NEW SECURITY FLAW DISCOVERED IN WI-FI ROUTERS

YINING WANG

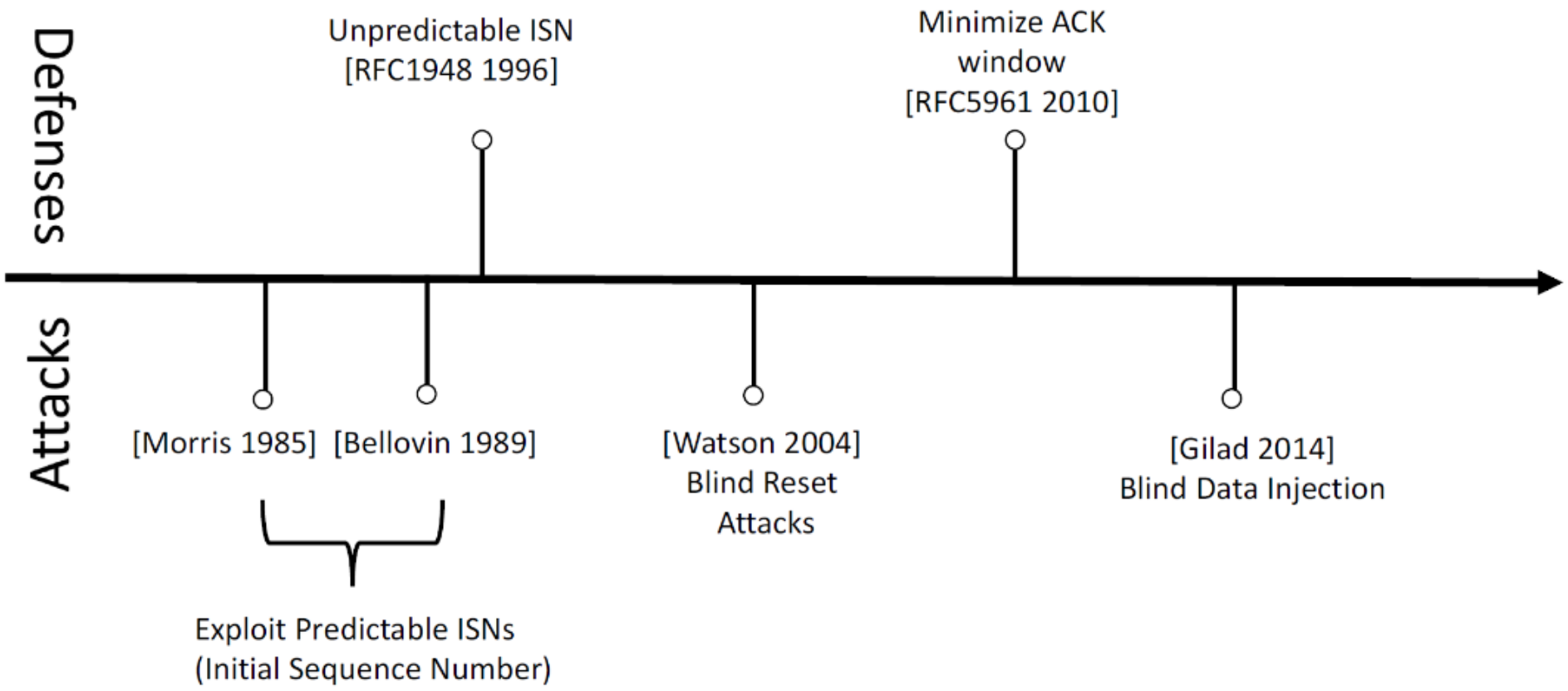
SOME BACKGROUND KNOWLEDGE

- TCP BASICS
- UNIDIRECTIONAL NATURE OF HALF-DUPLEX WIRELESS

TCP: TRANSMISSION CONTROL PROTOCOL

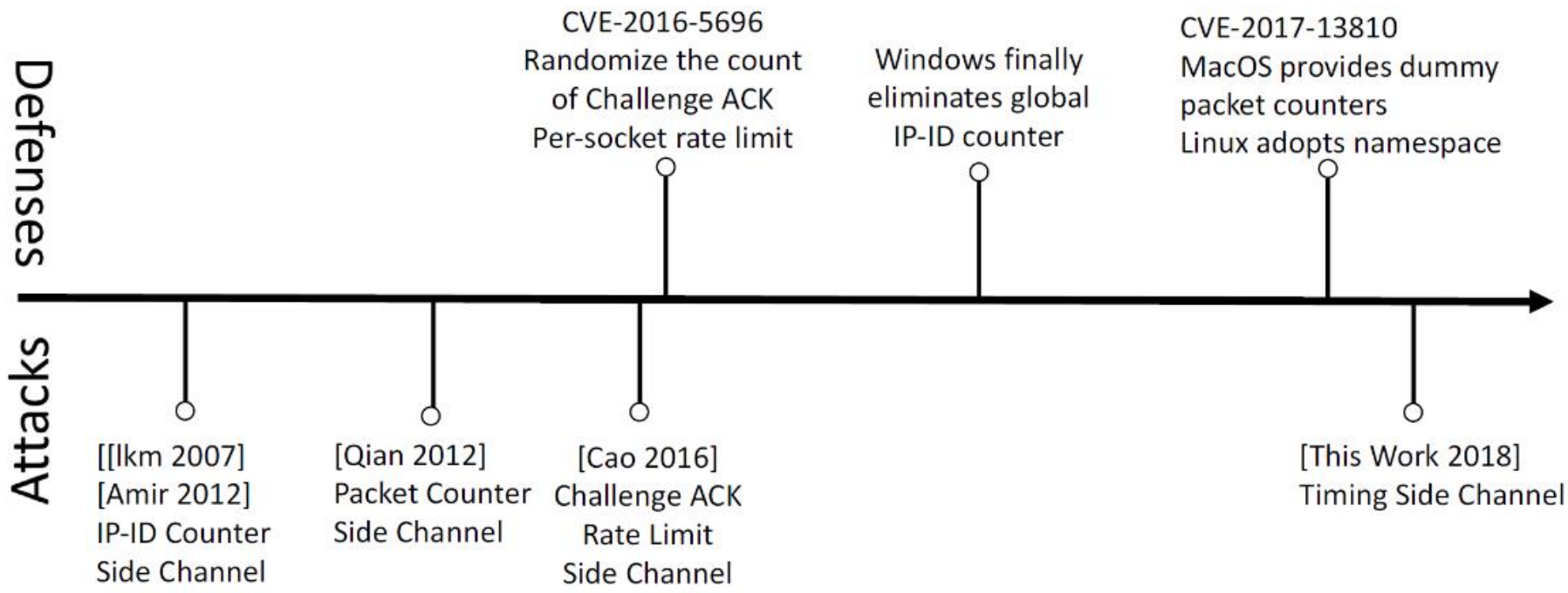
- TCP BREAKS INFORMATION INTO MANAGEABLE CHUNKS
- EACH CHUNK, KNOWN AS A “PACKET,” RECEIVES A NUMBER WITHIN A SEQUENCE UNIQUE TO THAT PARTICULAR COMMUNICATION
