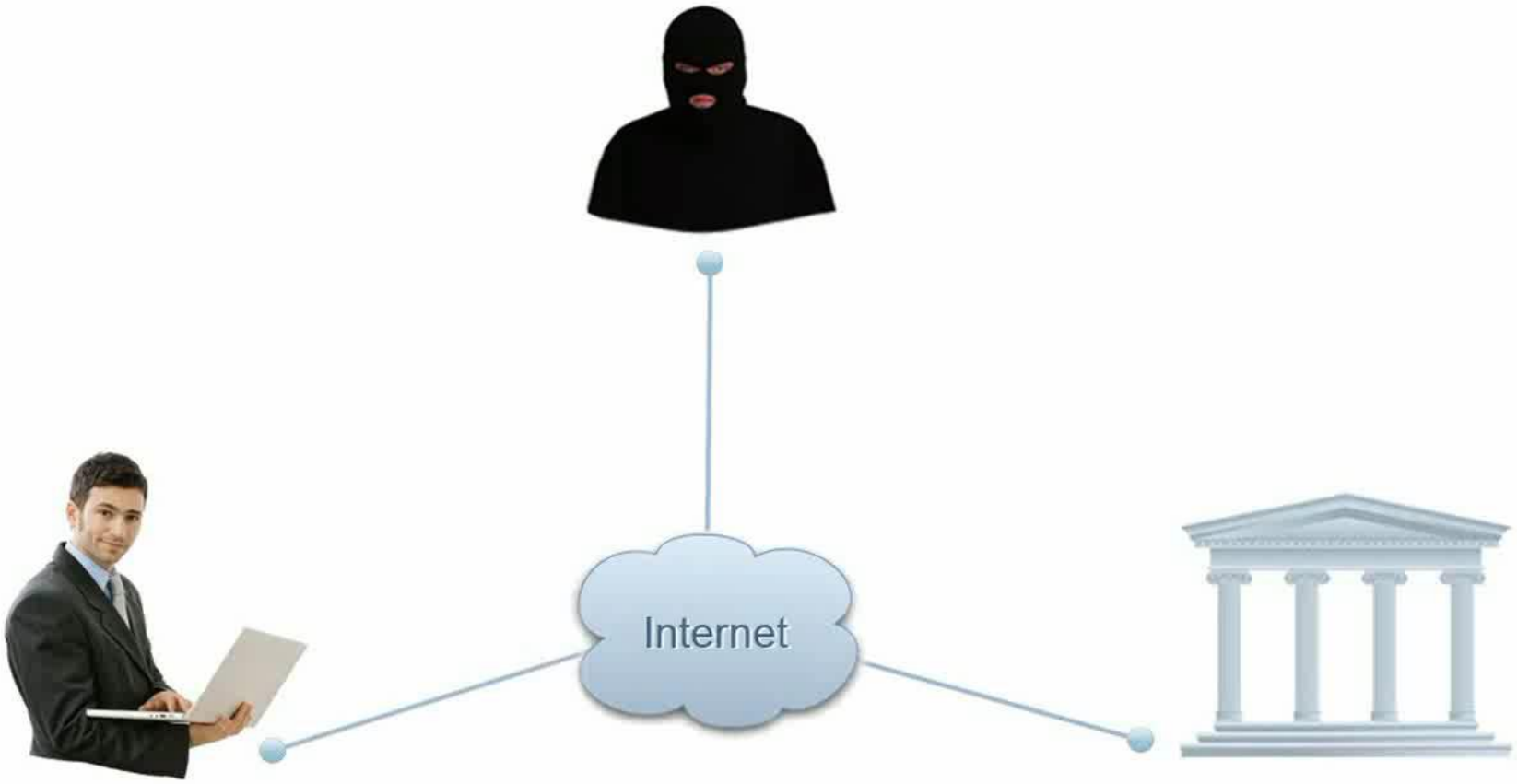
Hámarks öryggi

Í takt við stefnu

What prompted this

