Wireless Security

Survey by Evi Bernitsas
18-750 Wireless

Definition: Wireless Security

- "Wireless network security primarily **protects a wireless network** from unauthorized and malicious access attempts.
- … Typically, wireless network security is **delivered through wireless devices** (usually a wireless router/switch)
- … which **encrypts and secures** all wireless communication by default."

Common Security Types

Wired Equivalent Privacy (WEP)

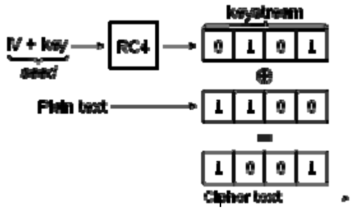
- Security **algorithm** for IEE 802.11
- Part of original 802.11 ratified in 1997 to provide **confidentiality**, which the traditional wired network did not provide
- WEP uses 40 or 104 bit keys.
- WEP has now been replaced by Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA)

- Developed because of weaknesses found in WEP
- WPA also referred to as IEEE 802.11i standard (WPA2 released in 2004)
- Instead of 40 or 104 bit keys, uses Temporal Key Integrity Protocol (**TKIP**)
- TKIP **dynamically generates** new 128-bit key for each packet

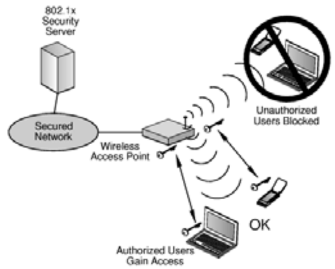
Wired Equivalent Privacy (WEP) Algorithm

- Uses RC4 stream cypher (now unsafe)
- uses 40-bit key (WEP-40) and is concatenated with a 24-bit initialization vector (IV) to form the RC4 key
- This key stream is then used to **encrypt** the plain text using XOR
- This produces the cipher text which is then sent.



Wi-Fi Protected Access (WPA/WPA2) Algorithm

- WPA uses Temporal Key Integrity Protocol (TKIP) uses a unique **key** for each packet that is **dynamically generated** (128 bits)
- WPA2 encrypts the network with a 256-bit key and uses the encryption method called **AES (Advanced Encryption Standard)**
- Includes **message integrity check** to prevent altering and resending of data packets.



A few Security Issues with WPA/WPA2

- **Weak Password**
- **WPA packet decryption:** injection attacks
- **No forward secrecy:** once an adverse person discovers the pre-shared key, they can decrypt all encrypted Wi-Fi packets transmitted in the future and even past
- **Predictable Group Temporal Key (GTK):** The random number generator is not entirely random

Wireless Security Publication #1: *Keystroke Recognition Using Wi-Fi Signals*

Kamran Ali, Alex X. Liu, Wei Wang, Muhammad Shahzad

Dept. of Computer Science and Engineering, Michigan State University, USA
State Key Laboratory for Novel Software Technology, Nanjing University, China

Wireless Security Publication #1: Keystroke Recognition Using Wi-Fi Signals

- Keystroke privacy is critical
- WiFi signals can be exploited to recognize keystrokes
- While typing a certain key, your hands and fingers move in a certain formation and direction, which generates a unique pattern in the time series of **Channel State Information** (CSI) values.
- This produces a CSI waveform
- This paper proposes a system to recognize keystrokes called **WiKey**.
- WiKey uses simply a router (sender) and a laptop (receiver) and achieves 97.5% detection rate for detecting keystroke, and 93.5% accuracy for continuously typed sentences.

Definition: Channel State Information (CSI)

In wireless communications, channel state information **(CSI)** refers to known **channel properties** of a communication link. This information describes how a **signal propagates from the transmitter to the receiver** and represents the combined effect of, for example, scattering, fading, and power decay with distance.

Typical keystroke recognition approaches

- **Acoustic emission**: different keys produce different typing sounds OR sounds from keys arrive at surrounding smartphones at different times.
- **Electromagnetic emission**: electromagnetic emanations from the circuit underneath are different for each key.
- **Computer Vision**: recognize keystrokes with a camera.