- THE FIRST NUMBER OF THE INITIAL SEQUENCE IS RANDOMLY CHOSEN, BUT THE NEXT NUMBERS WILL INCREASE PREDICTABLY, SO THE RECEIVING COMPUTER CAN ARRANGE THEM PROPERLY IF THEY ARRIVE OUT OF ORDER.
- VULNERABILITY

A Time-Line of TCP Injection Attacks



(Initial Sequence Number)

A Time-Line of TCP Injection Attacks (Cont)

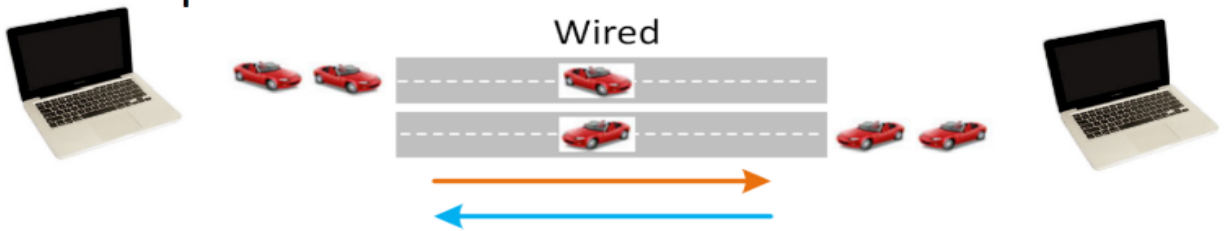


UNIDIRECTIONAL NATURE OF HALF-DUPLEX WIRELESS

Wireless Timing Channel

- **Half-duplex: A fundamental design of wireless protocol**
- **Shared Resource: The half-duplex wireless channel**

Full-duplex:

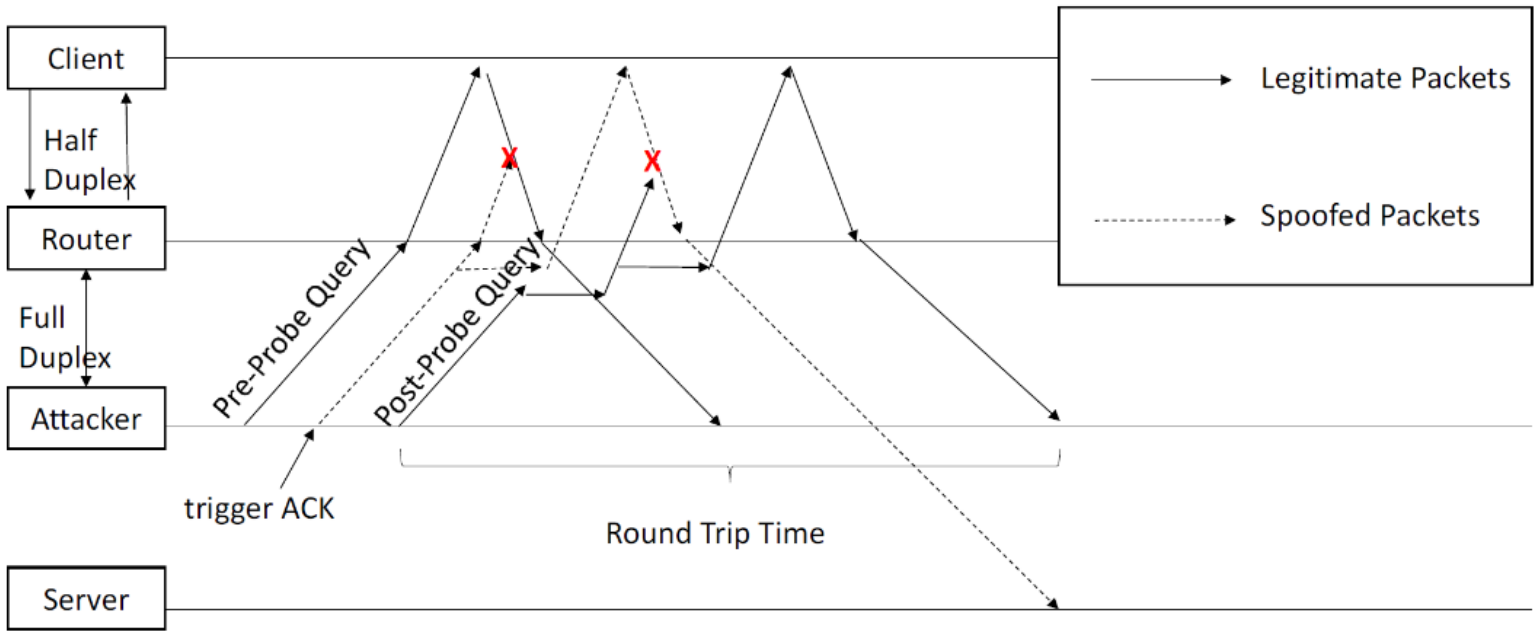


Half-duplex:

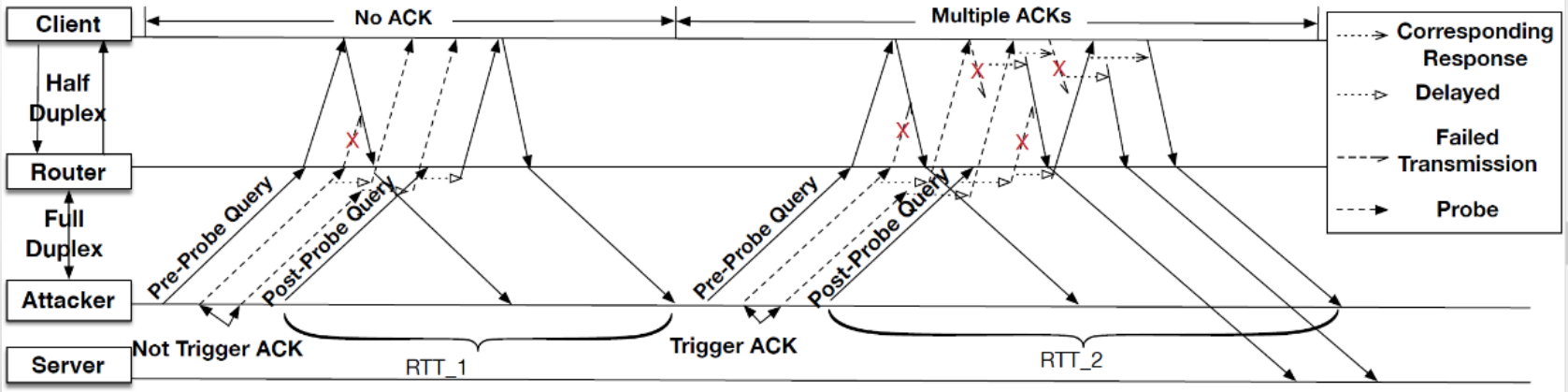
HOW DOES THOSE TWO THINGS WORK TOGETHER?