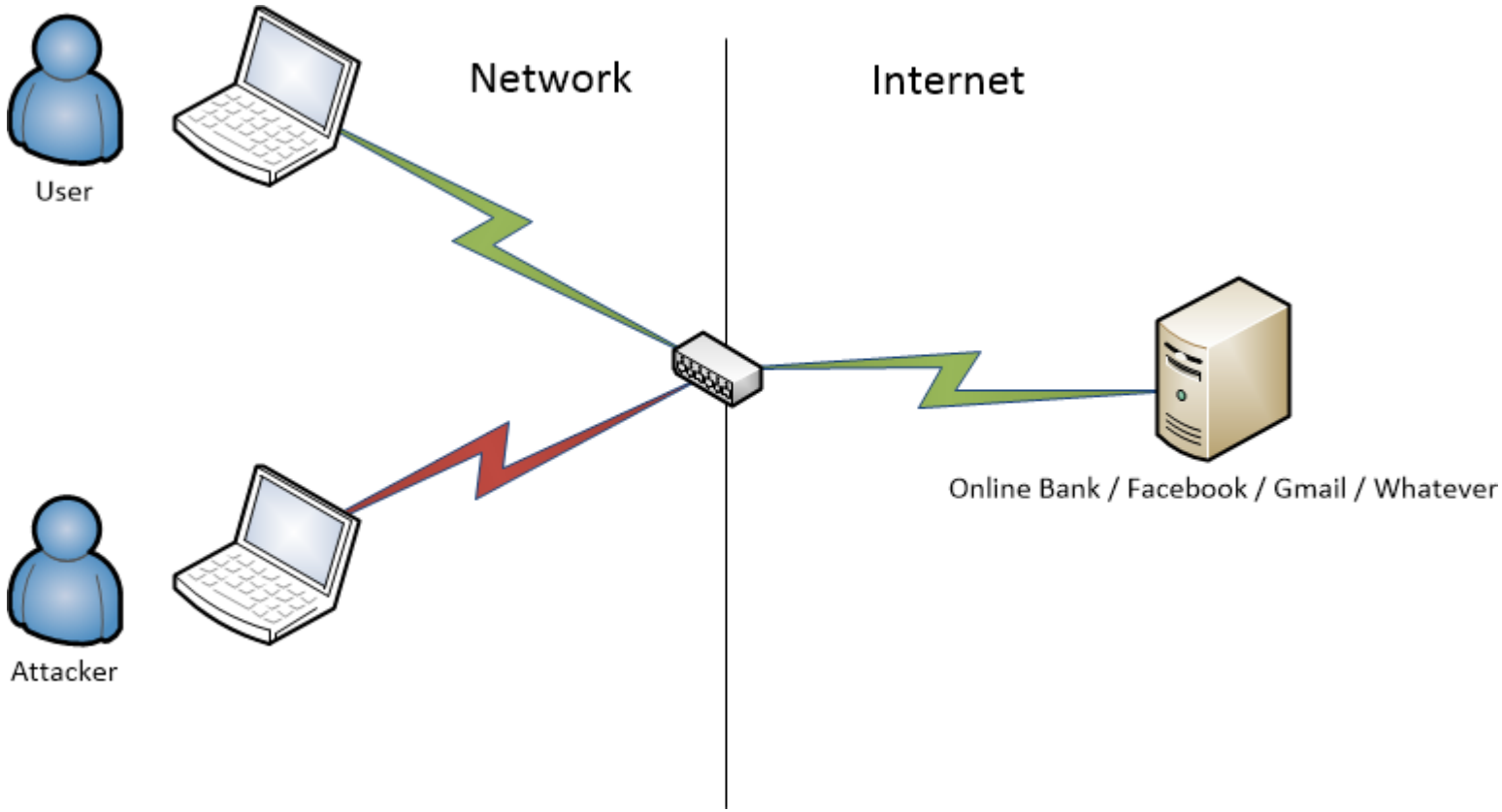
- A shadow grows in the east…
- New MITM attacks!
  - MITB
  - SSL Stripping