WiKey System

- WiFi signals can be exploited based on how keystrokes affect how the signal propagates (affects the Channel State Information (CSI))
- They call this the **CSI-waveform**
- Because of high data rates, WiFi cards provide enough CSI values within the duration of a keystroke to construct a high resolution CSI-waveform for each keystroke

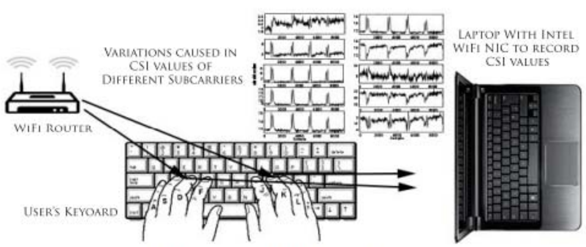


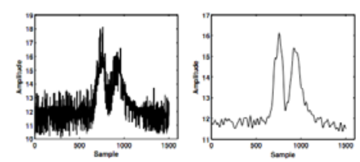
Figure 1: WiKey System

Technical Challenges

1. Finding the beginning and the end points of individual keystrokes

2. Distinguishing features for each of the 37 keys

   - Typical features such as power, mean amplitude, rate of change and signal energy cannot be used because these are almost identical between keys.
   - Discrete Wavelet Transform (DWT) is used to reduce the number of samples but still preserve the **shape**. Classification is done based on shape of the wave.



(a) Original time series (b) Filtered time series

Figure 2: Original and filtered CSI time series

Steps to filtering CSI-Waveform

1. Channel State Information: All Information about the channel state

2. Noise Removal: Low Pass Filtering

1. Frequencies due to hand movements are between 3Hz and 80Hz

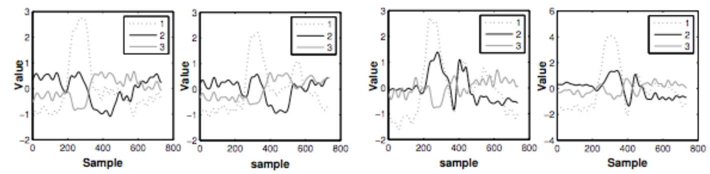
3. Noise Removal: PCA Based Filtering

1. maximizes variance of data
2. minimizes mean squared distance

4. Keystroke Extraction

5. Feature Extraction

Keystroke Waveforms



(a) Keystroke waveforms for key **i** (b) Keystroke waveforms for key **o**

Conclusion:
Keystroke Recognition Using Wi-Fi Signals

- WiKey achieves 97.5% detection rate for detecting keystroke, and 93.5% accuracy for continuously typed sentences.
- This only works in a controlled environment.
- Future testing will be conducted in harsher wireless environments.

Wireless Security Publication #2: *Acoustic Eavesdropping through Wireless Vibrometry*

Teng Wei, Shu Wang, Anfu Zhou and Xinyu Zhang

University of Wisconsin - Madison, Institute of Computing Technology, Chinese Academy of Sciences

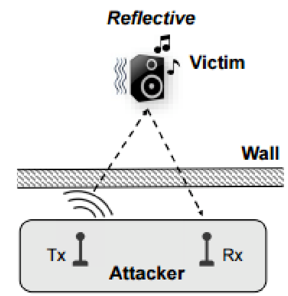
Wireless Security Publication #2:

Acoustic Eavesdropping through Wireless Vibrometry

- **Acoustic eavesdropping** is used to decode a lot of subtle acoustic sounds like keystrokes and printers, but is **only useful** if the microphone is in close **proximity**.
- Loudspeakers refer to anything from large entertainment systems to your PC or smartphone loudspeakers
- Loudspeakers cause **acoustic vibration**
- This paper is based on decoding noises emitted by loudspeakers from a **distance**
- The vulnerability lies in the translation between acoustic vibration and radio signal fluctuation.
- Contaminated radio waves can be captured by a receiver and decoded to find the original sound coming from the loudspeakers

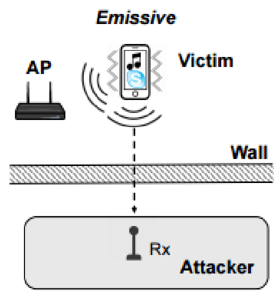
Reflective Vibrometry

- Adversary: pair of radio transmitter and receiver
- Transmitter continuously sends radio signals as receiver decodes the sound vibration from the signals disturbed by the loudspeaker vibration