- COMPUTER WOULD GIVE A RESPONSE AFTER RECEIVING A TCP TRUNK
- TIME RELEVANT TO IF IT IS ‘GOOD’ BECAUSE OF THE HALF-DUPLEX NATURE OF THE WIFE ROUTER

Probing Strategy (Cont)



Timing Difference (Cont)

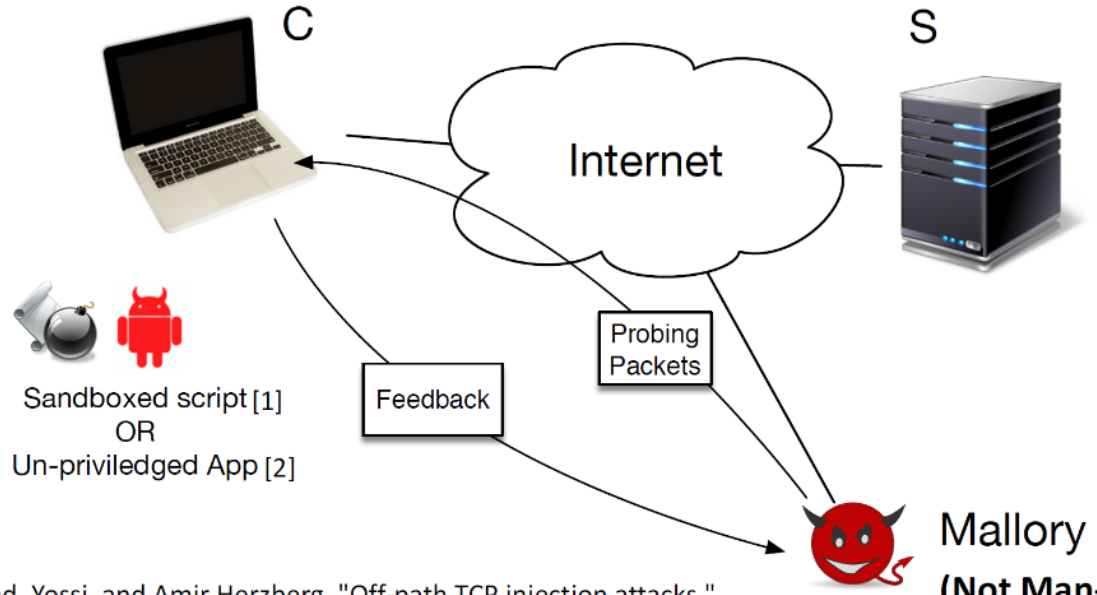


- **More Probing Packets ➔ More Contention ➔ Larger RTTS**

HOW DOES THE ATTACK WORK?

1

Generic Threat Model



[1] Gilad, Yossi, and Amir Herzberg. "Off-path TCP injection attacks."
[2]Qian, Zhiyun, Z. Morley Mao, and Yinglian Xie. "Collaborative TCP sequence number inference attack: how to crack sequence number under a second."

2

An attack using packet counter side channel

inject their own copy of the banking webpage into the browser cache: Web cache poisoning

- HTTPS://WWW.YOUTUBE.COM/WATCH?TIME_CONTINUE=76&V=XT8NYXGZTUW

SOMETHING WE COULD DO

- APPLICATION LAYER: HTTPS AND HSTS
- WIRELESS LAYER: FULL-DUPLEX WI-FI TECHNOLOGY
- DON'T CLICK ON SUSPICIOUS LINKS !

THE END

- OFF-PATH TCP EXPLOIT: HOW WIRELESS ROUTERS CAN JEOPARDIZE YOUR SECRETS, WEITENG CHEN AND ZHIYUN QIAN, UNIVERSITY OF CALIFORNIA, RIVERSIDE (HTTPS://WWW.USENIX.ORG/CONFERENCE/USENIXSECURITY18/PRESENTATION/CHEN-WEITENG)