Man in the browser



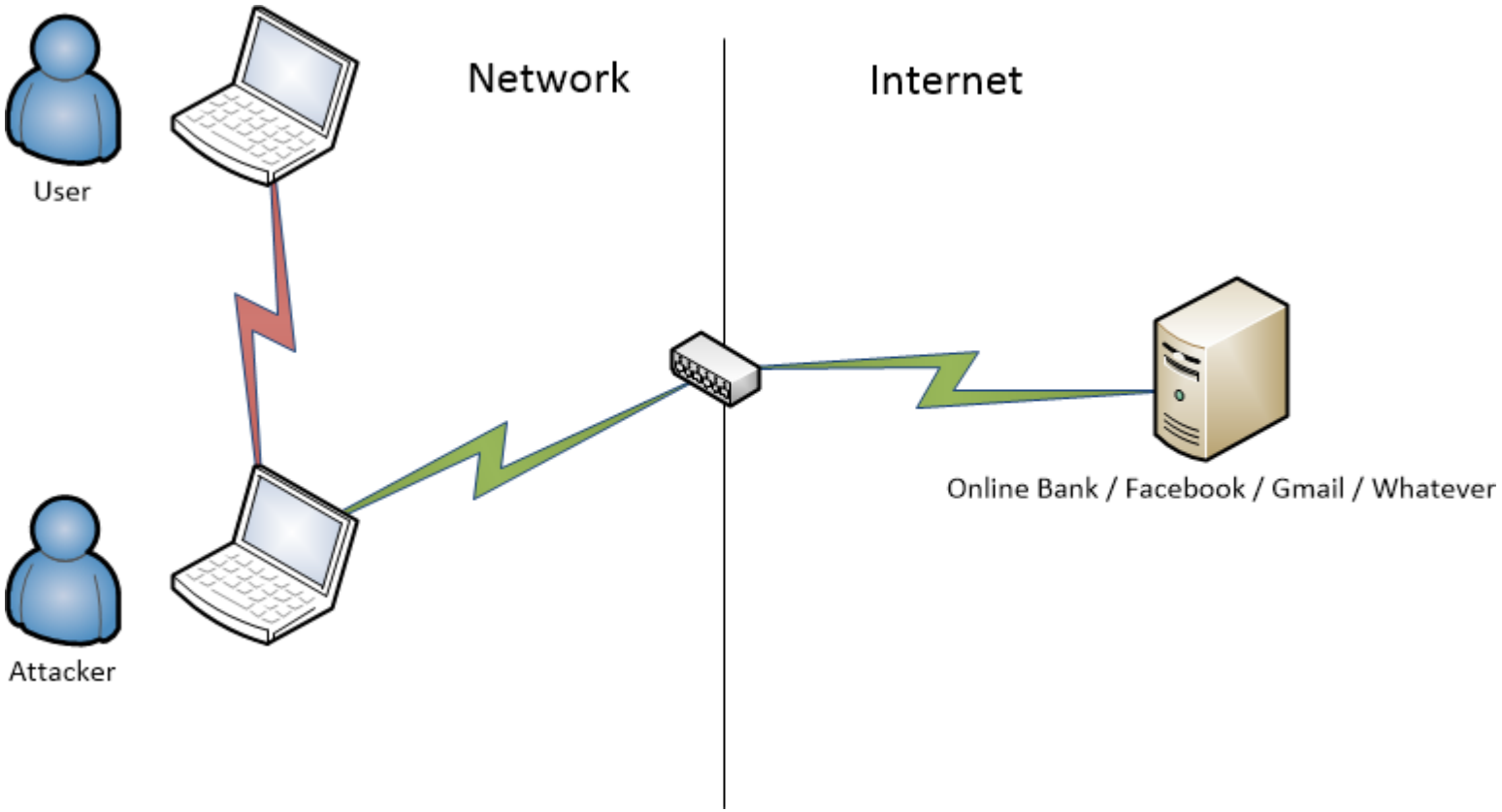
SSL Stripping

- Easy attack involving ARP spoofing



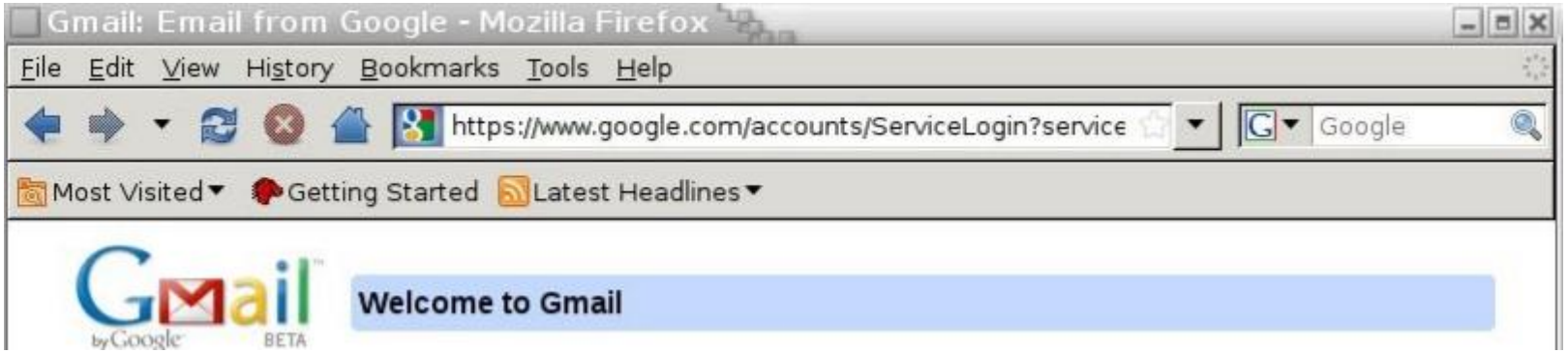
SSL Stripping

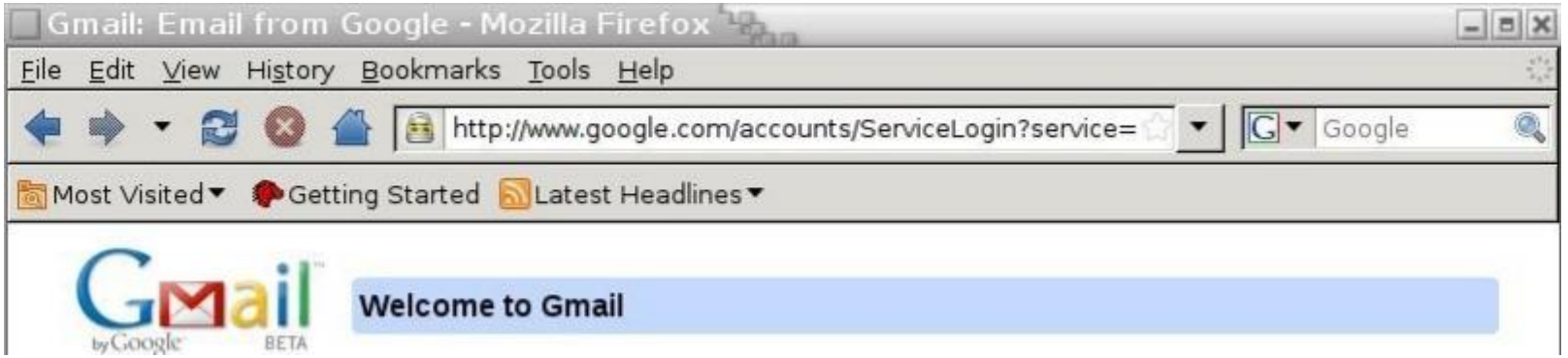
- Server sees a nice secure connection to the client



WHERE'S MY HTTPS

- The social engineering aspect.





These attacks highlight something

- If you go for the “Hard Candy” security model, people will get in to your soft chewy, delicious, sugary core.
- People have a single place to focus their lasers.
- Its an arms race.

“If you’re still racking your brains about how to keep the bad guys out, you’re already way behind,”

Art Coviello - 2013

How do we identify a Fraudster?

Susan Boyle is a Fraudster????

- In the SSL strip attack everything seems normal server side
- In the MITB attack everything seems normal server side

- What is the identifying factor here?

We watch what they do

- In reality how the user LOOKS is only part of the picture.
- We must also pay attention to what the user DOES.
- RSA IPV (Identity Protection and Verification Suite)

- Multi layered approach to security
  - E-Fraud Network – access to information on fraud trends and threats globally
  - Risk – Integration with risk department bringing a human element to the table.

What about the Online Bank

- Integration project took 9 months. 3 Months of planning + 6 months of development and testing.
  - Every member of the development team (even our RSA counterparts) had a child during this period. So we are pretty sure it was 9 months.