Emissive Vibrometry

- Adversary: radio receiver
- Target loudspeaker is located near a WiFi radio on the same platform (smartphone)
- Loudspeaker's motion causes tiny variation in the WiFi radio's outgoing signals, which is then heard and recovered by the receiver



Basic Audio-radio Transformation (ART) Algorithm

- Audio vibrations modulate the radio signal magnitude/phase
- Harnesses the received signal strength (RSS) and phase information to "demodulate" acoustic signals from the target loudspeaker.
  - Isolates irrelevant radio signal components
  - extrapolates the audio signals
  - projects them onto the time-domain (which is audible to humans)

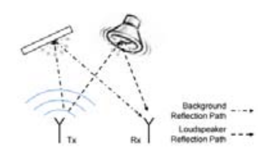


Figure 2: Illustration of loudspeaker modulation and multipath effects of reflective radio vibrometry.

Demodulating Transformed Audio

- Get one audio sample from every m radio samples
- For each radio sample, we segment it into S segments containing m samples.
- FFT - time-frequency domain translation to get this closer to human hearing
- Bandpass filter to keep only frequencies between 20 Hz and 1500 Hz (range of human voice)

Algorithm 1 Decoding the audio that is modulated by ART

INPUT: received radio samples $y[t]$
OUTPUT: recovered audio samples $d^*[s]$
/*Get one audio sample from every m radio samples*/
foreach segment s in set $[0{:}S)$
    $y_s \leftarrow y[sm+1,(s+1)m]$ /*Segment radio signals*/
    $z(v) \leftarrow \sum_{u=1}^{m} y_s(u) e^{\frac{-i2\pi vu}{m}}$ /*FFT analysis*/
    $g(s) \leftarrow \left|\frac{z(\lfloor \frac{f_c}{f_b} \times m \rfloor)}{m}\right|^2$ /*Pick RSS of CW's freq.*/
endforeach
$d^* \leftarrow filter_{bandpass}(g)$ /*Filter out the DC component*/

Conclusion:
Experimental Validation of Accuracy vs. Microphone

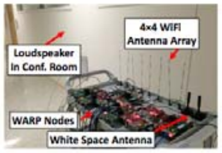


Figure 15: ART hardware platform. Testing ART outside a conference room.

Figure 16: Testing ART performance. Loudspeaker is inside a soundproof room.

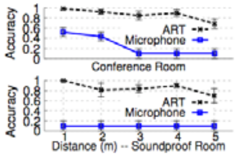


Figure 17: Through-wall recognition accuracy of ART compared with a microphone.

Wireless Security Publication #3:
SafeSlinger: Easy-to-Use and Secure Public-Key Exchange

Michael Farb - CyLab / CMU
Yue-Hsun Lin - CyLab / CMU
Tiffany Hyun-Jin Kim - CyLab / CMU
Jonathan McCune - Google Inc.
Adrian Perrig- ETH Zürich, CyLab / CMU

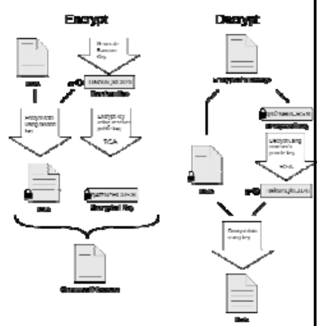
Wireless Security Publication #3:

SafeSlinger: Easy-to-Use and Secure Public-Key Exchange

- Security on the internet is entirely a **leap of faith for users** without more advanced knowledge
- **SafeSlinger** is a system currently on **Android and iOS apps**
- It allows users to **exchange public keys** between each other to support **secure messaging** and file exchange
- Also provides an **API** for importing **applications**' public keys into the user's contact information
- SafeSlinger proposes "**secure introductions**" to help ensure that messages sent between two people with the same public key are safe from attackers
- https://www.youtube.com/watch?v=IFXL8fUqNKY

Comparable Security Protocols

- SSL/TLS (Secure Socket Layer / Transport Layer Security)
  - Uses generated unique keys and TLS handshake protocol, and uses a message authentication code (MAC) to prevent altered data.
  - **Drawbacks**: Many known attacks including timing attacks on padding and RC4 (keystream) attacks. Security):
- PGP (Pretty Good Privacy)
  - Encrypts data using **random key**, encrypts key using **public key** from receiver.
  - Receiver decrypts **random key** using **private key** and uses that to decrypt the data.
  - **Drawbacks**:
    - **Key maintenance** is difficult administratively
    - Organizations cannot secure **large files** this way
    - No **email receipt** confirmation
    - Cannot scan incoming PGP email with **anti-virus**



PGP

Goals of SafeSlinger

- **Scalable:** can be done in groups
- **Easy to use:** usability of interface
- **Portability:** support heterogeneous platforms to enable interactions among smartphones of different manufacturers and OS (operating systems)
- **Authenticity:** each user should be able to obtain correct contact information from other users
- **Secrecy:** contact information is only available to other group members after the completion of a physical exchange to authenticate

Multi-Value Commitments

- Cryptographic commitment protocol is used to lock an entity to the value V without letting them know what V is
- Ex. **C = H(V,R)**
- C is the commitment value, H is the cryptographic hash function that is **one-way, collision free** and has **pseudo-random** output if R is a random and unpredictable one-time use input
- V cannot be inferred from C
- Multi-Value: **C = H(H(V1) || H(V2))**
- (|| = concatenated with)

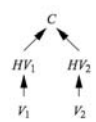
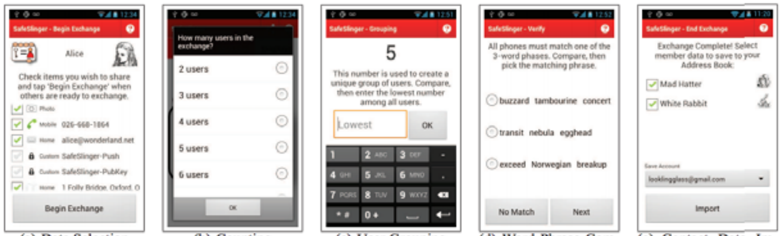


Figure 1: Multi-value commitment structure for authenticating and disclosing either V_1 or V_2.

Possible Attacks on SafeSlinger

- **Malicious Bystander:** someone who overhears the non-digital agreement and can attack the protocol by controlling the local wireless communication performing **Man-in-the-Middle attack**
- **Malicious Group Member:** A member who impersonates someone else by injecting incorrect information for another user.
- **Information Leakage after protocol abort:** Adversary may be able to cause a protocol abort and trigger leakage.

Secure Information Exchange Sequence



(a) Data Selection (b) Counting (c) User Grouping (d) Word Phrase Comparison (e) Contact Data Import

Figure 5: Secure contact information exchange sequence.

Works Cited

1. Ali, Kamran, Alex Xiao Liu, Wei Wang, and Muhammad Shahzad. "Keystroke Recognition Using WiFi Signals." Proceedings of the 21st Annual International Conference on Mobile Computing and Networking - MobiCom '15 (2015): n. pag. Web.

2. Wei, Teng, Shu Wang, Anfu Zhou, and Xinyu Zhang. "Acoustic Eavesdropping through Wireless Vibrometry." Proceedings of the 21st Annual International Conference on Mobile Computing and Networking - MobiCom '15 (2015): n. pag. Web.

3. Farb, Michael, Yue-Hsun Lin, Tiffany Hyun-Jin Kim, Jonathan Mccune, and Adrian Perrig. "SafeSlinger." Proceedings of the 19th annual international conference on Mobile computing & networking - MobiCom '13 (2013): n. pag. Web.

4. "What is Wireless Network Security? - Definition from Techopedia." Techopedia.com. N.p., n.d. Web.

5. "Limitations of Securing Email With PGP." CitizenTekk. N.p., 28 Sept. 2016. Web.

6. https://www.cs.cmu.edu/~bapoczos/other_presentations/PCA_24_10_2009.pdf

7. "Wireless security." Wikipedia. Wikimedia Foundation, 27 Apr. 2017. Web.