- We enabled learning mode in July 2012
- We launched full step up mode in November 2012

User behavior analysis

1. User performs an action
2. Online Bank records various signals and attributes
3. System does a real time risk assessment taking into account:
    1. Action details
    2. Environment details
4. System returns a risk score for that action
5. If risk exceeds a comfortable threshold we will step up the authentication level

Variable Authentication

- One level of authentication is not very user friendly.
  - i.e. Checking balance is a low risk operation and maybe doesn't require much authentication. Making large transactions on the other hand…
- We feel it is a more sophisticated approach to ask for an increase in auth only when and where it is needed.
- You begin your session at the baseline and as you use the product your actions determine our authentication requirements from you.

BUT YOU TOOK AWAY TODOS KEYS

- Yes ok. In reality we migrated the perimeter away from explicit 2 factor auth toward implicit multi factor auth.

- Device fingerprinting.
  - Very common today.

- Again, behavior.

- Plus more

What's next?

- The behavioral analysis gets stronger with time.
- Pluggable authentication means we can quickly add more sophisticated and stronger authentication schemes.
- Constant assessment of the threat landscape using our partners.
- We need to be prepared for the point when Iceland is opened up for unrestricted international transactions.

Questions

- Questions?
- Questions!
- Ask them.
- Now.

Thank you!